FORTALECIMIENTO DEL MODELO DE SEGURIDAD DE RED Y CONTROL DE ACCESO LÓGICO PARA UNA ENTIDAD

PRESENTADO POR:
JUAN CARLOS MORENO MORENO
JUAN CAMILO GÓMEZ ECHEVERRÍA

ASESOR TÉCNICO DE PROYECTO:
ING. EDUARDO CHAVARRO OVALLE

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMÁTICAS
BOGOTÁ, COLOMBIA
JULIO 2020

AGRADECIMIENTO

Primero que todo, queremos agradecer a Dios por permitirnos estar donde estamos, por darnos la oportunidad de estudiar esta Especialización en esta Institución Educativa y darnos las ganas y las herramientas necesarias para sacarla adelante.

No fue un proceso sencillo, por lo que también queremos agradecer a cada una de las personas que nos acompañaron durante este tiempo, nuestros padres, familia, y compañeros de estudio que siempre fueron un apoyo importante y constante.

Por último, queremos agradecer a los profesores por compartir con nosotros su conocimiento y sus experiencias para demostrar la aplicabilidad de esta Especialización y a lo que nos seguiremos enfrentando en el futuro.

Gracias a todos aquellos que aportaron algo de sí mismos para ayudarnos a nosotros a culminar este proyecto y esta Especialización.

DEDICATORIA

A mi hijo Juan Sebastián Moreno Jiménez, no he conocido alegría tan grande como cuando te vi por primera vez y verte crecer es todo un privilegio.

A mi esposa Magda Jiménez quien me brindó su amor, su cariño, su estímulo y su apoyo constante, que me mostro otra visión del mundo y me dio fortaleza para continuar cuando mis fuerzas flaquearon.

A mis padres, Gloria Sofía Moreno, Carlos Arturo Moreno y mi hermano Luis Fernando Moreno, siempre estaré agradecido por permitirme nacer entre ustedes, la fortuna más grande es tenerlos conmigo, agradeciendo eternamente cada uno de los valores que me inculcaron.

A ese ser superior que impulsa en mi interior los sentimientos de alegría, tranquilidad y serenidad en cada momento de debilidad y da ese empujón para culminar con tanto esfuerzo.

A mi compañero y amigo Juan Camilo Gómez por acompañarme en este esfuerzo y brindarme su conocimiento para la culminación de este proyecto.

Juan Carlos Moreno Moreno

Quiero dedicar este esfuerzo a toda mi familia, a los que me acompañaron con su presencia y su voz de aliento, y a los que no pudieron estar presentes para ver este logro en mi vida profesional, pero que de algún modo sé que me acompañan y están orgullosos.

Quiero también hacer mención especial a mi compañero Juan Carlos Moreno Moreno, quien me apoyó y me compartió su conocimiento para poder llevar a cabo este proyecto.

Juan Camilo Gómez Echeverría.

Resumen

Este documento presenta el trabajo realizado para llevar a cabo el cumplimiento de los objetivos propuestos desde el inicio del proyecto. Se muestra el análisis y las recomendaciones hechas para reforzar y limitar el acceso a los recursos de la entidad asegurando los dispositivos de red LAN y WLAN, e implementando un demo de una solución NAC catalogada como una de las mejores en el mercado.

El análisis de vulnerabilidad se ha desarrollado bajo un procedimiento de descubrimiento, identificación y clasificación de los riesgos encontrados para posteriormente proponer un plan de remediación basado en la elaboración de una plantilla de aseguramiento aplicable a equipos de red, los cuales constituyen la columna vertebral de toda infraestructura de tecnología. Por otro lado, la idea de implementar un demo de la solución NAC elegida, es con el fin de brindar a la entidad una muestra y unas recomendaciones que se deben tener en cuenta en el momento en el que se quiera expandir la implementación del control de acceso a toda la red.

Palabras Clave – Endurecimiento, control de acceso, vulnerabilidad, riesgo, aseguramiento, defensa, escaneo, LAN, WLAN, VLAN, 802.1X, política de seguridad, dispositivos de red.

Abstract

This document presents the accomplish work in order to comply the goals proposed at the beginning of the project. It shows the analysis and recommendations made to strengthen and limit the access to the entity resources securing the LAN and WLAN devices, and implementing a NAC solution demo kown as one of the best in the market.

The vulnerability analysis was developed in a process of detection, identification and clasification of found risks to later propose a remediation plan based on the elaboration of a secure template which can be apply to network devices, the ones that are the spinal column of an IT infrastructure. In the other side, the idea of implementing a demo of the chosen NAC solution is to give the entity a sample and recommendation that they would have to take into account at the moment when they want to expands the implementation of the access control around the network.

Keywords – Hardening, access control, vulnerability, risk, secure, defense, scanner, LAN, WLAN, VLAN, 802.1X, security policy, network devices.

Contenido

Lista de Figuras

Lista de Tablas

1. Título

FORTALECIMIENTO DEL MODELO DE SEGURIDAD DE RED Y CONTROL DE ACCESO LÓGICO PARA UNA ENTIDAD

2. Introducción

El avance tecnológico en las empresas es imparable, todos los sectores productivos se encuentran en un momento en que la inversión en tecnología es indispensable a la hora de soportar el crecimiento y la optimización de recursos. Este crecimiento hace referencia a la red de comunicación y al aumento de dispositivos interconectados. Por ejemplo, los dispositivos móviles llevan bastante tiempo siendo parte de las redes en las organizaciones debido a que en la actualidad son recursos indispensables en la labor diaria de las personas. Por esto, es cada vez más normal que la administración de la red sea menos centralizada por la gran ventaja de movilidad que ofrecen estos dispositivos.

Por lo anterior, es necesario expandir además del servicio, el soporte para esas alternativas, pensar en soluciones que faciliten la gestión de las redes, soluciones que garanticen la seguridad de la información y de los recursos de la empresa, soluciones que tengan un control sobre los equipos que consumen los servicios ofrecidos y validen su seguridad y protección; hoy en día todas las organizaciones, y en especial las grandes empresas, son objeto de innumerables intentos de ataques a sus sistemas.

3. Descripción del proyecto

3.1 Definición del problema

La entidad objeto de este proyecto es un organismo Gubernamental enfocado en la inclusión social y la asistencia a las víctimas de la violencia. Tiene su sede principal en la ciudad de Bogotá y oficinas de atención en cada ciudad capital a nivel nacional.

Los sistemas de información misional son los activos más importantes a los que se puede acceder mediante LAN y/o WLAN, son la base del negocio de la entidad y de la

administración que soporta la operación diaria. A estos sistemas se ingresa mediante credenciales gestionadas por el directorio activo y cada sistema de información maneja sus políticas de seguridad y acceso. La seguridad de la información, plataformas y herramientas de uso institucional son componentes que se deben tener en cuenta por los responsables de red, es por esto que a medida que va creciendo la entidad se ha ratificado la estrategia de confidencialidad y seguridad de la información mediante un sistema estático donde no se contempla la movilidad y la facilidad de acceso a los recursos de la red, como las nuevas tecnologías lo requieren hoy en día.

La red LAN, WLAN y la red de comunicaciones están conformadas por dispositivos del fabricante CISCO en los niveles de acceso, distribución y core. Esta infraestructura permite el uso de servicios desde 1600 equipos de cómputo propios de la entidad entre los cuales hay estaciones de trabajo, impresoras, portátiles, etc. Por otra parte, dispone de una red WLAN con SSID independientes para directivos, funcionarios y visitantes, que en promedio es utilizada por 700 dispositivos, que en su mayoría son equipos personales (no administrados), permitiendo la comunicación e interoperabilidad entre éstos y dispositivos de funcionarios de la entidad. Algunos de estos equipos son sensibles en gran parte por la información que almacenan, información que es importante para los intereses institucionales y gubernamentales teniendo en cuenta que el sector de la inclusión social y la asistencia a las víctimas de la violencia es un pilar en la política de gobierno del país. Por otro lado, se evidencia falta de protección en esta información, ya que las medidas de seguridad de la red son básicas y se convierte en una red de datos vulnerable comprometiendo la integridad, confidencialidad y disponibilidad de la información por accesos no autorizados que a su vez repercuten en retrasos en los servicios que presta la entidad. Estas fallas y retrasos pueden acarrear sanciones legales y fiscales para la organización y los funcionarios responsables. Las causas más representativas al catalogar la red como vulnerable son:

- Ausencia de gestión de actividad de usuarios: Conexión de usuarios sin registro de logs, que impide verificar el comportamiento de éstos en caso de presentarse algún incidente.
- Uso de recursos de la red sin restricción: Consumo de los servicios de la entidad que podría sobrepasar lo esperado.

- Acceso no autorizado a la información: Acceso de usuarios no autorizados que podría atentar con la confidencialidad, integridad y disponibilidad de la información.
- Debilidad ante presencia de posibles amenazas o equipos infectados: Acceso de dispositivos a la red sin un previo chequeo de seguridad, lo cual implica exposición a cualquier tipo de virus o amenaza.
- Los equipos de cómputo o móviles de usuarios visitantes pueden tener comunicación con otros dispositivos de cómputo de la entidad, lo cual abre la posibilidad que se presente fuga de información sensible para la organización.
- No se cuenta con un inventario actualizado ni se tienen mecanismos de control que permitan responder a los interrogantes de quién, cuándo, dónde, cómo, o qué aplicaciones y qué amenazas o vulnerabilidades están generando los dispositivos que se conectan a la red bien sea a través de cables o inalámbricamente.

Actualmente el acceso a los recursos de red en las diferentes áreas de la entidad se realiza mediante la red cableada o red inalámbrica. Para el acceso a la red cableada no hay controles definidos, más que la conexión a los puntos de red o basados en VLANs, pero el control se realiza mediante el puerto físico de los switch, y sumado al constante movimiento de los usuarios, ocasiona que la gestión de esto sea compleja, permitiendo que independientemente del tipo de equipo, ya sea de la entidad o no, se conecte a la red y consuma sin restricción los servicios disponibles. Por otro lado, el acceso por la red inalámbrica se controla con contraseñas generales, las cuales no se cambian periódicamente y puede generar el riesgo que éstas se difundan fácilmente.

La conectividad y operatividad necesaria en la entidad deriva en una gran demanda de infraestructura que se implementa para dar solución a la necesidad, dejando de lado el aspecto de seguridad y así trayendo consigo las siguientes implicaciones:

- A mayor infraestructura se aumentan los costos funcionales, los procesos de gestión y operación y las personas encargadas de gestionar esos procesos.
- Al aumentar los procesos hay mayor exposición a riesgos porque éstos involucran servicios, que, a su vez, pueden involucrar nuevos permisos o el uso de nuevos

puertos que pueden ser vulnerables a ataques.

- A medida que la infraestructura es más compleja se dificulta el cumplimiento de las regulaciones y requerimientos de seguridad.
- Garantizar la disponibilidad e integridad de la información es más complicado porque al haber más infraestructura hay más puntos de acceso a la información, lo que también implica que más personas tengas acceso a ésta.
- El perímetro de la red se hace más extenso y puede ser confuso debido a la falta de visibilidad.

Por lo anterior, los aspectos a solucionar serían los siguientes:

- Acceso sin monitoreo a la red.
- Uso de recursos de la red sin restricción ni controles adecuados.
- Monitoreo o control de acceso no autorizado a la información.
- Debilidad ante presencia de posibles amenazas o equipos infectados.
- Comunicación de equipos propios de la entidad con dispositivos de usuarios externos sin la debida segmentación, así como sin restricción ni control.
- Falta de trazabilidad para verificar el comportamiento y las acciones de los usuarios y equipos conectados a la red.
- Incremento de las exposiciones por la masificación de dispositivos móviles de propiedad de los usuarios (BYOD).

3.2 Solución propuesta

Para mitigar los riesgos presentados anteriormente, se propone el diseño de una plantilla de aseguramiento como recomendación a la entidad para realizar un endurecimiento (hardening) de la capa de red interna del modelo de defensa en profundidad. Además, se propone limitar las fronteras de acceso a los recursos de red aplicando políticas de seguridad en el acceso, reduciendo riesgos de intrusión, y brindando mayor flexibilidad y control a personal administrativo de TI.

Dando respuesta a lo anterior, se requiere de una solución que permita que los usuarios independientemente de su ubicación o tipo de dispositivo acceda a los recursos

que le hayan sido autorizados, mediante un tipo de acceso apoyado en el protocolo 802.1x, que por su diseño permite autenticación, autorización y registro de las actividades que ejecuta cada usuario en la red, control con el uso de políticas, y perfilamiento del usuario final, complementada con unas recomendaciones de aseguramiento de los equipos de red para reducir las vulnerabilidades en los mismos, atendiendo las buenas prácticas de los fabricantes.

A mediano y largo plazo, la implementación del control de acceso en la red tendrá una relación costo/beneficio favorable para la organización por diferentes motivos: permite establecer perfiles definidos y requisitos de conexión. Además, facilita el descubrimiento de cada dispositivo conectado a la red controlando su comportamiento y adaptándolo a los requerimientos establecidos, con lo cual, logra detectar cualquier equipo infectado y apartarlo del resto para obtener un entorno seguro. Hoy en día, diferentes amenazas intentan comprometer los sistemas de las empresas, por ejemplo, cada vez es más recurrente los ataques asociados a BYOD, ya que hay muchos empleados que utilizan dispositivos propios para temas laborales y que por alguna razón necesitan acceder a los servicios de la organización. Además, la implementación del control ayuda bastante a la administración de la red promoviendo el acceso basado en roles, ya que el manejo de grandes cantidades de permisos a los recursos compartidos de la empresa puede convertirse en una tarea complicada, al igual que el control de todos los puntos de acceso a la red, ya que pueden ser muchos y aumentar en el tiempo. Un control de acceso permitirá verificar la apertura y la restricción de estas puertas de entrada.

4. Estado del arte

4.1 Marco de referencia teórico

Cuando el propósito de un proyecto es la seguridad, es conveniente investigar sobre antecedentes o experiencias de trabajos existentes para extraer puntos clave que ayuden a optimizar su desarrollo. De acuerdo a lo anterior, en la investigación realizada se encontró que existe varia documentación con diferentes puntos de vista de aseguramiento de infraestructura tecnológica. Ana Gabriela Caiza Navas, en su trabajo de investigación *"DISEÑO DE UN PROCESO DE HARDENING DE SERVIDORES PARA UNA INSTITUCIÓN*

FINANCIERA DEL SECTOR PÚBLICO"[1] (2019), cita información obtenida de proyectos realizados anteriormente en los que se mencionan puntos importantes a tener en cuenta como:

- Realización de un análisis previo de seguridad de la red informática.
- Indagación de medidas de *hardening* para equipos basados en un SO específico.
- Exposición del *hardening* como una alternativa para robustecer la seguridad en la infraestructura.
- Indagación sobre herramientas que permitan cumplir con el propósito.
- Conocimiento del negocio de la organización, el detalle de aplicaciones y servicios necesarios para ésta.
- El enfoque de *hardening* está basado en el concepto de defensa en profundidad.
- Identificación de vulnerabilidades.

Por otro lado, Daniel Omar Esmoris en su investigación, *"CONTROL DE ACCESO A REDES"*[2], resalta la importancia de la implementación de un control de acceso a la red dando como ejemplo situaciones que pueden poner en riesgo la seguridad de las empresas. Para mencionar solo uno de ellos, si un atacante logra por alguna circunstancia ingresar a la red de la empresa con su propio dispositivo y aloja un archivo malicioso en algún servidor, el hecho que un empleado sin conocimiento lo consulte e infecte su computador puede ser el inicio de una propagación de virus a lo largo de toda la red de la entidad. Por lo anterior, Daniel aborda el problema y su investigación hacia tres tecnologías que pueden proveer la seguridad necesaria, el NAC de Cisco, NAP de Microsoft y TNC (Trusted Computing Group).

Jimmy Eduardo Jaén Solórzano, en su trabajo de Maestría *"DISEÑO E IMPLEMENTACIÓN DEL CONTROL DE ACCESO A LA RED CISCO ISE"* [3] (2015), nos habla de los beneficios de la solución propuesta en su proyecto, además de mencionar que sirve de guía en el momento de elegir lo apropiado para nuestra entidad objetivo, por ejemplo, visibilidad, autenticación y disponibilidad de cumplimiento.

[1] https://repositorio.uisek.edu.ec/bitstream/123456789/3346/1/TESIS_AnaCaiza.pdf
[2] https://postgrado.info.unlp.edu.ar/wp-content/uploads/2014/07/Esmoris.pdf
[3] http://www.dspace.espol.edu.ec/xmlui/handle/123456789/34981

4.2 Marco de referencia tecnológico

El control de acceso a la red es un componente principal en la estrategia global de seguridad. El objetivo es comprobar el estado de cumplimiento de un equipo que intenta acceder a la red, de modo que solo se permita el ingreso a dispositivos "seguros" y bloquee la entrada a aquellos equipos que no cumplan con los requisitos mínimos de seguridad exigidos. La solución debe poder ser aplicable a todos los métodos de acceso: red LAN y WLAN, ya que debe ser diseñado para el acceso desde cualquier dispositivo.

5. Glosario de términos

BYOD (Bring Your Own Device): Es una nueva tendencia tecnológica que permite a los trabajadores llevar sus dispositivos portátiles personales para llevar a cabo tareas del trabajo y conectarse a la red y recursos corporativos.

DEFENSA EN PROFUNDIDAD: filosofía que establece que: "los sistemas de seguridad de un sistema deben ser entendidos y contenidos dentro de capas, cada una independiente de la anterior de forma funcional y conceptual".

HARDENING (Endurecimiento)[4]: Proceso de asegurar un sistema reduciendo sus vulnerabilidades o agujeros de seguridad, para los que se está más propenso cuantas más funciones desempeña. En principio, un sistema con una única función es más seguro que uno con muchos propósitos.

NAC (Network Access Control): Tecnología que permite controlar de forma muy granular qué dispositivos pueden acceder a la red, permitiendo establecer políticas de gestión de los dispositivos.

PRUEBA DE CONCEPTO[5]: PoC (por sus siglas en inglés) es una implementación parcial o incompleta de un método o de una idea, realizada con el propósito de verificar que el concepto o teoría en cuestión es susceptible de ser explotada de una manera útil. La PoC

[4] https://es.wikipedia.org/wiki/Endurecimiento_(inform%C3%A1tica)
[5] https://es.wikipedia.org/wiki/Prueba_de_concepto

se considera habitualmente un paso importante en el proceso de crear un prototipo realmente operativo. En seguridad informática el término PoC se utiliza, a menudo, como sinónimo de Zero-Day Exploit. Esta es una vulnerabilidad que, por ser muy reciente, no aprovecha en su totalidad todas las ventajas que podría proporcionar. En este ámbito, la prueba de concepto se utiliza como demostración de que una aplicación o servicio puede ser vulnerable.

6. Justificación

Actualmente, la información es uno de los activos más importantes para una empresa. Es por esto, que la estructura de la red juega un papel prioritario para su protección. La infraestructura debe cumplir con ciertos requisitos de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información.

Tradicionalmente, las organizaciones establecen políticas de seguridad, entre éstas está establecer un punto de acceso entre su red y el Internet. Sin embargo, con el crecimiento que han tenido las redes y los servicios que se ofrecen, dicho punto de seguridad se ha desvirtuado. Hoy en día, una gran cantidad de los ataques a la información de una organización no provienen de la parte externa sino desde el interior de la misma (Solarte, Rosero, & del Carmen Benavides, 2015).

Por lo anterior, es de suma importancia para la empresa tener un control del acceso a la red que sea capaz de dar solución todos los posibles efectos que se presentan. Asegurar que la información sensible de la entidad no sufra ataques cumpliendo con la confidencialidad, disponibilidad e integridad para que la entidad pueda garantizar el buen servicio y la continuidad de negocio, complementado con la recomendación de aplicación de un aseguramiento estándar definido de acuerdo a las necesidades de la organización (hardening), y dirigido a los equipos de red de acuerdo a las buenas prácticas del fabricante.

7. Objetivos

7.1. General

Reforzar el acceso seguro a los recursos informáticos de la entidad mediante el

aseguramiento de los equipos de red y una propuesta de implementación de un sistema de control de acceso.

7.2. Específicos

- Realizar análisis de vulnerabilidades de la red LAN y WLAN en la estructura actual de red.
- Desarrollar ficha técnica de adquisición e implementación de sistema de control de acceso como apoyo a la viabilidad técnica y financiera.
- Diseñar una plantilla de aseguramiento que mitigue las vulnerabilidades identificadas en los dispositivos de red LAN y WLAN de la infraestructura actual, acogiendo las buenas prácticas de la industria.

8. Requerimientos

Conociendo el objetivo principal de un control de acceso a la red, como requerimiento funcional se debe permitir que todos los equipos, de cualquier sistema operativo e independientemente de su ruta o red de entrada, puedan ingresar a la red luego de ser analizados y cumplir con políticas de seguridad. El proceso de análisis de seguridad debe ser totalmente transparente para el usuario final, sobre todo si el dispositivo que se utiliza entra en el grupo del BYOD, ya que la solución no debe ser intrusiva ni perjudicar el rendimiento del equipo.

- Identificación y Detección de Usuarios y Dispositivos
- Implementación de Políticas de Acceso
- Autenticación 802.1X RADIUS
- Autorización de Cambios
- Clasificación de dispositivos e integración con LDAP
- Administración Gráfica
- Gestión Centralizada
- Escalabilidad

Por otro lado, el endurecimiento de los equipos se debe realizar mediante la aplicación de una plantilla que cumpla con mejorar la seguridad y minimizar los riesgos a

partir de tres planos fundamentales, los cuales proveen diferentes funcionalidades que necesitan ser protegidas: el plano de la administración el cual se encarga de administrar el tráfico enviado a los dispositivos de red; el plano de control del dispositivo el cual se encarga de procesar el tráfico para mantener el funcionamiento de la infraestructura de red; y por último, el plano de los datos que es el encargado de enviar la información a través de la red.

Debido a la disponibilidad de equipos, y para demostrar el cumplimiento de los objetivos a partir de la gestión realizada, es necesario mencionar que la plantilla de aseguramiento a elaborar es aplicable a toda la infraestructura con la que cuenta la entidad a nivel nacional. Por otro lado, se pretende demostrar el funcionamiento del control de acceso a la red, donde se puede evidenciar la implementación de mecanismos de seguridad a nivel de la capa de acceso de una red corporativa cableada e inalámbrica, mostrando todas las características planificadas para lograr lo propuesto.

El diseño se basa en seguridad a nivel lógico, pero no físico (control de acceso físico a instalaciones, equipos de TI, electricidad, cableado y etiquetado, dispositivos flexibles).

La simulación no contempla: seguridad encriptada desde el host hacia el switch (MACsec9), debido a que se necesita un módulo físico a nivel de hardware, así como TrustSec10, pxGrid11, ni integración con el firewall.

Los acuerdos de confidencialidad indican que no se puede revelar información a terceros sin previa autorización de la entidad, por lo anterior, toda la documentación a entregar como soporte de este proyecto será ajustada con el fin de dar cumplimiento a los acuerdos. Además, se acordarán los horarios y el tiempo de las ventanas para realizar la prueba de concepto y la aplicación del hardening a los equipos de red seleccionados.

9. Metodología

Fase 1: Planeación: Se realiza un análisis de vulnerabilidades en la infraestructura actual con el fin de establecer los posibles riesgos, teniendo en cuenta los equipos que hay y su respectivo sistema operativo. Este alcance está relacionado a los dispositivos de red LAN y WLAN al igual que el análisis de la respectiva información.

Fase 2: Ejecución: Se realiza el diseño formal de la solución de control de acceso a la red, estableciendo topologías lógicas y físicas. De igual forma, se hacen configuraciones sobre los componentes de la plataforma y equipos que intervienen, mediante la simulación del entorno de red. Además, se elabora una plantilla de aseguramiento que sirva como guía a la entidad para la mitigación de las vulnerabilidades identificadas en los dispositivos de red LAN y WLAN de la infraestructura actual, aplicando las buenas prácticas del fabricante.

Fase 3: Presentación: Se documenta los resultados obtenidos a partir de las diferentes pruebas realizadas. Esta etapa se compone de una ficha técnica en la que se definen los requerimientos del software, así como también las ventajas, desventajas y consideraciones que se deben tener en cuenta a la hora de realizar la implementación del control de acceso a la red sobre toda la entidad.

Fase 4: Conclusiones y entrega de documento.

10. Desarrollo

10.1. Ejecución – Fase 1: Análisis de Vulnerabilidad

La planeación del proyecto comienza con el escaneo de red y el análisis de vulnerabilidad realizado a un grupo de equipos seleccionados con el fin de descubrir la estructura de la red y su estado en materia de seguridad, tal y como se indica en el apartado *9. Metodología (Fase 1)*. A partir de este resultado, se conoce lo que se tiene y lo que se debe mejorar, siendo así más sencillo establecer los requerimientos que debe tener el control de acceso y la plantilla de aseguramiento propuesto. Con el reconocimiento inicial, la idea es identificar los segmentos críticos de la red para enfocarse específicamente en las vulnerabilidades que puedan hallarse en los dispositivos pertenecientes a éstos.

De acuerdo con lo mencionado anteriormente, conociendo el tamaño de la red y el tipo de equipos que la componen, el paso a seguir es definir un plan de remediación para mitigar aquellas vulnerabilidades críticas halladas que se tendrán en cuenta para la elaboración de la plantilla de aseguramiento. Además, por otro lado, se define la solución más apropiada para el control de acceso a la red basado en algunos criterios importantes

de funcionalidad y compatibilidad, con el fin de proteger la red LAN y WLAN de cualquier riesgo.

NOTA: Con el fin de conservar la confidencialidad y reserva de la entidad, todas las direcciones IP mostradas en este documento fueron cambiadas para cumplir con el manual de políticas y lineamientos de Seguridad de la Información: *"El principal activo o valor de una entidad, es sin duda la información. Es por ello que se debe propender por preservar sus valores y prestarle la seguridad adecuada"*[6].

10.1.1. Visión General

Un análisis de vulnerabilidad se puede definir como un proceso en el que se involucran una serie de etapas como: descubrimiento y clasificación de criticidad de los recursos, identificación y análisis de las vulnerabilidades en éstos, y realización de un plan de remediación para mitigar dichas brechas de seguridad.

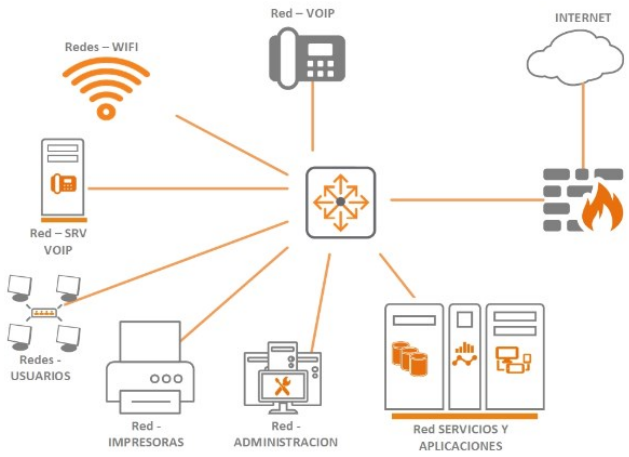


Figura 1. Diagrama de red de la entidad.

Para el desarrollo de este proceso se realizaron los siguientes pasos:

[6] Manual de políticas y lineamiento de Seguridad de la Información de la Entidad.

- Comunicación Previa: Se entrevistó al personal de la entidad para recopilar información del sistema, conocer la topología, segmentación y direccionamiento de red utilizado.

- Escaneo y Análisis de Vulnerabilidades: Se realizó el escaneo de la red con dos aplicaciones que se describen más adelante. En este paso, hay que tener en cuenta que el alcance del proyecto son los equipos de red LAN y WLAN, sin embargo, para dimensionar el nivel de exposición de los activos de información se extendió el escaneo a otros segmentos de red.

10.1.2. Descubrimiento y clasificación

Para iniciar, se determinó que el escaneo se ejecutara desde adentro de la entidad, más exactamente desde la red WiFi de *Invitados* como se muestra en la Figura 2.

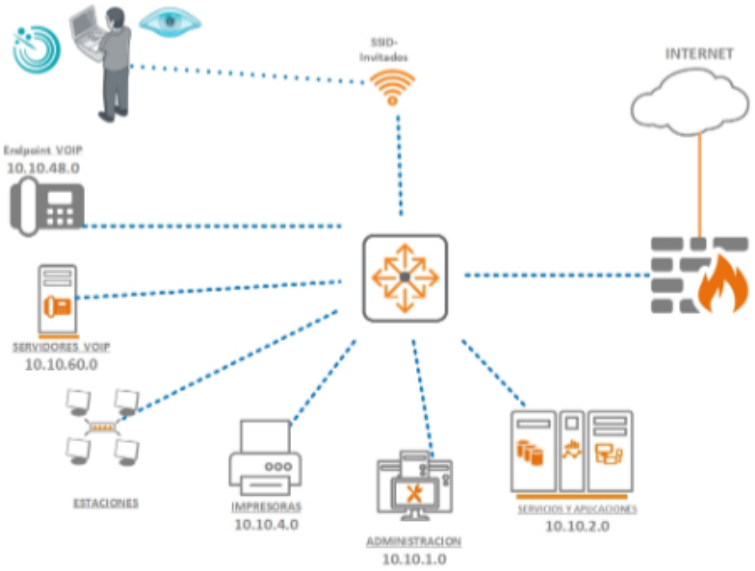


Figura 2. Diagrama de red para escaneo y descubrimiento.

El descubrimiento se llevó a cabo por medio de un escaneo a la red como primer chequeo sobre la infraestructura. Para esto, se utilizó la herramienta *Nmap* en su versión con interfaz gráfica **Zenmap** (Ver Anexo 01).

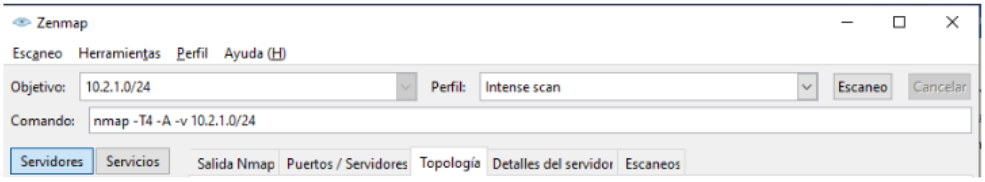


Figura 3. Ejemplo escaneo en Zenmap y opciones de configuración.

Los parámetros de configuración son los siguientes:

- Objetivo: Dirección IP o en este caso segmento de red a escanear.
- Perfil: Es una lista desplegable que contiene una serie de perfiles de exploración predeterminados. El utilizado para este caso fue *Intensive Scan*.

- Comando:
    - Opción **-A**: Habilita la detección de sistema operativo y versión.
    - Opción **-T4**: Acelera el proceso.
    - Opción **-v**: Aumenta la cantidad de información sobre el progreso del análisis que muestra Zenmap por pantalla.

Con esta herramienta, se logró detectar todos los puertos y servicios disponibles sobre cada uno de los equipos activos y evidenciar que hay comunicación bidireccional hacia todos los segmentos de la red LAN como se muestra en la Figura 4. Cuantos más puertos abiertos, más grande es el círculo. El círculo negro es el origen del escaneo, los blancos representan un host intermedio en una ruta de red que no se escaneó, los verdes representan un host con menos de tres puertos abiertos, los amarillos entre tres y seis puertos abiertos, y los rojos son hosts con más de seis puertos abiertos[7].

[7] https://nmap.org/book/zenmap-topology.html#zenmap-topology-legend

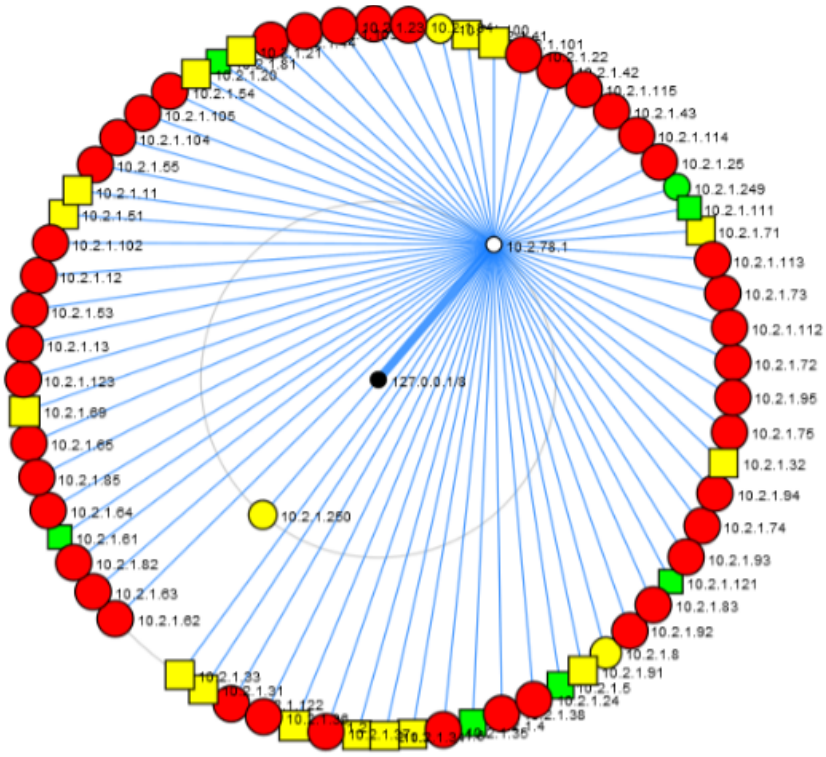


Figura 4. Topología de escaneo de la 10.2.1.0 (Administración).

Por lo anterior, los siguientes segmentos se identificaron como los más críticos: el de servidores, equipos de administración, telefonía IP e impresoras. Por otro lado, para un escaneo más completo, identificando vulnerabilidades y demás, se utilizó la herramienta **Nessus**, la cual se instaló como una máquina virtual que se interconecta con *Tenable.IO*, una suite de gestión de vulnerabilidades. Nessus hace uso de un listado de *plugins* disponibles para atacar los puertos que encuentra activos y mostrar una clasificación de la criticidad del riesgo sobre los recursos (Ver Anexos 02-03-04-05-06). Debido a que la herramienta es licenciada, para poder realizar esta etapa el proyecto fue necesario contactar al fabricante en Colombia, quienes nos brindaron una licencia de 30 días con todas las funcionalidades.

En base al resultado del escaneo, se procedió a identificar los equipos con mayor riesgo y con alta probabilidad de afectar la red de la entidad. Lo anterior, debido a que no todas las vulnerabilidades encontradas lo son realmente, es decir, el sistema puede responder al escaneo de una manera que nos indica ser vulnerable a cierto tipo de ataque pero que en realidad no lo es. A estos hallazgos se les conoce

como *falsos positivos*, y el objetivo en esta parte del proceso es descartar el mayor número de falsos positivos para así poder enfocarse en los verdaderos riesgos descubiertos.

10.1.3. Identificación

En los Anexos 07-08-09-10-11 se puede evidenciar el resultado de la identificación realizada a las vulnerabilidades encontradas y clasificadas según su criticidad (Críticas, Altas, Medias, Bajas e Informativas) sobre los equipos que pertenecen a cada uno de los segmentos mencionados anteriormente. Para continuar con el proceso, y dando cumplimiento al alcance de este proyecto, se realiza un análisis del riesgo que implica la situación actual de los equipos de red LAN y WLAN dentro de la infraestructura.

10.1.4. Análisis

Las vulnerabilidades enlistadas a continuación se validaron e investigaron en el portal oficial de NVD[8] (National Vulnerablity Database), el cual es el repositorio de administración de vulnerabilidades del gobierno de los Estados Unidos. También se utilizó la descripción de cada uno de los *plugins* utilizados por Nessus para el escaneo.

- **CVE-2013-2566:** El algoritmo RC4 tiene muchos sesgos de un solo byte, lo que hace más fácil para el atacante perpetrar ataques de recuperación de texto en claro por medio de análisis estático[9].
- **CVE-2015-2808:** El equipo soporta el uso de RC4 en sus cifrados. El cifrado RC4 es débil en la generación de bytes aleatorios debido a una gran variedad de pequeños sesgos que se introducen en el flujo[10].
- **CVE-2016-2183:** Los algoritmos de cifrado DES y 3DES tienen un límite aproximado de 4 millones de bloques, lo que hace más fácil para el

[8] https://nvd.nist.gov/
[9] https://nvd.nist.gov/vuln/detail/CVE-2013-2566
[10] https://nvd.nist.gov/vuln/detail/CVE-2015-2808

atacante obtener el texto cifrado en claro[11].

- **CVE-2004-2761:** El algoritmo MD5 es vulnerable al ataque de colisiones, lo que hace más fácil para el atacante realizar ataques de *spoofing*[12].
- **CVE-2019-15262:** Existe una vulnerabilidad en el manejo de SSH en el software de los WLC de Cisco que permite a un atacante realizar denegación de servicio en el dispositivo afectado. La vulnerabilidad existe porque el proceso SSH no se borra correctamente después de que se desconecta la sesión SSH, y una forma de *explotar* la vulnerabilidad es abriendo varias sesiones SSH para consumir los recursos de la máquina[13].
- **CVE-2019-15276:** Existe una vulnerabilidad en la interfaz web en el software de los WLC de Cisco que permite a un atacante realizar denegación de servicio en el dispositivo afectado. La vulnerabilidad existe debido a una falla en el motor de análisis de HTTP[14].
- **CVE-2008-1657:** La versión actual de OpenSSH permite a un atacante evitar la directiva ForceCommand de *sshd_config* modificando el archivo de sesión *.ssh/rc*[15].
- **CVE-2006-0393:** La versión actual de OpenSSH permite a un atacante realizar denegación de servicio intento iniciar sesión con un usuario inexistente[16].
- **CVE-2005-2798:** La versión actual de OpenSSH permite exponer las credenciales de GSSAPI a usuarios que inicien sesión con un método diferente a la autenticación GSSAPI cuando el *GSSAPIDelegateCredentials* está habilitado[17].
- **CVE-2005-2797:** La versión actual de OpenSSH permite posiblemente habilitar la funcionalidad *GatewayPorts* cuando no se provee una dirección de escucha. Lo anterior es debido a que OpenSSH no maneja

[11] https://nvd.nist.gov/vuln/detail/CVE-2016-2183
[12] https://nvd.nist.gov/vuln/detail/CVE-2004-2761
[13] https://nvd.nist.gov/vuln/detail/CVE-2019-15262
[14] https://nvd.nist.gov/vuln/detail/CVE-2019-15276
[15] https://nvd.nist.gov/vuln/detail/CVE-2008-1657
[16] https://nvd.nist.gov/vuln/detail/CVE-2006-0393
[17] https://nvd.nist.gov/vuln/detail/CVE-2005-2798

correctamente el reenvío de puertos dinámicos[18].

- **CVE-1999-0517:** Es posible obtener el nombre de comunidad del servidor remoto SNMP. Un atacante puede utilizar esta información para conocer más acerca del host o para cambiar alguna configuración del mismo[19].
- **CVE-2006-0225:** La funcionalidad SCP de la versión actual de OpenSSH permite a los atacantes ejecutar comandos arbitrarios por medio de archivos que contengan meta caracteres *Shell* o espacios[20].
- **CVE-2007-4752:** La versión actual de OpenSSH permite a un atacante adquirir privilegios sobre el dispositivo haciendo que se confía en un cliente extraño. Lo anterior debido a que la versión de SSH no maneja apropiadamente la situación cuando una *cookie* sin confianza no se puede crear, y en su lugar utiliza una de confianza[21].
- **CVE-2007-2243:** La versión actual de OpenSSH permite a un atacante determinar la existencia de cuentas de usuarios intentando autenticarse vía S/KEY, ya que muestra un mensaje diferente cuando la cuenta del usuario existe. Lo anterior pasa cuando *ChallengeResponseAuthentication* está habilitado[22].
- **CVE-2006-5794:** La versión actual de OpenSSH es afectada por una vulnerabilidad de separación de privilegios, lo que permite a un atacante evitar la autenticación debido a una débil verificación en el proceso[23].
- **CVE-2006-4925:** El *packet.c* de SSH en la versión actual de OpenSSH permite a un atacante realizar denegación de servicio enviando secuencias inválidas de protocolo con *USERAUTH_SUCCESS* antes de *NEWKEYS*, lo que causa que este parámetro sea nulo[24].
- **CVE-2007-0726:** El proceso de generación de la llave SSH permite a un atacante causar denegación de servicio conectándose al servidor antes

[18] https://nvd.nist.gov/vuln/detail/CVE-2005-2797
[19] https://nvd.nist.gov/vuln/detail/CVE-1999-0517
[20] https://nvd.nist.gov/vuln/detail/CVE-2006-0225
[21] https://nvd.nist.gov/vuln/detail/CVE-2007-4752
[22] https://nvd.nist.gov/vuln/detail/CVE-2007-2243
[23] https://nvd.nist.gov/vuln/detail/CVE-2006-5794
[24] https://nvd.nist.gov/vuln/detail/CVE-2006-4925

que el proceso de las llaves acabe[25].

Además de la anteriores, se identificaron algunas otras vulnerabilidades las cuales no están catalogadas oficialmente en la base de datos de la NVD, pero que, de acuerdo a lo experimentado en clases y laboratorios, pueden resultar causales de un ataque. Por ejemplo, se descubrió que es posible conocer el SO con su versión en la mayoría de dispositivos. También se evidenció que es posible conocer el resultado de un *TraceRoute* lo que permitiría a un atacante conocer e inferir más acerca de la topología de la red. En el escaneo también se pudo evidenciar que es posible obtener información de la entidad a través de certificados SSL, obtener la dirección MAC de algunos equipos, la versión que soporta de los protocolos TLS, entre otras.

10.1.5. Plan de Remediación

Para finalizar con el proceso, y de acuerdo a lo evidenciado en el análisis, se debe establecer el plan de remediación para mitigar los riesgos críticos encontrados. Como solución, se recomienda la aplicación de una plantilla de endurecimiento (hardening) a partir de una plantilla diseñada como propuesta inicial de este proyecto. Para llevar a cabo esta labor, nos remitimos a la investigación hecha en el apartado *4. Estado del Arte* donde se encontró que hay varios puntos a tener en cuenta a la hora de realizar un hardening, por ejemplo, la identificación y el análisis de las vulnerabilidades y la indagación de medidas de hardening para equipos con un mismo sistema operativo. En el planteamiento y definición del problema se indicó que los equipos de red de la entidad pertenecen todos al fabricante CISCO, lo que significa que éstos comparten el mismo sistema operativo y en algunos casos los mismos procesos y servicios. Es por esto que, siguiendo las buenas prácticas dadas por el fabricante, y las recomendaciones dadas por Nessus en el escaneo, se elaboró la plantilla de aseguramiento mostrada en el Anexo 12 con un enfoque a partir de tres planos fundamentales. El *plano de administración*, donde se resaltan aspectos como manejo correcto de contraseñas, algoritmos de cifrados seguros,

[25] https://nvd.nist.gov/vuln/detail/CVE-2007-0726

administración de usuarios, manejo de servicios, control de sesiones activas, consumo de recursos de máquina, control de acceso, cifrado de sesiones de administración, control de puertos activos y manejo de Logs. Por otro lado, se encuentra el *plano de control*, donde se asegura el funcionamiento de los protocolos y procesos para la comunicación entre los dispositivos. Y, por último, el *plano de los datos*, que asegura el envío de la información a través de la red, donde se establecieron puntos como: seguridad de la IP origen, seguridad de puerto, configuración anti spoofing, etc.

10.2. Ejecución – Fase 2: Control de Acceso

10.2.1. Elección Solución NAC

En principio, una solución NAC debe ofrecer como mínimo ciertas características para ayudar a cumplir con los propósitos de seguridad que las empresas necesitan. Dentro de estas características se encuentra en primer lugar el descubrimiento y perfilamiento de los dispositivos, que hace referencia a un primer chequeo en la red para ofrecer al usuario una visibilidad esperada del 100% de los dispositivos conectados. En segundo lugar, valga la redundancia, la solución debe ofrecer el control de acceso a la red, el cual hace referencia a la posibilidad de negarle o permitirle a un dispositivo nuevo conectarse o no a ésta. Otra característica importante en la solución es la revisión de postura, la cual es la que se encarga principalmente de revisar el cumplimiento de los criterios definidos por la administración para permitir, denegar, o poner en cuarentena a determinado dispositivo. Además de las anteriores, un NAC debe tener la posibilidad de administrar los dispositivos invitados, es decir, debe poder controlar los recursos a los que el dispositivo se va a conectar. Por último, y no menos importante, una solución de control de acceso a la red debe tener una buena integración bidireccional con otros productos de seguridad, ya que al final, todas las herramientas implementadas en la empresa deben aportar su especialidad para garantizar la seguridad.

Por otro lado, a parte de las características mencionadas anteriormente, otros criterios que se deben tener en cuenta a la hora de elegir la solución indicada son:

la compatibilidad con el entorno tecnológico de la empresa, y la complejidad de implementación en ésta. Actualmente, existen gran cantidad de soluciones NAC, pero para tener una mejor guía de las herramientas que podemos analizar para implementar, se decidió consultar varios sitios sobre reseñas de soluciones tecnológicas, entre las cuales se encuentran *Gartner Peer Insights*[26], *Alacrinet*[27], *IT Central Station*[28] y *Expert Insights*[29], donde se evidenció que las mejores tres herramientas para el control de acceso a la red actualmente (2020) son: Cisco ISE, Aruba ClearPass, y ForeScout. Teniendo este grupo específico de herramientas se debió identificar cuál es la que mejor se adapta a los criterios de selección mencionados anteriormente. Para la elección, a parte de la guía en los portales web citados, nos guiamos también de reseñas hechas por la comunidad tecnológica y de profesionales en el negocio, y a partir de eso, para cada solución se extrajeron sus respectivas ventajas y desventajas.

- Cisco ISE:
    - Plataforma de gestión de políticas de seguridad que automatiza y aplica el acceso de seguridad sensible al contexto a los recursos de la red. Esta herramienta de Cisco ofrece una visibilidad superior del usuario y del dispositivo para respaldar las experiencias de movilidad empresarial y controlar el acceso. Comparte datos con soluciones integradas para acelerar sus capacidades para identificar, mitigar y remediar amenazas[30].
    - Ventajas:
        - Permite identificar y aislar un equipo infectado o propenso a infectarse.
        - Es compatible con los productos de Microsoft.
        - Tiene características como la evaluación de postura, administración de políticas, asignación de VLAN, y servicios de BYOD.

[26] https://www.gartner.com/reviews/market/network-access-control
[27] https://www.alacrinet.com/security-solutions/nac
[28] https://www.itcentralstation.com/categories/network-access-control
[29] https://www.expertinsights.com/services/network-access-control/reviews
[30] https://www.cisco.com/c/dam/global/es_es/assets/publicaciones/06-10-Cisco-NAC-interoperable.pdf

        - Ofrece visibilidad de todos los cambios que se hacen en los equipos que se quieran monitorear.
    - Desventajas:
        - Un aspecto que se puede mejorar es el agente. Se podría pensar en una implementación sin agente.
        - Se debe mejorar el soporte al usuario.
        - Los equipos permitidos no tienen acceso completo a la red debido a defectos del agente.

- Aruba ClearPass:
    - Visibilidad sin agente y control de acceso basado en roles para una aplicación y respuesta de seguridad sin interrupciones en redes cableadas y no cableadas. Aruba es un proveedor líder de soluciones NAC de próxima generación para empresas móviles. Es una plataforma de administración de políticas que muchas empresas están implementando para mantener su red segura. Permite una conexión segura entre el negocio y los dispositivos personales que cumplen con políticas de seguridad.
    - Ventajas:
        - Control de políticas sin agente y respuesta automatizada.
        - Acceso seguro a dispositivos invitados.
        - Tiene buenas herramientas para reportes.
    - Desventajas:
        - La interfaz del usuario debería ser más sencilla y mejorada.
        - Algunas funciones del mecanismo de logs y reportes deberían mejorar.
- Forescout:
    - La plataforma Forescout ofrece visibilidad y control del dispositivo para permitir a las empresas y agencias gubernamentales obtener una visibilidad completa de su entorno y organizar la acción. Esta plataforma ofrece capacidades integrales de control de acceso a la red y más, basadas en la visibilidad en tiempo real de los

dispositivos en el instante en que acceden a la red. Escanea continuamente redes y monitorea la actividad de los dispositivos conocidos, propiedad de la compañía, así como dispositivos desconocidos, personales y no autorizados.

- Ventajas:
  - Ofrece visibilidad total de dispositivos conectados a la red.
  - Se puede bloquear dispositivos externos.
  - Tiene buenas funcionalidades para sacar reportes.
  - Su implementación no necesita agente.
  - Monitoreo pasivo de la red.
- Desventajas:
  - Debería mejorar en el análisis de los dispositivos para determinar si su comportamiento es malicioso o no.
  - A veces se experimentan errores de detección en la revisión de cumplimiento.
  - Muy costoso.

Cabe anotar que el número de ventajas y desventajas varía de acuerdo al número de reseñas hechas por los expertos en cada uno de los portales consultados. En cuanto a la compatibilidad de cada solución con el entorno tecnológico de la empresa no se presentan diferencias, ya que los dispositivos de red de la entidad son del fabricante Cisco, los cuales son soportados por la mayoría de soluciones NAC en el mercado. Teniendo en cuenta lo anterior, y más importante aún, la opinión de la entidad, se decidió optar por utilizar la solución Cisco ISE para el desarrollo del proyecto.

10.2.2. Revisión de la solución para el control de acceso

De acuerdo al objetivo planteado, y con el fin de desarrollar una ficha técnica que le ayude a la Entidad a entender la viabilidad técnica y financiera de la implementación de una solución NAC para el control de acceso a los recursos de la red mitigando riesgos de seguridad, se montó un demo de la herramienta para evidenciar el alcance de la solución y sus ventajas.

Una estrategia de seguridad de la información es disponer de elementos de red que permitan habilitar un control de acceso perimetral como lo son los *firewalls*. Para complementar la seguridad en el acceso lógico, las empresas implementan soluciones de control de acceso a la red, es decir, que permita a los administradores de red establecer políticas de cumplimiento para el acceso e identificación de los usuarios y sus equipos, conocer información de lugar y hora de ingreso a la red corporativa, y limitar el uso de los recursos de acuerdo a los permisos otorgados al rol de la persona.

Como se dispone de una red compuesta por equipos de red del fabricante Cisco, es conveniente implementar, como se mencionó en un apartado anterior, una solución que sea compatible con el entorno tecnológico de la empresa para poder explotar todas sus funcionalidades y tener el mayor cubrimiento en soporte posible. Por lo anterior, se decidió buscar al fabricante de los elementos de comunicación de la entidad con los cuales se logró obtener una completa licencia sin restricción durante 90 días para montar un demo de implementación de la solución **Cisco Identity Service Engine (ISE)**, que como se mostró en la sección *10.2.1*, es una herramienta que se encuentra dentro de las mejor catalogadas por los profesionales en el negocio.

SITUACIÓN ACTUAL DE ACCESO A LA RED CABLEADA

La entidad no dispone de seguridad en la red LAN cableada, los puertos están en modo acceso y pertenecen a una VLAN determinada para un uso específico.

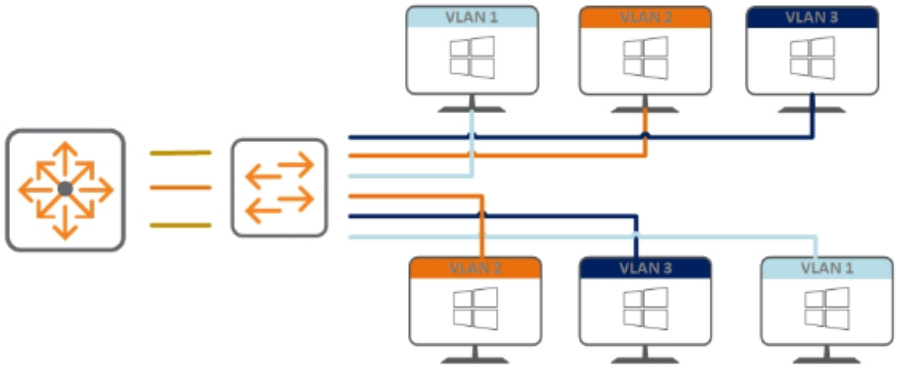


Figura 5. Acceso a la red sin restricción.

SITUACIÓN ACTUAL DE LA RED INALÁMBRICA

La red inalámbrica se encuentra centralizada y configurada en un WLC, que cuenta con seguridad WAP2-SPK en todos los SSID de la empresa.

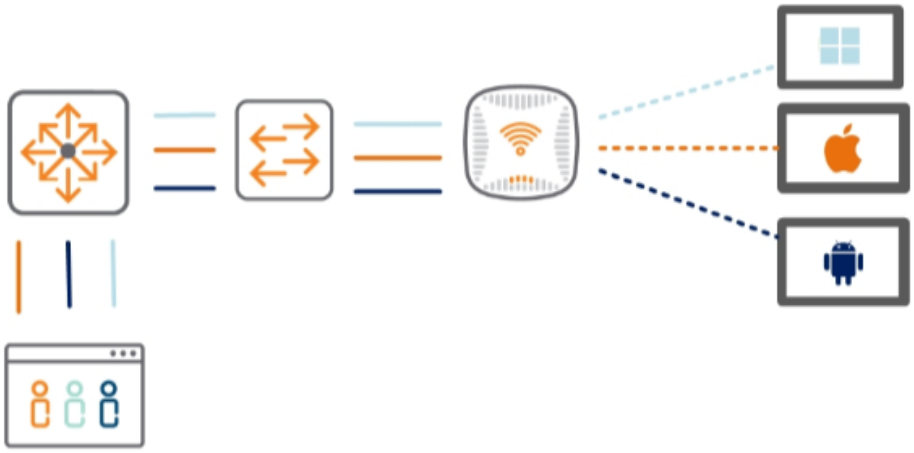


Figura 6. Configuración de red inalámbrica.

CONFIGURACIÓN REALIZADA PARA EL MONTAJE DEL DEMO

Para la red cableada se configuró un Stack de 4 switches con los diferentes segmentos de red que hay distribuidos en la entidad. Su uso fue exclusivo para las pruebas de verificación del control de acceso. En la herramienta se configuraron políticas para usuarios internos y su autenticación se basó en accesos definidos con ACL. También se configuró una política perfilada para los teléfonos con ACL. Por

último, se configuraron políticas de revisión de postura a los equipos de los funcionarios internos.

Por otro lado, para la red inalámbrica se crearon 3 SSID de prueba con autenticación al ISE.

- SSID VIP con autenticación MAC.
- SSID de *Funcionarios* con autenticación por DA y revisión de postura.
- SSID de *Invitados* con autenticación de registro de usuario con patrocinador.

En la Tabla 1 se muestran las políticas con ACL creadas para los tipos de acceso mencionadas anteriormente.

No.	Tipo de Acceso	Tipo de Usuario	Autenticación	Perfilamiento por Dispositivo	Asiganción de VLAN	Servicios a alcanzar	Revisión de postura
1	Wired	Interno	DA	PC - Teléfono IP	La VLAN del respectivo piso	10.2.2.0/23 (Servidores) 10.2.4.0/23 (Impresoras)	Funcionarios
2	Wired	Externo	ISE		Invitados	10.2.2.2 (DHCP) 10.2.2.91 (DNS)	Invitados
3	Wireless	Externo	ISE		Invitados	10.2.2.2 (DHCP) 10.2.2.91 (DNS)	Invitados
4	Wireless	Interno	DA	PC - Teléfono Móvil	Funcionarios	10.2.2.0/23 (Servidores) 10.2.4.0/23 (Impresoras)	Funcionarios

Tabla 1. Políticas configuradas para la entidad.

METAS PROPUESTAS A PARTIR DEL MONTAJE DEL DEMO

Con el despliegue de la herramienta y la prueba demo se espera verificar lo siguiente:

- Cómo se protege la red desde las conexiones de acceso al medio.
- Cómo se garantiza una conexión diferenciada entre usuarios internos y

externos brindando seguridad en la red.

- Cómo simplificar las tareas de administración y protección al centralizar estas tareas en el servicio de Cisco ISE.
- La limitación del acceso a los recursos dependiendo de los permisos otorgados.

MÉTODOS DE AUTENTICACIÓN

Durante el proceso, se identificó que la herramienta proporciona tres funciones para permitir un control de acceso a la red más escalable, las cuales son: autenticación, clasificación y autorización.

La autenticación identifica los endpoints mediante la adquisición y validación de las credenciales del dispositivo. En el proceso de autenticación, el sistema correlaciona atributos de los dispositivos con políticas específicas clasificándolos en una categoría o grupo, una vez se cumple lo anterior, se concede la autorización de acceso a la red.

Existen tres métodos de autenticación:

- Autenticación de endpoint basada en 802.1X[31].
- Bypass de autenticación MAC: Este método se utiliza para autenticar un dispositivo usando su dirección MAC como credencial[32].
- Autenticación web mediante portal cautivo: Este método se utiliza cuando el endpoint se atiende con un usuario, pero no hay un solicitante 802.1X instalado o habilitado en la máquina[33].

[31] https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26.html
[32] https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26.html
[33] https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26.html

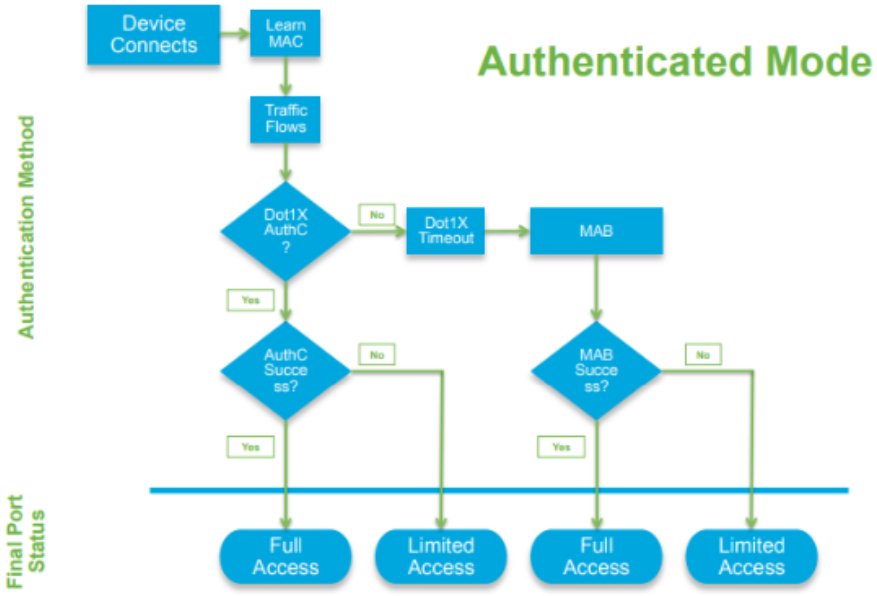


Figura 7. Diagrama de flujo de autenticación Cisco ISE[34].

Como el comportamiento predeterminado de 802.1X es negar el acceso a la red cuando falla una autenticación, se debe usar el *bypass* de autenticación MAC para todas las impresoras y otros dispositivos no autenticados. Para este tipo de equipos, una vez surta el tiempo de espera del *dot1x*, se producirá un *bypass* de autenticación (MAB) con previo registro de la dirección MAC en el Cisco ISE.

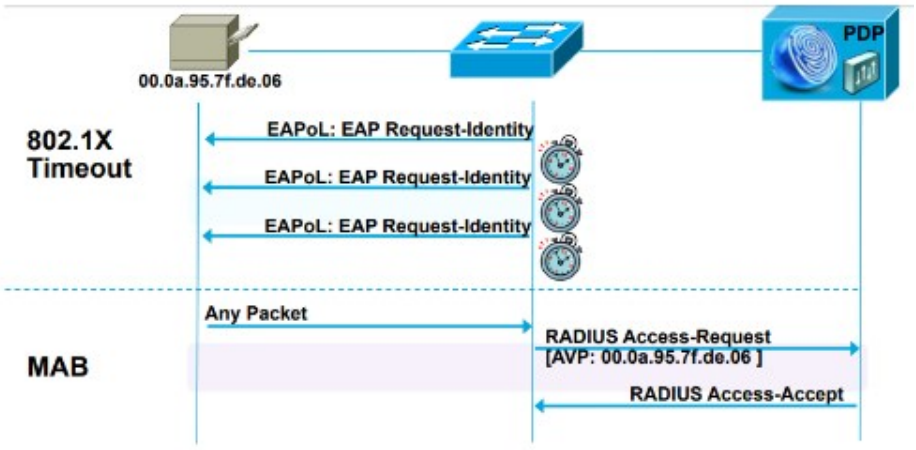


Figura 8. Dispositivos sin autenticación 802.1X[35].

[34] http://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/TrustSec_2-0/trustsec_2-0_dig.pdf
[35] http://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/TrustSec_2-0/trustsec_2-0_dig.pdf

VALIDACIÓN DE COMPATIBILIDAD DE DISPOSITIVOS

De acuerdo a uno de los parámetros de elección mencionado en el apartado anterior *10.2.1. Elección Solución NAC*, se revisó la matriz de compatibilidad de Cisco ISE a partir de los dispositivos que hay en la entidad.

Se extrajeron de la tabla de la Tabla 2 los switches con los que cuenta la entidad, además de verificar que todos los dispositivos cuentan con SO superior al mínimo solicitado.

Por otro lado, de la Tabla 3 se extrajo la controladora con la que cuenta la entidad, e igualmente se verificó la versión de sistema operativo.

Device	Validated OS [1] / Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
Catalyst 2960–XR Catalyst 2960–X	Cisco IOS 15.2(2)E6 Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2 Cisco IOS 15.2.6E1(ED) Cisco IOS 15.2(2)E9	✓	✓	✓	✓	✓	✓	✓	✓
	Cisco IOS 15.0.2A-EX5	✓	✓	✓	✓	✓	✓	✓	✓
Catalyst 4500-X	Cisco IOS XE 3.6.6 E Cisco IOS 15.2(2)E5 Cisco IOS 15.2(4)E2 Cisco IOS 15.2(6)E	✓	✓	✓	✓	✓	✓	✓	✓
	Cisco IOS XE 3.4.4 SG	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 6807-XL	Cisco IOS 152-1.SY1a	✓	✓	✓	✓	✗	✓	✓	✓
Catalyst 6880-X (VS-S2T-10G)	Cisco IOS 15.0(1)SY1	✓	✓	✓	✓	✗	✓	✓	✓
[1] Validated OS is the version tested for compatibility and stability.									
[2] See the Cisco TrustSec Product Bulletin for a complete list of Cisco TrustSec feature support.									
[3] Minimum OS is the version in which the features got introduced									

Tabla 2. Switches de acceso compatibles con Cisco ISE[36].

[36] https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/compatibility/b_ise_sdt_26.html#supportedciscoaccessswitches

Device	Validated OS [4]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec
WLC 8540	AireOS 8.1.131.0	√	√	√	√	X	√	√	X
	AireOS 8.1.122.0 (minimum)	√	√	√	√	X	√	√	X
[4] Validated OS is the version tested for compatibility and stability									

Tabla 3. Controladores compatibles con Cisco ISE.

Luego de verificar los switches y la controladora, se procedió a verificar la compatibilidad de los puntos de acceso como se muestra en la Tabla 4, en la que se extrae el dispositivo que se encuentra en la entidad.

Cisco Access Point	**Minimum Cisco Mobility Express Version**	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec
Cisco Aironet 3800 Series	Cisco Mobility Express 8.7.106.0	✓	X	✓	✓	X	X	X	X

Tabla 4. Puntos de acceso compatibles con Cisco ISE.

A parte de los equipos de red, y como parte de la verificación de compatibilidad, se validaron también los llamados *External Indentity Source*. Para que Cisco ISE se integre con el AD, fue necesario disponer de *User* y *Password* con privilegios para agregar y borrar dispositivos.

External Identity Source	OS/Version
Active Directory [5] [6] [7]	
Microsoft Windows Active Directory 2016	—
Microsoft Windows Active Directory 2019 [8]	—
[5] Cisco ISE OCSP functionality is available only on Microsoft Windows Active Directory 2008 and later.	
[6] Microsoft Windows Active Directory version 2000 or its functional level is not supported by Cisco ISE.	
[7] You can only add up to 200 Domain Controllers on ISE. On exceeding the limit, you will receive the following error: Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200	
[8] Cisco ISE supports all the legacy features in Microsoft Windows Active Directory 2019, from Cisco ISE Release	

Tabla 5. External Identity Source compatibles con Cisco ISE.

Por último, para terminar la verificación de compatibilidad, se validó el sistema operativo de los clientes. Todos los solicitantes 802.1X se pueden usar con Cisco ISE versión 2.4 con sus características estándar y avanzadas superiores, siempre y cuando admitan método de autenticación compatible con Cisco ISE.

Client Machine Operating System	Web Browser	Supplicants (802.1X)	Cisco ISE	Cisco Temporal Agent	AnyConnect
Microsoft Windows 10					
Windows 19H2	Microsoft IE 11	Microsoft Windows 10 802.1X Client	2.6	4.5 or later	4.6.01098 or later
Windows 19H1	Mozilla Firefox	AnyConnect Network Access Manager			
Windows 10 Enterprise	Google Chrome				
Microsoft Windows 8					
Windows 8.1	Microsoft IE 11	Microsoft Windows 8 802.1X Client	2.6	4.5 or later	4.6.01098 or later
Windows 8	Mozilla Firefox	AnyConnect Network Access Manager			
Windows 8 x64	Google Chrome				

Tabla 6. Microsoft Windows compatible con Cisco ISE.

10.2.3 Implementación Demo

La topología implementada para el control de acceso a la red se basó en una máquina virtual de Cisco ISE donde se tienen los servicios de administración, políticas, y monitoreo. Esta máquina se ejecuta sobre una plataforma de virtualización que en este caso es VMware ESX, que, para efectos de redundancia y ahorro en esquemas de licenciamiento, se implementó en alta disponibilidad para evitar así el uso de otra máquina.

Teniendo en cuenta la información obtenida de la *Fase I del Análisis de*

Vulnerabilidad sobre la infraestructura tecnológica, y la topología de la red, los problemas de seguridad que se pretendieron corregir con la implementación del control de acceso a la red son:

- Control de Acceso: El método empleado en la entidad para los procesos de autenticación se basa únicamente en el acceso al SO del dispositivo mediante el AD. Para lograr acceso a los recursos corporativos solo se requiere conectar el dispositivo a un punto de red o al servicio WiFi, con lo que ya tendría alcance a todos los segmentos de red.

  Debido a lo anterior, con la plataforma Cisco ISE se realiza el control de acceso a la red aplicando el protocolo 802.1X de autenticación, con el cual la idea es crear una comunicación con el servidor RADIUS, que a su vez se comunica con el AD para validar las credenciales ingresadas por parte del usuario solicitante, y de ser correcto, se realiza el perfilamiento para darle acceso solo a lo que tenga permitido.

- Visibilidad en la red: Durante el proceso de entrevistas iniciales, no se pudo determinar cómo se monitoreaban las redes alcanzadas por los usuarios conectados a la red LAN ni la identificación de equipos.

  Con Cisco ISE, mediante el proceso de autenticación AAA, se pueden conocer los horarios de inicio sesión, ubicación e identificación en los dispositivos de red, obteniendo información que permite diseñar políticas de control aplicables a múltiples usuarios de la entidad.

- Perfilamiento: Se evidenció que para los dispositivos tales como Impresoras y Teléfonos IP, el perfilamiento se realiza por medio de la asignación de una VLAN en un punto de red dedicado y por medio de una configuración de VLAN de voz respectivamente.

  Utilizando *bypass* de autenticación MAC es posible asignar este tipo de

dispositivos a grupos de políticas configuradas para utilizar el perfilamiento de Cisco ISE.

DISEÑO

La solución propuesta para el control de acceso a la red se basa en un sistema dinámico de autenticación, permitiendo el acceso a los recursos de red de una manera segura y confiable.

Mediante el protocolo 802.1X y las características AAA de autenticación, autorización y contabilidad, se aumenta la visibilidad y se mejora el proceso de comparación utilizado, resaltando que el manejo se realiza desde un punto central.

Para aplicar las políticas de autenticación y autorización, la solución se integró con el AD de la entidad a partir de una cuenta con privilegios para consultar usuarios y grupos ya creados, y agregar o eliminar equipos en el AD. De igual forma, se registró en el DNS interno con el nombre correspondiente.

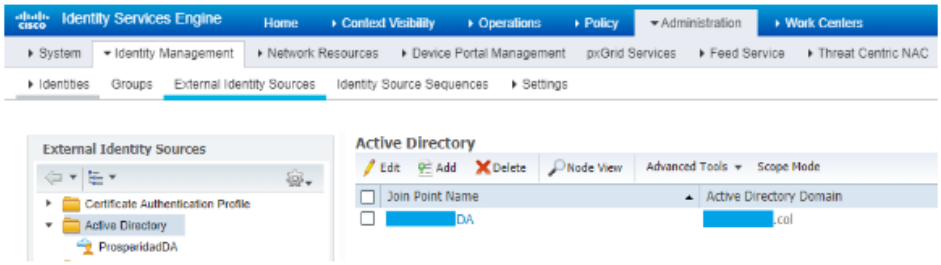


Figura 9. Integración con el AD.

CONFIGURACIÓN GLOBAL DE EQUIPOS ACTIVOS

Aunque Cisco ISE se encarga de todo el proceso de autenticación, es necesario configurar los equipos que intervienen para que esa comunicación sea posible. Cabe mencionar nuevamente que las configuraciones mostradas en las figuras a continuación se realizaron sobre equipos de marca Cisco, por lo que los comandos son estándar y tomados de las recomendaciones dadas por el fabricante

para implementar en sus dispositivos. La documentación de cada comando es con el objetivo de entender su función[37].

Configuración Global AAA
Habilitar la autenticación, autorización y contabilidad en los conmutadores de acceso. Por defecto, el "subsistema" AAA del conmutador Cisco está deshabilitado. Antes de habilitar el subsistema AAA, ninguno de los comandos requeridos estará disponible en la configuración. • (config)#**aaa new-model** comandos AAA necesarios para la autenticación 802.1x con Cisco ISE. • (config)# **aaa group server radius ISE** • (config)# **server 10.2.2.61 auth-port 1812 acct-port 1813** Asocia un servidor RADIUS particular con el servidor definido para el grupo. Cada servidor de seguridad se identifica por su dirección IP y número de puerto UDP. Se crea un método de autenticación para 802.1X. se requiere un método de autenticación para instruir al conmutador sobre qué grupo de servidores RADIUS usar para Solicitudes de autenticación 802.1X. • (config) #**aaa authentication dot1x default group ISE** Use local database • (config) #**aaa authorization exec default local** Con el paso anterior se permitirá que la identidad del usuario / dispositivo (nombre de usuario / contraseña o certificado) sea validado por el servidor RADIUS. Sin embargo, simplemente tener credenciales válidas no es suficiente. Debe haber una autorización también. La autorización es lo que define que el usuario o dispositivo puede acceder la red y qué nivel de acceso se permite realmente. • (config) # **aaa authorization network default group ISE** Configura la autorización de red a través de RADIUS. Se usa para gobernar la asignación de direcciones, la aplicación de listas de acceso y varias otras cantidades por usuario. • (config) # **aaa authorization auth-proxy default group ISE**

[37] http://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/TrustSec_2-0/trustsec_2-0_dig.pdf

Los usuarios normalmente están bloqueados por ACL. Proxy de autenticación (auth-proxy)
permite a los navegadores ir al firewall y autenticarse a través de RADIUS, el servidor
Permite acceso adicional.

- (config) # **aaa accounting update periodic**

Método de contabilidad para 802.1X.
Los paquetes de contabilidad RADIUS. Este tipo de paquetes ayudará a garantizar que el servidor RADIUS (Cisco ISE) conozca el estado exacto del puerto de conmutación y el punto final.
Sin los paquetes de contabilidad, Cisco ISE solo tendría conocimiento de la autenticación y comunicación de autorización. Los paquetes de contabilidad proporcionan información sobre la duración de la sesión autorizada, así como las decisiones locales tomadas por el conmutador (como la asignación de VLAN AuthFail, etc.)

- (config)# **aaa accounting dot1x default start-stop group ISE**

Habilitar cambio de autorización (CoA).
Definida la dirección IP del servidor RADIUS al que el conmutador enviará mensajes RADIUS.
Sin embargo, definimos los servidores que pueden realizar operaciones de Cambio de autorización (RFC 3576) en una lista diferente, también dentro del modo de configuración global.

- (config) #**aaa server radius dynamic-author**
- (config) #**client 10.2.2.61 server-key #####**

Tabla 7. Habilitación servicios AAA.

Para que el conmutador realice el redireccionamiento de URL para la autenticación web, así como la redirección del tráfico de descubrimiento desde el agente de postura (Agente Cisco NAC) hacia el servidor Cisco ISE, se habilitó el protocolo 802.1X en los dispositivos activos como se muestra a continuación:

Configuración Global 802.1X.
Habilitar 802.1X globalmente en el conmutador. • (config) # **dot1x system-auth-control** Habilitar las ACL descargables para que funcionen. Las listas de control de acceso descargables (DACL) son un mecanismo de aplicación muy común en un Cisco, Para que las DACL funcionen correctamente en un conmutador, el seguimiento del dispositivo IP debe ser habilitado. • (config) # #**ip device tracking**

Tabla 8. Habilitación protocolo 802.1X.

Se configuró un método proactivo para verificar la disponibilidad del servidor RADIUS. Con esto, el interruptor envía mensajes de autenticación de prueba periódica al servidor RADIUS (Cisco ISE).

Configuración Global RADIUS.
Se agrega los servidores Cisco ISE al grupo RADIUS. En este paso agregaremos cada punto de decisión de política (PDP) de Cisco ISE a la configuración del conmutador. • (config) # **radius-server host 10.2.2.61 auth-port 1812 acct-port 1813 key PS#ise** Habilita el equilibrio de carga menos destacado para un grupo de servidores con nombre. • (config) # **load-balance method least-outstanding batch-size** Establecer los criterios muertos. El conmutador se configuró para verificar proactivamente el servidor Cisco ISE en busca de respuestas RADIUS. Ahora configure los contadores en el conmutador para determinar si el servidor está vivo o muerto. Nuestra configuración será esperar 30 segundos para una respuesta del servidor RADIUS e intente la prueba 3 veces antes de marcar el servidor muerto. Si un servidor Cisco ISE no tiene una respuesta válida en 30 segundos, se marcará como inactivo. • (config) # **radius-server dead-criteria time 30 tries 3** Configure el conmutador para usar los atributos específicos del proveedor de Cisco.

Aquí configuramos el conmutador para enviar cualquier atributo específico del proveedor (VSA) definido a los PDP de Cisco ISE durante solicitudes de autenticación y actualizaciones contables.

- (config)#**radius-server vsa send authentication**
- (config)#**radius-server vsa send accounting**

Habilitaremos los atributos específicos del proveedor

- (config) # **radius-server attribute 6 on-for-login-auth**

Hace que la presencia del atributo de tipo de servicio sea obligatoria en los mensajes RADIUS Access-Accept.

- (config) # **radius-server attribute 6 support-multiple**

Admite múltiples valores de tipo de servicio para cada perfil RADIUS.

- (config) # **radius-server attribute 8 include-in-access-req**

Envía la dirección IP del usuario al servidor RADIUS antes de la autenticación del usuario, para que las aplicaciones de servicio pueden comenzar a preparar la información de inicio de sesión del usuario después de la autenticación exitosa del usuario.

Hacer que los servidores no disponibles se omitan inmediatamente o en el período de tiempo, en minutos, durante el cual las solicitudes de transacciones omiten un servidor RADIUS.

- (config) # **radius-server deadtime 30**

Tabla 9. Habilitación servicios RADIUS.

CONFIGURACIÓN DE INTERFACES DE LOS EQUIPOS ACTIVOS

Esta sección se centra en la creación de una configuración aplicable a una interfaz de conexión de los equipos activos y se repite cuantas veces se necesite en los puertos de conexión de los dispositivos finales.

Configuración de Interfaces.

Asegúrese de que los puertos sean puertos de conmutación de capa 2 y en modo acceso y perteneciente a una vlan.

- (config) #**switchport mode access**

En nuestro caso la asignación de la vlan en el puerto será la que este configurada en el switch, ya que esto ya se encuentra organizado por el administrador de red en la entidad.

- (config) #**switchport access vlan X**

Las siguientes configuraciones son las que se encontraron en los puertos de cada equipo activo y no fueron modificadas por petición de la entidad.

- (config) #**spanning-tree bpduguard enable**
- (config) #**spanning-tree portfast**

Se configure la prioridad del método de autenticación en los puertos de conmutación. La mejor práctica es preferir siempre el método de autenticación más fuerte (dot1x). El método dot1x también es el valor predeterminado de todos los conmutadores Cisco.

- (config-if-range) #**authentication priority dot1x mab**

Se configura el orden del método de autenticación en los puertos de conmutación Autenticación 802.1X y luego MAC (MAB).

- (config-if-range) #**authentication order dot1x mab**

Se configura el puerto para usar Flex-Auth.

- (config-if-range) #**authentication event fail action next-method**

Acción de violación.
El modo "restringir", permitirá el primer dispositivo autenticado para continuar con su autorización y denegar cualquier dispositivo adicional.

- (config-if-range) #**authentication violation restrict**

El modo Multi-Auth permite sesión para cada dirección MAC, La autenticación permitirá una sola dirección MAC en el dominio DATA y una sola dirección MAC en la voz
dominio por puerto.

- (config-if-range) #**authentication host-mode multi-auth**

Autenticación activa

- (config-if-range) #**authentication port-control auto**

Se configura el puerto para usar una VLAN local cuando el servidor RADIUS esté "muerto" y reinicialice la autenticación cuando el servidor vuelva a estar "vivo".

- (config-if-range) #**authentication event server dead action authorize vlan vlan-id**
- (config-if-range) #**authentication event server alive action reinitialize**

Se habilita MAC Authentication Bypass en el puerto.

- (config-if-range) #**mab**

Se habilita IEEE 802.1X Authentication en el puerto

- (config-if-range) #**dot1x pae authenticator**

El temporizador tx-period proporcionando una espera predeterminada antes de que un switchport comience el siguiente método de autenticación y comience el MAB proceso para dispositivos no autenticados.

Configure the tx-period timer.

- (config-if-range) #**dot1x timeout tx-period 10**

Tabla 10. Configuración dispositivo activo.

CONFIGURACIÓN EQUIPOS WLAN

Para iniciar, se requirió la IP del servidor Cisco ISE y la clave para asociar. Con estos datos, se procedió a realizar la configuración de los servidores AAA en la Controladora de Red Inalámbrica.

La siguiente configuración no es necesaria para la autenticación 802.1X, pero se requiere para la creación de perfiles en Cisco ISE de los dispositivos que se conectan a la red WLAN, ya que con la dirección MAC versus la IP, el servicio de políticas ISE puede descubrir y recopilar atributos para fines de clasificación.

Figura 10. Servidor autenticación RADIUS.

Atributo	Value
Server Index (Priority)	1
Server IP Address	10.2.2.61
Shared Secret Format	ASCII
Shared Secret	#######
Key Wrap	(Not checked)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	Enabled (checked)
Management	Enabled (checked)
Tunnel Proxy	(Not checked)
IPSec	(Not checked)

Tabla 11. Configuración autenticación servidor RADIUS.

Atributo	Valor
Server Index (Priority)	1
Server IP Address	10.2.2.61
Shared Secret Format	ASCII
Shared Secret	######
Port Number	1813
Server Status Enabled	Enable
Server Timeout	2 seconds
Network User Enabled	(checked)
Tunnel Proxy	(Not checked)
IPSec	(Not checked)

Tabla 12. Configuración servidor de accounting RADIUS.

Una vez configurados los servidores, se configuraron los SSID asociándolos con la solución Cisco para el control de la autenticación y autorización.

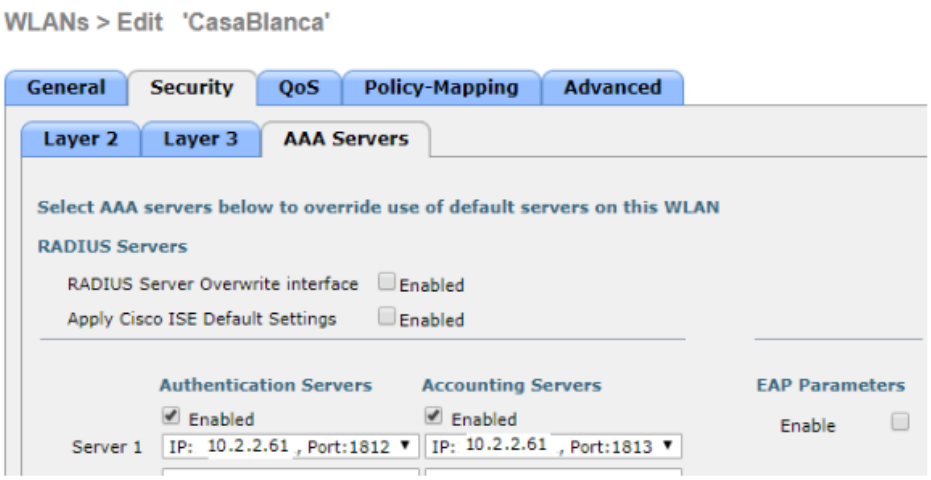


Figura 11. Habilitación de servidores AAA en SSID.

Para completar la configuración en la pestaña *Advance* se debió chequear la opción *allow AAA Override*.

ADICIÓN DE DISPOSITIVOS DE RED A CISCO ISE

Una vez realizada la configuración de los dispositivos de red para el proceso de autenticación, se deben integrar con Cisco ISE los encargados de la autorización y control de los dispositivos de red.

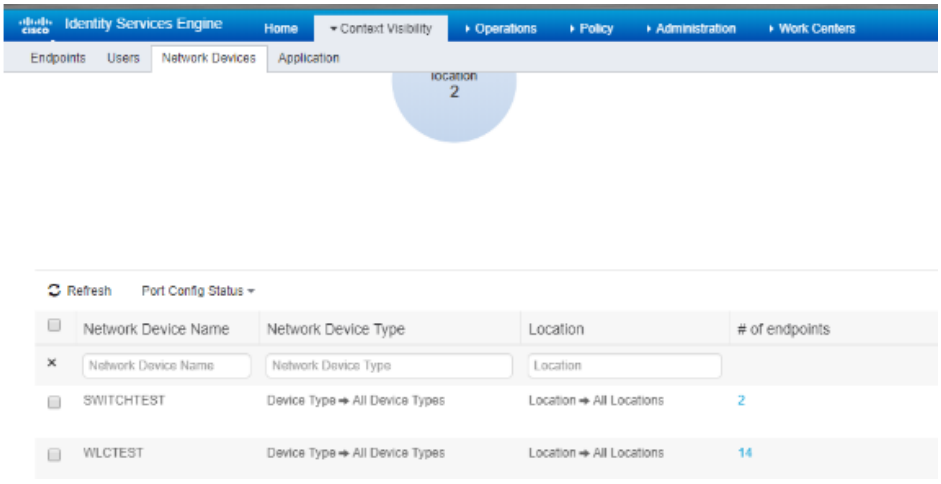


Figura 12. Registro dispositivos de red en Cisco ISE.

CONFIGURACIÓN DE ACCESO A LOS RECURSOS

Los componentes básicos de esta arquitectura se describen a continuación:

- NAD (Network Access Device): Dispositivo de acceso a la red que puede ser cableado (switch), inalámbrico (AP) o Firewall (VPN).
- Servidor RADIUS: Función que cumple Cisco ISE.
- Suplicante del cliente: Puede ser nativo, propio de la plataforma o descargable en el momento del acceso.

El ISE como punta de la directiva proporciona los parámetros de autorización como la lista de control de acceso descargada (DACL) /VLAN/Redirect-URL/Redirect. Tradicionalmente, para que la revisión de postura suceda, se requiere NADs para soportar el cambio de dirección (dar instrucciones al usuario o al software agente que el nodo de ISE debe ser contactado), y el cambio de la autorización (CoA) de *reauthenticate* al usuario después de que el estado de la postura del endpoint se determina[38].

Existe una política de autenticación que detecta si un usuario está intentando entrar por medio de uno de los métodos *dot1x*, *MAB*, etc. La autenticación se aplica al usuario o endpoint que se está conectando sin darle una autorización todavía. Para que eso suceda, hay una política de autorización que revisa varios parámetros como grupo de AD, dominio del PC y tipo de dispositivo, que, según su valor, le da un nivel de acceso al endpoint. La lógica más simple para pensar en las condiciones es:

- *Si <Condición>, entonces <Resultado>.*
- *Si <Tipo de Autenticación>, entonces <Usar almacén de identidades>.*
- *Si <Usuario y/o endpoint cumple con esta condición>, entonces <Conceder cierto nivel de acceso>[39].*

[38] https://www.cisco.com/c/es_mx/support/docs/security/identity-services-engine-22/210523-ISE-posture-style-comparison-for-pre-and.html
[39] http://www.network-node.com/blog/2015/12/31/ise-20-dot1x-policy-configuration

A continuación, se muestra la configuración de las DACL que, para nuestro caso, es la que permite delimitar las fronteras de acceso a los recursos de la entidad. La vida útil de la ACL es la duración de la sesión del usuario. Estas son ACLs portátiles, es decir, si el usuario o el endpoint se desconecta, ésta no permanece en la configuración NAD una vez finalizada la sesión.

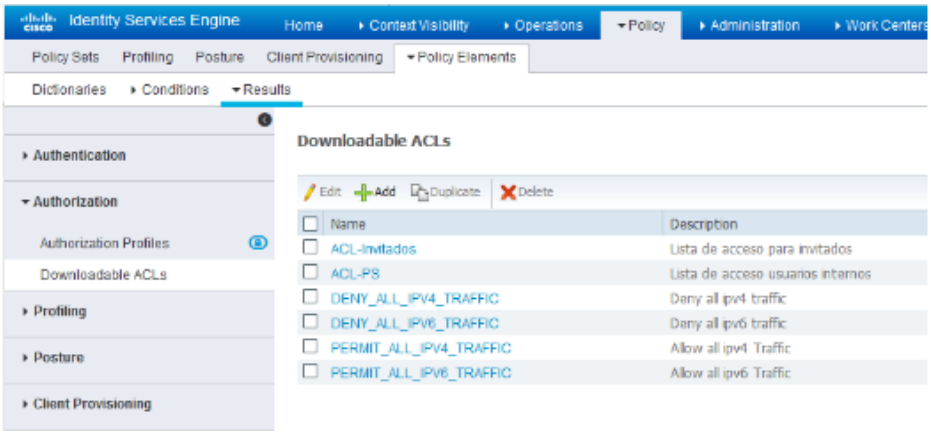


Figura 13. ACLs configuradas.

Se determinó que el acceso para *Invitados* y *Funcionarios* se realizara de la misma forma para conexiones cableadas e inalámbricas, por lo que solo se requiere de dos ACL para esta configuración. En el caso de una conexión de invitados, solo se tiene acceso a los servicios de DHCP, DNS y salida a internet. Para el caso de funcionarios, se tiene acceso a la red de servidores, impresoras, su propio segmento y a internet.

ACL Invitados	ACL-PS
permit udp any any eq domain	permit udp any any eq domain
permit udp any any eq bootpc	permit udp any any eq bootpc
permit ip any host 10.2.2.2	permit ip any 10.2.2.0 0.0.1.255
permit ip any host 10.2.2.91	permit ip any 10.2.4.0 0.0.1.255
deny ip any 10.2.0.0 0.0.255.255	deny ip any 10.2.0.0 0.0.255.255
permit ip any any	permit ip any any

Tabla 13. Detalle de las ACL.

Para el acceso por WiFi, la ACL se creó en la Controladora WiFi (WLC), y en ISE le indica qué aplicar.

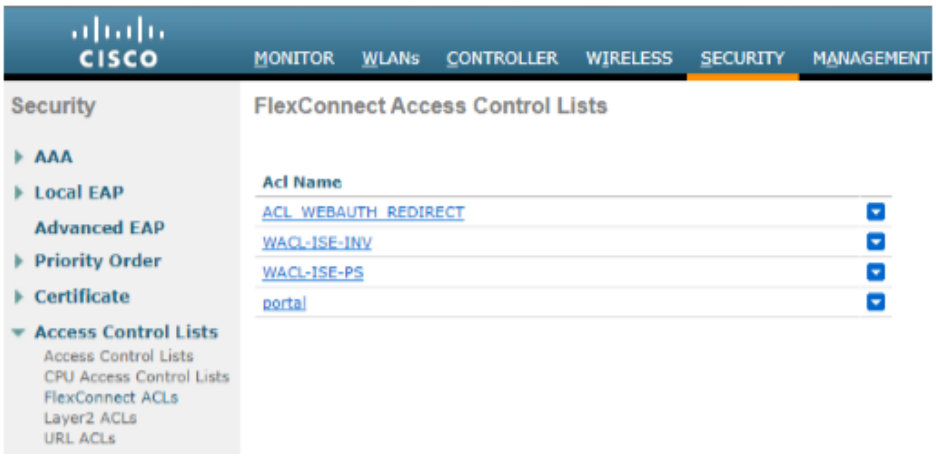


Figura 14. ACL en el WLC.

DESCRIPCIÓN DE LAS ACLs

La siguiente ACL redirecciona el tráfico hacia el ISE para autenticación web.

ACL_WEBAUTH_REDIRECT							
Seq	**Action**	**Source IP/Mask**	**Destination IP/Mask**	**Protocol**	**Source Port**	**Dest Port**	**DSCP**
1	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	UDP	DNS	Any	Any
2	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	UDP	Any	DNS	Any
3	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	UDP	DHCP Client	DHCP Server	Any
4	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	UDP	DHCP Server	DHCP Client	Any
5	Permit	10.2.2.61/ 255.255.255.255	0.0.0.0/0.0.0.0	TCP	8443	Any	Any
6	Permit	0.0.0.0/0.0.0.0	10.2.2.61/ 255.255.255.255	TCP	Any	8443	Any

Tabla 14. ACL para autenticación web.

La siguiente ACL es para el acceso de invitados a Internet.

WACL-ISE-INV							
Seq	**Action**	**Source IP/Mask**	**Destination IP/Mask**	**Protocol**	**Source Port**	**Dest Port**	**DSCP**
1	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	UDP	DNS	Any	Any
2	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	UDP	Any	DNS	Any
3	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	UDP	DHCP Client	DHCP Server	Any
4	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	UDP	DHCP Server	DHCP Client	Any
5	Deny	0.0.0.0/0.0.0.0	10.20.0.0/ 255.255.254.0	Any	Any	Any	Any
6	Deny	0.0.0.0/0.0.0.0	10.20.2.0/ 255.255.254.0	Any	Any	Any	Any
7	Deny	0.0.0.0/0.0.0.0	10.20.4.0/ 255.255.254.0	Any	Any	Any	Any
8	Deny	0.0.0.0/0.0.0.0	10.20.6.0/ 255.255.254.0	Any	Any	Any	Any
9	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	Any	Any	Any	Any

Tabla 15. ACL acceso invitados a internet.

La siguiente ACL es para el acceso de los funcionarios.

WACL-ISE-PS							
Seq	**Action**	**Source IP/Mask**	**Destination IP/Mask**	**Protocol**	**Source Port**	**Dest Port**	**DSCP**
1	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	UDP	DNS	Any	Any
2	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	UDP	Any	DNS	Any
3	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	UDP	DHCP Client	DHCP Server	Any
4	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	UDP	DHCP Server	DHCP Client	Any
5	Permit	10.2.72.0/ 255.255.254.0	10.2.72.0/ 255.255.254.0	Any	Any	Any	Any
6	Permit	0.0.0.0/0.0.0.0	10.2.2.0/ 255.255.254.0	Any	Any	Any	Any
7	Permit	10.2.2.0/ 255.255.254.0	0.0.0.0/0.0.0.0	Any	Any	Any	Any
8	Deny	0.0.0.0/0.0.0.0	10.20.0.0/ 255.255.0.0	Any	Any	Any	Any
6	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	Any	Any	Any	Any

Tabla 16. ACL para acceso de funcionarios.

El perfil de la autorización contiene la configuración que da lugar a los atributos que se pasan desde el Cisco ISE a los dispositivos de acceso a la red (NAD), los cuales se utilizan para determinar el nivel de acceso deseado[40].

[40] https://www.cisco.com/c/es_mx/support/docs/security/identity-services-engine/214975-configure-eap-tls-authentication-with-is.html

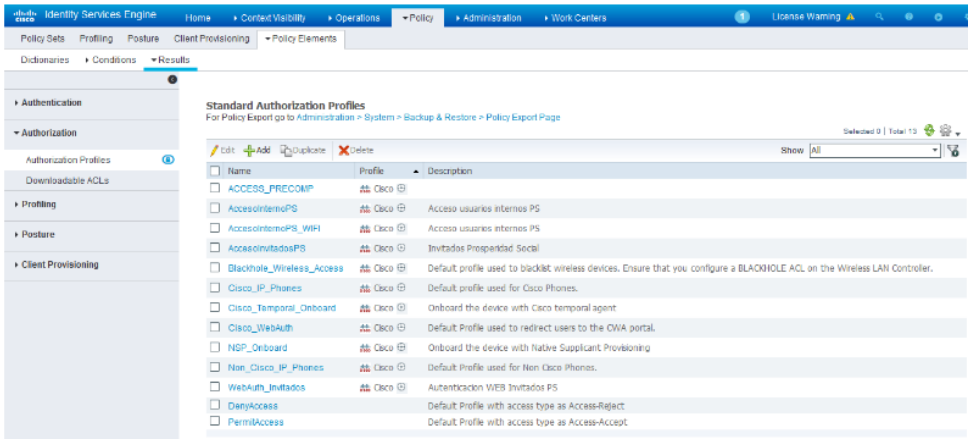


Figura 15. Perfiles de autorización creados.

10.2.4 Experiencia del Usuario

Para el control de las conexiones y del equipo, se puede utilizar el cliente *Cisco AnyConnect* para realizar la integración a la red. De igual forma, el agente es indispensable para realizar la revisión de postura a los equipos que se quieran conectar.

- Al escoger la red para ingresar, ya sea red cableada o WiFi, el cliente hace la detección automáticamente de la conexión.
- Se solicitan credenciales de acceso al usuario interno y a su vez, la validación del certificado (en el caso de la demo, al no estar desplegado, se solicita validar el certificado).

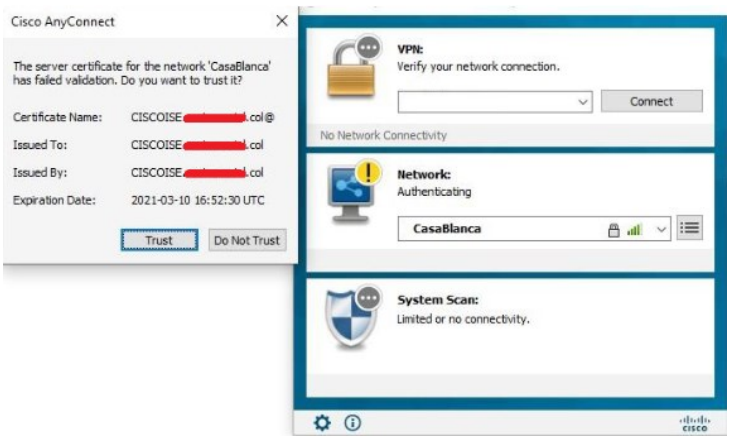


Figura 16. Conexión a la red con agente.

El uso del cliente mencionado anteriormente no es mandatorio para acceder

a la red si las políticas únicamente se limitan a la autenticación desde el administrador de conexiones del sistema operativo. Esto aplica también para la conexión cableada y debe activarse el servicio de Windows *Configuración automática de redes cableadas* para que detecte el protocolo 802.1X.

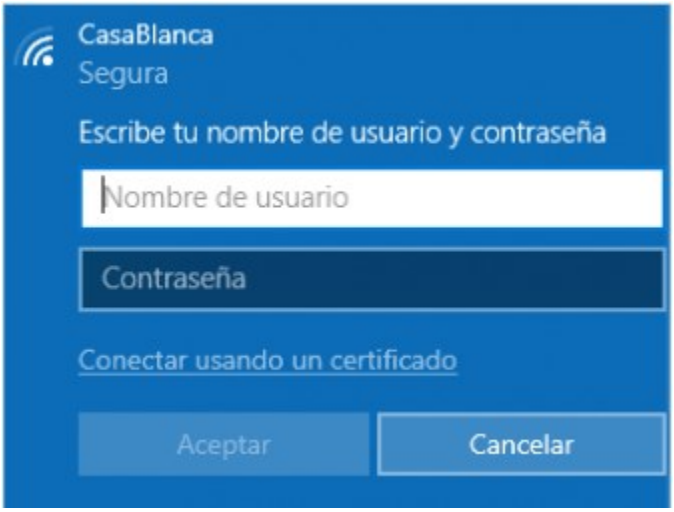
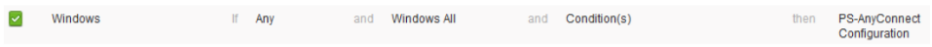


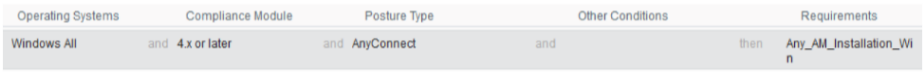
Figura 17. Solicitud de autenticación sin agente.

Por otro lado, se configuró en la demo una política de postura para que se valide el cumplimiento de ciertas condiciones de seguridad al intentar acceder a la red. Por ejemplo:

- Se requiere que el equipo tenga instalado el cliente *Cisco AnyConnect*.



- Se requiere que el equipo tenga instalado un antivirus.



Para verificar los requerimientos se realizó la prueba intentando acceder a la red con un equipo que no tenía el cliente de Cisco instalado. Al momento del ingreso y detectar que no hay cliente, la herramienta lleva al equipo a un *Portal de*

Autoaprovisionamiento.

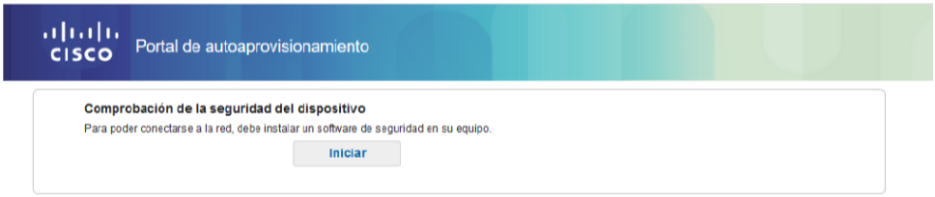


Figura 18. Portal de autoaprovisionamiento.

En el portal, la herramienta descarga el cliente desde el servidor ISE sin necesidad de una conexión a internet. Lo que se requiere es que el usuario tenga permisos de administrador sobre la máquina para instalar el cliente.

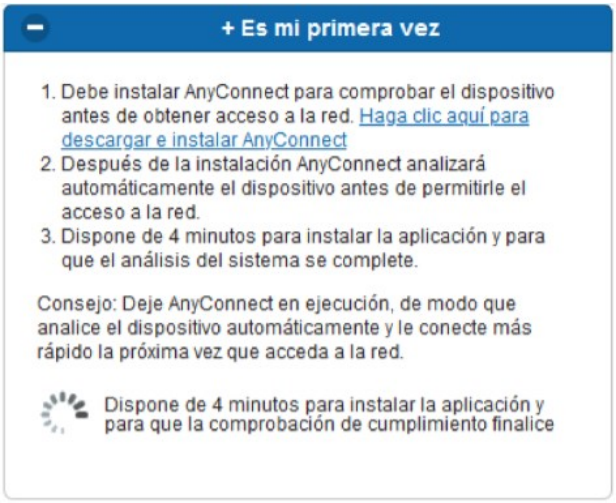


Figura 19. Instalación del cliente.

Una vez instalado el cliente, se realiza la validación de postura para verificar el cumplimiento de la política de seguridad.

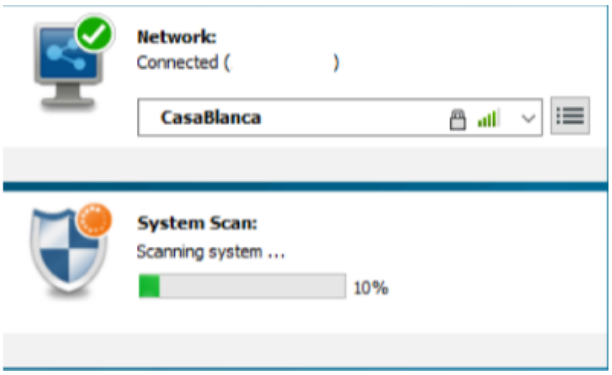


Figura 20. Proceso de escaneo.

Cuando se verifica el cumplimiento de la política de postura, que para este caso es tener instalado un antivirus, la herramienta genera un aviso donde se confirma el permiso para el acceso a la red. Por otro lado, de no cumplir con la política, mostraría un mensaje con el motivo de la no autorización.

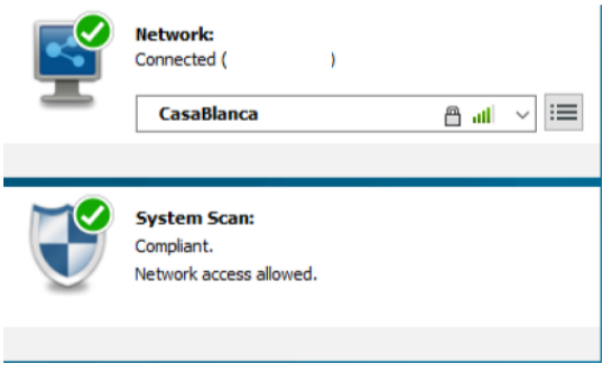


Figura 21. Acceso autorizado.

CONEXIÓN DE USUARIOS INVITADOS

En el proceso se configuró una red para la conexión de los usuarios invitados, lo que les permite acceso solamente a internet para así proteger las redes internas.

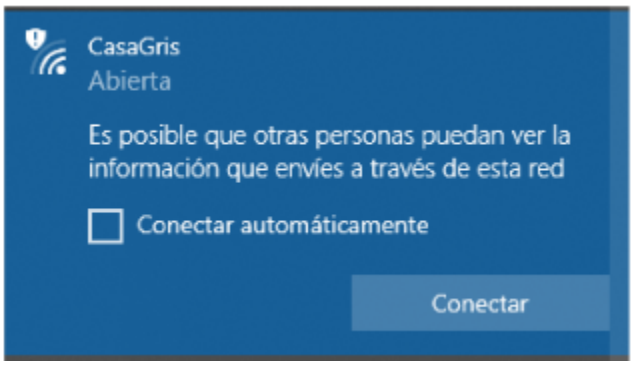


Figura 22. SSID para Invitados.

Como se observa en la Figura 22, la red está abierta para libre conexión de las personas.

El usuario al conectarse, abre un portal de autenticación, en el que pide credenciales para ingresar. Si el invitado ya tiene usuario, deberá ingresarlo y seguir con la conexión, en caso contrario, el invitado deberá registrarse para obtener un nombre de usuario. Para este caso, se habilitó el auto – registro para realizar la prueba de forma práctica. La opción se encuentra en la parte de debajo de la pantalla como muestra la siguiente figura.

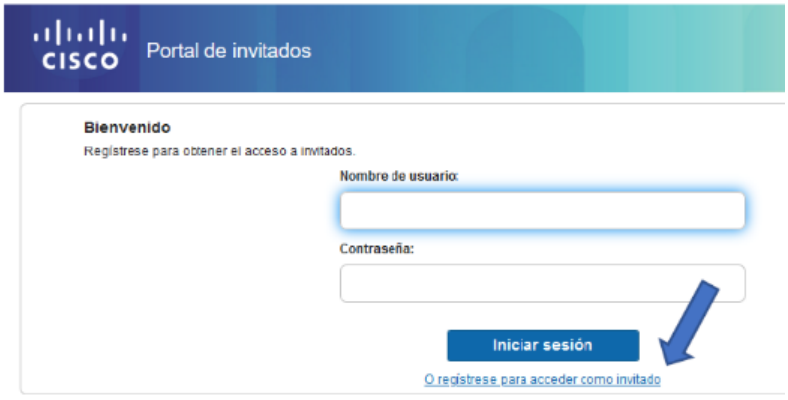


Figura 23. Portal de Invitados.

En el auto – registro aparece un formulario, el cual se puede personalizar según la información que requiera recolectar la entidad.

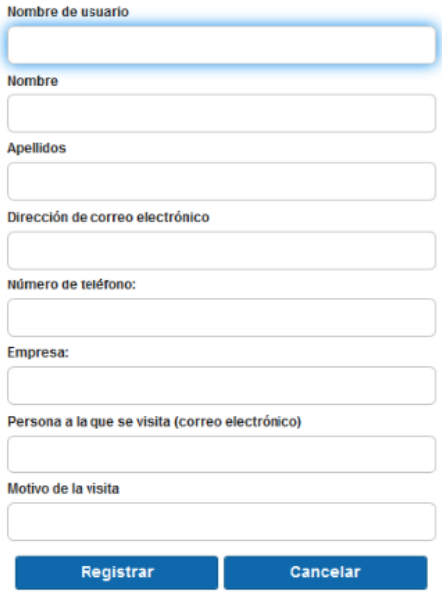


Figura 24. Formulario de registro.

Además de lo anterior, para la conexión de Invitados se tienen las siguientes opciones:

- Usuarios previamente registrados
- Auto – registro con autorización
- Auto – registro sin autorización
- Sin autenticación y política de aceptación
- Códigos de autorización (sin usuario y clave)

10.3. Ejecución – Fase 2: Mitigación de las vulnerabilidades identificadas

La idea principal de este apartado es brindar un conjunto de actividades que se deben llevar a cabo para mitigar y reforzar en la medida de lo posible la seguridad en los equipos de red LAN y WLAN, con la intención de mejorar la dificultad que tendría un atacante en caso de presentarse un acceso no autorizado aprovechando las vulnerabilidades que tienen los equipos. Como se determinó en la etapa del plan de remediación en el análisis de vulnerabilidades realizado en la *Fase I*, las actividades descritas a continuación hacen parte de la plantilla de hardening elaborada como parte de este proyecto y que se puede observar en el Anexo 12. Además, dado que la mayoría de vulnerabilidades encontradas en los equipos de red son temas de versión obsoleta de aplicaciones y protocolos de cifrado, la plantilla de aseguramiento mitigaría los riesgos a

partir de su plano de administración.

- Actualización del SO de los equipos.

  Como con cualquier equipo tecnológico, es importante mantener actualizado el software tal y como recomienda el fabricante. En general, la ruta de migración para una versión del software Cisco IOS es tener siempre la última disponible, ya que ésta incorpora los parches de software actuales, el soporte de hardware y nuevas funcionalidades[41].

CISCO SWITCH	
Versiones encontradas	**Versión instalada**
15.2(4)E7 del 18-Sep-18 15.2(2)E7 del 12-Jul-17 15.2(2)E6 del 08-Aug-2017 15.0(2)EX5 del 21-Apr-2015	15.2.7E1 del 10-Dec-2019

Tabla 17. Versión de IOS en switch de borde.

Actualmente, el fabricante recomienda la versión 15.2.7E2 ED, pero al ser una versión de despliegue temprano (ED), es decir, lanzamiento de software con nuevas funciones que no se requieren, se instala la versión 15.2.7E1. El procedimiento para la actualización se muestra a continuación.

Previamente se realizó la descarga de las versiones de software recomendada e igualmente se validó el espacio en la memoria del dispositivo para copiar la nueva imagen.

Se realiza backup de la configuración del dispositivo y se dirección la copia a un servidor tftp en este caso

#**copy running-config tftp**

Se copia el archivo del IOS desde la ubicación remota por medio del servidor TFTP

#**copy tftp: flash1:**
Address or name of remote host [10.2.7.13]?
Source filename [c2960x-universalk9-mz.152-7.E1.bin]?

[41] https://www.cisco.com/c/es_mx/about/security-center/ios-nx-os-reference-guide.html

Se verifica la integridad de la imagen copiada #**remote command 1 verify /md5 flash:/** c2960x-universalk9-mz.152-7.E1.bin Se modifica el arranque del dispositivo apuntando a la nueva imagen del sistema operativo. (config)#**boot system switch all flash:/** c2960x-universalk9-mz.152-7.E1.bin Se verifica la aplicación del comando #**show boot** BOOT path-list: flash:/ c2960x-universalk9-mz.152-7.E1.bin Por último, se reinicia el dispositivo para que inicie con la nueva versión de software.

Tabla 18. Procedimiento actualización SO.

- Servidor externo AAA para la autenticación de usuario.

  Como buena práctica de seguridad es recomendable usar un servidor externo AAA (TACACS + o RADIUS) para manejar la autenticación, autorización y contabilidad del acceso de los usuarios a los dispositivos.

  #config terminal
  (config)# aaa new-model
  (config)# aaa authentication login default group radius enable
  (config)# radius-server <IP>;
  (config)# radius-server key 'secret-key'
  (config)# line vty 0 4
  (config-line)# login authentication default
  (config-line)# exit
  (config)# line con 0
  config-line)# login authentication default

- Creación de contraseñas con privilegios de administración

  Para otorgar acceso privilegiado de administración al dispositivo IOS, se debe crear una contraseña segura utilizando el comando **enable secret**. Utilizar una contraseña con al menos 10 caracteres de largo que consista

en símbolos alfanuméricos y especiales.
(config)# enable secret strongpassword

- Cifrado de contraseñas en el dispositivo
  Cifrar las contraseñas de texto y evitar que se muestren en el archivo de configuración.
  (config)# service password-encryption

- Eliminación de contraseñas con cifrado inseguro
  Eliminar las contraseñas creadas bajo la ejecución del comando **enable password**.

- Encripción de contraseña de usuario
  Para encriptar la contraseña de los usuarios con hash MD5, se utiliza el comando username secret.
  (config)# username <user> secret <password>

- Intentos máximos de autenticación fallida
  Configurar el número máximo de intentos fallidos de inicio de sesión para que un usuario quede bloqueado después de este umbral.
  (config)# aaa new-model
  (config)# aaa local authentication attempts max-fail <max-attempts>
  (config)# aaa authentication login default local

- Recuperación de contraseña
  Impedir el borrado de contraseña accidental, e impedir a usuarios maliciosos cambiar la configuración registrada y el acceso a NVRAM.
  (config)# no service password-recovery

- Cuentas locales separadas para la autenticación de usuario
  A falta de un servidor AAA externo, crear cuentas locales separadas para cualquier persona a la que le dé acceso a sus dispositivos.

(config)# username <username> secret <password>

- Deshabilitación de servicios no utilizados

  Todo servicio que no se utilice debe ser deshabilitado, en especial, aquellos que utilizan UDP.

  no ip finger, no ip bootp server, ip dhcp bootp ignore, no service dhcp, no mop enabled, no ip domain-lookup, no service pad, no ip http server, no ip http secure-server, no service config, no cdp enable, no cdp run.

- Protocolo de tiempo de red (NTP)

  Tener una configuración de reloj precisa y uniforme en todos los dispositivos de red para que los datos de registro se marquen con la hora y zona horaria correctas.

  (config)#ntp authenticate

  (config)#ntp authentication-key 5 md5 ciscotime

  (config)#ntp trusted-key 5

  (config)#ntp server <IP> key 5

- Redirección de paquetes ICMP

  Un atacante puede explotar la habilidad del router de redireccionar paquetes ICMP y puede ocasionar afectación en el rendimiento del router.

  (config)#no ip redirects

- Inalcanzable ICMP

  La generación de mensajes ICMP a destinos inalcanzables se debe deshabilitar.

  (config)#no ip unreachables

- Proxy ARP

  Ataque de MiTM permite a un host en la red suplantar la MAC de un router. Proxy ARP se puede deshabilitar.

  no ip proxy-arp

- Reemplazo de configuración y reversión de configuración

  Características de reemplazo de configuración y rollback de configuración archivando la configuración del dispositivo Cisco IOS.

  "archive
  path disk0:archived-config
  maximum 14
  time-period 1440
  write-memory"

- Configuración resistente del software Cisco IOS

  Almacenar de forma segura una copia de la imagen del software Cisco IOS y la configuración del dispositivo. Cuando esta función está habilitada, no es posible alterar o eliminar estos archivos de respaldo.

  secure boot-image
  secure boot-config!

- Acceso exclusivo a cambios de configuración

  Solo un administrador realiza cambios de configuración en un dispositivo Cisco IOS en un momento dado.

  configuration mode exclusive auto

- Notificación de cambio de configuración y registro

  Historial de cambios de configuración de un dispositivo Cisco IOS utiliza el comando de configuración de notificación de syslog para permitir la generación de mensajes de syslog cuando se realiza un cambio de configuración.

  archive
  log config
  logging enable
  logging size 200
  hidekeys
  notify syslog

- Unicast RPF

  Permite que un dispositivo verifique que la dirección de origen de un paquete reenviado se pueda alcanzar a través de la interfaz que recibió el paquete.

  interface <interface>

  ip verify unicast source reachable-via <mode>

- Seguridad de IP origen

  Prevención de suplantación de identidad.

  ip dhcp snooping

  ip dhcp snooping vlan <vlan-range>

  Después de que la inspección DHCP está habilitada, estos comandos habilitan IPSG:

  interface <interface-id>

  ip verify source

- Seguridad de Puerto

  Mitigar la suplantación de direcciones MAC en la interfaz de acceso.

  interface <interface>

  switchport

  switchport mode access

  switchport port-security

  switchport port-security mac-address sticky

  switchport port-security maximum <number>

  switchport port-security violation <violation-mode>

- Inspección dinámica de ARP

  Mitigar los ataques de envenenamiento por ARP en segmentos locales.

  ip dhcp snooping

  ip dhcp snooping vlan <vlan-range>

  ip arp inspection vlan <rango-vlan>

- Anti – Spoofing ACL

  La suplantación de identidad se puede minimizar en el tráfico que se origina en la red local si aplica ACL salientes que limitan el tráfico a direcciones locales válidas.

  ip access-list extended ACL-ANTISPOOF-IN
  deny ip <IP> 0.255.255.255 any
  deny ip <IP> 0.0.255.255 any
  !
  interface <interface>
  ip access-group ACL-ANTISPOOF-IN in

11. Resultados

11.1 Fase 1: Resultados Análisis de Vulnerabilidad

El análisis de vulnerabilidad sobre los segmentos catalogados como críticos dentro de la entidad muestra el riesgo que ésta corre actualmente, ya que si bien la mayoría de riesgos descubiertos tienen fácil solución, esto no impide que exista la posibilidad de sufrir los efectos con, o sin intención. En el escaneo se pudieron encontrar gran cantidad de equipos activos en toda la red, y con estos, gran cantidad de vulnerabilidades clasificadas como *críticas* y/o *altas*.

Por ejemplo, en el segmento de *Servidores* se descubrieron 181 equipos activos dentro de la red 10.2.2.0/23, y de los cuales 55 tienen riesgos *Críticos* y/o *Altos* (Ver Tabla 19). Además, se descubrieron 199 riesgos diferentes a lo largo de esta red (Ver Anexo 13) que hacen referencia a inseguridad en el uso de protocolos, aplicaciones con versiones obsoletas y configuración de las máquinas.

Dispositivos en SERVIDORES con vulnerabilidades Críticas y/o Altas						
IP	**Critical**	**High**	**Medium**	**Low**	**Info**	**Total**
10.2.2.11	0	1	13	1	38	53
10.2.2.12	1	0	6	0	27	34
10.2.2.28	0	1	9	1	37	48
10.2.2.42	0	1	13	2	34	50
10.2.2.62	0	3	16	1	39	59
10.2.2.67	0	1	13	3	36	53
10.2.2.73	2	0	11	2	38	53
10.2.2.77	0	1	8	1	39	49
10.2.2.79	0	1	12	2	34	49
10.2.2.81	1	1	13	3	40	58
10.2.2.89	0	1	10	0	42	53
10.2.2.103	2	1	11	1	34	49
10.2.2.105	1	1	10	2	35	49
10.2.2.106	0	1	13	3	32	49
10.2.2.107	2	0	11	2	36	51
10.2.2.118	1	1	13	3	36	54
10.2.2.131	0	1	13	1	36	51
10.2.2.132	0	1	13	1	36	51
10.2.2.142	0	1	11	2	37	51
10.2.2.149	0	1	8	0	29	38
10.2.2.150	0	1	8	0	29	38
10.2.2.194	0	1	7	1	29	38
10.2.2.196	0	5	14	0	25	44
10.2.2.197	0	1	11	0	37	49
10.2.2.205	3	7	17	1	40	68
10.2.2.208	1	1	12	1	38	53
10.2.2.228	1	0	0	2	14	17
10.2.3.3	0	1	12	3	38	54
10.2.3.9	0	1	10	2	30	43
10.2.3.64	0	1	10	2	36	49
10.2.3.79	2	0	11	2	41	56
10.2.3.99	2	3	14	2	49	70
10.2.3.100	0	1	13	3	38	55
10.2.3.101	2	0	11	2	37	52
10.2.3.120	0	1	10	2	34	47
10.2.3.144	1	1	10	2	36	50
10.2.3.146	1	0	8	1	38	48
10.2.3.171	2	1	14	3	43	63
10.2.3.178	0	1	13	2	38	54
10.2.3.182	0	1	11	2	36	50
10.2.3.192	1	0	12	1	36	50
10.2.3.204	0	2	13	3	21	39
10.2.3.205	0	2	13	3	21	39
10.2.3.206	0	2	13	3	19	37
10.2.3.207	0	2	13	3	21	39
10.2.3.208	0	2	13	3	20	38
10.2.3.209	0	2	13	3	21	39
10.2.3.210	0	2	13	4	24	43
10.2.3.211	0	2	12	2	25	41
10.2.3.212	0	2	13	3	21	39
10.2.3.213	0	1	7	4	22	34
10.2.3.214	0	1	7	2	22	32
10.2.3.215	0	2	13	3	19	37
10.2.3.216	0	2	13	3	19	37
10.2.3.243	1	1	15	4	48	69

Tabla 19. Dispositivos en la red Servidores.

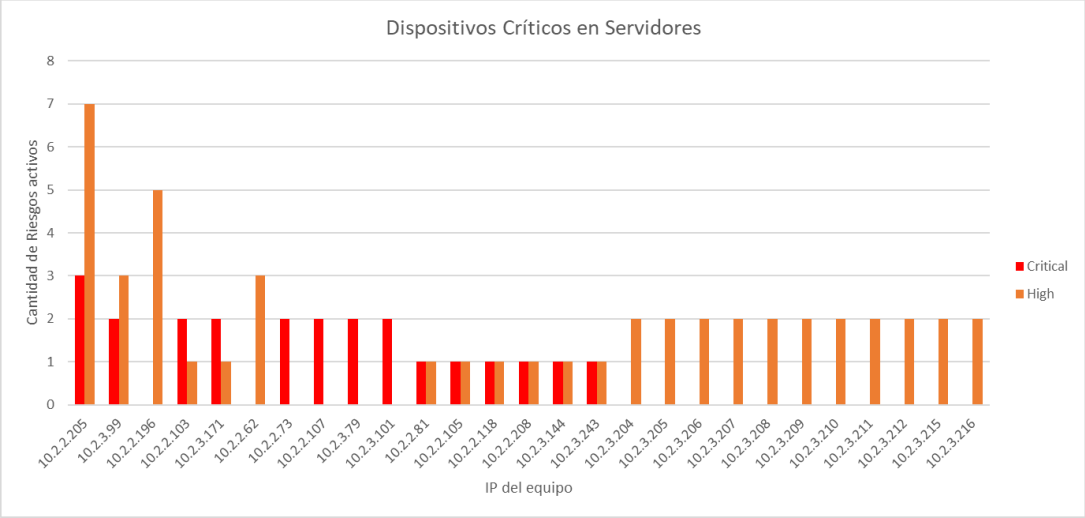


Figura 25. Dispositivos críticos en Servidores.

La Figura 25 muestra los equipos con más vulnerabilidades críticas y altas encontradas en la red de *Servidores*, y en realidad de toda la red, dentro de las cuales, las que más se presentan se observan a continuación.

Plugin ID Nessus	Descripción	Severidad	Cantidad
108797	Unsupported Windows OS (remote)	Crítica	8
125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	Crítica	7
102431	HP Data Protector 8.x < 8.17 / 9.x < 9.09 Multiple Vulnerabilities (HPSBGN03732)	Crítica	5
79638	MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	Crítica	2
20007	SSL Version 2 and 3 Protocol Detection	Alta	39
134976	iLO 3 < 1.90 / iLO 4 < 2.61 / iLO 5 < 1.35 Remote Code Execution Vulnerability (HPESBHF03866)	Alta	11
69552	Oracle TNS Listener Remote Poisoning	Alta	4
130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.	Alta	2

Tabla 20. Vulnerabilidades críticas y altas en Servidores.

Como se evidencia en la Tabla 20, son pocas las vulnerabilidades que causan la mayor parte de riesgo dentro de la red. De los 55 equipos con riesgos críticos y/o altos, el 15% presenta la posibilidad de sufrir un ataque por causa de tener una versión de sistema operativo fuera de soporte. El 13% es vulnerable al CVE-2019-0708, que es un riesgo referente al protocolo RDP en los equipos, pero que ya existen parches de seguridad que mitigan este riesgo. Por otro lado, y para mencionar las clasificadas con criticidad *Alta*, el 71% de las máquinas sufre el riesgo de ser afectado por el uso de protocolos de encriptación débil, y el 25% tiene riesgos con la versión de PHP instalada, la cual tiene asociada varias vulnerabilidades que se pueden ver en el Anexo 07.

Para la red 10.2.1.0/24 de *Administración*, el cual fue el enfoque del análisis realizado, se encontraron 69 dispositivos activos, de los cuales solo 3 tienen vulnerabilidades clasificadas como *Altas* (Ver Tabla 21). Además, se encontraron 107 riesgos diferentes que hacen referencia a versión obsoleta de aplicaciones y uso de protocolos de cifrado débil que se pueden ver en el Anexo 13, pero de los cuales solo 5 tienen severidad *Alta* y se pueden ver en la Tabla 22.

Dispositivos en ADMINISTRACIÓN con vulnerabilidades Críticas y/o Altas						
IP	**Critical**	**High**	**Medium**	**Low**	**Info**	**Total**
10.2.1.3	0	1	8	2	22	33
10.2.1.20	0	1	6	2	25	34
10.2.1.249	0	3	16	7	41	67

Tabla 21. Dispositivos en la red de Administración.

Plugin ID Nessus	**Descripción**	**Severidad**	**Cantidad**
20007	SSL Version 2 and 3 Protocol Detection	Alta	1
130208	Cisco Wireless LAN Controller Secure Shell (SSH) Denial of Service Vulnerability (cisco-sa-20191016-wlc-ssh-dos)	Alta	1
41028	SNMP Agent Default Community Name (public)	Alta	1
44078	OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass	Alta	1
44077	OpenSSH < 4.5 Multiple Vulnerabilities	Alta	1

Tabla 22. Vulnerabilidades altas en Administración.

Por otro lado, en el segmento de los *Servidores de la Telefonía IP* se encontraron 22 equipos activos pertenecientes a la red 10.2.60.0/24 de los cuales 15 de éstos tienen vulnerabilidades *Críticas y/o Altas* (Ver Tabla 23). Así mismo, se encontraron 100 riesgos diferentes dentro de estos equipos que se pueden ver en el Anexo 13.

Dispositivos en SERVIDORES TELEFONÍA con vulnerabilidades Críticas y/o Altas						
IP	**Critical**	**High**	**Medium**	**Low**	**Info**	**Total**
10.2.60.5	0	3	7	1	27	38
10.2.60.6	1	0	4	1	34	40
10.2.60.10	0	3	7	0	24	34
10.2.60.14	1	0	4	0	28	33
10.2.60.34	1	0	10	1	37	49
10.2.60.54	1	0	6	1	30	38
10.2.60.55	1	0	6	1	30	38
10.2.60.56	1	0	6	1	32	40
10.2.60.57	1	0	6	1	32	40
10.2.60.58	1	0	4	0	28	33
10.2.60.59	1	0	4	0	28	33
10.2.60.60	1	0	4	0	29	34
10.2.60.61	1	0	4	0	29	34
10.2.60.67	0	1	13	2	37	53
10.2.60.100	0	3	5	0	23	31

Tabla 23. Dispositivos en la red de Servidores para Telefonía.

Plugin ID Nessus	**Descripción**	**Severidad**	**Cantidad**
33850	Unix Operating System Unsupported Version Detection	Crítica	10
16321	3Com 3CServer/3CDaemon FTP Server Multiple Vulnerabilities (OF, FS, PD, DoS)	Crítica	1
118885	ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check)	Alta	3
123518	ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check)	Alta	3
118466	ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check)	Alta	3
20007	SSL Version 2 and 3 Protocol Detection	Alta	1

Tabla 24. Vulnerabilidades críticas y altas activas en Servidores de Telefonía.

Como se observa en la Tabla 24, el riesgo más común en esta red es la presencia de un sistema operativo no soportado por el fabricante y que además puede ser afectado por múltiples vulnerabilidades. Además del sistema operativo de los equipos, también se evidencia alta presencia de riesgos asociados a la versión de VMware utilizada o a la falta de parches de seguridad instalados.

Otro segmento escaneado fue el de *Impresoras*, perteneciente a la red 10.2.5.0/24, en la que se encontraron 44 dispositivos activos y solo uno de ellos con una vulnerabilidad clasificada como *Alta* (Ver Tabla 25). Los riesgos encontrados en esta red fueron 56 y se pueden ver en el Anexo 13.

Dispositivos IMPRESORAS con vulnerabilidades Críticas y/o Altas						
IP	**Critical**	**High**	**Medium**	**Low**	**Info**	**Total**
10.2.5.83	0	1	5	1	23	30

Tabla 25. Dispositivos en la red de Impresoras.

La única vulnerabilidad alta mostrada anteriormente es la identificada por Nessus con el ID 20007 y hace referencia al uso de versiones de protocolos de cifrado débiles.

Por último, en el segmento de los *Teléfonos*, perteneciente a la red 10.2.48.0/24, se encontraron 6 dispositivos activos y solo dos de éstos con vulnerabilidades *Altas* (Ver Tabla 26), que al igual que en la red de *Impresoras*, el riesgo presente es el uso de protocolos de cifrado débil. En el Anexo 13 se muestran los diferentes riesgos encontrados en estos dispositivos.

Dispositivos de TELÉFONOS con vulnerabilidades Críticas y/o Altas						
IP	**Critical**	**High**	**Medium**	**Low**	**Info**	**Total**
10.2.48.7	0	1	5	1	28	35
10.2.48.13	0	1	9	1	25	36

Tabla 26. Dispositivos en la red de Telefonía.

Para finalizar el análisis enfocado en cada segmento y resumir un poco lo descubierto en la entidad, es necesario mencionar que, en su mayoría, los riesgos detectados hacen referencia a: Falta de instalación de parches de seguridad, uso de versiones obsoletas en

protocolos de la capa de transporte, uso de versiones obsoletas en aplicaciones, configuraciones del equipo que no están ligadas a las buenas prácticas recomendadas por los fabricantes. Sin embargo, cabe destacar que la solución a los riegos se puede lograr con acciones fijas y concretas que son fáciles de llevar a cabo.

Por otro lado, para mostrar un resultado más estadístico y una visión más general del estado y las condiciones actuales de la red de la entidad, a continuación, se muestran datos obtenidos del escaneo y el análisis realizado.

Se descubrieron un total de 322 equipos con sistema operativo distribuido como se observa en la Figura 26.

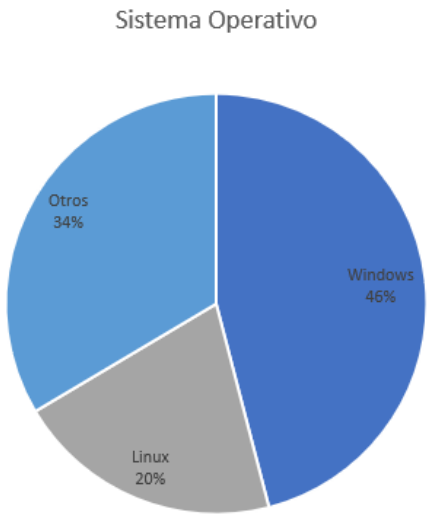


Figura 26. Distribución de Sistema Operativo.

Se descubrieron un total de 255 riesgos de seguridad diferentes distribuidos por su criticidad como se muestra en la Figura 27.

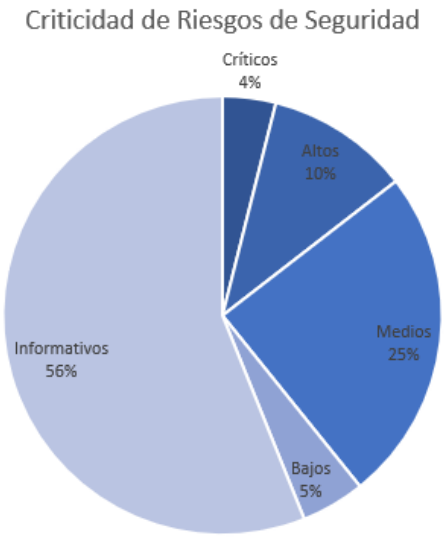


Figura 27. Distribución de criticidad de riesgos descubiertos.

Además, se evidenció que los riesgos críticos afectan a 29 equipos, los riesgos de criticidad alta afectan a 55 equipos, y los de criticidad media afectan a 225 equipos. Cabe mencionar que las cuentas realizadas anteriormente no son excluyentes y que es posible que haya un equipo que entre en los tres grupos.

Por otro lado, se encontraron 215 vulnerabilidades registradas en la NVD, las cuales se encuentran en 86 de los 255 riesgos de seguridad descubiertos, es decir, el 34% de los riesgos totales hallados como se ve en la Figura 28.

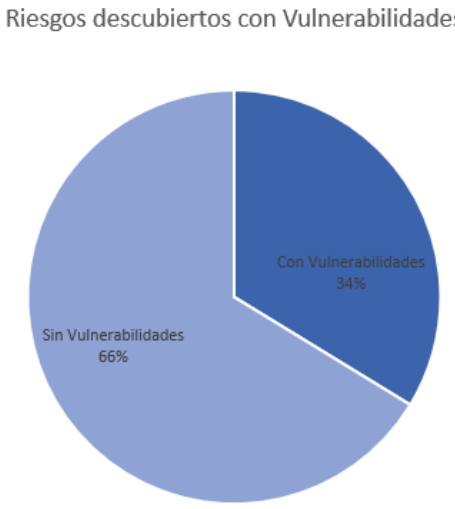


Figura 28. Distribución de vulnerabilidades presentes.

Por último, de las 215 vulnerabilidades mencionadas anteriormente, hay 17 que tienen un *exploit* disponible para ser explotada a través de *Metasploit*, *Core Impact* y/o *CANVAS*, lo que hace que incremente su riesgo de impacto. Estas 17 vulnerabilidades afectan al 25% de los equipos de la entidad, y se distribuyen según su criticidad como se muestra en la siguiente figura.

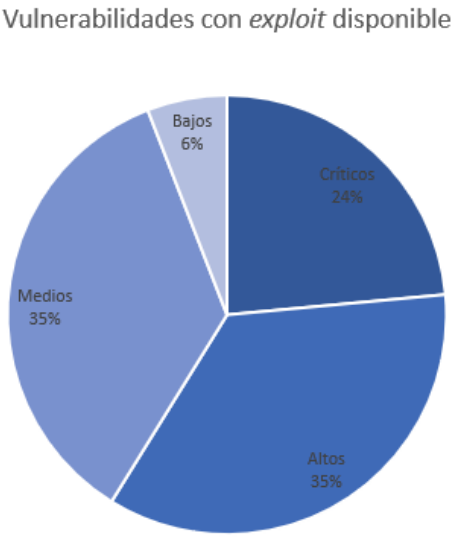


Figura 29. Distribución de vulnerabilidades con exploit disponible.

11.2 Fase 2: Resultados Control de Acceso a la Red

Con la implementación del demo de la herramienta Cisco ISE se logró mejorar el control de acceso a la red cableada, minimizar los riesgos de intrusión, delimitar fronteras de acceso a los recursos, además de brindar flexibilidad y administración centralizada. Lo anterior, se logró respecto a la situación inicial de la red de la entidad gracias al redireccionamiento de ingreso de usuarios internos y externos a través del protocolo IEEE 802.1X, apoyado por las políticas y listas de control de acceso configuradas.

Para los dispositivos que no manejan el protocolo 802.1X y/o no pertenecen a la entidad, se logró validar el acceso por medio de MAC Address Bypass (MAB), generando control sobre dispositivos tales como impresoras, Access Points, telefonía IP, proyectores, etc. Al igual que los dispositivos mencionados anteriormente, para los equipos de cómputo que no manejan el protocolo 802.1X, la autenticación se logró validar a partir del portal

de invitados con el que cuenta la herramienta, por medio del registro de las personas y la captura de los datos para su validación.

Para el acceso inalámbrico, se limitó el acceso por medio de un perfilamiento, garantizando así el acceso solo a los recursos permitidos. Lo anterior también por medio del portal facilitado por la herramienta para el registro de usuarios o la autenticación de usuarios previamente registrados.

FICHA TÉCNICA

ITEM	CARACTERISTICAS TECNICAS MINIMAS	CUMPLE SI/NO
	Todas las características solicitadas deben poderse aplicar en la red cableada, inalámbrica y/o VPN	
	Permitir configurar y administrar de manera centralizada en una consola tipo web los servicios de perfil, postura, invitado, autenticación y autorización.	
	Creación de políticas flexibles basadas en reglas y atributos para control de acceso.	
	Creación de atributos de identidad de usuario y punto final, validación de postura, protocolos de autenticación e identidad del dispositivo.	
	Permitir la creación de políticas de acceso por usuario o grupo de usuarios.	
	Permitir la integración mínima con los siguientes repositorios de usuarios: Microsoft Active Directory Lightweight Directory Access Protocol (LDAP) RADIUS RSA one-time password (OTP) Autoridades de certificación para autenticación y autorización – Open Database Connectivity (ODBC)	
	Permitir el uso de múltiples métodos de autenticación para los usuarios de la entidad.	
	Permitir mínimo el uso de RADIUS, 802.1X, MAC Authentication Bypass, MACSec.	
	Permitir el perfilamiento de hasta 1000 dispositivos de usuario final para la aplicación de políticas de acceso y seguridad dentro de la red.	
	Permitir perfilamientos de dispositivos con plantillas predefinidas y reutilizables para mínimo los siguientes tipos de dispositivos: Teléfonos IP, Impresoras, Cámaras IP, Teléfonos Inteligentes y Tabletas.	

ITEM	CARACTERISTICAS TECNICAS MINIMAS	CUMPLE SI/NO
	Aplicación de políticas de postura de hasta 800 dispositivos de usuario final con el fin de garantizar las condiciones mínimas de seguridad para el acceso a la red.	
	Permitir el uso de agentes para las actividades de postura, compatible con sistemas operativos Microsoft Windows 8 o superior y MAC OS X 10.8 o superior.	
	Debe poder reconocer el tipo de dispositivo que se conecta a la red y perfilarlo de acuerdo al directorio de perfiles de dispositivo almacenado en la plataforma.	
	Debe permitir la personalización de los perfiles existentes o creación de nuevos perfiles, para dispositivos especiales.	
	Dentro de las técnicas de detección de dispositivos, se deben poder utilizar protocolos como DNS, Netflow, SNMP, NMAP, HTTP, Radius, DHCP entre otros.	
	Debe poder identificar quién y desde que tipo de dispositivo se está conectando a la red.	
	Debe soportar el servicio de BYOD (Bring Your Own Device) simplificado, a través de la capacidad de registrar dispositivos personales de forma automática.	
	Debe tener la capacidad de construir políticas de control de acceso que puedan incluir la identidad del usuario, el método de acceso, la hora de la conexión, la ubicación geográfica, el tipo de dispositivo utilizado y el estado de postura del mismo.	
	Debe tener mínimo la capacidad de integrarse con soluciones MDM como Microsoft Intune y Microsoft SCCM.	
	La solución debe ser basada en RADIUS.	
	Debe tener la capacidad de funcionar de forma centralizada o descentralizada.	
	Debe permitir el aprovisionamiento, notificación y la generación de reportes de las cuentas de invitados.	
	Debe realizar análisis de postura de los dispositivos PC y MAC que se conecten a la red. El software encargado de dicho análisis debe presentarse en formato instalable para los empleados regulares y no instalable para usuarios ocasionales de la red.	
	El agente encargado de validar la postura de dispositivos PC y MAC, debe estar en capacidad de ser suplicante 802.1X, así como cliente de VPN.	
	El análisis de postura debe realizarse una vez las estaciones han levantado procesos de arranque y el usuario se ha autenticado en la estación de trabajo.	
	Debe estar en capacidad de aplicar controles con base en VLANs y adicionalmente, aplicar listas de control de acceso en capa cuatro, en cada puerto en el switch, o por usuario en la controladora inalámbrica. Esto de acuerdo a la capacidad que se tenga en la infraestructura de red desplegada.	

ITEM	CARACTERISTICAS TECNICAS MINIMAS	CUMPLE SI/NO
	Debe tener un modelo de políticas basado en atributos y en reglas de control de acceso flexibles y relevantes. Ofrecer la capacidad de crear políticas detalladas al extraer atributos de diccionarios predefinidos.	
	Debe tener mínimo las siguientes opciones de control de acceso: listas de control de acceso descargables (DACL), asignaciones de LAN virtual (VLAN), redirecciones de URL, ACL nombradas y grupos de seguridad (SG) con tecnología CISCO trustSec.	
	Implementación y personalización de acceso a la red de invitados.	
	Proporcionar una experiencia simplificada de acceso a la red invitados.	
	Registrar el acceso a través de la red para seguridad, cumplimiento y auditoria completa de invitados.	
	Proporcionar la provisión automática de suplicantes y la inscripción de certificados para PC estándar y plataformas de computación móvil.	
	Debe integrar la autenticación, autorización y registro (AAA), perfiles, postura, y servicios de los clientes.	
	Debe soportar los siguientes protocolos de autenticación: PAP MS-CHAP Extensible Authentication Protocol (EAP)-MD5 Protected EAP(PEAP) EAP-Flexible Authentication vía Secure Tunneling (EAP-FAST) EAP – Transport Layer Security (EAP-TLS)	
	Debe admitir el protocolo TACACS+.	
	Ofrecer una autoridad de certificación interna.	
	Proporcionar una consola única para administrar puntos finales y certificados, la revocación del certificado debe ser automática.	
	Facilitar la creación manual de certificados a granel o individuales y pares de claves para conectar dispositivos a la red con un alto grado de seguridad.	
	Ofrecer la posibilidad de crear políticas potentes que incluyan verificaciones de los últimos parches del SO, paquetes de antivirus y antispyware con variables de archivos de definición actuales (versión, fecha, etc.), administración de parches, cifrado de disco, bloqueo de PIN móvil o estado rooteado, presencia de medios conectados a USB.	
	Proporcionar inventario de hardware para una vista completa de la red	
	Debe proveer una herramienta de fácil administración que permita la personalización de los portales cautivos para el acceso de invitados.	
	Debe permitir presentar un portal cautivo que se ajuste al tipo de dispositivo que utilice el invitado.	
	Debe estar en capacidad de integrarse con soluciones de mensajería para enviar token de autenticación vía SMS.	
	Debe tener la capacidad de enviar mensajes de aviso al invitado cuando su cuenta este próxima a expirar.	

ITEM	CARACTERISTICAS TECNICAS MINIMAS	CUMPLE SI/NO
	Debe permitir la aprobación o negación de acceso por un administrador a cuentas auto – registradas o de auto – servicio.	
	Debe estar en capacidad de crear cuentas de invitado de forma masiva, cargando un archivo .CSV con la información de los usuarios a registrar.	
	Debe permitir gestionar la validez de las cuentas de invitados en tiempo real, con el fin de extender, modificar o terminar la vigencia de las mismas.	
	Debe permitir limpiar el número de dispositivos asociados a un mismo invitado.	
	Debe permitir la gestión de invitados a través de una REST API.	
	Debe estar en capacidad de hacer una doble validación de autenticación antes de permitir el acceso de un equipo a la red (EAP – Chaining) de forma que solo se permita el acceso cuando se verifique la identidad del usuario y que el equipo sea de la compañía.	
	Integración con fabricante de SIEM y análisis de tráfico como ArcSight, Logrythm, Splunk, entre otros con el fin de compartir información de telemetría.	
	Debe tener la capacidad de gestionar políticas de cifrado de datos en L2(Macsec).	
	Debe estar en capacidad de brindar control de acceso con base en las amenazas y vulnerabilidades detectadas en los dispositivos, dicha información poder ser obtenida a partir de la integración con soluciones como CISCO AMP, CTRA, QUALYS, RAPID7 NEXPOSE O TENABLE SECURITY CENTER.	
	Contar con mínimo 2000 licencias para servicios de autenticación y control de acceso.	
	Contar con mínimo 2000 licencias para servicio de perfilamiento.	
	Contar con mínimo 320 licencias para servicio de evaluación de postura.	
	Debe estar en capacidad de integrarse con soluciones de NGFW así como soluciones de detección de amenazas por medio de análisis y telemetría del tráfico de red, soluciones de filtrado web, y soluciones de escaneo de vulnerabilidades con el fin de tomar decisiones inteligentes de políticas de seguridad.	
	Debe estar en capacidad de cambiar el acceso del usuario con base en puntajes de amenaza tales como el Common Vulnerability Scoring System (CVSS) y Structured Threat Information Expression (STIX).	
	Debe ser totalmente compatible con la infraestructura de red implementada.	
	Debe integrarse con el CISCO PRIME instalado.	
	Debe quedar funcional y operable en la infraestructura de red.	
	Debe quedar desplegada con políticas, controles, auditorias, y aplicando todos los beneficios de esta herramienta según las necesidades.	

Tabla 27. Ficha Técnica.

12. Discusión

Luego de analizar y determinar el cumplimiento de los objetivos, se establece que se llega a los resultados esperados debido a que la información obtenida a partir del desarrollo del proyecto fue la comprometida con la entidad para poder tomar la decisión de una implementación a mayor escala y más robusta. Desde el principio se planteó el problema que hay cuando existe comunicación bidireccional sin restricción entre equipos de personas externas y equipos de funcionarios, por lo que limitar el acceso de acuerdo a políticas de seguridad como se evidenció en la ejecución del proyecto ayuda a proteger lo que es la red interna de la entidad.

Cabe mencionar que el análisis de vulnerabilidad realizado aplica solamente sobre la infraestructura actual de la red, por lo que cualquier otro despliegue requerirá de un nuevo análisis. Sin embargo, del análisis realizado se pueden sacar tareas para hacer de forma periódica y que sin lugar a dudas mantendría a la red más segura. De igual forma, se llevó a cabo bajo un procedimiento estándar que se identificó en la investigación de este proyecto, y que la entidad puede tomar como base para futuros análisis.

En cuanto al control de acceso a la red, con la ficha técnica elaborada se pretende brindar una línea base para una posterior revisión y toma de decisiones por parte de la entidad. Sin embargo, de acuerdo a las investigaciones realizadas y las consultas hechas a investigaciones de otros autores, las características técnicas propuestas son las mínimas requeridas de acuerdo al apartado *10.2.1 Elección Solución NAC* de este texto, las cuales son fundamentales para la razón de ser un control de acceso a la red.

En la entidad quedó implementado el control de acceso para la red alámbrica e inalámbrica y las políticas mínimas consideradas para proteger la red de las brechas de seguridad encontradas. Con esto a la entidad le queda realizar la contratación para la adquisición del respectivo licenciamiento y la configuración en las sedes donde considere necesario limitar el acceso; cabe anotar que las configuraciones a realizar son las que se indicaron en el apartado *10.2.3 IMPLEMENTACIÓN DEMO* disminuyendo la inversión en gastos de implementación.

13. Conclusiones

En primera medida, con el análisis de vulnerabilidad realizado se pudo evidenciar que la mayor debilidad de la entidad es el uso de tecnología obsoleta en diferentes frentes, desde sistema operativo de equipos hasta protocolos de cifrado débil. También se encontraron aplicaciones cuyas versiones son afectadas por múltiples vulnerabilidades que se pueden explotar de manera relativamente sencilla. Por lo anterior, se sugiere a la entidad, o al personal indicado de seguridad, elaborar un completo inventario de software instalado a lo largo de toda la infraestructura, y actualizarlo periódicamente, para validar las fechas de vencimiento de soporte que ofrecen los fabricantes y/o desarrolladores de las aplicaciones.

Se pudo evidenciar que los riesgos encontrados hay algunos que podrían explotarse por actividades de los usuarios internos sin tener este conocimiento de ello; por ejemplo, falta de administración en el control de las sesiones SSH de las cuales existen muchos riesgos, y que en realidad podría impactar los servicios sin necesidad de ser un ataque mal intencionado.

La plantilla de aseguramiento elaborada para este proyecto busca brindar a la entidad una línea base de seguridad para los equipos de red. De acuerdo al análisis, fue posible registrar en la plantilla las configuraciones básicas que recomienda el fabricante y que mitigarían en gran medida los riesgos encontrados en estos equipos, así como mejorar la brecha de seguridad y contener la explotación de vulnerabilidades.

Con el demo implementado de la solución NAC elegida, se generan mecanismos de control donde se puede identificar quién, cuándo, dónde y cómo se conectan a la red, limitando las fronteras de acceso a los recursos de la red cableada y/o inalámbrica. Todo el trabajo realizado con la implementación sirvió como insumo fundamental para la construcción de la ficha técnica para la adquisición de una plataforma que cubra las necesidades de la entidad.

14. Documentos de Referencia

- Dictamen final sobre Auditoria de Seguridad Información; Jesús González, Juan Arturo Nolazco, Tecnológico de Monterrey – mayo 2017.
- Análisis de vulnerabilidad de la Red LAN de la UTPL; Angélica del Cisne Espinosa Otavalo, Universidad Técnica Particular de Loja – 2010.
- Análisis de vulnerabilidad de una red corporativa mediante herramientas de descubrimiento activas; Jairo Manuel Palacios Domínguez, Escuela Técnica Superior de Ingeniería Universidad de Sevilla – 2015.
- Cisco Identity Services Engine Administrator Guide, Release 2.6; Cisco Systems, Inc –2019.
- Cisco Wireless LAN Controller (WLC) Configuration Best Practices; Cisco Systems, Inc –2018.

15. Anexos

- ANEXO 1: Escaneo Nmap a segmento de Administración.
- ANEXO 2: Escaneo Nessus a segmento de Servidores.
- ANEXO 3: Escaneo Nessus a segmento de Administración.
- ANEXO 4: Escaneo Nessus a segmento de Servidores de Telefonía.
- ANEXO 5: Escaneo Nessus a segmento de Impresoras.
- ANEXO 6: Escaneo Nessus a segmento de Teléfonos IP.
- ANEXO 7: Lista de riesgos del segmento de Servidores.
- ANEXO 8: Lista de riesgos del segmento de Administración.
- ANEXO 9: Lista de riesgos del segmento de Servidores de Telefonía.
- ANEXO 10: Lista de riesgos del segmento de Impresoras.
- ANEXO 11: Lista de riesgos del segmento de Teléfonos IP.
- ANEXO 12: Plantilla de aseguramiento S.O. Cisco.
- ANEXO 13: Descripción de todos los riesgos encontrados.
- ANEXO 14: Matriz de riesgos de vulnerabilidades.
- ANEXO 15: Informe gerencial.

ANEXO 01

NOTA: Todas las direcciones IP fueron modificadas para conservar la confidencialidad y reserva de la entidad.

Estado	Nombre	IP	Fabricante	Dirección MAC	Usuario	Comentarios
Activado	10.2.1.2	10.2.1.2		00:00:00:00:00:00		
	HTTP: Cisco IOS http config HTTPS: Tunnel is ssl: Cisco IOS http config Radmin:					
Activado	10.2.1.3	10.2.1.3		00:00:00:00:00:00		
	HTTP: Cisco IOS http config HTTPS: Tunnel is Cisco IOS ssl: unknown service Radmin:					
Activado	10.2.1.4	10.2.1.4		00:00:00:00:00:00		
	Radmin:					
Activado	10.2.1.5	10.2.1.5		00:00:00:00:00:00		
	Radmin:					
Activado	10.2.1.6	10.2.1.6		00:00:00:00:00:00		
	HTTP: Cisco IOS http config HTTPS: Tunnel is ssl: Cisco IOS http config Radmin:					
Activado	Server.Entidad.col	10.2.1.8		00:00:00:00:00:00		
	RDP: Tunnel is Microsoft SChannel TLS: unknown service Radmin:					
Activado	10.2.1.11	10.2.1.11		00:00:00:00:00:00		
	HTTP: Cisco IOS http config HTTPS: Tunnel is ssl: Cisco IOS http config Radmin:					
Activado	10.2.1.12	10.2.1.12		00:00:00:00:00:00		
	Radmin:					
Activado	10.2.1.13	10.2.1.13		00:00:00:00:00:00		
	Radmin:					
Activado	10.2.1.20	10.2.1.20		00:00:00:00:00:00		
	HTTPS: Tunnel is ssl: unknown service Radmin:					
Activado	10.2.1.21	10.2.1.21		00:00:00:00:00:00		
	HTTP: Cisco IOS http config					

	HTTPS: Tunnel is ssl: Cisco IOS http config Radmin:		
Activado	10.2.1.22	10.2.1.22	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.23	10.2.1.23	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.24	10.2.1.24	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.25	10.2.1.25	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.31	10.2.1.31	00:00:00:00:00:00
	HTTP: Cisco IOS http config HTTPS: Tunnel is TLSv1: Cisco IOS http config Radmin:		
Activado	10.2.1.32	10.2.1.32	00:00:00:00:00:00
	HTTP: Cisco IOS http config HTTPS: Tunnel is TLSv1: Cisco IOS http config Radmin:		
Activado	10.2.1.33	10.2.1.33	00:00:00:00:00:00
	HTTP: Cisco IOS http config HTTPS: Tunnel is TLSv1: Cisco IOS http config Radmin:		
Activado	10.2.1.34	10.2.1.34	00:00:00:00:00:00
	HTTP: Cisco IOS http config HTTPS: Tunnel is TLSv1: Cisco IOS http config Radmin:		
Activado	10.2.1.35	10.2.1.35	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.36	10.2.1.36	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.37	10.2.1.37	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.38	10.2.1.38	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.41	10.2.1.41	00:00:00:00:00:00
	HTTP: Cisco IOS http config HTTPS: ? Radmin:		
Activado	10.2.1.42	10.2.1.42	00:00:00:00:00:00

Radmin:
Activado 10.2.1.43 10.2.1.43 00:00:00:00:00:00
Radmin:
Activado 10.2.1.44 10.2.1.44 00:00:00:00:00:00
Radmin:
Activado 10.2.1.45 10.2.1.45 00:00:00:00:00:00
Radmin:
Activado 10.2.1.51 10.2.1.51 00:00:00:00:00:00
HTTP:
Cisco IOS http config
HTTPS:
Tunnel is TLSv1: Cisco IOS http config
Radmin:
Activado 10.2.1.53 10.2.1.53 00:00:00:00:00:00
Radmin:
Activado 10.2.1.54 10.2.1.54 00:00:00:00:00:00
Radmin:
Activado 10.2.1.55 10.2.1.55 00:00:00:00:00:00
Radmin:
Activado 10.2.1.61 10.2.1.61 00:00:00:00:00:00
Radmin:
Activado 10.2.1.62 10.2.1.62 00:00:00:00:00:00
Radmin:
Activado 10.2.1.63 10.2.1.63 00:00:00:00:00:00
Radmin:
Activado 10.2.1.64 10.2.1.64 00:00:00:00:00:00
Radmin:
Activado 10.2.1.65 10.2.1.65 00:00:00:00:00:00
Radmin:
Activado 10.2.1.69 10.2.1.69 00:00:00:00:00:00
HTTP:
Cisco IOS http config
HTTPS:
?
Radmin:
Activado 10.2.1.71 10.2.1.71 00:00:00:00:00:00
HTTP:
Cisco IOS http config
HTTPS:
Tunnel is ssl: Cisco IOS http config
Radmin:
Activado 10.2.1.72 10.2.1.72 00:00:00:00:00:00
Radmin:
Activado 10.2.1.73 10.2.1.73 00:00:00:00:00:00
Radmin:
Activado 10.2.1.74 10.2.1.74 00:00:00:00:00:00
Radmin:
Activado 10.2.1.75 10.2.1.75 00:00:00:00:00:00
Radmin:

Activado	10.2.1.81	10.2.1.81	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.82	10.2.1.82	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.83	10.2.1.83	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.84	10.2.1.84	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.85	10.2.1.85	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.91	10.2.1.91	00:00:00:00:00:00
	HTTP: Cisco IOS http config HTTPS: Tunnel is TLSv1: Cisco IOS http config Radmin:		
Activado	10.2.1.92	10.2.1.92	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.93	10.2.1.93	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.94	10.2.1.94	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.95	10.2.1.95	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.100	10.2.1.100	00:00:00:00:00:00
	HTTPS: Tunnel is ssl: unknown service Radmin:		
Activado	10.2.1.101	10.2.1.101	00:00:00:00:00:00
	HTTP: Cisco IOS http config HTTPS: ? Radmin:		
Activado	10.2.1.102	10.2.1.102	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.103	10.2.1.103	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.104	10.2.1.104	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.105	10.2.1.105	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.111	10.2.1.111	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.112	10.2.1.112	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.113	10.2.1.113	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.114	10.2.1.114	00:00:00:00:00:00

	Radmin:		
Activado	10.2.1.115	10.2.1.115	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.121	10.2.1.121	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.122	10.2.1.122	00:00:00:00:00:00
	Radmin:		
Activado	10.2.1.123	10.2.1.123	00:00:00:00:00:00
	Radmin:		
Activado	DPS-Exinda	10.2.1.249	00:00:00:00:00:00
	HTTPS: Tunnel is ssl: Apache httpd Radmin:		
Activado	10.2.1.250	10.2.1.250	00:00:00:00:00:00
	HTTP: Cisco IOS http config HTTPS: ? Radmin:		

ANEXO 02

NOTA: Todas las direcciones IP fueron modificadas para conservar la confidencialidad y reserva de la entidad.

Tenable.io Report

Thu, 23 Apr 2020 00:55:43 UTC

Table Of Contents

10.2.2.54

10.2.2.58

10.2.2.59

10.2.2.61

10.2.2.62

10.2.2.63

10.2.2.64

10.2.2.65

10.2.2.66

10.2.2.67

10.2.2.73

10.2.2.77

10.2.2.79

10.2.2.81

10.2.2.85

10.2.2.89

10.2.2.91

10.2.2.96

10.2.2.97

10.2.2.98

10.2.2.99

10.2.2.103

10.2.2.105

10.2.2.106

10.2.2.107

10.2.2.110

10.2.2.112

10.2.2.113

10.2.2.114

10.2.2.115

10.2.2.118

10.2.2.119

10.2.2.129

10.2.2.131

10.2.2.132

10.2.2.135

10.2.2.141

10.2.2.142

10.2.2.149

10.2.2.150

10.2.2.157

10.2.2.171

10.2.2.182

10.2.2.188

10.2.2.190

10.2.2.193

10.2.2.194

10.2.2.196

10.2.2.197

10.2.2.198

10.2.2.200

10.2.2.203

10.2.2.205

10.2.2.208

10.2.2.212

10.2.2.218

10.2.2.225

10.2.2.227

10.2.2.228

10.2.2.229

10.2.2.231

10.2.3.1

10.2.3.3

10.2.3.5

10.2.3.7

10.2.3.8

10.2.3.9

10.2.3.11

10.2.3.12

10.2.3.16

10.2.3.19

10.2.3.22

10.2.3.23

10.2.3.25

10.2.3.26

10.2.3.30

10.2.3.36

10.2.3.38

10.2.3.49

10.2.3.50

10.2.3.51

10.2.3.64

10.2.3.79

10.2.3.80

10.2.3.81

10.2.3.83

10.2.3.91

10.2.3.92

10.2.3.99

10.2.3.100

10.2.3.101

10.2.3.103

10.2.3.105

10.2.3.107

10.2.3.108

10.2.3.112

10.2.3.114

10.2.3.115

10.2.3.117

10.2.3.119

10.2.3.120

10.2.3.121

10.2.3.122

10.2.3.125

10.2.3.129

10.2.3.131

10.2.3.132

10.2.3.142

10.2.3.143

10.2.3.144

10.2.3.145

10.2.3.146

10.2.3.147

10.2.3.149

10.2.3.150

10.2.3.171

10.2.3.173

10.2.3.174

10.2.3.178

10.2.3.182

10.2.3.184

10.2.3.185

10.2.3.186

10.2.3.190

10.2.3.192

10.2.3.193

10.2.3.194

10.2.3.195

10.2.3.198

10.2.3.199

10.2.3.200

10.2.3.201

10.2.3.202

10.2.3.203

10.2.3.204

Remediations

Vulnerabilities By Host

[-] Collapse All

[+] Expand All

10.2.2.2

Scan Information

Start time: 2020/04/22 19:42

End time: 2020/04/23 00:29

Host Information

DNS Name: Server.Entidad.col

Netbios Name: TITAN

OS: [0: Windows Server 2016 Standard 14393]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	1	37	46

Results Details

/

10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
24786 - Nessus Windows Scan Not Performed with Admin Privileges	[-/+]
11219 - Nessus SYN scanner	[-/+]
11002 - DNS Server Detection	[-/+]
26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	[-/+]
10736 - DCE Services Enumeration	[-/+]
10863 - SSL Certificate Information	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
35297 - SSL Service Requests Client Certificate	[-/+]
110723 - No Credentials Provided	[-/+]

25701 - LDAP Crafted Search Request Server Information Disclosure	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
22964 - Service Detection	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
20870 - LDAP Server Detection	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
19506 - Nessus Scan Information	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
10884 - Network Time Protocol (NTP) Server Detection	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
10394 - Microsoft Windows SMB Log In Possible	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
35372 - DNS Server Dynamic Update Record Injection	[-/+]
43829 - Kerberos Information Disclosure	[-/+]
135860 - WMI Not Available	[-/+]
10287 - Traceroute Information	[-/+]
11936 - OS Identification	[-/+]

57582 - SSL Self-Signed Certificate [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

57608 - SMB Signing not required [-/+]

54615 - Device Type [-/+]

10.2.2.6

Scan Information

Start time: 2020/04/22 19:42

End time: 2020/04/23 06:15

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	2	0	23	25

Results Details

/

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

42823 - Non-compliant Strict Transport Security (STS) [-/+]

21643 - SSL Cipher Suites Supported [-/+]

42336 - AlienVault OSSIM Web Front End Detection [-/+]

11219 - Nessus SYN scanner [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

50350 - OS Identification Failed [-/+]

22964 - Service Detection [-/+]

10107 - HTTP Server Type and Version [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

19506 - Nessus Scan Information [-/+]

117530 - Errors in nessusd.dump [-/+]

10287 - Traceroute Information [-/+]

10267 - SSH Server Type and Version Information [-/+]

48204 - Apache HTTP Server Version [-/+]

42822 - Strict Transport Security (STS) Detection [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

57582 - SSL Self-Signed Certificate [-/+]

10881 - SSH Protocol Versions Supported [-/+]

10386 - Web Server No 404 Error Code Check [-/+]

106658 - JQuery Detection [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

10863 - SSL Certificate Information [-/+]

56984 - SSL / TLS Versions Supported [-/+]

10.2.2.7

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 21:04

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	DRACO
OS:	[0: Microsoft Windows 10]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	0	30	38

Results Details

/

10736 - DCE Services Enumeration [-/+]

22964 - Service Detection [-/+]

46180 - Additional DNS Hostnames [-/+]

45590 - Common Platform Enumeration (CPE)	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
10107 - HTTP Server Type and Version	[-/+]
11219 - Nessus SYN scanner	[-/+]
11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
54615 - Device Type	[-/+]
19506 - Nessus Scan Information	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10863 - SSL Certificate Information	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
135860 - WMI Not Available	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
110723 - No Credentials Provided	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

57608 - SMB Signing not required [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

56984 - SSL / TLS Versions Supported [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

11936 - OS Identification [-/+]

10287 - Traceroute Information [-/+]

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) [-/+]

64814 - Terminal Services Use SSL/TLS [-/+]

10.2.2.8

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 21:29

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	CRONOS
OS:	[0: Microsoft Windows 8][1: Microsoft Windows 7][2: Microsoft Windows Server 2008 R2][3: Microsoft Windows Server 2003][4: M...

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	6	0	29	35

Results Details

/

11219 - Nessus SYN scanner [-/+]

10736 - DCE Services Enumeration [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

22964 - Service Detection [-/+]

45590 - Common Platform Enumeration (CPE)	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
10107 - HTTP Server Type and Version	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
110723 - No Credentials Provided	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10863 - SSL Certificate Information	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
19506 - Nessus Scan Information	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
117530 - Errors in nessusd.dump	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
11936 - OS Identification	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
135860 - WMI Not Available	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
54615 - Device Type	[-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

10287 - Traceroute Information [-/+]

56984 - SSL / TLS Versions Supported [-/+]

57608 - SMB Signing not required [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

46180 - Additional DNS Hostnames [-/+]

10.2.2.11

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 04:35

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	SVFILES01
OS:	[0: Microsoft Windows Server 2012 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	13	1	38	53

Results Details

/

10736 - DCE Services Enumeration [-/+]

21643 - SSL Cipher Suites Supported [-/+]

57608 - SMB Signing not required [-/+]

18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness [-/+]

19506 - Nessus Scan Information [-/+]

10863 - SSL Certificate Information [-/+]

57690 - Terminal Services Encryption Level is Medium or Low [-/+]

45411 - SSL Certificate with Wrong Hostname [-/+]

46180 - Additional DNS Hostnames [-/+]

10940 - Windows Terminal Services Enabled	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
22964 - Service Detection	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
110723 - No Credentials Provided	[-/+]
54615 - Device Type	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
50845 - OpenSSL Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote	[-/+]

check)

64814 - Terminal Services Use SSL/TLS	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
11936 - OS Identification	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
10107 - HTTP Server Type and Version	[-/+]
48204 - Apache HTTP Server Version	[-/+]
135860 - WMI Not Available	[-/+]
66173 - RDP Screenshot	[-/+]
10287 - Traceroute Information	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
10394 - Microsoft Windows SMB Log In Possible	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
51891 - SSL Session Resume Supported	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]

10.2.2.12

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 20:33

Host Information

OS:	[0: Linux Kernel 2.6]

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	6	0	27	34

Results Details

/

94761 - SSL Root Certification Authority Certificate Information [-/+]

11936 - OS Identification [-/+]

19689 - Embedded Web Server Detection [-/+]

135187 - Dell iDRAC Buffer Overflow Vulnerability (CVE-2020-5344) [-/+]

10881 - SSH Protocol Versions Supported [-/+]

21643 - SSL Cipher Suites Supported [-/+]

10107 - HTTP Server Type and Version [-/+]

51185 - Dell Integrated Remote Access Controller (iDRAC) Detection [-/+]

54615 - Device Type [-/+]

56984 - SSL / TLS Versions Supported [-/+]

10863 - SSL Certificate Information [-/+]

22964 - Service Detection [-/+]

10267 - SSH Server Type and Version Information [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

57582 - SSL Self-Signed Certificate [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

10287 - Traceroute Information [-/+]

131730 - Dell iDRAC Improper Authorization (DSA-2019-137) [-/+]

135290 - Apache 2.4.x < 2.4.42 Multiple Vulnerabilities [-/+]

19506 - Nessus Scan Information [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

11219 - Nessus SYN scanner [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

117530 - Errors in nessusd.dump [-/+]

110723 - No Credentials Provided [-/+]

66334 - Patch Report [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

119833 - Dell iDRAC Products Multiple Vulnerabilities (December 2018) [-/+]

48204 - Apache HTTP Server Version [-/+]

84821 - TLS ALPN Supported Protocol Enumeration [-/+]

10.2.2.14

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 03:51

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	VMFOCALIZACION
OS:	[0: Windows]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	6	0	23	29

Results Details

/

10736 - DCE Services Enumeration [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

42410 - Microsoft Windows NTLMSSP Authentication Request [-/+]

Remote Network Name Disclosure	
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
110723 - No Credentials Provided	[-/+]
11936 - OS Identification	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
11219 - Nessus SYN scanner	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
135860 - WMI Not Available	[-/+]
19506 - Nessus Scan Information	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
10287 - Traceroute Information	[-/+]
10863 - SSL Certificate Information	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
54615 - Device Type	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
57608 - SMB Signing not required	[-/+]

57582 - SSL Self-Signed Certificate [-/+]

10940 - Windows Terminal Services Enabled [-/+]

10.2.2.15

Scan Information

Start time: 2020/04/22 19:42

End time: 2020/04/22 22:16

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	3	1	24	28

Results Details

/

10287 - Traceroute Information [-/+]

11219 - Nessus SYN scanner [-/+]

39520 - Backported Security Patch Detection (SSH) [-/+]

22964 - Service Detection [-/+]

84821 - TLS ALPN Supported Protocol Enumeration [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

21643 - SSL Cipher Suites Supported [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

10881 - SSH Protocol Versions Supported [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

19506 - Nessus Scan Information [-/+]

59861 - Remote web server screenshot [-/+]

56984 - SSL / TLS Versions Supported [-/+]

10863 - SSL Certificate Information [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

50845 - OpenSSL Detection [-/+]

87242 - TLS NPN Supported Protocol Enumeration [-/+]

35297 - SSL Service Requests Client Certificate [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

10267 - SSH Server Type and Version Information [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

50350 - OS Identification Failed [-/+]

62564 - TLS Next Protocols Supported [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

10.2.2.16

Scan Information

Start time: 2020/04/22 19:42

End time: 2020/04/22 20:33

Host Information

DNS Name: campusvirtualth.EntidadSocial.gov.co

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	3	1	26	30

Results Details

/

57323 - OpenSSL Version Detection [-/+]

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) [-/+]

11219 - Nessus SYN scanner [-/+]

48204 - Apache HTTP Server Version [-/+]

84574 - Backported Security Patch Detection (PHP) [-/+]

59861 - Remote web server screenshot [-/+]

11213 - HTTP TRACE / TRACK Methods Allowed	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
48243 - PHP Version Detection	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
50350 - OS Identification Failed	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
84821 - TLS ALPN Supported Protocol Enumeration	[-/+]
10863 - SSL Certificate Information	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
39521 - Backported Security Patch Detection (WWW)	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
22964 - Service Detection	[-/+]
50845 - OpenSSL Detection	[-/+]
10107 - HTTP Server Type and Version	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
19506 - Nessus Scan Information	[-/+]
10287 - Traceroute Information	[-/+]

10.2.2.17

Scan Information

Start time: 2020/04/22 19:42

End time: 2020/04/23 00:55

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	5	0	25	30

Results Details

/

10287 - Traceroute Information	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
11219 - Nessus SYN scanner	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
48204 - Apache HTTP Server Version	[-/+]
10107 - HTTP Server Type and Version	[-/+]
59861 - Remote web server screenshot	[-/+]
10386 - Web Server No 404 Error Code Check	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
19506 - Nessus Scan Information	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
117530 - Errors in nessusd.dump	[-/+]
50350 - OS Identification Failed	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
42823 - Non-compliant Strict Transport Security (STS)	[-/+]
84821 - TLS ALPN Supported Protocol Enumeration	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]

57582 - SSL Self-Signed Certificate [-/+]

10267 - SSH Server Type and Version Information [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

22964 - Service Detection [-/+]

10881 - SSH Protocol Versions Supported [-/+]

42822 - Strict Transport Security (STS) Detection [-/+]

50845 - OpenSSL Detection [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

56984 - SSL / TLS Versions Supported [-/+]

10863 - SSL Certificate Information [-/+]

10.2.2.18

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 21:04

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	KORE
OS:	[0: Microsoft Windows 10]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	6	0	30	36

Results Details

/

10736 - DCE Services Enumeration [-/+]

11219 - Nessus SYN scanner [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

21643 - SSL Cipher Suites Supported [-/+]

59861 - Remote web server screenshot [-/+]

57608 - SMB Signing not required	[-/+]
10863 - SSL Certificate Information	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
135860 - WMI Not Available	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
54615 - Device Type	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
10287 - Traceroute Information	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
46180 - Additional DNS Hostnames	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
110723 - No Credentials Provided	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
11936 - OS Identification	[-/+]
10107 - HTTP Server Type and Version	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
22964 - Service Detection	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) [-/+]

19506 - Nessus Scan Information [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

64814 - Terminal Services Use SSL/TLS [-/+]

10.2.2.22

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 00:55

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	METIS
OS:	[0: Microsoft Windows 10]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	0	34	41

Results Details

/

51192 - SSL Certificate Cannot Be Trusted [-/+]

10736 - DCE Services Enumeration [-/+]

64814 - Terminal Services Use SSL/TLS [-/+]

19506 - Nessus Scan Information [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

59861 - Remote web server screenshot [-/+]

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

51891 - SSL Session Resume Supported [-/+]

10107 - HTTP Server Type and Version	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
11219 - Nessus SYN scanner	[-/+]
135860 - WMI Not Available	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
57608 - SMB Signing not required	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
10287 - Traceroute Information	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
11936 - OS Identification	[-/+]
22964 - Service Detection	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
10863 - SSL Certificate Information	[-/+]
54615 - Device Type	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]

57582 - SSL Self-Signed Certificate [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

110723 - No Credentials Provided [-/+]

46180 - Additional DNS Hostnames [-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

10.2.2.23

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 21:52

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	MORFEO
OS:	[0: Microsoft Windows 10]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	0	35	43

Results Details

/

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) [-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure [-/+]

10736 - DCE Services Enumeration [-/+]

57582 - SSL Self-Signed Certificate [-/+]

10107 - HTTP Server Type and Version [-/+]

10863 - SSL Certificate Information [-/+]

48243 - PHP Version Detection [-/+]

11011 - Microsoft Windows SMB Service Detection	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10287 - Traceroute Information	[-/+]
135860 - WMI Not Available	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
11219 - Nessus SYN scanner	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
59861 - Remote web server screenshot	[-/+]
19506 - Nessus Scan Information	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
110723 - No Credentials Provided	[-/+]
51891 - SSL Session Resume Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]

117886 - Local Checks Not Enabled (info) [-/+]

22964 - Service Detection [-/+]

10940 - Windows Terminal Services Enabled [-/+]

54615 - Device Type [-/+]

57608 - SMB Signing not required [-/+]

46180 - Additional DNS Hostnames [-/+]

11936 - OS Identification [-/+]

56984 - SSL / TLS Versions Supported [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) [-/+]

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only [-/+]

10.2.2.24

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 06:15

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	6	1	24	31

Results Details

/

11219 - Nessus SYN scanner [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

56984 - SSL / TLS Versions Supported [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

84502 - HSTS Missing From HTTPS Server [-/+]

22964 - Service Detection [-/+]

21643 - SSL Cipher Suites Supported [-/+]

10881 - SSH Protocol Versions Supported [-/+]

10267 - SSH Server Type and Version Information [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

51891 - SSL Session Resume Supported [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10107 - HTTP Server Type and Version [-/+]

10092 - FTP Server Detection [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

90317 - SSH Weak Algorithms Supported [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

10287 - Traceroute Information [-/+]

39520 - Backported Security Patch Detection (SSH) [-/+]

15901 - SSL Certificate Expiry [-/+]

50350 - OS Identification Failed [-/+]

10863 - SSL Certificate Information [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

57582 - SSL Self-Signed Certificate [-/+]

117530 - Errors in nessusd.dump [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

19506 - Nessus Scan Information [-/+]

10386 - Web Server No 404 Error Code Check [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

90591 - Cisco Prime Infrastructure Detection [-/+]

10.2.2.26

Scan Information

Start time: 2020/04/22 19:42

End time: 2020/04/22 21:04

Host Information

DNS Name: Server.Entidad.col

Netbios Name: CILENE

OS: [0: Windows Server 2016 Datacenter 14393]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	0	27	34

Results Details

/

10287 - Traceroute Information	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
10736 - DCE Services Enumeration	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
54615 - Device Type	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
11219 - Nessus SYN scanner	[-/+]
43815 - NetBIOS Multiple IP Address Enumeration	[-/+]

45590 - Common Platform Enumeration (CPE)	[-/+]
10863 - SSL Certificate Information	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
19506 - Nessus Scan Information	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
135860 - WMI Not Available	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
57608 - SMB Signing not required	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
110723 - No Credentials Provided	[-/+]
11936 - OS Identification	[-/+]

10.2.2.28

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 01:32

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	ELARA
OS:	[0: Microsoft Windows Server 2012 R2 Datacenter]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	9	1	37	48

Results Details

/

51891 - SSL Session Resume Supported	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
10736 - DCE Services Enumeration	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
11219 - Nessus SYN scanner	[-/+]
46180 - Additional DNS Hostnames	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
22964 - Service Detection	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
110723 - No Credentials Provided	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
19506 - Nessus Scan Information	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
10107 - HTTP Server Type and Version	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]

25220 - TCP/IP Timestamps Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
54615 - Device Type	[-/+]
57608 - SMB Signing not required	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
10287 - Traceroute Information	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
135860 - WMI Not Available	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
59861 - Remote web server screenshot	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
11936 - OS Identification	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote	[-/+]

check)

64814 - Terminal Services Use SSL/TLS [-/+]

10.2.2.31

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 05:41

Host Information

DNS Name:	vm-Server.Entidad.col
Netbios Name:	VM-PLANEACION
OS:	[0: Microsoft Windows 8.1 Pro]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	1	26	34

Results Details

/

10287 - Traceroute Information [-/+]

10736 - DCE Services Enumeration [-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) [-/+]

21643 - SSL Cipher Suites Supported [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

64814 - Terminal Services Use SSL/TLS [-/+]

56984 - SSL / TLS Versions Supported [-/+]

10863 - SSL Certificate Information [-/+]

11219 - Nessus SYN scanner [-/+]

57582 - SSL Self-Signed Certificate [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
54615 - Device Type	[-/+]
11936 - OS Identification	[-/+]
110723 - No Credentials Provided	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
19506 - Nessus Scan Information	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
135860 - WMI Not Available	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
57608 - SMB Signing not required	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]

10.2.2.33

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 03:51

Host Information

DNS Name: Server.Entidad.col

Netbios Name: PANCRACIA

OS: [0: Microsoft Windows 10]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	0	32	40

Results Details

/

10736 - DCE Services Enumeration	[-/+]
11936 - OS Identification	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
10863 - SSL Certificate Information	[-/+]
54615 - Device Type	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
11219 - Nessus SYN scanner	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
10107 - HTTP Server Type and Version	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
19506 - Nessus Scan Information	[-/+]

22964 - Service Detection	[-/+]
135860 - WMI Not Available	[-/+]
51891 - SSL Session Resume Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
46180 - Additional DNS Hostnames	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
57608 - SMB Signing not required	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
10287 - Traceroute Information	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
110723 - No Credentials Provided	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]

10.2.2.38

Scan Information

Start time: 2020/04/22 19:42

End time: 2020/04/23 05:05

Host Information

DNS Name: Server.Entidad.col

Netbios Name: METHONE

OS: [0: Microsoft Windows 10]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	0	31	38

Results Details

/

117886 - Local Checks Not Enabled (info) [-/+]

10736 - DCE Services Enumeration [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

11219 - Nessus SYN scanner [-/+]

10107 - HTTP Server Type and Version [-/+]

19506 - Nessus Scan Information [-/+]

57608 - SMB Signing not required [-/+]

46180 - Additional DNS Hostnames [-/+]

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) [-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

54615 - Device Type [-/+]

56984 - SSL / TLS Versions Supported [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10287 - Traceroute Information [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

135860 - WMI Not Available [-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
22964 - Service Detection	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
11936 - OS Identification	[-/+]
110723 - No Credentials Provided	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
10863 - SSL Certificate Information	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]

10.2.2.39

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 23:50

Host Information

DNS Name: Server.Entidad.col

Netbios Name: ARTEMISA

OS: [0: Microsoft Windows 8.1][1: Microsoft Windows 10 Enterprise Insider Preview][2: Microsoft Windows Server 2012 R2]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	0	39	47

Results Details

/

11219 - Nessus SYN scanner	[-/+]
19601 - HP Data Protector Detection	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
135860 - WMI Not Available	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
22964 - Service Detection	[-/+]
10736 - DCE Services Enumeration	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
110723 - No Credentials Provided	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
10107 - HTTP Server Type and Version	[-/+]
117530 - Errors in nessusd.dump	[-/+]
10287 - Traceroute Information	[-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
17975 - Service Detection (GET request)	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
10386 - Web Server No 404 Error Code Check	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
54615 - Device Type	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
67121 - HP Data Protector Components Version Detection	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
46180 - Additional DNS Hostnames	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
57608 - SMB Signing not required	[-/+]
10863 - SSL Certificate Information	[-/+]
11936 - OS Identification	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]

84821 - TLS ALPN Supported Protocol Enumeration [-/+]

57582 - SSL Self-Signed Certificate [-/+]

19506 - Nessus Scan Information [-/+]

90151 - Flexera FlexNet Publisher Detection [-/+]

10.2.2.42

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 22:16

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	MENIPE
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	13	2	34	50

Results Details

/

11219 - Nessus SYN scanner [-/+]

20007 - SSL Version 2 and 3 Protocol Detection [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) [-/+]

10736 - DCE Services Enumeration [-/+]

22964 - Service Detection [-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) [-/+]

11936 - OS Identification [-/+]

110723 - No Credentials Provided [-/+]

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) [-/+]

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure [-/+]

18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
10863 - SSL Certificate Information	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
57608 - SMB Signing not required	[-/+]
135860 - WMI Not Available	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
10107 - HTTP Server Type and Version	[-/+]
46180 - Additional DNS Hostnames	[-/+]
10287 - Traceroute Information	[-/+]
66173 - RDP Screenshot	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
124410 - SSL Root Certification Authority Distrusted	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]

24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
15901 - SSL Certificate Expiry	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)	[-/+]
54615 - Device Type	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
19506 - Nessus Scan Information	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]

10.2.2.54

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 06:15

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	FENRI
OS:	[0: Microsoft Windows 10]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	0	34	41

Results Details

/

57582 - SSL Self-Signed Certificate	[-/+]
10736 - DCE Services Enumeration	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
59861 - Remote web server screenshot	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
46180 - Additional DNS Hostnames	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
19506 - Nessus Scan Information	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
10107 - HTTP Server Type and Version	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
22964 - Service Detection	[-/+]
10287 - Traceroute Information	[-/+]

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
11936 - OS Identification	[-/+]
24242 - Microsoft .NET Handlers Enumeration	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
110723 - No Credentials Provided	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
135860 - WMI Not Available	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
57608 - SMB Signing not required	[-/+]
106658 - JQuery Detection	[-/+]
54615 - Device Type	[-/+]

10.2.2.58

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 02:09

Host Information

DNS Name:	dafne-Server.Entidad.col
Netbios Name:	DAFNE-DB
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total

0	0	6	0	26	32

Results Details

/

10736 - DCE Services Enumeration	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
11219 - Nessus SYN scanner	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
57608 - SMB Signing not required	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
110723 - No Credentials Provided	[-/+]
135860 - WMI Not Available	[-/+]
19506 - Nessus Scan Information	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
10287 - Traceroute Information	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]

54615 - Device Type [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

11936 - OS Identification [-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

57582 - SSL Self-Signed Certificate [-/+]

10.2.2.59

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 00:29

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	CHARON
OS:	[0: Microsoft Windows Server 2012 Datacenter]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	0	27	35

Results Details

/

11936 - OS Identification [-/+]

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) [-/+]

11219 - Nessus SYN scanner [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
110723 - No Credentials Provided	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
10736 - DCE Services Enumeration	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
10287 - Traceroute Information	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
19506 - Nessus Scan Information	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
135860 - WMI Not Available	[-/+]
43815 - NetBIOS Multiple IP Address Enumeration	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
57608 - SMB Signing not required	[-/+]
54615 - Device Type	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]

117886 - Local Checks Not Enabled (info) [-/+]

10863 - SSL Certificate Information [-/+]

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

21643 - SSL Cipher Suites Supported [-/+]

10.2.2.61

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 00:29

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	4	0	22	26

Results Details

/

56984 - SSL / TLS Versions Supported [-/+]

10386 - Web Server No 404 Error Code Check [-/+]

10863 - SSL Certificate Information [-/+]

10287 - Traceroute Information [-/+]

42823 - Non-compliant Strict Transport Security (STS) [-/+]

21643 - SSL Cipher Suites Supported [-/+]

94761 - SSL Root Certification Authority Certificate Information [-/+]

19506 - Nessus Scan Information [-/+]

22964 - Service Detection [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

11219 - Nessus SYN scanner [-/+]

10881 - SSH Protocol Versions Supported [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

42822 - Strict Transport Security (STS) Detection [-/+]

10267 - SSH Server Type and Version Information [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

57582 - SSL Self-Signed Certificate [-/+]

117530 - Errors in nessusd.dump [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

50350 - OS Identification Failed [-/+]

10107 - HTTP Server Type and Version [-/+]

10.2.2.62

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 21:52

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	IPAM
OS:	[0: Windows]

Results Summary

Critical	High	Medium	Low	Info	Total
0	3	16	1	39	59

Results Details

/

11219 - Nessus SYN scanner [-/+]

110723 - No Credentials Provided [-/+]

11011 - Microsoft Windows SMB Service Detection	[-/+]
128531 - PHP 7.3.x < 7.3.9 Multiple Vulnerabilities.	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
42981 - SSL Certificate Expiry - Future Expiry	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
48243 - PHP Version Detection	[-/+]
10736 - DCE Services Enumeration	[-/+]
128116 - OpenSSL 1.1.1 < 1.1.1d Multiple Vulnerabilities	[-/+]
10107 - HTTP Server Type and Version	[-/+]
129557 - PHP 7.3.x < 7.3.10 Heap-Based Buffer Overflow Vulnerability.	[-/+]
15901 - SSL Certificate Expiry	[-/+]
22964 - Service Detection	[-/+]
132725 - OpenSSL 1.1.1 < 1.1.1e-dev Procedure Overflow Vulnerability	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
135860 - WMI Not Available	[-/+]
11936 - OS Identification	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
135290 - Apache 2.4.x < 2.4.42 Multiple Vulnerabilities	[-/+]
46180 - Additional DNS Hostnames	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
48204 - Apache HTTP Server Version	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]

11213 - HTTP TRACE / TRACK Methods Allowed	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
66334 - Patch Report	[-/+]
128033 - Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	[-/+]
57323 - OpenSSL Version Detection	[-/+]
51891 - SSL Session Resume Supported	[-/+]
134944 - PHP 7.3.x < 7.3.16 Multiple Vulnerabilities	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
130276 - PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
83298 - SSL Certificate Chain Contains Certificates Expiring Soon	[-/+]
10287 - Traceroute Information	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
84821 - TLS ALPN Supported Protocol Enumeration	[-/+]
121479 - web.config File Information Disclosure	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
50845 - OpenSSL Detection	[-/+]
117530 - Errors in nessusd.dump	[-/+]

57608 - SMB Signing not required [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

19506 - Nessus Scan Information [-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) [-/+]

54615 - Device Type [-/+]

45411 - SSL Certificate with Wrong Hostname [-/+]

10.2.2.63

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 02:09

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	REDMON
OS:	[0: Windows]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	9	0	33	42

Results Details

/

135860 - WMI Not Available [-/+]

10863 - SSL Certificate Information [-/+]

19506 - Nessus Scan Information [-/+]

22964 - Service Detection [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

10736 - DCE Services Enumeration [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

10940 - Windows Terminal Services Enabled	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
51891 - SSL Session Resume Supported	[-/+]
11219 - Nessus SYN scanner	[-/+]
110723 - No Credentials Provided	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
10107 - HTTP Server Type and Version	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
11936 - OS Identification	[-/+]
46180 - Additional DNS Hostnames	[-/+]
10386 - Web Server No 404 Error Code Check	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
54615 - Device Type	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

10287 - Traceroute Information [-/+]

57608 - SMB Signing not required [-/+]

64814 - Terminal Services Use SSL/TLS [-/+]

94761 - SSL Root Certification Authority Certificate Information [-/+]

117530 - Errors in nessusd.dump [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check) [-/+]

10.2.2.64

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 23:50

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	INGRESOSOCIAL
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	10	2	31	43

Results Details

/

11011 - Microsoft Windows SMB Service Detection [-/+]

57582 - SSL Self-Signed Certificate [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

10736 - DCE Services Enumeration [-/+]

135860 - WMI Not Available [-/+]

45590 - Common Platform Enumeration (CPE)	[-/+]
11219 - Nessus SYN scanner	[-/+]
22964 - Service Detection	[-/+]
57608 - SMB Signing not required	[-/+]
54615 - Device Type	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
19506 - Nessus Scan Information	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
11936 - OS Identification	[-/+]
10287 - Traceroute Information	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
110723 - No Credentials Provided	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
66173 - RDP Screenshot	[-/+]
10107 - HTTP Server Type and Version	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
46180 - Additional DNS Hostnames	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]

10.2.2.65

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 05:05

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	DAFNE
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	1	41	50

Results Details

/

50845 - OpenSSL Detection	[-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
48204 - Apache HTTP Server Version	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
59861 - Remote web server screenshot	[-/+]
10863 - SSL Certificate Information	[-/+]
10736 - DCE Services Enumeration	[-/+]
57608 - SMB Signing not required	[-/+]
66318 - McAfee ePolicy Orchestrator Application Server Detection	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
10287 - Traceroute Information	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
10107 - HTTP Server Type and Version	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
35297 - SSL Service Requests Client Certificate	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
54615 - Device Type	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
110723 - No Credentials Provided	[-/+]

94761 - SSL Root Certification Authority Certificate Information	[-/+]
42822 - Strict Transport Security (STS) Detection	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
22964 - Service Detection	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
11936 - OS Identification	[-/+]
19506 - Nessus Scan Information	[-/+]
84821 - TLS ALPN Supported Protocol Enumeration	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
42823 - Non-compliant Strict Transport Security (STS)	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
46180 - Additional DNS Hostnames	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
135860 - WMI Not Available	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]

10.2.2.66

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 20:33

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	HALLEY
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	10	2	39	51

Results Details

/

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
10736 - DCE Services Enumeration	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
10107 - HTTP Server Type and Version	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
11219 - Nessus SYN scanner	[-/+]
11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
22964 - Service Detection	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
11936 - OS Identification	[-/+]
57608 - SMB Signing not required	[-/+]

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
59861 - Remote web server screenshot	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
38157 - Microsoft SharePoint Server Detection	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
117530 - Errors in nessusd.dump	[-/+]
19506 - Nessus Scan Information	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
110723 - No Credentials Provided	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
135860 - WMI Not Available	[-/+]
108804 - Microsoft Exchange Server Detection (Uncredentialed)	[-/+]
10263 - SMTP Server Detection	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]

11153 - Service Detection (HELP Request) [-/+]

54615 - Device Type [-/+]

57582 - SSL Self-Signed Certificate [-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

10287 - Traceroute Information [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

46180 - Additional DNS Hostnames [-/+]

66173 - RDP Screenshot [-/+]

10863 - SSL Certificate Information [-/+]

21643 - SSL Cipher Suites Supported [-/+]

10.2.2.67

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 21:04

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	NEMESIS
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	13	3	36	53

Results Details

/

35291 - SSL Certificate Signed Using Weak Hashing Algorithm [-/+]

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

108761 - MSSQL Host Information in NTLM SSP [-/+]

21643 - SSL Cipher Suites Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
11936 - OS Identification	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
69482 - Microsoft SQL Server STARTTLS Support	[-/+]
57608 - SMB Signing not required	[-/+]
10144 - Microsoft SQL Server TCP/IP Listener Detection	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
10736 - DCE Services Enumeration	[-/+]
66173 - RDP Screenshot	[-/+]
10287 - Traceroute Information	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
110723 - No Credentials Provided	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
54615 - Device Type	[-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
46180 - Additional DNS Hostnames	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
10674 - Microsoft SQL Server UDP Query Remote Version Disclosure	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
22964 - Service Detection	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
135860 - WMI Not Available	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
10107 - HTTP Server Type and Version	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
19506 - Nessus Scan Information	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant [-/+]

10.2.2.73

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 02:46

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	ORFEO
OS:	[0: Microsoft Windows Server 2008 R2 Standard Service Pack 1]

Results Summary

Critical	High	Medium	Low	Info	Total
2	0	11	2	38	53

Results Details

/

11011 - Microsoft Windows SMB Service Detection [-/+]

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only [-/+]

10287 - Traceroute Information [-/+]

110723 - No Credentials Provided [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

11219 - Nessus SYN scanner [-/+]

10107 - HTTP Server Type and Version [-/+]

57582 - SSL Self-Signed Certificate [-/+]

19506 - Nessus Scan Information [-/+]

10394 - Microsoft Windows SMB Log In Possible [-/+]

56984 - SSL / TLS Versions Supported [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

66173 - RDP Screenshot [-/+]

11936 - OS Identification [-/+]

10736 - DCE Services Enumeration	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
54615 - Device Type	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
51891 - SSL Session Resume Supported	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
108797 - Unsupported Windows OS (remote)	[-/+]
46180 - Additional DNS Hostnames	[-/+]
14773 - Service Detection: 3 ASCII Digit Code Responses	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10092 - FTP Server Detection	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
66334 - Patch Report	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
135860 - WMI Not Available	[-/+]

57608 - SMB Signing not required	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
24786 - Nessus Windows Scan Not Performed with Admin Privileges	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
22964 - Service Detection	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]

10.2.2.77

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 06:15

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	ALBORIX
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	8	1	39	49

Results Details

/

10863 - SSL Certificate Information	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
10107 - HTTP Server Type and Version	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
24242 - Microsoft .NET Handlers Enumeration	[-/+]
59861 - Remote web server screenshot	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
135860 - WMI Not Available	[-/+]
11219 - Nessus SYN scanner	[-/+]
83298 - SSL Certificate Chain Contains Certificates Expiring Soon	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
10287 - Traceroute Information	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
22964 - Service Detection	[-/+]
95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)	[-/+]

42981 - SSL Certificate Expiry - Future Expiry	[-/+]
11936 - OS Identification	[-/+]
10736 - DCE Services Enumeration	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
54615 - Device Type	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
46180 - Additional DNS Hostnames	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
110723 - No Credentials Provided	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
106658 - JQuery Detection	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
19506 - Nessus Scan Information	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
57608 - SMB Signing not required	[-/+]

10.2.2.79

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 03:51

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	DANTE
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	12	2	34	49

Results Details

/

11219 - Nessus SYN scanner	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
46180 - Additional DNS Hostnames	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
22964 - Service Detection	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
54615 - Device Type	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
10736 - DCE Services Enumeration	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
57608 - SMB Signing not required	[-/+]
135860 - WMI Not Available	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
10107 - HTTP Server Type and Version	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
11936 - OS Identification	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
10287 - Traceroute Information	[-/+]
10863 - SSL Certificate Information	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]

110723 - No Credentials Provided [-/+]

94761 - SSL Root Certification Authority Certificate Information [-/+]

66173 - RDP Screenshot [-/+]

19506 - Nessus Scan Information [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

45411 - SSL Certificate with Wrong Hostname [-/+]

10940 - Windows Terminal Services Enabled [-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check) [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure [-/+]

10.2.2.81

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 21:29

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	ATLANTE
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
1	1	13	3	40	58

Results Details

/

135860 - WMI Not Available [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

10940 - Windows Terminal Services Enabled [-/+]

57582 - SSL Self-Signed Certificate [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
19601 - HP Data Protector Detection	[-/+]
11936 - OS Identification	[-/+]
11219 - Nessus SYN scanner	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
22964 - Service Detection	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
108761 - MSSQL Host Information in NTLM SSP	[-/+]
69482 - Microsoft SQL Server STARTTLS Support	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
10736 - DCE Services Enumeration	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
17975 - Service Detection (GET request)	[-/+]
10863 - SSL Certificate Information	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
102431 - HP Data Protector 8.x < 8.17 / 9.x < 9.09 Multiple Vulnerabilities (HPSBGN03732)	[-/+]

66173 - RDP Screenshot	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
57608 - SMB Signing not required	[-/+]
10107 - HTTP Server Type and Version	[-/+]
10144 - Microsoft SQL Server TCP/IP Listener Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
54615 - Device Type	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
19506 - Nessus Scan Information	[-/+]
67121 - HP Data Protector Components Version Detection	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
110723 - No Credentials Provided	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
10674 - Microsoft SQL Server UDP Query Remote Version Disclosure	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]

46180 - Additional DNS Hostnames [-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check) [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

66334 - Patch Report [-/+]

10287 - Traceroute Information [-/+]

10.2.2.85

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 03:25

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	OMEGA
OS:	[0: Microsoft Windows 10]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	0	33	40

Results Details

/

11219 - Nessus SYN scanner [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

10736 - DCE Services Enumeration [-/+]

11936 - OS Identification [-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure [-/+]

51891 - SSL Session Resume Supported [-/+]

21643 - SSL Cipher Suites Supported [-/+]

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) [-/+]

110723 - No Credentials Provided [-/+]

43111 - HTTP Methods Allowed (per directory)	[-/+]
57608 - SMB Signing not required	[-/+]
54615 - Device Type	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
135860 - WMI Not Available	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10107 - HTTP Server Type and Version	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
22964 - Service Detection	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
46180 - Additional DNS Hostnames	[-/+]
10863 - SSL Certificate Information	[-/+]
117530 - Errors in nessusd.dump	[-/+]
10287 - Traceroute Information	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure [-/+]

10940 - Windows Terminal Services Enabled [-/+]

19506 - Nessus Scan Information [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

10.2.2.89

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 02:09

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	EGERIA
OS:	[0: Microsoft Windows 10]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	10	0	42	53

Results Details

/

69482 - Microsoft SQL Server STARTTLS Support [-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

21643 - SSL Cipher Suites Supported [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

10940 - Windows Terminal Services Enabled [-/+]

54615 - Device Type [-/+]

20007 - SSL Version 2 and 3 Protocol Detection [-/+]

10107 - HTTP Server Type and Version	[-/+]
11219 - Nessus SYN scanner	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
57608 - SMB Signing not required	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
10736 - DCE Services Enumeration	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10863 - SSL Certificate Information	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
19506 - Nessus Scan Information	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
10287 - Traceroute Information	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]

59861 - Remote web server screenshot	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
110723 - No Credentials Provided	[-/+]
22964 - Service Detection	[-/+]
19689 - Embedded Web Server Detection	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
135860 - WMI Not Available	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
10144 - Microsoft SQL Server TCP/IP Listener Detection	[-/+]
10674 - Microsoft SQL Server UDP Query Remote Version Disclosure	[-/+]
11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
11936 - OS Identification	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
50845 - OpenSSL Detection	[-/+]
46180 - Additional DNS Hostnames	[-/+]
108761 - MSSQL Host Information in NTLM SSP	[-/+]

10.2.2.91

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 21:04

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	SKOLL

OS: [0: Windows]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	0	33	41

Results Details

/

10736 - DCE Services Enumeration	[-/+]
10394 - Microsoft Windows SMB Log In Possible	[-/+]
10287 - Traceroute Information	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
10919 - Open Port Re-check	[-/+]
26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
110723 - No Credentials Provided	[-/+]
10884 - Network Time Protocol (NTP) Server Detection	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
10863 - SSL Certificate Information	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
11936 - OS Identification	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
25701 - LDAP Crafted Search Request Server Information Disclosure	[-/+]
57608 - SMB Signing not required	[-/+]
11002 - DNS Server Detection	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
19506 - Nessus Scan Information	[-/+]
22964 - Service Detection	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
20870 - LDAP Server Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
35372 - DNS Server Dynamic Update Record Injection	[-/+]
54615 - Device Type	[-/+]
43829 - Kerberos Information Disclosure	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
24786 - Nessus Windows Scan Not Performed with Admin Privileges	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
135860 - WMI Not Available	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]

10.2.2.96

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 21:04

Host Information

DNS Name: Server.Entidad.col

Netbios Name: FREDA

OS: [0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	9	1	30	40

Results Details

/

11219 - Nessus SYN scanner	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
110723 - No Credentials Provided	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
54615 - Device Type	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
10736 - DCE Services Enumeration	[-/+]
10144 - Microsoft SQL Server TCP/IP Listener Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
19506 - Nessus Scan Information	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]

57608 - SMB Signing not required	[-/+]
69482 - Microsoft SQL Server STARTTLS Support	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
10287 - Traceroute Information	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
108761 - MSSQL Host Information in NTLM SSP	[-/+]
135860 - WMI Not Available	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
11936 - OS Identification	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]

10.2.2.97

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 03:51

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	ADMETE
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	10	2	41	53

Results Details

/

66173 - RDP Screenshot	[-/+]
11219 - Nessus SYN scanner	[-/+]
57608 - SMB Signing not required	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10736 - DCE Services Enumeration	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
19601 - HP Data Protector Detection	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
19506 - Nessus Scan Information	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
110723 - No Credentials Provided	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
11153 - Service Detection (HELP Request)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
38157 - Microsoft SharePoint Server Detection	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]

17975 - Service Detection (GET request)	[-/+]
10107 - HTTP Server Type and Version	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
108804 - Microsoft Exchange Server Detection (Uncredentialed)	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
10263 - SMTP Server Detection	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
46180 - Additional DNS Hostnames	[-/+]
11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
54615 - Device Type	[-/+]
22964 - Service Detection	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
59861 - Remote web server screenshot	[-/+]

10287 - Traceroute Information [-/+]

11936 - OS Identification [-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure [-/+]

135860 - WMI Not Available [-/+]

117530 - Errors in nessusd.dump [-/+]

21643 - SSL Cipher Suites Supported [-/+]

57582 - SSL Self-Signed Certificate [-/+]

56984 - SSL / TLS Versions Supported [-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) [-/+]

10.2.2.98

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 21:04

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	LUCIA
OS:	[0: Windows Server 2016 Standard 14393]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	0	28	36

Results Details

/

10287 - Traceroute Information [-/+]

19506 - Nessus Scan Information [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]

11219 - Nessus SYN scanner	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
10736 - DCE Services Enumeration	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
135860 - WMI Not Available	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
10863 - SSL Certificate Information	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
57608 - SMB Signing not required	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
10658 - Oracle Database tnslsnr Service Remote Version Disclosure	[-/+]

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only [-/+]

110723 - No Credentials Provided [-/+]

54615 - Device Type [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

11936 - OS Identification [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

22073 - Oracle Database Detection [-/+]

10.2.2.99

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 06:15

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	VPROMETEOS
OS:	[0: Windows Server 2016 Standard 14393]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	0	26	34

Results Details

/

11011 - Microsoft Windows SMB Service Detection [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

19506 - Nessus Scan Information [-/+]

10736 - DCE Services Enumeration [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check) [-/+]

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
10287 - Traceroute Information	[-/+]
110723 - No Credentials Provided	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
11219 - Nessus SYN scanner	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
54615 - Device Type	[-/+]
135860 - WMI Not Available	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
11936 - OS Identification	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
57608 - SMB Signing not required	[-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure [-/+]

10940 - Windows Terminal Services Enabled [-/+]

10.2.2.103

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 03:51

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	LETO
OS:	[0: Microsoft Windows Server 2008 R2 Standard Service Pack 1]

Results Summary

Critical	High	Medium	Low	Info	Total
2	1	11	1	34	49

Results Details

/

10658 - Oracle Database tnslsnr Service Remote Version Disclosure [-/+]

51891 - SSL Session Resume Supported [-/+]

66173 - RDP Screenshot [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

11219 - Nessus SYN scanner [-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check) [-/+]

69552 - Oracle TNS Listener Remote Poisoning [-/+]

24786 - Nessus Windows Scan Not Performed with Admin Privileges [-/+]

10863 - SSL Certificate Information [-/+]

10736 - DCE Services Enumeration [-/+]

11936 - OS Identification [-/+]

51192 - SSL Certificate Cannot Be Trusted	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
108797 - Unsupported Windows OS (remote)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
10287 - Traceroute Information	[-/+]
26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
19506 - Nessus Scan Information	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
10394 - Microsoft Windows SMB Log In Possible	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
110723 - No Credentials Provided	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
66334 - Patch Report	[-/+]
135860 - WMI Not Available	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]

35291 - SSL Certificate Signed Using Weak Hashing Algorithm [-/+]

125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check) [-/+]

57608 - SMB Signing not required [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

54615 - Device Type [-/+]

21643 - SSL Cipher Suites Supported [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

22073 - Oracle Database Detection [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]

64814 - Terminal Services Use SSL/TLS [-/+]

10.2.2.105

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 06:15

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	ANDROMACA
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
1	1	10	2	35	49

Results Details

/

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

66334 - Patch Report [-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
10736 - DCE Services Enumeration	[-/+]
10674 - Microsoft SQL Server UDP Query Remote Version Disclosure	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
54615 - Device Type	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
135860 - WMI Not Available	[-/+]
19601 - HP Data Protector Detection	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
11936 - OS Identification	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
10863 - SSL Certificate Information	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
17975 - Service Detection (GET request)	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
19506 - Nessus Scan Information	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
67121 - HP Data Protector Components Version Detection	[-/+]
108761 - MSSQL Host Information in NTLM SSP	[-/+]
102431 - HP Data Protector 8.x < 8.17 / 9.x < 9.09 Multiple Vulnerabilities (HPSBGN03732)	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
10287 - Traceroute Information	[-/+]
57608 - SMB Signing not required	[-/+]
69482 - Microsoft SQL Server STARTTLS Support	[-/+]
110723 - No Credentials Provided	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
10144 - Microsoft SQL Server TCP/IP Listener Detection	[-/+]

10.2.2.106

Scan Information

Start time: 2020/04/22 19:42

End time: 2020/04/22 22:16

Host Information

DNS Name: Server.Entidad.col

Netbios Name: ASTRA

OS: [0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	13	3	32	49

Results Details

/

11219 - Nessus SYN scanner [-/+]

45411 - SSL Certificate with Wrong Hostname [-/+]

57582 - SSL Self-Signed Certificate [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

57690 - Terminal Services Encryption Level is Medium or Low [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

110723 - No Credentials Provided [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

10144 - Microsoft SQL Server TCP/IP Listener Detection [-/+]

45410 - SSL Certificate 'commonName' Mismatch [-/+]

10736 - DCE Services Enumeration [-/+]

56984 - SSL / TLS Versions Supported [-/+]

21643 - SSL Cipher Suites Supported [-/+]

54615 - Device Type [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

35291 - SSL Certificate Signed Using Weak Hashing Algorithm [-/+]

10674 - Microsoft SQL Server UDP Query Remote Version Disclosure	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
19506 - Nessus Scan Information	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
135860 - WMI Not Available	[-/+]
69482 - Microsoft SQL Server STARTTLS Support	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
10863 - SSL Certificate Information	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
10287 - Traceroute Information	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
108761 - MSSQL Host Information in NTLM SSP	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
57608 - SMB Signing not required	[-/+]

66173 - RDP Screenshot [-/+]

18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness [-/+]

11936 - OS Identification [-/+]

30218 - Terminal Services Encryption Level is not FIPS-140 Compliant [-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure [-/+]

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits [-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) [-/+]

10.2.2.107

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 05:41

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	JOVENES
OS:	[0: Microsoft Windows Server 2008 R2 Standard Service Pack 1]

Results Summary

Critical	High	Medium	Low	Info	Total
2	0	11	2	36	51

Results Details

/

25220 - TCP/IP Timestamps Supported [-/+]

10736 - DCE Services Enumeration [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

11219 - Nessus SYN scanner [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
51891 - SSL Session Resume Supported	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
19506 - Nessus Scan Information	[-/+]
135860 - WMI Not Available	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
10394 - Microsoft Windows SMB Log In Possible	[-/+]
26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
57608 - SMB Signing not required	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
11936 - OS Identification	[-/+]
22964 - Service Detection	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
108797 - Unsupported Windows OS (remote)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
54615 - Device Type	[-/+]

125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
10107 - HTTP Server Type and Version	[-/+]
110723 - No Credentials Provided	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
24786 - Nessus Windows Scan Not Performed with Admin Privileges	[-/+]
46180 - Additional DNS Hostnames	[-/+]
10863 - SSL Certificate Information	[-/+]
66334 - Patch Report	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
10287 - Traceroute Information	[-/+]
66173 - RDP Screenshot	[-/+]

10.2.2.110

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 03:25

Host Information

DNS Name: Server.Entidad.col

Netbios Name: VATLAS

OS: [0: Microsoft Windows Server 2012 R2 Datacenter]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	1	28	36

Results Details

/

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

19506 - Nessus Scan Information [-/+]

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) [-/+]

10736 - DCE Services Enumeration [-/+]

11936 - OS Identification [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

10287 - Traceroute Information [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

54615 - Device Type [-/+]

43815 - NetBIOS Multiple IP Address Enumeration [-/+]

51891 - SSL Session Resume Supported [-/+]

135860 - WMI Not Available [-/+]

57608 - SMB Signing not required [-/+]

11219 - Nessus SYN scanner [-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
10863 - SSL Certificate Information	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
110723 - No Credentials Provided	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]

10.2.2.112

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 03:25

Host Information

DNS Name:	jovenescapacitacion.EntidadSocial.gov.co
OS:	[0: Microsoft Windows 8][1: Microsoft Windows 7][2: Microsoft Windows Server 2008 R2][3: Microsoft Windows Server 2003][4: M...

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	5	0	20	25

Results Details

/

21643 - SSL Cipher Suites Supported	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
11219 - Nessus SYN scanner	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
10107 - HTTP Server Type and Version	[-/+]
10287 - Traceroute Information	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
22964 - Service Detection	[-/+]
51891 - SSL Session Resume Supported	[-/+]
54615 - Device Type	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
66173 - RDP Screenshot	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
11936 - OS Identification	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]

19506 - Nessus Scan Information [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

10.2.2.113

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 06:15

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	SOFIA
OS:	[0: Windows Server 2016 Standard 14393]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	0	27	35

Results Details

/

51891 - SSL Session Resume Supported [-/+]

10736 - DCE Services Enumeration [-/+]

21643 - SSL Cipher Suites Supported [-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure [-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check) [-/+]

11219 - Nessus SYN scanner [-/+]

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

11936 - OS Identification [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

10863 - SSL Certificate Information [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

10940 - Windows Terminal Services Enabled	[-/+]
57608 - SMB Signing not required	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
10287 - Traceroute Information	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
110723 - No Credentials Provided	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
135860 - WMI Not Available	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
19506 - Nessus Scan Information	[-/+]
54615 - Device Type	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]

10.2.2.114

Scan Information

Start time: 2020/04/22 19:42

End time: 2020/04/23 05:05

Host Information

DNS Name: Server.Entidad.col

Netbios Name: TELESTO

OS: [0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	2	36	45

Results Details

/

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) [-/+]

10736 - DCE Services Enumeration [-/+]

10940 - Windows Terminal Services Enabled [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

11219 - Nessus SYN scanner [-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) [-/+]

56984 - SSL / TLS Versions Supported [-/+]

22964 - Service Detection [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

11936 - OS Identification [-/+]

57608 - SMB Signing not required [-/+]

10287 - Traceroute Information [-/+]

10863 - SSL Certificate Information [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

21643 - SSL Cipher Suites Supported [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
19506 - Nessus Scan Information	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
135860 - WMI Not Available	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
54615 - Device Type	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
10107 - HTTP Server Type and Version	[-/+]
59861 - Remote web server screenshot	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
110723 - No Credentials Provided	[-/+]
46180 - Additional DNS Hostnames	[-/+]
10881 - SSH Protocol Versions Supported	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure [-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check) [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

10.2.2.115

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 05:05

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	AMALTEA
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	1	35	43

Results Details

/

10736 - DCE Services Enumeration [-/+]

11219 - Nessus SYN scanner [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

11153 - Service Detection (HELP Request) [-/+]

38157 - Microsoft SharePoint Server Detection [-/+]

21643 - SSL Cipher Suites Supported [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

10107 - HTTP Server Type and Version [-/+]

11936 - OS Identification [-/+]

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
19506 - Nessus Scan Information	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
110723 - No Credentials Provided	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
22964 - Service Detection	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
57608 - SMB Signing not required	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
46180 - Additional DNS Hostnames	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
10287 - Traceroute Information	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
135860 - WMI Not Available	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
54615 - Device Type	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

10940 - Windows Terminal Services Enabled [-/+]

10863 - SSL Certificate Information [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

11422 - Web Server Unconfigured - Default Install Page Present [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

117530 - Errors in nessusd.dump [-/+]

10.2.2.118

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 02:09

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	PERSEFONE
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
1	1	13	3	36	54

Results Details

/

10736 - DCE Services Enumeration [-/+]

135860 - WMI Not Available [-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check) [-/+]

69482 - Microsoft SQL Server STARTTLS Support [-/+]

45410 - SSL Certificate 'commonName' Mismatch [-/+]

66173 - RDP Screenshot [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

67121 - HP Data Protector Components Version Detection	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
11219 - Nessus SYN scanner	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
57608 - SMB Signing not required	[-/+]
10144 - Microsoft SQL Server TCP/IP Listener Detection	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
108761 - MSSQL Host Information in NTLM SSP	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
11936 - OS Identification	[-/+]
19506 - Nessus Scan Information	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
10674 - Microsoft SQL Server UDP Query Remote Version	[-/+]

Disclosure	
57582 - SSL Self-Signed Certificate	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
10287 - Traceroute Information	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
66334 - Patch Report	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
19601 - HP Data Protector Detection	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
102431 - HP Data Protector 8.x < 8.17 / 9.x < 9.09 Multiple Vulnerabilities (HPSBGN03732)	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
54615 - Device Type	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
110723 - No Credentials Provided	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
17975 - Service Detection (GET request)	[-/+]

10.2.2.119

Scan Information

Start time: 2020/04/22 19:42

End time: 2020/04/22 20:33

Host Information

DNS Name: Server.Entidad.col

Netbios Name: CELIO

OS: [0: Windows]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	1	27	35

Results Details

/

10863 - SSL Certificate Information	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
57608 - SMB Signing not required	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
10736 - DCE Services Enumeration	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
11219 - Nessus SYN scanner	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
11936 - OS Identification	[-/+]
71049 - SSH Weak MAC Algorithms Enabled	[-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
135860 - WMI Not Available	[-/+]
54615 - Device Type	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
22964 - Service Detection	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
110723 - No Credentials Provided	[-/+]
19506 - Nessus Scan Information	[-/+]
51891 - SSL Session Resume Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
10287 - Traceroute Information	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]

10.2.2.129

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 05:41

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	COLOSO

OS: [0: Microsoft Windows Server 2012 R2 Datacenter]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	10	2	30	42

Results Details

/

43815 - NetBIOS Multiple IP Address Enumeration	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
57608 - SMB Signing not required	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
135860 - WMI Not Available	[-/+]
10736 - DCE Services Enumeration	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
10287 - Traceroute Information	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
83298 - SSL Certificate Chain Contains Certificates Expiring Soon	[-/+]
42981 - SSL Certificate Expiry - Future Expiry	[-/+]
66173 - RDP Screenshot	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
11936 - OS Identification	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
19506 - Nessus Scan Information	[-/+]
10863 - SSL Certificate Information	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
11219 - Nessus SYN scanner	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
54615 - Device Type	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
110723 - No Credentials Provided	[-/+]

10.2.2.131

Scan Information

Start time: 2020/04/22 19:42

End time: 2020/04/23 00:55

Host Information

DNS Name: Server.Entidad.col

Netbios Name: URANIA

OS: [0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	13	1	36	51

Results Details

/

11219 - Nessus SYN scanner [-/+]

54615 - Device Type [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

10736 - DCE Services Enumeration [-/+]

10287 - Traceroute Information [-/+]

22964 - Service Detection [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

10107 - HTTP Server Type and Version [-/+]

18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness [-/+]

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

11422 - Web Server Unconfigured - Default Install Page Present [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

46180 - Additional DNS Hostnames [-/+]

57582 - SSL Self-Signed Certificate [-/+]

21643 - SSL Cipher Suites Supported [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
15901 - SSL Certificate Expiry	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
51891 - SSL Session Resume Supported	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
59861 - Remote web server screenshot	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
11936 - OS Identification	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
66173 - RDP Screenshot	[-/+]
10863 - SSL Certificate Information	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]

19506 - Nessus Scan Information	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
57608 - SMB Signing not required	[-/+]
135860 - WMI Not Available	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
110723 - No Credentials Provided	[-/+]

10.2.2.132

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 00:29

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	AGENOR
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	13	1	36	51

Results Details

/

104743 - TLS Version 1.0 Protocol Detection	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
10736 - DCE Services Enumeration	[-/+]
15901 - SSL Certificate Expiry	[-/+]

10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
19506 - Nessus Scan Information	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
57608 - SMB Signing not required	[-/+]
11219 - Nessus SYN scanner	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
22964 - Service Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
11936 - OS Identification	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
59861 - Remote web server screenshot	[-/+]
10107 - HTTP Server Type and Version	[-/+]
11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
10287 - Traceroute Information	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
51891 - SSL Session Resume Supported	[-/+]
110723 - No Credentials Provided	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
54615 - Device Type	[-/+]
10863 - SSL Certificate Information	[-/+]
46180 - Additional DNS Hostnames	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
135860 - WMI Not Available	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
66173 - RDP Screenshot	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]

10.2.2.135

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 03:25

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	SKADI
OS:	[0: Windows Server 2016 Datacenter 14393]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	0	27	35

Results Details

/

11011 - Microsoft Windows SMB Service Detection	[-/+]
10736 - DCE Services Enumeration	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
11219 - Nessus SYN scanner	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
110723 - No Credentials Provided	[-/+]
43815 - NetBIOS Multiple IP Address Enumeration	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]

121010 - TLS Version 1.1 Protocol Detection	[-/+]
135860 - WMI Not Available	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
57608 - SMB Signing not required	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
11936 - OS Identification	[-/+]
10287 - Traceroute Information	[-/+]
10863 - SSL Certificate Information	[-/+]
19506 - Nessus Scan Information	[-/+]
54615 - Device Type	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]

10.2.2.141

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 22:16

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	VKORE
OS:	[0: Microsoft Windows Server 2012 R2 Datacenter]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	10	2	30	42

Results Details

/

10736 - DCE Services Enumeration	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
19506 - Nessus Scan Information	[-/+]
66173 - RDP Screenshot	[-/+]
54615 - Device Type	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
11219 - Nessus SYN scanner	[-/+]
10863 - SSL Certificate Information	[-/+]
57608 - SMB Signing not required	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
11936 - OS Identification	[-/+]
110723 - No Credentials Provided	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
42981 - SSL Certificate Expiry - Future Expiry	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
10287 - Traceroute Information	[-/+]

18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
83298 - SSL Certificate Chain Contains Certificates Expiring Soon	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
135860 - WMI Not Available	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
43815 - NetBIOS Multiple IP Address Enumeration	[-/+]

10.2.2.142

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 05:41

Host Information

DNS Name: Server.Entidad.col

Netbios Name: THEMIS

OS: [0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	11	2	37	51

Results Details

/

10736 - DCE Services Enumeration	[-/+]
11219 - Nessus SYN scanner	[-/+]
11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
19506 - Nessus Scan Information	[-/+]
10287 - Traceroute Information	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
54615 - Device Type	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
57608 - SMB Signing not required	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]

45590 - Common Platform Enumeration (CPE)	[-/+]
11153 - Service Detection (HELP Request)	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
11936 - OS Identification	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
59861 - Remote web server screenshot	[-/+]
135860 - WMI Not Available	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
15901 - SSL Certificate Expiry	[-/+]
10107 - HTTP Server Type and Version	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
46180 - Additional DNS Hostnames	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
38157 - Microsoft SharePoint Server Detection	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]

110723 - No Credentials Provided [-/+]

22964 - Service Detection [-/+]

20007 - SSL Version 2 and 3 Protocol Detection [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

10940 - Windows Terminal Services Enabled [-/+]

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) [-/+]

10863 - SSL Certificate Information [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

10.2.2.149

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 04:35

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	DAMIAN
OS:	[0: Windows Server 2016 Standard 14393]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	8	0	29	38

Results Details

/

10863 - SSL Certificate Information [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

11219 - Nessus SYN scanner [-/+]

21643 - SSL Cipher Suites Supported [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only [-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) [-/+]

56984 - SSL / TLS Versions Supported	[-/+]
10736 - DCE Services Enumeration	[-/+]
22073 - Oracle Database Detection	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
69552 - Oracle TNS Listener Remote Poisoning	[-/+]
57608 - SMB Signing not required	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
11936 - OS Identification	[-/+]
110723 - No Credentials Provided	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
66334 - Patch Report	[-/+]
10658 - Oracle Database tnslsnr Service Remote Version Disclosure	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
135860 - WMI Not Available	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]

64814 - Terminal Services Use SSL/TLS [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

10287 - Traceroute Information [-/+]

57582 - SSL Self-Signed Certificate [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

54615 - Device Type [-/+]

19506 - Nessus Scan Information [-/+]

10.2.2.150

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 21:52

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	VAR
OS:	[0: Windows Server 2016 Standard 14393]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	8	0	29	38

Results Details

/

10736 - DCE Services Enumeration [-/+]

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]

57608 - SMB Signing not required [-/+]

10658 - Oracle Database tnslsnr Service Remote Version Disclosure [-/+]

11219 - Nessus SYN scanner [-/+]

69552 - Oracle TNS Listener Remote Poisoning	[-/+]
10287 - Traceroute Information	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
10863 - SSL Certificate Information	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
54615 - Device Type	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
110723 - No Credentials Provided	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
66334 - Patch Report	[-/+]
22073 - Oracle Database Detection	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
135860 - WMI Not Available	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check) [-/+]

56984 - SSL / TLS Versions Supported [-/+]

11936 - OS Identification [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

19506 - Nessus Scan Information [-/+]

10.2.2.157

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 00:29

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	CALYPSO
OS:	[0: Windows Server 2016 Standard 14393]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	0	26	33

Results Details

/

10863 - SSL Certificate Information [-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) [-/+]

10736 - DCE Services Enumeration [-/+]

96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) [-/+]

42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure [-/+]

11219 - Nessus SYN scanner [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check) [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

135860 - WMI Not Available	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
54615 - Device Type	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
110723 - No Credentials Provided	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
19506 - Nessus Scan Information	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
11936 - OS Identification	[-/+]
10287 - Traceroute Information	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
57608 - SMB Signing not required	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]

10.2.2.171

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 23:50

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	SICORAX
OS:	[0: Microsoft Windows Server 2012 R2 Datacenter]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	7	1	27	35

Results Details

/

11219 - Nessus SYN scanner	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
10736 - DCE Services Enumeration	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
19506 - Nessus Scan Information	[-/+]
54615 - Device Type	[-/+]
135860 - WMI Not Available	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]

11936 - OS Identification	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
43815 - NetBIOS Multiple IP Address Enumeration	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
10863 - SSL Certificate Information	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
57608 - SMB Signing not required	[-/+]
10287 - Traceroute Information	[-/+]
110723 - No Credentials Provided	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]

10.2.2.182

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/22 20:33

Host Information

DNS Name:	Server.Entidad.col

Netbios Name: SPONDE

OS: [0: Microsoft Windows Server 2012 R2 Datacenter]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	10	2	28	40

Results Details

/

21643 - SSL Cipher Suites Supported	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
135860 - WMI Not Available	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
10736 - DCE Services Enumeration	[-/+]
11936 - OS Identification	[-/+]
43815 - NetBIOS Multiple IP Address Enumeration	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
11219 - Nessus SYN scanner	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]

10287 - Traceroute Information	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
110723 - No Credentials Provided	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
54615 - Device Type	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
57608 - SMB Signing not required	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
66173 - RDP Screenshot	[-/+]
10863 - SSL Certificate Information	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
19506 - Nessus Scan Information	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]

10.2.2.188

Scan Information

Start time:	2020/04/22 19:42
End time:	2020/04/23 05:41

Host Information

DNS Name: Server.Entidad.col

OS: [0: Windows]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	15	16

Results Details

/

45590 - Common Platform Enumeration (CPE)	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
110723 - No Credentials Provided	[-/+]
54615 - Device Type	[-/+]
11219 - Nessus SYN scanner	[-/+]
10736 - DCE Services Enumeration	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
19506 - Nessus Scan Information	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
57608 - SMB Signing not required	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
10287 - Traceroute Information	[-/+]
11936 - OS Identification	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
135860 - WMI Not Available	[-/+]
10919 - Open Port Re-check	[-/+]

10.2.2.190

Scan Information

Start time: 2020/04/22 19:42

End time: 2020/04/23 01:32

Host Information

DNS Name:	Server.Entidad.col
Netbios Name:	BESTLA
OS:	[0: Microsoft Windows 10]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	0	35	43

Results Details

/

11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
10107 - HTTP Server Type and Version	[-/+]
51891 - SSL Session Resume Supported	[-/+]
10736 - DCE Services Enumeration	[-/+]
10863 - SSL Certificate Information	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
57608 - SMB Signing not required	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
19506 - Nessus Scan Information	[-/+]
22964 - Service Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
110723 - No Credentials Provided	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
135860 - WMI Not Available	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]

ANEXO 03

NOTA: Todas las direcciones IP fueron modificadas para conservar la confidencialidad y reserva de la entidad.

Tenable.io Report

Mon, 13 Apr 2020 18:47:58 UTC

Table Of Contents

10.2.1.37

10.2.1.38

10.2.1.41

10.2.1.42

10.2.1.43

10.2.1.44

10.2.1.45

10.2.1.51

10.2.1.53

10.2.1.54

10.2.1.55

10.2.1.61

10.2.1.62

10.2.1.63

10.2.1.64

10.2.1.65

10.2.1.69

10.2.1.71

10.2.1.72

10.2.1.73

10.2.1.74

10.2.1.75

10.2.1.81

10.2.1.82

10.2.1.83

10.2.1.84

10.2.1.85

10.2.1.91

10.2.1.92

10.2.1.93

10.2.1.94

10.2.1.95

10.2.1.100

10.2.1.101

10.2.1.102

10.2.1.103

10.2.1.104

10.2.1.105

10.2.1.111

10.2.1.112

10.2.1.113

10.2.1.114

10.2.1.115

10.2.1.121

10.2.1.122

10.2.1.123

10.2.1.249

10.2.1.250

Remediations

Suggested Remediations

Vulnerabilities By Host

[-] Collapse All

[+] Expand All

10.2.1.2

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 22:01

Host Information

OS:	[0: CISCO IOS][1: Cisco IOS XE]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	9	3	22	34

Results Details

/

15901 - SSL Certificate Expiry [-/+]

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
19689 - Embedded Web Server Detection	[-/+]
26928 - SSL Weak Cipher Suites Supported	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
10881 - SSH Protocol Versions Supported	[-/+]
11219 - Nessus SYN scanner	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
54615 - Device Type	[-/+]
22964 - Service Detection	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
10287 - Traceroute Information	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
10107 - HTTP Server Type and Version	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
42263 - Unencrypted Telnet Server	[-/+]
71049 - SSH Weak MAC Algorithms Enabled	[-/+]
10863 - SSL Certificate Information	[-/+]
19506 - Nessus Scan Information	[-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

105161 - Cisco Smart Install Detection [-/+]

10267 - SSH Server Type and Version Information [-/+]

110723 - No Credentials Provided [-/+]

35291 - SSL Certificate Signed Using Weak Hashing Algorithm [-/+]

11936 - OS Identification [-/+]

10.2.1.3

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 22:01

Host Information

OS:	[0: CISCO IOS][1: Cisco IOS XE]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	8	2	22	33

Results Details

/

78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) [-/+]

21643 - SSL Cipher Suites Supported [-/+]

56984 - SSL / TLS Versions Supported [-/+]

22964 - Service Detection [-/+]

11219 - Nessus SYN scanner [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

19689 - Embedded Web Server Detection [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) [-/+]

10881 - SSH Protocol Versions Supported [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

94761 - SSL Root Certification Authority Certificate Information [-/+]

20007 - SSL Version 2 and 3 Protocol Detection [-/+]

10107 - HTTP Server Type and Version [-/+]

110723 - No Credentials Provided [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

19506 - Nessus Scan Information [-/+]

57582 - SSL Self-Signed Certificate [-/+]

35291 - SSL Certificate Signed Using Weak Hashing Algorithm [-/+]

11936 - OS Identification [-/+]

10863 - SSL Certificate Information [-/+]

15901 - SSL Certificate Expiry [-/+]

105161 - Cisco Smart Install Detection [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

31422 - Reverse NAT/Intercepting Proxy Detection [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

26928 - SSL Weak Cipher Suites Supported [-/+]

10267 - SSH Server Type and Version Information [-/+]

54615 - Device Type [-/+]

71049 - SSH Weak MAC Algorithms Enabled [-/+]

10287 - Traceroute Information [-/+]

10.2.1.4

Scan Information

Start time: 2020/04/13 17:03

End time: 2020/04/13 22:01

Host Information

OS: [0: Cisco NX-OS]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	15	15

Results Details

/

- 10267 - SSH Server Type and Version Information [-/+]
- 11219 - Nessus SYN scanner [-/+]
- 45590 - Common Platform Enumeration (CPE) [-/+]
- 19506 - Nessus Scan Information [-/+]
- 70657 - SSH Algorithms and Languages Supported [-/+]
- 110723 - No Credentials Provided [-/+]
- 11936 - OS Identification [-/+]
- 25220 - TCP/IP Timestamps Supported [-/+]
- 54615 - Device Type [-/+]
- 10287 - Traceroute Information [-/+]
- 10881 - SSH Protocol Versions Supported [-/+]
- 22964 - Service Detection [-/+]
- 117886 - Local Checks Not Enabled (info) [-/+]
- 39520 - Backported Security Patch Detection (SSH) [-/+]
- 10884 - Network Time Protocol (NTP) Server Detection [-/+]

10.2.1.5

Scan Information

Start time: 2020/04/13 17:03

End time: 2020/04/13 22:01

Host Information

OS: [0: Cisco NX-OS]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	15	15

Results Details

/

10881 - SSH Protocol Versions Supported [-/+]

110723 - No Credentials Provided [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

11936 - OS Identification [-/+]

39520 - Backported Security Patch Detection (SSH) [-/+]

11219 - Nessus SYN scanner [-/+]

10267 - SSH Server Type and Version Information [-/+]

54615 - Device Type [-/+]

10884 - Network Time Protocol (NTP) Server Detection [-/+]

19506 - Nessus Scan Information [-/+]

22964 - Service Detection [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10287 - Traceroute Information [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

10.2.1.6

Scan Information

Start time: 2020/04/13 17:03

End time: 2020/04/13 22:01

Host Information

OS: [0: CISCO IOS][1: Cisco IOS XE]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	2	16	26

Results Details

/

54615 - Device Type	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
10107 - HTTP Server Type and Version	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
19506 - Nessus Scan Information	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
11936 - OS Identification	[-/+]
11219 - Nessus SYN scanner	[-/+]
10863 - SSL Certificate Information	[-/+]
10884 - Network Time Protocol (NTP) Server Detection	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
22964 - Service Detection	[-/+]
19689 - Embedded Web Server Detection	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
26928 - SSL Weak Cipher Suites Supported	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]

56984 - SSL / TLS Versions Supported [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

10287 - Traceroute Information [-/+]

60108 - SSL Certificate Chain Contains Weak RSA Keys [-/+]

10.2.1.8

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 22:01

Host Information

DNS Name:	DR-Host.Entidad.col
Netbios Name:	DR-Host
OS:	[0: Windows Server 2016 Standard 14393]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	0	32	40

Results Details

/

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

10736 - DCE Services Enumeration [-/+]

11219 - Nessus SYN scanner [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

42981 - SSL Certificate Expiry - Future Expiry [-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) [-/+]

110723 - No Credentials Provided [-/+]

86420 - Ethernet MAC Addresses [-/+]

57608 - SMB Signing not required [-/+]

58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only [-/+]

10287 - Traceroute Information	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
83298 - SSL Certificate Chain Contains Certificates Expiring Soon	[-/+]
43815 - NetBIOS Multiple IP Address Enumeration	[-/+]
11936 - OS Identification	[-/+]
10863 - SSL Certificate Information	[-/+]
35716 - Ethernet Card Manufacturer Detection	[-/+]
51891 - SSL Session Resume Supported	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
66173 - RDP Screenshot	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
54615 - Device Type	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]

21643 - SSL Cipher Suites Supported [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10940 - Windows Terminal Services Enabled [-/+]

19506 - Nessus Scan Information [-/+]

10.2.1.11

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 22:01

Host Information

OS:	[0: CISCO IOS][1: Cisco IOS XE]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	4	22	34

Results Details

/

56984 - SSL / TLS Versions Supported [-/+]

10884 - Network Time Protocol (NTP) Server Detection [-/+]

10881 - SSH Protocol Versions Supported [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

22964 - Service Detection [-/+]

10863 - SSL Certificate Information [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

54615 - Device Type [-/+]

94761 - SSL Root Certification Authority Certificate Information [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

71049 - SSH Weak MAC Algorithms Enabled [-/+]

11219 - Nessus SYN scanner [-/+]

21643 - SSL Cipher Suites Supported	[-/+]
26928 - SSL Weak Cipher Suites Supported	[-/+]
110723 - No Credentials Provided	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
19506 - Nessus Scan Information	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
19689 - Embedded Web Server Detection	[-/+]
10287 - Traceroute Information	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
10107 - HTTP Server Type and Version	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
15901 - SSL Certificate Expiry	[-/+]
11936 - OS Identification	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]

10.2.1.12

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 22:01

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

10107 - HTTP Server Type and Version	[-/+]
22964 - Service Detection	[-/+]
106628 - lighttpd HTTP Server Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
11936 - OS Identification	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
19506 - Nessus Scan Information	[-/+]
10287 - Traceroute Information	[-/+]
54615 - Device Type	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
110723 - No Credentials Provided	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]

10.2.1.13

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 22:01

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	17	18

Results Details

/

10107 - HTTP Server Type and Version [-/+]

110723 - No Credentials Provided [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

22964 - Service Detection [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

19506 - Nessus Scan Information [-/+]

11219 - Nessus SYN scanner [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10287 - Traceroute Information [-/+]

10267 - SSH Server Type and Version Information [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

54615 - Device Type [-/+]

11936 - OS Identification [-/+]

117530 - Errors in nessusd.dump [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

10.2.1.20

Scan Information

Start time: 2020/04/13 17:03

End time: 2020/04/13 22:01

Host Information

OS: [0: Linux Kernel 2.6]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	6	2	25	34

Results Details

/

11219 - Nessus SYN scanner	[-/+]
106658 - JQuery Detection	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
130208 - Cisco Wireless LAN Controller Secure Shell (SSH) Denial of Service Vulnerability (cisco-sa-20191016-wlc-ssh-dos)	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
22964 - Service Detection	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
11936 - OS Identification	[-/+]
70122 - Cisco Wireless LAN Controller (WLC) Version	[-/+]
110723 - No Credentials Provided	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
59861 - Remote web server screenshot	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]

19506 - Nessus Scan Information	[-/+]
10287 - Traceroute Information	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
91486 - Wireless Access Controller Detection	[-/+]
50845 - OpenSSL Detection	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
54615 - Device Type	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
130259 - Cisco Wireless LAN Controller Path Traversal Vulnerability	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
131230 - Cisco Wireless LAN Controller HTTP Parsing Engine Denial of Service Vulnerability	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]

10.2.1.21

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 22:01

Host Information

OS:	[0: CISCO IOS][1: Cisco IOS XE]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	5	2	16	23

Results Details

/

10107 - HTTP Server Type and Version	[-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
22964 - Service Detection	[-/+]
60108 - SSL Certificate Chain Contains Weak RSA Keys	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
11936 - OS Identification	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
10287 - Traceroute Information	[-/+]
19506 - Nessus Scan Information	[-/+]
10884 - Network Time Protocol (NTP) Server Detection	[-/+]
54615 - Device Type	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
19689 - Embedded Web Server Detection	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
11219 - Nessus SYN scanner	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
10863 - SSL Certificate Information	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]

10.2.1.22

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 22:01

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	17	18

Results Details

/

11219 - Nessus SYN scanner	[-/+]
106628 - lighttpd HTTP Server Detection	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
22964 - Service Detection	[-/+]
10107 - HTTP Server Type and Version	[-/+]
10287 - Traceroute Information	[-/+]
117530 - Errors in nessusd.dump	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
54615 - Device Type	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
110723 - No Credentials Provided	[-/+]
11936 - OS Identification	[-/+]
19506 - Nessus Scan Information	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]

10.2.1.23

Scan Information

Start time: 2020/04/13 17:03

End time: 2020/04/13 22:01

Host Information

OS: [0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

106628 - lighttpd HTTP Server Detection [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

11219 - Nessus SYN scanner [-/+]

22964 - Service Detection [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10107 - HTTP Server Type and Version [-/+]

54615 - Device Type [-/+]

11936 - OS Identification [-/+]

19506 - Nessus Scan Information [-/+]

10267 - SSH Server Type and Version Information [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10287 - Traceroute Information [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

110723 - No Credentials Provided [-/+]

10.2.1.24

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 22:01

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

11219 - Nessus SYN scanner	[-/+]
22964 - Service Detection	[-/+]
10107 - HTTP Server Type and Version	[-/+]
106628 - lighttpd HTTP Server Detection	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
54615 - Device Type	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
10287 - Traceroute Information	[-/+]
19506 - Nessus Scan Information	[-/+]
11936 - OS Identification	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
110723 - No Credentials Provided	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]

10.2.1.25

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 22:01

Host Information

OS:	[0: Linux Kernel 2.6]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	17	18

Results Details

/

11219 - Nessus SYN scanner	[-/+]
22964 - Service Detection	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
106628 - lighttpd HTTP Server Detection	[-/+]
10107 - HTTP Server Type and Version	[-/+]
54615 - Device Type	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10287 - Traceroute Information	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
11936 - OS Identification	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
110723 - No Credentials Provided	[-/+]
117530 - Errors in nessusd.dump	[-/+]
19506 - Nessus Scan Information	[-/+]

25220 - TCP/IP Timestamps Supported [-/+]

10.2.1.31

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	11	4	21	36

Results Details

/

97861 - Network Time Protocol (NTP) Mode 6 Scanner [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

19689 - Embedded Web Server Detection [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

56984 - SSL / TLS Versions Supported [-/+]

10881 - SSH Protocol Versions Supported [-/+]

10287 - Traceroute Information [-/+]

10107 - HTTP Server Type and Version [-/+]

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) [-/+]

11936 - OS Identification [-/+]

54615 - Device Type [-/+]

11219 - Nessus SYN scanner [-/+]

35291 - SSL Certificate Signed Using Weak Hashing Algorithm [-/+]

22964 - Service Detection [-/+]

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits [-/+]

21643 - SSL Cipher Suites Supported	[-/+]
10884 - Network Time Protocol (NTP) Server Detection	[-/+]
26928 - SSL Weak Cipher Suites Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
71049 - SSH Weak MAC Algorithms Enabled	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
19506 - Nessus Scan Information	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
60108 - SSL Certificate Chain Contains Weak RSA Keys	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
66848 - SSL Null Cipher Suites Supported	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
110723 - No Credentials Provided	[-/+]

10.2.1.32

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	10	4	20	34

Results Details

/

19506 - Nessus Scan Information	[-/+]
71049 - SSH Weak MAC Algorithms Enabled	[-/+]
10107 - HTTP Server Type and Version	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
11936 - OS Identification	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
10881 - SSH Protocol Versions Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
10863 - SSL Certificate Information	[-/+]
11219 - Nessus SYN scanner	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
19689 - Embedded Web Server Detection	[-/+]
110723 - No Credentials Provided	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
22964 - Service Detection	[-/+]
10287 - Traceroute Information	[-/+]
60108 - SSL Certificate Chain Contains Weak RSA Keys	[-/+]
66848 - SSL Null Cipher Suites Supported	[-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

26928 - SSL Weak Cipher Suites Supported [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

21643 - SSL Cipher Suites Supported [-/+]

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

54615 - Device Type [-/+]

57582 - SSL Self-Signed Certificate [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

10.2.1.33

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: CISCO IOS][1: Cisco IOS XE]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	11	2	17	30

Results Details

/

26928 - SSL Weak Cipher Suites Supported [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

10107 - HTTP Server Type and Version [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

97861 - Network Time Protocol (NTP) Mode 6 Scanner [-/+]

19506 - Nessus Scan Information	[-/+]
11936 - OS Identification	[-/+]
11219 - Nessus SYN scanner	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
66848 - SSL Null Cipher Suites Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
19689 - Embedded Web Server Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
54615 - Device Type	[-/+]
22964 - Service Detection	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
10884 - Network Time Protocol (NTP) Server Detection	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
10287 - Traceroute Information	[-/+]
15901 - SSL Certificate Expiry	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]

10.2.1.34

Scan Information

Start time: 2020/04/13 17:03

End time: 2020/04/13 21:09

Host Information

OS: [0: CISCO IOS][1: Cisco IOS XE]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	10	4	21	35

Results Details

/

19689 - Embedded Web Server Detection [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

10863 - SSL Certificate Information [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

11219 - Nessus SYN scanner [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

94761 - SSL Root Certification Authority Certificate Information [-/+]

22964 - Service Detection [-/+]

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

15901 - SSL Certificate Expiry [-/+]

71049 - SSH Weak MAC Algorithms Enabled [-/+]

26928 - SSL Weak Cipher Suites Supported [-/+]

54615 - Device Type [-/+]

11936 - OS Identification [-/+]

66848 - SSL Null Cipher Suites Supported	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
19506 - Nessus Scan Information	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
10107 - HTTP Server Type and Version	[-/+]
10881 - SSH Protocol Versions Supported	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
110723 - No Credentials Provided	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
10287 - Traceroute Information	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]

10.2.1.35

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

22964 - Service Detection	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
10107 - HTTP Server Type and Version	[-/+]
11219 - Nessus SYN scanner	[-/+]
106628 - lighttpd HTTP Server Detection	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
11936 - OS Identification	[-/+]
54615 - Device Type	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
10287 - Traceroute Information	[-/+]
19506 - Nessus Scan Information	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
110723 - No Credentials Provided	[-/+]

10.2.1.36

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total

0	0	0	1	17	18

Results Details

/

106628 - lighttpd HTTP Server Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
19506 - Nessus Scan Information	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
22964 - Service Detection	[-/+]
10107 - HTTP Server Type and Version	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
117530 - Errors in nessusd.dump	[-/+]
54615 - Device Type	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
110723 - No Credentials Provided	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
11936 - OS Identification	[-/+]
10287 - Traceroute Information	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]

10.2.1.37

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	17	18

Results Details

/

10107 - HTTP Server Type and Version	[-/+]
11219 - Nessus SYN scanner	[-/+]
54615 - Device Type	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
106628 - lighttpd HTTP Server Detection	[-/+]
22964 - Service Detection	[-/+]
110723 - No Credentials Provided	[-/+]
11936 - OS Identification	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
19506 - Nessus Scan Information	[-/+]
117530 - Errors in nessusd.dump	[-/+]
10287 - Traceroute Information	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]

10.2.1.38

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

106628 - lighttpd HTTP Server Detection	[-/+]
22964 - Service Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
10107 - HTTP Server Type and Version	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
19506 - Nessus Scan Information	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
11936 - OS Identification	[-/+]
10287 - Traceroute Information	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
110723 - No Credentials Provided	[-/+]
54615 - Device Type	[-/+]

10.2.1.41

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS: [0: CISCO IOS][1: Cisco IOS XE]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	10	10

Results Details

/

11936 - OS Identification [-/+]

22964 - Service Detection [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

11219 - Nessus SYN scanner [-/+]

10107 - HTTP Server Type and Version [-/+]

54615 - Device Type [-/+]

19689 - Embedded Web Server Detection [-/+]

19506 - Nessus Scan Information [-/+]

10287 - Traceroute Information [-/+]

10.2.1.42

Scan Information

Start time: 2020/04/13 17:03

End time: 2020/04/13 21:09

Host Information

OS: [0: Linux Kernel 2.6]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

11219 - Nessus SYN scanner [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

10107 - HTTP Server Type and Version [-/+]

22964 - Service Detection [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10267 - SSH Server Type and Version Information [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

10287 - Traceroute Information [-/+]

11936 - OS Identification [-/+]

19506 - Nessus Scan Information [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

54615 - Device Type [-/+]

110723 - No Credentials Provided [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

10.2.1.43

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

11219 - Nessus SYN scanner [-/+]

22964 - Service Detection [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

10107 - HTTP Server Type and Version [-/+]

10287 - Traceroute Information [-/+]

19506 - Nessus Scan Information [-/+]

11936 - OS Identification [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

110723 - No Credentials Provided [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10267 - SSH Server Type and Version Information [-/+]

54615 - Device Type [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

10.2.1.44

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: Linux Kernel 2.6]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	17	18

Results Details

/

11219 - Nessus SYN scanner [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

22964 - Service Detection [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

10107 - HTTP Server Type and Version [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

117530 - Errors in nessusd.dump [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

11936 - OS Identification [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

19506 - Nessus Scan Information [-/+]

10267 - SSH Server Type and Version Information [-/+]

54615 - Device Type [-/+]

110723 - No Credentials Provided [-/+]

10287 - Traceroute Information [-/+]

10.2.1.45

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

11219 - Nessus SYN scanner	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
106628 - lighttpd HTTP Server Detection	[-/+]
10107 - HTTP Server Type and Version	[-/+]
22964 - Service Detection	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
54615 - Device Type	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
11936 - OS Identification	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
110723 - No Credentials Provided	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
19506 - Nessus Scan Information	[-/+]
10287 - Traceroute Information	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]

10.2.1.51

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: CISCO IOS][1: Cisco IOS XE]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	10	4	21	35

Results Details

/

71049 - SSH Weak MAC Algorithms Enabled	[-/+]
19689 - Embedded Web Server Detection	[-/+]
54615 - Device Type	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
22964 - Service Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
26928 - SSL Weak Cipher Suites Supported	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
10881 - SSH Protocol Versions Supported	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
110723 - No Credentials Provided	[-/+]
11219 - Nessus SYN scanner	[-/+]
10287 - Traceroute Information	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
15901 - SSL Certificate Expiry	[-/+]
10107 - HTTP Server Type and Version	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
10267 - SSH Server Type and Version Information	[-/+]

56984 - SSL / TLS Versions Supported [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

66848 - SSL Null Cipher Suites Supported [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

19506 - Nessus Scan Information [-/+]

11936 - OS Identification [-/+]

10863 - SSL Certificate Information [-/+]

10.2.1.53

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	17	18

Results Details

/

11219 - Nessus SYN scanner [-/+]

22964 - Service Detection [-/+]

10107 - HTTP Server Type and Version [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

10287 - Traceroute Information [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

11936 - OS Identification [-/+]

110723 - No Credentials Provided [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

10267 - SSH Server Type and Version Information [-/+]

19506 - Nessus Scan Information [-/+]

117530 - Errors in nessusd.dump [-/+]

54615 - Device Type [-/+]

10.2.1.54

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

22964 - Service Detection [-/+]

10267 - SSH Server Type and Version Information [-/+]

11219 - Nessus SYN scanner [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

10107 - HTTP Server Type and Version [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

54615 - Device Type [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

11936 - OS Identification [-/+]

19506 - Nessus Scan Information [-/+]

110723 - No Credentials Provided [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

10287 - Traceroute Information [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10.2.1.55

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 21:09

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

106628 - lighttpd HTTP Server Detection [-/+]

10287 - Traceroute Information [-/+]

11219 - Nessus SYN scanner [-/+]

10107 - HTTP Server Type and Version [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

22964 - Service Detection [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

19506 - Nessus Scan Information [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

110723 - No Credentials Provided [-/+]

10267 - SSH Server Type and Version Information [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

11936 - OS Identification [-/+]

54615 - Device Type [-/+]

10.2.1.61

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	14	17

Results Details

/

97861 - Network Time Protocol (NTP) Mode 6 Scanner [-/+]

10267 - SSH Server Type and Version Information [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

19506 - Nessus Scan Information [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

54615 - Device Type [-/+]

71049 - SSH Weak MAC Algorithms Enabled [-/+]

10881 - SSH Protocol Versions Supported [-/+]

10287 - Traceroute Information [-/+]

10884 - Network Time Protocol (NTP) Server Detection [-/+]

11936 - OS Identification [-/+]

110723 - No Credentials Provided [-/+]

11219 - Nessus SYN scanner [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

22964 - Service Detection [-/+]

10.2.1.62

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: Linux Kernel 2.6]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	17	18

Results Details

/

10267 - SSH Server Type and Version Information [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

22964 - Service Detection [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

10107 - HTTP Server Type and Version [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

11219 - Nessus SYN scanner [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

19506 - Nessus Scan Information [-/+]

11936 - OS Identification [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

10287 - Traceroute Information [-/+]

54615 - Device Type [-/+]

117530 - Errors in nessusd.dump [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

110723 - No Credentials Provided [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10.2.1.63

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

11219 - Nessus SYN scanner [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

110723 - No Credentials Provided [-/+]

10107 - HTTP Server Type and Version [-/+]

22964 - Service Detection [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

54615 - Device Type [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10267 - SSH Server Type and Version Information [-/+]

11936 - OS Identification [-/+]

19506 - Nessus Scan Information [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10287 - Traceroute Information [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

10.2.1.64

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

10107 - HTTP Server Type and Version [-/+]

22964 - Service Detection [-/+]

19506 - Nessus Scan Information [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

11219 - Nessus SYN scanner [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

11936 - OS Identification [-/+]

110723 - No Credentials Provided [-/+]

54615 - Device Type [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10287 - Traceroute Information [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10267 - SSH Server Type and Version Information [-/+]

10.2.1.65

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: Linux Kernel 2.6]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

11219 - Nessus SYN scanner [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

22964 - Service Detection [-/+]

10107 - HTTP Server Type and Version [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

10267 - SSH Server Type and Version Information [-/+]

11936 - OS Identification [-/+]

110723 - No Credentials Provided [-/+]

19506 - Nessus Scan Information [-/+]

10287 - Traceroute Information [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

54615 - Device Type [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10.2.1.69

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	16	19

Results Details

/

117886 - Local Checks Not Enabled (info) [-/+]

10267 - SSH Server Type and Version Information [-/+]

10881 - SSH Protocol Versions Supported [-/+]

22964 - Service Detection [-/+]

19689 - Embedded Web Server Detection [-/+]

10287 - Traceroute Information [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

11219 - Nessus SYN scanner [-/+]

110723 - No Credentials Provided [-/+]

10107 - HTTP Server Type and Version [-/+]

10281 - Telnet Server Detection [-/+]

19506 - Nessus Scan Information [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

11936 - OS Identification [-/+]

71049 - SSH Weak MAC Algorithms Enabled [-/+]

42263 - Unencrypted Telnet Server [-/+]

54615 - Device Type [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

10.2.1.71

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: CISCO IOS][1: Cisco IOS XE]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	5	2	16	23

Results Details

/

19506 - Nessus Scan Information	[-/+]
11219 - Nessus SYN scanner	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
11936 - OS Identification	[-/+]
60108 - SSL Certificate Chain Contains Weak RSA Keys	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
10287 - Traceroute Information	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
54615 - Device Type	[-/+]
19689 - Embedded Web Server Detection	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
10107 - HTTP Server Type and Version	[-/+]
22964 - Service Detection	[-/+]
10863 - SSL Certificate Information	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
10884 - Network Time Protocol (NTP) Server Detection	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]

10.2.1.72

Scan Information

Start time: 2020/04/13 17:03

End time: 2020/04/13 19:58

Host Information

OS: [0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

- 24260 - HyperText Transfer Protocol (HTTP) Information [-/+]
- 10107 - HTTP Server Type and Version [-/+]
- 110723 - No Credentials Provided [-/+]
- 22964 - Service Detection [-/+]
- 106628 - lighttpd HTTP Server Detection [-/+]
- 11219 - Nessus SYN scanner [-/+]
- 10267 - SSH Server Type and Version Information [-/+]
- 70657 - SSH Algorithms and Languages Supported [-/+]
- 45590 - Common Platform Enumeration (CPE) [-/+]
- 117886 - Local Checks Not Enabled (info) [-/+]
- 11154 - Unknown Service Detection: Banner Retrieval [-/+]
- 25220 - TCP/IP Timestamps Supported [-/+]
- 10287 - Traceroute Information [-/+]
- 19506 - Nessus Scan Information [-/+]
- 11936 - OS Identification [-/+]
- 70658 - SSH Server CBC Mode Ciphers Enabled [-/+]
- 54615 - Device Type [-/+]

10.2.1.73

Scan Information

Start time: 2020/04/13 17:03

End time: 2020/04/13 19:58

Host Information

OS: [0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

10107 - HTTP Server Type and Version [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

11219 - Nessus SYN scanner [-/+]

22964 - Service Detection [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

110723 - No Credentials Provided [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

10287 - Traceroute Information [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

19506 - Nessus Scan Information [-/+]

10267 - SSH Server Type and Version Information [-/+]

54615 - Device Type [-/+]

11936 - OS Identification [-/+]

10.2.1.74

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

- 10107 - HTTP Server Type and Version [-/+]
- 106628 - lighttpd HTTP Server Detection [-/+]
- 25220 - TCP/IP Timestamps Supported [-/+]
- 11219 - Nessus SYN scanner [-/+]
- 22964 - Service Detection [-/+]
- 24260 - HyperText Transfer Protocol (HTTP) Information [-/+]
- 117886 - Local Checks Not Enabled (info) [-/+]
- 10287 - Traceroute Information [-/+]
- 19506 - Nessus Scan Information [-/+]
- 11154 - Unknown Service Detection: Banner Retrieval [-/+]
- 11936 - OS Identification [-/+]
- 10267 - SSH Server Type and Version Information [-/+]
- 54615 - Device Type [-/+]
- 45590 - Common Platform Enumeration (CPE) [-/+]
- 70657 - SSH Algorithms and Languages Supported [-/+]
- 110723 - No Credentials Provided [-/+]
- 70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

10.2.1.75

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
11219 - Nessus SYN scanner	[-/+]
22964 - Service Detection	[-/+]
106628 - lighttpd HTTP Server Detection	[-/+]
54615 - Device Type	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
10107 - HTTP Server Type and Version	[-/+]
19506 - Nessus Scan Information	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
110723 - No Credentials Provided	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10287 - Traceroute Information	[-/+]
11936 - OS Identification	[-/+]

10.2.1.81

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	14	17

Results Details

/

- 11936 - OS Identification [-/+]
- 10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]
- 10287 - Traceroute Information [-/+]
- 10884 - Network Time Protocol (NTP) Server Detection [-/+]
- 97861 - Network Time Protocol (NTP) Mode 6 Scanner [-/+]
- 10267 - SSH Server Type and Version Information [-/+]
- 110723 - No Credentials Provided [-/+]
- 10881 - SSH Protocol Versions Supported [-/+]
- 70657 - SSH Algorithms and Languages Supported [-/+]
- 117886 - Local Checks Not Enabled (info) [-/+]
- 45590 - Common Platform Enumeration (CPE) [-/+]
- 11219 - Nessus SYN scanner [-/+]
- 54615 - Device Type [-/+]
- 19506 - Nessus Scan Information [-/+]
- 70658 - SSH Server CBC Mode Ciphers Enabled [-/+]
- 22964 - Service Detection [-/+]
- 71049 - SSH Weak MAC Algorithms Enabled [-/+]

10.2.1.82

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	17	18

Results Details

/

106628 - lighttpd HTTP Server Detection [-/+]

11219 - Nessus SYN scanner [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

10107 - HTTP Server Type and Version [-/+]

22964 - Service Detection [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

54615 - Device Type [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

110723 - No Credentials Provided [-/+]

19506 - Nessus Scan Information [-/+]

10267 - SSH Server Type and Version Information [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

117530 - Errors in nessusd.dump [-/+]

11936 - OS Identification [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10287 - Traceroute Information [-/+]

10.2.1.83

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

11219 - Nessus SYN scanner [-/+]

22964 - Service Detection [-/+]

10107 - HTTP Server Type and Version [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

10267 - SSH Server Type and Version Information [-/+]

10287 - Traceroute Information [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

11936 - OS Identification [-/+]

54615 - Device Type [-/+]

110723 - No Credentials Provided [-/+]

19506 - Nessus Scan Information [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

10.2.1.84

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: Linux Kernel 2.6]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

10107 - HTTP Server Type and Version [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

22964 - Service Detection [-/+]

54615 - Device Type [-/+]

11219 - Nessus SYN scanner [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

110723 - No Credentials Provided [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

10287 - Traceroute Information [-/+]

11936 - OS Identification [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

19506 - Nessus Scan Information [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10267 - SSH Server Type and Version Information [-/+]

10.2.1.85

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 19:58

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

106628 - lighttpd HTTP Server Detection [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

10107 - HTTP Server Type and Version [-/+]

11219 - Nessus SYN scanner [-/+]

22964 - Service Detection [-/+]

10287 - Traceroute Information [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

110723 - No Credentials Provided [-/+]

10267 - SSH Server Type and Version Information [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

19506 - Nessus Scan Information [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

54615 - Device Type [-/+]

11936 - OS Identification [-/+]

10.2.1.91

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 18:47

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	10	4	20	34

Results Details

/

83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam) [-/+]

10267 - SSH Server Type and Version Information [-/+]

10107 - HTTP Server Type and Version [-/+]

60108 - SSL Certificate Chain Contains Weak RSA Keys [-/+]

19506 - Nessus Scan Information [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

110723 - No Credentials Provided [-/+]

11936 - OS Identification [-/+]

19689 - Embedded Web Server Detection [-/+]

22964 - Service Detection [-/+]

21643 - SSL Cipher Suites Supported [-/+]

11219 - Nessus SYN scanner [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
10881 - SSH Protocol Versions Supported	[-/+]
54615 - Device Type	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
71049 - SSH Weak MAC Algorithms Enabled	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
66848 - SSL Null Cipher Suites Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
10287 - Traceroute Information	[-/+]
26928 - SSL Weak Cipher Suites Supported	[-/+]
10863 - SSL Certificate Information	[-/+]

10.2.1.92

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 18:47

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

22964 - Service Detection	[-/+]
106628 - lighttpd HTTP Server Detection	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
11219 - Nessus SYN scanner	[-/+]
10107 - HTTP Server Type and Version	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
54615 - Device Type	[-/+]
10287 - Traceroute Information	[-/+]
11936 - OS Identification	[-/+]
19506 - Nessus Scan Information	[-/+]
110723 - No Credentials Provided	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]

10.2.1.93

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 18:47

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3:

Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

106628 - lighttpd HTTP Server Detection	[-/+]
22964 - Service Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10107 - HTTP Server Type and Version	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
110723 - No Credentials Provided	[-/+]
11936 - OS Identification	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
10287 - Traceroute Information	[-/+]
54615 - Device Type	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
19506 - Nessus Scan Information	[-/+]

10.2.1.94

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 18:47

Host Information

OS: [0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	17	18

Results Details

/

22964 - Service Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
106628 - lighttpd HTTP Server Detection	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
10107 - HTTP Server Type and Version	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
11936 - OS Identification	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
54615 - Device Type	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
110723 - No Credentials Provided	[-/+]
19506 - Nessus Scan Information	[-/+]
10287 - Traceroute Information	[-/+]
117530 - Errors in nessusd.dump	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]

10.2.1.95

Scan Information

Start time: 2020/04/13 17:03

End time: 2020/04/13 18:47

Host Information

OS: [0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	17	18

Results Details

/

- 22964 - Service Detection [-/+]
- 24260 - HyperText Transfer Protocol (HTTP) Information [-/+]
- 11154 - Unknown Service Detection: Banner Retrieval [-/+]
- 106628 - lighttpd HTTP Server Detection [-/+]
- 11219 - Nessus SYN scanner [-/+]
- 10107 - HTTP Server Type and Version [-/+]
- 11936 - OS Identification [-/+]
- 54615 - Device Type [-/+]
- 70658 - SSH Server CBC Mode Ciphers Enabled [-/+]
- 117886 - Local Checks Not Enabled (info) [-/+]
- 19506 - Nessus Scan Information [-/+]
- 110723 - No Credentials Provided [-/+]
- 117530 - Errors in nessusd.dump [-/+]
- 10267 - SSH Server Type and Version Information [-/+]
- 45590 - Common Platform Enumeration (CPE) [-/+]
- 70657 - SSH Algorithms and Languages Supported [-/+]
- 25220 - TCP/IP Timestamps Supported [-/+]
- 10287 - Traceroute Information [-/+]

10.2.1.100

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 18:47

Host Information

OS:	[0: FortiOS on Fortinet FortiGate]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	3	0	24	27

Results Details

/

10267 - SSH Server Type and Version Information	[-/+]
22964 - Service Detection	[-/+]
110723 - No Credentials Provided	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
10881 - SSH Protocol Versions Supported	[-/+]
11219 - Nessus SYN scanner	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
11936 - OS Identification	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
19506 - Nessus Scan Information	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
42822 - Strict Transport Security (STS) Detection	[-/+]
10863 - SSL Certificate Information	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]

10287 - Traceroute Information [-/+]

54615 - Device Type [-/+]

56984 - SSL / TLS Versions Supported [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

21643 - SSL Cipher Suites Supported [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

17367 - Fortinet FortiGate Web Console Management Detection [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

10.2.1.101

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 18:47

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	16	19

Results Details

/

11219 - Nessus SYN scanner [-/+]

22964 - Service Detection [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

54615 - Device Type [-/+]

10267 - SSH Server Type and Version Information [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

11936 - OS Identification [-/+]

42263 - Unencrypted Telnet Server [-/+]

10107 - HTTP Server Type and Version [-/+]

110723 - No Credentials Provided [-/+]

10881 - SSH Protocol Versions Supported [-/+]

19689 - Embedded Web Server Detection [-/+]

19506 - Nessus Scan Information [-/+]

71049 - SSH Weak MAC Algorithms Enabled [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

10287 - Traceroute Information [-/+]

10281 - Telnet Server Detection [-/+]

10.2.1.102

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 18:47

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	16	17

Results Details

/

11219 - Nessus SYN scanner [-/+]

22964 - Service Detection [-/+]

54615 - Device Type [-/+]

10107 - HTTP Server Type and Version [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

10267 - SSH Server Type and Version Information [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

11936 - OS Identification [-/+]

110723 - No Credentials Provided [-/+]

10287 - Traceroute Information [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

19506 - Nessus Scan Information [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10.2.1.103

Scan Information

Start time:	2020/04/13 17:03
End time:	2020/04/13 18:47

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	1	17	18

Results Details

/

22964 - Service Detection [-/+]

106628 - lighttpd HTTP Server Detection [-/+]

10107 - HTTP Server Type and Version [-/+]

11219 - Nessus SYN scanner [-/+]

10287 - Traceroute Information [-/+]

11154 - Unknown Service Detection: Banner Retrieval	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
54615 - Device Type	[-/+]
19506 - Nessus Scan Information	[-/+]
117530 - Errors in nessusd.dump	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
110723 - No Credentials Provided	[-/+]

ANEXO 04

NOTA: Todas las direcciones IP fueron modificadas para conservar la confidencialidad y reserva de la entidad.

Tenable.io Report

Wed, 29 Apr 2020 13:04:35 UTC

Table Of Contents

10.2.60.129

Vulnerabilities By Host

[-] Collapse All

[+] Expand All

10.2.60.1

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:14

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	16	19

Results Details

/

- 19506 - Nessus Scan Information [-/+]
- 97861 - Network Time Protocol (NTP) Mode 6 Scanner [-/+]
- 10107 - HTTP Server Type and Version [-/+]
- 22964 - Service Detection [-/+]
- 70658 - SSH Server CBC Mode Ciphers Enabled [-/+]
- 10881 - SSH Protocol Versions Supported [-/+]
- 117886 - Local Checks Not Enabled (info) [-/+]
- 19689 - Embedded Web Server Detection [-/+]
- 11219 - Nessus SYN scanner [-/+]
- 10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]
- 11936 - OS Identification [-/+]
- 10267 - SSH Server Type and Version Information [-/+]
- 110723 - No Credentials Provided [-/+]

71049 - SSH Weak MAC Algorithms Enabled [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10287 - Traceroute Information [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

54615 - Device Type [-/+]

10884 - Network Time Protocol (NTP) Server Detection [-/+]

10.2.60.5

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:26

Host Information

OS:	[0: VMware ESXi 6.5.0 build-5969303]

Results Summary

Critical	High	Medium	Low	Info	Total
0	3	7	1	27	38

Results Details

/

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

21643 - SSL Cipher Suites Supported [-/+]

11219 - Nessus SYN scanner [-/+]

118885 - ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check) [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

10386 - Web Server No 404 Error Code Check [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

23777 - SLP Server Detection (TCP) [-/+]

50845 - OpenSSL Detection [-/+]

123518 - ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check) [-/+]

117886 - Local Checks Not Enabled (info)	[-/+]
22964 - Service Detection	[-/+]
110723 - No Credentials Provided	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
10881 - SSH Protocol Versions Supported	[-/+]
134878 - VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS (VMSA-2018-0018) (remote check)	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
20301 - VMware ESX/GSX Server detection	[-/+]
10863 - SSL Certificate Information	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
19506 - Nessus Scan Information	[-/+]
111759 - ESXi 5.5 / 6.0 / 6.5 / 6.7 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (remote check)	[-/+]
23778 - SLP Server Detection (UDP)	[-/+]
57396 - VMware vSphere Detect	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
54615 - Device Type	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
10287 - Traceroute Information	[-/+]
105614 - ESXi 6.5 < Build 6765664 Heap Buffer Overflow (VMSA-2017-0021) (remote check)	[-/+]
118466 - ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check)	[-/+]

84502 - HSTS Missing From HTTPS Server [-/+]

105486 - ESXi 5.5 / 6.0 / 6.5 / Multiple Vulnerabilities (VMSA-2017-0021) (VMSA-2018-0002) (Spectre) (remote check) [-/+]

11936 - OS Identification [-/+]

10.2.60.6

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:40

Host Information

OS:	[0: Linux Kernel 4.1 on openSUSE 42.1]

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	4	1	34	40

Results Details

/

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

11219 - Nessus SYN scanner [-/+]

10386 - Web Server No 404 Error Code Check [-/+]

10287 - Traceroute Information [-/+]

62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection [-/+]

22964 - Service Detection [-/+]

10107 - HTTP Server Type and Version [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

10881 - SSH Protocol Versions Supported [-/+]

11935 - IPSEC Internet Key Exchange (IKE) Version 1 Detection [-/+]

39446 - Apache Tomcat Detection	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
110723 - No Credentials Provided	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
10863 - SSL Certificate Information	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
39521 - Backported Security Patch Detection (WWW)	[-/+]
18261 - Apache Banner Linux Distribution Disclosure	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
39520 - Backported Security Patch Detection (SSH)	[-/+]
19506 - Nessus Scan Information	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
51891 - SSL Session Resume Supported	[-/+]
117530 - Errors in nessusd.dump	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
48204 - Apache HTTP Server Version	[-/+]
33850 - Unix Operating System Unsupported Version Detection	[-/+]
17975 - Service Detection (GET request)	[-/+]
54615 - Device Type	[-/+]
11936 - OS Identification	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]

10.2.60.10

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:52

Host Information

OS:	[0: VMware ESXi 6.5.0 build-5969303]

Results Summary

Critical	High	Medium	Low	Info	Total
0	3	7	0	24	34

Results Details

/

105486 - ESXi 5.5 / 6.0 / 6.5 / Multiple Vulnerabilities (VMSA-2017-0021) (VMSA-2018-0002) (Spectre) (remote check)	[-/+]
10863 - SSL Certificate Information	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
11936 - OS Identification	[-/+]
11219 - Nessus SYN scanner	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
10287 - Traceroute Information	[-/+]
23777 - SLP Server Detection (TCP)	[-/+]
134878 - VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS (VMSA-2018-0018) (remote check)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
57396 - VMware vSphere Detect	[-/+]
20301 - VMware ESX/GSX Server detection	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]

22964 - Service Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
118885 - ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check)	[-/+]
111759 - ESXi 5.5 / 6.0 / 6.5 / 6.7 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (remote check)	[-/+]
50845 - OpenSSL Detection	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
54615 - Device Type	[-/+]
118466 - ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check)	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
19506 - Nessus Scan Information	[-/+]
23778 - SLP Server Detection (UDP)	[-/+]
110723 - No Credentials Provided	[-/+]
10386 - Web Server No 404 Error Code Check	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
105614 - ESXi 6.5 < Build 6765664 Heap Buffer Overflow (VMSA-2017-0021) (remote check)	[-/+]
123518 - ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check)	[-/+]

10.2.60.14

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 13:16

Host Information

OS:	[0: Linux Kernel 4.1 on openSUSE 42.1]

Results Summary

Critical	High	Medium	Low	Info	Total

1	0	4	0	28	33

Results Details

/

51891 - SSL Session Resume Supported	[-/+]
11219 - Nessus SYN scanner	[-/+]
10386 - Web Server No 404 Error Code Check	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
39521 - Backported Security Patch Detection (WWW)	[-/+]
10863 - SSL Certificate Information	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
10287 - Traceroute Information	[-/+]
48204 - Apache HTTP Server Version	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
33850 - Unix Operating System Unsupported Version Detection	[-/+]
22964 - Service Detection	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
11935 - IPSEC Internet Key Exchange (IKE) Version 1 Detection	[-/+]
11936 - OS Identification	[-/+]
117530 - Errors in nessusd.dump	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection	[-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

18261 - Apache Banner Linux Distribution Disclosure [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10107 - HTTP Server Type and Version [-/+]

17975 - Service Detection (GET request) [-/+]

56984 - SSL / TLS Versions Supported [-/+]

54615 - Device Type [-/+]

39446 - Apache Tomcat Detection [-/+]

19506 - Nessus Scan Information [-/+]

10.2.60.33

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:40

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	16	19

Results Details

/

71049 - SSH Weak MAC Algorithms Enabled [-/+]

10267 - SSH Server Type and Version Information [-/+]

10287 - Traceroute Information [-/+]

97861 - Network Time Protocol (NTP) Mode 6 Scanner [-/+]

10107 - HTTP Server Type and Version [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

11219 - Nessus SYN scanner [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10884 - Network Time Protocol (NTP) Server Detection [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

22964 - Service Detection [-/+]

19689 - Embedded Web Server Detection [-/+]

10881 - SSH Protocol Versions Supported [-/+]

54615 - Device Type [-/+]

110723 - No Credentials Provided [-/+]

19506 - Nessus Scan Information [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

11936 - OS Identification [-/+]

10.2.60.34

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 13:28

Host Information

Netbios Name:	XPRESSIONS
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	10	1	37	49

Results Details

/

10287 - Traceroute Information [-/+]

22964 - Service Detection [-/+]

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) [-/+]

11219 - Nessus SYN scanner [-/+]

51192 - SSL Certificate Cannot Be Trusted	[-/+]
10092 - FTP Server Detection	[-/+]
66173 - RDP Screenshot	[-/+]
19506 - Nessus Scan Information	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
10863 - SSL Certificate Information	[-/+]
10107 - HTTP Server Type and Version	[-/+]
10736 - DCE Services Enumeration	[-/+]
10394 - Microsoft Windows SMB Log In Possible	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
19689 - Embedded Web Server Detection	[-/+]
57608 - SMB Signing not required	[-/+]
16321 - 3Com 3CServer/3CDaemon FTP Server Multiple Vulnerabilities (OF, FS, PD, DoS)	[-/+]
100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry	[-/+]
24786 - Nessus Windows Scan Not Performed with Admin Privileges	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]

54615 - Device Type	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]
43815 - NetBIOS Multiple IP Address Enumeration	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
11936 - OS Identification	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
135860 - WMI Not Available	[-/+]
17975 - Service Detection (GET request)	[-/+]
110723 - No Credentials Provided	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
11819 - TFTP Daemon Detection	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]

10.2.60.54

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:40

Host Information

OS: [0: Linux Kernel 4.1 on openSUSE 42.1]

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	6	1	30	38

Results Details

/

19506 - Nessus Scan Information [-/+]

11219 - Nessus SYN scanner [-/+]

10863 - SSL Certificate Information [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

57582 - SSL Self-Signed Certificate [-/+]

48204 - Apache HTTP Server Version [-/+]

22964 - Service Detection [-/+]

54615 - Device Type [-/+]

21642 - Session Initiation Protocol Detection [-/+]

10386 - Web Server No 404 Error Code Check [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

51891 - SSL Session Resume Supported [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

17975 - Service Detection (GET request) [-/+]

56984 - SSL / TLS Versions Supported [-/+]

10287 - Traceroute Information [-/+]

62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

10107 - HTTP Server Type and Version [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
39521 - Backported Security Patch Detection (WWW)	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
15901 - SSL Certificate Expiry	[-/+]
39446 - Apache Tomcat Detection	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
50845 - OpenSSL Detection	[-/+]
117530 - Errors in nessusd.dump	[-/+]
11936 - OS Identification	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
18261 - Apache Banner Linux Distribution Disclosure	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
33850 - Unix Operating System Unsupported Version Detection	[-/+]
11935 - IPSEC Internet Key Exchange (IKE) Version 1 Detection	[-/+]

10.2.60.55

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:14

Host Information

OS:	[0: Linux Kernel 4.1 on openSUSE 42.1]

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	6	1	30	38

Results Details

/

10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
50845 - OpenSSL Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
117530 - Errors in nessusd.dump	[-/+]
10386 - Web Server No 404 Error Code Check	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
22964 - Service Detection	[-/+]
10107 - HTTP Server Type and Version	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
17975 - Service Detection (GET request)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
19506 - Nessus Scan Information	[-/+]
33850 - Unix Operating System Unsupported Version Detection	[-/+]
10863 - SSL Certificate Information	[-/+]
39446 - Apache Tomcat Detection	[-/+]
11936 - OS Identification	[-/+]
10287 - Traceroute Information	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
48204 - Apache HTTP Server Version	[-/+]

57582 - SSL Self-Signed Certificate [-/+]

62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection [-/+]

51891 - SSL Session Resume Supported [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

11935 - IPSEC Internet Key Exchange (IKE) Version 1 Detection [-/+]

21642 - Session Initiation Protocol Detection [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

21643 - SSL Cipher Suites Supported [-/+]

56984 - SSL / TLS Versions Supported [-/+]

18261 - Apache Banner Linux Distribution Disclosure [-/+]

54615 - Device Type [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

39521 - Backported Security Patch Detection (WWW) [-/+]

15901 - SSL Certificate Expiry [-/+]

10.2.60.56

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:40

Host Information

OS:	[0: Linux Kernel 4.1 on openSUSE 42.1]

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	6	1	32	40

Results Details

/

17975 - Service Detection (GET request) [-/+]

94761 - SSL Root Certification Authority Certificate Information [-/+]

11219 - Nessus SYN scanner [-/+]

21643 - SSL Cipher Suites Supported	[-/+]
18261 - Apache Banner Linux Distribution Disclosure	[-/+]
19506 - Nessus Scan Information	[-/+]
10386 - Web Server No 404 Error Code Check	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
11936 - OS Identification	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
15901 - SSL Certificate Expiry	[-/+]
10287 - Traceroute Information	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
48204 - Apache HTTP Server Version	[-/+]
62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
10107 - HTTP Server Type and Version	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
22964 - Service Detection	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
33850 - Unix Operating System Unsupported Version Detection	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
117530 - Errors in nessusd.dump	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
91263 - SSL/TLS Service Requires Client Certificate	[-/+]

51891 - SSL Session Resume Supported [-/+]

21642 - Session Initiation Protocol Detection [-/+]

39446 - Apache Tomcat Detection [-/+]

54615 - Device Type [-/+]

35297 - SSL Service Requests Client Certificate [-/+]

84502 - HSTS Missing From HTTPS Server [-/+]

50845 - OpenSSL Detection [-/+]

10863 - SSL Certificate Information [-/+]

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits [-/+]

39521 - Backported Security Patch Detection (WWW) [-/+]

11935 - IPSEC Internet Key Exchange (IKE) Version 1 Detection [-/+]

10.2.60.57

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 11:56

Host Information

OS:	[0: Linux Kernel 4.1 on openSUSE 42.1]

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	6	1	32	40

Results Details

/

11219 - Nessus SYN scanner [-/+]

22964 - Service Detection [-/+]

10107 - HTTP Server Type and Version [-/+]

21643 - SSL Cipher Suites Supported [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

51891 - SSL Session Resume Supported [-/+]

84502 - HSTS Missing From HTTPS Server	[-/+]
39446 - Apache Tomcat Detection	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
11935 - IPSEC Internet Key Exchange (IKE) Version 1 Detection	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
117530 - Errors in nessusd.dump	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
91263 - SSL/TLS Service Requires Client Certificate	[-/+]
33850 - Unix Operating System Unsupported Version Detection	[-/+]
11936 - OS Identification	[-/+]
62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection	[-/+]
54615 - Device Type	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
10386 - Web Server No 404 Error Code Check	[-/+]
35297 - SSL Service Requests Client Certificate	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
39521 - Backported Security Patch Detection (WWW)	[-/+]
21642 - Session Initiation Protocol Detection	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]

50845 - OpenSSL Detection [-/+]

10287 - Traceroute Information [-/+]

15901 - SSL Certificate Expiry [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

48204 - Apache HTTP Server Version [-/+]

18261 - Apache Banner Linux Distribution Disclosure [-/+]

19506 - Nessus Scan Information [-/+]

17975 - Service Detection (GET request) [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

10.2.60.58

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:26

Host Information

OS:	[0: Linux Kernel 4.1 on openSUSE 42.1]

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	4	0	28	33

Results Details

/

62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

11935 - IPSEC Internet Key Exchange (IKE) Version 1 Detection [-/+]

18261 - Apache Banner Linux Distribution Disclosure [-/+]

11219 - Nessus SYN scanner [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

33850 - Unix Operating System Unsupported Version Detection [-/+]

10386 - Web Server No 404 Error Code Check [-/+]

21643 - SSL Cipher Suites Supported	[-/+]
10287 - Traceroute Information	[-/+]
22964 - Service Detection	[-/+]
48204 - Apache HTTP Server Version	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
11936 - OS Identification	[-/+]
39521 - Backported Security Patch Detection (WWW)	[-/+]
51891 - SSL Session Resume Supported	[-/+]
54615 - Device Type	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
19506 - Nessus Scan Information	[-/+]
10107 - HTTP Server Type and Version	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
39446 - Apache Tomcat Detection	[-/+]
17975 - Service Detection (GET request)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
10863 - SSL Certificate Information	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
117530 - Errors in nessusd.dump	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]

10.2.60.59

Scan Information

Start time: 2020/04/29 11:43

End time: 2020/04/29 12:26

Host Information

OS: [0: Linux Kernel 4.1 on openSUSE 42.1]

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	4	0	28	33

Results Details

/

11219 - Nessus SYN scanner	[-/+]
10386 - Web Server No 404 Error Code Check	[-/+]
11936 - OS Identification	[-/+]
22964 - Service Detection	[-/+]
33850 - Unix Operating System Unsupported Version Detection	[-/+]
11935 - IPSEC Internet Key Exchange (IKE) Version 1 Detection	[-/+]
62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
117530 - Errors in nessusd.dump	[-/+]
39521 - Backported Security Patch Detection (WWW)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
17975 - Service Detection (GET request)	[-/+]
10107 - HTTP Server Type and Version	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]

19506 - Nessus Scan Information [-/+]

21643 - SSL Cipher Suites Supported [-/+]

10287 - Traceroute Information [-/+]

39446 - Apache Tomcat Detection [-/+]

51891 - SSL Session Resume Supported [-/+]

18261 - Apache Banner Linux Distribution Disclosure [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

54615 - Device Type [-/+]

56984 - SSL / TLS Versions Supported [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

10863 - SSL Certificate Information [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

94761 - SSL Root Certification Authority Certificate Information [-/+]

48204 - Apache HTTP Server Version [-/+]

10.2.60.60

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 13:04

Host Information

OS:	[0: Linux Kernel 4.1 on openSUSE 42.1]

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	4	0	29	34

Results Details

/

11219 - Nessus SYN scanner [-/+]

22964 - Service Detection [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
18261 - Apache Banner Linux Distribution Disclosure	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
10107 - HTTP Server Type and Version	[-/+]
11154 - Unknown Service Detection: Banner Retrieval	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
51891 - SSL Session Resume Supported	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
11935 - IPSEC Internet Key Exchange (IKE) Version 1 Detection	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
11936 - OS Identification	[-/+]
39521 - Backported Security Patch Detection (WWW)	[-/+]
10386 - Web Server No 404 Error Code Check	[-/+]
39446 - Apache Tomcat Detection	[-/+]
10287 - Traceroute Information	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
54615 - Device Type	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
17975 - Service Detection (GET request)	[-/+]
48204 - Apache HTTP Server Version	[-/+]
10863 - SSL Certificate Information	[-/+]

62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection [-/+]

19506 - Nessus Scan Information [-/+]

33850 - Unix Operating System Unsupported Version Detection [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

56984 - SSL / TLS Versions Supported [-/+]

117530 - Errors in nessusd.dump [-/+]

10.2.60.61

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:52

Host Information

OS:	[0: Linux Kernel 4.1 on openSUSE 42.1]

Results Summary

Critical	High	Medium	Low	Info	Total
1	0	4	0	29	34

Results Details

/

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

56984 - SSL / TLS Versions Supported [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

19506 - Nessus Scan Information [-/+]

62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection [-/+]

11936 - OS Identification [-/+]

51891 - SSL Session Resume Supported [-/+]

11219 - Nessus SYN scanner [-/+]

10107 - HTTP Server Type and Version [-/+]

117530 - Errors in nessusd.dump [-/+]

21643 - SSL Cipher Suites Supported [-/+]

22964 - Service Detection [-/+]

11935 - IPSEC Internet Key Exchange (IKE) Version 1 Detection [-/+]

17975 - Service Detection (GET request) [-/+]

33850 - Unix Operating System Unsupported Version Detection [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

10287 - Traceroute Information [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

18261 - Apache Banner Linux Distribution Disclosure [-/+]

39446 - Apache Tomcat Detection [-/+]

84502 - HSTS Missing From HTTPS Server [-/+]

10386 - Web Server No 404 Error Code Check [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

39521 - Backported Security Patch Detection (WWW) [-/+]

54615 - Device Type [-/+]

10863 - SSL Certificate Information [-/+]

57582 - SSL Self-Signed Certificate [-/+]

94761 - SSL Root Certification Authority Certificate Information [-/+]

11154 - Unknown Service Detection: Banner Retrieval [-/+]

48204 - Apache HTTP Server Version [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

10.2.60.65

Scan Information

Start time: 2020/04/29 11:43

End time: 2020/04/29 12:01

Host Information

OS: [0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	16	19

Results Details

/

45590 - Common Platform Enumeration (CPE) [-/+]

22964 - Service Detection [-/+]

10107 - HTTP Server Type and Version [-/+]

11219 - Nessus SYN scanner [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10287 - Traceroute Information [-/+]

19506 - Nessus Scan Information [-/+]

54615 - Device Type [-/+]

97861 - Network Time Protocol (NTP) Mode 6 Scanner [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

10884 - Network Time Protocol (NTP) Server Detection [-/+]

10881 - SSH Protocol Versions Supported [-/+]

11936 - OS Identification [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

110723 - No Credentials Provided [-/+]

10267 - SSH Server Type and Version Information [-/+]

19689 - Embedded Web Server Detection [-/+]

71049 - SSH Weak MAC Algorithms Enabled [-/+]

10.2.60.67

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:52

Host Information

Netbios Name:	WIN-RB7INVLKNMF
OS:	[0: Microsoft Windows Server 2012 R2 Standard]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	13	2	37	53

Results Details

/

56984 - SSL / TLS Versions Supported	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
11219 - Nessus SYN scanner	[-/+]
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	[-/+]
10736 - DCE Services Enumeration	[-/+]
22964 - Service Detection	[-/+]
10863 - SSL Certificate Information	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
11936 - OS Identification	[-/+]
57582 - SSL Self-Signed Certificate	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
11422 - Web Server Unconfigured - Default Install Page Present	[-/+]
108761 - MSSQL Host Information in NTLM SSP	[-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check)	[-/+]
57608 - SMB Signing not required	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	[-/+]
54615 - Device Type	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
19506 - Nessus Scan Information	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
66173 - RDP Screenshot	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	[-/+]
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	[-/+]
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only	[-/+]
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
10674 - Microsoft SQL Server UDP Query Remote Version Disclosure	[-/+]
57690 - Terminal Services Encryption Level is Medium or Low	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]

110723 - No Credentials Provided	[-/+]
10287 - Traceroute Information	[-/+]
69482 - Microsoft SQL Server STARTTLS Support	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
10107 - HTTP Server Type and Version	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
135860 - WMI Not Available	[-/+]
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
10144 - Microsoft SQL Server TCP/IP Listener Detection	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	[-/+]

10.2.60.97

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:40

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	14	17

Results Details

/

110723 - No Credentials Provided	[-/+]
11219 - Nessus SYN scanner	[-/+]
71049 - SSH Weak MAC Algorithms Enabled	[-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10881 - SSH Protocol Versions Supported [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10884 - Network Time Protocol (NTP) Server Detection [-/+]

97861 - Network Time Protocol (NTP) Mode 6 Scanner [-/+]

11936 - OS Identification [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

22964 - Service Detection [-/+]

54615 - Device Type [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

10287 - Traceroute Information [-/+]

19506 - Nessus Scan Information [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

10267 - SSH Server Type and Version Information [-/+]

10.2.60.100

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 13:28

Host Information

OS:	[0: VMware ESXi 6.5.0 build-8294253]

Results Summary

Critical	High	Medium	Low	Info	Total
0	3	5	0	23	31

Results Details

/

21643 - SSL Cipher Suites Supported [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

10863 - SSL Certificate Information [-/+]

11219 - Nessus SYN scanner	[-/+]
19506 - Nessus Scan Information	[-/+]
118885 - ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check)	[-/+]
50845 - OpenSSL Detection	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
111759 - ESXi 5.5 / 6.0 / 6.5 / 6.7 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (remote check)	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
20301 - VMware ESX/GSX Server detection	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
23778 - SLP Server Detection (UDP)	[-/+]
10287 - Traceroute Information	[-/+]
11936 - OS Identification	[-/+]
54615 - Device Type	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
22964 - Service Detection	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
57396 - VMware vSphere Detect	[-/+]
10386 - Web Server No 404 Error Code Check	[-/+]
118466 - ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
123518 - ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-	[-/+]

0005) (Remote Check)

110723 - No Credentials Provided [-/+]

23777 - SLP Server Detection (TCP) [-/+]

134878 - VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS (VMSA-2018-0018) (remote check) [-/+]

10.2.60.101

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:40

Host Information

OS:	[0: Linux Kernel 2.2][1: Linux Kernel 2.4][2: Linux Kernel 2.6]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	5	1	27	33

Results Details

/

57582 - SSL Self-Signed Certificate [-/+]

11219 - Nessus SYN scanner [-/+]

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits [-/+]

10881 - SSH Protocol Versions Supported [-/+]

35291 - SSL Certificate Signed Using Weak Hashing Algorithm [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

94761 - SSL Root Certification Authority Certificate Information [-/+]

10863 - SSL Certificate Information [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

10884 - Network Time Protocol (NTP) Server Detection [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

22964 - Service Detection [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
10107 - HTTP Server Type and Version	[-/+]
10287 - Traceroute Information	[-/+]
54615 - Device Type	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
10267 - SSH Server Type and Version Information	[-/+]
110723 - No Credentials Provided	[-/+]
19506 - Nessus Scan Information	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
50845 - OpenSSL Detection	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
39520 - Backported Security Patch Detection (SSH)	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
11936 - OS Identification	[-/+]
117530 - Errors in nessusd.dump	[-/+]
48204 - Apache HTTP Server Version	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]

10.2.60.102

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 12:14

Host Information

OS:	[0: Linux Kernel 3.13][1: Linux Kernel 3.10][2: Linux Kernel 4.2][3: Linux Kernel 4.8]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	6	1	27	34

Results Details

/

51192 - SSL Certificate Cannot Be Trusted	[-/+]
21642 - Session Initiation Protocol Detection	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
117530 - Errors in nessusd.dump	[-/+]
11219 - Nessus SYN scanner	[-/+]
10107 - HTTP Server Type and Version	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
19506 - Nessus Scan Information	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
22964 - Service Detection	[-/+]
94761 - SSL Root Certification Authority Certificate Information	[-/+]
39520 - Backported Security Patch Detection (SSH)	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
10287 - Traceroute Information	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
110723 - No Credentials Provided	[-/+]

10267 - SSH Server Type and Version Information [-/+]

11936 - OS Identification [-/+]

57582 - SSL Self-Signed Certificate [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

35291 - SSL Certificate Signed Using Weak Hashing Algorithm [-/+]

10881 - SSH Protocol Versions Supported [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

50845 - OpenSSL Detection [-/+]

15901 - SSL Certificate Expiry [-/+]

10863 - SSL Certificate Information [-/+]

54615 - Device Type [-/+]

48204 - Apache HTTP Server Version [-/+]

10.2.60.129

Scan Information

Start time:	2020/04/29 11:43
End time:	2020/04/29 13:28

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	16	19

Results Details

/

22964 - Service Detection [-/+]

10267 - SSH Server Type and Version Information [-/+]

71049 - SSH Weak MAC Algorithms Enabled [-/+]

10884 - Network Time Protocol (NTP) Server Detection [-/+]

19689 - Embedded Web Server Detection [-/+]

110723 - No Credentials Provided	[-/+]
10881 - SSH Protocol Versions Supported	[-/+]
10107 - HTTP Server Type and Version	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
19506 - Nessus Scan Information	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
54615 - Device Type	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
11219 - Nessus SYN scanner	[-/+]
97861 - Network Time Protocol (NTP) Mode 6 Scanner	[-/+]
70657 - SSH Algorithms and Languages Supported	[-/+]
10287 - Traceroute Information	[-/+]
11936 - OS Identification	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]

This is a report from Tenable.io.
Tenable.io is published by Tenable, Inc
7021 Columbia Gateway Drive Suite 500, Columbia, MD 21046
© 2020 Tenable, Inc. All rights reserved.

ANEXO 05

NOTA: Todas las direcciones IP fueron modificadas para conservar la confidencialidad y reserva de la entidad.

Tenable.io Report

Tue, 28 Apr 2020 17:35:01 UTC

Table Of Contents

10.2.5.48

10.2.5.49

10.2.5.50

10.2.5.51

10.2.5.52

10.2.5.53

10.2.5.54

10.2.5.55

10.2.5.56

10.2.5.58

10.2.5.60

10.2.5.61

10.2.5.63

10.2.5.64

10.2.5.69

10.2.5.70

10.2.5.71

10.2.5.74

10.2.5.75

10.2.5.76

10.2.5.80

10.2.5.83

10.2.5.85

Vulnerabilities By Host

[-] Collapse All

[+] Expand All

10.2.4.180

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:50

Results Summary

Critical	High	Medium	Low	Info	Total

0	0	0	0	3	3

Results Details

/

14274 - Nessus SNMP Scanner [-/+]

11933 - Do not scan printers [-/+]

19506 - Nessus Scan Information [-/+]

10.2.4.200

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 18:08

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	16	19

Results Details

/

19506 - Nessus Scan Information [-/+]

11219 - Nessus SYN scanner [-/+]

10881 - SSH Protocol Versions Supported [-/+]

22964 - Service Detection [-/+]

110723 - No Credentials Provided [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

19689 - Embedded Web Server Detection [-/+]

54615 - Device Type [-/+]

70658 - SSH Server CBC Mode Ciphers Enabled [-/+]

10287 - Traceroute Information [-/+]

97861 - Network Time Protocol (NTP) Mode 6 Scanner [-/+]

10107 - HTTP Server Type and Version [-/+]

10267 - SSH Server Type and Version Information [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

71049 - SSH Weak MAC Algorithms Enabled [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

10884 - Network Time Protocol (NTP) Server Detection [-/+]

11936 - OS Identification [-/+]

10.2.5.11

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 18:10

Host Information

DNS Name:	npi4flmpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	3	3

Results Details

/

14274 - Nessus SNMP Scanner [-/+]

11933 - Do not scan printers [-/+]

19506 - Nessus Scan Information [-/+]

10.2.5.17

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 18:00

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	5	5

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]

10.2.5.20

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:50

Host Information

DNS Name:	npic8Impresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11933 - Do not scan printers	[-/+]
11219 - Nessus SYN scanner	[-/+]
19506 - Nessus Scan Information	[-/+]

10.2.5.22

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:58

Host Information

DNS Name:	mps5501b-feImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total

0	0	0	0	6	6

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
19506 - Nessus Scan Information	[-/+]
11933 - Do not scan printers	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
135860 - WMI Not Available	[-/+]

10.2.5.23

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:43

Host Information

DNS Name:	npib4Impresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11219 - Nessus SYN scanner	[-/+]
19506 - Nessus Scan Information	[-/+]
11933 - Do not scan printers	[-/+]

10.2.5.25

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 18:10

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	3	3

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
19506 - Nessus Scan Information	[-/+]
11933 - Do not scan printers	[-/+]

10.2.5.26

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:50

Host Information

DNS Name:	npi5dImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11219 - Nessus SYN scanner	[-/+]
11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]

10.2.5.28

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 18:10

Host Information

DNS Name:	mps5501b-feImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total

0	0	0	0	7	7

Results Details

/

11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]
11219 - Nessus SYN scanner	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
135860 - WMI Not Available	[-/+]
10287 - Traceroute Information	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]

10.2.5.30

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:57

Host Information

DNS Name:	npi27Impresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	3	3

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
19506 - Nessus Scan Information	[-/+]
11933 - Do not scan printers	[-/+]

10.2.5.33

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:50

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	5	5

Results Details

/

11011 - Microsoft Windows SMB Service Detection	[-/+]
14274 - Nessus SNMP Scanner	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
19506 - Nessus Scan Information	[-/+]
11933 - Do not scan printers	[-/+]

10.2.5.34

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:54

Host Information

DNS Name:	hp90Impresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	3	3

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
19506 - Nessus Scan Information	[-/+]
11933 - Do not scan printers	[-/+]

10.2.5.38

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:54

Host Information

DNS Name:	piso9-bImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner	[-/+]
19506 - Nessus Scan Information	[-/+]
11933 - Do not scan printers	[-/+]
10287 - Traceroute Information	[-/+]

10.2.5.39

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 18:12

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner	[-/+]
10287 - Traceroute Information	[-/+]
19506 - Nessus Scan Information	[-/+]
11933 - Do not scan printers	[-/+]

10.2.5.40

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:41

Host Information

DNS Name:	piso17-bImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner	[-/+]
19506 - Nessus Scan Information	[-/+]
10287 - Traceroute Information	[-/+]
11933 - Do not scan printers	[-/+]

10.2.5.41

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 18:12

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	3	3

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]

10.2.5.42

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:43

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner	[-/+]
10287 - Traceroute Information	[-/+]
11933 - Do not scan printers	[-/+]

19506 - Nessus Scan Information [-/+]

10.2.5.43

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 18:00

Host Information

DNS Name: piso10-bImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner [-/+]

11933 - Do not scan printers [-/+]

19506 - Nessus Scan Information [-/+]

10287 - Traceroute Information [-/+]

10.2.5.46

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 17:56

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner [-/+]

19506 - Nessus Scan Information [-/+]

10287 - Traceroute Information [-/+]

11933 - Do not scan printers [-/+]

10.2.5.47

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:38

Host Information

DNS Name:	piso5-bImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner	[-/+]
10287 - Traceroute Information	[-/+]
11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]

10.2.5.48

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 18:00

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11219 - Nessus SYN scanner	[-/+]
11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]

10.2.5.49

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 17:52

Host Information

DNS Name: piso17-bImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

10287 - Traceroute Information [-/+]

11933 - Do not scan printers [-/+]

11219 - Nessus SYN scanner [-/+]

19506 - Nessus Scan Information [-/+]

10.2.5.50

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 17:38

Host Information

DNS Name: piso13-bImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

10287 - Traceroute Information [-/+]

11219 - Nessus SYN scanner [-/+]

19506 - Nessus Scan Information [-/+]

11933 - Do not scan printers [-/+]

10.2.5.51

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 17:35

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

19506 - Nessus Scan Information [-/+]

11219 - Nessus SYN scanner [-/+]

10287 - Traceroute Information [-/+]

11933 - Do not scan printers [-/+]

10.2.5.52

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 17:38

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner [-/+]

10287 - Traceroute Information [-/+]

19506 - Nessus Scan Information [-/+]

11933 - Do not scan printers [-/+]

10.2.5.53

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 17:41

Results Summary

Critical	High	Medium	Low	Info	Total

0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner	[-/+]
11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]
10287 - Traceroute Information	[-/+]

10.2.5.54

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:38

Host Information

DNS Name:	piso6-bImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner	[-/+]
10287 - Traceroute Information	[-/+]
19506 - Nessus Scan Information	[-/+]
11933 - Do not scan printers	[-/+]

10.2.5.55

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:57

Host Information

DNS Name:	npib4Impresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total

0	0	0	0	4	4

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11219 - Nessus SYN scanner	[-/+]
11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]

10.2.5.56

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 18:02

Host Information

DNS Name:	npib4Impresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11219 - Nessus SYN scanner	[-/+]
19506 - Nessus Scan Information	[-/+]
11933 - Do not scan printers	[-/+]

10.2.5.58

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:50

Host Information

DNS Name:	chgpc299Impresora.Entidad.col
Netbios Name:	CHGPC29961EQ
OS:	[0: Microsoft Windows 8][1: Microsoft Windows 7][2: Microsoft

Windows Server 2008 R2][3: Microsoft Windows Server 2003][4: M...

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	6	0	29	35

Results Details

/

121010 - TLS Version 1.1 Protocol Detection	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
10107 - HTTP Server Type and Version	[-/+]
11219 - Nessus SYN scanner	[-/+]
10287 - Traceroute Information	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
110723 - No Credentials Provided	[-/+]
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure	[-/+]
10736 - DCE Services Enumeration	[-/+]
54615 - Device Type	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]
22964 - Service Detection	[-/+]
17975 - Service Detection (GET request)	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
11936 - OS Identification	[-/+]
117886 - Local Checks Not Enabled (info)	[-/+]
57608 - SMB Signing not required	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
64814 - Terminal Services Use SSL/TLS	[-/+]
10940 - Windows Terminal Services Enabled	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]

19506 - Nessus Scan Information [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

46180 - Additional DNS Hostnames [-/+]

100871 - Microsoft Windows SMB Versions Supported (remote check) [-/+]

56984 - SSL / TLS Versions Supported [-/+]

51192 - SSL Certificate Cannot Be Trusted [-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported [-/+]

106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) [-/+]

57582 - SSL Self-Signed Certificate [-/+]

10863 - SSL Certificate Information [-/+]

135860 - WMI Not Available [-/+]

10.2.5.60

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:50

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

10287 - Traceroute Information [-/+]

11219 - Nessus SYN scanner [-/+]

11933 - Do not scan printers [-/+]

19506 - Nessus Scan Information [-/+]

10.2.5.61

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 18:02

Host Information

DNS Name:	piso2-bImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner	[-/+]
11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]
10287 - Traceroute Information	[-/+]

10.2.5.63

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:43

Host Information

DNS Name:	piso2-bImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	3	3

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]

10.2.5.64

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 17:36

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner [-/+]

11933 - Do not scan printers [-/+]

10287 - Traceroute Information [-/+]

19506 - Nessus Scan Information [-/+]

10.2.5.69

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 17:35

Host Information

DNS Name: npib4Impresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

11219 - Nessus SYN scanner [-/+]

14274 - Nessus SNMP Scanner [-/+]

19506 - Nessus Scan Information [-/+]

11933 - Do not scan printers [-/+]

10.2.5.70

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 17:36

Host Information

DNS Name: npic8Impresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11219 - Nessus SYN scanner	[-/+]
11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]

10.2.5.71

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 18:02

Host Information

DNS Name: npib4Impresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	4	4

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11219 - Nessus SYN scanner	[-/+]
19506 - Nessus Scan Information	[-/+]
11933 - Do not scan printers	[-/+]

10.2.5.74

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 17:35

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	3	3

Results Details

/

14274 - Nessus SNMP Scanner [-/+]

11933 - Do not scan printers [-/+]

19506 - Nessus Scan Information [-/+]

10.2.5.75

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 18:03

Host Information

DNS Name: piso5-clmpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	3	3

Results Details

/

14274 - Nessus SNMP Scanner [-/+]

11933 - Do not scan printers [-/+]

19506 - Nessus Scan Information [-/+]

10.2.5.76

Scan Information

Start time: 2020/04/28 17:32

End time: 2020/04/28 17:52

Host Information

DNS Name: hpcp4520_nnImpresora.Entidad.col

Results Summary

Critical	High	Medium	Low	Info	Total

0	0	0	0	3	3

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]

10.2.5.80

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:43

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	5	5

Results Details

/

14274 - Nessus SNMP Scanner	[-/+]
11933 - Do not scan printers	[-/+]
19506 - Nessus Scan Information	[-/+]
11011 - Microsoft Windows SMB Service Detection	[-/+]
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure	[-/+]

10.2.5.83

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 17:50

Host Information

DNS Name:	sip-Impresora.Entidad.col
OS:	[0: Yealink SIP Device]

Results Summary

Critical	High	Medium	Low	Info	Total

0	1	5	1	23	30

Results Details

/

121010 - TLS Version 1.1 Protocol Detection	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
11219 - Nessus SYN scanner	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
11936 - OS Identification	[-/+]
50845 - OpenSSL Detection	[-/+]
21642 - Session Initiation Protocol Detection	[-/+]
10107 - HTTP Server Type and Version	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
51891 - SSL Session Resume Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
46215 - Inconsistent Hostname and IP Address	[-/+]
22964 - Service Detection	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
54615 - Device Type	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
46180 - Additional DNS Hostnames	[-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]

19506 - Nessus Scan Information [-/+]

56984 - SSL / TLS Versions Supported [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

84502 - HSTS Missing From HTTPS Server [-/+]

20007 - SSL Version 2 and 3 Protocol Detection [-/+]

10287 - Traceroute Information [-/+]

10.2.5.85

Scan Information

Start time:	2020/04/28 17:32
End time:	2020/04/28 18:12

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	5	5

Results Details

/

14274 - Nessus SNMP Scanner [-/+]

19506 - Nessus Scan Information [-/+]

11011 - Microsoft Windows SMB Service Detection [-/+]

10150 - Windows NetBIOS / SMB Remote Host Information Disclosure [-/+]

11933 - Do not scan printers [-/+]

This is a report from Tenable.io.
Tenable.io is published by Tenable, Inc
7021 Columbia Gateway Drive Suite 500, Columbia, MD 21046
© 2020 Tenable, Inc. All rights reserved.

ANEXO 06

NOTA: Todas las direcciones IP fueron modificadas para conservar la confidencialidad y reserva de la entidad.

Tenable.io Report

Wed, 29 Apr 2020 18:06:56 UTC

Table Of Contents

Vulnerabilities By Host

[-] Collapse All

[+] Expand All

10.2.48.7

Scan Information

Start time:	2020/04/29 16:55
End time:	2020/04/30 00:03

Host Information

DNS Name:	sip-Telefono.Entidad.col
OS:	[0: Yealink SIP Device]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	5	1	28	35

Results Details

/

46215 - Inconsistent Hostname and IP Address	[-/+]
50345 - Missing or Permissive X-Frame-Options HTTP Response Header	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
11219 - Nessus SYN scanner	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
21642 - Session Initiation Protocol Detection	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
22964 - Service Detection	[-/+]
46180 - Additional DNS Hostnames	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
10287 - Traceroute Information	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
10863 - SSL Certificate Information	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
50845 - OpenSSL Detection	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
10107 - HTTP Server Type and Version	[-/+]
91815 - Web Application Sitemap	[-/+]

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	[-/+]
51891 - SSL Session Resume Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
43111 - HTTP Methods Allowed (per directory)	[-/+]
117530 - Errors in nessusd.dump	[-/+]
11936 - OS Identification	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
54615 - Device Type	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
19506 - Nessus Scan Information	[-/+]
10919 - Open Port Re-check	[-/+]

10.2.48.13

Scan Information

Start time:	2020/04/29 16:55
End time:	2020/04/29 23:49

Host Information

DNS Name:	sip-Telefono.Entidad.col
OS:	[0: Yealink SIP Device]

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	9	1	25	36

Results Details

/

21642 - Session Initiation Protocol Detection	[-/+]
51891 - SSL Session Resume Supported	[-/+]
46180 - Additional DNS Hostnames	[-/+]
91815 - Web Application Sitemap	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]

57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
11219 - Nessus SYN scanner	[-/+]
10107 - HTTP Server Type and Version	[-/+]
19506 - Nessus Scan Information	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
20007 - SSL Version 2 and 3 Protocol Detection	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
22964 - Service Detection	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
50345 - Missing or Permissive X-Frame-Options HTTP Response Header	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
50845 - OpenSSL Detection	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
11936 - OS Identification	[-/+]
26928 - SSL Weak Cipher Suites Supported	[-/+]

10287 - Traceroute Information [-/+]

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header [-/+]

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32) [-/+]

54615 - Device Type [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah) [-/+]

10.2.48.19

Scan Information

Start time:	2020/04/29 16:55
End time:	2020/04/29 21:27

Host Information

DNS Name:	Telefono.Entidad.col
OS:	[0: Linux Kernel 2.6]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	5	1	26	32

Results Details

/

10287 - Traceroute Information [-/+]

11936 - OS Identification [-/+]

25220 - TCP/IP Timestamps Supported [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits [-/+]

21642 - Session Initiation Protocol Detection [-/+]

45590 - Common Platform Enumeration (CPE) [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

10919 - Open Port Re-check [-/+]

50345 - Missing or Permissive X-Frame-Options HTTP Response Header	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
10863 - SSL Certificate Information	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
10662 - Web mirroring	[-/+]
121010 - TLS Version 1.1 Protocol Detection	[-/+]
12053 - Host Fully Qualified Domain Name (FQDN) Resolution	[-/+]
50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	[-/+]
91815 - Web Application Sitemap	[-/+]
11219 - Nessus SYN scanner	[-/+]
84502 - HSTS Missing From HTTPS Server	[-/+]
19506 - Nessus Scan Information	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
22964 - Service Detection	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
54615 - Device Type	[-/+]
50845 - OpenSSL Detection	[-/+]

10.2.48.63

Scan Information

Start time: 2020/04/29 16:55

End time: 2020/04/29 18:06

Host Information

DNS Name: Telefono.Entidad.col

OS: [0: Linux Kernel 2.6]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	5	1	25	31

Results Details

/

54615 - Device Type	[-/+]
19506 - Nessus Scan Information	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
10662 - Web mirroring	[-/+]
50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
50845 - OpenSSL Detection	[-/+]
10287 - Traceroute Information	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
22964 - Service Detection	[-/+]
50345 - Missing or Permissive X-Frame-Options HTTP Response Header	[-/+]
11219 - Nessus SYN scanner	[-/+]
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported	[-/+]
21642 - Session Initiation Protocol Detection	[-/+]

35291 - SSL Certificate Signed Using Weak Hashing Algorithm [-/+]

121010 - TLS Version 1.1 Protocol Detection [-/+]

11936 - OS Identification [-/+]

91815 - Web Application Sitemap [-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]

10863 - SSL Certificate Information [-/+]

70544 - SSL Cipher Block Chaining Cipher Suites Supported [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

104743 - TLS Version 1.0 Protocol Detection [-/+]

84502 - HSTS Missing From HTTPS Server [-/+]

56984 - SSL / TLS Versions Supported [-/+]

10114 - ICMP Timestamp Request Remote Date Disclosure [-/+]

24260 - HyperText Transfer Protocol (HTTP) Information [-/+]

10.2.48.66

Scan Information

Start time:	2020/04/29 16:55
End time:	2020/04/29 23:33

Host Information

DNS Name:	sip-Telefono.Entidad.col
OS:	[0: Yealink SIP Device]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	8	1	27	36

Results Details

/

26928 - SSL Weak Cipher Suites Supported [-/+]

19506 - Nessus Scan Information [-/+]

91815 - Web Application Sitemap [-/+]

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	[-/+]
45410 - SSL Certificate 'commonName' Mismatch	[-/+]
11219 - Nessus SYN scanner	[-/+]
21643 - SSL Cipher Suites Supported	[-/+]
70544 - SSL Cipher Block Chaining Cipher Suites Supported	[-/+]
24260 - HyperText Transfer Protocol (HTTP) Information	[-/+]
22964 - Service Detection	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)	[-/+]
56984 - SSL / TLS Versions Supported	[-/+]
51192 - SSL Certificate Cannot Be Trusted	[-/+]
10287 - Traceroute Information	[-/+]
50845 - OpenSSL Detection	[-/+]
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits	[-/+]
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)	[-/+]
46215 - Inconsistent Hostname and IP Address	[-/+]
10863 - SSL Certificate Information	[-/+]
10919 - Open Port Re-check	[-/+]
11936 - OS Identification	[-/+]
117530 - Errors in nessusd.dump	[-/+]
104743 - TLS Version 1.0 Protocol Detection	[-/+]
45411 - SSL Certificate with Wrong Hostname	[-/+]
35291 - SSL Certificate Signed Using Weak Hashing Algorithm	[-/+]
46180 - Additional DNS Hostnames	[-/+]
25220 - TCP/IP Timestamps Supported	[-/+]

81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK) [-/+]

10107 - HTTP Server Type and Version [-/+]

21642 - Session Initiation Protocol Detection [-/+]

43111 - HTTP Methods Allowed (per directory) [-/+]

84502 - HSTS Missing From HTTPS Server [-/+]

12053 - Host Fully Qualified Domain Name (FQDN) Resolution [-/+]

50345 - Missing or Permissive X-Frame-Options HTTP Response Header [-/+]

54615 - Device Type [-/+]

10.2.48.200

Scan Information

Start time:	2020/04/29 16:55
End time:	2020/04/29 22:20

Host Information

OS:	[0: CISCO IOS 12][1: CISCO PIX][2: Cisco IOS XE][3: CISCO IOS 15]

Results Summary

Critical	High	Medium	Low	Info	Total
0	0	1	2	16	19

Results Details

/

11219 - Nessus SYN scanner [-/+]

22964 - Service Detection [-/+]

70657 - SSH Algorithms and Languages Supported [-/+]

10267 - SSH Server Type and Version Information [-/+]

117886 - Local Checks Not Enabled (info) [-/+]

19506 - Nessus Scan Information [-/+]

11936 - OS Identification [-/+]

54615 - Device Type [-/+]

10881 - SSH Protocol Versions Supported [-/+]

10107 - HTTP Server Type and Version	[-/+]
70658 - SSH Server CBC Mode Ciphers Enabled	[-/+]
10884 - Network Time Protocol (NTP) Server Detection	[-/+]
10114 - ICMP Timestamp Request Remote Date Disclosure	[-/+]
10287 - Traceroute Information	[-/+]
71049 - SSH Weak MAC Algorithms Enabled	[-/+]
45590 - Common Platform Enumeration (CPE)	[-/+]
110723 - No Credentials Provided	[-/+]
19689 - Embedded Web Server Detection	[-/+]
97861 - Network Time Protocol (NTP) Mode 6 Scanner	[-/+]

This is a report from Tenable.io.
Tenable.io is published by Tenable, Inc
7021 Columbia Gateway Drive Suite 500, Columbia, MD 21046
© 2020 Tenable, Inc. All rights reserved.

ANEXO 07

NOTA: Todas las direcciones IP fueron modificadas para conservar la confidencialidad y reserva de la entidad.

IP	Nessus Plugin ID	Nombre	Descripción	Severidad	Referencias de Vulnerabilidades
10.2.2.2	35372	DNS Server Dynamic Update Record Injection	El servidor DNS permite actualizaciones dinámicas.	Media	
	57608	SMB Signing not required	No se requiere autenticación para el ingreso al servidor SMB.	Media	
	25701	LDAP Crafted Search Request Server Information Disclosure	Es posible obtener información del servidor LDAP.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10150	Windows NetBIOS / SMB Remote Host Information Disclosure	Es posible obtener información de la entidad.	Info	
10.2.2.42	20007	SSL Version 2 and 3 Protocol Detection	El servicio remoto cifra el tráfico usando un protocolo con debilidades conocidas.	Alta	
	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Es posible tener acceso remoto al host.	Media	CVE-2005-1794
	57608	SMB Signing not required	No se requiere autenticación para el ingreso al servidor SMB.	Media	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	46180	Additional DNS Hostnames	Es posible obtener información de otros equipos de la red.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	10150	Windows NetBIOS / SMB Remote Host Information Disclosure	Es posible obtener información de la entidad.	Info	

10.2.2.73	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	108797	Unsupported Windows OS (remote)	El equipo utiliza un sistema operativo que ya no tiene soporte.	Crítica	
	46180	Additional DNS Hostnames	Es posible obtener información de otros equipos de la red.	Info	
	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	El equipo puede ser afectado por una vulnerabilidad de ejecución de código remoto.	Crítica	CVE-2019-0708
	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Es posible tener acceso remoto al host.	Media	CVE-2005-1794
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	10150	Windows NetBIOS / SMB Remote Host Information Disclosure	Es posible obtener información de la entidad.	Info	
10.2.2.77	20007	SSL Version 2 and 3 Protocol Detection	El servicio remoto cifra el tráfico usando un protocolo con debilidades conocidas.	Alta	
	57608	SMB Signing not required	No se requiere autenticación para el ingreso al servidor SMB.	Media	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	46180	Additional DNS Hostnames	Es posible obtener información de otros equipos de la red.	Info	
	10150	Windows NetBIOS / SMB Remote Host Information Disclosure	Es posible obtener información de la entidad.	Info	

10.2.2.79	20007	SSL Version 2 and 3 Protocol Detection	El servicio remoto cifra el tráfico usando un protocolo con debilidades conocidas.	Alta	
	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Es posible tener acceso remoto al host.	Media	CVE-2005-1794
	57608	SMB Signing not required	No se requiere autenticación para el ingreso al servidor SMB.	Media	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
10.2.2.91	57608	SMB Signing not required	No se requiere autenticación para el ingreso al servidor SMB.	Media	
	35372	DNS Server Dynamic Update Record Injection	El servidor DNS permite actualizaciones dinámicas.	Media	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10150	Windows NetBIOS / SMB Remote Host Information Disclosure	Es posible obtener información de la entidad.	Info	
10.2.2.103	69552	Oracle TNS Listener Remote Poisoning	Es posible que haya uso indebido del sniffer TNS de Oracle.	Alta	CVE-2012-1675
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	108797	Unsupported Windows OS (remote)	El equipo utiliza un sistema operativo que ya no tiene soporte.	Crítica	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	El equipo puede ser afectado por una vulnerabilidad de ejecución de código remoto.	Crítica	CVE-2019-0708

10.2.2.103	22073	Oracle Database Detection	Se detectó un servicio de base de datos escuchando por un puerto.	Info	
	10150	Windows NetBIOS / SMB Remote Host Information Disclosure	Es posible obtener información de la entidad.	Info	
10.2.2.107	57608	SMB Signing not required	No se requiere autenticación para el ingreso al servidor SMB.	Media	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	108797	Unsupported Windows OS (remote)	El equipo utiliza un sistema operativo que ya no tiene soporte.	Crítica	
	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	El equipo puede ser afectado por una vulnerabilidad de ejecución de código remoto.	Crítica	CVE-2019-0708
	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Es posible tener acceso remoto al host.	Media	CVE-2005-1794
	10150	Windows NetBIOS / SMB Remote Host Information Disclosure	Es posible obtener información de la entidad.	Info	
	46180	Additional DNS Hostnames	Es posible obtener información de otros equipos de la red.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
10.2.2.196	127131	PHP 7.2.x < 7.2.21 Multiple Vulnerabilities.	Una aplicación instalada puede ser afectada por múltiples vulnerabilidades.	Media	CVE-2019-11042 / CVE-2019-11041
	121353	PHP 7.2.x < 7.2.14 Multiple vulnerabilities.	Una aplicación instalada puede ser afectada por múltiples vulnerabilidades.	Alta	CVE-2019-9024 / CVE-2019-9023 / CVE-2019-9020 / CVE-2019-9022 / CVE-2019-9021 / CVE-2018-19935 / CVE-2019-6977 / CVE-2016-10166
	119766	PHP 7.2.x < 7.2.13 Multiple vulnerabilities	Una aplicación instalada puede ser afectada por múltiples vulnerabilidades.	Alta	CVE-2018-19518 / CVE-2018-20783

10.2.2.196	124763	PHP 7.2.x < 7.2.18 Heap-based Buffer Overflow Vulnerability.	Una aplicación instalada es vulnerable a un ataque de desbordamiento de búfer.	Media	CVE-2019-11036
	121385	OpenSSL 1.1.1 < 1.1.1a Multiple Vulnerabilities	Un servicio que corre en el equipo puede sr afectado por múltiples vulnerabilidades.	Media	CVE-2018-0734 / CVE-2018-0735
	125639	PHP 7.2.x < 7.2.19 Multiple Vulnerabilities.	Una aplicación instalada puede ser afectada por múltiples vulnerabilidades.	Media	CVE-2019-11040 / CVE-2019-11039 / CVE-2019-11038
	123754	PHP 7.2.x < 7.2.17 Multiple vulnerabilities.	Una aplicación instalada puede ser afectada por múltiples vulnerabilidades.	Media	CVE-2019-11035 / CVE-2019-11034
	128116	OpenSSL 1.1.1 < 1.1.1d Multiple Vulnerabilities	El servicio remoto puede ser afectado por múltiples vulnerabilidades.	Media	CVE-2019-1547 / CVE-2019-1549 / CVE-2019-1552
	132725	OpenSSL 1.1.1 < 1.1.1e-dev Procedure Overflow Vulnerability	El servicio remoto es vulnerable a un ataque de desbordamiento de procesos.	Media	CVE-2019-1551
	48204	Apache HTTP Server Version	Es posible obtener la versión del servidor Apache.	Info	
	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.	Una aplicación instalada en el equipo es vulnerable a un ataque de ejecución de código remoto.	Alta	CVE-2019-11043
	123642	Apache 2.4.x < 2.4.39 Multiple Vulnerabilities	El servidor web puede ser afectado por múltiples vulnerabilidades.	Alta	CVE-2019-0215 / CVE-2019-0217 / CVE-2019-0197 / CVE-2019-0196 / CVE-2019-0220 / CVE-2019-0211
	121355	Apache 2.4.x < 2.4.38 Multiple Vulnerabilities	El servidor web puede ser afectado por múltiples vulnerabilidades.	Media	CVE-2018-17199 / CVE-2018-17189 / CVE-2019-0190
	125641	OpenSSL 1.1.1 < 1.1.1c Vulnerability	El servicio remoto puede ser afectado por una vulnerabilidad.	Media	CVE-2019-1543
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	

10.2.2.196	135290	Apache 2.4.x < 2.4.42 Multiple Vulnerabilities	El servidor web puede ser afectado por múltiples vulnerabilidades.	Media	CVE-2020-1934 / CVE-2020-1927
	128033	Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	El servidor web puede ser afectado por múltiples vulnerabilidades.	Media	CVE-2019-10097 / CVE-2019-10098 / CVE-2019-9517 / CVE-2019-10082 / CVE-2019-10081 / CVE-2019-10092
	48243	PHP Version Detection	Es posible obtener la versión de PHP del equipo.	Info	
	123828	PHP 7.2.x < 7.2.16 Multiple vulnerabilities.	Una aplicación instalada puede ser afectada por múltiples vulnerabilidades.	Alta	CVE-2019-9640 / CVE-2019-9641 / CVE-2019-9637 / CVE-2019-9639 / CVE-2019-9638
10.2.2.205	39480	PHP < 5.2.10 Multiple Vulnerabilities	El servidor web utiliza una versión de PHP que puede ser afectado por múltiples vulnerabilidades.	Media	CVE-2009-2687 / CWE:20
	10150	Windows NetBIOS / SMB Remote Host Information Disclosure	Es posible obtener información de la entidad.	Info	
	51139	PHP 5.2 < 5.2.15 Multiple Vulnerabilities	El servidor web utiliza una versión de PHP que puede ser afectado por múltiples vulnerabilidades.	Media	CVE-2010-4698 / CVE-2010-4697 / CVE-2011-0752 / CVE-2010-3709 / CVE-2010-4150 / CVE-2010-3436
	41014	PHP < 5.2.11 Multiple Vulnerabilities	El servidor web utiliza una versión de PHP que puede ser afectado por múltiples vulnerabilidades.	Alta	CVE-2009-4018 / CVE-2009-5016 / CVE-2009-3293 / CVE-2009-3294 / CVE-2009-3291 / CVE-2009-3292 / CWE:134 / CWE:20 / CWE:264
	108797	Unsupported Windows OS (remote)	El equipo utiliza un sistema operativo que ya no tiene soporte.	Crítica	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	

10.2.2.205	43351	PHP < 5.2.12 Multiple Vulnerabilities	El servidor web utiliza una versión de PHP que puede ser afectado por múltiples vulnerabilidades.	Media	CVE-2009-4017 / CVE-2009-3557 / CVE-2009-4143 / CVE-2009-4142 / CVE-2009-3558 / CWE:79 / CWE:264
	73289	PHP PHP_RSHUTDOWN_FUNCTION Security Bypass	El servidor web utiliza una versión de PHP que puede ser afectado por múltiples vulnerabilidades.	Media	CVE-2012-1171
	35067	PHP < 5.2.8 Multiple Vulnerabilities	El servidor web utiliza una versión de PHP que puede ser afectado por múltiples vulnerabilidades.	Alta	CVE-2008-5844 / CVE-2008-5814 / CWE:16 / CWE:79
	51439	PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS	El servidor web utiliza una versión de PHP que puede ser afectado por múltiples vulnerabilidades.	Media	CVE-2010-4645
	35043	PHP 5 < 5.2.7 Multiple Vulnerabilities	El servidor web utiliza una versión de PHP que puede ser afectado por múltiples vulnerabilidades.	Alta	CVE-2008-2371 / CVE-2008-3660 / CVE-2008-5557 / CVE-2008-5624 / CVE-2008-2665 / CVE-2008-7068 / CVE-2014-8626 / CVE-2008-2666 / CVE-2008-5625 / CVE-2008-5658 / CVE-2008-3658 / CVE-2008-3659 / CVE-2008-2829 / CWE:22 / CWE:20 / CWE:264 / CWE:119
	57537	PHP < 5.3.9 Multiple Vulnerabilities	El servidor web utiliza una versión de PHP que puede ser afectado por múltiples vulnerabilidades.	Alta	CVE-2012-0789 / CVE-2012-0788 / CVE-2011-4566 / CVE-2011-4885 / CVE-2011-3379 / CVE-2012-0057 / CVE-2012-0781
	44921	PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities	El servidor web utiliza una versión de PHP que puede ser afectado por múltiples vulnerabilidades.	Media	CVE-2010-1130 / CVE-2010-1129 / CVE-2010-1128
	35750	PHP < 5.2.9 Multiple Vulnerabilities	El servidor web utiliza una versión de PHP que puede ser afectado por múltiples vulnerabilidades.	Media	CVE-2008-5498 / CVE-2009-1272 / CVE-2009-1271 / CWE:200 / CWE:20

10.2.2.205	48243	PHP Version Detection	Es posible obtener la versión de PHP del equipo.	Info	
	58988	PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution	El servidor web utiliza una versión de PHP que puede ser afectado por múltiples vulnerabilidades.	Alta	CVE-2012-1823
	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	El equipo puede ser afectado por una vulnerabilidad de ejecución de código remoto.	Crítica	CVE-2019-0708
	46180	Additional DNS Hostnames	Es posible obtener información de otros equipos de la red.	Info	
	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Es posible tener acceso remoto al host.	Media	CVE-2005-1794
	58966	PHP < 5.3.11 Multiple Vulnerabilities	El servidor Web utiliza una versión de PHP afectado por múltiples vulnerabilidades.	Alta	CVE-2012-0831 / CVE-2011-1398 / CVE-2012-1172
	58987	PHP Unsupported Version Detection	El servidor Web utiliza una versión de PHP no soportada.	Crítica	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	48244	PHP 5.2 < 5.2.14 Multiple Vulnerabilities	El servidor Web utiliza una versión de PHP afectado por múltiples vulnerabilidades.	Alta	CVE-2010-2191 / CVE-2010-2190 / CVE-2010-0397 / CVE-2010-1860 / CVE-2010-2531 / CVE-2010-2100 / CVE-2010-2101 / CVE-2010-2484 / CVE-2010-3065 / CVE-2010-2097 / CVE-2007-1581 / CVE-2010-1864 / CVE-2010-1862 / CVE-2010-2225
10.2.3.79	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	

10.2.3.79	108797	Unsupported Windows OS (remote)	El equipo utiliza un sistema operativo que ya no tiene soporte.	Crítica	
	10150	Windows NetBIOS / SMB Remote Host Information Disclosure	Es posible obtener información de la entidad.	Info	
	46180	Additional DNS Hostnames	Es posible obtener información de otros equipos de la red.	Info	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	El equipo puede ser afectado por una vulnerabilidad de ejecución de código remoto.	Crítica	CVE-2019-0708
	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Es posible tener acceso remoto al host.	Media	CVE-2005-1794
	57608	SMB Signing not required	No se requiere autenticación para el ingreso al servidor SMB.	Media	
10.2.3.99	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	14255	Microsoft Outlook Web Access (OWA) Version Detection	Es posible obtener la versión del servidor Exchange.	Info	
	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	El equipo puede ser afectado por una vulnerabilidad de ejecución de código remoto.	Crítica	CVE-2019-0708
	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Es posible tener acceso remoto al host.	Media	CVE-2005-1794
	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)	El equipo puede ser afectado por múltiples vulnerabilidades.	Alta	CVE-2017-0148 / CVE-2017-0147 / CVE-2017-0146 / CVE-2017-0145 / CVE-2017-0144 / CVE-2017-0143
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	

10.2.3.99	11422	Web Server Unconfigured - Default Install Page Present	El servidor web no está configurado o está mal configurado.	Info	
	20007	SSL Version 2 and 3 Protocol Detection	El servicio remoto cifra el tráfico usando un protocolo con debilidades conocidas.	Alta	
	10263	SMTP Server Detection	Se detectó un servicio de SMTP.	Info	
	108797	Unsupported Windows OS (remote)	El equipo utiliza un sistema operativo que ya no tiene soporte.	Crítica	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	El equipo es vulnerable a un ataque que permite desencriptar el tráfico TLS.	Media	CVE-2016-0800
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities	El equipo puede ser afectado por múltiples vulnerabilidades.	Alta	CVE-2017-0277 / CVE-2017-0267 / CVE-2017-0278 / CVE-2017-0268 / CVE-2017-0279 / CVE-2017-0269 / CVE-2017-0280 / CVE-2017-0270 / CVE-2017-0271 / CVE-2017-0272 / CVE-2017-0273 / CVE-2017-0274 / CVE-2017-0275 / CVE-2017-0276
10.2.3.101	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	46180	Additional DNS Hostnames	Es posible obtener información de otros equipos de la red.	Info	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310

10.2.3.101	10150	Windows NetBIOS / SMB Remote Host Information Disclosure	Es posible obtener información de la entidad.	Info	
	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Es posible tener acceso remoto al host.	Media	CVE-2005-1794
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	108797	Unsupported Windows OS (remote)	El equipo utiliza un sistema operativo que ya no tiene soporte.	Crítica	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	El equipo puede ser afectado por una vulnerabilidad de ejecución de código remoto.	Crítica	CVE-2019-0708
10.2.3.171	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	10144	Microsoft SQL Server TCP/IP Listener Detection	Se detectó un servicio de base de datos escuchando por un puerto.	Info	
	20007	SSL Version 2 and 3 Protocol Detection	El servicio remoto cifra el tráfico usando un protocolo con debilidades conocidas.	Alta	
	11422	Web Server Unconfigured - Default Install Page Present	El servidor web no está configurado o está mal configurado.	Info	
	10674	Microsoft SQL Server UDP Query Remote Version Disclosure	Es posible obtener la versión y las instancias de SQL Server.	Info	
	53641	HP Data Protector Remote Command Execution	El servicio remoto permite la ejecución de comandos sin autenticación.	Crítica	CVE-2011-0923
	79233	HP Data Protector 'EXEC_INTEGUTIL' Arbitrary Command Execution	El equipo puede ser afectado por cualquier vulnerabilidad de ejecución de comandos.	Crítica	

10.2.3.171	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	46180	Additional DNS Hostnames	Es posible obtener información de otros equipos de la red.	Info	
	10150	Windows NetBIOS / SMB Remote Host Information Disclosure	Es posible obtener información de la entidad.	Info	

ANEXO 08

NOTA: Todas las direcciones IP fueron modificadas para conservar la confidencialidad y reserva de la entidad.

IP	Nessus Plugin ID	Nombre	Descripción	Severidad	Referencias de Vulnerabilidades
10.2.1.2	15901	SSL Certificate Expiry	El certificado SSL del servidor expiró.	Media	
	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	El dispositivo soporta cifrado RC4.	Media	CVE-2013-2566 / CVE-2015-2808
	104743	TLS Version 1.0 Protocol Detection	El servicio remoto encripta tráfico con versión una versión obsoleta de TLS.	Media	
	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934
	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	El servicio remoto soporta cifrado SSL de fuerza media.	Media	CVE-2016-2183
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	42263	Unencrypted Telnet Server	El equipo transmite tráfico en claro.	Media	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
10.2.1.3	20007	SSL Version 2 and 3 Protocol Detection	El servicio remoto cifra el tráfico usando un protocolo con debilidades conocidas.	Alta	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	

10.2.1.3	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	10107	HTTP Server Type and Version	Es posible obtener el tipo y versión de servidor web.	Info	
10.2.1.4	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
10.2.1.5	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
10.2.1.6	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	104743	TLS Version 1.0 Protocol Detection	El servicio remoto encripta tráfico con versión una versión obsoleta de TLS.	Media	
	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	El dispositivo soporta cifrado RC4.	Media	CVE-2013-2566 / CVE-2015-2808
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934

10.2.1.6	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	El servicio remoto soporta cifrado SSL de fuerza media.	Media	CVE-2016-2183
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
10.2.1.11	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	El servicio remoto soporta cifrado SSL de fuerza media.	Media	CVE-2016-2183
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	El dispositivo soporta cifrado RC4.	Media	CVE-2013-2566 / CVE-2015-2808
	15901	SSL Certificate Expiry	El certificado SSL del servidor expiró.	Media	
	104743	TLS Version 1.0 Protocol Detection	El servicio remoto encripta tráfico con versión una versión obsoleta de TLS.	Media	
10.2.1.20	130208	Cisco Wireless LAN Controller Secure Shell (SSH) Denial of Service Vulnerability (cisco-sa-20191016-wlc-ssh-dos)	Al dispositivo remoto le hace falta un parche suministrado por el proveedor.	Alta	CVE-2019-15262 / CWE:20
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	70122	Cisco Wireless LAN Controller (WLC) Version	Es posible obtener la versión del WLC.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	

10.2.1.20	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	131230	Cisco Wireless LAN Controller HTTP Parsing Engine Denial of Service Vulnerability	Al dispositivo remoto le hace falta un parche suministrado por el proveedor.	Media	CVE-2019-15276 / CWE:20
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
10.2.1.21	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	104743	TLS Version 1.0 Protocol Detection	El servicio remoto encripta tráfico con versión una versión obsoleta de TLS.	Media	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
10.2.1.22	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10107	HTTP Server Type and Version	Es posible obtener el tipo y versión de servidor web.	Info	
10.2.1.31	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	El dispositivo soporta cifrado RC4.	Media	CVE-2013-2566 / CVE-2015-2808
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934

10.2.1.31	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	121010	TLS Version 1.1 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	El servicio remoto soporta cifrado SSL de fuerza media.	Media	CVE-2016-2183
	66848	SSL Null Cipher Suites Supported	El servicio remoto soporta cifrados SSL nulos.	Media	
	104743	TLS Version 1.0 Protocol Detection	El servicio remoto encripta tráfico con versión una versión obsoleta de TLS.	Media	
10.2.1.32	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	El dispositivo soporta cifrado RC4.	Media	CVE-2013-2566 / CVE-2015-2808
	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	El servicio remoto soporta cifrado SSL de fuerza media.	Media	CVE-2016-2183
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	66848	SSL Null Cipher Suites Supported	El servicio remoto soporta cifrados SSL nulos.	Media	
	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934
	104743	TLS Version 1.0 Protocol Detection	El servicio remoto encripta tráfico con versión una versión obsoleta de TLS.	Media	
	121010	TLS Version 1.1 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	

10.2.1.33	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934
	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	El servicio remoto soporta cifrado SSL de fuerza media.	Media	CVE-2016-2183
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	104743	TLS Version 1.0 Protocol Detection	El servicio remoto encripta tráfico con versión una versión obsoleta de TLS.	Media	
	66848	SSL Null Cipher Suites Supported	El servicio remoto soporta cifrados SSL nulos.	Media	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	El dispositivo soporta cifrado RC4.	Media	CVE-2013-2566 / CVE-2015-2808
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	15901	SSL Certificate Expiry	El certificado SSL del servidor expiró.	Media	
	121010	TLS Version 1.1 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
10.2.1.34	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	104743	TLS Version 1.0 Protocol Detection	El servicio remoto encripta tráfico con versión una versión obsoleta de TLS.	Media	
	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	El servicio remoto soporta cifrado SSL de fuerza media.	Media	CVE-2016-2183
	15901	SSL Certificate Expiry	El certificado SSL del servidor expiró.	Media	

10.2.1.34	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	66848	SSL Null Cipher Suites Supported	El servicio remoto soporta cifrados SSL nulos.	Media	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	El dispositivo soporta cifrado RC4.	Media	CVE-2013-2566 / CVE-2015-2808
	121010	TLS Version 1.1 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
10.2.1.35	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	10107	HTTP Server Type and Version	Es posible obtener el tipo y versión de servidor web.	Info	
10.2.1.41	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
10.2.1.51	121010	TLS Version 1.1 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310

10.2.1.51	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	El servicio remoto soporta cifrado SSL de fuerza media.	Media	CVE-2016-2183
	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	El dispositivo soporta cifrado RC4.	Media	CVE-2013-2566 / CVE-2015-2808
	15901	SSL Certificate Expiry	El certificado SSL del servidor expiró.	Media	
	66848	SSL Null Cipher Suites Supported	El servicio remoto soporta cifrados SSL nulos.	Media	
	104743	TLS Version 1.0 Protocol Detection	El servicio remoto encripta tráfico con versión una versión obsoleta de TLS.	Media	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
10.2.1.61	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
10.2.1.71	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	104743	TLS Version 1.0 Protocol Detection	El servicio remoto encripta tráfico con versión una versión obsoleta de TLS.	Media	
10.2.1.81	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	

10.2.1.91	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	121010	TLS Version 1.1 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)	El servicio remoto soporta cifrado SSL de fuerza media.	Media	CVE-2016-2183
	104743	TLS Version 1.0 Protocol Detection	El servicio remoto encripta tráfico con versión una versión obsoleta de TLS.	Media	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	66848	SSL Null Cipher Suites Supported	El servicio remoto soporta cifrados SSL nulos.	Media	
	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	El dispositivo soporta cifrado RC4.	Media	CVE-2013-2566 / CVE-2015-2808
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
10.2.1.100	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	17367	Fortinet FortiGate Web Console Management Detection	Se detectó el servicio de administración de FW.	Info	

10.2.1.101	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	42263	Unencrypted Telnet Server	El equipo transmite tráfico en claro.	Media	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
10.2.1.111	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
10.2.1.121	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
10.2.1.249	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934
	44079	OpenSSH < 4.9 'ForceCommand' Directive Bypass	El equipo puede afectarse por una vulnerabilidad de ByPass.	Media	CVE-2008-1657 / CWE:264
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	10107	HTTP Server Type and Version	Es posible obtener el tipo y versión de servidor web.	Info	
	90317	SSH Weak Algorithms Supported	El servidor SSH permite algoritmos de ecripción débiles.	Media	
	19592	OpenSSH < 4.2 Multiple Vulnerabilities	El servidor SSH puede ser afectado por múltiples vulnerabilidades.	Baja	CVE-2006-0393 / CVE-2005-2798 / CVE-2005-2797
	41028	SNMP Agent Default Community Name (public)	Es posible obtener información del servidor SNMP.	Media	CVE-1999-0517

10.2.1.249	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	44076	OpenSSH < 4.3 scp Command Line Filename Processing Command Injection	La versión de SSH es vulnerable a un ataque de inyección de comandos.	Media	CVE-2006-0225
	86420	Ethernet MAC Addresses	Es posible obtener la dirección MAC de otros equipos.	Info	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	44078	OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass	Es posible que un atacante evite la autenticación	Alta	CVE-2007-4752 / CVE-2007-2243 / CWE:287 / CWE:20
	44077	OpenSSH < 4.5 Multiple Vulnerabilities	El servicio SSH puede ser afectado por múltiples vulnerabilidades.	Alta	CVE-2006-5794 / CVE-2006-4925 / CVE-2007-0726
10.2.1.250	10107	HTTP Server Type and Version	Es posible obtener el tipo y versión de servidor web.	Info	
	54615	Device Type	Es posible conocer el tipo de dispositivo que es.	Info	
	10267	SSH Server Type and Version Information	Es posible conocer el tipo y la versión del servidor SSH.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	

ANEXO 09

NOTA: Todas las direcciones IP fueron modificadas para conservar la confidencialidad y reserva de la entidad.

IP	Nessus Plugin ID	Nombre	Descripción	Severidad	Referencias de Vulnerabilidades
10.2.60.5	118885	ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check)	Al equipo Vmware ESXi le hace falta un parche de seguridad y puede ser atacado por múltiples vulnerabilidades.	Alta	CVE-2018-6982 / CVE-2018-6981
	123518	ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check)	Al equipo Vmware ESXi le hace falta un parche de seguridad y puede ser atacado por múltiples vulnerabilidades.	Alta	CVE-2019-5519 / CVE-2019-5518
	134878	VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS (VMSA-2018-0018) (remote check)	Al equipo Vmware ESXi le hace falta un parche de seguridad y puede ser atacado por múltiples vulnerabilidades.	Media	CVE-2018-6972
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	111759	ESXi 5.5 / 6.0 / 6.5 / 6.7 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (remote check)	Al equipo Vmware ESXi le hace falta un parche de seguridad y puede ser atacado por múltiples vulnerabilidades.	Media	CVE-2018-3646
	57396	VMware vSphere Detect	Se detectó que el equipo corre en Vmware.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	105614	ESXi 6.5 < Build 6765664 Heap Buffer Overflow (VMSA-2017-0021) (remote check)	El equipo puede ser atacado por una vulnerabilidad de desbordamiento de búfer.	Media	CVE-2017-4933
	118466	ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check)	El equipo puede ser atacado por una vulnerabilidad de lectura fuera de límites.	Alta	CVE-2018-6974
	105486	ESXi 5.5 / 6.0 / 6.5 / Multiple Vulnerabilities (VMSA-2017-0021) (VMSA-2018-0002) (Spectre) (remote check)	El equipo puede ser atacado por múltiples vulnerabilidades.	Media	CVE-2017-5753 / CVE-2017-4940 / CVE-2017-4941 / CVE-2017-5715

10.2.60.5	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
10.2.60.6	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	10107	HTTP Server Type and Version	Es posible obtener el tipo y versión de servidor web.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	48204	Apache HTTP Server Version	Es posible obtener la versión del servidor Apache.	Info	
	33850	Unix Operating System Unsupported Version Detection	El equipo utiliza un sistema operativo que ya no tiene soporte.	Crítica	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
10.2.60.10	105486	ESXi 5.5 / 6.0 / 6.5 / Multiple Vulnerabilities (VMSA-2017-0021) (VMSA-2018-0002) (Spectre) (remote check)	El equipo puede ser atacado por múltiples vulnerabilidades.	Media	CVE-2017-5753 / CVE-2017-4940 / CVE-2017-4941 / CVE-2017-5715
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	134878	VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS (VMSA-2018-0018) (remote check)	Al equipo Vmware ESXi le hace falta un parche de seguridad y puede ser atacado por múltiples vulnerabilidades.	Media	CVE-2018-6972
	57396	VMware vSphere Detect	Se detectó que el equipo corre en Vmware.	Info	
	118885	ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check)	Al equipo Vmware ESXi le hace falta un parche de seguridad y puede ser atacado por múltiples vulnerabilidades.	Alta	CVE-2018-6982 / CVE-2018-6981
	111759	ESXi 5.5 / 6.0 / 6.5 / 6.7 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (remote check)	Al equipo Vmware ESXi le hace falta un parche de seguridad y puede ser atacado por múltiples vulnerabilidades.	Media	CVE-2018-3646

10.2.60.10	118466	ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check)	El equipo puede ser atacado por una vulnerabilidad de lectura fuera de límites.	Alta	CVE-2018-6974
	105614	ESXi 6.5 < Build 6765664 Heap Buffer Overflow (VMSA-2017-0021) (remote check)	El equipo puede ser atacado por una vulnerabilidad de desbordamiento de búfer.	Media	CVE-2017-4933
	123518	ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check)	Al equipo Vmware ESXi le hace falta un parche de seguridad y puede ser atacado por múltiples vulnerabilidades.	Alta	CVE-2019-5519 / CVE-2019-5518
10.2.60.34	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	10092	FTP Server Detection	Se detectó un servicio FTP.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	16321	3Com 3CServer/3CDaemon FTP Server Multiple Vulnerabilities (OF, FS, PD, DoS)	El servidor FTP puede ser afectado por múltiples vulnerabilidades.	Crítica	CVE-2005-0419 / CVE-2005-0276 / CVE-2005-0277 / CVE-2005-0278
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Es posible tener acceso remoto al host.	Media	CVE-2005-1794
10.2.60.67	20007	SSL Version 2 and 3 Protocol Detection	El servicio remoto cifra el tráfico usando un protocolo con debilidades conocidas.	Alta	
	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Es posible tener acceso remoto al host.	Media	CVE-2005-1794
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	

10.2.60.67	11422	Web Server Unconfigured - Default Install Page Present	El servidor web no está configurado o está mal configurado.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	10144	Microsoft SQL Server TCP/IP Listener Detection	Se detectó un servicio de base de datos escuchando por un puerto.	Info	
10.2.60.100	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	118885	ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check)	Al equipo Vmware ESXi le hace falta un parche de seguridad y puede ser atacado por múltiples vulnerabilidades.	Alta	CVE-2018-6982 / CVE-2018-6981
	111759	ESXi 5.5 / 6.0 / 6.5 / 6.7 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (remote check)	Al equipo Vmware ESXi le hace falta un parche de seguridad y puede ser atacado por múltiples vulnerabilidades.	Media	CVE-2018-3646
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	57396	VMware vSphere Detect	Se detectó que el equipo corre en Vmware.	Info	
	118466	ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check)	El equipo puede ser atacado por una vulnerabilidad de lectura fuera de límites.	Alta	CVE-2018-6974
	123518	ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check)	Al equipo Vmware ESXi le hace falta un parche de seguridad y puede ser atacado por múltiples vulnerabilidades.	Alta	CVE-2019-5519 / CVE-2019-5518
	134878	VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS (VMSA-2018-0018) (remote check)	Al equipo Vmware ESXi le hace falta un parche de seguridad y puede ser atacado por múltiples vulnerabilidades.	Media	CVE-2018-6972

ANEXO 10

NOTA: Todas las direcciones IP fueron modificadas para conservar la confidencialidad y reserva de la entidad.

IP	Nessus Plugin ID	Nombre	Descripción	Severidad	Referencias de Vulnerabilidades
10.2.4.200	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
10.2.5.58	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	46180	Additional DNS Hostnames	Es posible obtener información de otros equipos de la red.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
10.2.5.83	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10863	SSL Certificate Information	Es posible obtener información de la entidad a través del certificado.	Info	
	46180	Additional DNS Hostnames	Es posible obtener información de otros equipos de la red.	Info	
	20007	SSL Version 2 and 3 Protocol Detection	El servicio remoto cifra el tráfico usando un protocolo con debilidades conocidas.	Alta	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	

ANEXO 11

NOTA: Todas las direcciones IP fueron modificadas para conservar la confidencialidad y reserva de la entidad.

IP	Nessus Plugin ID	Nombre	Descripción	Severidad	Referencias de Vulnerabilidades
10.2.48.7	20007	SSL Version 2 and 3 Protocol Detection	El servicio remoto cifra el tráfico usando un protocolo con debilidades conocidas.	Alta	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	121010	TLS Version 1.1 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
	104743	TLS Version 1.0 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
	11936	OS Identification	Encriptación de tráfico con protocolos obsoletos.	Media	
10.2.48.13	20007	SSL Version 2 and 3 Protocol Detection	El servicio remoto cifra el tráfico usando un protocolo con debilidades conocidas.	Alta	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	104743	TLS Version 1.0 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
	121010	TLS Version 1.1 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934

10.2.48.19	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	104743	TLS Version 1.0 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
	121010	TLS Version 1.1 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
10.2.48.63	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
	121010	TLS Version 1.1 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	104743	TLS Version 1.0 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
10.2.48.66	26928	SSL Weak Cipher Suites Supported	El servicio remoto soporta cifrado SSL débil.	Media	CWE:326 / CWE:327 / CWE:720 / CWE:753 / CWE:928 / CWE:803 / CWE:934
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	
	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	104743	TLS Version 1.0 Protocol Detection	Encriptación de tráfico con protocolos obsoletos.	Media	
	35291	SSL Certificate Signed Using Weak Hashing Algorithm	Se detectó un hash débil en un certificado SSL.	Media	CVE-2004-2761 / CWE:310
10.2.48.200	11936	OS Identification	Es posible obtener información del sistema operativo.	Info	
	10287	Traceroute Information	Es posible obtener información de la red por medio de Traceroute.	Info	

ANEXO 12

CHECKLIST– HARDENING CISCO IOS - Software release minimo12.4 (2) o superior

EQUIPO:			
DIRECCIÓN IP:		FECHA:	
FUNCIÓN DEL EQUIPO		HORA:	
RESPONSABLE EQUIPO		DURACIÓN:	
VERSION IOS INSTALADA			

Tema:	**1. Administración**				
Ejecutada	***Exitosa***	***Parámetro / Componente***	***Valor o cambio a implantar***	***Procedimiento para su implantación***	***Observación***
		Servidor externo AAA para la autenticación de usuario	Como buena práctica de seguridad es recomendable usar un servidor externo AAA (TACACS + o RADIUS) para manejar la autenticación, autorización y contabilidad del acceso de los usuarios a los dispositivos. NOTA: se adjunta procedimiento AAA, que no requiere licenciamiento.	RADIUS # config terminal (config)# aaa new-model (config)# aaa authentication login default group radius enable (config)# radius-server <host> (config)# radius-server key 'secret-key' (config)# line vty 0 4 (config-line)# login authentication default (config-line)# exit (config)# line con 0 config-line)# login authentication default	
		Creación de contraseña con privilegios administrativos	Para otorgar acceso privilegiado de administración al dispositivo IOS, se debe crear una contraseña segura utilizando el comando **enable secret**. Utilizar una contraseña con al menos 10 caracteres de largo que consista en símbolos alfanuméricos y especiales.	#config terminal (config)# enable secret **strongpassword**	
		Cifrado de contraseñas en el dispositivo	Cifrar las contraseñas de texto y evitar que se muestren en el archivo de configuración.	# config terminal (config)# service password-encryption	
		Eliminación de contraseñas con cifrado inseguro	Eliminar las contraseñas creadas bajo la ejecución del comando **enable password**.		
		Encripción de contraseña de usuario	Para encriptar la contraseña de los usuarios con hash MD5, se utiliza el comando **username secret**.	# config terminal (config)# username <user> secret <password>	
		Intentos máximos de autenticación fallida	Configurar el número máximo de intentos fallidos de inicio de sesión para que un usuario quede bloqueado después de este umbral.	# config terminal (config)# aaa new-model (config)# aaa local authentication attempts max-fail <max-attempts> (config)# aaa authentication login default local	
		Recuperación de contraseña	Impedir el borrado de contraseña accidental, e impedir a usuarios maliciosos cambiar la configuración registrada y el acceso a NVRAM.	# config terminal (config)# no service password-recovery	
		Cuentas locales separadas para la autenticación de usuario	A falta de un servidor AAA externo,crear cuentas locales separadas para cualquier persona a la que le dé acceso a sus dispositivos.	# config terminal (config)# username <username> secret <password>	
		Deshabilitación de servicios no utilizados	Todo servicio que no se utilice debe ser deshabilitado, en especial, aquellos que utilizan UDP. Para versiones menores a 12.0 utilizar el comando **no service tcp-small-servers** y **no serviceudp-small-servers**.	no ip finger, no ip bootp server, ip dhcp bootp ignore, no service dhcp, no mop enabled, no ip domain-lookup, no service pad, no ip http server, no ip http secure-server, no service config, no cdp enable, no cdp run	
		EXEC Timeout	Establecer el intervalo que el intérprete de comandos EXEC espera la entrada del usuario antes de que finalice una sesión,	línea con 0 exec-timeout <minutes> [segundos] línea vty 0 4 exec-timeout <minutes> [segundos]	
		Keepalives para sesiones TCP	Esta configuración debe usarse para habilitar TCP *keepalives* en conexiones entrantes al dispositivo y conexiones salientes desde el dispositivo. Esto garantiza que el dispositivo en el extremo remoto de la conexión aún sea accesible y que las conexiones medio abiertas o huérfanas se eliminen del dispositivo Cisco IOS local	service tcp-keepalives-in service tcp-keepalives-out	
		Uso de la interfaz de gestión	Se recomienda agregar una interfaz de bucle invertido a cada dispositivo como interfaz de administración y que se use exclusivamente para el plano de administración	interface Loopback0 ip address <IP> <MASK>	
		Notificación de umbral de memoria	La Notificación de umbral de memoria genera un mensaje de registro para indicar que la memoria libre en un dispositivo ha caído por debajo del umbral configurado	memory free low-watermark processor <threshold> memory free low-watermark io <threshold> memory reserve critical <value>	
		Notificación de umbral de CPU	Permite detectar y recibir notificaciones cuando la carga de CPU en un dispositivo cruza un umbral configurado	snmp-server enable traps cpu threshold snmp-server host <host-address> <community-string> cpu process cpu threshold type <type> rising <percentage> interval <seconds> [falling <percentage> interval <seconds>] process cpu statistics limit entry-percentage <number> [size <seconds>]	
		Reserva de memoria para acceso a la consola	Utilizar para reservar suficiente memoria para garantizar el acceso de la consola a un dispositivo Cisco IOS con fines administrativos y de resolución de problemas	memory reserve console 4096	
		Pérdida de memoria	Utilizar **show memory debug leaks** para la detección de pérdida de la memoria	show memory debug leaks	
		Desbordamiento de búfer: detección y corrección de la corrupción de Redzone	Habilitar para detectar y corregir un desbordamiento del bloque de memoria y continuar las operaciones.	exception memory ignore overflow io exception memory ignore overflow processor	

ANEXO 12

CHECKLIST– HARDENING CISCO IOS - Software release minimo12.4 (2) o superior

EQUIPO:						
DIRECCIÓN IP:						FECHA:
FUNCIÓN DEL EQUIPO						HORA:
RESPONSABLE EQUIPO						DURACIÓN:
VERSION IOS INSTALADA						
			Protocolo de tiempo de red (NTP)	Tener una configuración de reloj precisa y uniforme en todos los dispositivos de red para que los datos de registro se marquen con la hora y zona horaria correctas	# config terminal Cliente: (config)#ntp authenticate (config)#ntp authentication-key 5 md5 ciscotime (config)#ntp trusted-key 5 (config)#ntp server <IP> key 5 Servidor: (config)#ntp authenticate (config)#ntp authentication-key 5 md5 ciscotime (config)#ntp trusted-key 5	
			Restricción del acceso de administración a los dispositivos solo a IP específicas	Restringir qué direcciones IP pueden usar SSH a sus dispositivos. Esto debería limitarse a unos pocos sistemas de administración usados para administrar la red.	# config terminal (config)# access-list 10 permit <IP> 0.0.0.15 (config)# line vty 0 15 (config)# access-class 10 in	
			Listas de Control de Acceso (ACL)	Evitar la comunicación directa no autorizada a los dispositivos de red	ip access-list extended ACL-INFRASTRUCTURE-IN permit tcp host <trusted-egbp-peer> host <local-egbp-address> eq <service port> deny ip any <infrastructure-address-space> <mask> permit ip any any	
			Habilitación de registro	Habilitar el registro en un búfer interno del dispositivo o en un servidor de registro externo. Hay 8 niveles de registro diferentes (de 0 a 7), cada uno de los cuales proporciona progresivamente más detalles de datos de registro. Debe evitar iniciar sesión en el nivel 7 (depuración) ya que sobrecargará el dispositivo.	# configure terminal (config) # logging trap 6 (config) # service timestamps log datetime msec show-timezone (config) # host de registro <IP> (config) # logging source-interface ethernet 1/0	
			Filtrado de paquetes ICMP	El sistema operativo de Cisco provee de la funcionalidad para filtrar específicamente mensajes ICMP por nombre o tipo, como, **ping** o **traceroute**.	ip access-list extended ACL-INFRASTRUCTURE-IN permit icmp host <trusted-management-stations> any echo permit icmp host <trusted-netmgmt-servers> any echo deny ip any <infrastructure-address-space> <mask> permit ip any any	
			Filtrado de fragmentos IP	La información de capa 4 que es usada para filtrar paquetes TCP y UDP está presente solamente en el fragmento inicial.	ip access-list extended ACL-FRAGMENT-EXAMPLE permit tcp any host <IP> eq 80 deny tcp any host <IP> eq 22 deny tcp any any fragments deny udp any any fragments deny icmp any any fragments deny ip any any fragments deny ip any <infrastructure-address-space> <mask> permit ip any any	
			Filtrado de valor TTL con ACL	Si el número de paquetes que están próximos a vencer es alto, la transmisión de todos los mensajes puede consumir toda la CPU de la máquina.	ip access-list extended ACL-INFRASTRUCTURE-IN deny ip any any ttl lt 6 deny ip any <infrastructure-address-space> <mask> permit ip any any	
			Protocolos de gestión segura	Utilizar SSH para la administración en lugar de Telnet.	# config terminal (config)# hostname <hostname> London(config)# ip domain-name mydomain.com London(config)# ip ssh version 2 London(config)# crypto key generate rsa modulus 2048 London(config)# ip ssh time-out 60 London(config)# ip ssh authentication-retries 3 London(config)# line vty 0 15 London(config-line)# transport input ssh	
			Restricción y aseguramiento del acceso SNMP	Además de configurar una cadena de comunidad fuerte, el filtrado de IP también debe aplicarse para permitir el acceso SNMP solo desde estaciones de confianza mediante ACL	# config terminal (config) # access-list 11 permit <IP> 0.0.0.15 (config) # access-list 12 permit <IP> (config) # snmp-server community Cbd43@ # w5SDF RO 11 (config) # snmp-server community Xcv4 # 56 & 454sdS RW 12	
			Fortalecimiento del protocolo simple de administración de red	Proteger la confidencialidad, integridad y disponibilidad tanto de los datos de red como de los dispositivos de red a través de los cuales transitan estos datos	snmp-server community READONLY RO snmp-server community READWRITE RW	
			Protección del plano de gestión	Restringir las interfaces de tráfico que un dispositivo puede recibir. Esto permite al administrador un control adicional sobre un dispositivo y cómo se accede al dispositivo.	control-plane host management-interface GigabitEthernet 0/1 allow ssh https	
			Protección del plano de control	Restringir el tráfico que va destinado al procesador de ruteo del dispositivo. Permite al administrador clasificar y restringir el tráfico enviado al dispositivo con propósito de administración.		

ANEXO 12

CHECKLIST– HARDENING CISCO IOS - Software release minimo12.4 (2) o superior

EQUIPO:					
DIRECCIÓN IP:					FECHA:
FUNCIÓN DEL EQUIPO					HORA:
RESPONSABLE EQUIPO					DURACIÓN:
VERSION IOS INSTALADA					
		Encripción sesión de administración	Encriptar el tráfico de las sesiónes de administración para que usuarios malintencionados no puesdan acceder a los datos que se transmiten. El usuario puede esteblecer conexiones encriptadas a través de SSH, HTTPS o SCP.	This configuration example enables SSH services: ip domain-name example.com crypto key generate rsa modulus 2048 ip ssh time-out 60 ip ssh authentication-retries 3 ip ssh source-interface GigabitEthernet 0/1 line vty 0 4 transport input ssh This configuration example enables SCP services: ip scp server enable This is a configuration example for HTTPS services: crypto key generate rsa modulus 2048 ip http secure-server	
		Consola y puertos AUX	El puerto AUX de un dispositivo debe estar deshabilitado para evitar el acceso no autorizado	line aux 0 transport input none transport output none no exec exec-timeout 0 1 no password	
		Control de líneas vty y tty	Autenticación mediante el uso de AAA recomendado,o en su defecto con el uso de la base de datos de usuarios local, o mediante la autenticación de contraseña simple configurada directamente en la línea vty o tty.		
		Control de transporte para líneas vty y tty	Se deben configurar vty y tty para aceptar solo conexiones de administración de acceso remoto encriptadas	transport input ssh transport input one transport output transport output none transport output ssh	
		Banners de advertencia	Un banner de inicio de sesión no debe contener información específica sobre el nombre, modelo, software o propiedad del enrutador		
		Enviar Logs a una locación central	Enviar información de logueo a un servidor remoto para correlacionar y auditar la red y eventos de seguridad a lo largo de ésta.	logging host <ip address>	
		Nivel de Log	Cada mensaje de log en Cisco tiene una severidad en una escala de 8 niveles que va desde nivel 0 "Emergencia" hasta nivel 7 "Debug". Se debe evitar el logueo en nivel 7 ya que genera alto consumo de máquina y puede generar inestabilidad.	logging trap <severity> logging buffered <severity>	
		No mensajes de logs en consola o sesiones de monitoreo	No enviar mensajes de logs a sesiones de monitoreo o a consola porque puede elevar el consumo de la máquina. Utilizar los comandos **no logging console** y **no logging monitor**.	no logging console no logging monitor	
		Mensajes de logs en buffer local	Utilizar un buffer local para almacenar los logs.	logging buffer <size> logging buffer <severity>	
		Marcas de tiempo de logs	La configuración de marcas de tiempo ayuda a la correlación de eventos a lo largo de toda la red.	service timestamps log datetime msec show-timezone	
Tema:	**2. Control**				
Ejecutada	***Exitosa***	***Parámetro / Componente***	***Valor o cambio a implantar***	***Procedimiento para su implantación***	***Observación***
		Redirección de paquetes ICMP	Un atacante puede explotar la habilidad del router de redireccionar paquetes ICMP y puede ocasionar afectación en el rendimiento del router.	no ip redirects	
		Inalcanzable ICMP	La genreación de mensajes ICMP a destinos inalcanzables se debe deshabilitar.	no ip unreachables	
		Proxy ARP	Ataque de MiTM permite a un host en la red suplantar la MAC de un router. Proxy ARP se puede deshabilitar.	no ip proxy-arp	
		Reemplazo de configuración y reversión de configuración	Características de reemplazo de configuración y rollback de configuración archivando la configuración del dispositivo Cisco IOS.	archive path disk0:archived-config maximum 14 time-period 1440 write-memory	
		Configuración resistente del software Cisco IOS	Almacenar de forma segura una copia de la imagen del software Cisco IOS y la configuración del dispositivo. Cuando esta función está habilitada, no es posible alterar o eliminar estos archivos de respaldo	secure boot-image secure boot-config!	
		Acceso exclusivo a cambios de configuración	Solo un administrador realiza cambios de configuración en un dispositivo Cisco IOS en un momento dado	configuration mode exclusive auto	
		Notificación de cambio de configuración y registro	Historial de cambios de configuración de un dispositivo Cisco IOS Utilizar el comando de configuración de notificación de syslog para permitir la generación de mensajes de syslog cuando se realiza un cambio de configuración.	archive log config logging enable logging size 200 hidekeys notify syslog	
		Backup de configuracion	Se debe realizar un Backup completo del equipo por parte de los administradores del mismo	Realizar un backup completo del equipo y guardarlo en un lugar seguro	

ANEXO 12

CHECKLIST– HARDENING CISCO IOS - Software release minimo12.4 (2) o superior

EQUIPO:			
DIRECCIÓN IP:		FECHA:	
FUNCIÓN DEL EQUIPO		HORA:	
RESPONSABLE EQUIPO		DURACIÓN:	
VERSION IOS INSTALADA			

Tema: **3. Datos**

Ejecutada	*Exitosa*	*Parámetro / Componente*	*Valor o cambio a implantar*	*Procedimiento para su implantación*	*Observación*
		Unicast RPF	Permite que un dispositivo verifique que la dirección de origen de un paquete reenviado se pueda alcanzar a través de la interfaz que recibió el paquete	interface <interface> ip verify unicast source reachable-via <mode>	
		Seguridad de IP origen	Prevención de suplantación de identidad	ip dhcp snooping ip dhcp snooping vlan <vlan-range> Después de que la inspección DHCP está habilitada, estos comandos habilitan IPSG: interface <interface-id> ip verify source	
		Seguridad de Puerto	Mitigar la suplantación de direcciones MAC en la interfaz de acceso	interface <interface> switchport switchport mode access switchport port-security switchport port-security mac-address sticky switchport port-security maximum <number> switchport port-security violation <violation-mode>	
		Inspección dinámica de ARP	Mitigar los ataques de envenenamiento por ARP en segmentos locales	ip dhcp snooping ip dhcp snooping vlan <vlan-range> ip arp inspection vlan <rango-vlan>	
		Anti-Spoofing ACL	La suplantación de identidad se puede minimizar en el tráfico que se origina en la red local si aplica ACL salientes que limitan el tráfico a direcciones locales válidas	ip access-list extended ACL-ANTISPOOF-IN deny ip <IP> 0.255.255.255 any deny ip <IP> 0.0.255.255 any ! interface <interface> ip access-group ACL-ANTISPOOF-IN in	

https://www.networkstraining.com/cisco-router-switch-security-configuration-guide/

https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html#anc38

ANEXO 13

Descripción de Vulnerabilidad en SERVIDORES

100464 - Microsoft Windows SMBv1 Multiple Vulnerabilities
100871 - Microsoft Windows SMB Versions Supported (remote check)
10092 - FTP Server Detection
10107 - HTTP Server Type and Version
10114 - ICMP Timestamp Request Remote Date Disclosure
10144 - Microsoft SQL Server TCP/IP Listener Detection
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure
102431 - HP Data Protector 8.x < 8.17 / 9.x < 9.09 Multiple Vulnerabilities (HPSBGN03732)
10263 - SMTP Server Detection
10267 - SSH Server Type and Version Information
10287 - Traceroute Information
10302 - Web Server robots.txt Information Disclosure
10342 - VNC Software Detection
10386 - Web Server No 404 Error Code Check
10394 - Microsoft Windows SMB Log In Possible
104743 - TLS Version 1.0 Protocol Detection
104887 - Samba Version
106375 - nginx HTTP Server Detection
10658 - Oracle Database tnslsnr Service Remote Version Disclosure
106658 - JQuery Detection
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
10674 - Microsoft SQL Server UDP Query Remote Version Disclosure
10719 - MySQL Server Detection
10736 - DCE Services Enumeration
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
10863 - SSL Certificate Information
108659 - SMTP Host Information in NTLM SSP
108761 - MSSQL Host Information in NTLM SSP
108797 - Unsupported Windows OS (remote)
108804 - Microsoft Exchange Server Detection (Uncredentialed)
10881 - SSH Protocol Versions Supported
10884 - Network Time Protocol (NTP) Server Detection
10919 - Open Port Re-check
10940 - Windows Terminal Services Enabled
11002 - DNS Server Detection
11011 - Microsoft Windows SMB Service Detection
110723 - No Credentials Provided
11153 - Service Detection (HELP Request)
11213 - HTTP TRACE / TRACK Methods Allowed

11219 - Nessus SYN scanner
11422 - Web Server Unconfigured - Default Install Page Present
117530 - Errors in nessusd.dump
117886 - Local Checks Not Enabled (info)
11936 - OS Identification
119766 - PHP 7.2.x < 7.2.13 Multiple vulnerabilities
119833 - Dell iDRAC Products Multiple Vulnerabilities (December 2018)
12053 - Host Fully Qualified Domain Name (FQDN) Resolution
121010 - TLS Version 1.1 Protocol Detection
121353 - PHP 7.2.x < 7.2.14 Multiple vulnerabilities.
121355 - Apache 2.4.x < 2.4.38 Multiple Vulnerabilities
121385 - OpenSSL 1.1.1 < 1.1.1a Multiple Vulnerabilities
121479 - web.config File Information Disclosure
121516 - JBoss Remoting Detection
122187 - iLO 3 < 1.88 / iLO 4 < 2.44 XSS Vulnerability
122188 - iLO 3 < 1.65 / iLO 4 < 1.32 Multiple Vulnerabilities
122191 - iLO 3 < 1.85 / iLO 4 < 2.22 Denial of Service Vulnerability
122244 - iLO 3 < 1.88 Information Disclosure Vulnerability
123642 - Apache 2.4.x < 2.4.39 Multiple Vulnerabilities
123754 - PHP 7.2.x < 7.2.17 Multiple vulnerabilities.
123828 - PHP 7.2.x < 7.2.16 Multiple vulnerabilities.
124410 - SSL Root Certification Authority Distrusted
124763 - PHP 7.2.x < 7.2.18 Heap-based Buffer Overflow Vulnerability.
125313 - Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
125639 - PHP 7.2.x < 7.2.19 Multiple Vulnerabilities.
125641 - OpenSSL 1.1.1 < 1.1.1c Vulnerability
127131 - PHP 7.2.x < 7.2.21 Multiple Vulnerabilities.
128033 - Apache 2.4.x < 2.4.41 Multiple Vulnerabilities
128116 - OpenSSL 1.1.1 < 1.1.1d Multiple Vulnerabilities
128148 - Flexera FlexNet Publisher < 11.16.2 Multiple Vulnerabilities
128531 - PHP 7.3.x < 7.3.9 Multiple Vulnerabilities.
129557 - PHP 7.3.x < 7.3.10 Heap-Based Buffer Overflow Vulnerability.
130276 - PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
131730 - Dell iDRAC Improper Authorization (DSA-2019-137)
132725 - OpenSSL 1.1.1 < 1.1.1e-dev Procedure Overflow Vulnerability
134944 - PHP 7.3.x < 7.3.16 Multiple Vulnerabilities
134976 - iLO 3 < 1.90 / iLO 4 < 2.61 / iLO 5 < 1.35 Remote Code Execution Vulnerability (HPESBHF03866)
135187 - Dell iDRAC Buffer Overflow Vulnerability (CVE-2020-5344)
135290 - Apache 2.4.x < 2.4.42 Multiple Vulnerabilities
135860 - WMI Not Available
14255 - Microsoft Outlook Web Access (OWA) Version Detection
14773 - Service Detection: 3 ASCII Digit Code Responses
15901 - SSL Certificate Expiry

17975 - Service Detection (GET request)
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
19506 - Nessus Scan Information
19601 - HP Data Protector Detection
19689 - Embedded Web Server Detection
20007 - SSL Version 2 and 3 Protocol Detection
20094 - VMware Virtual Machine Detection
20285 - HP Integrated Lights-Out (iLO) Detection
20870 - LDAP Server Detection
21642 - Session Initiation Protocol Detection
21643 - SSL Cipher Suites Supported
22073 - Oracle Database Detection
22319 - MSRPC Service Detection
22964 - Service Detection
24242 - Microsoft .NET Handlers Enumeration
24260 - HyperText Transfer Protocol (HTTP) Information
24786 - Nessus Windows Scan Not Performed with Admin Privileges
25220 - TCP/IP Timestamps Supported
25701 - LDAP Crafted Search Request Server Information Disclosure
26024 - PostgreSQL Server Detection
26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
26928 - SSL Weak Cipher Suites Supported
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant
32318 - Web Site Cross-Domain Policy File Detection
33850 - Unix Operating System Unsupported Version Detection
35043 - PHP 5 < 5.2.7 Multiple Vulnerabilities
35067 - PHP < 5.2.8 Multiple Vulnerabilities
35291 - SSL Certificate Signed Using Weak Hashing Algorithm
35297 - SSL Service Requests Client Certificate
35372 - DNS Server Dynamic Update Record Injection
35716 - Ethernet Card Manufacturer Detection
35750 - PHP < 5.2.9 Multiple Vulnerabilities
38157 - Microsoft SharePoint Server Detection
39480 - PHP < 5.2.10 Multiple Vulnerabilities
39520 - Backported Security Patch Detection (SSH)
39521 - Backported Security Patch Detection (WWW)
41014 - PHP < 5.2.11 Multiple Vulnerabilities
42088 - SMTP Service STARTTLS Command Support
42149 - FTP Service AUTH TLS Command Support
42336 - AlienVault OSSIM Web Front End Detection
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
42822 - Strict Transport Security (STS) Detection
42823 - Non-compliant Strict Transport Security (STS)

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
42981 - SSL Certificate Expiry - Future Expiry
43111 - HTTP Methods Allowed (per directory)
43351 - PHP < 5.2.12 Multiple Vulnerabilities
43815 - NetBIOS Multiple IP Address Enumeration
43829 - Kerberos Information Disclosure
44921 - PHP < 5.3.2 / 5.2.13 Multiple Vulnerabilities
45410 - SSL Certificate 'commonName' Mismatch
45411 - SSL Certificate with Wrong Hostname
45590 - Common Platform Enumeration (CPE)
46180 - Additional DNS Hostnames
46215 - Inconsistent Hostname and IP Address
48204 - Apache HTTP Server Version
48243 - PHP Version Detection
48244 - PHP 5.2 < 5.2.14 Multiple Vulnerabilities
50350 - OS Identification Failed
50845 - OpenSSL Detection
51139 - PHP 5.2 < 5.2.15 Multiple Vulnerabilities
51185 - Dell Integrated Remote Access Controller (iDRAC) Detection
51192 - SSL Certificate Cannot Be Trusted
51439 - PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS
51891 - SSL Session Resume Supported
53641 - HP Data Protector Remote Command Execution
54580 - SMTP Authentication Methods
54615 - Device Type
56984 - SSL / TLS Versions Supported
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported
57323 - OpenSSL Version Detection
57537 - PHP < 5.3.9 Multiple Vulnerabilities
57582 - SSL Self-Signed Certificate
57608 - SMB Signing not required
57690 - Terminal Services Encryption Level is Medium or Low
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only
58966 - PHP < 5.3.11 Multiple Vulnerabilities
58987 - PHP Unsupported Version Detection
58988 - PHP < 5.3.12 / 5.4.2 CGI Query String Code Execution
59861 - Remote web server screenshot
62564 - TLS Next Protocols Supported
64814 - Terminal Services Use SSL/TLS
65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
66173 - RDP Screenshot
66318 - McAfee ePolicy Orchestrator Application Server Detection
66334 - Patch Report

67121 - HP Data Protector Components Version Detection
69482 - Microsoft SQL Server STARTTLS Support
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
69552 - Oracle TNS Listener Remote Poisoning
70544 - SSL Cipher Block Chaining Cipher Suites Supported
70657 - SSH Algorithms and Languages Supported
70658 - SSH Server CBC Mode Ciphers Enabled
71049 - SSH Weak MAC Algorithms Enabled
73289 - PHP PHP_RSHUTDOWN_FUNCTION Security Bypass
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
79233 - HP Data Protector 'EXEC_INTEGUTIL' Arbitrary Command Execution
79638 - MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)
81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
83298 - SSL Certificate Chain Contains Certificates Expiring Soon
83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
84047 - Hyper-V Virtual Machine Detection
84502 - HSTS Missing From HTTPS Server
84574 - Backported Security Patch Detection (PHP)
84821 - TLS ALPN Supported Protocol Enumeration
86420 - Ethernet MAC Addresses
87242 - TLS NPN Supported Protocol Enumeration
89058 - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
90151 - Flexera FlexNet Publisher Detection
90317 - SSH Weak Algorithms Supported
90510 - MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
90591 - Cisco Prime Infrastructure Detection
94761 - SSL Root Certification Authority Certificate Information
95631 - SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Descripción de Vulnerabilidad en ADMINISTRACIÓN

100871 - Microsoft Windows SMB Versions Supported (remote check)
10107 - HTTP Server Type and Version
10114 - ICMP Timestamp Request Remote Date Disclosure
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure
10267 - SSH Server Type and Version Information
10281 - Telnet Server Detection
10287 - Traceroute Information
10302 - Web Server robots.txt Information Disclosure
104743 - TLS Version 1.0 Protocol Detection
105161 - Cisco Smart Install Detection
10550 - SNMP Query Running Process List Disclosure
10551 - SNMP Request Network Interfaces Enumeration
106628 - lighttpd HTTP Server Detection
106658 - JQuery Detection
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
10736 - DCE Services Enumeration
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
10800 - SNMP Query System Information Disclosure
10863 - SSL Certificate Information
10881 - SSH Protocol Versions Supported
10884 - Network Time Protocol (NTP) Server Detection
10940 - Windows Terminal Services Enabled
11011 - Microsoft Windows SMB Service Detection
110723 - No Credentials Provided
11154 - Unknown Service Detection: Banner Retrieval
11219 - Nessus SYN scanner
117530 - Errors in nessusd.dump
117886 - Local Checks Not Enabled (info)
11936 - OS Identification
12053 - Host Fully Qualified Domain Name (FQDN) Resolution
121010 - TLS Version 1.1 Protocol Detection
12218 - mDNS Detection (Remote Network)
130208 - Cisco Wireless LAN Controller Secure Shell (SSH) Denial of Service Vulnerability (cisco-sa-20191016-wlc-ssh-dos)
130259 - Cisco Wireless LAN Controller Path Traversal Vulnerability
131230 - Cisco Wireless LAN Controller HTTP Parsing Engine Denial of Service Vulnerability
14274 - Nessus SNMP Scanner
15901 - SSL Certificate Expiry
17367 - Fortinet FortiGate Web Console Management Detection
19506 - Nessus Scan Information
19592 - OpenSSH < 4.2 Multiple Vulnerabilities
19689 - Embedded Web Server Detection
20007 - SSL Version 2 and 3 Protocol Detection

21643 - SSL Cipher Suites Supported
22964 - Service Detection
24260 - HyperText Transfer Protocol (HTTP) Information
25220 - TCP/IP Timestamps Supported
26928 - SSL Weak Cipher Suites Supported
31422 - Reverse NAT/Intercepting Proxy Detection
31737 - OpenSSH X11 Forwarding Session Hijacking
34022 - SNMP Query Routing Information Disclosure
35291 - SSL Certificate Signed Using Weak Hashing Algorithm
35296 - SNMP Protocol Version Detection
35297 - SSL Service Requests Client Certificate
35716 - Ethernet Card Manufacturer Detection
39520 - Backported Security Patch Detection (SSH)
40448 - SNMP Supported Protocols Detection
41028 - SNMP Agent Default Community Name (public)
42263 - Unencrypted Telnet Server
42822 - Strict Transport Security (STS) Detection
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
42981 - SSL Certificate Expiry - Future Expiry
43111 - HTTP Methods Allowed (per directory)
43815 - NetBIOS Multiple IP Address Enumeration
44065 - OpenSSH < 5.2 CBC Plaintext Disclosure
44075 - OpenSSH < 4.0 known_hosts Plaintext Host Information Disclosure
44076 - OpenSSH < 4.3 scp Command Line Filename Processing Command Injection
44077 - OpenSSH < 4.5 Multiple Vulnerabilities
44078 - OpenSSH < 4.7 Trusted X11 Cookie Connection Policy Bypass
44079 - OpenSSH < 4.9 'ForceCommand' Directive Bypass
44080 - OpenSSH X11UseLocalhost X11 Forwarding Port Hijacking
45590 - Common Platform Enumeration (CPE)
48204 - Apache HTTP Server Version
50845 - OpenSSL Detection
51192 - SSL Certificate Cannot Be Trusted
51891 - SSL Session Resume Supported
53841 - Portable OpenSSH ssh-keysign ssh-rand-helper Utility File Descriptor Leak Local Information Disclosure
54615 - Device Type
56984 - SSL / TLS Versions Supported
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported
57582 - SSL Self-Signed Certificate
57608 - SMB Signing not required
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only
59861 - Remote web server screenshot
60108 - SSL Certificate Chain Contains Weak RSA Keys
64814 - Terminal Services Use SSL/TLS

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
66173 - RDP Screenshot
66334 - Patch Report
66848 - SSL Null Cipher Suites Supported
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
70122 - Cisco Wireless LAN Controller (WLC) Version
70544 - SSL Cipher Block Chaining Cipher Suites Supported
70657 - SSH Algorithms and Languages Supported
70658 - SSH Server CBC Mode Ciphers Enabled
71049 - SSH Weak MAC Algorithms Enabled
76474 - SNMP 'GETBULK' Reflection DDoS
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
83298 - SSL Certificate Chain Contains Certificates Expiring Soon
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
84502 - HSTS Missing From HTTPS Server
86420 - Ethernet MAC Addresses
90317 - SSH Weak Algorithms Supported
91486 - Wireless Access Controller Detection
91572 - OpenSSL AES-NI Padding Oracle MitM Information Disclosure
94761 - SSL Root Certification Authority Certificate Information
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
97861 - Network Time Protocol (NTP) Mode 6 Scanner

Descripción de Vulnerabilidad en SERVIDORES DE TELEFONIA

100871 - Microsoft Windows SMB Versions Supported (remote check)
10092 - FTP Server Detection
10107 - HTTP Server Type and Version
10114 - ICMP Timestamp Request Remote Date Disclosure
10144 - Microsoft SQL Server TCP/IP Listener Detection
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure
10267 - SSH Server Type and Version Information
10287 - Traceroute Information
10386 - Web Server No 404 Error Code Check
10394 - Microsoft Windows SMB Log In Possible
104743 - TLS Version 1.0 Protocol Detection
105486 - ESXi 5.5 / 6.0 / 6.5 / Multiple Vulnerabilities (VMSA-2017-0021) (VMSA-2018-0002) (Spectre) (remote check)
105614 - ESXi 6.5 < Build 6765664 Heap Buffer Overflow (VMSA-2017-0021) (remote check)
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
10674 - Microsoft SQL Server UDP Query Remote Version Disclosure
10736 - DCE Services Enumeration
10785 - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
10863 - SSL Certificate Information
108761 - MSSQL Host Information in NTLM SSP
10881 - SSH Protocol Versions Supported
10884 - Network Time Protocol (NTP) Server Detection
10940 - Windows Terminal Services Enabled
11011 - Microsoft Windows SMB Service Detection
110723 - No Credentials Provided
11154 - Unknown Service Detection: Banner Retrieval
111759 - ESXi 5.5 / 6.0 / 6.5 / 6.7 Speculative Execution Side Channel Vulnerability (Foreshadow) (VMSA-2018-0020) (remote ch
11219 - Nessus SYN scanner
11422 - Web Server Unconfigured - Default Install Page Present
117530 - Errors in nessusd.dump
117886 - Local Checks Not Enabled (info)
11819 - TFTP Daemon Detection
118466 - ESXi 6.0 / 6.5 / 6.7 Out-of-Bounds Read Vulnerability (VMSA-2018-0026) (Remote Check)
118885 - ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2018-0027) (Remote Check)
11935 - IPSEC Internet Key Exchange (IKE) Version 1 Detection
11936 - OS Identification
121010 - TLS Version 1.1 Protocol Detection
123518 - ESXi 6.0 / 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2019-0005) (Remote Check)
134878 - VMware ESXi 5.5 / 6.0 / 6.5 / 6.7 DoS (VMSA-2018-0018) (remote check)
135860 - WMI Not Available
15901 - SSL Certificate Expiry
16321 - 3Com 3CServer/3CDaemon FTP Server Multiple Vulnerabilities (OF, FS, PD, DoS)
17975 - Service Detection (GET request)

18261 - Apache Banner Linux Distribution Disclosure
18405 - Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
19506 - Nessus Scan Information
19689 - Embedded Web Server Detection
20007 - SSL Version 2 and 3 Protocol Detection
20301 - VMware ESX/GSX Server detection
21642 - Session Initiation Protocol Detection
21643 - SSL Cipher Suites Supported
22964 - Service Detection
23777 - SLP Server Detection (TCP)
23778 - SLP Server Detection (UDP)
24260 - HyperText Transfer Protocol (HTTP) Information
24786 - Nessus Windows Scan Not Performed with Admin Privileges
25220 - TCP/IP Timestamps Supported
26917 - Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
30218 - Terminal Services Encryption Level is not FIPS-140 Compliant
33850 - Unix Operating System Unsupported Version Detection
35291 - SSL Certificate Signed Using Weak Hashing Algorithm
35297 - SSL Service Requests Client Certificate
39446 - Apache Tomcat Detection
39520 - Backported Security Patch Detection (SSH)
39521 - Backported Security Patch Detection (WWW)
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
43111 - HTTP Methods Allowed (per directory)
43815 - NetBIOS Multiple IP Address Enumeration
45410 - SSL Certificate 'commonName' Mismatch
45411 - SSL Certificate with Wrong Hostname
45590 - Common Platform Enumeration (CPE)
48204 - Apache HTTP Server Version
50845 - OpenSSL Detection
51192 - SSL Certificate Cannot Be Trusted
51891 - SSL Session Resume Supported
54615 - Device Type
56984 - SSL / TLS Versions Supported
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported
57396 - VMware vSphere Detect
57582 - SSL Self-Signed Certificate
57608 - SMB Signing not required
57690 - Terminal Services Encryption Level is Medium or Low
58453 - Terminal Services Doesn't Use Network Level Authentication (NLA) Only
62695 - IPSEC Internet Key Exchange (IKE) Version 2 Detection
64814 - Terminal Services Use SSL/TLS

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
66173 - RDP Screenshot
69482 - Microsoft SQL Server STARTTLS Support
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
70544 - SSL Cipher Block Chaining Cipher Suites Supported
70657 - SSH Algorithms and Languages Supported
70658 - SSH Server CBC Mode Ciphers Enabled
71049 - SSH Weak MAC Algorithms Enabled
78479 - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
83875 - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
84502 - HSTS Missing From HTTPS Server
91263 - SSL/TLS Service Requires Client Certificate
94761 - SSL Root Certification Authority Certificate Information
96982 - Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
97861 - Network Time Protocol (NTP) Mode 6 Scanner

Descripción de Vulnerabilidad en IMPRESORAS

100871 - Microsoft Windows SMB Versions Supported (remote check)
10107 - HTTP Server Type and Version
10114 - ICMP Timestamp Request Remote Date Disclosure
10150 - Windows NetBIOS / SMB Remote Host Information Disclosure
10267 - SSH Server Type and Version Information
10287 - Traceroute Information
104743 - TLS Version 1.0 Protocol Detection
106716 - Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
10736 - DCE Services Enumeration
10863 - SSL Certificate Information
10881 - SSH Protocol Versions Supported
10884 - Network Time Protocol (NTP) Server Detection
10940 - Windows Terminal Services Enabled
11011 - Microsoft Windows SMB Service Detection
110723 - No Credentials Provided
11219 - Nessus SYN scanner
117886 - Local Checks Not Enabled (info)
11933 - Do not scan printers
11936 - OS Identification
12053 - Host Fully Qualified Domain Name (FQDN) Resolution
121010 - TLS Version 1.1 Protocol Detection
135860 - WMI Not Available
14274 - Nessus SNMP Scanner
17975 - Service Detection (GET request)
19506 - Nessus Scan Information
19689 - Embedded Web Server Detection
20007 - SSL Version 2 and 3 Protocol Detection
21642 - Session Initiation Protocol Detection
21643 - SSL Cipher Suites Supported
22964 - Service Detection
24260 - HyperText Transfer Protocol (HTTP) Information
35291 - SSL Certificate Signed Using Weak Hashing Algorithm
42410 - Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
43111 - HTTP Methods Allowed (per directory)
45410 - SSL Certificate 'commonName' Mismatch
45411 - SSL Certificate with Wrong Hostname
45590 - Common Platform Enumeration (CPE)
46180 - Additional DNS Hostnames
46215 - Inconsistent Hostname and IP Address
50845 - OpenSSL Detection
51192 - SSL Certificate Cannot Be Trusted

51891 - SSL Session Resume Supported
54615 - Device Type
56984 - SSL / TLS Versions Supported
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported
57582 - SSL Self-Signed Certificate
57608 - SMB Signing not required
64814 - Terminal Services Use SSL/TLS
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
70544 - SSL Cipher Block Chaining Cipher Suites Supported
70657 - SSH Algorithms and Languages Supported
70658 - SSH Server CBC Mode Ciphers Enabled
71049 - SSH Weak MAC Algorithms Enabled
84502 - HSTS Missing From HTTPS Server
97861 - Network Time Protocol (NTP) Mode 6 Scanner

Descripción de Vulnerabilidad en TELEFONOS

10107 - HTTP Server Type and Version
10114 - ICMP Timestamp Request Remote Date Disclosure
10267 - SSH Server Type and Version Information
10287 - Traceroute Information
104743 - TLS Version 1.0 Protocol Detection
10662 - Web mirroring
10863 - SSL Certificate Information
10881 - SSH Protocol Versions Supported
10884 - Network Time Protocol (NTP) Server Detection
10919 - Open Port Re-check
110723 - No Credentials Provided
11219 - Nessus SYN scanner
117530 - Errors in nessusd.dump
117886 - Local Checks Not Enabled (info)
11936 - OS Identification
12053 - Host Fully Qualified Domain Name (FQDN) Resolution
121010 - TLS Version 1.1 Protocol Detection
19506 - Nessus Scan Information
19689 - Embedded Web Server Detection
20007 - SSL Version 2 and 3 Protocol Detection
21642 - Session Initiation Protocol Detection
21643 - SSL Cipher Suites Supported
22964 - Service Detection
24260 - HyperText Transfer Protocol (HTTP) Information
25220 - TCP/IP Timestamps Supported
26928 - SSL Weak Cipher Suites Supported
35291 - SSL Certificate Signed Using Weak Hashing Algorithm
42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)
43111 - HTTP Methods Allowed (per directory)
45410 - SSL Certificate 'commonName' Mismatch
45411 - SSL Certificate with Wrong Hostname
45590 - Common Platform Enumeration (CPE)
46180 - Additional DNS Hostnames
46215 - Inconsistent Hostname and IP Address
50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
50345 - Missing or Permissive X-Frame-Options HTTP Response Header
50845 - OpenSSL Detection
51192 - SSL Certificate Cannot Be Trusted
51891 - SSL Session Resume Supported
54615 - Device Type
56984 - SSL / TLS Versions Supported
57041 - SSL Perfect Forward Secrecy Cipher Suites Supported

65821 - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
69551 - SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
70544 - SSL Cipher Block Chaining Cipher Suites Supported
70657 - SSH Algorithms and Languages Supported
70658 - SSH Server CBC Mode Ciphers Enabled
71049 - SSH Weak MAC Algorithms Enabled
81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
84502 - HSTS Missing From HTTPS Server
91815 - Web Application Sitemap
97861 - Network Time Protocol (NTP) Mode 6 Scanner

ANEXO 14

Probabilidad	Impacto				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Muy Baja	Muy Bajo	Muy Bajo	Bajo	Bajo	Medio
Baja	Muy Bajo	Bajo	Medio	Medio	Alto
Media	Bajo	Medio	Medio	Alto	Alto
Alta	Bajo	Medio	Alto	Alto	Muy Alto
Muy Alta	Medio	Alto	Alto	Muy Alto	Muy Alto

CVE	Descripción	Probabilidad	Impacto	Riesgo
CVE-1999-0517	Es posible obtener el nombre de comunidad del servidor remoto SNMP. Un atacante puede utilizar esta información para conocer más acerca del host o para cambiar alguna configuración del mismo	Alta	Alto	Alto
CVE-2004-2761	El algoritmo MD5 es vulnerable al ataque de colisiones, lo que hace más fácil para el atacante realizar ataques de spoofing	Alta	Medio	Alto
CVE-2005-2797	La versión actual de OpenSSH permite posiblemente habilitar la funcionalidad GatewayPorts cuando no se provee una dirección de escucha. Lo anterior es debido a que OpenSSH no maneja correctamente el reenvío de puertos dinámicos	Alta	Medio	Alto
CVE-2005-2798	La versión actual de OpenSSH permite exponer las credenciales de GSSAPI a usuarios que inicien sesión con un método diferente a la autenticación GSSAPI cuando el GSSAPIDelegateCredentials está habilitado	Alta	Medio	Alto
CVE-2006-0225	La funcionalidad SCP de la versión actual de OpenSSH permite a los atacantes ejecutar comandos arbitrarios por medio de archivos que contengan meta caracteres Shell o espacios	Alta	Medio	Alto
CVE-2006-0393	La versión actual de OpenSSH permite a un atacante realizar denegación de servicio intento iniciar sesión con un usuario inexistente	Baja	Medio	Medio

CVE-2006-4925	El packet.c de SSH en la versión actual de OpenSSH permite a un atacante realizar denegación de servicio enviando secuencias inválidas de protocolo con USERAUTH_SUCCESS antes de NEWKEYS, lo que causa que este parámetro sea nulo	Alta	Medio	Alto
CVE-2006-5794	La versión actual de OpenSSH es afectada por una vulnerabilidad de separación de privilegios, lo que permite a un atacante evitar la autenticación debido a una débil verificación en el proceso	Alta	Alto	Alto
CVE-2007-0726	El proceso de generación de la llave SSH permite a un atacante causar denegación de servicio conectándose al servidor antes que el proceso de las llaves acabe	Alta	Medio	Alto
CVE-2007-2243	La versión actual de OpenSSH permite a un atacante determinar la existencia de cuentas de usuarios intentando autenticarse vía S/KEY, ya que muestra un mensaje diferente cuando la cuenta del usuario existe. Lo anterior pasa cuando ChallengeResponseAuthentication está habilitado	Alta	Medio	Alto
CVE-2007-4752	La versión actual de OpenSSH permite a un atacante adquirir privilegios sobre el dispositivo haciendo que se confía en un cliente extraño. Lo anterior debido a que la versión de SSH no maneja apropiadamente la situación cuando una cookie sin confianza no se puede crear, y en su lugar utiliza una de confianza	Alta	Alto	Alto
CVE-2008-1657	La versión actual de OpenSSH permite a un atacante evitar la directiva ForceCommand de sshd_config modificando el archivo de sesión .ssh/rc	Media	Medio	Medio
CVE-2013-2566	El algoritmo RC4 tiene muchos sesgos de un solo byte, lo que hace más fácil para el atacante perpetrar ataques de recuperación de texto en claro por medio de análisis estático	Media	Medio	Medio

CVE-2015-2808	El equipo soporta el uso de RC4 en sus cifrados. El cifrado RC4 es débil en la generación de bytes aleatorios debido a una gran variedad de pequeños sesgos que se introducen en el flujo	Media	Medio	Medio
CVE-2016-2183	Los algoritmos de cifrado DES y 3DES tienen un límite aproximado de 4 millones de bloques, lo que hace más fácil para el atacante obtener el texto cifrado en claro	Alta	Alto	Alto
CVE-2019-15262	Existe una vulnerabilidad en el manejo de SSH en el software de los WLC de Cisco que permite a un atacante realizar denegación de servicio en el dispositivo afectado. La vulnerabilidad existe porque el proceso SSH no se borra correctamente después de que se desconecta la sesión SSH, y una forma de explotar la vulnerabilidad es abriendo varias sesiones SSH para consumir los recursos de la máquina	Alta	Alto	Alto
CVE-2019-15276	Existe una vulnerabilidad en la interfaz web en el software de los WLC de Cisco que permite a un atacante realizar denegación de servicio en el dispositivo afectado. La vulnerabilidad existe debido a una falla en el motor de análisis de HTTP	Alta	Medio	Alto

ANEXO 15

Situación actual y recomendaciones finales

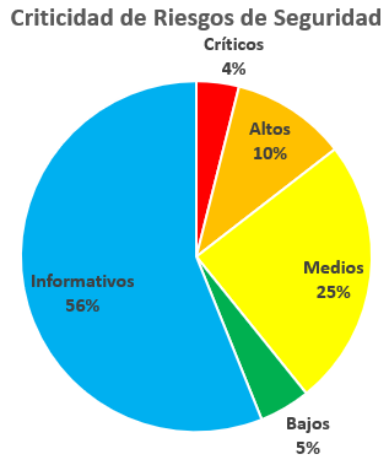
Introducción

Teniendo como base el desarrollo del proyecto **Fortalecimiento del modelo de seguridad de red y control de acceso lógico para una entidad**, y con el objetivo de informar a la entidad los resultados obtenidos y las recomendaciones finales, se realiza este informe como anexo al documento general de planeación y ejecución.

ANÁLISIS DE VULNERABILIDADES:

Los resultados obtenidos no demuestran una red crítica en la seguridad, sin embargo, se recomienda tomar las acciones correctivas establecidas en este documento para evitar posibles ataques en contra de la entidad que pueden poner en riesgo la información y/o la operación de la entidad.

A continuación, se muestra de forma resumida los riegos con más presencia



Riesgo	Recomendación
Sistemas operativos sin soporte.	Actualizar sistema operativo a una versión que tenga soporte.
Aplicaciones afectadas por múltiples vulnerabilidades.	Actualizar las aplicaciones mencionadas en los otros Anexos a sus versiones más recientes.
Certificados SSL vencidos.	Renovar los certificados SSL con su CA.
Falta de actualizaciones de seguridad.	Programar actualizaciones periódicas de los equipos.
Exposición de información sensible.	Mejorar la configuración de encriptación en los equipos.

Adicionalmente, para llevar un mejor registro de lo que tiene la entidad, se sugiere elaborar un completo inventario de software actualmente instalado, con el cual, se pueda llevar a cabo una comparación periódica con las versiones liberadas por fabricantes y desarrolladores. Con esto, se busca mantener la red más segura sin tener tecnología obsoleta y vulnerable.

CONTROL DE ACCESO LÓGICO A LA RED:

La solución de control de acceso permitió el descubrimiento y perfilamiento de los dispositivos, ofreciendo una visibilidad esperada del 100% de los dispositivos conectados bien sea de funcionarios o invitados. Con la finalidad de negarle o permitirle a un dispositivo nuevo conectarse o no a ésta. Otra característica importante en la solución es la revisión de postura, la cual es la que se encarga principalmente de revisar el cumplimiento de los criterios definidos por la administración para permitir, denegar, o poner en cuarentena a determinado dispositivo.
Por lo anterior y con el fin de que el control de acceso se vuelva una herramienta que ayude a la gestión de la seguridad además de que afecta directamente la operación de la red en caso de algún percance en la implementación se muestra el esquema de conexión del usuario final y un plan de comunicaciones para socialización del control de acceso.

Plan de comunicaciones para el control de acceso lógico

Con el fin de facilitar el cumplimiento de los objetivos de este trabajo, se requiere una comunicación efectiva a los clientes internos y externos de la Entidad, manteniendo informados a los funcionarios, grupos de interés y partes interesadas, con la debida oportunidad, claridad y transparencia, sobre la implementación e informando lo que deberían hacer al respecto.

Este es un lineamiento, que de manera general tiene en cuenta, la población objetivo, la prioridad y seguridad del proyecto; y comprende las siguientes etapas:

Con esto se pretende lograr el fortalecimiento de la comunicación y socialización del proyecto con el fin de:

- Comprometer y motivar a los diferentes usuarios
- Mantener informados a los usuarios, sobre los proyectos, los cambios y su impacto en la Entidad.

Costos de Licenciamiento

Por otra parte, con el fin de dar continuidad al control de acceso se cotizo el licenciamiento requerido para los dispositivos en la entidad, el cual se muestra a continuación:

No Parte	Descripción	Cantidad	Valor Unitario	Valor Total
R-ISE-VMS-K9	Cisco ISE Virtual Machine Small	2	$22.280.595,48	$44.561.190,97
L-ISE-BSE-P4	Cisco ISE Base License - Sessions 1000 to 2499	2000	$18.966,98	$37.933.956,36
L-ISE-PLS-1Y-S2	Cisco ISE Plus License, 1Y, 250 - 499 Sessions	320	$27.911,63	$8.931.722,45
CON-ECMU-RISEV9SM	SWSS UPGRADES Cisco ISE Virtual Machine Small	2	$5.566.323,15	$11.132.646,29
Total				**$102.559.516,08**