ANÁLISIS DE CIBERSEGURIDAD PARA UNA EMPRESA DE EDUCACIÓN VIRTUAL.

PRESENTADO POR:
JUAN PABLO ANGEL ESPEJO
CRISTIAN ARLEY BERNAL REINOSO
MARÍA ALEJANDRA SEGURA GRECO

ASESOR TÉCNICO DE PROYECTO:
MSc. EDUARDO CHAVARRO OVALLE

UNIVERSIDAD EL BOSQUE
FACULTAD DE INGENIERÍA ELECTRÓNICA
ESPECIALIZACIÓN EN SEGURIDAD DE REDES TELEMÁTICAS
BOGOTÁ, COLOMBIA
13/01/2020

A Dios por permitirnos desarrollar el proyecto sin contratiempos,
a nuestros padres por habernos enseñado el don de la ética y los valores,
a nuestras parejas por condescender en los tiempos que no se compartió a su lado,
a nuestros profesores por transmitir sus conocimientos sin recelo alguno,
y a nuestros compañeros quienes nos asistieron y batallaron a nuestro lado.

Agradecimientos

Desde que iniciamos a desarrollar el presente trabajo, muchas personas nos han proporcionado una ayuda inestimable y nos han influido dando forma a nuestras ideas sobre cómo organizar y llevar a feliz término este proyecto. MUCHAS GRACIAS a todos aquellos que abnegada e incondicionalmente han colocado su grano de arena. Gracias especiales a:

Camilo León Alcázar
Nasly Alcázar Castillo
Andrés Felipe Mendoza

Por último, queremos emitir un agradecimiento al Ingeniero Eduardo Chavarro Ovalle, nuestro Director de Proyecto, quien gracias a su asesoría técnica, imparcial y permanente, a los conocimientos brindados y transmitidos con arrojo y voluntad, y a su acompañamiento inconmensurable, fue posible lograr un resultado tácito e implícito.

RESUMEN

El crecimiento que ha tenido la empresa y sus aliados la ha llevado a identificar que es necesario evaluar la seguridad de los recursos informáticos y digitales de la compañía, y a su vez, que las políticas de seguridad creadas en un comienzo ya no hacen un cubrimiento actual de sus necesidades.

"La Compañía Training and Education" ha crecido en funciones, en información y en usuarios lo que la lleva a la necesidad de poder brindar sus servicios con seguridad a sus Y Aliados y así mismo a sus usuarios finales.

El presente trabajo de grado tiene como objetivo presentar el estudio de seguridad informática realizado a la empresa "La Compañía / Y Aliados" en el marco de la Especialización en Seguridad de Redes Telemáticas en la universidad El Bosque sede Bogotá.

El estudio de seguridad informática realizado a la empresa, incluyó la realización de pruebas de identificación y análisis de vulnerabilidad a equipos de cómputo, de red, web institucional, conexión a base de datos de clientes, análisis de seguridad física y la verificación de las políticas de seguridad de la información existentes.

El objetivo fue realizar el análisis de tal manera que permitiera a la empresa definir y visualizar cuál era el estado de sus activos informáticos y de información de manera que pudiese posteriormente y por medio del informe entregado, definir un plan de trabajo para mitigar los riesgos que arrojaron los estudios y las pruebas ejecutadas.

PALABRAS CLAVE

Seguridad informática, redes de computadores, Crimen computacional, control de acceso, amenazas, vulnerabilidades.

ABSTRACT

The growth of the company "La Compañía / Y Aliados" has led them to identify that it is necessary to evaluate the security of the company's computer and digital resources. The security policies created for the company are old and no longer make a current coverage of their needs.

"La Compañía" has grown in functions, in information and in users, which leads it to the need to be able to provide its services with security to its allies and also to its end users.

The purpose of this project is to present the computer security tests and analysis study carried out to the company "La Compañía / Y Aliados" in the framework of the Specialization in Telematics Network Security at El Bosque University.

The computer security study conducted to the company included the performance of Vulnerability Assessment to computer equipment, network, and institutional web, connection to customer database, physical security analysis and verification of the security policies of the existing information.

The objective was to carry out the analysis in such a way that it allowed the company to define and visualize the status of its IT assets and information so that it could subsequently and through the report delivered, to define out a work plan to mitigate the risks that threw the studies and the tests carried out.

KEYWORDS

Cyber-security, computer networks, Computer Crime, Access control, threats, vulnerabilities.

Tabla de contenido

Índice de Tablas

Índice de Figuras

1. Título.

ANÁLISIS DE CIBERSEGURIDAD PARA UNA EMPRESA DE EDUCACIÓN VIRTUAL.

2. Introducción.

En los últimos años se han incrementado los ciberataques a las diferentes empresas y fundamentalmente a las pymes. Este es el caso de la empresa involucrada en este proyecto "La Compañía / Y Aliados Educación". Este tipo de empresas, son un claro objetivo para los ciber-delincuentes, ya que disponen de menos recursos para protegerse y por tanto las convierten en compañías más vulnerables a un ataque informático. Uno de los ataques más habituales en la actualizad, es el denominado "ransomware" o en otras palabras "secuestro de datos"; el ataque consiste fundamentalmente en la encriptación de la información por un ciberdelicuente que impide su acceso y solicita alguna cantidad económica para devolver la información tal y como la empresa la requiere. El acceso se logra abriendo una puerta de entrada a la red de la empresa, la cual suele obtenerse introduciendo un software malicioso (malware), normalmente vía correo electrónico o internet, que infecta el ordenador o dispositivo desde el que se ejecuta. Existen muchos agentes más que podrían ocasionar problemas en la empresa: virus, hackers, errores humanos y proveedores sin conocimiento sobre ciberseguridad, son algunos de ellos.

Por lo anterior, la seguridad en las redes y los computadores se ha convertido en una actividad de primer orden para las empresas que ven en las nuevas tecnologías la herramienta más importante para el desarrollo futuro; las mayores amenazas informáticas para las empresas modernas provienen de la falta de conocimiento al interior de las compañías sobre las causas y las consecuencias de la seguridad en los computadores. Así mismo, se debe tener claro que los riesgos de ciberseguridad no son una cuestión del departamento de IT, sino que deben formar parte de la estrategia general del negocio por su indudable impacto en la sostenibilidad de las organizaciones; desde esta perspectiva, el análisis de los riesgos de ciberseguridad debe realizarse de manera que sea un tema dentro de los comités de dirección, y formar parte de la matriz global de riesgos de las compañías. Resulta esencial evaluar de forma pormenorizada los riesgos por área: sistemas, funciones, personal, legal, activos, etc., así como los objetivos que se pretenden alcanzar para tomar decisiones sobre qué, donde, y en qué medida destinar los recursos para su mitigación, y por supuesto, realizar un seguimiento continuo de los mismos.

Partiendo de la premisa que indica que la seguridad absoluta no existe, las decisiones estratégicas generadas del análisis a realizar en este proyecto deberán ir enfocadas a priorizar aquellos riesgos que por su probabilidad de ocurrencia y nivel de impacto podrían hacer más daño al negocio, centrando la mayor parte de los recursos disponibles en "¿cómo mitigarlos?".

El nombre y las direcciones IP de la compañía(s) han sido cambiados con el fin de mantener la confidencialidad de información de la misma. Sin embargo, se aclara que las pruebas y la información descrita en este trabajo son reales.

3. Descripción general del proyecto.

3.1. Definición del problema.

3.1.1. Manifestación.

El crecimiento que ha tenido la empresa la ha llevado a identificar que es necesario evaluar la seguridad de los recursos informáticos y digitales de la compañía, y a su vez que las políticas de seguridad creadas en un comienzo ya no hacen un cubrimiento actual de las necesidades de la compañía. *"La Compañía"* ha crecido en funciones, en información y en usuarios lo que la lleva a la necesidad de poder brindar sus servicios con seguridad a sus Aliados y así mismo, a sus usuarios finales.

Para entender el funcionamiento de la empresa a continuación se describen las plataformas tecnológicas con las que cuenta y otros datos generales que permitirán ver los diferentes enfoques que puede manejar este proyecto para el análisis correspondiente de ciberseguridad, las respuestas se dan orientados hacia "LA COMPAÑÍA.COM.CO" el cual es el sitio web que el usuario final requiere para tomar sus clases ("Core" de negocio) en "LA COMPAÑÍA.ACADEMY".

<u>Plataforma:</u>

- La página web y la plataforma educativa de la organización hacen parte del "Core" del negocio de La Compañía, razón por la cual, es de vital importancia hacer el análisis necesario que permita determinar si los activos de conocimiento (información) del negocio está siendo gestionado y asegurado de manera adecuada.

- La plataforma "LA COMPAÑÍA.ACADEMY" maneja certificados y "OFFICE 365" de "Microsoft" el cual es el proveedor encargado del manejo de los archivos y seguridad de los mismos (todo se encuentra alojado en la nube).

- La plataforma es accesible a nivel mundial, pero solo se maneja el idioma en español para los cursos. Para LA COMPAÑÍA.ACADEMY y OFFICE 365 se maneja una disponibilidad de multi idiomas en la plataforma, pero los cursos están diseñados 100% en español.

- La Compañía se encarga de desarrollar todo el contenido de los cursos y la información interna la brinda el cliente/aliado interesado. Es requerido definir la mejor manera de asegurar esta información.

- Se maneja una disponibilidad de 24/7 durante todo el año.

Conexión a base de datos de Y Aliados Educación:

- La Compañía cuenta con acceso a la base de datos de usuarios educativos de cursos presenciales y virtuales de Y Aliados.

Políticas de seguridad de la información:

- Se cuenta con políticas de seguridad generadas durante la creación de la empresa. Estas no han sido actualizadas.

- Las políticas de información requieren de una revisión y nueva aprobación que permita establecer el marco actual de los procesos de las compañías La Compañía / Y Aliados.

Otra información:

- No existen acuerdos de confidencialidad.

- No se tienen diagramas de la estructura de cómo funciona la solución.

- Se puede pagar en línea, mediante un botón de PayU.

- La certificación de los cursos es por tiempo variable. La certificación en salud tiene una validez de 2 años. Al momento de vencer esta certificación uno de sus colaboradores se comunica con el estudiante informándole y ofertando la nueva certificación.

- Tanto Y Aliados como La Compañía cuentan con sus respectivas campañas de venta. La mayoría de clientes que Y Aliados consigue, son egresados a los que en sus trabajos les exigen estas certificaciones relacionadas con temas salud para trabajar. Los clientes que capta La Compañía provienen de campañas de fb ads, Google ads, y tele mercadeo.

3.1.2. Contexto.

La Compañía Training and Education, nace en el año 2017 como un emprendimiento de dos jóvenes ingenieros, cansados de la oferta actual de cursos virtuales (para el sector salud como *"Core"* de negocio), donde la mayoría de los casos cuentan con plataformas confusas y complicadas para el aprendizaje, sumado a esto la baja calidad de los contenidos: Solo lecturas, y links a videos públicos en la web; este cambio se plantea logrando una total inmersión del estudiante, por medio de contenidos dinámicos e interactivos, los cuales brindaran la sensación al aprendiz de estar en un aula de clase, con la ventaja de poder manejar su tiempo y ritmo de aprendizaje (todo esto desarrollado desde una moderna e intuitiva plataforma). En busca de garantizar la más alta calidad de los contenidos educativos se gestó una alianza con Y Aliados Institución de Educación para el Trabajo y Desarrollo Humano, líder del segmento de educación técnica en Bogotá, con más de 24 años de experiencia.

El presente trabajo se enfocará en asistir a La Compañía / Y Aliados Educación en realizar un análisis de los aspectos tecnológicos que se consideren más importantes para la alianza y así determinar que vulnerabilidades puede tener la misma en aspectos de seguridad de la información, y a su vez determinar cuáles son los pasos a seguir con el fin lograr asegurar sus activos físicos y lógicos que involucran la información del negocio de la organización.

La empresa tiene pendiente brindar información de ¿Cuantos estudiantes son?", ¿Cuantas personas en el área administrativa?", ¿hay dominio de red?, ¿cuenta con claridad de los activos informáticos de la compañía? ¿Los equipos cuentan con una hoja de vida con trazabilidad de mantenimientos y actualizaciones de hardware y software?

De manera previa a la realización del levantamiento, a continuación se describen los principales activos tecnológicos de la empresa:

Plataforma:

- La plataforma "LA COMPAÑÍA.ACADEMY" maneja certificados y "OFFICE 365" de "Microsoft" el cual es el proveedor encargado del manejo de los archivos y seguridad de los mismos (todo está en la nube).
    - El "Hosting" de la página está alojado en "Digital Ocean".
    - La plataforma de cursos (La Compañía Academy) es un re-direccionamiento de la página principal, la cual está sobre (Talent LMS – en AWS).

- Se tiene un proveedor adicional para realizar backups periódicamente (Digital Ocean para LA COMPAÑÍA.COM.CO y TalentLMS para LA COMPAÑÍA.ACADEMY).

- La Compañía se encarga de desarrollar todo el contenido de los cursos y la información interna la brinda el cliente/aliado interesado. Se requiere asegurar su custodia corporativa.

Infraestructura:

- Se cuenta con una red de área local con 46 máquinas en la sede principal (computadores).

Conexión a base de datos de Y Aliados Educación:

- La Compañía cuenta con acceso a la base de datos de usuarios educativos de cursos presenciales y virtuales de Y Aliados. Esta base de datos está montada en una plataforma llamada Q10.

Seguridad física de las instalaciones sede F:

- Basados y más que todo apoyados en normativa ISO 27001 se realizará un análisis de amenazas, riesgos de la seguridad física de la sede con el fin de mitigar y controlar vulnerabilidades que la compañía pueda presentar y de esta manera evitar posible fuga, modificación o indisponibilidad de la información de la alianza La Compañía / Y Aliados.

Políticas de seguridad de la información:

- La Compañía / Y Aliados cuentan con políticas de información las cuales requieren de una revisión y nueva aprobación que permita establecer el marco actual de los procesos de las compañías La Compañía / Y Aliados.

3.1.2.1. Información de acceso a plataforma.

- Se manejan diferentes roles para entrar al sistema: administrador, usuario, y profesor. Cada uno de estos roles tiene permisos diferentes y no pueden ver ni ejecutar el mismo contenido.

- Cada curso tiene una serie de tareas llamadas trabajos autónomos, foros, cuestionarios llamadas evidencias de aprendizajes adquiridos y taller presencial (no todos los cursos tiene taller presencial). La nota definitiva se da por el promedio de estas notas. Se califica de 0-100, siendo 70% la nota mínima de aprobación. Una vez culminado el curso el estudiante ingresa a la plataforma y descarga su certificación en PDF.

- Cada certificación contiene un código único alfanumérico de 16 caracteres lo cual permite verificar la validez del certificado. (Por el momento solo se realiza solicitando dicho certificado al correo indicado en la compañía).

3.1.3. Causas.

Este proyecto se plantea y ejecuta dada la necesidad de solucionar los siguientes aspectos:

- Las políticas de seguridad no cubren el actual entorno del servicio prestado por la empresa.

- No se cuenta con diagramas del funcionamiento tecnológico de la organización.

- No se cuenta con acuerdos de confidencialidad.

- No se cuenta con un esquema de aseguramiento de la Información desarrollada para los cursos.

- No se cuenta con cifrado de los datos del estudiante.

- No se cuenta con un listado puntual de los activos tecnológicos de la empresa u organización.

- No se cuenta con un plan de contingencia generalizado propio de la empresa.

- No se cuenta con diagramas del diseño a nivel de hardware.

3.1.4. Efectos.

Se presume que actualmente La Compañía está operando bajo los siguientes riesgos no controlados:

- Vulnerabilidades expuestas al público por ser un servicio 100% web.

- Recurrencia en incidentes de seguridad.

- Fugas de información.

- Fraude y robo de información.

- Problemas en la planificación de continuidad de negocio.

- Indisponibilidad de la información crítica del negocio.

- Modificación de la información.

3.2. Aspectos a solucionar.

Este proyecto se enfocara en solucionar los siguientes aspectos:

- Las políticas de seguridad no cubren el actual entorno del servicio prestado por la empresa.

- No se cuenta con conocimiento del estado de vulnerabilidades de aplicaciones (web) y equipos de cómputo.

- No se cuenta con un esquema de aseguramiento de la Información desarrollada para los cursos.

- No se cuenta con un listado puntual de los activos tecnológicos de la empresa u organización.

3.3. Solución propuesta.

Realizar un análisis de ciberseguridad y seguridad física de la infraestructura de una empresa dedicada a prestar servicios de educación virtual especializados en el área de salud, para esto se realizará un levantamiento de la información que no se tiene al momento y se generarán documentos con nuevas políticas y recomendaciones.

A continuación, se describe cada una de las actividades del plan de Análisis de Ciberseguridad a realizar:

- Ejecución de una evaluación de vulnerabilidades a los computadores (usuarios operativos, clientes y/o servidores en el caso que aplique) de la sede con el fin de determinar vulnerabilidades y definir las recomendaciones para la implementación de los controles que permitan mitigarlas o reducirlas.

  Entregable para la compañía:
  Informe de resultados de pruebas y recomendaciones con Check List de actividades a ejecutar por la empresa para controlar y mitigar los riesgos.

  Notas: Pueden presentarse actividades adicionales menores que complementen el entregable.

- Análisis del tipo de conexión a la base de datos de usuarios de Y Aliados (Q10). En este punto se analizará el canal de comunicación y los protocolos para el establecimiento de la conexión, así como una revisión de las prácticas de acceso (manejo de usuarios y contraseña).

  Entregable para la compañía:
  Informe de resultados de pruebas y análisis de resultados de la conexión a bases de datos Y Aliados.

  Notas: Pueden presentarse actividades adicionales menores que complementen el entregable.

- Inspección y análisis de seguridad física de las instalaciones principales de La Compañía, con el fin de determinar si existen vulnerabilidades físicas que puedan evidenciar amenazas que coloquen en riesgo la seguridad de la información de la compañía. Se verificará el sector y el barrio donde está ubicada (manzana a la redonda), zona de acceso de empleados, usuarios, publico, zona de computadores de usuarios, servidores y redes (Centros de Cómputo o Data Center), Control de Acceso, CCTV y perímetros.

  Entregable para la compañía:
  Informe de resultados de inspección y recomendaciones, descripción de puntos débiles y controles a implementar con el fin de conocer las posibilidades para reducir y mitigar los riesgos.

  Notas: Pueden presentarse actividades adicionales menores que complementen el entregable.

- Ejecución de pruebas y análisis de vulnerabilidades a la página web con URL http://La Compañía.com.co/ de la compañía, con el fin de determinar vulnerabilidades y definir las recomendaciones para la implementación de los controles que permitan mitigarlas o reducirlas. Este análisis incluye:

- Hosting (Digital Ocean).
- Plataforma (Talent Lms - AWS).
- Almacenamiento de Contenidos.

Entregable para la compañía:
Informe de resultados de análisis de vulnerabilidades y recomendaciones con Check List de actividades a ejecutar por la empresa para controlar y mitigar los riesgos.

Notas: Pueden presentarse actividades adicionales menores que complementen el entregable.

- Revisión y actualización de las políticas de seguridad de la información de la compañía. Esta modificación se realizará de acuerdo con los resultados de las actividades anteriormente descritas y con el fin de alinearlas y actualizarlas a los servicios actualmente prestados por La Compañía.

Entregable para la compañía:
Revisión de las políticas de seguridad de la información de la compañía. Se elaborará una actualización de las políticas entregadas por La Compañía a los estudiantes de la Especialización. Esta actualización será acorde con los resultados de cada uno de los puntos anteriores y nuevas recomendaciones que puedan surgir del análisis de la información recopilada durante el desarrollo de las actividades anteriormente descritas.

4. Estado del arte.

4.1. Marco de referencia teórico.

- "The Practice of network security monitoring: Understanding incident detection and response (Richard Bejtlich)": Este libro brinda un análisis de diferentes herramientas para monitoreo en la red acompañando cada herramienta de casos prácticos que facilitan su lectura y comprensión y además pueden resultar interesantes en la vida profesional.

- "X1Red+Segura Informando y Educando V1.0": Es un libro enfocado a concientizar a todos los usuarios de internet, especialmente a los que no disponen de conocimientos técnicos, de los riesgos y amenazas que nos acechan en la red; conocer los peligros y saber que sus consecuencias atraviesan los monitores y pantallas de nuestros dispositivos para así disfrutar de internet de forma mucho más segura y aprovechando las infinitas nuevas tecnologías que aportan y también da una introducción a los principales riesgos a los que todo internauta se enfrenta.

- "El Cisne Negro: el impacto de lo altamente improbable": Esta obra de Nassim Nicholas Taleb enseña a reconocer dentro de la complejidad de la era digital que no todo está predeterminado ni determinado, que siempre es posible que aparezca en el horizonte de lo improbable un "cisne negro", una excepción o un caso raro o extraño que haga reflexionar y cuestionar toda la situación a la que se está enfrentando en ese momento. Ese cisne puede entonces determinar el devenir de los próximos pasos, algo no contemplado ni previsto que aparece sin previo aviso y lo cambia todo. En resumen, es una forma interesante de contar que el 100% de la ciberseguridad no existe, y que todo hecho tiene una probabilidad (por baja que sea) de ocurrir e influir en unos hechos.

- "Hardening – Network infrastructure: Wesley J. Noonan entrega una herramienta invaluable para cualquiera que se enfrente a los desafíos de la seguridad en un entorno de negocios. Entregando un esquema paso a paso para la construcción y despliegue de infraestructura manteniendo en todo momento la seguridad como premisa principal de desarrollo y operación.

4.2. Marco de referencia tecnológico.

"Tesis: Ciberseguridad en Infraestructuras Criticas de información (Universidad de Buenos Aires, Ing. Arsenio Aguirre)": Este trabajo final de maestría analiza la importancia de la ciberseguridad en las infraestructuras críticas de información, las actividades que se han desarrollado en este sentido de manera general en algunos países y el apoyo de las organizaciones internacionales que colaboran en el área de la ciberseguridad. Sobre esta base, propone un modelo para la identificación de los sectores y servicios críticos de una economía y una serie de controles mínimos para su protección.

En efecto, las tecnologías de la información se han esparcido rápidamente en todos los sectores de la sociedad y prácticamente no existen servicios críticos que no dependan de aplicaciones, bases de datos, servidores, redes de comunicaciones, centros de datos, etc. La falta de controles de ciberseguridad ha ocasionado que algunos servicios se vean afectados a nivel mundial, como lo demuestran los incidentes de ciberseguridad que se describen en el presente trabajo y que impactaron en el funcionamiento de diferentes servicios críticos de tres países.

La mayoría de sectores que están utilizando tecnologías de información, proveen servicios importantes a la población. Sin embargo, debido a la falta de metodologías de clasificación de estos servicios, no se ha podido identificar cuáles son realmente críticos y que por lo tanto, cuáles requieren una protección acorde por parte de los operadores que los proveen. Un aporte adicional del trabajo es el análisis del estado actual de la ciberseguridad en el Ecuador. En esta sección se analiza la situación de ese país, incluyendo las normativas y regulaciones que ha desarrollado para fortalecer la ciberseguridad en las empresas públicas y a nivel privado. Este libro nos brinda un análisis de diferentes herramientas para monitoreo en la red acompañando cada herramienta de casos prácticos que facilitan su lectura y comprensión y además pueden resultar interesantes en la vida profesional.

4.3. Línea de investigación.

Antes de desarrollar el trabajo, y una vez que se tenía una idea clara del objetivo de este, se realizó un estudio de las distintas implementaciones existentes, tanto a nivel académico, como a nivel comercial, que puedan cumplir las necesidades con la que surge este proyecto.

4.4. Ámbito Comercial.

A nivel comercial, se han encontrado, las siguientes herramientas, que tratan aspectos parecidos a este trabajo, aunque de distinta forma, a continuación, se citan y se describen de forma básica sin profundizar en ellas:

A) **Nessus**: Herramienta para la realización del escaneo de vulnerabilidades de forma automática, que cuenta además con su propio escáner de puertos, así como de un lanzador de exploits, y que, puede generar informes en diversos formatos de salida.

B) **Shodan**: Es un motor de búsqueda diseñado para buscar dispositivos y sistemas de ordenadores conectados a Internet a través de una variedad de filtros. Recoge datos de todos los servicios, incluyendo los puertos HTTP:80, HTTPS:443 – 8443, FTP:21, SSH:22, Telnet:23, SNMP:161 y SIP:5060.

C) **Qualys SSL**: Es una herramienta online y gratuita para comprobar la seguridad de una página web. Esta automatiza el trabajo de verificar qué suites de cifrado y certificados digitales utiliza un sitio web, de esta forma, poder configurar el HTTPS de un sitio web con la máxima seguridad posible.

D) **OSSAMS**: Framework para la correlación de los datos arrojados de un Pentesting.

E) **Sparta**: Herramienta de automatización de pruebas de pentesting.

F) **GoLismero**: Framework para la automatización de auditorías de seguridad a nivel web principalmente.

G) **Discover**: Herramienta para la automatización mediante scripts de herramientas de descubrimiento de información.

H) **SpeedPhish Framework**: Framework para la automatización de tareas relacionadas con la recolección de información y pruebas de ingeniería social.

5. Glosario de términos.

Amenaza: Acción que aprovecha una vulnerabilidad detectada, afectando la seguridad de la información. Potencial efecto negativo sobre los activos informativos de una organización (virus, fraude, robo, ocultación, interrupción, modificación). Pueden ser internas o externas.

Análisis: Examen detallado de una cosa para reconocer sus características o cualidades, o su estado, y extraer conclusiones, que se realiza separando o considerando por separado las partes que la constituyen.

Asesoramiento: Es la acción y efecto de asesorar o asesorarse; este verbo hace referencia a dar o recibir consejo o dictamen.

Ciberseguridad: También conocida como seguridad informática o seguridad de tecnología de la información; es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circularmente a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

Consultoría: Es un servicio profesional prestado por empresas, o por profesionales en forma individual (conocidas como consultores respectivamente) con experiencia o conocimiento específico en un área, asesorando personas, asesorando a otras empresas, a grupos de empresas, a países o a organizaciones en general.

Informática: También llamada computación, es una ciencia que administra métodos, técnicas y procesos con el fin de almacenar, procesar y transmitir información y datos en formato digital.

Vulnerabilidad: Debilidad de un sistema que coloca en riesgo la seguridad de la información, haciendo posible la pérdida de la confidencialidad, integridad o disponibilidad de la información.

Seguridad: Se puede referir a la ausencia de riesgo o a la confianza en algo o en alguien, sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia en la seguridad. En términos generales, la seguridad se define como "el estado de bienestar que percibe y disfruta el ser humano".

Telemática: Es la disciplina científica y tecnológica que analiza e implementa servicios y aplicaciones que usan tanto los sistemas informáticos como los de telecomunicación, como resultado de la unión de ambas disciplinas.

6. Justificación.

Aunque La Compañía nació como una empresa pequeña ha tenido un crecimiento exponencial en los años que lleva de funcionamiento, obteniendo cada vez más aliados, así como una base de datos mucho más grande a nivel de información y de personal (incluyendo usuarios finales y administrativos).

Por lo anterior, nace la necesidad de establecer una línea de base para una estrategia cibernética dirigida hacia amenazas, y en consecuencia hacer un análisis completo de seguridad para el funcionamiento de la empresa.

Como beneficios puntuales planteados de este análisis de ciberseguridad se tienen:

- Mejorar la imagen corporativa de La Compañía ante sus aliados.

- Toma de mejores decisiones en las inversiones tecnológicas a futuro para el crecimiento de la empresa en diferentes aspectos.

- Control y medición de posibles incidentes/accidentes de seguridad, lo que permite mejorar la prevención de otros similares.

- Conocer los riesgos a los que la empresa se enfrenta diariamente acotando su impacto. A futuro poder disponer de un sistema que le permita a la empresa actuar de manera más rápida y eficiente ante posibles ataques.

- Generar una adecuada información para mantener al personal administrativo siempre informado de las prácticas sobre seguridad.

7. Objetivos.

7.1. General.

Realizar un análisis de ciberseguridad y seguridad física, apuntando todo a mejores prácticas que favorezcan el crecimiento de la empresa y generando nuevos documentos de políticas y recomendaciones para la compañía. Para esto se plantea el desarrollo indicado en el numeral 3.3. Solución propuesta.

7.2. Específicos.

- Hacer un estudio general de la empresa, el cual genere la documentación necesaria faltante como listado de activos, diagramas funcionales, acuerdos de confidencialidad, entre otros.

- Analizar la seguridad física que se maneja en los diferentes procesos que se realiza en la empresa.

- Hacer un análisis de ciberseguridad que genere recomendaciones, documentos de pruebas, documentos de análisis, posibles vulnerabilidades a futuro y replanteamiento de las políticas de seguridad actuales de la empresa.

- Análisis de conectividad directa a los datos del aliado principal de la empresa.

8. Requerimientos.

8.1. Requerimientos funcionales.

- Revisión de seguridad de la infraestructura de la empresa.

- Análisis de cumplimiento de políticas para los diferentes usuarios que pueden entrar al sistema.

8.2. Requerimientos no funcionales.

- Listado de todos los activos tecnológicos que maneja la empresa.
- Diagrama de la estructura de la empresa.
- Diagrama de la funcionalidad de la empresa.
- Pruebas ejecutadas al sistema en cada usuario.
- Acuerdos de confidencialidad en los casos que es necesario (generar una plantilla propia de la empresa para cuando se necesite en el futuro).
- Listado de vulnerabilidades encontradas.
- Listado de posibles vulnerabilidades contemplando el futuro crecimiento de la compañía.
- Replanteamiento de las políticas de seguridad actuales de la empresa.
- Replanteamiento de los acuerdos de "Aceptación de términos y condiciones" de los usuarios y profesores que utilizan la plataforma.
- Listado de recomendación de ciberseguridad.
- Listado de recomendaciones de seguridad física.

9. Metodología.

La metodología de desarrollo a utilizar es SCRUM, se escoge en base a las características que tiene para trabajar en equipo a partir de iteraciones o Sprints, lo que la convierte en una metodología ágil, que genera que su objetivo sea controlar y planificar proyectos con un gran volumen de cambios de última hora, en donde la incertidumbre sea elevada.

Las fases en las que se divide un proceso Scrum y las cuales son las mismas que se van a manejar para darle solución a este proyecto:

- "¿Qué y quién?" El producto al que se quiere llegar una vez terminemos el Sprint, y los roles de equipo con sus tareas asignadas.

- "¿Dónde y cuándo?" El plazo y el contenido del Sprint.

- "¿Por qué y cómo?" Las distintas herramientas para aplicar esta metodología ágil.

Las etapas que se van a manejar en cada uno de los Sprint son:

- Reunión para la planificación del Sprint: En ella, se divide el tiempo de duración del Sprint, así como el objetivo y entregable del mismo. Además, el equipo de desarrollo deberá saber cómo realizarlo.

- Scrum diario: Se basa en poner en común y sincronizar actividades para elaborar el plan del día.

- Trabajo de desarrollo durante el Sprint: Nos aseguramos que los objetivos se están cumpliendo, que no se producen cambios que alteran el objetivo del Sprint y se mantiene un feedback constante con el área administrativa de la empresa.

- Revisión del Sprint: Reunión con el cliente o dueño del proyecto, en la que se estudia y revisa el Product Backlog del Sprint. Se definen los aspectos a cambiar, en caso necesario, de mayor valor o probables para planificarlo en el siguiente Sprint.

- Retrospectiva del proyecto: Oportunidad del equipo de desarrollo para mejorar su proceso de trabajo y aplicar los cambios en los siguientes Sprints.

- La metodología Scrum tiene unos roles y responsabilidades principales, asignados a sus procesos de desarrollo, los cuales ajustamos a nuestro proyecto de la siguiente manera:
    - Project Owner (Director Ingeniero Eduardo Chavarro): Se asegura de que el proyecto se esté desarrollando acorde con la estrategia del negocio. Escribe historias de usuario, las prioriza, y las coloca en el Product Backlog.
    - Master Scrum o Facilitador (El área administrativa de la empresa y María Alejandra Segura): Elimina los obstáculos que impiden que el equipo cumpla con su objetivo.
    - Development Team Member (Juan Pablo Ángel, Cristian Bernal y María Alejandra Segura): Los encargados de crear el producto para que pueda estar listo con los requerimientos necesarios.

- La herramienta a utilizar es Smartsheet.

10. Recursos Necesarios.

10.1. Humanos.

Estudiantes de la especialización "Seguridad en redes telemáticas":

- Juan Pablo Ángel Espejo, Cristian Arley Bernal Reinoso y María Alejandra Segura Greco.

Acompañamiento por parte de la empresa:

- Felipe Mendoza y Camilo Alcázar.

Director del proyecto:

- Ingeniero Eduardo Chavarro.

Asesor Metodológico:

- Ingeniero Oscar Arias.

10.2. Técnicos.

Herramientas para soportar el análisis de seguridad a realizar: Nessus, Acunetix, NMap, OpenVAs, OWASP ZAP, KaliLinux, NetScan, MBSA, Qualys (Microsoft Baseline Security Analyzer), Office, Open Office, entre otros.

10.3. Institucionales.

Se generan permisos a nivel de LA COMPAÑÍA.ACADEMY-LMS para tener completa visión del funcionamiento de la empresa.

10.3.1. Normas y modelos.

A continuación, se citan y describen brevemente los estándares y modelos que existen actualmente y se marcan como referencia, ayuda o cualquier procedimiento relacionado de alguna forma u otra con la seguridad a nivel informática o de telecomunicaciones.

PTES es un estándar recientemente creado por un conjunto de comunidades que han participado para estandarizar los pasos y procesos a seguir durante la realización de un pentesting. Consta de una guía técnica de uso y divide los procesos en los que se llevan a cabo en una auditoría.

OWASP es un proyecto de código abierto que permite determinar las vulnerabilidades en el software. Proporciona una guía de buenas prácticas en el desarrollo de aplicaciones y un documento de autoevaluación.

OSSTMM es una metodología estructurada donde se explica cómo llevar a cabo las pruebas de auditoria correspondientes a distintos ámbitos. En esta metodología se explica que es un análisis de seguridad, como enfocarlo, cuáles son las métricas de seguridad operativas, como se debe estructurar el flujo de trabajo, las pruebas de seguridad que se deben realizar a las personas (ingeniería social, seguridad en las telecomunicaciones, Wireless, entornos físicos, de red) y se recoge también una guía para generar los informes.

CWE proporciona un marco unificado para catalogar las vulnerabilidades de software. Es una lista de información sobre vulnerabilidades conocidas, donde cada una dispone de una referencia, para proporcionar de esta forma a los usuarios una manera de entender los problemas. Además, proporciona una clasificación estandarizada y normalizada con la que los auditores podrán comparar diferentes auditorias con un enfoque real, asignando ponderaciones junto a una clasificación, para así poder compararlas.

OWISAM proporciona una solución a la necesidad de definir y asignar controles de seguridad que se deben verificar sobre redes de comunicaciones inalámbricas. De esta manera se puede identificar riesgos en este tipo de redes y aplicar procedimientos en las auditorias de este tipo de redes.

ISACA es una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.

COBIT es una guía de mejores prácticas dirigidas al control y supervisión de las tecnologías de la información. Tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un framework, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión.

ISO 17799/ ISO 27002 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización. Define la información como un activo que posee valor para la organización y requiere, por tanto, de una protección adecuada. El objetivo es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.

ISO/IEC 27001 es un estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI). La certificación de un SGSI es un proceso mediante el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad, su grado de implantación real y su eficacia y, en caso positivo, se emite el correspondiente certificado.

OpenSCAP provee una infraestructura poderosa para la elaboración de análisis e informes sobre vulnerabilidades en los sistemas de información, utilizando un conjunto de especificaciones del NIST (formatos y nomenclaturas) para manipular información relacionada con la seguridad sobre fallos y configuraciones de una forma estandarizada. De esta forma se permite automatizar, en cierto grado, el chequeo (búsqueda) de vulnerabilidades, evaluar posibles impactos de vulnerabilidades, la gestión de vulnerabilidades, mediciones de seguridad y evaluación de políticas a adoptar.

10.4. Tiempos.

Se tiene programado un tiempo de 20 semanas para toda la ejecución del proyecto, manejando aproximadamente un aporte de 3 horas a la semana por cada uno de los estudiantes. De parte de La Compañía el tiempo límite para el entregable es que no se pase del año en curso 2019.

10.5. Compromisos.

Se tiene un acuerdo de confidencialidad con la empresa, en donde se compromete a manejar toda la información de los análisis solo con el área administrativa de la misma. (Una vez la empresa nos entregue el acuerdo firmado y en físico se anexara el documento en el capítulo de anexos).

10.6. Referencias Documentales.

- "Seguridad Informática, de lujo a necesidad" (4 de diciembre de 1997), El Tiempo {Online}. Consultado en: https://www.eltiempo.com/archivo/documento/MAM-664024

- "La importancia de la seguridad informática en tu empresa" (14 de enero de 2019), CIC Consulting Informático {Online}. Consultado en: https://www.cic.es/seguridad-informatica-empresa/

- "Ciberseguridad: una preocupación de empresas grandes y pequeña", editorial {Online}. Consultado en: https://destinonegocio.com/pe/gestion-pe/ciberseguridad-una-preocupacion-de-empresas-grandes-y-pequenas/

- "Ciberseguridad: Como abrir un correo puede costarle mucho dinero", editorial {Online}. Consultado en: https://destinonegocio.com/pe/gestion-pe/ciberseguridad-como-abrir-un-correo-puede-costarle-mucho-dinero/

- La Compañía Training And Education, La Compañía {Online}. Consultado en: https://La Compañía.com.co/quienes-somos/

11. Cronograma de Actividades.

El siguiente cronograma se adjunta también como Anexo para su fácil lectura y análisis.

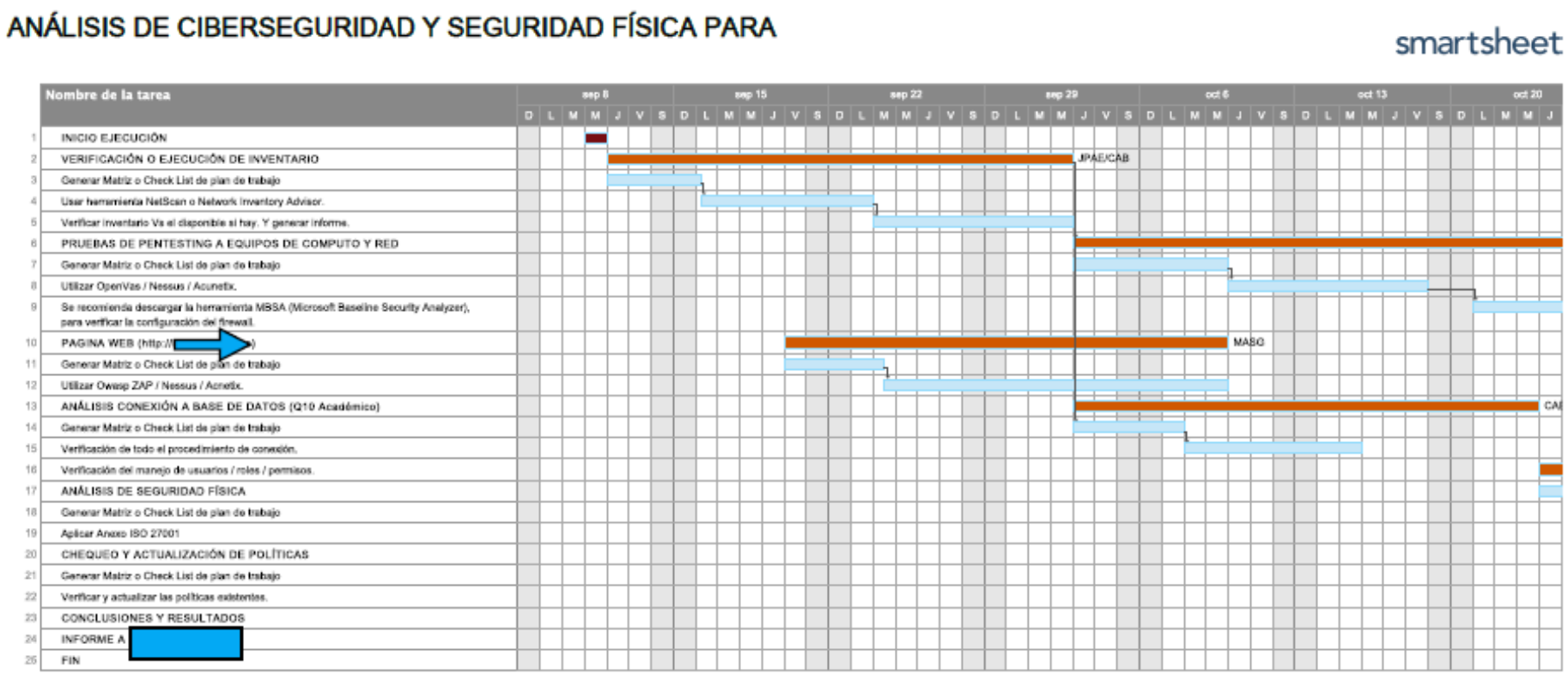


Figura 1 Cronograma de ejecución parte 1.

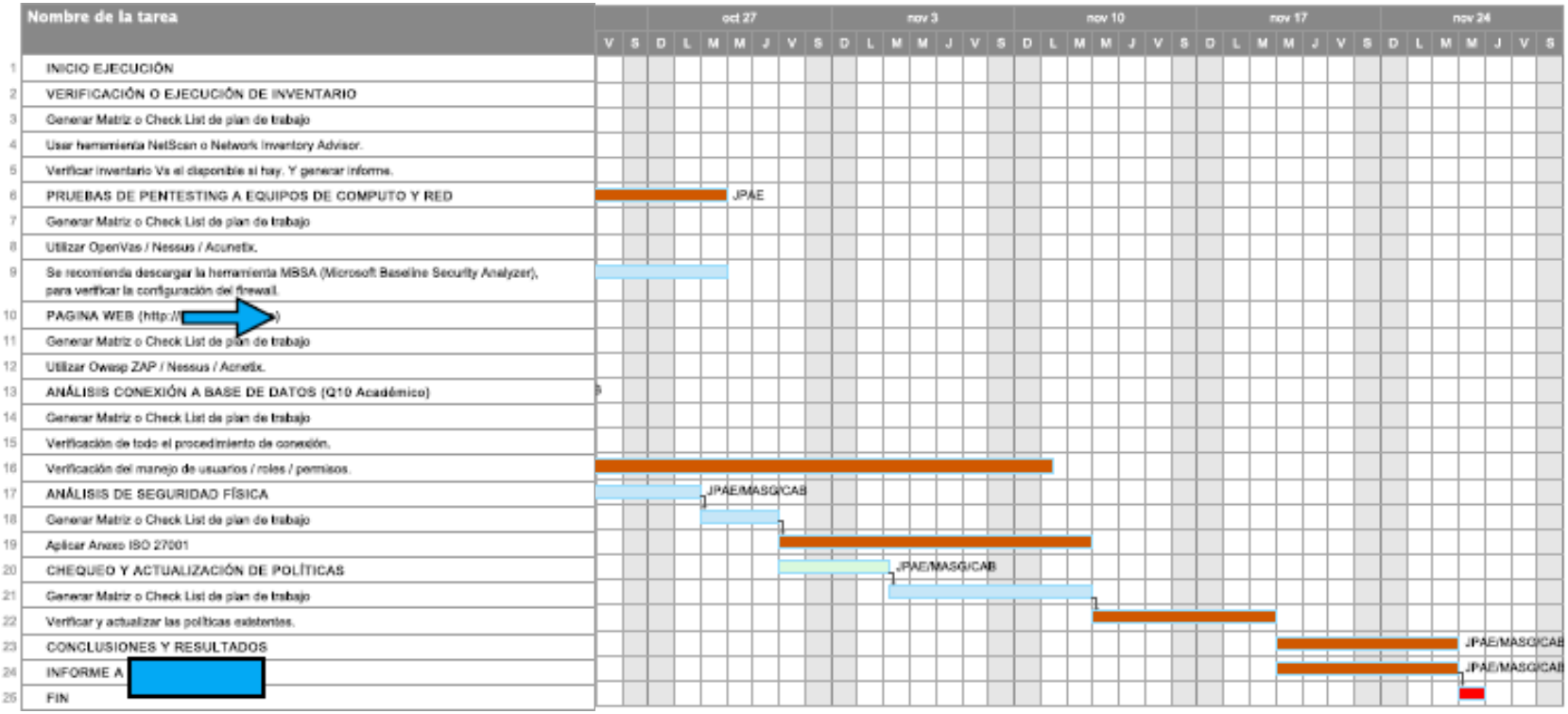


Figura 2 Cronograma de ejecución parte 2.

Cronograma Inicial	
Objetivos	**Tiempo aproximado**
Hacer un estudio general de la empresa, el cual genere la documentación necesaria faltante como listado de activos, diagramas funcionales, acuerdos de confidencialidad, diagramas de infraestructura, entre otros.	4 semanas
Analizar la seguridad física que se maneja en los diferentes procesos que se realiza en la empresa.	4 semanas
Hacer un análisis de ciberseguridad que genere recomendaciones, documentos de pruebas, documentos de análisis, posibles vulnerabilidades a futuro y replanteamiento de las políticas de seguridad actuales de la empresa.	10 semanas
Análisis de conectividad directa a los datos del aliado principal de la empresa.	2 semanas

Objetivos	Tareas Específicas
Hacer un estudio general de la empresa, el cual genere la documentación necesaria faltante como listado de activos, diagramas funcionales, acuerdos de confidencialidad, diagramas de infraestructura, entre otros.	Tener reuniones constantes con el área administrativa de la empresa.
	Tener reuniones constantes con el grupo de trabajo del proyecto para tener una base de los datos necesarios a generar para la solución del proyecto.
	Revisión del funcionamiento de la empresa.
	Revisión de los objetivos de la empresa.
	Revisión de la plataforma virtual (manejo para el usuario).
	Revisión de las conectividades de la empresa hacia otras compañías.
Analizar la seguridad física que se maneja en los diferentes procesos que se realiza en la empresa.	Ir a las instalaciones físicas de la empresa.
	Hacer reuniones con el grupo de trabajo del proyecto para validar todas las revisiones ejecutadas y generar los documentos que serán entregados al cliente.
Hacer un análisis de ciberseguridad que genere recomendaciones, documentos de pruebas, documentos de análisis, posibles vulnerabilidades a futuro y replanteamiento de las políticas de seguridad actuales de la empresa.	Revisar toda la página de la empresa (como funciona y quien la utiliza).
	Ejecutar las diferentes herramientas para el análisis de vulnerabilidades (en las características que aplique).
	Reuniones con los integrantes del grupo del proyecto para ir generando conclusiones y resultados para los documentos a entregar.
	Hacer los diferentes análisis manuales del funcionamiento de la empresa (en las características que aplique).
	Revisar y entender a detalle las políticas y documentos actuales que maneja la empresa.

Tabla 1. Descripción actividades y tiempos.

12. Desarrollo.

12.1. Verificación inventario.

Aunque el proceso de inventario se ha ido adelantando desde etapas previas, mediante la consulta a los colaboradores de La Compañía / Y Aliados, el día 12 de septiembre se realizó el inventario detallado de los equipos de la Organización. Se encontraron equipos de escritorio, laptops, equipos de telecomunicaciones (switches, routers y módems), así como equipos audiovisuales con y sin conexión a red e impresoras. A continuación se incluye la información básica de los equipos a los cuales se ha seleccionado para realizar evaluación de vulnerabilidades (Por razones de acuerdo de confidencialidad se omite información relevante para la organización).

ítem	Tipo de equipo	Marca	Fecha Última revisión	Verificado	SO
1	Desktop	Lenovo	06/12/2019	SI	WIN8
2	Desktop	Lenovo	06/12/2019	Sin acceso o apagado	WIN10
3	Desktop	COMPAQ	06/12/2019	Sin acceso o apagado	WIN8
4	Desktop	Lenovo	06/12/2019	Sin acceso o apagado	
5	Desktop	Lenovo	06/11/2019	SI	WIN10
6	Desktop	Lenovo	06/11/2019	Sin acceso o apagado	WIN10
7	Desktop	Lenovo	06/11/2019	SI	WIN10
8	Desktop	Lenovo	06/11/2019	Sin acceso o apagado	WIN10
9	Desktop	Lenovo	06/11/2019	SI	WIN10
10	Desktop	Lenovo	06/10/2019	SI	WIN10
11	Desktop	Lenovo	06/10/2019	SI	WIN10
12	Desktop	Lenovo	06/10/2019	SI	WIN10
13	Desktop	Lenovo	06/10/2019	SI	WIN10
14	Desktop	Lenovo	06/10/2019	Sin acceso o apagado	
15	Desktop	LG	14/6/2019	SI	WIN8

ítem	Tipo de equipo	Marca	Fecha Última revisión	Verificado	SO
16	Desktop	HP	14/6/2019	Sin acceso o apagado	
17	Desktop	Lenovo	14/6/2019	Sin acceso o apagado	
18	Desktop	COMPAQ	14/6/2019	SI	WIN8
19	Desktop	HP	17/6/2019	Sin acceso o apagado	
20	Desktop	Lenovo	17/6/2019	SI	WIN8
21	Desktop	COMPAQ	17/6/2019	Sin acceso o apagado	
22	Desktop	LG	17/6/2019	SI	WIN8
23	Desktop	LG	17/6/2019	SI	WIN8
24	Desktop	HP	17/6/2019	SI	WIN8
25	Desktop	Lenovo	14/6/2019	SI	WIN8
26	Desktop	HP	14/6/2019	SI	WIN8
27	Desktop	DELL	14/6/2019	SI	WIN8
28	Desktop	HP	14/6/2019	SI	WIN8
29	Desktop	DELL	14/6/2019	SI	WIN8
30	Desktop	DELL	14/6/2019	SI	WIN8
31	Desktop	Lenovo	14/6/2019	SI	WIN8
32	Desktop	COMPAQ	17/6/2019	SI	
33	Desktop	COMPAQ	18/7/2019	Sin acceso o apagado	
34	Desktop	COMPAQ	18/7/2019	Sin acceso o apagado	
35	Desktop	COMPAQ	18/7/2019	Sin acceso o apagado	
36	Desktop	COMPAQ	18/7/2019	Sin acceso o apagado	
37	Desktop	LG	19/7/2019	Sin acceso o apagado	
38	Desktop	DELL	20/8/2019	Sin acceso o apagado	
39	Desktop	DELL	18/7/2019	Sin acceso o apagado	
40	Desktop	COMPAQ	10/05/2017	TEMPORALMENTE FUERA DE SERVICIO	

ítem	Tipo de equipo	Marca	Fecha Última revisión	Verificado	SO
41	Desktop			SI	WIN8
42	Desktop			SI	WIN8
43	Desktop			SI	WIN8
44	Desktop			SI	WIN8
45	Telecomunicaciones	TPLINK	Router/wireless	SI	
46	Telecomunicaciones	TPLINK	Router/wireless	SI	
47	Telecomunicaciones	PANASONIC		SI	
48	Telecomunicaciones	NEXX	Router/wireless	SI	
49	Telecomunicaciones	SAGEMCOM		SI	
50	Telecomunicaciones	SCIENTIFIC ATLANTA			
51	Telecomunicaciones	TPLINK	Router/wireless	SI	
52	Laptop			SI	
53	Laptop			SI	

Tabla 2. Inventario verificado.

A los equipos a los cuales se les marco la columna de verificados se les realizo un match con los equipos del inventario interno con el fin de determinar qué tan actualizado y acertado se encontraba, se aprovechó para verificar alguna información adicional.

Los equipos que no fueron verificados, se encontraban ocupados o fuera de alcance durante esta visita.

Como valor agregado a La Compañía se planteará realizar un *"scan"* de software instalado en los equipos con el fin de determinar si hay software no esperado instalado y así evitar vulnerabilidades adicionales.

12.2. Análisis de vulnerabilidades.

Las responsabilidades de la creación y el mantenimiento de una red de computadores que incluye servicios de aplicación basadas en cliente servidor o servicios web dentro de una organización, implican un gran esfuerzo técnico y económico de las empresas.

Las premisas de su creación siempre van enfocadas y encaminadas a permitir gestionar, utilizar, resguardar y disponer de la información como recurso de vital importancia para el desarrollo económico de las compañías.

Para que una red de computación y aplicaciones como servicio se constituya en un activo esencial para este desarrollo del negocio de las corporaciones, es importante implementar de manera correcta cada uno de sus componentes de manera que se encuentren siempre actualizados y de esta manera operen adecuadamente.

Uno de los conceptos fundamentales en la actualidad es hacer que los recursos informáticos y las redes de computadoras sean configurados en términos de seguridad con el fin de evitar que se puedan presentar ataques maliciosos que puedan poner en riesgo la información del negocio de la organización. Recursos que permiten esto pueden ser; firewall de hardware o software, antivirus, sistemas de detección, prevención, antispam, antimalware, o incluso el correcto parcheo de los sistemas.

El *"penetration testing"* es una metodología que consiste en planificar un ataque a una red o aplicación, independientemente de su tamaño, o sobre equipos individuales, con el fin de revelar vulnerabilidades en el objeto de prueba.

Para el ejercicio actual, más que un *"penetration testing",* se realizará un análisis de vulnerabilidades, pues no se llegará a la etapa de explotación. La razón del porque realizar un análisis de las vulnerabilidades y no *"penetration testing",* es simple; los sistemas se encuentran en producción y un *"penetration testing"* puede dejar fuera de servicio un sistema.

Para estas pruebas se realizará un análisis de vulnerabilidades a equipos de red, computadores y aplicativos web utilizando herramientas de análisis de vulnerabilidades y dinámico como:

- NMap
- Openvas
- Nessus
- Acunetix
- RouterCheck
- Owasp ZAP
- Qualys
- Shodan

12.2.1. Procedimiento.

En este numeral, se explica la realización de un análisis de vulnerabilidades informáticas de una organización. Está metodología, permite dar una orientación, pero generalmente común en la mayoría de auditorías, ya que en general es de obligatorio cumplimiento.

Cuando se realiza un test de intrusión, tenemos un objetivo claro, llegar a ser administradores de los equipos internos de la red, ya que desde ahí es posible acceder a todos los equipos e información de la red. Tanto si realizamos el test de intrusión de manera remota como si lo hacemos de manera presencial en las propias instalaciones del cliente, vamos a seguir una serie de pasos para intentar no dejar nada atrás. A continuación se describe el procedimiento a ejecutar para realizar las pruebas a equipos en red local y sus dispositivos más relevantes:

- Descubrir la red.
    - Identificar rangos de ips
    - Análisis de tráfico
- Análisis de vulnerabilidades (Shodan, Qualys SSL, Nessus, NMap, OpenVas, Jhon The ripper).
- Exploit (no está dentro del alcance de este trabajo de grado).
- Informe de resultados.

12.2.1.1. Finalidad.

Los test de intrusión o *"pentesting"* evalúan los niveles de seguridad de un sistema informático o red mediante la simulación, en un entorno controlado, de un ataque por parte de un usuario malicioso.[1] Esto implica un proceso de análisis activo en el sistema en busca de posibles vulnerabilidades, que podrían resultar de una mala o inadecuada configuración de un sistema, de defectos en el software (conocidos o no), de fallos de seguridad en un sistema operativo o hardware.

Este análisis se realiza desde la posición de un atacante potencial, y puede implicar la explotación activa de vulnerabilidades de seguridad. Los problemas de seguridad que se encuentren, se presentarán al propietario del sistema junto con una evaluación del impacto que supondrían dentro de la organización, además de unas propuestas de mitigación o una solución técnica.

En otras palabras, hay que llevar a cabo la parte de intrusión y pruebas de seguridad, y, por otro lado, preparar las contramedidas y procedimientos que serán llevados a cabo en caso de detectar y explotar dichas vulnerabilidades. La suma de ambas partes constituye una evaluación de seguridad global, que es realmente lo que el cliente contrata y espera.

Dado que las pruebas de penetración están diseñadas para simular un ataque y utilizar herramientas y técnicas que pueden ser restringidas por la ley, las regulaciones nacionales y la política de la organización, es imprescindible obtener un permiso formal para la realización de pruebas de penetración.

12.2.1.2. Fases de un "Pentesting".[2]

Los pasos a seguir para llevar a cabo un test de penetración son generalmente independientes del tipo de auditorías que se pretenden realizar, aunque es imperativo recordar que se persigue un objetivo común, que es preservar la seguridad. Se pueden distinguir las siguientes fases:

[1] González, Pablo; Sánchez, Germán & Soriano, José. (2013). Pentesting con Kali. Edición 0xWORD. España. [978-84-616-7738-2].
[2] http://www.pentest-standard.org/index.php/Main_Page.

A) Recolección de información: Es una etapa meramente práctica. El equipo ejecutor utiliza técnicas como el Footprinting, Fingerprinting, Google Hacking, entre otras para intentar obtener la mayor cantidad de información sobre la organización a verificar. Otras vías muy comunes de localizar información son a través de redes sociales o mediante ingeniería social, enfocada a los trabajadores de la empresa. Todo ello, lleva a la posibilidad de que el auditor consiga tener una clara imagen del objetivo, saber su funcionamiento, como fue concebido e incluso saber los posibles y más comunes fallos de implementación.

B) Modelado de amenazas: El modelado utilizado debe ser coherente en cuanto a la representación de las amenazas, sus capacidades, y sus calificaciones según el riesgo asignado por la organización que se está sometiendo al test de penetración.

   El objetivo de este modelado es que, de ser aplicado en varias ocasiones para pruebas futuras, se puedan medir los mismos resultados. Se deberá tener en cuenta tanto la parte atacante como la propia, identificando los objetivos primarios y secundarios y asignándoles el riesgo pertinente.

C) Análisis de las vulnerabilidades: Después de recolectar toda la información disponible en la red o mediante las técnicas necesarias, aún queda analizar y organizar todos los resultados, ya que a partir de ellos se pueden hallar agujeros de seguridad y con todo ello, se podría planificar el método de acción o ataque que mejor se adapte a la situación.

   Después de esto, y tras un breve estudio, se podrá determinar el método de ataque más eficaz para la situación, simulando los procedimientos que un atacante común realizaría para explotar las debilidades en la seguridad de un sistema.

   El uso de escáneres y análisis de puertos, entre otros, son los procedimientos habituales en esta etapa.

D) Explotación de las vulnerabilidades (informativo - no aplica a este trabajo): Basándose en la información recopilada anteriormente y fundamentándose en la experiencia de trabajo adquirida por el equipo ejecutor, se logran superar las barreras de seguridad que plantean las organizaciones, dejando al descubierto las vías por las cuales un atacante externo puede hacerse con el control del sistema víctima.

E) Post-explotación (informativo - no aplica a este alcance): Es una fase muy importante, ya que se supone que ya se posee el acceso al sistema o a parte del mismo, en este punto, se intenta realizar la técnica de pivote o escalada de privilegios, es decir, saltar de un equipo a otro con la intención de controlar a todos los equipos que conforman la red corporativa. Se establece que, al obtener el acceso a un equipo, es como si se estuviese físicamente dentro de la red institucional.

F) Generación de reportes: Es la parte más importante del *"pentesting"*, ya que se informa al cliente de cada una de las acciones y pruebas que se han realizado y los resultados que se han obtenido en cada una de ellas, documentando los procedimientos realizados con capturas de pantalla, rutas donde se han encontrado parámetros vulnerables, registros de logs, etcétera.

   Es importante que después de realizar cada acción, ésta sea debidamente documentada y no esperar al último momento, ya que si no la tarea podría ser mucho más tediosa e incluso podrían pasarse por alto algunas de las acciones que han supuesto el descubrimiento de vulnerabilidades.

G) Para finalizar se realiza un informe técnico y un informe ejecutivo. Un informe puede tener al menos dos perspectivas claras como son el punto de vista técnico y el ejecutivo. Sea cual sea el informe que se requiera preparar, los informes deben dar información clara y estructurada de las acciones llevadas a cabo por el auditor.

12.2.1.3. Metodología.[3]

12.2.1.3.1. Recopilación de información.

*"**Footprinting**":* Primera etapa de un test de intrusión en la que el atacante recoge información de todo tipo sobre el objetivo. Su fuente es toda Internet, por lo que se puede llegar a encontrar gran cantidad de información. Posteriormente, hay que filtrarla para obtener los datos más relevantes. Tradicionalmente, este proceso de recogida de información se encuentra dividido en dos fases:

- *"External Footprinting":* Detalla el procedimiento seguido para recolectar información de forma externa a la organización. Este proceso de recolección de información desde el exterior esta categorizado en dos categorías en función del grado de agresividad de las mismas:
    - "*Active Footprinting*": Descubrimiento activo, que destaca por interactuar directamente con la infraestructura de la empresa objetivo mediante consultas al DNS, análisis de las cabeceras HTTP, enumeración de puertos y sus servicios, etcétera. Las herramientas utilizadas en este proceso podrían ser el descubrimiento DNS, Banner Grabbing, Maltego, Whatweb, BlindElephant, Plecost, theHarvester etcétera.
    - *"Pasive Footprinting"*: Descubrimiento pasivo, que recurre a la consulta de información previamente indexada por motores de búsqueda, registros públicos, foros, etcétera. Las herramientas utilizadas en este proceso podrían ser el protocolo Whois, Google/Bing Hacking, Shodan, Robtex, etcétera.

- "*Internal Footprinting*": Se centra en las actividades que se pueden realizar una vez que el atacante ha conseguido acceso parcial a la red interna, y donde intentará volver a conseguir la mayor cantidad de información posible, para seguir escalando el ataque a otros equipos dentro de la organización. Las herramientas utilizadas en este proceso podrían ser IDS como Suricata, Bro o Snort.

[3] Palacios, Jairo. [En línea]. Análisis de Vulnerabilidades de una red corporativa mediante herramientas de descubrimiento activas. Trabajo Fin de Grado. Universidad de Sevilla.

"***Fingerprinting***": Recolección de información que consiste en interactuar directamente con los sistemas para aprender más sobre su configuración y comportamiento.

Estas técnicas llevarán a cabo un escaneo de puertos para el estudio de los posibles puertos abiertos que se encuentren y determinar qué servicios se están ejecutando, además de la versión del producto que se encuentra detrás del puerto. Las herramientas utilizadas en este proceso podrían ser Half Scan, ACK Scan, Null Scan, Xmas Scan, FIN Scan, NMap, etcétera.

12.2.1.3.2. Análisis de vulnerabilidades y "pentesting".

Auditoría Perimetral: Estas permiten a un auditor conocer el estado de seguridad del perímetro de la organización analizando las posibles entradas del exterior hacia la DMZ y zonas internas. El auditor no conoce la configuración del perímetro, por ello se denomina también auditoría ciega, y en ella, se estudia el estado de seguridad de los elementos que se pueden analizar desde el exterior.

El objetivo final es obtener acceso a la red interna de la organización o a la DMZ, así como obtener información interna y detectar vulnerabilidades que pongan en peligro la información de la organización. Gracias a este tipo de auditoría, se dispone de una primera visión de vulnerabilidades existentes para una posterior corrección de ellas.

Este tipo de auditorías donde se depende mucho de los servidores y servicios que una organización dispone en el perímetro, puede tener diferentes tipos de pruebas debido a la heterogeneidad del entorno Por esta razón, los procedimientos que se puedan llevar a cabo independientemente del tipo de entorno son los siguientes:

A) Identificación de servicios: La determinación de servicios mediante técnicas de Fingerprinting para obtener ideas y analizar vías por donde atacar la seguridad de los distintos servicios. Las herramientas utilizadas en este proceso podrían ser NMap, Nessus, Nexpose, etcétera.
B) Análisis de vulnerabilidades, recopilación y ejecución de exploits. Las herramientas utilizadas en este proceso podrían ser Metasploit y sus distintos módulos.

C) Análisis de información: Tras la recogida de esta se debe realizar un análisis y las primeras pruebas. La realización de técnicas de fuzzing y crawling ayudan a completar los mapas de información. Los puntos de entrada deben ser encontrados y se debe verificar la seguridad de estos. Las herramientas utilizadas en este proceso podrían ser Burpsuite, DirBuster, WFuzz, FOCA, etcétera.
D) Detección de malas configuraciones y exposiciones no deseadas por parte de la organización. Las herramientas utilizadas en este proceso podrían ser SQL Injection, Cross-Site Scripting, CSRF, LDAP Injection, XPath Injection, etcétera.
E) Detección y explotación: Realización de análisis del protocolo SSL, manipulación de parámetros, análisis de cookies y utilización de técnicas de hacking web.

Auditoría Interna: Proporcionan un estado de la seguridad de los distintos segmentos de red de una empresa. Estos segmentos de red son ubicaciones internas las cuales no disponen de grandes privilegios de conectividad, con sistemas que contienen información sensible.

Dicho de otro modo, uno de los posibles roles del auditor o ejecutor será el de un empleado cuyo equipo se encuentra en uno de dichos segmentos de la red, con el fin de encontrar las vías que dispone este supuesto empleado, para acceder a información sensible a la que no está autorizado.

Otro posible rol que es utilizado en este tipo de auditorías es el de un invitado de la empresa, que se conecta con su equipo a la red corporativa con el mismo objetivo, visualizar o sustraer información sensible. Los procedimientos, de la misma forma que antes, son los siguientes:

A) Diseño, análisis de la topología de red y análisis de la segmentación
B) Análisis de seguridad de VLAN
C) Seguridad de los puntos de acceso (ARP spoofing)
D) Sniffing de red y análisis del tráfico de red
E) Escalada de privilegios en la red
F) Obtención de credenciales
G) Cifrado de comunicaciones
H) Análisis global de la información obtenida

Otras auditorias: De manera específica podemos encontrar un número importante de auditorías que implican la validación de desempeño técnico de servicios y tecnologías adjuntas a la infraestructura que pueden representar una importante brecha para el acceso no deseado de la información:

A) Auditoría Wireless
B) Auditoría web
C) Auditoría de aplicaciones
D) Auditoría forense

12.2.1.3.3. Análisis a realizar.

La tarea más importante del proyecto ha sido automatizar, dentro de lo que cabe y orientándolo siempre a los resultados que se buscan y que se han considerado importantes, las herramientas de auditoría y descubrimiento de vulnerabilidades.

Se ha definido como Análisis al conjunto de pruebas que proporcionan información suficiente como para obtener conclusiones acerca del estado de una red y de los servicios, hosts y puertos que se encuentran activos.

En el análisis se utilizan principalmente las herramientas NMap, OpenVAS, Nessus y Shodan, en las que su función se detallará en los siguientes sub-apartados.

Análisis NMap[4]

Se encarga de determinar para cada host activo, desde la dirección IP y la dirección MAC hasta el tipo de vendedor del dispositivo, pasando por parámetros como pueden ser el estado de los puertos, la duración del estado de cada puerto, los servicios que se ejecutan, el nombre asociado a cada dispositivo, el último reinicio, etcétera, todo ello redirigido a un fichero de salida con formato XML.

[4] Palacios, Jairo. [En línea]. Análisis de Vulnerabilidades de una red corporativa mediante herramientas de descubrimiento activas. Trabajo Fin de Grado. Universidad de Sevilla.

NMap, además de analizar los puertos que están activos y los servicios que se ejecutan en ellos, mide la detección del sistema operativo en base a la comprobación de huellas TCP/IP. Para comprobarlo, NMap envía una serie de paquetes TCP y UDP al sistema remoto y analiza prácticamente todos los bits de las respuestas, posteriormente, compara los resultados de las pruebas como pueden ser el análisis de ISN de TCP, el soporte de opciones TCP, el análisis de IPID y las comprobaciones de tamaño inicial de ventana, con su base de datos. Esta base de datos consta de más de 1500 huellas de sistema operativo y cuando existe una coincidencia, se presentan los detalles del sistema operativo.

Análisis con SHODAN

Es una herramienta de evaluación web, una utilidad particular para los pentesters. Puede ser utilizado para recoger una serie de información inteligente sobre los dispositivos que están conectados a la Internet.

Podemos, por ejemplo, buscar para ver si todos los dispositivos de red, como routers, VoIP, impresoras, cámaras, etc, están en su lugar.

Para buscar si algún servicio se está ejecutando en el dominio, la sintaxis sería: hostname:target.com port:80,21,22. Si deseamos simplemente conocer los resultados sobre el nombre de host, simplemente, la sintaxis seria: hostname:target.com

Análisis de Protocolos

NMap, a través del sondeo IP permite determinar qué protocolos (TCP, ICMP, IGMP, etcétera) soportan los sistemas objetivos. Esto no es técnicamente un sondeo de puertos, dado que cambian los números de protocolo IP en lugar de los números de puerto TCP o UDP.

El sondeo de protocolos utiliza mecanismos parecidos al sondeo UDP, enviando cabeceras de paquetes IP. Las cabeceras generalmente están vacías y no contienen datos. De hecho, ni siquiera tienen una cabecera apropiada para el protocolo que se indica. Las tres excepciones son TCP, UDP e ICMP.

Este tipo de sondeo espera la recepción de mensajes de ICMP (no alcanzable) en lugar de mensajes ICMP (puerto no alcanzable). NMap marca el puerto como abierto si recibe una respuesta en cualquier protocolo del sistema objetivo. Se marca como cerrado si se recibe un error ICMP de protocolo no. Si se reciben otros errores ICMP (no alcanzable) el puerto se marca como filtrado (aunque al mismo tiempo indican que el protocolo ICMP está abierto) y se marca como abierto/filtrado si no se recibe ninguna respuesta después de las retransmisiones.

Herramientas	Función principal	Características
NESSUS	Escaneo de vulnerabilidades de forma automática.	- Utiliza un escáner de puertos propio. - Realiza lanzamiento de exploits. - En la versión libre, sólo opera hasta 16 host. - Genera informes en diversos formatos. - Puede generar que los servicios se caigan. - Verifica la configuración errónea de un sistema y los parches faltantes.
SHODAN	Motor de búsqueda de dispositivos y host conectados a Internet con puertos abiertos.	- Utiliza una variedad de filtros. - Recoge datos de todos los servicios, incluyendo los puertos HTTP:80, HTTPS:443 – 8443, FTP:21, SSH:22, Telnet:23, SNMP:161 y SIP:5060. - Es una herramienta de evaluación web. - En la versión libre, sólo opera hasta 10 host. - Ayuda a localizar diversas tecnologías como webcams, impresoras, VoIP, routers, conmutadores, sistemas SCADA, etc.
QUALYS SSL	Verifica los suites de cifrado y los certificados digitales que utiliza un sitio web.	- Realiza un análisis profundo de la configuración de un servidor web SSL. - Permite configurar el HTTPS de un sitio web con la máxima seguridad. - Utiliza las tecnologías SSL, TLS y PKI.
OPENVAS	Escaneo de vulnerabilidades.	- Es un framework para la evaluación de vulnerabilidades. - Interconectado con más de 35.000 NVT (Network Vulnerability Test). - Utiliza el protocolo de transferencia OpenVAS (OTP). - Verifica el cifrado SSL para la comunicación. - Muestra las vulnerabilidades por CVE.
NMAP	Exploración y auditoría de seguridad de redes TCP/IP.	- Es gratuita de código abierto. - Diseñado para escanear rápida, sigilosa y eficazmente host individuales y redes de gran tamaño. - Explora equipos remotos mediante secuencias de paquetes TCP/IP. - Muestra la tabla de puertos abiertos de los servicios que no se utilizan. - Muestra los protocolos, servicios, directorios, usuarios y vulnerabilidades, los cuales utiliza para su acceso o explotación.

Tabla 3. Matriz de Apps de Pruebas de análisis de vulnerabilidades / penetración.

12.2.2. Descubrimiento y análisis de vulnerabilidades equipos en la red (LAN).

El presente numeral presenta las actividades realizadas en las redes internas de la compañía. Se describen las actividades realizadas para determinar las tecnologías operativas y contenidas en los equipos de cómputo y de comunicaciones, así como las pruebas ejecutadas para determinar las vulnerabilidades en cada una.

El primer objetivo de las pruebas realizadas a las redes locales, es realizar un escaneo y verificación de los operativos instalados, puertos abiertos, aplicaciones y tecnologías que hacen parte de cada una. Mediante la identificación de los sistemas, se ha considerado incluir una plantilla de aseguramiento de las más relevantes (WIN10), con el fin de que La Compañía mantenga el control mínimo requerido y así asegurar su correcto funcionamiento minimizando las vulnerabilidades de cada recurso informático. Si bien los equipos de cómputo de las redes internas, no alojan directamente información de la compañía, es necesario mantener los equipos en condiciones de seguridad adecuadas con el fin de evitar que puedan acceder de manera mal intencionada a la información de los usuarios y contraseñas de las plataformas y así contar con accesos no autorizados al recurso de información y contenidos de la empresa.

El segundo objetivo tiene que ver con la realización de un análisis de vulnerabilidades aplicando tecnologías disponibles. Este análisis se realizará con el fin de alertar a la compañía y a sus aliados sobre posibles puertas que hacen actualmente vulnerable su(s) sistema(s). El resultado será un compendio de recomendaciones a cerca de las acciones a ejecutar que permitan aplicar los controles adecuados minimizando su exposición y la probabilidad de que una amenaza se materialice (modificación, acceso no deseado, extracción, ransomware, perdida, DoS en la información de la organización).

12.2.2.1. Recopilación de información en campo.

La primera actividad fue realizar una recopilación en campo de la información. Es decir nos entrevistamos con el personal tanto administrativo como técnico con el fin de obtener información relevante de los sistemas (ver numeral 12.1. Verificación inventario.).

De los recursos tecnológicos de usuario final o computadores, se encontró que al menos 19 de ellos (de 46 equipos del inventario) cuentan con sistema operativo Windows 8 el resto tienen Windows 10 instalado. De acuerdo con la información suministrada las maquinas cuentan con su licencia al día. El servicio de office se accede por medio de 365.

De acuerdo con esto, como primera medida se recomendará migrar estas máquinas WIN8 a WIN10, pues el soporte tipo Mainstream de WIN8 ya caducó.

Client operating systems	Latest update or service pack	End of mainstream support	End of extended support
Windows XP	Service Pack 3	14 April 2009	8 April 2014
Windows Vista	Service Pack 2	10 April 2012	11 April 2017
Windows 7 *	Service Pack 1	13 January 2015	14 January 2020
Windows 8	Windows 8.1	9 January 2018	10 January 2023
Windows 10, released in July 2015 **	N/A	13 October 2020	14 October 2025

Figura 3 Soporte Microsoft S.O.

Por otra parte, los equipos no se encuentran en red tipo "Active Directory" o Dominio. Operan en grupo de trabajo lo que hace que su administración no sea centralizada, haciéndola más compleja. Recordemos que una red con un dominio configurado permite implementar políticas de seguridad entre muchas otras características que permitirán contar con una red más segura y más estable, ya que todos los equipos se regirían por parámetros de centralización y administración única.

Una vez realizada la inspección y verificación de los activos, se logró establecer otras características de la red que nos permitieron perfilar su estado y posibles vulnerabilidades, es decir, ir armando un perfil de las posibles vulnerabilidades. Acorde con este análisis inicial logramos encontrar que:

- El estado de la red cableada, cuenta con puntos de red desplegados en categoría 5, 5E y 6. Su administración aunque es centralizada, se encuentra expuesta físicamente y en cualquier momento podría prestarse por ejemplo para la conexión de un sniffer.

- De igual manera el cableado cuenta con puntos en desuso y/u obsolescencia, lo que hace que puedan existir puntos de conexión no controlados, permitiendo posible acceso no autorizado a la red.

- Los equipos de red local cableada ethernet no son administrables, y aunque no se encontraron problemas o vulnerabilidades, no permiten asegurar de la mejor manera la red (Equipos TP-LINK). Aun cuando estos equipos no se encontraban incluidos en el alcance inicial de verificación, se realizó una corrida con NMap para verificar su estado.

- Existen 4 redes inalámbricas, cada una cuenta con una cantidad no muy organizada de equipos. Puede presentarse un crack de las redes inalámbricas exponiendo el tráfico que pasa por estás. Aun cuando estos equipos no se encontraban incluidos en el alcance inicial de verificación, se realizó una corrida con NMap para verificar su estado. Se recomienda que esta conexión cuente con una red de invitados y el resto de equipos internos accedan por medio de control de las MAC que se conectan (hay que verificar que los Access Point permitan esta configuración).

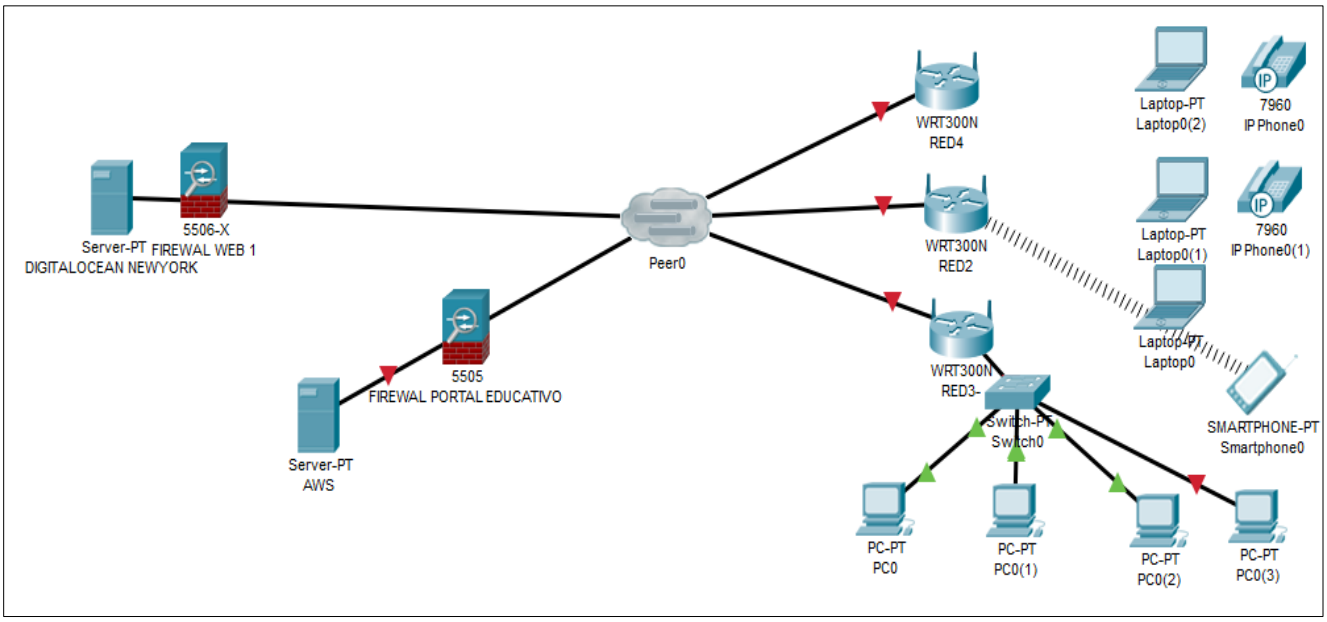


Figura 4 Diagrama de red – aplicativos.

12.2.2.2. Análisis de vulnerabilidades de la red interna.

A continuación, se presentan las actividades realizadas en la red interna de la sede F de La compañía. Se describen las actividades realizadas para determinar las tecnologías operativas, así como las pruebas ejecutadas para determinar las vulnerabilidades en cada una.

Actividades sobre las redes 2, 3 y 4:

El primer objetivo de las pruebas realizadas al interior de la red local de la sede F, es realizar un escaneo de aplicaciones o tecnologías detectando sistemas operativos. Mediante la identificación de las aplicaciones operantes, se ha considerado incluir las plantillas de aseguramiento de las más relevantes, con el fin de que La Compañía mantenga el control mínimo requerido, y así, asegurar su correcto funcionamiento minimizando las vulnerabilidades de cada sistema operativo.

El segundo objetivo tiene que ver con la realización de un análisis de vulnerabilidades aplicando las tecnologías disponibles. Este análisis se realizará con el fin de alertar a la compañía y a sus aliados sobre posibles puertas que hacen actualmente vulnerable su(s) sistema(s). El resultado será un compendio de recomendaciones a cerca de las acciones a ejecutar que permitan aplicar los controles adecuados minimizando su exposición y la probabilidad de que una amenaza se materialice (virus, malware, adware, spyware, worms, TroyanHorse, Hijackers, keylogger y crackers), afectando los usuarios de la empresa e incluso recopilando información que pueda permitir el acceso a las plataformas criticas (portales web).

Para mantener la protección de la información de la compañía, se mencionaran los segmentos de red como Red 2, 3 y 4 (la red 1 no cuenta con hosts asignados actualmente). Al llamarlas red 2, 3 y 4 queremos indicar que están segmentadas y que no cuentan con conectividad entre sí.

La primera actividad realizada posterior a la identificación física de las instalaciones, fue realizar un escaneo inicial para descubrir los host existentes en cada segmento de red.

Para realizar este escaneo se utilizó Nessus y Nmap. Durante la primera sesión de escaneo se tuvo problemas para realizar el análisis, ya que no había claridad sobre la configuración y topología lógica de las redes. Esta información no estuvo disponible desde el grupo de IT, lo cual dificultó el proceso de descubrimiento. Si bien esto representó una dificultad, el reto para el grupo era determinar el grado de seguridad de la infraestructura, precisamente tratando de ingresar sin contar con mayor información.

Durante la realización de la actividad de descubrimiento, se presentaron algunos inconvenientes con las herramientas de escaneo especialmente con Nessus y OpenVas pues presentaron problemas de instalación y no arrojaban resultados de las pruebas ejecutadas (aun cuando se conoce el potencial de OpenVas, este no funcionó correctamente en el proceso de ejecución del proyecto).

Una vez se garantizó el correcto funcionamiento de las aplicaciones de análisis de vulnerabilidades, se realizó una nueva visita para ejecutar nuevas pruebas, en donde la conexión a los sistemas y su descubrimiento se logró establecer de manera correcta. En este caso el apoyo del personal de IT indicando algunas características de las conexiones a red, facilitó el proceso y correcto descubrimiento de los equipos dentro de la red. El descubrimiento se ejecutó por medio de NMAP y Nessus.

Posteriormente, con estas mismas herramientas se realizó el escaneo completo para determinar las vulnerabilidades de los sistemas encontrados dentro de la red. Durante la ejecución y corrida de los escaneos planteados, la herramienta Nessus bloqueó la ejecución de algunos de los procesos por haber superado las IP de la versión de evaluación, con lo cual fue necesario finalizar algunas de las direcciones con NMAP (Red 3 específicamente). Los resultados se muestran en el Capítulo 13.1.Resultados sobre análisis de redes internas.

12.2.3. Análisis de vulnerabilidades a portales web.

A continuación, se presentan las actividades realizadas en las plataformas web de la compañía, se describen las actividades realizadas para determinar las tecnologías operativas y contenidas en los portales, así como las pruebas ejecutadas para determinar las vulnerabilidades.

El primer objetivo de las pruebas realizadas a las plataformas publicadas en internet, es realizar un escaneo de aplicaciones o tecnologías que hacen parte de cada una. Mediante la identificación de las aplicaciones operantes, se ha considerado incluir las plantillas de aseguramiento de las más relevantes, con el fin de que La Compañía mantenga el control mínimo requerido y así asegurar su correcto funcionamiento minimizando las vulnerabilidades del sistema informático. Como las aplicaciones basadas en servicios web se encuentran en "*hosting"*, al entregar las plantillas de aseguramiento a estos terceros, se asegurará que los servicios se encuentren bajo los parámetros mínimos para mantener el sistema asegurado y bajo sus propios requerimientos.

El segundo objetivo tiene que ver con la realización de un análisis de vulnerabilidades aplicando tecnologías disponibles. Este análisis se realizará con el fin de alertar a la compañía y a sus aliados sobre posibles puertas que hacen actualmente vulnerable su(s) sistema(s). El resultado será un compendio de recomendaciones a cerca de las acciones a ejecutar que permitan aplicar los controles adecuados minimizando su exposición y la probabilidad de que una amenaza se materialice (modificación, acceso no deseado, extracción, ransomware, perdida, DoS en la información de la organización). Es de resaltar que las pruebas se realizaron de manera externa, es decir no se realizaron con autenticación.

12.2.3.1. https://LaCompañía.com.co.

La primera actividad ejecutada fue usando la aplicación Wappalyzer, que permite identificar bajo que plataformas se encuentra desarrollado el portal web.

Posteriormente, se realizó un *"scan"* con SHODAN que es "un motor de búsqueda de "*banners"* de servicios, que son metadatos que el servidor envía de vuelta al cliente. Esta información puede ser sobre el software de servidor, qué opciones admite el servicio, un mensaje de bienvenida o cualquier otra cosa que el cliente pueda saber antes de interactuar con el servidor."[5]

[5] https://es.wikipedia.org/wiki/Shodan#cite_note-shodanabout-1

Para finalizar el escaneo inicial de verificación del sitio en internet, se ejecutó un motor web disponible que permite determinar en qué lugar se encuentra la IP y el *"page"* (hosting en este caso Digital Ocean).

12.2.3.1.1. Análisis de vulnerabilidades con Acunetix.

La siguiente actividad realizada estuvo directamente orientada a verificar la salud del sitio web. Se realizó un escaneo para verificar qué vulnerabilidades se podían encontrar en el portal web. El primero fue realizado con la herramienta Acunetix. Durante la ejecución, la herramienta produjo lentitud en el servicio web y a causa de esto fue necesario abortar la corrida dada la gran cantidad de recursos de red y peticiones que solicitaba la herramienta sobre el portal. Sin embargo, se obtuvieron resultados que demuestran que la ejecución de la tarea aun cuando tuvo que ser abortada, entrego resultados significativos. Los resultados de la corrida se presentan en el numeral
13.2.2. Vulnerabilidades Acunetix.

12.2.3.1.2. Análisis de vulnerabilidades con OWASP ZAP.

Luego de abortar el escaneo con la herramienta Acunetix, se realiza un nuevo escaneo a la aplicación web por medio de ZAP (OWASP). Esta aplicación permite realizar una configuración tal, que hace que la misma no represente una amenaza de daño o caída del activo a ser probado.

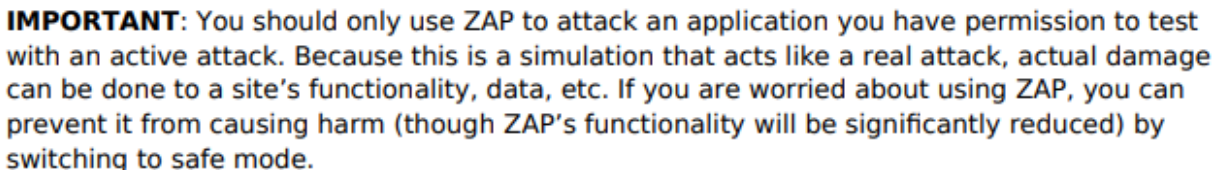


Figura 5 Mensaje de advertencia de ZAP.

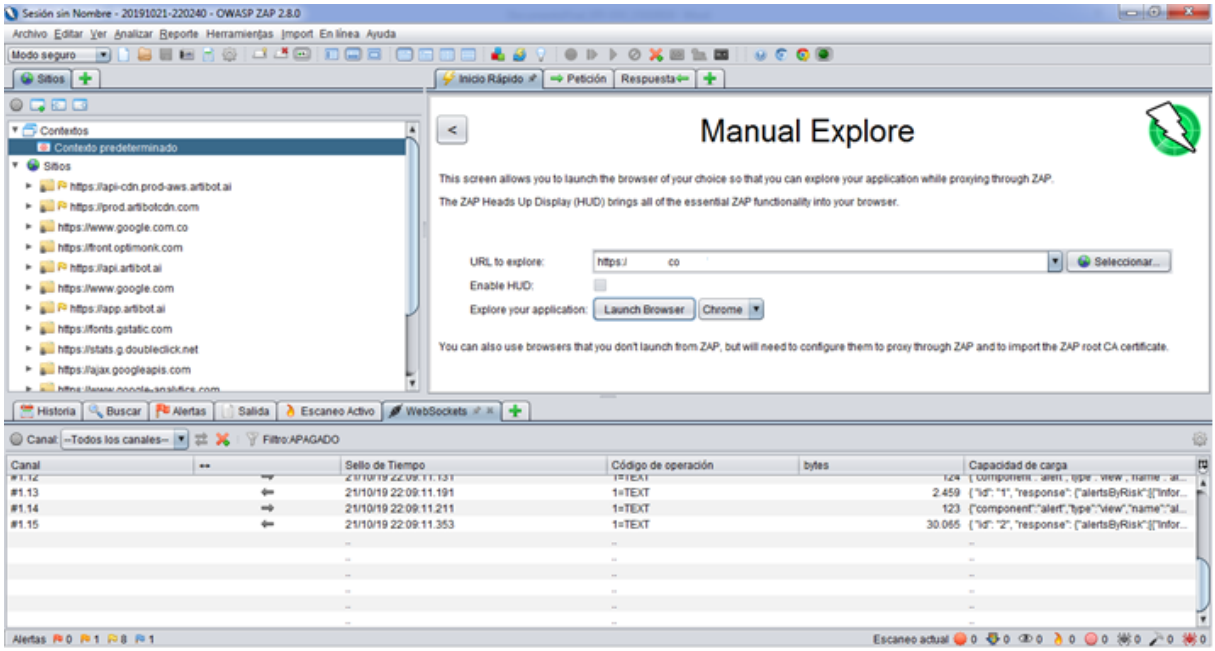


Figura 6 Pantalla Exploración manual de ZAP.

Los resultados se presentan en el numeral
13.2.3. Vulnerabilidades OWASP ZAP.

12.2.3.2. https://Lacompañía.academy.

De manera similar que con el portal lacompañia.com.co, la primera actividad ejecutada fue usando la aplicación Wappalyzer, que permite identificar bajo que plataformas se encuentra desarrollado el portal web.

Posteriormente, se realizó un *"scan"* con SHODAN que es "un motor de búsqueda de "*banners"* de servicios, que son metadatos que el servidor envía de vuelta al cliente. Esta información puede ser sobre el software de servidor, qué opciones admite el servicio, un mensaje de bienvenida o cualquier otra cosa que el cliente pueda saber antes de interactuar con el servidor."

Para finalizar el escaneo inicial de verificación del sitio en internet, se ejecutó un motor web disponible que permite determinar en qué lugar se encuentra la IP y el "page" (hosting en este caso Digital Ocean).

12.2.3.2.1. Análisis de vulnerabilidades con Acunetix.

La siguiente actividad realizada estuvo directamente orientada a verificar la salud del sitio web. Se realizó un escaneo para verificar qué vulnerabilidades podía presentar el portal web. El primero fue realizado con la herramienta Acunetix. A diferencia de la lentitud presentada en el portal web lacompañía.com.co, Acunetix finalizó el análisis sobre el portal Academy al 100% (Recordemos que esta cuenta esta bajo AWS). Se obtuvieron resultados los cuales son presentados en el numeral
13.2.2. Vulnerabilidades Acunetix.

12.2.3.2.2. Análisis de vulnerabilidades con OWASP ZAP.

Luego de abortar el escaneo con la herramienta Acunetix, y de igual manera que con el portal (lacompañia.com.co) se realizó un nuevo escaneo a la aplicación web por medio de ZAP (OWASP).

Los resultados se presentan en el numeral
13.2.3. Vulnerabilidades OWASP ZAP.

12.2.3.3. Análisis conexión base de datos.

Para esta plataforma se solicitaron permisos especiales de ventana de mantenimiento (Q10 / Talent IMS) para realizar pruebas, pero no asignaron el espacio para su realización.

12.2.4. Análisis y resultados de seguridad física.

Uno de los primeros pasos de la revisión de seguridad tiene que ver con la seguridad física y del entorno que permitan determinar si la información bajo las condiciones existentes se encuentra bajo niveles aceptables de riesgo.

El análisis de seguridad física realizado a las instalaciones de La Compañía / Y Aliados, se basan en los controles definidos en la norma ISO 27001 – 2013 (A.11).

ISO Ref.	Controles ISO/IEC 27001:13	Detalle del Control según la Norma	Notas	Descripción del cumplimiento	COSTO DEL CONTROL
A.11.	**SEGURIDAD FÍSICA Y AMBIENTAL**				
A.11.1.	**Áreas Seguras:** ***Objetivo***. *Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización. Aplicado a instalaciones de La Compañía / Y Aliados de la sede F (No aplica a servicios en hosting o tercerizados)*				
A.11.1.1.	Perímetro de seguridad física	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	N/A	**CUMPLE.** Las oficinas se encuentran localizadas en la sede F a una cuadra de la alcaldía de esta localidad. La amenaza por riesgo público para la compañía podría considerarse como bajo, ya que la probabilidad de que se presenten disturbios o una asonada en el área es baja (los disturbios más cercanos se presentaron en 2016 hacia la calle 13 con Av. Boyacá). De darse esto su impacto sería medio pues podrían darse pérdidas físicas (hardware) aunque no de información. Las oficinas se encuentran en un edificio de 3 pisos que en la parte inferior cuenta con oficinas de un Banco muy reconocido. Las cámaras del CCTV del banco brindan protección a La Compañía / Y Aliados pues el perímetro es compartido. (Y Aliados se encuentra en el piso 2 y 3). El ingreso a Y Aliados / La Compañía es por una puerta única, que se mantiene cerrada y únicamente se abre desde el interior (Recepcionista realiza apertura) por medio de una puerta controlado por electroimán. La entrada cuenta con enfoque de una cámara de video vigilancia interna.	N/A
A.11.1.2.	Controles físicos de entrada	Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	Costo aproximado del control kit de control de acceso y puerta.	**NO CUMPLE.** La zona o cuarto de los equipos de cómputo principales de la sede cuentan con una ruta oculta, pues para llegar a allí, se pasa por una pequeña oficina en donde se encuentran dos (02) puestos de trabajo. Es decir, el acceso de personal externo no es sencillo lo que brinda una buena protección a los equipos. Sin embargo, las personas que están dentro de esta pequeña oficina sí podrían entrar en contacto con los equipos. De la localización de los equipos de comunicaciones se tienen los siguientes comentarios: ✓ Los equipos se encuentran expuestos al contacto de cualquier persona que ingrese a esta área pues no hay una puerta que permita asegurar el acceso a los mismos. ✓ No se cuenta con un diagrama de red, que permita tener claridad de las conexiones físicas entre equipos. ✓ No hay hojas de vida de los equipos de comunicaciones que permitan determinar si el firmware esta actualizado o cual es el estado y configuración de los equipos. **Recomendaciones**: 1) Se recomienda implementar una puerta con seguridad electrónica que permita controlar el acceso a este recinto. Si no es posible implementar un control electrónico, se recomienda incluir una puerta con candado (la llave del candado deberá ser asignada a solo al personal definido para operar y mantener, y a la alta dirección o gerencia). 2) La documentación de hojas de vida de equipos y de diagrama de red es importante, pues evita que se tenga dependencia del personal encargado. Se recomienda realizar peinado de cableado en racks (uso de velcro o cintillos) y marquillado de puntos en los dos extremos.	2.000.000,00 COP

ISO Ref.	Controles ISO/IEC 27001:13	Detalle del Control según la Norma	Notas	Descripción del cumplimiento	COSTO DEL CONTROL
A.11.1.3.	Seguridad de oficinas, salones e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.	N/A	**CUMPLE**. Las instalaciones cuentan con seguridad perimetral y control de acceso para ingreso de personas. Al ingresar a las zonas comunes están protegidas con cámaras de CCTV IP. **Recomendación**: 1) Se recomienda mantener cerradas las salas que cuentan con equipos y que solo se abran cuando se requiera.	N/A
A.11.1.4.	Protección contra amenazas externas y ambientales	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	N/A	**CUMPLE**. La construcción del edificio en sí, está basada en edificación estructural tradicional (se desconoce si cumple NSR10). Al interior se implementa drywall para el cuarto de cómputo. En general los equipos de comunicación están protegidos en un recinto dedicado. Adicionalmente los equipos de comunicaciones cuentan con UPS (se recomienda verificar su funcionamiento y realizar mantenimiento y cambio de baterías de acuerdo con lo recomendado por el fabricante). **Recomendaciones**: 1) Revisar estructura de paredes internas del centro de cómputo. Si es drywall verificar que tenga refuerzo. EL cuarto aparenta estar en buenas condiciones sin embargo es necesario que se revise para determinar si hay un costo asociado para su mejora. 2) Implementar control A.11.1.2.	N/A
A.11.1.5.	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	Se recomienda para control interno para La Compañía / Y Aliados.	N/A	N/A
A.11.1.6.	Áreas de despacho y carga	Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde puedan ingresar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	N/A	N/A	N/A
A.11.2.	**Equipos:** ***Objetivo***. *Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. Aplicado a instalaciones de La Compañía / Y Aliados de la sede F (No aplica a servicios en hosting o tercerizados)*				
A.11.2.1.	Ubicación y protección de los equipos	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.	N/A	**NO CUMPLE**. Los equipos principales de telecomunicaciones se encuentran instalados en un rack de telecomunicaciones de 19". En cuanto al no cumplimiento Ver Control A.11.1.2. **Recomendación**: 1) Mejorar la instalación y disposición física de los Access Pont y Modem de Proveedores de servicio.	N/A

ISO Ref.	Controles ISO/IEC 27001:13	Detalle del Control según la Norma	Notas	Descripción del cumplimiento	COSTO DEL CONTROL
A.11.2.2.	Servicios públicos de soporte	Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.	Una UPS tipo torre puede costar 2500 USD. Pero se recomienda para rack con el fin de facilitar su organización.	**CUMPLE**. Los equipos de telecomunicaciones cuentan con UPS para entregar energía regulada a los equipos principales. Los equipos de usuario final no se encuentran conectados a una UPS, sin embargo la energía en el sector es estable. Los equipos de mayor relevancia como servidores de aplicaciones web (Digital Ocean-AWS3), contenido (Drive), BD (Q10) y Plataforma de cursos (AWS-Talent Lms) se encuentran en la nube tercerizados. Estos se encuentran cubiertos por las políticas de seguridad de la compañía que indican que la protección física, está definida y suministrada por sus contratistas y aceptadas por La Compañía / Y Aliados. La compañía cuenta con salida a internet de dos proveedores y aunque la operación de La Compañía / Y Aliados normalmente utiliza un proveedor especifico, se cuenta con la posibilidad de realizar un cambio para la contingencia. **Recomendación**: 1) Implementar UPS en todos los equipos de la empresa incluso en los de usuario final, con el fin de asegurar la energía a los equipos para evitar daños por sobretensiones o sobre corrientes. Se considera que se puede implementar una UPS de 5 KVA para rack, la cual puede costar unos 3500 USD + instalaciones adicionales.	13.475.000,00 COP
A.11.2.3.	Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.	Ver el costo en el control A.11.1.2.	**NO CUMPLE**. La zona o cuarto de los equipos de cómputo principales de la sede F cuentan con una ruta oculta, pues para llegar a allí, se pasa por una pequeña oficina en donde se encuentran dos (02) puestos de trabajo. Es decir, el acceso de personal externo no es sencillo lo que brinda una buena protección a los equipos. Sin embargo, las personas que están dentro de esta pequeña oficina sí podrían entrar en contacto con los equipos. De la localización de los equipos de comunicaciones se tienen los siguientes comentarios: ✓ Los equipos se encuentran expuestos al contacto de cualquier persona que ingrese a esta área pues no hay una puerta que permita asegurar el acceso a los mismos. ✓ No se cuenta con un diagrama de red, que permita tener claridad de las conexiones físicas entre equipos. ✓ No hay hojas de vida de los equipos de comunicaciones que permitir determinar si el firmware esta actualizado o cual es el estado y configuración de los equipos. **Recomendaciones**: 1) Se recomienda implementar una puerta con seguridad electrónica que permita controlar el acceso a este recinto. Si no es posible implementar un control electrónico, se recomienda incluir una puerta con candado (la llave del candado deberá ser asignada a solo al personal definido para operar y mantener y a la alta dirección o gerencia). 2) La documentación de hojas de vida de equipos y de diagrama de red es importante pues evita que se tenga dependencia del personal encargado. Se recomienda realizar peinado de cableado en racks (uso de velcro o cintillos) y marquillado de puntos en los dos extremos.	SIN DATOS

ISO Ref.	Controles ISO/IEC 27001:13	Detalle del Control según la Norma	Notas	Descripción del cumplimiento	COSTO DEL CONTROL
A.11.2.4.	Mantenimiento de equipos	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	N/A	**CUMPLE**. Se realizó revisión de las hojas de vida de los equipos. Se logró evidenciar que los equipos cuentan con mantenimiento preventivo y predictivo con fechas del segundo semestre del año en curso.	N/A
A.11.2.5.	Retiro de activos	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	N/A	**CUMPLE**. Aun cuando no se cuenta con una política de alta o baja de equipos, se entrevistó al personal que nos indicó que hay procedimientos y restricciones para el retiro de equipos y/o activos de la empresa. **Recomendación**: 1) Implementar una política de administración, manejo y control de activos informáticos / electrónicos.	N/A
A.11.2.6.	Seguridad de equipos y activos fuera del predio	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.	La mayoría de equipos son internos a excepción de los de ingeniería y gerencia. (4)	N/A	N/A
A.11.2.7.	Disposición segura o reutilización de los equipos	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.	La información está siempre en las plataformas de la empresa y no en equipos locales.	N/A	N/A
A.11.2.8.	Equipos sin supervisión de los usuarios	Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.	N/A	**CUMPLE**. Las aplicaciones y los equipos de cómputo cuentan con cierre y bloqueo de sesión automático.	N/A
A.11.2.9.	Política de escritorio limpio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	N/A	**NO CUMPLE**. No se evidencia que la empresa cuente una política diseñada para este control. Sin embargo, la mayoría de la información siempre se accede a través de aplicaciones web. **Recomendación**: 1) Elaborar política de escritorio limpio. (Aplicable más que todo a personal administrativo).	N/A

Tabla 4. Controles Seguridad Física – ISO 27001.

12.2.5. Verificación y actualización de políticas.

Del resultado del análisis de vulnerabilidades en cuanto a seguridad física se obtiene el nacimiento de dos nuevas políticas relacionadas con seguridad informática y de la información.

- POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA V0
- POLÍTICA DE GESTIÓN DE ACTIVOS INFORMÁTICOS V0

Si bien uno de los objetivos indicaba la necesidad de realizar una evaluación de las políticas existentes, durante el desarrollo del proyecto se confirmó la necesidad de crear estas dos nuevas políticas, las cuales se adjuntan como Anexo.

13. Resultados.

El presente capitulo describe los resultados de las pruebas realizadas a todos los objetivos descritos en el capítulo 12. Desarrollo. Las soluciones a estos resultados se describen en las tablas presentadas en el capítulo de discusión.

13.1. Resultados sobre análisis de redes internas.

A continuación, se describen los resultados encontrados durante las corridas de análisis de vulnerabilidades aplicadas a las redes internas de la sede F de la compañía, esencialmente se realizaron pruebas de penetración (sin explotación) por medio de Nessus y NMAP.

Al llamarlas red 2, 3 y 4 se quiere indicar que están segmentadas y que no cuentan con conectividad entre sí. Así mismo, cuando se refiere a un equipo por un número éste fue descrito de acuerdo con el **último octeto de la dirección IP**. El servidor DHCP contaba con rangos diferentes, por lo que se encontraran con números como 176 por ejemplo, sin que esto quiera decir que consecutivamente la empresa cuente con esa cantidad de hosts en la red. Para proteger la información de la compañía se ha omitido informaciones como nombres de red de equipos y direcciones MAC.

Red 1:

No presentó hosts asociados. Se realizó un escaneo con NMAP y Nessus. El descubrimiento arrojo cero (00) resultados. Posteriormente se realizó un chequeo con el personal de IT y se confirmó que en este segmento no había equipos asignados.

Por medio de Nessus se realizó un escaneo para verificar que no hubiese hosts, el resultado fue el esperado.

Red 2:

Por medio de Nessus se ejecutó un escaneo tipo "Discovery" el cual permitió determinar que en este segmento se encontraban cuatro (04) equipos conectados en red.

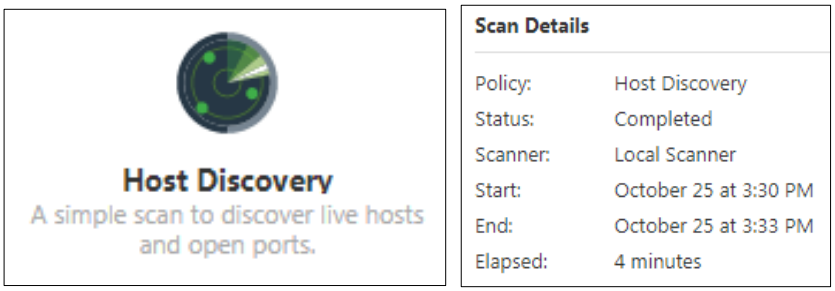


Figura 7 Nessus "Discovery" Red 2.

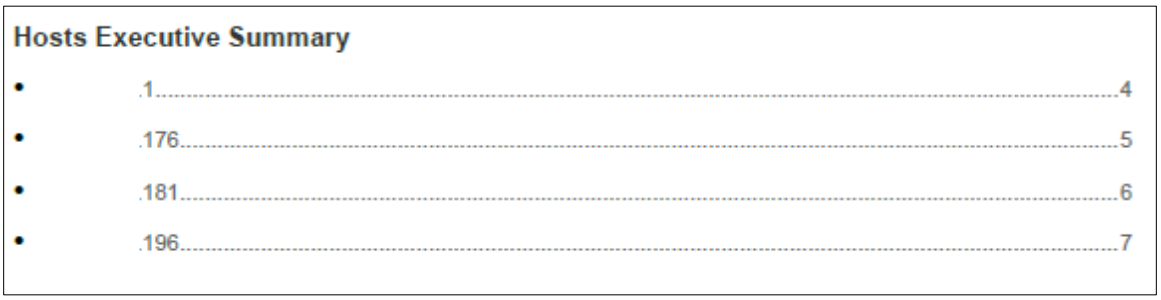


Figura 8 Nessus "Discovery" Red 2 ES.

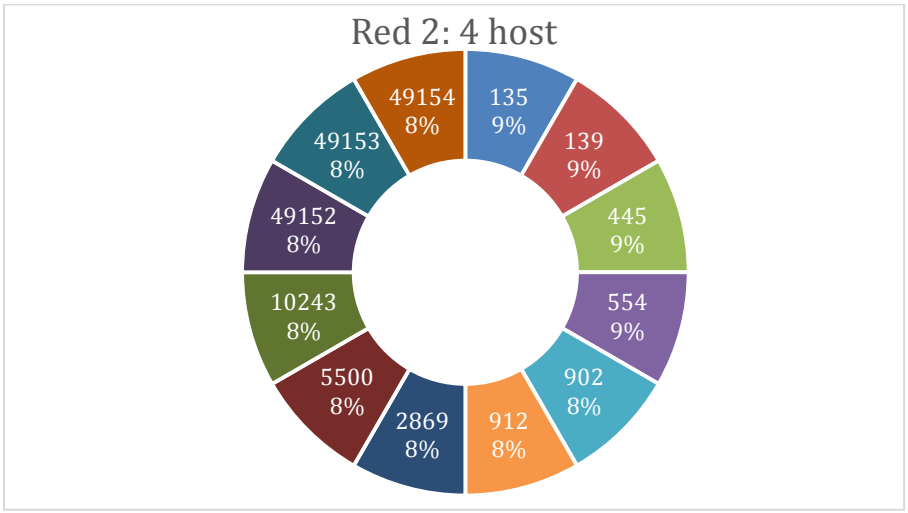


Figura 9 Puertos Red 2.

Como se puede observar, y mediante las diferentes herramientas, se obtiene los puertos abiertos en común para todos los hosts.

A continuación, se proceden a mostrar las gráficas que más información pueden aportar, así como una descripción de las mismas, explicando cuales son los campos relacionados entre sí, de qué herramientas se ha extraído esta información y que importancia tienen en el análisis. Actualmente el protocolo de seguridad más utilizado en las webs es el TLS 1.2, sin embargo, el protocolo TLS 1.3 es utilizado por los principales navegadores, quienes ya lo soportan.

Como el descubrimiento de red es exitoso, posteriormente se procede con las pruebas de vulnerabilidad, por medio de un escaneo básico completo. Es en este momento cuando la herramienta principal (Nessus), no permite realizar más pruebas, debido al uso del formato gratuito. Las máquinas que no se listan presentaron vulnerabilidades bajas o no presentan.

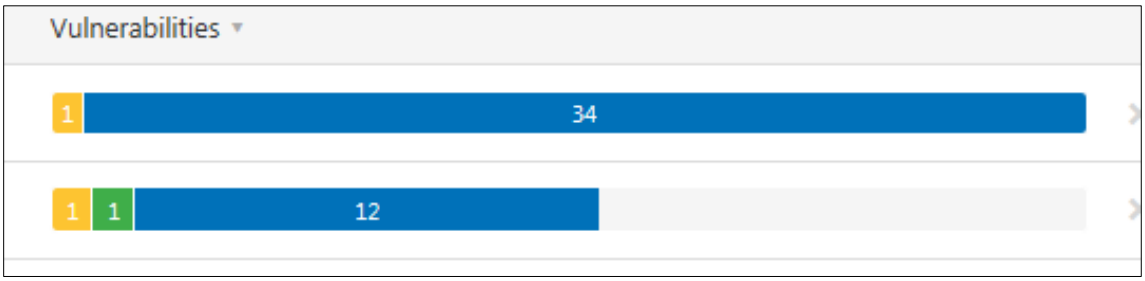


Figura 10 Nessus "Scan" Red 2 ES.

Los resultados hasta este momento, mostraron las siguientes vulnerabilidades:

1) **Equipo 1: 50686 - IP Forwarding Enabled.**

   Medio. El host remoto tiene habilitado el reenvío de IP. Un atacante lo puede explotar para enrutar paquetes a través del host y potencialmente omitir algunos firewalls / enrutadores / filtros NAC. A menos que el host remoto sea un enrutador, se recomienda deshabilitar el reenvío de IP. De acuerdo con la MAC address, este posiblemente es un equipo activo de red, razón por la cual la vulnerabilidad será informativa.

2) **Equipo 176: 57608 - SMB Signing not required.**

   Medio. No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado lo puede explotar para realizar ataques man-in-the-middle contra el servidor SMB.

Red 3:

Por medio de Nessus se ejecutó un escaneo tipo "Discovery", el cual permitió determinar que en este segmento se encontraban (17) equipos conectados en red.

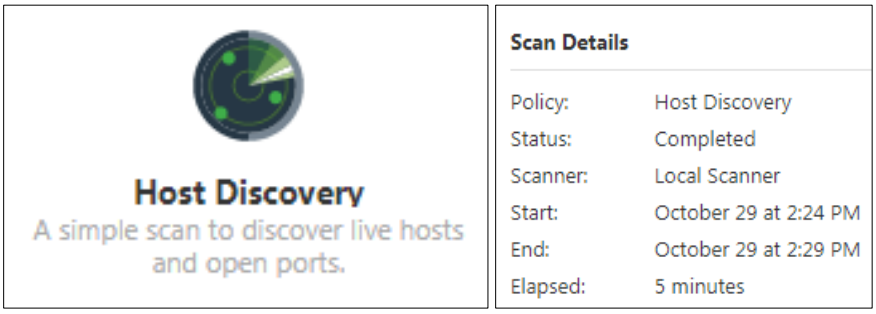


Figura 11 Nessus "Discovery" Red 3.

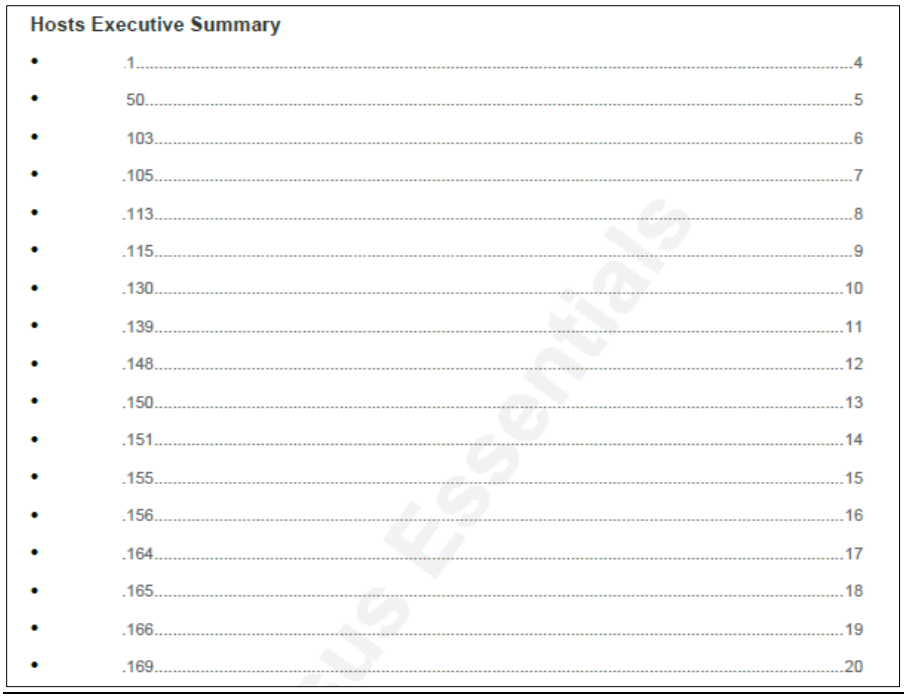


Figura 12 Nessus "Discovery" Red 3 ES.

Como el descubrimiento de red es exitoso, posteriormente se procede con las pruebas de vulnerabilidad, por medio de un escaneo básico completo. Es en este momento cuando la herramienta principal (Nessus), no permite realizar más pruebas, debido al uso del formato gratuito.

Los resultados hasta este momento mostraron la siguiente cantidad de vulnerabilidades para tres (03) máquinas:

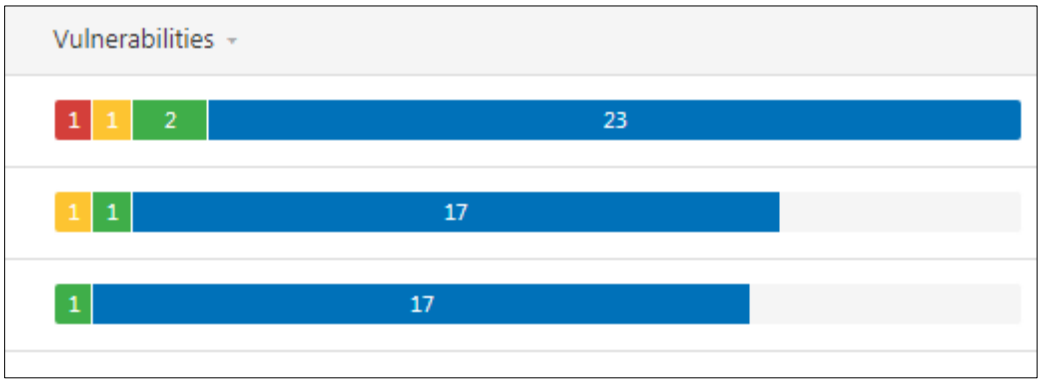


Figura 13 Nessus "Basic Scan" Red 3.

A continuación, se encuentra la descripción de tres (03) de las vulnerabilidades de severidad Alta y Media encontradas en estos tres (03) equipos:

1) **Equipo 50: Operative System: TP-LINK TL-WA901ND 4.0 Dropbear SSH Server < 2016.72 Multiple Vulnerabilities.**

   Alta. Dropbear SSH Server anterior a 2013.59 genera mensajes de error durante un intento de inicio de sesión fallido con diferentes retardos de tiempo en función de si existe la cuenta de usuario, lo que permite a atacantes remotos para descubrir los nombres de usuario válidos.

   Impacto:

   - Vector de acceso: A través de red.
   - Complejidad de Acceso: Baja.
   - Autenticación: No requerida para explotarla.

   Tipo de impacto:

   - No hay impacto en la integridad del sistema.
   - Afecta parcialmente a la confidencialidad del sistema.
   - No hay impacto en la disponibilidad del sistema.

2) **Equipo 50: Operative System: TP-LINK TL-WA901ND 4.0 Dropbear SSH Server < 2016.72 Multiple Vulnerabilities.**

Medio. Según su banner auto informado, la versión de Dropbear SSH que se ejecuta en este puerto es anterior a 2013.59. Como tal, se ve potencialmente afectado por múltiples vulnerabilidades:

- Una vulnerabilidad de denegación de servicio causada por la forma en que la función 'buf_decompress ()' maneja los archivos comprimidos. (CVE-2013-4421).
- La enumeración de usuarios es posible debido a un error de tiempo al autenticar a los usuarios. (CVE-2013-4434).

Posteriormente sobre la red 3 se continúa con las pruebas de vulnerabilidades **utilizando NMAP desde KaliLinux.** Las pruebas con NMAP se implementan mediante la ejecución del script:

```
root@kali:~# nmap -Pn -script vuln XXX.XXX.XXX.XXX/MASK
```

Ver: (https://www.stationx.net/nmap-cheat-sheet/) (https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/)

Por medio de este escaneo, se pudo determinar que en este segmento o red se encontraban (30) equipos conectados en red.

Las máquinas que no se listan presentaron vulnerabilidades bajas o no presentan. De la ejecución de NMAP se puede destacar los siguientes puertos abiertos:

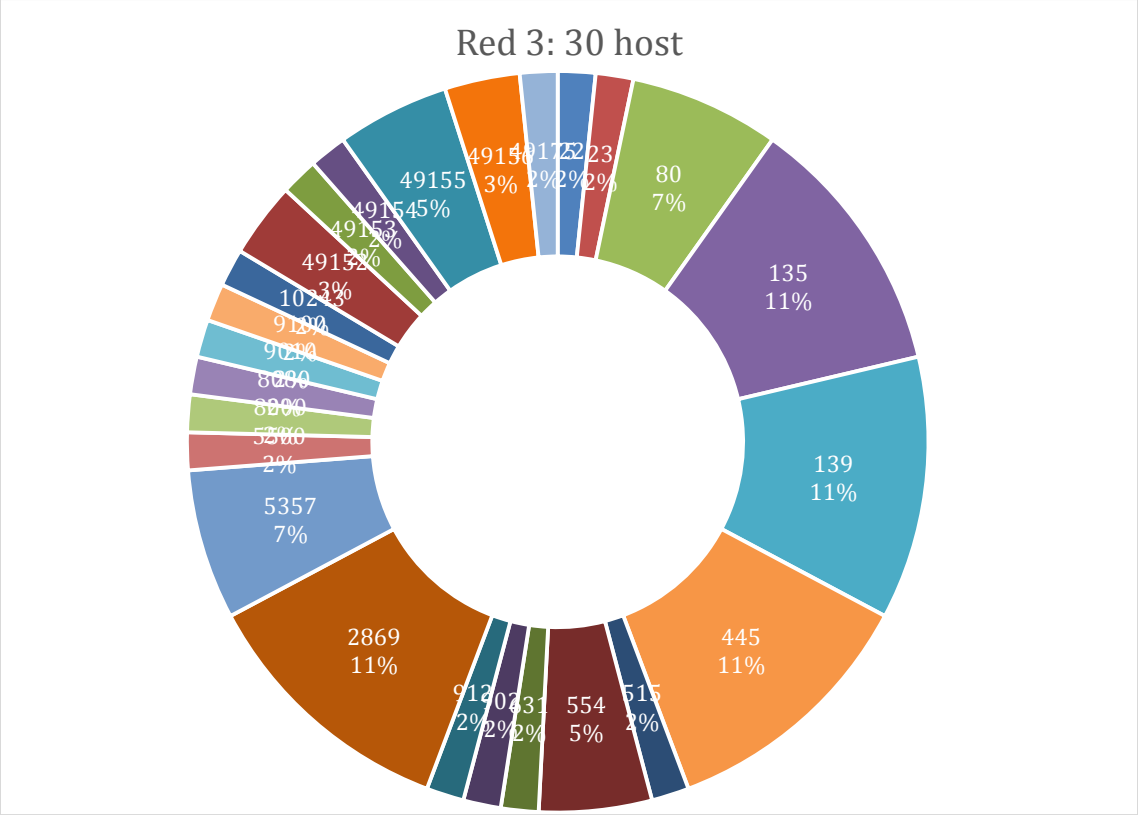


Figura 14 Puertos Red 3.

A) Equipo 1: 80 http consola sin autenticación requerida; 5500 tcp hotline.

B) Equipo 50: 20 ssh; 80 http; 49152 unknown.

C) Equipo 105: 80 tco http; 554 tcp rstp; 8000 tcp http-alt; 9010 tcp sdr.

D) Equipo 150: 80 http; 554 rtsp: 8000 http alt; 9010 tcp open sdr.

E) Equipo 115: 135 tcp msrpc; 139 tcp net-Biosssn; 445 tcp microsoft ds; 2869 tcp icslap; 49145 rcp desconocido.

F) Equipo 150: 135 tcp msrpc; 139 tcp netbios-ssn; 445 tcp microsoft-ds; 2869 tcp icslap; 5357/tcp wsdapi; 49155 tcp unknown.

G) Equipo 151: 135 tcp msrpc; 139 tcp netbios-ssn; 445 tcp microsoft-ds; 2869 tcp icslap; 5357/tcp wsdapi; 49155 tcp open unknown.

H) Equipo 155: 135 tcp msrpc; 139 tcp netbios-ssn; 445 tcp microsoft-ds; 2869 tcp icslap; 554 tcp rstp; 902 tcp iss-realsecure; 912 tcp apex mesh; 49162 – 10243 – 49153 – 49154 - 49175 tcp open unknown.

I) Equipo 181: 135 tcp msrpc; 139 tcp netbios-ssn; 445 tcp microsoft-ds; 2869 tcp icslap; 5357 tcp wsdapi; 49156 tcp unknown.

J) Equipo 188: 135 tcp msrpc; 139 tcp netbios-ssn; 445 tcp microsoft-ds; 554 tcp restp 2869 tcp icslap.
K) Equipo 189: 23 tcp telnet; 80 tcp http; 515 tcp printer; 631 tcp ipp; 8080 tcp http proxy; 9100 tcp jetdirect.

Sera necesario para La compañía / Y aliados, verificar qué servicios realmente requieren que estos puertos se encuentren abiertos y determinar qué aplicaciones cuentan en escucha los puertos desconocidos, para ejecutar los controles necesarios ya sea permitiéndoles este estado u obligando su cierre.

En esta misma corrida de NMAP, se encontraron las siguientes vulnerabilidades:

No vulnerabilidad, Equipos en general. Los equipos no son vulnerables a: Una denegación de servicio (bucle infinito) a través de un paquete UDP (1) IPv4 o (2) IPv6 vacíos al puerto 5353. NOTA: Esta vulnerabilidad existe debido a una corrección incorrecta del CVE-2010-2244. Esta prueba la ejecuta NMAp al iniciar el script.

1) **Equipo 1: Puerto 80 abierto. |_ /jmx-console/: Authentication was not required. cve2010-0738.**

   Alta. Este es un equipo de comunicaciones y su acceso por el puerto no requiere autenticación para entrar al web browser de configuración.

2) **Equipo 50: |_ /jmx-console/:Authentication was not required. cve2010-0738.**

   Ídem anterior.

   Medio. La aplicación web JMX-Console en JBossAs en Red Hat JBoss Enterprise Application Platform (también conocida como JBoss EAP o JBEAP) 4.2 antes 4.2.0.CP09 y 4.3 antes 4.3.0.CP08 realiza el control de acceso solo para los métodos GET y POST, lo que permite atacantes remotos para enviar solicitudes al controlador GET de esta aplicación utilizando un método diferente.

Medio. IDs: CVE:CVE-2007-6750 El servidor HTTP Apache 1.xy 2.x permite a los atacantes remotos causar una denegación de servicio (interrupción del demonio) a través de solicitudes HTTP parciales, como lo demuestra Slowloris, relacionado con la falta del módulo mod_reqtimeout en versiones anteriores a 2.2.15.

3) **Equipo 105: Vulnerabilidad en JBossAs en Red Hat JBoss Enterprise Application Platform (CVE-2010-0738).**

Medio. La aplicación web JMX-Console en JBossAs en Red Hat JBoss Enterprise Application Platform (también conocida como JBoss EAP o JBEAP) 4.2 antes 4.2.0.CP09 y 4.3 antes 4.3.0.CP08 realiza el control de acceso solo para los métodos GET y POST, lo que permite atacantes remotos para enviar solicitudes al controlador GET de esta aplicación utilizando un método diferente.

4) **Equipos 115/150/151/155/181: Vulnerables a CVE:CVE-2017-0143 - WannaCrypt attacks.**

Alta. La vulnerabilidad ha sido encontrada en Microsoft Windows (Operating System) y clasificada como **extremadamente crítica**. Una función desconocida del componente SMB es afectada por esta vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad. Existe una vulnerabilidad crítica de ejecución remota de código en los servidores SMBv1 de Microsoft (ms17-010).

El error fue descubierto el 2017-03-14. La vulnerabilidad fue publicada el 2017-03-14 con identificación MS17-010 con un bulletin (Technet) (confirmado). El advisory puede ser descargado de technet.microsoft.com. La vulnerabilidad es identificada como CVE-2017-0143. La vulnerabilidad es relativamente popular y aunque es muy compleja. El ataque puede ser realizado a través de la red. La explotación no requiere ninguna forma de autentificación. No son conocidos los detalles técnicos, pero hay un exploit público disponible.

Un *"exploit"* ha sido desarrollado por Sean Dillon en Python y publicado 2 meses después del anuncio. Fue declarado como altamente funcional. El exploit puede ser descargado de exploit-db.com. Hay un gusano que ya está automáticamente aprovechándose de la vulnerabilidad. Para el scanner Nessus se dispone de un plugin ID 97833 (MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) **(WannaCry)** (EternalRocks) (Petya) (uncredentialed check)), que puede ayudar a determinar la existencia del riesgo analizado.

Impacto:

- Vector de acceso: A través de red.
- Complejidad de Acceso: Baja.
- Autenticación: No requerida para explotarla.

Observación: Básicamente es posible tomar control del recurso informático.

5) Equipo 188: Vulnerable a smb-vuln-cve2009-3103 - Error en la gestión de recursos - cve2009-3103.

Alta. Error de índice de matriz en la implementación del protocolo SMBv2 en srv2.sys en Windows Vista versión Gold, SP1 y SP2, Windows Server 2008 versión Gold y SP2, y Windows 7 RC, de Microsoft, permite a los atacantes remotos ejecutar código arbitrario o causar una denegación de servicio (bloqueo de sistema) por medio de un carácter & (ampersand) en un campo de encabezado Process ID High en un paquete NEGOTIATE PROTOCOL REQUEST, que activa un intento de referencia de una ubicación de memoria fuera de límites, también se conoce como "SMBv2 Negotiation Vulnerability". NOTA: Algunos de estos datos fueron obtenidos de la información de terceros.

Tipo de impacto:

- Compromiso total de la integridad del sistema.
- Compromiso total de la confidencialidad del sistema.
- Compromiso total de la disponibilidad del sistema.

Red 4:

Por medio de Nessus se ejecutó un escaneo tipo "Discovery" el cual nos permitió determinar que en este segmento se encontraban ocho (08) equipos conectados en red.

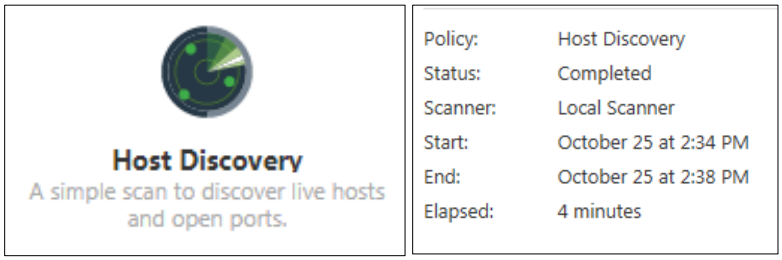
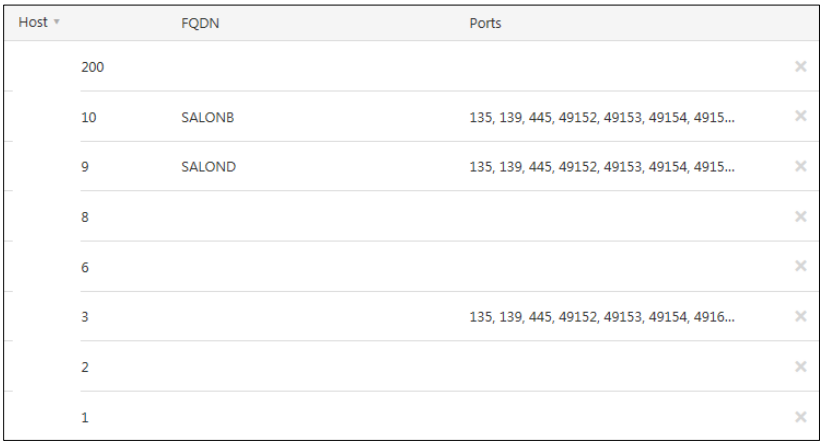


Figura 15 Nessus "Discovery" Red 4.



Host	FQDN	Ports
200		
10	SALONB	135, 139, 445, 49152, 49153, 49154, 4915...
9	SALOND	135, 139, 445, 49152, 49153, 49154, 4915...
8		
6		
3		135, 139, 445, 49152, 49153, 49154, 4916...
2		
1		

Figura 16 Nessus "Discovery" Red 4 ES.

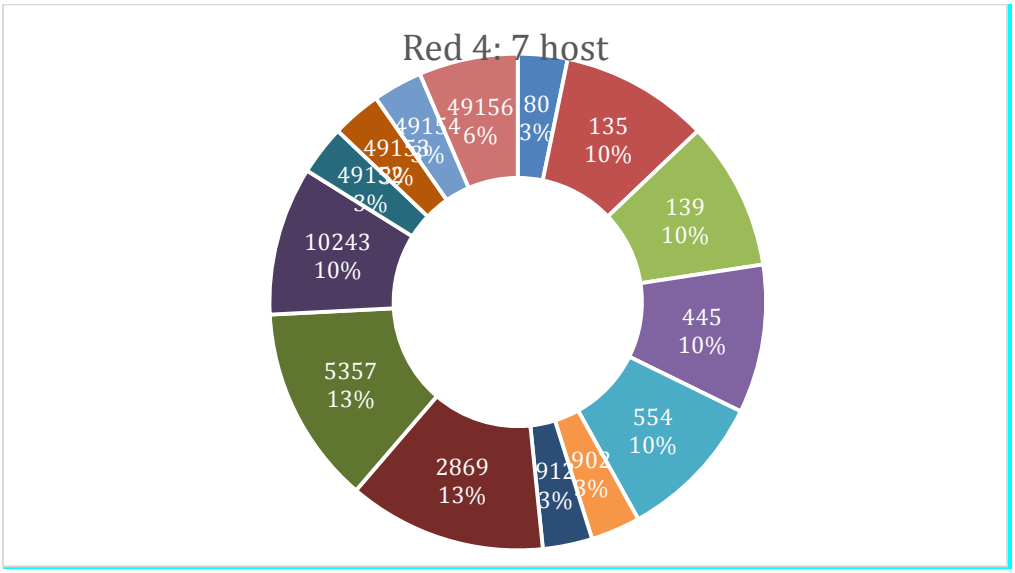


Figura 17 Puertos Red 4.

Es de notar, que en el análisis de vulnerabilidades de la Red 4, se encontraron 2 host vulnerables, con factor de riesgo alto y con CVE-2017-0143 (ms17-010).[6]

Esta actualización resuelve vulnerabilidades en Microsoft Windows. La más grave de estas vulnerabilidades podría permitir la ejecución remota de código si un atacante envía mensajes especialmente diseñados a un servidor de Microsoft Server Message Block 1.0 (SMBv1). Esta actualización de seguridad se considera crítica para todas las versiones compatibles de Microsoft Windows. La actualización de seguridad corrige las vulnerabilidades al corregir cómo SMBv1 maneja las solicitudes especialmente diseñadas.

Como el descubrimiento de red es exitoso, posteriormente se procede con las pruebas de vulnerabilidad, por medio de un escaneo básico completo. Las máquinas que no se listan presentaron vulnerabilidades bajas o no presentan.

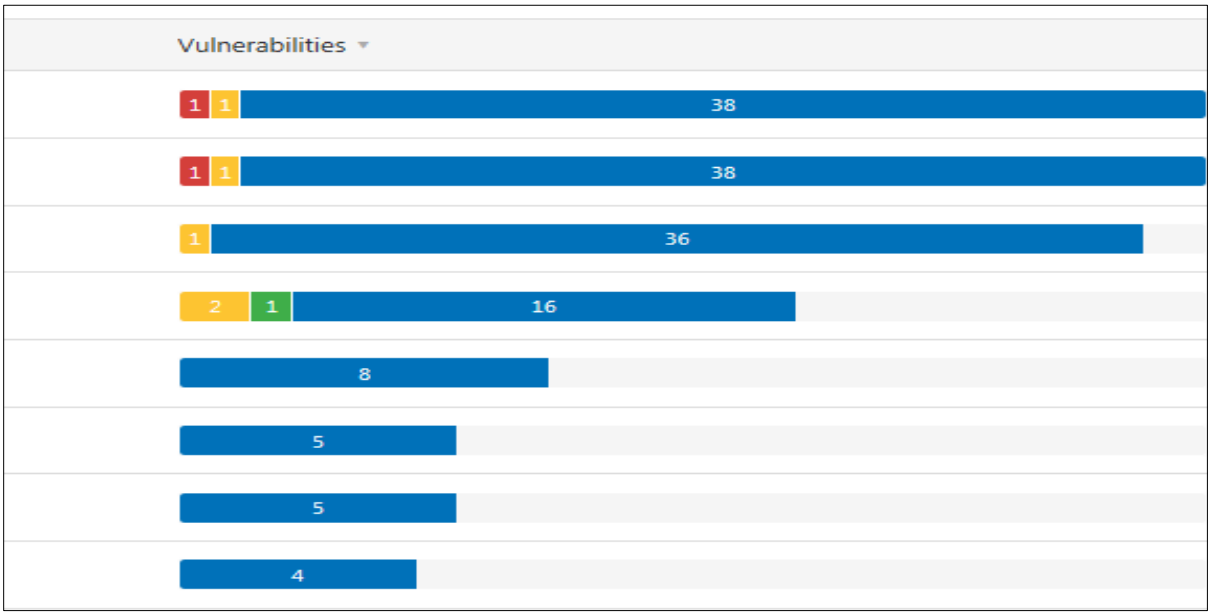


Figura 18 Nessus "Scan" Red 4 ES.

[6] Microsoft. (14-mar-2017). Boletín de Seguridad de Microsoft MS17-010 – Crítico. Tomado de: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010?redirectedfrom=MSDN

Los resultados hasta este momento mostraron las siguientes vulnerabilidades:

1) **Equipo 1 Telecomunicaciones: 12217 - DNS Server Cache Snooping Remote Information Disclosure.**

   Medio. El servidor DNS remoto responde a las consultas de dominios de terceros que no tienen establecido el bit de recursividad. Esto puede permitir que un atacante remoto determine qué dominios se han resuelto recientemente a través de este servidor de nombres, y, por lo tanto, qué hosts han sido visitados recientemente. Por ejemplo, si un atacante estaba interesado en saber si su empresa utiliza los servicios en línea de un particular o institución financiera, podrían usar este ataque para construir un modelo estadístico sobre el uso de la compañía de esa institución financiera. Por supuesto, el ataque también se puede utilizar para encontrar socios B2B, patrones de navegación web, servidores de correo externos y más.

2) **Equipo 1: 50686 - IP Forwarding Enabled.**

   Medio. El host remoto tiene habilitado el reenvío de IP. Un atacante puede explotar esto para enrutar paquetes a través del host y potencialmente omitir algunos firewalls / enrutadores / filtros NAC. A menos que el host remoto sea un enrutador, se recomienda deshabilitar el reenvío de IP. De acuerdo con la MAC address, este posiblemente es un equipo activo de red, razón por la cual la vulnerabilidad será informativa.

3) **Equipos 9 y 10: Vulnerable a CVE:CVE-2017-0143 - WannaCrypt attacks.**

   Alta. La vulnerabilidad ha sido encontrada en Microsoft Windows (Operating System) y clasificada como **extremadamente crítica**. Una función desconocida del componente SMB es afectada por esta vulnerabilidad. Por la manipulación de un input desconocido se causa una vulnerabilidad de clase desbordamiento de búfer. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad. Existe una vulnerabilidad crítica de ejecución remota de código en los servidores SMBv1 de Microsoft (ms17-010).

El error fue descubierto el 2017-03-14. La vulnerabilidad fue publicada el 2017-03-14 con identificación MS17-010 con un bulletin (Technet) (confirmado). El advisory puede ser descargado de technet.microsoft.com. La vulnerabilidad es identificada como CVE-2017-0143. La vulnerabilidad es relativamente popular y aunque es muy compleja. El ataque puede ser realizado a través de la red. La explotación no requiere ninguna forma de autentificación. No son conocidos los detalles técnicos, pero hay un exploit público disponible.

Un *"exploit"* ha sido desarrollado por Sean Dillon en Python y publicado 2 meses después del anuncio. Fue declarado como altamente funcional. El exploit puede ser descargado de exploit-db.com. Hay un gusano que ya está automáticamente aprovechándose de la vulnerabilidad. Para el scanner Nessus se dispone de un plugin ID 97833 (MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) **(WannaCry)** (EternalRocks) (Petya) (uncredentialed check)), que puede ayudar a determinar la existencia del riesgo analizado.

Impacto:

- Vector de acceso: A través de red.
- Complejidad de Acceso: Baja.
- Autenticación: No requerida para explotarla.

Observación: Básicamente es posible tomar control del recurso informático.

4) Equipos 9 y 10: 57608 - SMB Signing not required.

Medio. No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede explotar esto para realizar ataques man-in-the-middle contra el servidor SMB.

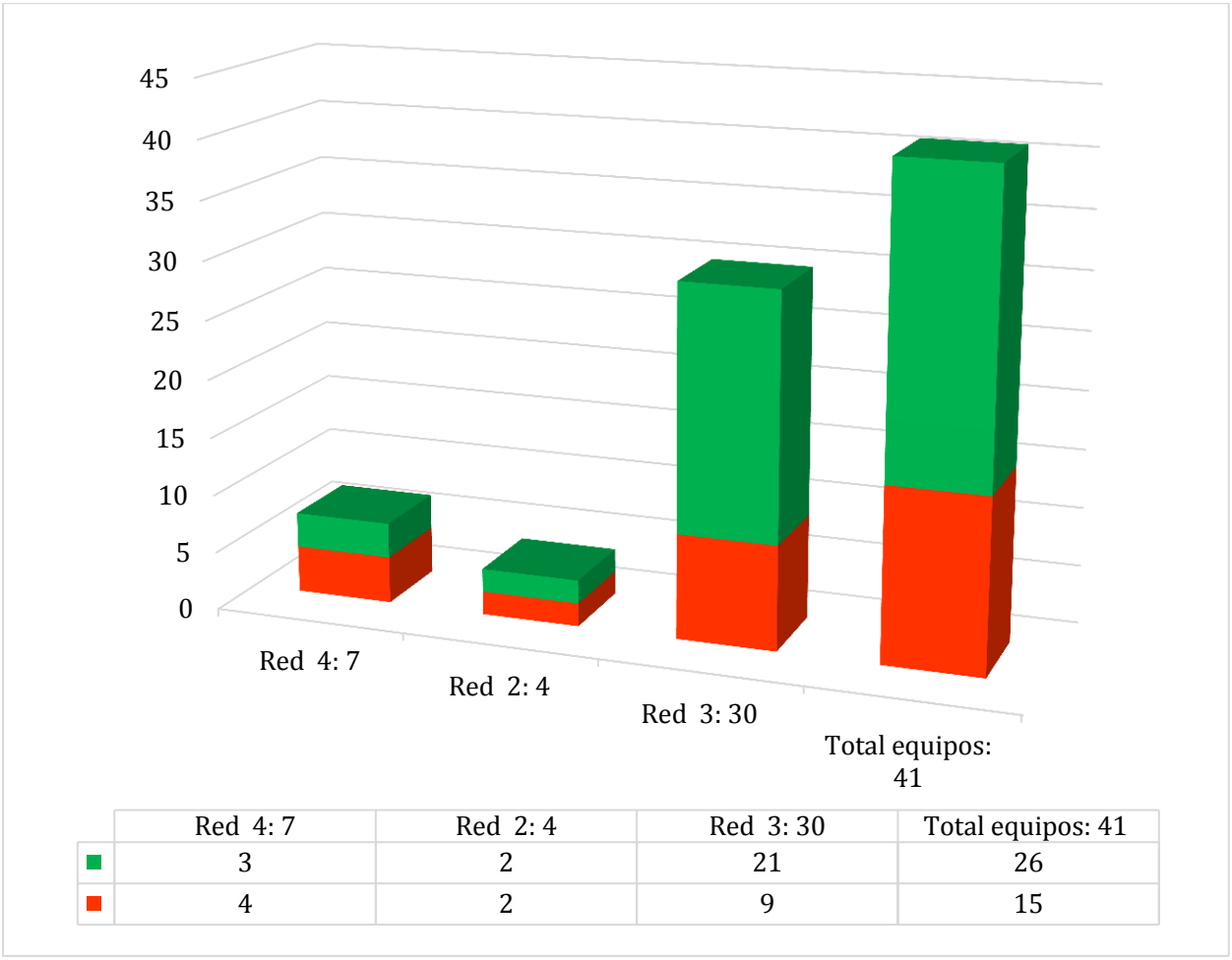
Aplicar la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva 'Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)'.

En Samba, la configuración se llama 'firma del servidor'. Puede configurar esta característica de seguridad abriendo la política adecuada y expandiendo el árbol de la consola como tal: Configuración del equipo \ Configuración de Windows \ Configuración de seguridad \ Políticas locales \ Opciones de seguridad \.

Para obtener instrucciones específicas sobre cómo configurar la configuración de la política de seguridad, consulte Editar la configuración de seguridad en un objeto de Política de grupo.

13.2.1. Resumen resultados sobre red interna.

Como se puede observar, y mediante las diferentes herramientas, se obtiene el 36% de los equipos con vulnerabilidades.



	Red 4: 7	Red 2: 4	Red 3: 30	Total equipos: 41
■	3	2	21	26
■	4	2	9	15

Figura 19 Resumen equipos (Verde: OK – Naranja: Vulnerable).

De acuerdo al histograma anterior y según en el análisis de vulnerabilidades de las diferentes redes de la entidad, se puede observar que existe un total de quince (15) equipos vulnerables, de los cuales diez (10) presentan factor de riesgo ALTO y nueve (09) con factor MEDIO (recordemos que hay equipos con vulnerabilidades con factor de riesgo medio y alto simultáneamente).

Las vulnerabilidades más sobresalientes se encuentran distribuidas en las redes existentes de la institución de acuerdo al siguiente gráfico, así:

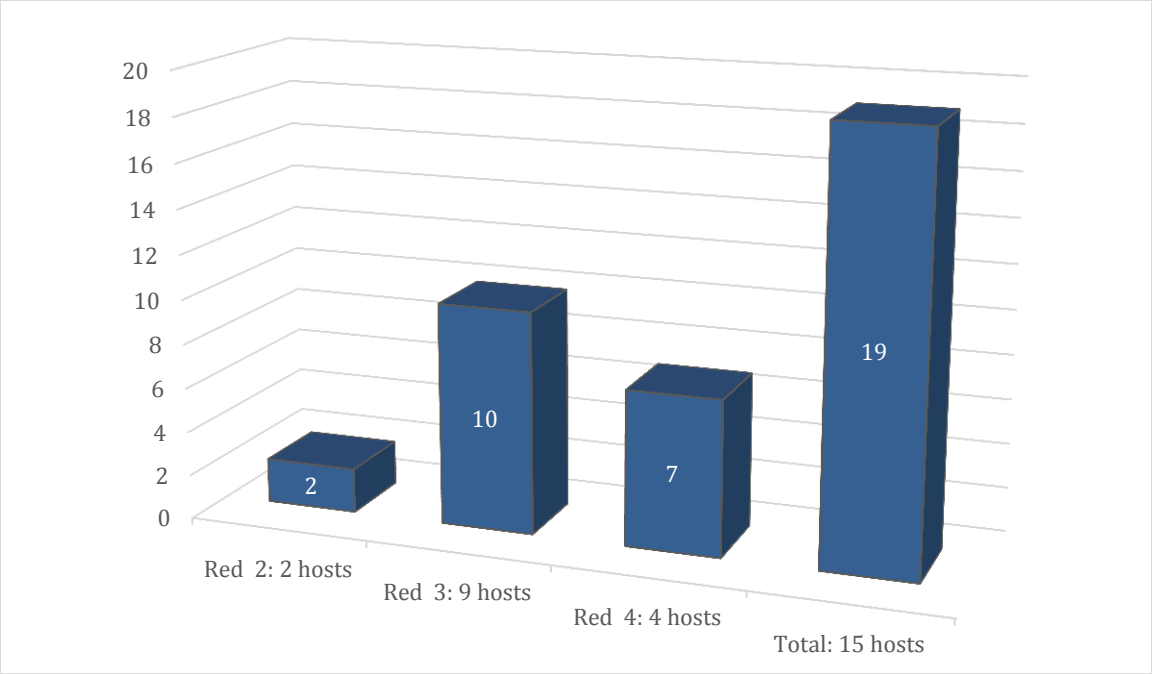


Figura 20 Resumen cantidad vulnerabilidades medias y alta.

Estas vulnerabilidades se encuentran documentadas anteriormente, y según el CVE están distribuidas entre las diferentes redes, así:

RED 2	RED 3	RED 4
2 host CVE-1999-0511 CVE-1999-0524	9 host CVE-2009-3103 CVE-2017-0143 CVE-2007-6750 CVE-2010-0738	4 host CVE-2017-0143

Figura 21 Vulnerabilidades.

Así mismo, se puede evidenciar la cantidad de equipos comprometidos por cada una de las vulnerabilidades, así:

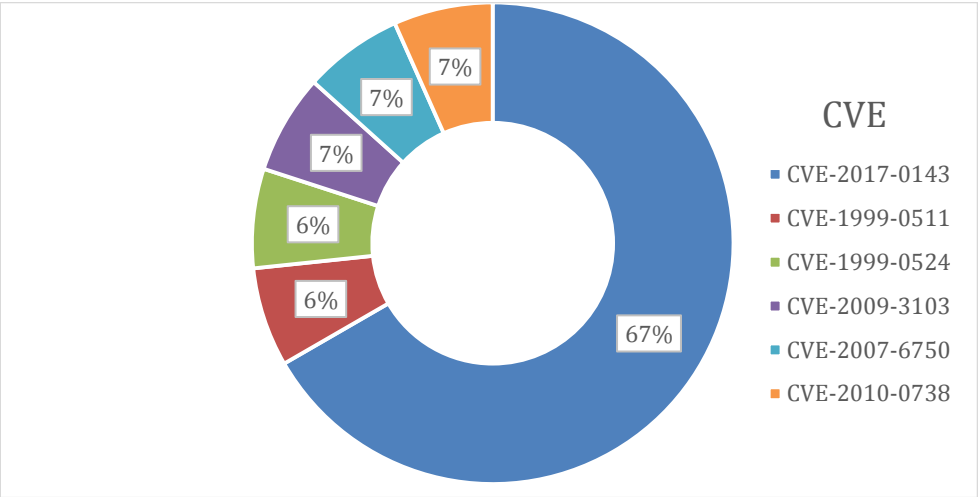


Figura 22 Vulnerabilidades 2.

De acuerdo al diagrama anterior, es posible denotar que el **60%** de los equipos o nueve (09) hosts, tienen la vulnerabilidad CVE-2017-0143 (ms17-010), el **06%** o un (01) host tiene las vulnerabilidades CVE-1999-0511 y CVE-1999-0524, y el resto posee las vulnerabilidades CVE-2009-3103, CVE-2007-6750 y CVE-2010-0738, estás dos últimas con factor de riesgo medio.

13.2. Resultados sobre https://La Compañía.com.co

A continuación se describen los resultados encontrados durante las corridas del análisis de vulnerabilidades aplicadas al portal web principal de la compañía. Es de anotar, que este se realizó esencialmente por medio de Qualys, Wappalyzer (reconocimiento de plataformas), Shodan (reconocimiento de plataformas), Acunetix ("Web *Pentesting tool*") y ZAP ("Web *Pentesting tool*").

Mediante el test de SSL de la empresa Qualys SSL Labs, se puede observar como la suma de los certificados de las aplicaciones que soportan la página educativa reciben una calificación de "A", por lo que es posible lograr un servicio HTTPS seguro y confiable. La evaluación con Qualys se realiza independientemente a cuatro (04) diferentes direcciones que sobrelleva está web, ya que es la encargada de alojar aplicaciones formativas y didácticas necesarias para el negocio de la entidad.

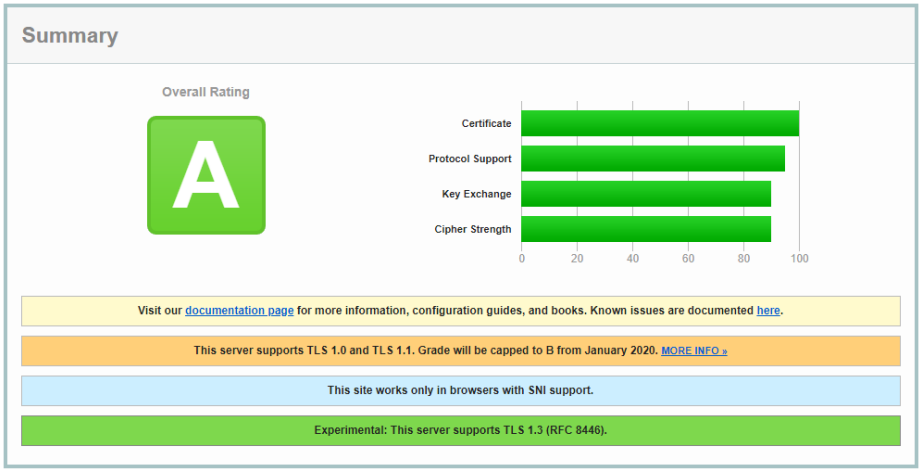


Figura 23 Qualys sobre lacompañia.com.co.

Sí se quiere obtener una evaluación de "A+", se deben realizar algunas configuraciones en el servidor de HTTPS.

13.2.1. Plataformas de desarrollo y operación.

Una vez ejecutada la aplicación Wappalyzer, las plataformas más relevantes encontradas en https://La Compañía.com.co fueron:

- Wordpress (gestor de contenidos web)
- Apache 2.4.18 (Servidor web)
- Ubuntu (sistema operativo)
- Mysql (Base de datos)

A continuación se muestran los resultados sin exponer información de la empresa:

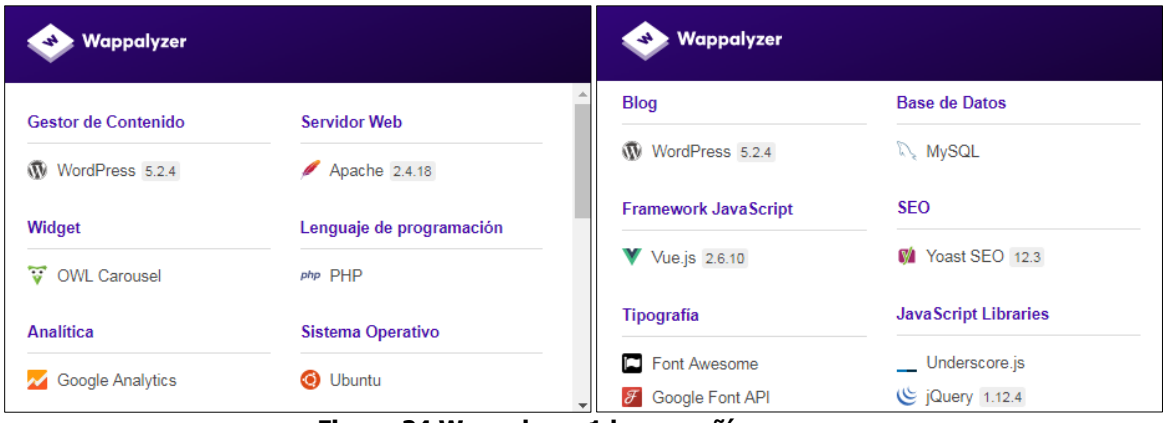


Figura 24 Wappalyzer 1 lacompañía.com.co.

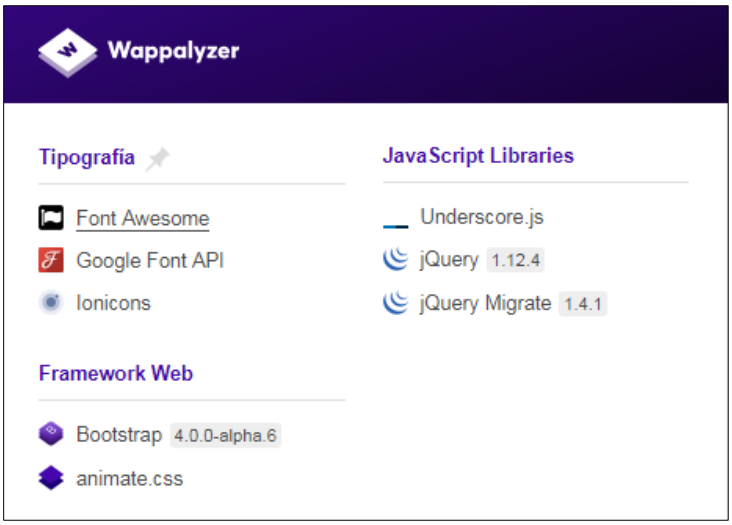


Figura 25 Wappalyzer 2 lacompañía.com.co.

Posteriormente al realizar las pruebas con SHODAN, en donde la seguridad de la plataforma no permitió que esta aplicación realizara escaneos y por consiguiente no muestra resultado alguno. Esto permite concluir que la pagina cuenta con protección y bloqueo contra escaneo externo. El bloqueo se presenta realizando consultas tanto en URL como con dirección IP.

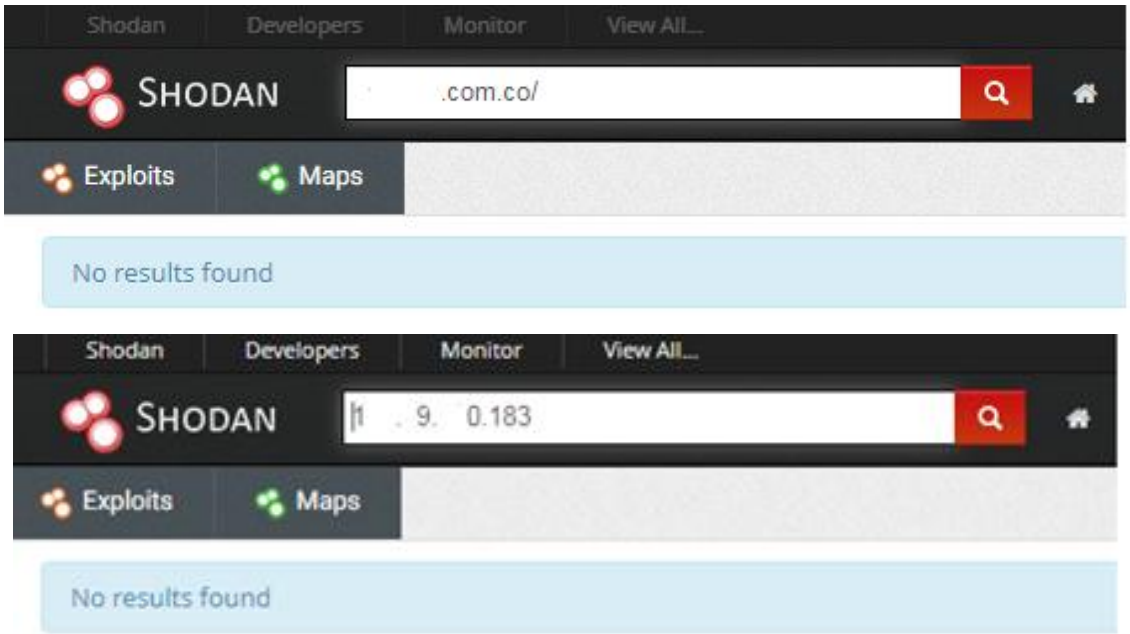
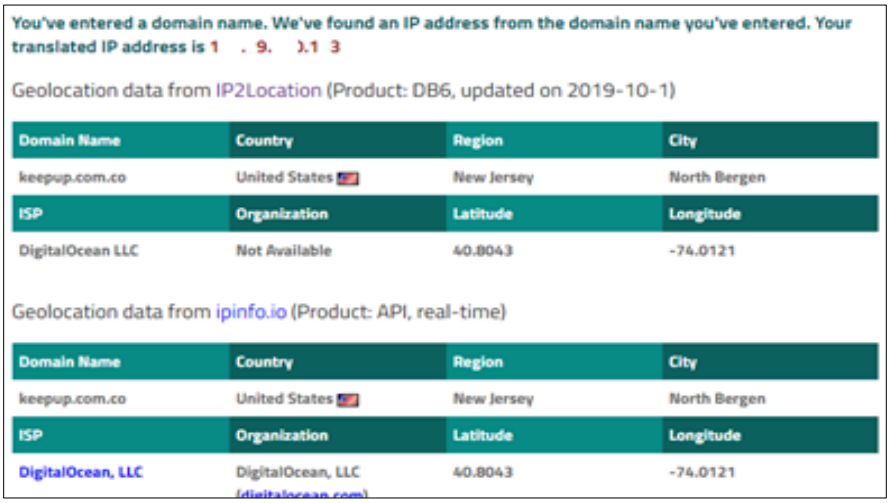


Figura 26 Shodan.

Para finalizar se utiliza un motor de localización de IP para determinar si los aplicativos se encuentran localizados de acuerdo con lo indicado y esperado por la compañía. Con esta información se verifica el dominio y la IP con la que se realizaron pruebas con Shodan.



You've entered a domain name. We've found an IP address from the domain name you've entered. Your translated IP address is 1 . 9.).1 3

Geolocation data from IP2Location (Product: DB6, updated on 2019-10-1)

Domain Name	Country	Region	City
keepup.com.co	United States	New Jersey	North Bergen
ISP	**Organization**	**Latitude**	**Longitude**
DigitalOcean LLC	Not Available	40.8043	-74.0121

Geolocation data from ipinfo.io (Product: API, real-time)

Domain Name	Country	Region	City
keepup.com.co	United States	New Jersey	North Bergen
ISP	**Organization**	**Latitude**	**Longitude**
DigitalOcean, LLC	DigitalOcean, LLC	40.8043	-74.0121

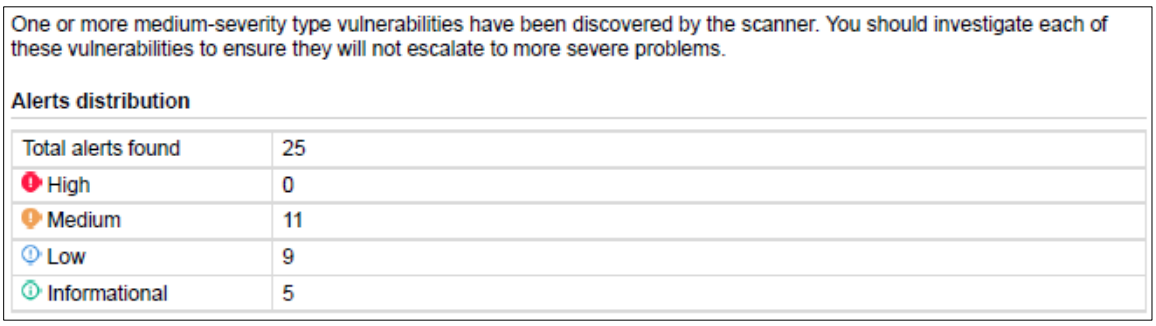
Figura 27 Localización portal web.

13.2.2. Vulnerabilidades Acunetix.

Por medio de Acunetix se logró identificar que el portal Web presenta las siguientes vulnerabilidades:

- 11 Vulnerabilidades de Severidad Media
- 09 Vulnerabilidades de Severidad Baja
- 05 Vulnerabilidades de tipo Informativo

Durante la ejecución de Acunetix, fue necesario parar el ataque pues la aplicación realiza muchas peticiones y ralentizó el tiempo de respuesta de la página web. Al abortar el ataque, este llevaba un avance de 67% en donde arrojo los siguientes resultados:



One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	25
High	0
Medium	11
Low	9
Informational	5

Figura 28 Resultados Acunetix portal web.

Por motivos de seguridad se omiten las pantallas en donde se puede visualizar la configuración y el objetivo del escaneo.

A continuación, se encuentra la descripción de cuatro (04) de las vulnerabilidades de severidad Media:

1) **Web Server - HTML form without CSRF protection.** Acunetix encontró un formulario HTML sin aparente protección anti-CSRF implementada. Consultar la sección 'Detalles del ataque' para obtener más información sobre el formulario HTML afectado.

   La técnica recomendada y más utilizada para prevenir los ataques de CSRF es conocido como un token anti-CSRF, también conocido como token sincronizador.

2) **Web Server - Slow HTTP Denial of Service Attack.** El servidor web es vulnerable a ataques HTTP DoS (denegación de servicio) lentos. Los ataques de Slowloris y Slow HTTP POST DoS se basan en el hecho de que el protocolo HTTP, por diseño, requiere que el servidor reciba completamente las solicitudes antes de que se procesen. Si una solicitud HTTP no está completa, o si la velocidad de transferencia es muy baja, el servidor mantiene sus recursos ocupados esperando el resto de los datos. Si el servidor mantiene demasiados recursos ocupados, esto crea una denegación de servicio.

3) **Web Server - TLS 1.0 enabled.** El servidor web admite el cifrado a través de TLS 1.0. TLS 1.0 no se considera una "criptografía sólida" según lo definido y requerido por el Estándar de seguridad de datos PCI 3.2 (.1) cuando se usa para proteger la información confidencial transferida hacia o desde sitios web.

4) **Web Server - Cookie(s) without HttpOnly flag set (verified).** Esta cookie no tiene establecido el indicador HttpOnly. Cuando una cookie se configura con el indicador HttpOnly, le indica al navegador que solo el servidor puede acceder a la cookie y no los scripts del lado del cliente. Esta es una protección de seguridad importante para las cookies de sesión.

13.2.3. Vulnerabilidades OWASP ZAP.

Una vez realizado el primer análisis, se realizó un escaneo con esta nueva herramienta (ZAP), para verificar que vulnerabilidades se encuentran en el portal web de la compañía. Este nuevo análisis arrojó los siguientes resultados:

- 02 Vulnerabilidades de Severidad Media
- 19 Vulnerabilidades de Severidad Baja
- 01 Vulnerabilidades de tipo Informativa

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	19
Informational	1

Figura 29 Resultados exploración manual de ZAP.

Por motivos de seguridad se omiten las pantallas en donde se puede visualizar la configuración y el objetivo del escaneo.

A continuación, se encuentra la descripción de algunas de las vulnerabilidades encontradas:

1) **Encabezado X-Frame-Options no establecido.** El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.

2) **Incompleto o no Cache-control y sistema de encabezado HTTP Pragma.** El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.

3) **Absence of Anti-CSRF Tokens**. No Anti-CSRF tokens were found in a HTML submission form.

Los ataques de CSRG son muy efectivos en varias situaciones, que incluyen:

a. La victima tiene una sesión activa en el sitio de destino.
b. La víctima se autoriza por medio de la autenticación HTTP en el sitio de destino.
c. La víctima se encuentra en la misma red local que el sitio de destino.

4) **Protección de buscador de web XSS no disponible.** La protección del buscador de web XSS no está disponible, o está deshabilitada por la configuración de la cabecera de respuesta de HTTP 'X-XSS-Protection' en el servidor de web.

13.3. Resultados sobre https://lacompañía.academy.

A continuación se describen los resultados encontrados durante las corridas del análisis de vulnerabilidades aplicadas al portal educativo de la compañía. Es de anotar, que este se realizó esencialmente por medio de Qualys, Wappalyzer (reconocimiento de plataformas), Shodan (reconocimiento de plataformas), Acunetix ("Web Pentesting tool") y ZAP ("Web Pentesting tool").

Mediante el test de SSL de la empresa Qualys SSL Labs, se puede observar como la suma de los certificados de las aplicaciones que soportan la página educativa reciben una calificación de "A", por lo que es posible lograr un servicio HTTPS seguro y confiable.

En el siguiente caso, se puede observar como el certificado que soporta la página de la empresa recibe una calificación de "A", por lo que es posible lograr un servicio HTTPS seguro y confiable.

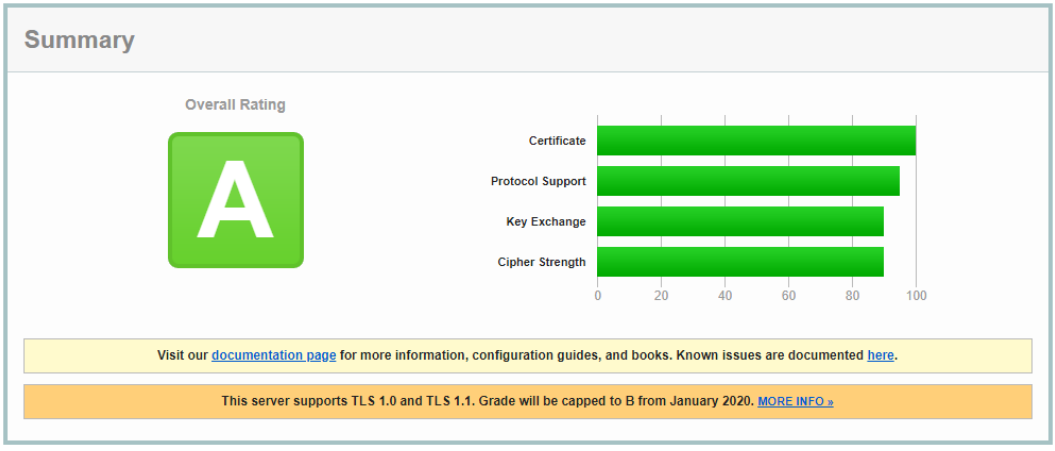


Figura 30 Qualys sobre lacompañia.academy.

Aunque su calificación es de "A", deja entrever que el server no soporta los protocolos TLS 1.2 y 1.3, lo que supone que se está sacrificando ya sea velocidad o seguridad. La implementación del protocolo HTTPS en una página web, hace que está se vuelva más lenta y perjudicaría a los usuarios.

Para ello, es necesaria la migración de SSL a TLS, con el fin de mejorar la seguridad de este protocolo, reduciendo el tiempo de espera en las negociaciones para reducir lo máximo posible los tiempos de espera o respuesta de la web.

13.3.1. Plataformas de desarrollo y operación.

Una vez ejecutada la aplicación Wappalyzer, las plataformas encontradas en https://lacompañía.academy fueron:

- Cloudflare (es un administrador de zonas DNS, que incorpora un proxy inverso para ofrecer sus servicios de CDN (Content Delivery Network) y seguridad para aplicaciones web.)
- Animate.css (permite animación de elementos de documentos HTML utilizando CSS)
- Select2 (un plugin jQuery)
- jQuery (es una librería de JavaScript de código abierto que permite agregar interactividad y efectos visuales en un sitio web.)

A continuación se muestran los resultados sin exponer información de la empresa:

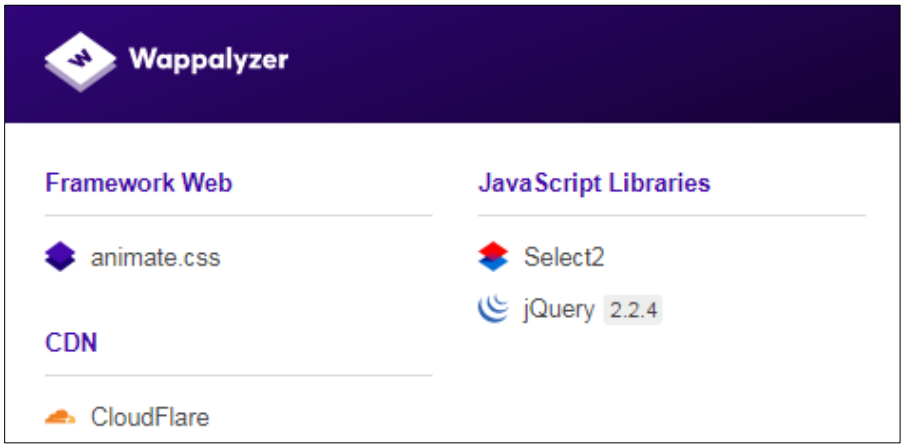


Figura 31 Resultados Wappalyzer lacompañia.academy.

Posteriormente al realizar las pruebas con SHODAN, en donde únicamente por medio de la búsqueda de la dirección IP publica del portal *"academy"*, fue que se obtuvieron resultados.

Una vez ejecutada la aplicación, las plataformas encontradas y diferenciadas en https://lacompañía.academy fueron:

- MySQL (Bases de Datos)
- PHP (lenguaje de código abierto adecuado para desarrollo web)
- Wordpress (gestor de contenidos web)
- Zepto.js (java script minimalista)

Adicionalmente, se pueden destacar los siguientes puertos abiertos:

- 80 http
- 443 https
- 2083 Secure Radius Service
- 2086 GNUnet
- 2087 ELI - Event Logging Integration
- 8080 http
- 8443 https
- 8880 CDDBP

A continuación se muestran los resultados sin exponer información de la empresa:

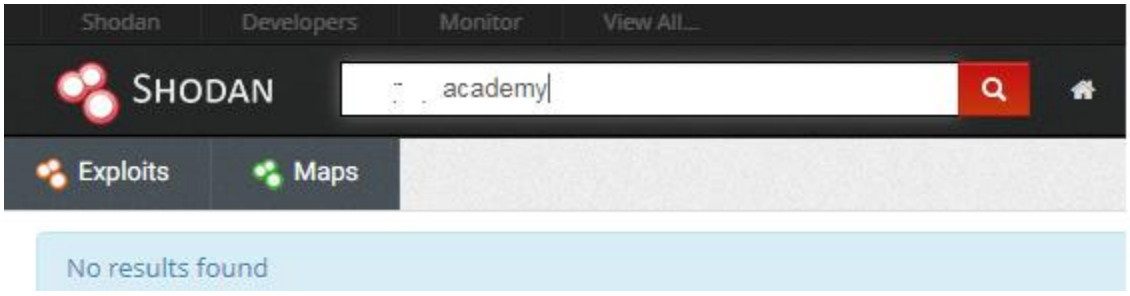


Figura 32 Resultados Shodan por URL.academy.

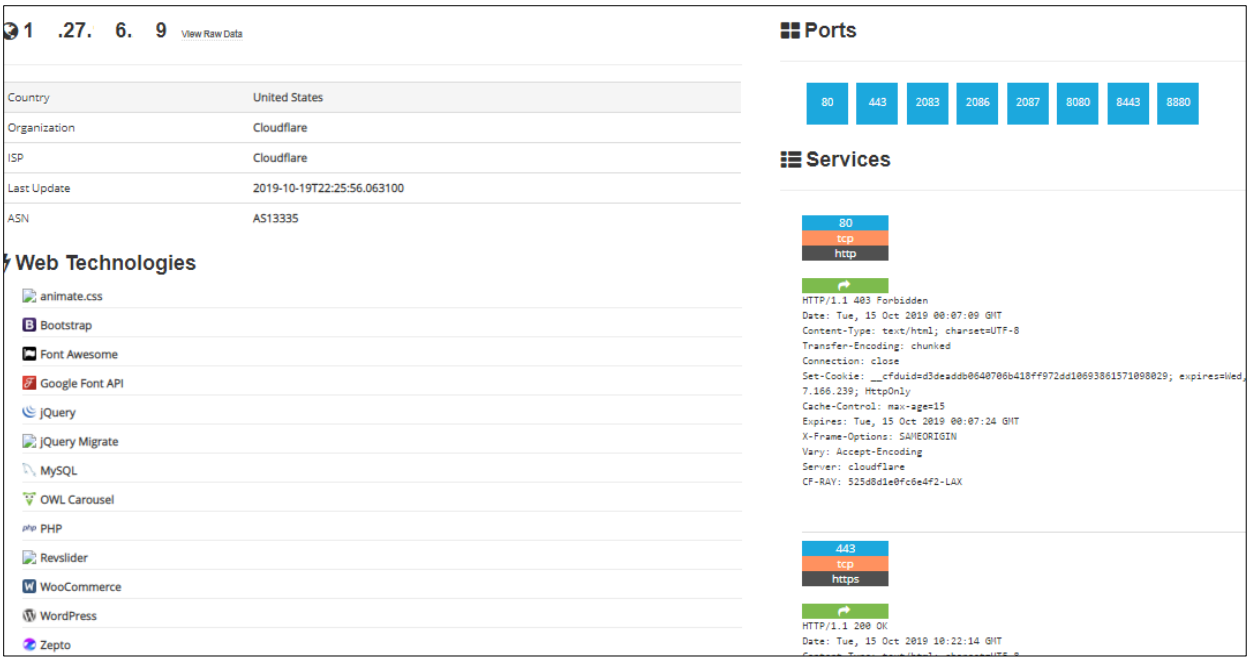


Figura 33 Resultados Shodan por IP.

Para finalizar, se utilizó un motor de localización de IP para determinar si los aplicativos se encuentran localizados de acuerdo con lo indicado y esperado por la compañía. Con esta información se verifica el dominio y la IP con la que se realizaron las pruebas con Shodan.

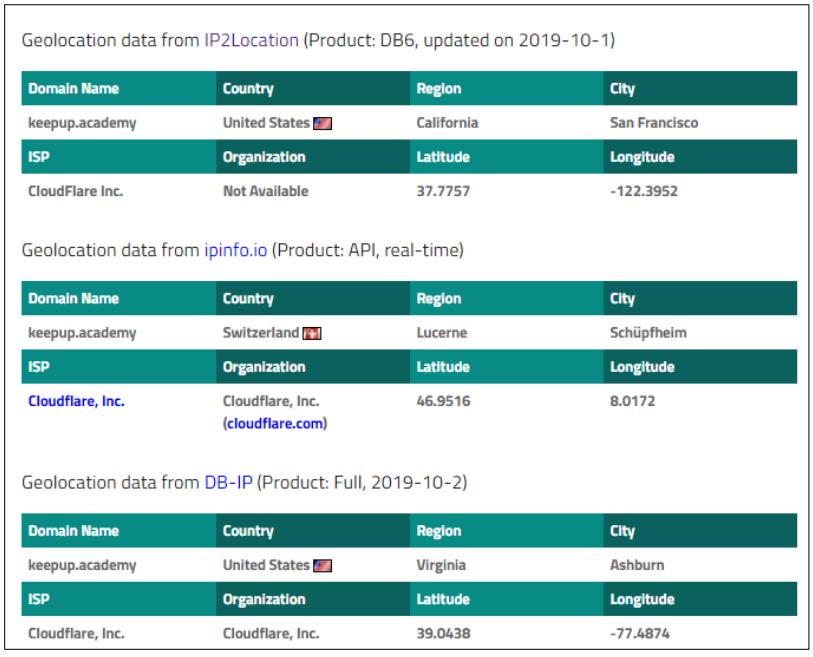
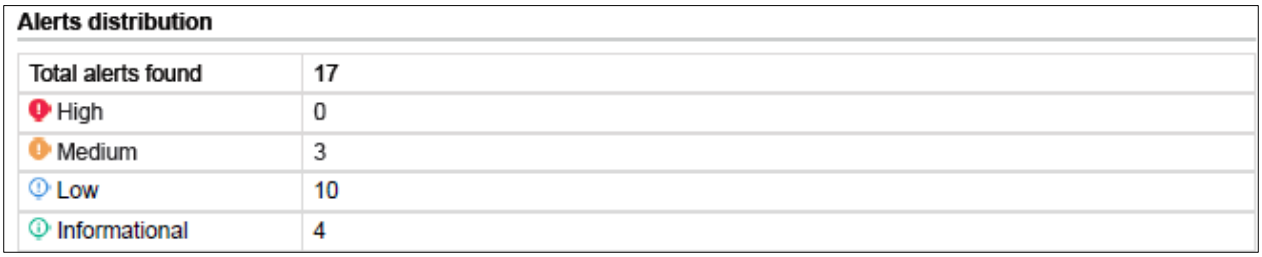


Figura 34 Localización portal URL.academy.

13.3.2. Vulnerabilidades Acunetix.

Por medio Acunetix se logró identificar que el portal Web presenta las siguientes vulnerabilidades:

- 03 Vulnerabilidades de Severidad Media
- 10 Vulnerabilidades de Severidad Baja
- 04 Vulnerabilidades de tipo Informativo



Alerts distribution	
Total alerts found	17
High	0
Medium	3
Low	10
Informational	4

Figura 35 Resultados Acunetix portal lacompañia.academy.

Por motivos de seguridad se omiten las pantallas en donde se puede visualizar la configuración y el objetivo del escaneo.

A continuación, se encuentra la descripción de las vulnerabilidades de severidad Media y algunas de las más relevantes de severidad baja:

1) **Se encontraron tres (03) vulnerabilidades medias relacionadas con el - Web Server - "HTML form without CSRF protection".** Acunetix encontró un formulario HTML sin aparente protección anti-CSRF implementada. Consultar la sección 'Detalles del ataque' para obtener más información sobre el formulario HTML afectado.

2) **Web Server - Apache mod_negotiation filename bruteforcing.** mod_negotiation Es un módulo de Apache responsable de seleccionar el documento que mejor se adapte a las capacidades de los clientes, de uno de varios documentos disponibles. Si el cliente proporciona un encabezado de aceptación no válido, el servidor responderá con un error 406 No aceptable que contiene una lista de pseudo directorio.

Este comportamiento puede ayudar a un atacante a aprender más sobre su objetivo, por ejemplo, generar una lista de nombres base, generar una lista de extensiones interesantes, buscar archivos de respaldo, etc.

3) **Web Server - Content Security Policy (CSP) not implemented.** Content Security Policy (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. La Política de seguridad de contenido (CSP) se puede implementar agregando un encabezado de Política de seguridad de contenido. El valor de este encabezado es una cadena que contiene las directivas de política que describen su Política de seguridad de contenido. Para implementar CSP, debe definir listas de orígenes permitidos para todos los tipos de recursos que utiliza su sitio. Por ejemplo, si tiene un sitio simple que necesita cargar scripts, hojas de estilo e imágenes alojadas localmente, así como desde jQuery biblioteca de su CDN, el encabezado CSP podría tener el siguiente aspecto:

```
Content-Security-Policy:
        default-src 'self';
        script-src 'self' https://code.jquery.com;
```

4) **Web Server - Cookie(s) without Secure flag set (verified).** Esta cookie no tiene establecido el indicador de seguridad. Cuando se configura una cookie con el indicador Seguro, le indica al navegador que solo se puede acceder a la cookie a través de canales SSL / TLS seguros. Esta es una protección de seguridad importante para las cookies de sesión.

5) **Web Server - Login page password-guessing attack.** Una amenaza común que enfrentan los desarrolladores web es un ataque de adivinación de contraseña conocido como ataque de fuerza bruta. Un ataque de fuerza bruta es un intento de descubrir una contraseña probando sistemáticamente todas las combinaciones posibles de letras, números y símbolos hasta que descubra la combinación correcta que funciona.

13.3.3. Vulnerabilidades OWASP ZAP.

Se realizó un escaneo con esta herramienta para verificar que vulnerabilidades se encuentran en el portal web de la compañía. Este nuevo análisis arrojó los siguientes resultados:

- 02 Vulnerabilidades de Severidad Media
- 15 Vulnerabilidades de Severidad Baja
- 00 Vulnerabilidades de tipo Informativa

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	15
Informational	0

Figura 36 Resultados exploración manual de ZAP.

Por motivos de seguridad se omiten las pantallas en donde se puede visualizar la configuración y el objetivo del escaneo.

A continuación, se encuentra la descripción de algunas de las vulnerabilidades encontradas:

1) **Encabezado X-Frame-Options no establecido.** El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.

2) **No se encuentra encabezado X-Content-Type-Options Header.** El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado. Estos (principios de 2014) y versiones antiguas de Firefox preferiblemente usarán el tipo de contenido declarado (si hay uno establecido), antes que ejecutar el MIME-Sniffing.

Este inconveniente aún aplica para páginas de error (401, 403, 500, etc.) ya que esas páginas a menudo todavía están afectadas por problemas de inyección, en cuyos casos aún hay preocupación de buscadores rastreando páginas fuera de su tipo de contenido verídico. En límite 'alto' este escáner no alertará sobre las respuestas de error al cliente o servidor.

3) **Incompleto o no Cache-control y sistema de encabezado HTTP Pragma.** El cache-control y encabezado HTTP Pragma no han sido establecidos apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.

4) **Absence of Anti-CSRF Tokens.** No Anti-CSRF tokens were found in a HTML submission form.

Los ataques de CSRG son muy efectivos en varias situaciones, que incluyen:

a. La victima tiene una sesión activa en el sitio de destino.
b. La víctima se autoriza por medio de la autenticación HTTP en el sitio de destino.
c. La víctima se encuentra en la misma red local que el sitio de destino.

5) **Cookie sin bandera asegurada.** Una cookie ha sido enviada sin la bandera asegurada, lo que significa que la cookie puede ser accedida mediante conexiones sin cifrar.

14. Discusión.

14.1. Discusión sobre redes internas.

A continuación se plantean una serie de soluciones sobre las diferentes vulnerabilidades encontradas, así:

RED	Equipo	Vulnerabilidad	Criticidad	Solución
2	1	50686 - IP Forwarding Enabled	Alta para computadores	N/A Este equipo es un router.

RED	Equipo	Vulnerabilidad	Criticidad	Solución
2	176	57608 - SMB Signing not required	Media	Aplicar la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva 'Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)'. En Samba, la configuración se llama 'firma del servidor'. Puede configurar esta característica de seguridad abriendo la política adecuada y expandiendo el árbol de la consola como tal: Configuración del equipo \ Configuración de Windows \ Configuración de seguridad \ Políticas locales \ Opciones de seguridad \. Para obtener instrucciones específicas sobre cómo configurar la configuración de la política de seguridad, consulte Editar la configuración de seguridad en un objeto de Política de grupo.
3	50	Operative System: TP-LINK TL-WA901ND 4.0 Dropbear SSH Server < 2016.72 Multiple Vulnerabilities.	Medio	Actualice a Dropbear SSH versión 2016.74 o posterior.
3	50	Puerto 80 abierto. |_ /jmx-console/: Authentication was not required.	Medio	Solución más aplicada: Los detalles para la solución están disponibles en PLE 19053890. El equipo es de telecomunicaciones, por cuanto debe actualizar su "firmware" y verificar si la vulnerabilidad desaparece. Equipo TP-LINK.
3	105	Puerto 80 abierto. |_ /jmx-console/: Authentication was not required.	Alto	Solución más aplicada: Los detalles para la solución están disponibles en PLE 19053890. El equipo es de telecomunicaciones, por cuanto debe actualizar su "firmware" y verificar si la vulnerabilidad desaparece. Equipo TP-LINK.
3	115/150/ 151/155/ 181	Vulnerables a CVE:CVE-2017-0143 - WannaCrypt attacks.	Alto	Aplicando el parche MS17-010 es posible eliminar el problema. El parche puede ser descargado de technet.microsoft.com. Una solución posible ha sido publicada inmediatamente después de la publicación de la vulnerabilidad. La vulnerabilidad también está documentada en las bases de datos SecurityFocus (BID 96703) y Tenable (97833).

RED	Equipo	Vulnerabilidad	Criticidad	Solución
3	188	Error en la gestión de recursos - cve2009-3103.	Alto	Una actualización elimina esta vulnerabilidad. Aplicando el parche MS09-050 es posible eliminar el problema. El parche puede ser descargado de microsoft.com. El mejor modo sugerido para mitigar el problema es actualizar a la última versión. Una solución posible ha sido publicada 2 meses después de la publicación de la vulnerabilidad. Si usted tiene habilitadas las actualizaciones automáticas solo debe asegurarse de contar con el parche requerido.
4	1	DNS Server Cache Snooping Remote Information Disclosure	Medio	El servidor DNS remoto responde a las consultas de dominios de terceros que no tienen establecido el bit de recursividad. Nota: Si este es un servidor DNS interno al que no pueden acceder redes externas, los ataques se limitarían a la red interna. Esto puede incluir empleados, consultores y potencialmente usuarios en una red de invitados o conexión WiFi si es compatible.
4	1	50686 - IP Forwarding Enabled	Alto para computadores	N/A Este equipo es un router.
4	9 y 10	Vulnerables a CVE:CVE-2017-0143 - WannaCrypt attacks.	Alto	Aplicando el parche MS17-010 es posible eliminar el problema. El parche puede ser descargado de technet.microsoft.com. Una solución posible ha sido publicada inmediatamente después de la publicación de la vulnerabilidad. La vulnerabilidad también está documentada en las bases de datos SecurityFocus (BID 96703) y Tenable (97833).
4	9 y 10	57608 - SMB Signing not required	Medio	Aplicar la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de directiva 'Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)'. En Samba, la configuración se llama 'firma del servidor'. Puede configurar esta característica de seguridad abriendo la política adecuada y expandiendo el árbol de la consola como tal: Configuración del equipo \ Configuración de Windows \ Configuración de seguridad \ Políticas locales \ Opciones de seguridad \. Para obtener instrucciones específicas sobre cómo configurar la configuración de la política de seguridad, consulte Editar la configuración de seguridad en un objeto de Política de grupo.

Tabla 5. Soluciones planteadas a las vulnerabilidades - Red LAN.

14.2. Discusión sobre los portales WEB.

A continuación se describen las soluciones planteadas a las vulnerabilidades encontradas en cada portal.

14.2.1. Discusión sobre el análisis de plataformas de desarrollo y operación https://lacompañia.com.co/.

Como primer acercamiento a las buenas prácticas de seguridad de la información, en donde mantener su confidencialidad, integridad y disponibilidad es la prioridad para cualquier organización. A continuación se describen las recomendaciones y controles a implementar por "La compañía" con el fin de mantener la actividad preventiva y predictiva sobre los activos informáticos analizados (aplicable a los dos portales web y academy):

A) Dentro del desarrollo de las actividades de análisis de vulnerabilidades los estudiantes que ejecutaron el presente trabajo entregarán plantillas de aseguramiento de las plataformas encontradas más relevantes (Apache 2.4.18, Ubuntu y Mysql). Sin embargo, para cada plataforma que almacene, gestione, tenga acceso o manipule información debe contar con una plantilla de aseguramiento (Plantilla de *"hardening"*). Estas plantillas deben gestionarse con cada tercero involucrado en el desarrollo, operación y mantenimiento de las plataformas (según aplique) con el fin de asegurar que la configuración es segura.

B) En lo posible, y si la información es crítica, implemente técnicas de autenticación que incluyan una segunda capa (dos factores).

C) Asegúrese que los usuarios cuenten con perfiles acordes con las tareas a realizar, no permita que se excedan los privilegios necesarios.

D) Es importante que cada servidor y sistema se encuentre debidamente parchado y actualizado de acuerdo con las recomendaciones del fabricante.

E) Establezca de manera clara los roles y responsabilidades sobre los sistemas así como sobre quien es el propietario de cada tipo de información.

F) Siempre que haya transferencia de datos relevantes entre los usuarios y las plataformas, implemente controles de cifrado y establezca canales de comunicación seguros por medio de https, tunneling, VPNs, entre otros. Mantenga al personal encargado en constante actualización de manera que se evite el uso de controles criptográficos obsoletos o inseguros. Recuerde que cada día se rompen algoritmos y metodologías, así como al mismo tiempo se crean técnicas nuevas y más seguras.

G) Controle sus sistemas con antivirus, antispyware, antimalware, antispam, etc.

H) Realice backups de su información.

I) Realice auditorias periódicamente.

J) Para la plataforma lacompañia.academy se recomienda verificar si el listado de puertos indicados a continuación deben estar abiertos, pues fueron encontrados durante el análisis:

a. 2083 Secure Radius Service
b. 2086 GNUnet
c. 2087 ELI - Event Logging Integration
d. 8080 http
e. 8443 https
f. 8880 CDDBP

14.2.2. Discusión sobre https://La Compañía.com.co.

Se notificará a la compañía el detalle de los hallazgos establecidos durante todo el proceso de análisis de las plataformas web, de manera que internamente se tomen los correctivos que consideren aplicables en cada uno de los sistemas y subsistemas.

A continuación se realiza una descripción con las posibles soluciones de las vulnerabilidades detectadas y descritas puntualmente en el capítulo de resultados.

TOOL	APP	Vulnerabilidad	Criticidad	Solución
ACUNETIX	https://LaCompañía.com.co	Web Server - HTML form without CSRF protection. Acunetix encontró un formulario HTML sin aparente protección anti-CSRF implementada. Consultar la sección 'Detalles del ataque' para obtener más información sobre el formulario HTML afectado.	MEDIA	La técnica recomendada y más utilizada para prevenir los ataques de CSRF es conocido como un token anti-CSRF, también conocido como token sincronizador.
ACUNETIX	https://LaCompañía.com.co	Web Server - Slow HTTP Denial of Service Attack. El servidor web es vulnerable a ataques HTTP **DoS (denegación de servicio) lentos**. Los ataques de Slowloris y Slow HTTP POST DoS se basan en el hecho de que el protocolo HTTP, por diseño, requiere que el servidor reciba completamente las solicitudes antes de que se procesen. Si una solicitud HTTP no está completa, o si la velocidad de transferencia es muy baja, el servidor mantiene sus recursos ocupados esperando el resto de los datos. Si el servidor mantiene demasiados recursos ocupados, esto crea una denegación de servicio.	MEDIA	Se recomienda consultar las referencias web para obtener información sobre cómo proteger su servidor web contra este tipo de ataque. Como las soluciones son de diversa índole y aplicabilidad, se recomienda consultar el enlace https://blog.qualys.com/securitylabs/2011/11/02/how-to-protect-against-slow-http-attacks
ACUNETIX	https://LaCompañía.com.co	Web Server - TLS 1.0 enabled. El servidor web admite el cifrado a través de TLS 1.0. TLS 1.0 no se considera una "criptografía sólida" según lo definido y requerido por el Estándar de seguridad de datos PCI 3.2 (.1) cuando se usa para proteger la información confidencial transferida hacia o desde sitios web.	MEDIA	Web Server - TLS 1.0 enabled. El servidor web admite el cifrado a través de TLS 1.0. Según PCI, "el 30 de junio de 2018 era la fecha límite para deshabilitar SSL / TLS temprano e implementar un protocolo de cifrado más seguro: TLS 1.1 o superior (se recomienda encarecidamente TLS v1.2) para cumplir con el Estándar de seguridad de datos PCI (PCI DSS) para salvaguardar los datos de pago en donde aplique.
ACUNETIX	https://LaCompañía.com.co	Web Server - Cookie(s) without HttpOnly flag set (verified). Esta cookie no tiene establecido el indicador HttpOnly. Cuando una cookie se configura con el indicador HttpOnly, le indica al navegador que solo el servidor puede acceder a la cookie y no los scripts del lado del cliente. Esta es una protección de seguridad importante para las cookies de sesión.	MEDIA	Si es posible, se debe establecer el indicador HttpOnly para esta cookie.

TOOL	APP	Vulnerabilidad	Criticidad	Solución
ZAP	https://La Compañía .com.co	Encabezado X-Frame-Options no establecido. El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.	MEDIA	Los navegadores de web más modernos apoyan la cabecera HTTP X-Frame-Options, que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).
ZAP	https://La Compañía .com.co	Incompleto o no Cache-control y sistema de encabezado HTTP Pragma. El cache-control y encabezado HTTP Pragma no ha sido establecido apropiadamente o faltan, permitiendo al navegador y servidores proxy almacenar contenido.	MEDIA	Siempre que sea posible asegurarse que el encabezado HTTP cache-control está establecido con no-cache, no-store, must-revalidate, y que el encabezado HTTP pragma esté establecido con no-cache.
ZAP	https://La Compañía .com.co	Absence of Anti-CSRF Tokens. No Anti-CSRF tokens were found in a HTML submission form. Los ataques de CSRG son muy efectivos en varias situaciones, que incluyen: a. La victima tiene una sesión activa en el sitio de destino. b. La víctima se autoriza por medio de la autenticación HTTP en el sitio de destino. c. La víctima se encuentra en la misma red local que el sitio de destino.	MEDIA	La solución es compleja y requiere ejecutarse en fases; arquitectura y diseño e implementación con un par diferenciado de instancias. Esta información estará consignada en el informe para la compañía.
ZAP	https://La Compañía .com.co	Protección de buscador de web XSS no disponible. La protección del buscador de web XSS no está disponible, o está deshabilitada por la configuración de la cabecera de respuesta de HTTP 'X-XSS-Protection' en el servidor de web.	MEDIA	Asegúrese que el filtro XSS del navegador web está habilitado, estableciendo el encabezado de respuesta HTTP X-XSS-Protection en '1'.

Tabla 6. Soluciones planteadas a las vulnerabilidades – WEB 1.

14.2.3. Discusión sobre https://LaCompañía.academy.

De manera similar que en los numerales previos, se notificará a la compañía el detalle de los hallazgos establecidos durante todo el proceso de análisis de las plataformas web, de manera que internamente tomen los correctivos que se consideren aplicables en cada una de los sistemas y subsistemas.

A continuación se realiza una descripción con las posibles soluciones de las vulnerabilidades detectadas y descritas puntualmente en el capítulo de resultados.

TOOL	APP	Vulnerabilidad	Criticidad	Solución
ACUNETIX	https://LaCompañía.academy	Web Server - "HTML form without CSRF protection". Acunetix encontró un formulario HTML sin aparente protección anti-CSRF implementada. Consultar la sección 'Detalles del ataque' para obtener más información sobre el formulario HTML afectado.	MEDIA	Verifique si este formulario requiere protección anti-CSRF e implemente contramedidas CSRF si es necesario. La técnica recomendada y más utilizada para prevenir ataques de CSRF se conoce como un token anti-CSRF, también conocido como token de sincronizador.
ACUNETIX	https://LaCompañía.academy	Web Server - Apache mod_negotiation filename bruteforcing. mod_negotiation es un módulo de Apache responsable de seleccionar el documento que mejor se adapte a las capacidades de los clientes, de uno de varios documentos disponibles. Si el cliente proporciona un encabezado de aceptación no válido, el servidor responderá con un error 406 No aceptable que contiene una lista de pseudo directorio. Este comportamiento puede ayudar a un atacante a aprender más sobre su objetivo, por ejemplo, generar una lista de nombres base, generar una lista de extensiones interesantes, buscar archivos de respaldo, etc.	MEDIA	Deshabilite la directiva MultiViews del archivo de configuración de Apache y reinicie Apache. Puede deshabilitar MultiViews creando un archivo .htaccess que contenga la siguiente línea: Opciones – Multiviews.

TOOL	APP	Vulnerabilidad	Criticidad	Solución
ACUNETIX	https://La Compañía .academy	Web Server - Content Security Policy (CSP) not implemented. Content Security Policy (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. La Política de seguridad de contenido (CSP) se puede implementar agregando un encabezado de Política de seguridad de contenido. El valor de este encabezado es una cadena que contiene las directivas de política que describen su Política de seguridad de contenido. Para implementar CSP, debe definir listas de orígenes permitidos para todos los tipos de recursos que utiliza su sitio. Por ejemplo, si tiene un sitio simple que necesita cargar scripts, hojas de estilo e imágenes alojadas localmente, así como desde jQuery biblioteca de su CDN, el encabezado CSP podría tener el siguiente aspecto: Content-Security-Policy: default-src 'self'; script-src 'self' https://code.jquery.com;	MEDIA	Se recomienda implementar la Política de seguridad de contenido (CSP) en su aplicación web. La configuración de la Política de seguridad de contenido implica agregar el encabezado HTTP de política de seguridad de contenido a una página web y asignarle valores para controlar los recursos que el agente de usuario puede cargar para esa página.
ZAP	https://La Compañía .academy	Encabezado X-Frame-Options no establecido. El encabezado X-Frame_options no está incluido en la respuesta HTTP para proteger ante ataques 'ClickJacking'.	MEDIA	Los navegadores de web más modernos apoyan la cabecera HTTP X-Frame-Options. Asegúrese que está establecido en todas las páginas web devuelta por su sitio (si usted espera que la página este enmarcada solo por páginas en su servidor (por ejemplo, es parte de un FRAMESET) entonces usted querrá usar SAMEORIGIN, de otras forma si usted nunca espera que la página esté enmarcada, debería usar DENY. ALLOW-FROM permite a sitios web específicos enmarcar la página web en navegadores web compatibles).

TOOL	APP	Vulnerabilidad	Criticidad	Solución
ZAP	https://La Compañía .academy	No se encuentra encabezado X-Content-Type-Options Header. El encabezado Anti-MIME-Sniffing X-Content-Type-Options no estaba configurado para 'nosniff'. Esto permite versiones antiguas de Internet Explores y Chrome ejecutar MIME-sniffing en el cuerpo de la respuesta, causando potencialmente que el cuerpo de respuesta sea interpretado y desarrollado como un tipo de contenido diferente que el tipo de contenido declarado.	MEDIA	Asegúrese que el servidor de la aplicación/web establezca el encabezado Content-Type apropiadamente, y que esté establecido el encabezado X-Content-Type-Options en 'nosniff' para todas las páginas web. Si es posible, asegúrese que el último usuario usa un navegador web compatible con los estándares y moderno que no ejecute MIME-sniffing en absoluto, o que pueda ser dirigida por el servidor de la aplicación/web para no ejecutar MIME-sniffing.

Tabla 7. Soluciones planteadas a las vulnerabilidades – WEB 2 ACADEMY.

15. Conclusiones.

Generales

Con este proyecto se pudo establecer el impacto de no realizar una gestión adecuada de vulnerabilidades, en caso de materializar estas amenazas altas y criticas pueden llevar a la pérdida de confidencialidad, integridad o disponibilidad de información de la organización, afiliados y clientes.

En general, se concluye que la organización está protegida frente a ataque básicos externos con acceso solamente a través de internet; sin embargo, un atacante con el tiempo suficiente para realizar la exploración y explotación de vulnerabilidades medias y avanzadas le permitirían comprometer la seguridad de la organización.

Un atacante interno puede llegar a generar una afectación grave para la organización, sin embargo, algunas de las vulnerabilidades identificadas como críticas fueron mitigadas en gran medida implementando herramientas de actualización y aseguramiento de sistemas operativos.

Durante el planteamiento, planeación y ejecución del presente trabajo de grado para la especialización en Seguridad de Redes Telemáticas de la Universidad del Bosque sede Bogotá año 2019, se tuvo la posibilidad de valorar los criterios y especificaciones sobre los conceptos que rigen la seguridad informática en servicios tecnológicos publicados en internet (externo) como de forma local (interno) con el fin de mantener y "garantizar" su disponibilidad, integridad y confidencialidad.

Para La Compañía de Educación Virtual a la cual se realizó este análisis de vulnerabilidades, es de vital importancia asegurar sus activos informáticos de manera estricta y bajo parámetros periódicos que les evite bajar la guardia con el tiempo.

Si bien, dentro de La compañía la mayoría de los sistemas informáticos, de información, aplicaciones y redes implementadas cuentan con controles básicos que permiten mantener la seguridad de la información dentro de niveles de riesgo bajo, para La compañía será necesario implementar algunas modificaciones o inclusiones operativas, administrativas y de mantenimiento que permitan llevar los riesgos a niveles (muy bajos) aceptables y así seguir aumentando sus niveles de desempeño y calidad que le permitan aumentar su competitividad dentro de su gremio.

Específicas

- La gran mayoría de vulnerabilidades internas, se encuentran asociadas a la actualización de aplicaciones, sistemas operativos y parches de seguridad que no han sido aplicados; también se encuentran aplicaciones y sistemas operativos sin soporte que representan un riesgo importante para la infraestructura de la organización. Las máquinas de la red LAN requieren aplicar parches de manera urgente.

- Las acciones de hardening recomendadas para fortalecer la seguridad de los servicios han sido redactadas de forma general sin hacer referencia a ambientes organizacionales específicos, debido a esto su implementación puede variar según el contexto y red que se disponga. A su vez, es posible que en algunos casos estas acciones no puedan implementarse en su totalidad.

- Implementar un dominio (Active Directory o similar). Ayuda a centralizar la administración haciendo más seguro el entorno de la red.

- Mejorar la seguridad y control de acceso a los equipos de red.

- Se entregan formatos de hoja de vida e inventario con algunos aportes a los existentes que pueden ayudar en la mejora continua del proceso operativo informático.

- Implementar el uso de UPS que soporte todos los equipos, al menos para confiabilidad de entrega de energía eléctrica.

- Controlar la seguridad de contraseñas de acceso administrativo a los equipos de la red inalámbrica.

- Implementar las nuevas políticas entregadas en este estudio.

- Aplicar las plantillas de hardening de los sistemas operativos y plataformas de desarrollo, aun cuando los servicios se encuentren tercerizados (revisar plantillas de estos terceros si aplica).

- Parchar de manera frecuente los equipos de cómputo, aunque no cuentan con información de manera local, si se usan para acceder a plataformas web y a plataformas de usuario final que pueden ser de información de los usuarios.

- Atender y mitigar las vulnerabilidades, como mínimo aquellas con factor de riesgo alto y medio, las cuales son entregadas en el informe y los informes como anexos.

- Establecer un registro de logs en el que se almacenaran las IP, hora y fecha en la que un usuario no autorizado ha intentado acceder a la plataforma web.

- Establecer los protocolos o procedimientos de entrega y eliminación de los usuarios de passwords a nuevos empleados y empleados de baja (portales, drives, etc).

- Añadir múltiples herramientas orientadas a distintos tipos de servicio (VoIP, servidores, switches/routers) de cara a seguir descubriendo vulnerabilidades en la red, de forma más específica.

15.1. Recomendaciones adicionales.

Una vez terminado el análisis de vulnerabilidades de la empresa, cabe destacar que de cara al futuro se proponen múltiples mejoras, tal y como podrían ser las siguientes:

- Diseñar unas métricas para optimizar la información útil que aporta cada herramienta, es decir, realizar en primer lugar un escaneo de equipos y determinar su funcionalidad, y a partir de ella, establecer unos riesgos y prioridades de análisis, ya que, en este trabajo, se han realizado análisis a todos los equipos activos, y esto ha supuesto en algunos casos una pérdida de tiempo, debido a que había información que no era relevante.

- Implementar estas herramientas junto con herramientas pasivas encargadas de detectar el tráfico que circula por la red, y así establecer un mapa de red más completo, ya que existen casos en los que las herramientas activas, no analizan todo el espectro posible, y existe información, que solo se puede detectar analizando de forma pasiva la red.

- Existen otro tipo de amenazas como Cross-Side Request Forgery CSRF el cual no se profundizó durante el desarrollo del proyecto. Este ataque consiste en lanzar una petición desde una máquina donde exista una sesión autorizada, la petición puede ser lanzada desde contenido oculto de una URL u otro recurso como Correos Electrónicos. Por medio de esta amenaza se puede desarrollar acciones maliciosas como corrupción de datos o apertura de puertas traseras. Para prevenir este tipo de amenazas se puede inducir un dato aleatorio en todas las respuestas que otorga la Aplicación Web, luego cuando se realice la petición hacia la aplicación, se verificara este valor aleatorio y si es válido, la petición puede ser atendida. Otro tipo de mecanismos de defensa se especifican en la página oficial de OWASP (OWASP OPEN WEB APPLICATION SECURITY PROYECT).

- Cifrar los Correos Electrónicos por medio de Criptografía Asimétrica: Cifrar la comunicación a nivel de red por medio de TLS puede ser importante, sin embargo, es posible aún descifrar la capa de transporte aprovechándose de algunas debilidades del cifrado asimétrico. Para asegurar completamente que los correos se envían sobre un canal confidencial, se puede encapsular el propio correo electrónico haciendo uso de la criptografía de llave pública. Muchos de los proveedores de SMTP soportan estas capacidades, de hecho, es algo transparente para muchos de ellos y simplemente se puede lograr con la implementación de algunos plugins. Incluso existen proveedores como ProtonMail, que ofrecen estas capacidades por defecto. El cifrado del correo electrónico podría no incluir las cabeceras del protocolo de SMTP, ya que son necesarias para encontrar el destinatario del correo electrónico.

  Si no se cuenta con mucha experiencia sobre la Administración de Correos Electrónicos y configuración de Servidores SMTP, es preferible contratar un servicio externo. Muchos proveedores como Gmail, Outlook, ProtonMail; entre otros, ya cuentan con mecanismos de seguridad que ayudan a proteger la información de sus usuarios. Además de esto, ofrecen el servicio de correo a las diferentes empresas, lo cual es bastante conveniente para aquellas que no cuentan con el personal y recursos suficientes para configurar sus propios servicios de SMTP.

- Muchas de las acciones de hardening fueron extraídas de fuentes especializadas en el tema. Se recomienda que siempre que se deseen aplicar políticas de seguridad nuevas, se consulte a nivel organizacional sobre el posible impacto que puede generar esta nueva política, así mismo, asesorarse sobre fuentes oficiales para no incurrir en la apertura de una brecha de seguridad.

15.2. Herramientas.

Se dará una visión de lo que aportan estas herramientas, posteriormente, se enumeraran una serie de ideas y mejoras que se podrían realizar en torno a la seguridad de la entidad en un futuro.

Estas herramientas, aportan diferentes funcionalidades, entre ellas:

- Interfaz sencilla, escalable y transparente. La herramienta utilizada en este proyecto realiza los análisis en segundo plano, despreocupando al usuario final del conocimiento de las herramientas que se utilizan, así como de su funcionamiento, etcétera, proporcionando una interfaz sencilla, fácil de utilizar, en la que cualquier usuario, puede realizar un análisis sin disponer de conocimientos en ese campo y visualizar la información de estos.

- Utilización de herramientas OpenSource en su última versión. Si bien, existen otras herramientas, estás se encuentran en desuso o son instrumentales de pago, por lo que algunas podrían estar ya obsoletas e incluso no ser compatibles, en este aspecto, este trabajo, a día de la realización, aporta la última versión estable y actualizada de todas las herramientas utilizadas.

- Visualización dinámica de los resultados. Aunque existen otras herramientas que generan reportes en formato HTML o PDF bastante gráficos, estas herramientas proporcionan un tipo de reporte dinámico, en el cual se pueden realizar consultas de información en cualquier momento. De esta manera, la información, no queda acotada a un patrón específico, si no que el propio usuario, puede elegir qué información desea visualizar, así como establecer diversas relaciones entre los distintos campos de cada herramienta.

16. Documentación de Referencia.

- The Penetration Testing Execution Standard. [En línea]. Disponible en: http:// www.pentest-standard.org.
- González, Pablo. [En línea]. «Ethical Hacking: Teoría y práctica para la realización de un pentesting», 2014. [ISBN: 978-84-617-0576-4].
- Harris, Shon; Eagle, Chris, & Allen, Harper. [En línea]. «Hacking ético», 2005. [ISBN: 84-415-1874-2].

- Borja, Febrero & Holguín, José. [En línea]. «Pentest: Recolección de Información (Information Gathering)». Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_information_gathering.pdf
- González, Pablo; Sánchez, Germán & Soriano, José. [En línea]. «Pentesting con Kali», 2014. [ISBN: 978-84- 616-7738-2].
- Guía de referencia de Nmap (Página de manual). [En línea]. Disponible en: https://nmap.org/man/es/.
- OMP: OpenVAS Management Protocol. [En línea]. Disponible en: http://www.openvas.org/omp-6-0.html.
- Palacios, Jairo. [En línea]. Análisis de Vulnerabilidades de una red corporativa mediante herramientas de descubrimiento activas. Trabajo Fin de Grado. Universidad de Sevilla. 2015. Sevilla, España. Disponible en: http://bibing.us.es/proyectos/abreproy/90522/fichero/Memoria+del+Trabajo+Fin+de+Grado.pdf
- NMAP: https://www.stationx.net/nmap-cheat-heet/) (https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/)
- https://vuldb.com/

17. Anexos.

17.1. Anexo 1 Cronograma (Diagrama de Gantt) – PDT.

17.2. Anexo 2 Controles A11 ISO 270001 Seguridad Física.

17.3. Anexo 3 Políticas Nuevas.

17.4. Anexo 4 Formato Inventario de Activos informáticos.

17.5. Anexo 5 Formato Hoja de Vida PCs.

17.6. Anexo 6 Plantillas de aseguramiento.