APLICACIÓN DE LA METODOLOGÍA PTES EN LA PYME COLOMBIA LEDS SAS PARA LA IDENTIFICACIÓN DE VULNERABILIDADES DE CIBERSEGURIDAD.

EDUARD ANDRÉS FERNÁNDEZ PERALTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2023

APLICACIÓN DE LA METODOLOGÍA PTES EN LA PYME COLOMBIA LEDS SAS PARA LA IDENTIFICACIÓN DE VULNERABILIDADES DE CIBERSEGURIDAD.

EDUARD ANDRÉS FERNÁNDEZ PERALTA

Proyecto de Grado – Proyecto aplicado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Christian Reynaldo Angulo Rivera
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2023

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá D.C., 2023

DEDICATORIA

Este trabajo está dedicado a mi familia que con su apoyo incondicional han hecho posible la realización de esta especialización.

A la empresa Colombia Leds SAS por permitirme ese voto de confianza que permitió el desarrollo de este proyecto, fortaleciendo de esta manera los conocimientos adquiridos durante el transcurso de mis estudios.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACTIVO INFORMÁTICO: Recurso tecnológico

AMENAZA: es la acción para aprovechas una vulnerabilidad en un sistema informático.

BOTNET: red de computadores infectados con malware que son controlados por un atacante para conseguir un propósito.

CIBERDELINCUENTE: Persona que realiza actos delictivos haciendo uso de las tecnologías de la información.

CIBERSEGURIDAD: Conocida también como seguridad informática o seguridad digital, es la práctica de proteger la información contenida en los sistemas informáticos, las redes de comunicaciones y los dispositivos electrónicos.

DMZ: Zona desmilitarizada por sus siglas en inglés. Hace referencia al área de la red que está en contacto con redes no confiables como internet y que se aísla de la red interna.

EXPLOIT: Programa que explota una vulnerabilidad informática.

HACKER: Persona con avanzados conocimientos en computadores y redes informáticas que se dedica a programar y a buscar vulneraciones en los sistemas.

HACKING: Es un conjunto de técnicas utilizadas para vulnerar los sistemas saltándose la seguridad establecida.

HOST: Son los dispositivos conectados a una red y que actúan como punto inicial o final en la transferencia de datos. Estos pueden ser computadores, dispositivos móviles, entre otros.

INTRUSIÓN: intento no autorizado de ingresar a un sistema para obtener algún tipo de información o para provocar un daño en el mismo.

MALWARE: software malicioso. Es un programa o parte de este que está diseñado para alterar el normal funcionamiento de los dispositivos electrónicos, redes de comunicación o sistemas informáticos.

METERPRETER: Es un payload que proporciona al atacante una consola interactiva a la máquina objetivo para ejecutar código. Este está presente en el framework de Metasploit.

PAYLOAD: Denominado también carga útil es la que se ejecuta en una vulnerabilidad. Puede ejecutarse en varios exploits.

RAMSOMWARE: Es un software malicioso que secuestra la información de las víctimas para que no puedan acceder a su información y que solicitan una recompensa económica por la recuperación del sistema o los datos.

SERVIDOR: Equipo de cómputo conectado a una red y que provee servicios.

VECTOR DE ATAQUE: Ruta que se elige para aprovechar una vulnerabilidad en un sistema para realizar un ataque informático que permita ingreso al sistema para ejecutar algún tipo de malware para conseguir el objetivo propuesto.

VULNERABILIDAD INFORMÁTICA: Es una debilidad que existe en un sistema informático que puede ser usado por un intruso para comprometer la seguridad del sistema.

RESUMEN

Palabras clave: Ciberseguridad, pyme, PTES, vulnerabilidades, hacking.

El creciente porcentaje de ataques cibernéticos a las pymes y teniendo en cuenta que Colombia se ubicó en el sexto puesto de los países latinoamericanos con más ataques de ciberdelincuentes, se hace necesario fomentar la cultura de la ciberseguridad en esta clase de empresas. Como primer paso, un análisis de vulnerabilidades abre el espacio para la implementación de buenas prácticas de ciberseguridad que permita a las empresas cuidar su mayor activo, la información.

Dentro de las metodologías que mejor se adaptan a las diferentes empresas es la PTES con lo cual su implementación podrá aplicarse a cualquier empresa y razón social. Por eso, como objetivo principal de este trabajo es establecer las condiciones de ciberseguridad en la pyme de aplicación del proyecto basados en esta metodología con el fin de encontrar las vulnerabilidades a las que está expuesta la empresa y dar las recomendaciones con las líneas de acción que podrá tomar para aumentar sus niveles de ciberseguridad.

Generando de esta manera una mayor confianza de sus clientes y proveedores en la protección de sus datos personales, cumpliendo así la normatividad vigente en este aspecto y generando un valor agregado a su negocio como también aumentado el grado de concientización en temas de ciberseguridad en el sector de las pymes en Colombia.

ABSTRACT

Keywords: Cybersecurity, SME, PTES, vulnerabilities, hacking.

Due to the growing percentage of cyber-attacks on SMEs and considering that Colombia ranked sixth among Latin American countries with most attacks by cybercriminals, it is necessary to promote a culture of cybersecurity for this type of companies. The first step, a vulnerability analysis that opens a space for the implementation of good cybersecurity practices and allows companies to take care of their greatest asset, information.

One of the methodologies that best adapts to different companies is the PTES, whose implementation can be applied to any company and business name. Considering the previous scenario, the main objective of this paper is to establish the cybersecurity conditions in the project application for SMEs based on the PTES methodology in order to find vulnerabilities to which the company is exposed and provide recommendations and action plans that may apply in order to increase the levels of cybersecurity.

This way, creating greater confidence from customers and suppliers regarding the protection of their personal data by complying with current regulations for this matter and generating added value to the business as well as increasing the level of awareness on cybersecurity issues for the SMEs sector in Colombia.

INTRODUCCIÓN

En la actualizad el tema de ciberseguridad ha cobrado una gran importancia y eso se ve reflejado en el creciente número de ataques cibernéticos que se están presentando donde las empresas más pequeñas con las más vulnerables debido entre otros muchos factores, la concienciación de la importancia de la seguridad informática en su empresa con miras de proteger su mayor activo, la información.

Actualmente, la pyme Colombia Leds SAS desconoce cuáles son las vulnerabilidades en sus sistemas informáticos que la expongan a ataques cibernéticos donde se puedan comprometan sus sistemas y la información de sus clientes y proveedores, por tanto, peligrando la continuidad del negocio.

Con la propagación de los programas maliciosos como los ransomware, la empresa Colombia Leds SAS fue afectada por este tipo de ataque donde tuvieron pérdidas de información crítica para el negocio, afectación en su infraestructura tecnológica, y daños reputacionales, así como pérdidas económicas. Por ello, se ha tenido la necesidad de aplicar la metodología PTES que le permita detectar las brechas de seguridad en sus sistemas informáticos y evaluar las posibilidades para mitigar los riesgos de las vulnerabilidades encontradas.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

De acuerdo con el informe “Tendencias del cibercrimen en Colombia (2019-2020) [1] de la Cámara Colombiana de Informática y Telecomunicaciones CCIT el 60% de las pymes en Colombia no pudieron continuar con sus negocios después de ser víctimas de un ciberataque. Durante el periodo enero a octubre cuando se realizó la publicación de este informe, el ataque por malware (software malicioso) tuvo un crecimiento del 612% donde las empresas pagaron entre 32 y 160 millones por rescate de información.

De acuerdo con proyecciones del consultor internacional de ciberseguridad, coronel (RA) Fredy Bautista, las tendencias del cibercrimen se centrarán en la Inteligencia Artificial IA donde se ejecutan ataques suplantando altos directivos de las empresas, clientes y proveedores con el fin de solicitar transferencias de dinero.

La utilización de perfiles en redes sociales para la difusión de malware, uso de Botnet para ataques dirigidos, DDOS, ventas de datos financieros en la internet profunda. Cifras del DANE en el 2019 las pymes representan más del 90% del sector productivo de Colombia, generando de esta manera el 80% del empleo y aportando a la nación el 35% del PIB [2]. Lo que nos da a entender la gran importancia que tiene este sector en la sociedad colombiana.

Teniendo en cuenta que la ciberseguridad es de vital importancia para la continuidad del negocio donde las mipymes (micro, pequeñas y medias empresas) son las más vulnerables, se hace indispensable que este sector cuente con estrategias de ciberseguridad que les permitan evaluar y mitigar los riesgos.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo elaborar la implementación de la metodología de hacking ético PTES para identificar las vulnerabilidades de ciberseguridad en la pyme Colombia Leds SAS?

---

[1] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias del cibercrimen en Colombia 2019-2020.

[2] MINTRABAJO. [Sitio web]. Bogotá D.C.: MINISTERIO DE TRABAJO, “MiPymes representan más de 90% del sector productivo nacional y generan el 80% del empleo en Colombia”: ministra Alicia Arango. Disponible en: https://www.mintrabajo.gov.co/prensa/comunicados/2019/septiembre/mipymes-representan-mas-de-90-del-sector-productivo-nacional-y-generan-el-80-del-empleo-en-colombia-ministra-alicia-arango

2 JUSTIFICACIÓN

Debido a los antecedentes de ataques cibernéticos que ha sufrido la pyme Colombia Leds SAS en la cual se ha visto perjudicada en la pérdida irrecuperable de información vital para su negocio e información sensible de sus clientes y proveedores, se hace pertinente la aplicación de una metodología de hacking ético para realizar un estudio que nos permita la detección de vulnerabilidades de ciberseguridad en la empresa y de esta manera se puedan identificar las vulnerabilidades en los sistemas de tal forma que esto pueda ayudar a mitigar los crecientes ataques que están siendo objeto las pymes, realizando ajuste que nos permitan cerrar las brechas de seguridad en las vulnerabilidades encontradas.

Actualmente, la empresa no cuenta con algún tipo de metodología que le permita identificar las vulnerabilidades en sus sistemas informáticos, por tanto, se sugiere la aplicación de la metodología PTES con el fin de asegurar su información y aumentar los niveles de ciberseguridad.

Con la ejecución de este proyecto se ayudaría a fomentar la cultura de la ciberseguridad en las pymes en estudio interrelacionándolo con las actividades cotidianas en el aspecto personal de sus empleados aportando también de esta manera tener una mejor ciberseguridad en nuestra sociedad.

Por otro lado, con la ejecución de este proyecto se obtendrán valiosos conocimientos en la aplicación de la formación académica sé que se está realizando en la universidad y que es de gran aporte al perfil que como futuros especialistas en seguridad informática generando nuevos conocimientos en el área de ciberseguridad.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Evaluar las condiciones de ciberseguridad en la pyme Colombia LEDS SAS aplicando la metodología PTES con el fin identificar las vulnerabilidades y establecer estrategias de control que salvaguarden la información.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar la información más relevante referente a la estructura organizacional e infraestructura tecnológica de la pyme Colombia LEDS SAS para lograr aplicar adecuadamente la metodología PTES.
- Estructurar el ataque sobre la infraestructura tecnológica de la pyme Colombia LEDS SAS que permita hallar los puntos más vulnerables para su posterior explotación.
- Demostrar las vulnerabilidades asociadas a la infraestructura tecnológicas de la pyme Colombia LEDS SAS, mediante la aplicación de la metodología PTES con el fin conocer las condiciones de ciberseguridad.
- Proponer recomendaciones a partir de las vulnerabilidades encontradas mediante el uso de lineamientos de buenas prácticas de seguridad con el fin de salvaguardar la información.

4 MARCO REFERNCIAL

4.1 MARCO TEÓRICO

Desde la aparición de los sistemas informáticos y por la misma naturaleza del ser humano de ser curioso, de querer saber cómo funcionan las cosas y mejorarlas, surgieron las personas que a través de su ingeniero lograron adquirir habilidades para poder ingresar a los sistemas sin ser detectados, muchas veces solo por la satisfacción de lograrlo, sin embargo, muchos aprovecharon estas destrezas para conseguir algún beneficio. A estos se les denominó hacker y a sus actividades hacking, aunque este término está siendo mal utilizado, se prefiere llamar ciberdelincuente a aquellos que usando técnicas de hacking vulneran los sistemas sin autorización del dueño o administrador del sistema para algún fin.

La práctica del hacking es condenada a nivel mundial y Colombia no es la excepción con la ley 1273 de 2009 que penaliza los delitos informáticos donde se destaca el acceso no autorizado de los sistemas, la suplantación y el robo de información como elementos más sobresalientes de esta norma.

Por esto, los especialistas en seguridad informática han definido metodologías que permiten el análisis de ciberseguridad de forma sistemática permiten identificar las vulnerabilidades en los sistemas informáticos y de esta manera poderlas eliminar o mitigar. Dentro de las metodologías de análisis de vulnerabilidades se encuentra las siguientes:

Open Web Application Security Proyect Testing Guide OWASP [3]: Proyecto creado en 2001 apoyado por la Open Web Application Security Proyect Testing Guide OWASP [4]: Proyecto creado en 2001 apoyado por la fundación sin ánimo de lucro OWASP con el propósito de hacer software más seguro en especial en la construcción de aplicaciones y servicios web.
Actualmente existen dos modalidades principales basadas en OWASP 2017:

Auditoría OWASP TOP 10: Se enfoca en buscar las debilidades más habituales y que tienen un mayor impacto en la seguridad de un sistema.

Auditoría OWASP Completa: se valida 90 controles definidos por la metodología haciendo especial enfoque en los errores relacionados con lógica de negocio. Es ideal para plataformas críticas para blindar el sistema frente ataques informáticos.

[3] FUENTE MAESTRO, Antonio. Elaboración de una metodología de test de intrusión dentro de la auditoria de seguridad. p. 24.

Open Source Security Testing Methodology Manual [5]: Es una metodología de evaluación y de métrica, la cual es definida por la asociación ISECOM (Institute for Security and Open Methodology) igualmente sin ánimo de lucro creada en 2000. Está orientada a cualquier tipo de organización y aplicada a cualquier entorno donde se requieran aspectos de seguridad ya sea física, de procesos, de las telecomunicaciones y el espectro electromagnético. Introduce aspectos como:

- Estandarización a nivel de acreditación, presentando cinco certificaciones.
- Comercialización de los servicios ejecutados por los profesionales.
- Formalización de los resultados según las normas éticas y legales a cumplir.
- Planificación mostrando la trazabilidad y tiempos requeridos en cada una de las fases.

ISSAF (Information Systems Security Assessment Framework) [6]: Es una metodología estructurada de análisis de seguridad, está diseñada para la evaluación de los principales elementos de los sistemas informáticos y las comunicaciones de estos. Es un proyecto de OISSG (Open Information System Security Group), tiene una licencia GNU GLP lo que se puede usar de manera libre. Permite aplicarla a cualquier tipo de organización en el análisis de infraestructuras, sistemas operativos, aplicaciones y sistemas de gestión de las bases de datos. Esta metodología está organizada en "Criterios de evaluación" donde se describen objetivos, prerrequisitos, evaluación, contramedidas recomendadas y referencias a documentación externa.
ISSAF propone cinco fases:

Fase I: Planificación y preparación.
Fase II: Evaluación (impactos, riesgos, etc).
Fase III: Presentación de informes, limpieza y destrucción de artefactos.

PTES (Penetration Testing Execution Standar) [7]: El estándar de ejecución de pruebas de penetración está enfocado hacia la auditoría de sistemas permitiéndole a las empresas y los proveedores de servicios de seguridad tener un mismo lenguaje.

El PTES tiene siete etapas que son [8]:

- Interacciones previas al compromiso: En esta se establece los preacuerdos con el cliente donde se expondrán los alcances de la prueba de penetración, las herramientas a usar y los resultados esperados.

[5] Ibit., p. 13.
[6] Ibit., p. 22.
[7] PENETRATION TESTING EXECUTION STANDARD. PTES Technical Guidelines.
[8] ALCALDÍA DE BOGOTÁ. Guardianes de la información: Penetration Testing. p. 6.

- Recopilación de información: Se establecerá los mecanismos para recopilar la información de la empresa a realizar la prueba, se utilizará información pública y la que pueda dar el cliente y la que por medio de otros métodos podamos extraer de los empleados.
- Modelado de amenazas: Se planifica el ataque de acuerdo con la información obtenida en los pasos anterior. Este estándar no requiere la utilización de un modelo específico, por lo que de acuerdo con las características de la empresa se van definiendo, teniendo en cuenta que este esté dentro de los parámetros establecidos por este estándar, centrándose en el modelado de amenazas activos y atacante.
- Análisis de vulnerabilidades: En este proceso se descubre las vulnerabilidades de ciberseguridad de los sistemas auditados que puedan ser explotadas por un atacante. De acuerdo con lo pactado se realiza las pruebas: permisividad de ataques, enfoque o tipo de la prueba, presentación de evidencias recolectadas.
- Explotación: Teniendo las vulnerabilidades analizadas, se procede al ingreso al sistema saltando las seguridades existentes. Con esto se podrá identificar un punto por donde el atacante podrá tener el acceso.
- Informes: Se entrega un informe ejecutivo y técnico al responsable del área de sistemas en un lenguaje fácil de entender, dando solución a los problemas planteados al inicio de la prueba. Se informará de las contramedidas que puedan ser aplicadas para mitigar los riesgos encontrados durante la prueba.

De lo anterior y viendo el contexto en el cual se va a realizar la prueba de intrusión para identificar las vulnerabilidades en el sistema a estudio, se ha elegido la metodología PTES como el estándar para realizar dicha prueba.

El estudio de la seguridad informática en las pymes en Colombia ha despertado gran interés en el ámbito académico ya que este sector económico históricamente es el más afectado por los ataques cibernéticos debido a un número de factores que la hacen atractivos para los ciberdelincuentes como falta de: recursos económicos, conocimientos en ciberseguridad, cultura entre otros.

Una investigación por parte de Monsalve Pulido, Aponte Novoa y Chaves Tamayo [9] en que realizaron un estudio y gestión de vulnerabilidades informáticas en una empresa privada en el departamento de Boyacá, lograron después de aplicar el plan de gestión donde se utilizó una herramienta de análisis de vulnerabilidades la reducción del 70% en las vulnerabilidades del sistema en estudio. Lo que demuestra lo importante que es realizar una prueba de intrusión que nos permita detectar las vulnerabilidades para eliminar o mitigar el riesgo.

[9] MONSALVE PULIDO, Julián; APONTE NOVOA, Fredy & CHAVES TAMAYO, David. Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). p. 72.

Para Ramírez Montealegre, en su investigación “Medición de madurez de ciberseguridad en MiPymes colombianas” de 2016, cada segmento de las MiPymes tiene una particularidad de amenazas y vulnerabilidades que dependen en gran parte a lo económico y al grado de conciencia en ciberseguridad. Recomienda programas de conciencia dirigidas desde las cámaras de comercio y entidades de apoyo [10] de cada sector.

Por otro lado, Gonzáles Díaz y Pulido Sainea en su estudio “La ciberseguridad política clave dentro de las organizaciones” [11] hallaron que los retos más sobresalientes para las pymes en Colombia es la concienciación en temas de ciberseguridad desde las políticas internas de las empresas. Se expone la necesidad de invertir en recursos humanos y tecnológicos apropiados que permitan a las empresas eliminar, reducir y controlar las vulnerabilidades de ciberseguridad.

Una manera de proteger los activos y utilidades de las empresas por algún evento de ataque cibernético es a través de los seguros. Un estudio del impacto que conlleva el riesgo cibernético en las MiPymes (Micro, pequeñas y medianas empresas) en Colombia realizado por Villa Mesa en 2021 [12] concluyó que las aseguradoras si aporta en este propósito, sin embargo, al no contar con una información consolidada el análisis de riesgo cibernético es complejo de cuantificar. Por tanto, esta opción sería limitada en la protección contra ciberataques.

De las investigaciones mencionadas, se destaca la importancia de realizar una evaluación de ciberseguridad en las pymes y es la prueba de intrusión una herramienta importante que permite diagnosticar el estado de seguridad de una empresa. Estos estudios han validado la pertinencia y eficacia de las pruebas de intrusión en aumentar la ciberseguridad de las empresas.

La necesidad de mejorar los procesos de seguridad informática se ve reflejada en normatividad como lo son la serie de normas ISO/IEC 27000 que se enfoca en el sistema de gestión de seguridad de la información y metodologías que permiten evaluar la seguridad como PTES que se hacen necesarias para los temas relacionados con la auditoría de sistemas.

La metodología PTES fue creado en 2009 por seis consultores de seguridad informática que, tras encontrar problemas recurrentes en las pruebas de penetración, crearon un estándar para ayudar a los clientes y a los especialistas de ciberseguridad con herramientas, técnicas y elementos que les permitieran realizar

[10] RAMIREZ MONTEALEGRE, Benjamín José. Medición de madurez de ciberseguridad en pymes colombianas. p. 64.
[11] GONZÁLEZ DÍAZ, David & PULIDO SAINEA, Saúl. La ciberseguridad política clave dentro de las organizaciones. p. 12.
[12] VILLA MESA, Sara. Impacto del Riesgo Cibernético en el Bienestar del Segmento Mipyme. p. 31.

una prueba de penetración o intrusión [13] de forma generalizada. Lo cual es ideal para su aplicación en la empresa de estudio de este trabajo.

PTES al ser una reciente metodología de pruebas de penetración, su uso es algo limitado, sin embargo, se ha venido adelantando desde el área de la academia investigaciones de su aplicabilidad en las empresas colombianas como es el caso del proyecto aplicado “Aplicación de la metodología PTES en la clínica Medellín para la identificación de vulnerabilidades en historia clínica electrónica” [14] donde a través de la metodología propuesta se adelanta el análisis de vulnerabilidades con el fin de aumentar la ciberseguridad de la empresa de estudio.

Teniendo en cuenta lo anterior y la gran importancia de que la seguridad de la información para la continuidad de los negocios tiene, se hace muy pertinente la metodología PTES con miras de fortalecer los niveles de ciberseguridad en las empresas.

4.2 MARCO CONCEPTUAL

4.2.1 Seguridad informática: “Conjunto constituido por varias metodologías, documentos, software y hardware que determinan que los accesos a los recursos de un sistema informático sean llevados a cabo exclusivamente por lo elementos autorizados a hacerlo” [15] . Haciendo de ello un sistema fiable, teniendo en cuenta que un sistema sea fiable tener satisfacer las tres siguientes propiedades:

- Confidencialidad: Solo pueden acceder los recursos autorizados.
- Integridad: Solo pueden ser modificados o alterados por elementos autorizados para hacerlo.
- Disponibilidad: Los recursos del sistema tiene que permanecer accesibles a los elementos autorizados.

[13] CYBERSECURITY EDUCATION GUIDES. [Sitio web]. USA: What Is The PTES (Penetration Testing Execution Standard)? Disponible en: https://www.cybersecurityeducationguides.org/what-is-the-ptes-penetration-testing-execution-standard/

[14] BOISSON MORALES, Natalia. Aplicación de la metodología PTES en la clínica Medellín para la identificación de vulnerabilidades en historia clínica electrónica. p. 21.

[15] COLOBRAN HUGUET, Miguel; ARQUÉS SOLDEVILLA, José María y GALINDO, Eduard Marco. Administración de sistemas operativos en red. p. 213.

4.2.2 Prueba de intrusión o Pentesting: Una de las definiciones es la dada por la NIST “Prueba de seguridad donde los evaluadores imitan los ataques del mundo real en un intento de identificar formas de eludir las características de seguridad de una aplicación, sistema o red. Las pruebas de penetración a menudo implican la emisión de ataques reales a sistemas y datos reales, utilizando las mismas herramientas y técnicas que utilizan los atacantes reales” [16].

4.2.2.1 Tipos de prueba en los test de intrusión [17]: Se definen los siguientes:

- Test black box (caja negra): Es el método más realista, ya que corresponde a una situación más realista. En este caso el analista no posee ninguna información sobre la empresa a auditar simulando ser un atacante buscando de una vulnerabilidad que pueda explotar.

- Test grey box (caja gris): El consultor solo posee una cantidad limitada de información con lo cual puede llegar un poco más lejos que con el test de caja negra.

- Test White box (caja blanca): Es el más largo y con el que más profundo se puede llegar, sin embargo, es más costoso. Tiene como intensión probar cada servicio, verificar su configuración, las posibles vulnerabilidades y hacer una revisión completa para garantizar el blindaje.

4.2.2.2 Metodologías intrusión [18]: Conjunto de fases documentadas que se deben cumplir con un propósito de análisis de seguridad con el que se busca vulnerar una infraestructura para encontrar vulnerabilidades para luego explotarlas. Algunas de estas metodologías fueron expuestas en el marco teórico.

4.2.3 Herramientas de intrusión, testing e ingeniería social: A continuación, algunas de las herramientas más usadas:

Kali Linux: [19] Es una distribución de Linux basada en Debian, diseñada para la auditoría de seguridad, las pruebas de intrusión y la informática forense. Es una mejora sobre la famosa y conocida BackTrack. Esta es mantenida por la empresa Offsensive Security Ltda que utiliza paquetes GLP por lo que su fuente está

[16] NATIONAL INSTITUTE OF STANDAR AND TECHNOLOGY NIST. Technical Guide to Information Security Testing and Assessment. p. F-1.
[17] FUENTE MAESTRO, Antonio. Elaboración de una metodología de test de intrusión dentro de la auditoria de seguridad. p. 49.
[18] POSTIGO PALACIOS, Antonio. Seguridad informática. p. 195.
[19] SANTOS ORCERO, David. Kali Linux. p. 15.

disponible. El desarrollo está focalizado en un reducido grupo desarrolladores con lo cual controlan los paquetes GPG para evitar que se introduzcan troyanos en su distribución. Incluye más de 600 aplicaciones para la auditoría de seguridad e informática forense que incluye escáneres de puertos, sniffers, suites de creckeo de redes inalámbricas, suites para construir troyanos y exploits.

OpenVAS (Open Vulnerability Assessment System):[20] es un sistema que contiene herramientas de escaneo de red. Uno de sus principales componentes es un servidor que contiene test de vulnerabilidades de red NVT's con lo cual se logra detectar problemas de vulnerabilidades de los sistemas y aplicaciones remotas [21]. Actualmente, este sistema cambió a llamarse Greenbone donde se puede encontrar que se debe pagar por la versión full, también se encontra una versión trial por 14 días con la posibilidad de descargar las imágenes para máquinas virtuales ya listas, están en la versión para VirtualBox y VMware. También existe una versión gratis llamada Greenbone Source Edition (GSE) que es soportada y mantenida por la comunidad.

Sparta [22]: Herramienta en forma de interfaz de usuario para la realización de pentestin en la fase de exploración y enumeración. Cuenta con un conjunto de herramientas destinadas para la seguridad informática.
Puede definir tareas automatizadas para los servicios como, por ejemplo, servicio HTTP o SSLSCAN.

Nmap [23] (network mapper): Es un escáner de puertos disponibles para sistemas Windows y Linux, es la herramienta más usada para llevar a cabo un completo análisis de toda una red, de un rango de direcciones o de una sola IP, centrándose en determinar qué puertos y servicios se encuentran disponibles.

Metasploit [24]: Es una herramienta para desarrollar y ejecutar exploits (fragmento de software) contra una máquina remota con la intención de encontrar vulneraciones de seguridad para luego explotarlas.

Wireshark [25]: Herramienta para capturar paquetes disponibles para sistemas Windows y Linux, con el más amplio uso. Es de fácil uso y su funcionamiento radica en capturar paquetes para luego procesarlos aplicando un amplio conjunto de protocolos para que el usuario pueda analizarlo más fácilmente. Permite realizar filtros para seleccionar qué tipo de información necesita el usuario.

---

[20] GREENBONE. [Sitio web]. Osnabrück: Greenbone Networks GmbH, OpenVAS – Open Vulnerability Assessment Scanner. Disponible en: https://www.openvas.org/
[21] ARCHLINUX. [Sitio web]. Berlín: Levente Polyak & team, OpenVAS (español). https://wiki.archlinux.org/title/OpenVAS_(Espa%C3%B1ol)
[22] ORTEGA CANDEL, José Manuel. Hacking ético con herramientas Python. p. 58.
[23] ARBOLEDAS BRIHUEGA, David. BackTrack 5: Hacking de redes inalámbricas. p. 283.
[24] ORTEGA CANDEL, José Manuel. Hacking ético con herramientas Python. p. 250.
[25] POSTIGO PALACIOS, Antonio. Seguridad informática. p. 18.

Sqlmap: Herramienta escrita en Python para detectar vulnerabilidades tipo SQL Injection. Permite realizar peticiones a los parámetros de un URL que se le indique y detectar si para algún parámetro el dominio es vulnerable. Si llega a detectar alguna vulnerabilidad puede atacar el servidor para descubrir nombres de tablas, descargar la base de datos y realizar consultas SQL de forma automática.

John the Ripper: Es un programa de criptografía el cual aplica fuerza bruta para descifrar contraseñas, posee la habilidad de romper algoritmos de cifrado como DES, SHA-1 entre otros.

Hydra: Esta herramienta trata de averiguar contraseñas en cualquier servicio on-line. Por lo cual, tiene soporte en protocolos como SSH, FTP, IMAP, IRC, entre otros.

Burp Suite: Cuenta con una completa herramienta de analizadores de vulnerabilidades web. Es bajo licencia así que hay que pagar para obtenerla. Hay una versión gratuita pero no cuenta con todas las herramientas que esta suite ofrece. Es muy usada por los auditores de seguridad que en cuestión de segundos pueden hallar vulnerabilidades en la página web.

4.3 MARCO HISTÓRICO

Según los expertos en seguridad informática Deborah Rusell y GT Gangemi Sr en su libro Conceptos básicos de seguridad informática “La década de 1960 marcó el verdadero comienzo de la era de la seguridad informática” [26] cuando el uso de los sistemas informáticos se extendió, desarrollando nuevas maneras de trabajar y compartir el conocimiento cuando la utilización del sistema tiempo compartido en las computadoras permitió a varias personas trabajar en un mismo recurso informático al mismo tiempo.

Fue cuando en una convención en 1967, expertos en computación utilizaron el término “penetración” al referirse a un ataque a un sistema de computadores. Expresaron su preocupación por las vulnerabilidades a la privacidad de la información que esto conllevaba. Dentro de estos expertos se encontraban Willis Ware, Rein Turn y Harold Petersen de la empresa RAND Corporation, por parte de la NSA (National Security Agency) Bernard Peters y demás asistente concluyeron que la penetración de sistema de computadoras es una de las principales amenazas de seguridad en los sistemas informáticos.

[26] HMONG.ES. [Sitio web]. Madrid: HMONG.ES, Prueba de penetración. Disponible en: https://hmong.es/wiki/Penetration_test

Más adelante, en los años de 1970, el gobierno de los Estados Unidos y empresas privadas con la intención de conocer más a profundidad las brechas de seguridad en los sistemas informáticos de tiempo compartido y buscar como solucionarlos, crearon grupos de penetradores llamados “grupos tigre” que llegaron a tener incursiones a sistemas específicos con gran éxito. Con lo que se concluyó la gran utilidad que tiene las pruebas de penetración y su uso continuo para mejorar la seguridad de los sistemas informáticos.

A principios de 1971, el experto en penetración informática James P. Anderson ex trabajador de RAND Corporation, la NSA entre otras empresas del sector, propuso una serie de pasos para realizar las pruebas de intrusión:

1. Encuentra una vulnerabilidad explotable.
2. Diseña un ataque a su alrededor.
3. Prueba el ataque.
4. Aprovecha una línea en uso.
5. Entra en el ataque.
6. Aproveche la entrada para recuperar información.

Con el tiempo, las pruebas de intrusión han ido evolucionando y siendo más detalladas, han aparecido diferentes metodologías de aplicación de estas pruebas que responden a las necesidades actuales en cuestiones de ciberseguridad.

4.4 ANTECDENTES O ESTADO ACTUAL

La pyme Colombia Leds SAS, en el año 2017 fue víctima de un ataque cibernético que le causó grandes pérdidas tanto económicas como reputacionales, lo que les obligó en su momento a realizar una serie de actividades para mitigar los riesgos como:

- Actualización de los equipos de cómputo.
- Cambio de sistemas operativos para el equipo servidor y el sistema de almacenamiento de información.
- Implementación de reglas de firewall en el servidor.

Estas medidas en su momento le ayudaron a mitigar los riesgos más críticos, sin embargo, desde entonces no se ha realizado alguna mejora en cuestiones de ciberseguridad y se desconocen las vulnerabilidades de seguridad informática presentes en el sistema.

Actualmente, la empresa cuenta con las siguientes prácticas de ciberseguridad:

- Ingreso de sesión a los equipos de cómputo con PIN.
- Activación local de antivirus y contrafuego del sistema operativo de cada equipo.
- Utilización de contrafuegos en el servidor.
- Red inalámbrica para visitantes con control web.
- Control de acceso a los sistemas de información con usuario y contraseña.

4.5 MARCO LEGAL

4.5.1 Ley de delitos informáticos en Colombia: ley 1273 de 2009: Con esta ley se modifica el código penal con el cual se crea un bien tutelado con el nombre de "de la protección de la información de la información y de los datos [27]".

Con esta ley lo que busca es tipificar los delitos que por medios electrónicos se apropie ilícitamente de patrimonio de un tercero. En esto se puede encontrar la clonación de tarjetas bancarias, la interceptación de datos, vulneración de los sistemas de cómputo y su posterior alteración utilizando programas, la afectación de cajeros automáticos, entre otros.

Esta ley se divide en dos capítulos a considerar:

Capítulo I: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

- Artículo 269A: Acceso abusivo a un sistema informático. Si se ingresa a un sistema sin la autorización debida o por fuera de lo acordado se le podrá imponer una pena entre 48 y 96 meses de prisión más una multa entre 100 a 1000 SMLMV.
- Artículo 269B: Obstaculización ilegitima de sistema informático o red de telecomunicaciones. El que impida u obstaculice el funcionamiento o ingreso normal de la red. La pena estará entre 48 y 96 meses de prisión y una multa de 100 a 1000 SMLMV.
- Artículo 269C: Interceptación de datos informáticos. Para aquellos que intercepten sin orden judicial datos que procedan de sistemas informáticos. Prisión de 36 a 72 meses.
- Artículo 269D: Daño Informático. La persona destruya, dañe, borre o altere datos que procedan de sistemas informáticos tiene una prisión de 48 a 96 meses y una multa entre 100 a 1000 SMLMV.

[27] CONGRESO DE COLOMBIA. [Sitio web]. Bogotá D.C.: CONGRESO DE LA REPÚBLICA, Ley 1273 de 2009. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

- Artículo 269E: Uso de software malicioso. Toda aquella persona que produzca comercialice en cualquiera de sus etapas en Colombia software malicioso sin estar facultado para ello, podrá tener una prisión de 48 a 96 meses y una multa de 100 a 1000 SMLMV.
- Artículo 269F: Violación de datos personales. El que se aproveche sin estar facultado para ello para beneficio propio o de una tercera persona para obtener, compilar, sustraer, intercambiar, divulgar vender, modificar, etc. datos personales en cualquier tipo de formato digital tendrá prisión de 48 a 96 meses y una multa entre 100 y 1000 SMLMV.
- Artículo 269G: Suplantación de sitios web para capturar datos personales. Aquí se condena el denominado Phishing que es un tipo de fraude más común en el ámbito de los sistemas.
- Artículo 269H: Circunstancias de agravación punitiva: Los delitos mencionados en los puntos anteriores se agravan entre la mitad y tres cuartas partes de la pena cuando:
    - Los sistemas vulnerados son estatales y/o del sector financiero tanto nacional como extranjeros.
    - Cuando el que comete el delito es un funcionario público en ejercicio.
    - Aprovechamiento de confianza cuando exista un contrato.
    - Revelar información en contra de otro.
    - Obtención de beneficio para sí mismo o un tercero.
    - Con fines terroristas.
    - Utiliza a un tercero como instrumento.
    - Quien sea responsable de la administración de la información además de la pena se le inhabilitará para ejercer su profesión relacionada con sistemas de información.

Capítulo II: De los atentados informáticos y otras infracciones.

- Artículo 269I: Hurto por medios informáticos y semejantes. Aquellos que vulnere los sistemas saltando la seguridad de los sistemas con su manipulación o suplantando identidad podrá incurrir en penas de 3 a 8 años de prisión.
- Artículo 269J: Transferencia no consentida de activos. Para aquellas personas que con fines de lucro transfieran activos en contra de un tercero sin tener el permiso valiéndose de los sistemas de información tendrán prisión entre 48 hasta 120 meses y una multa entre 200 y 1500 SMLMV.

4.5.2 Ley de protección de datos: Ley 1581 de 2012: Conocida como ley de protección de datos personales, es una ley complementaria a la vigencia actual que tiene como fin la protección del derecho fundamental que tiene todas las personas naturales a autorizar sus datos almacenados en las bases de datos o archivos, también para hacer actualizaciones o correcciones [28].

Se define como dato personal a cualquier tipo de información que se pueda asociar a una o varias personas naturales teniendo en cuenta el tipo de información. A saber:

- Dato personal público: Son los datos que desde la constitución y la normatividad vigente son determinados como públicos y que por tanto no se necesita la autorización de la persona titular como lo puede ser nombre, número de identificación, profesión, estado civil, entre otros.
- Dato personal semiprivado: Es la información que no es ni pública ni tiene una connotación de íntima que puede interesar a un grupo de personas como por ejemplo datos financieros, dato crediticio, reportes centrales de riesgo. También fecha y lugar de nacimiento.
- Dato personal privado: Son datos íntimos que solo le interesa al titular y que por tanto se requiere de la autorización. Este dato pueden ser estudios, dirección, teléfono, datos laborales, infracciones administrativas y penales, fotografías, vídeos y cualquier otro dato del estilo de vida del titular.

En los siguientes casos no aplica esta ley:

- Cuando la información es usada de forma personal.
- Cuando se tenga la finalidad de la seguridad y defensa nacional.
- Si las bases de datos se usen para inteligencia y contrainteligencia.
- Si los datos y archivos son información periodística o editoriales.

[28] FUNCIÓN PÚBLICA GOBIERNO DE COLOMBIA. [Sitio web]. Bogotá D.C: Ley Estatutaria 1581 De 2012. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

5 DISEÑO METODOLÓGICO

Para la realización de este proyecto, se planea hacer uso de la metodología de hacking ético PTES desarrollando las fases que la componen. Estas fases son [29]:

1. Interacciones previas.
2. Recolección de información.
3. Modelado de amenazas.
4. Análisis de vulnerabilidades.
5. Explotación.
6. Post-explotación.
7. Informe final.

Debido a que esta metodología es aceptada como un estándar en seguridad informática, facilita al auditor la tarea de realizar una prueba pentesting para detectar las vulnerabilidades y su posterior explotación para entrar a detallar las brechas de seguridad encontrados. Esta metodología permite ser ejecutada en cualquier tipo de empresa y sector, lo que la hace ampliamente aceptada y su implementación sea sencilla.
Para la implementación de esta metodología se requieren algunas herramientas que según el escenario que se encuentre se adoptaran una u otras, sin embargo, esta metodología es flexible en ese aspecto y permite al auditor elegir la que mejor le parezca.

Por otro lado, se le dará uso la herramienta Greenbone (openVAS) en su edición Source Edition la cual nos permite hacer el análisis de vulnerabilidades de la red en la cual se realizará la prueba de penetración.

Como tipo de intrusión se elegido la por las características y los resultados esperados la prueba de caja gris, con lo cual la información del sistema será limitada.

Teniendo en cuenta esta metodología y alineándolo con los objetivos de este trabajo, se propone abordarlos de la siguiente manera:

- Objetivo 1: Interacciones previas y Recolección de información.
- Objetivo 2: Modelado de amenazas y Análisis de vulnerabilidades.
- Objetivo 3: Explotación y Post-explotación.
- Objetivo 4: Informe final.

[29] BOISSON MORALES, Natalia. Aplicación de la metodología PTES en la clínica Medellín para la identificación de vulnerabilidades en historia clínica electrónica. p. 33.

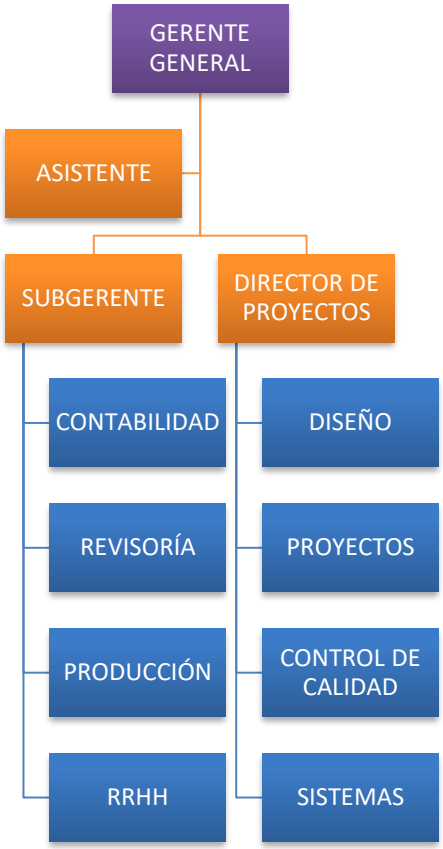
6 DESARROLLO DE LOS OBJETIVOS

6.1 ANALIZAR LA INFORMACIÓN MÁS RELEVANTE REFERENTE A LA ESTRUCTURA ORGANIZACIONAL E INFRAESTRUCTURA TECNOLÓGICA DE LA PYME COLOMBIA LEDS SAS PARA LOGRAR APLICAR ADECUADAMENTE LA METODOLOGÍA PTES.

Para el desarrollo de este objetivo, basados en la metodología PTES se hará uso de las fases 1 y 2 donde se realizarán las actividades de interacciones previas con el cliente donde se establecerán los alcances de esta prueba y se recolectará la información sobre la estructura de la empresa en la disposición del recurso humano y sus funciones, así como del área de infraestructura tecnológica, información necesaria para la seleccionar la más importante en miras de realizar una prueba de intrusión exitosa.

6.1.1 Estructura organizacional: En entrevista con el gerente de la empresa Colombia Leds S.A.S, se indaga sobre el modelo de negocio, cómo la infraestructura TI ayuda a soportar las operaciones y el funcionamiento de la empresa, además de proporcionar la estructura organizacional plasmada en la figura 1.

Figura 1. Estructura organizacional Colombia Leds SAS.



Fuente: Elaboración propia.

Colombia Leds SAS es una empresa familiar con domicilio en Bogotá D.C. que se dedica a la comercialización, diseño e instalación de sistemas de iluminación led.

Gerente general: Es el representante legal de la empresa, se encarga de realizar los contactos comerciales, hacer los negocios y relaciones públicas con los clientes y proveedores.

Subgerente: Es encargado del área administrativa de la empresa, así como el área de producción. Tiene a cargo las áreas de contabilidad, revisoría, RRHH y producción donde se fabrican perfiles y accesorios para los sistemas de iluminación led.

Director de proyectos: A su cargo está el área de proyectos, el diseño, control de calidad de los productos fabricados y el área de sistemas de la empresa.
Como responsable del área TI, se encarga de mantener los sistemas, administrar los recursos y dar soporte a los incidentes tecnológicos.

Análisis de estructura organizacional: De acuerdo con los datos obtenidos, la estructura organizacional en Colombia Leds SAS se encuentra dentro de lo que denomina “estructura organizacional funcional” que según Henri Fayol lo postula como la mejor forma de una organización la cual se basa en la distribución de funciones y sus respectivas subfunciones y procedimientos con sus respectivos puestos de trabajo [30].

Según Fayol, para aumentar la eficiencia de las empresas hay que desarrollar una serie de principios los cuales se describen las más sobresalientes que se ven claramente en la empresa Colombia Leds SAS:

- División del trabajo: del trabajo hay que hacer una división haciendo una especialización en las tareas. En la empresa Colombia Leds SAS estas funciones están divididas en áreas como contabilidad, revisoría, producción, RR.HH., diseño, proyectos, control de calidad y sistemas.
- Autoridad y responsabilidad: Dar órdenes y esperar acatamiento. Para Colombia Leds SAS hay tres líderes que son el gerente general, subgerente y director de proyectos los cuales imparten las órdenes de acuerdo con los objetivos de la empresa y sus subalternos responden con las tareas asignadas.
- Unidad de mando: Los empleados solo reciben órdenes de un solo jefe que para el caso de la empresa Colombia Leds SAS es el gerente general, subgerente y director cada uno sus áreas encargadas.
- Unidad de dirección: La dirección de la empresa está a cargo del gerente general que es el mayor accionista y este junto con la junta directiva hacen la toma de decisiones.
- Centralización: Para Colombia Leds la cabeza de la empresa y la toma de decisiones está a cargo del gerente general.

Por el tamaño de la empresa Colombia Leds SAS, este tipo de estructura organizacional es adecuada ya que se optimiza el recurso humano disponible, proporcionando el ambiente laboral adecuado a los empleados [31]. Es por eso por lo que las pymes en Colombia adoptan esta estructura en sus empresas.

Dentro del análisis que se hace para realizar adecuadamente la prueba de intrusión bajo la metodología PTEST es muy importante conocer la estructura organizacional de la empresa ya que con ello nos da información muy valiosa para poder considerar posibles vectores de ataques aumentando así las probabilidades de éxito.

[30] GESTIOPOLIS. [Sitio web]. Bogotá D.C.: Teoría de la organización y estructuras organizacionales. Disponible en: https://www.gestiopolis.com/teoria-organizacion-estructuras-organizacionales/
[31] PORTO SOLANO, Andrés. Estructuras organizacionales: Nuevas tendencias. p. 81.

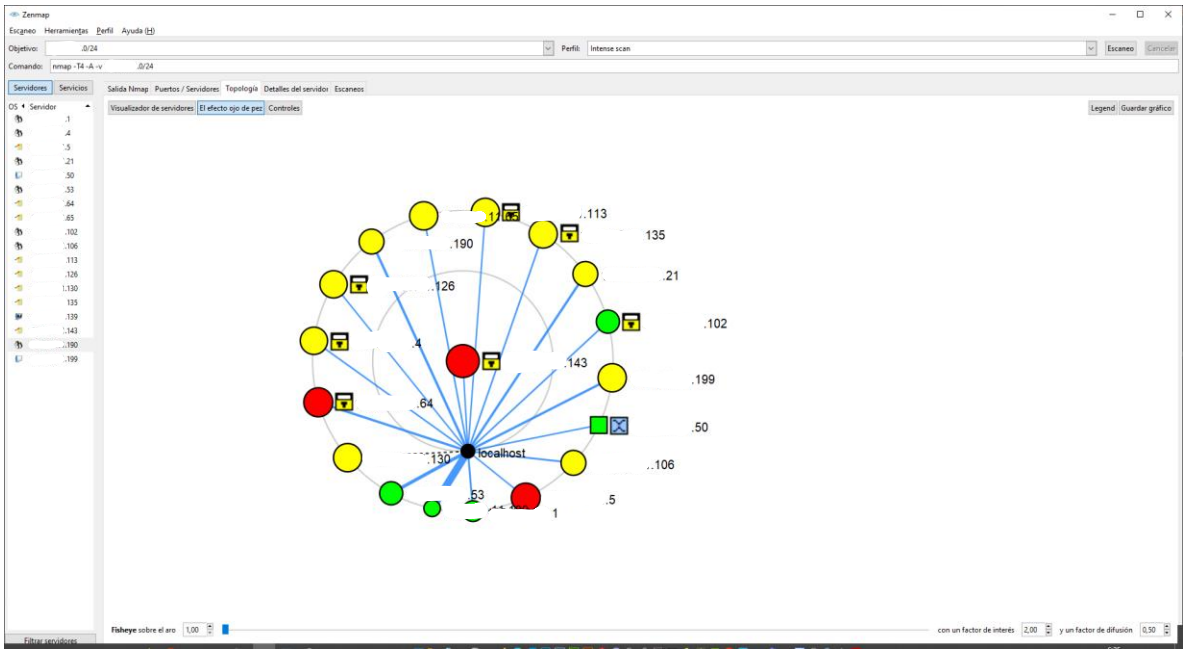
6.1.2 Estructura TI: El levantamiento de la información correspondiente al área TI de la empresa se realizó con entrevista al gerente y el encargado del área de sistemas, así como la utilización de herramientas de escaneo de red para la identificación de lo hosts.

6.1.2.1 Topología de red*:* Actualmente la empresa cuenta con la siguiente infraestructura tecnológica:

- ISP: El único proveedor de internet suministra una velocidad simétrica de 50 MB.
- Firewall: No cuenta con firewall dedicado, solo usa el firewall que viene integrado en el switch capa 3 y del sistema operativo del servidor principal.
- VPN: Se tiene un servicio de VPN configurado con la herramienta libre Wireguard que les permite a los empleados del área administrativa trabajar desde casa. Este trabaja bajo una semilla que genera el administrador del servidor y mediante un cliente de esta herramienta realiza la conexión a la red privada mediante protocolos de alto cifrado.
- Switch capa 3: Se encarga de distribuir los datos entre la red local, la DMZ y el acceso a internet.
- Servidor: Tiene configurado firewall local con reglas para la administración de la VPN, están bajo sistema operativo Linux, con lo cual no manejan algún antivirus.
- NAS: Se utiliza para almacenar el respaldo de la información más importante de la empresa como la base de datos de los inventarios, el sistema contable y archivos de los proyectos. Es administrado por el servidor.
- Red inalámbrica: Cuenta con una conexión inalámbrica para acceso a internet de los visitantes con administración desde consola y una red para la red local.
- Estaciones de trabajo: Están bajo sistema operativo Windows, con firewall local activo y antivirus del sistema operativo.
- Siigo: Este programa se encarga del sistema de facturación, la contabilidad y manejo de nómina de la empresa. Tiene licencia Stand Alone con la base de datos en un repositorio que se encuentra en el servidor del DMZ.

6.1.2.2 Escaneo de red y puertos: Para el levantamiento de la información de la red de la empresa Colombia Leds SAS se solicitó un punto de acceso con el cual se realizaron escaneo para el descubrimiento de los hosts utilizando la herramienta Zenmap, la versión para sistemas operativos Windows de NMAP, con la cual se identificaron los hosts de la red, su sistema operativo y los puertos abiertos en cada uno de ellos. El resultado de este escaneo se puede ver en la Figura 2.

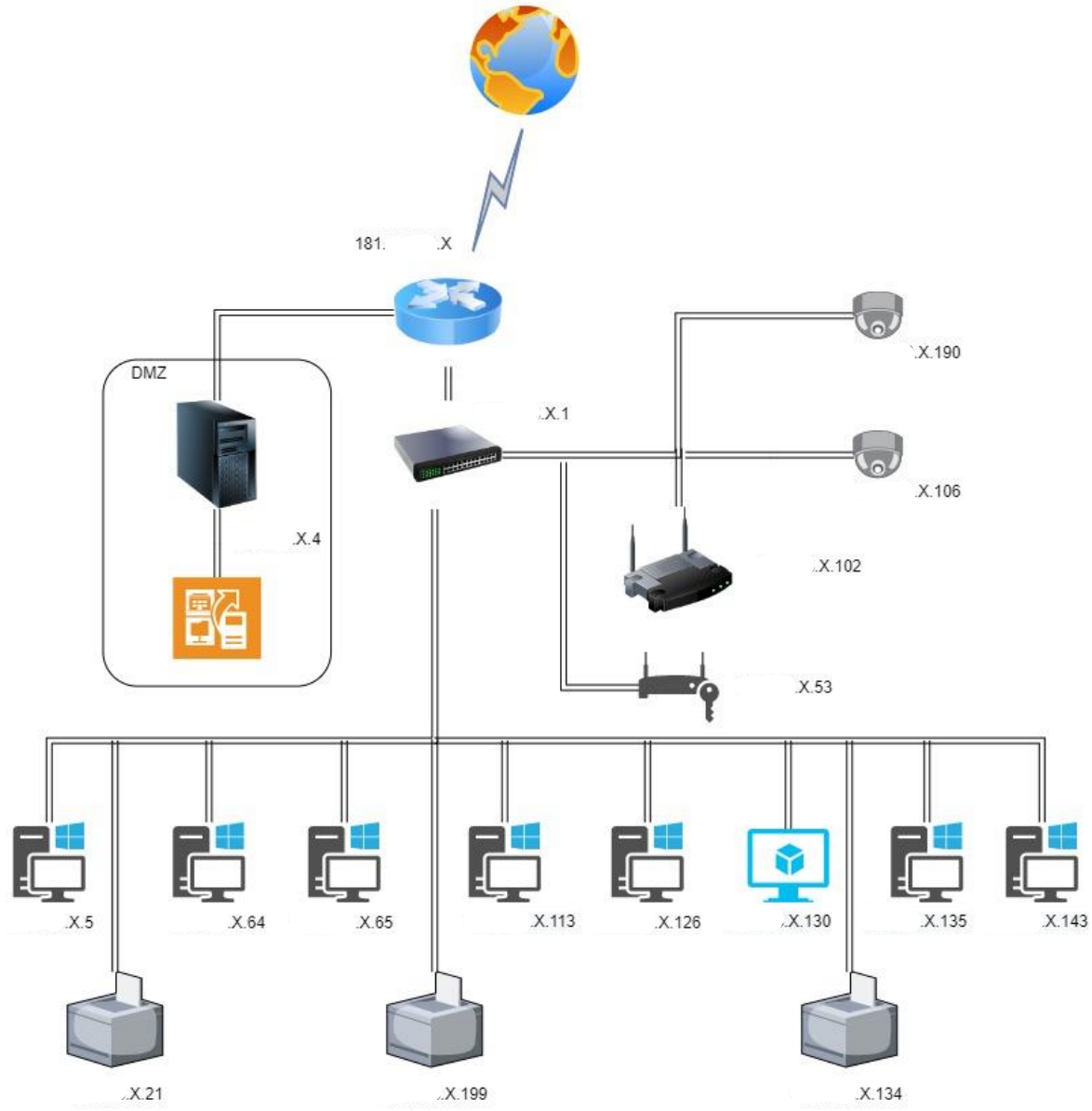
Figura 2. Resultados escaneo de red.



Fuente: Elaboración propia.

6.1.2.3 Diagrama de topología de la red según resultados del escaneo: Al entrevistar con el director de proyectos, quien es el encargado del área de sistemas de la empresa, dice que actualmente no se cuenta con algún esquema de la topología de red, por tanto, basados en la información obtenida en el escaneo de la red, se procede a realizar el levantamiento de la topología de la red en estudio en cual se puede ver en la Figura 3.

Figura 3. Topología de según análisis de escaneo.



Fuente: Elaboración propia.

De esta manera, haciendo uso de herramientas de descubrimiento de red se ha podido realizar la topología de la red de estudio con lo cual nos da el insumo básico para poder realizar las siguientes etapas del test de intrusión.

Análisis de estructura tecnológica: La red tecnológica de la empresa Colombia Leds SAS se encuentra dentro de lo más habitual para las pymes, donde se implementa una pequeña red local tanto cableada (LAN) como inalámbrica (WLAN) para compartir servicios como internet, impresión, página web y un repositorio. El uso de un servidor multipropósito que funciona como firewall, servidor web, servidor de archivos mediante SMB y que se encuentra en el DMZ es altamente vulnerable a posibles ataques. Lo ideal es que este servidor esté aislado de la red interna de la empresa.

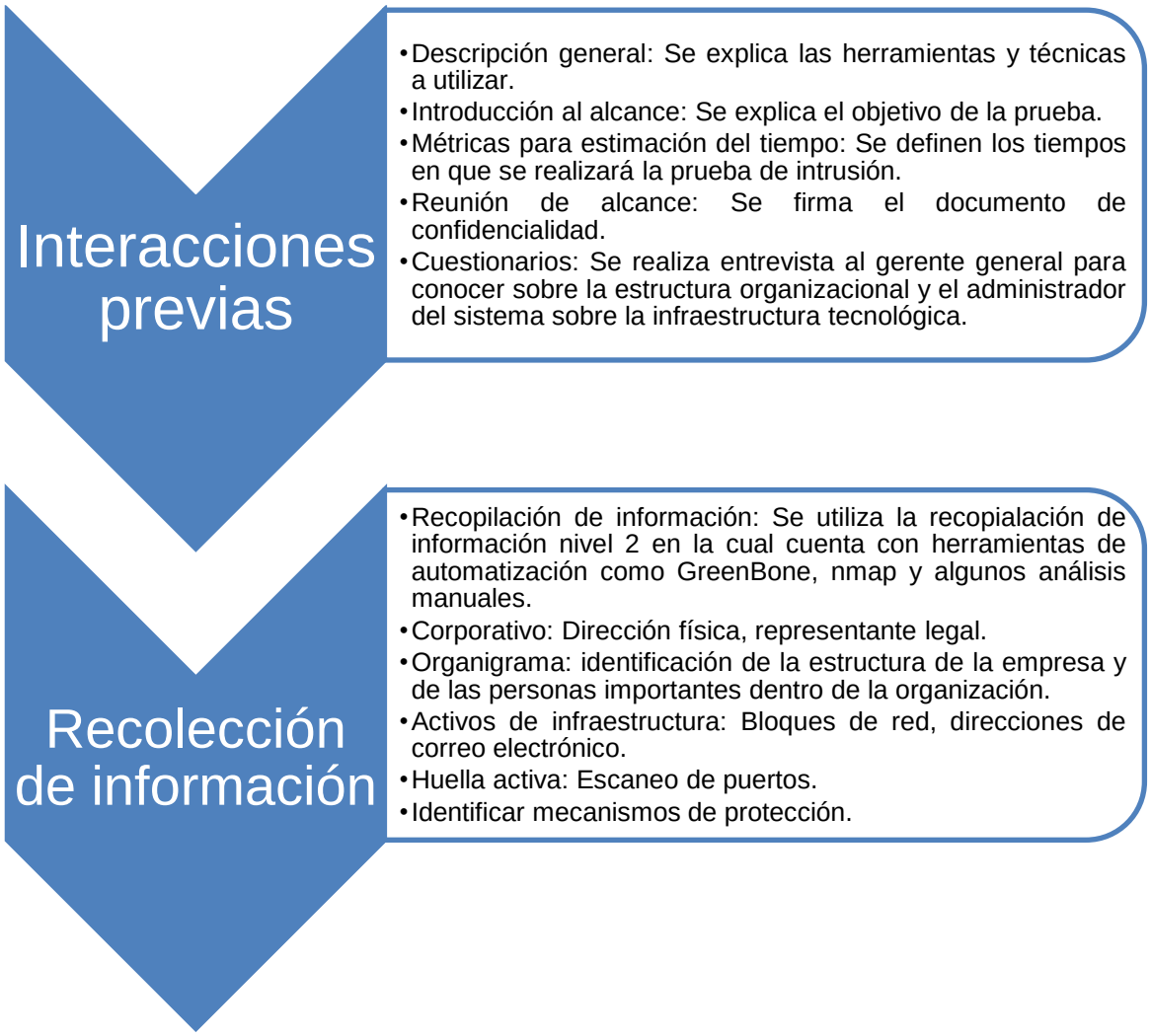
Las cámaras de seguridad IP se encuentran solamente para ser accedido desde la red interna, lo cual mejora la seguridad y evita la explotación de vulnerabilidades desde internet. Para poder acceder a las cámaras desde internet es necesario conectarse a la red LAN por medio de VPN.

Por ser una red muy pequeña y que se ajustan a las necesidades de la empresa, no es necesario la administración de los equipos de cómputo por medio de un directorio activo, por lo que se requiere una administración local. Teniendo en cuenta lo anterior, el administrador del sistema deberá realizar una revisión periódica en cada uno de los equipos para asegurar su correcto funcionamiento y que los parámetros de seguridad se encuentren al día como antivirus, actualizaciones automáticas y usuarios administradores locales.

En la figura 4 se aprecia los ítems que se aplicaron de las fases 1 y 2 de la metodología PTES en las cuales se basaron para el desarrollo de este objetivo. En primer lugar, en la fase de “Interacciones previas” se establecieron los acuerdos con el cliente objeto de esta prueba de intrusión donde se explicaron las herramientas a utilizar, el alcance de la prueba todo esto se hace a través de un documento de confidencialidad y dentro de la reunión con el gerente y el encargado del área TI de la empresa se realiza una entrevista sobre la estructura organizacional y tecnológica fundamental para el desarrollo de la prueba de intrusión.

La otra fase corresponde a la “recolección de información” la cual se tomó según la metodología PTES el nivel 2 de recolección de información que básicamente es la utilización de herramientas de automatización para la obtención de información de red como es GreenBone y Nmap que permiten el escaneo de puertos para conocer la infraestructura TI y por otro lado la detección de vulnerabilidades que existen dentro de la red de la empresa. Con la información obtenida en la fase 1 de la metodología PTES se realiza el organigrama, se identifica las personas principales en los cargos de alta dirección. Con el escaneo de puertos se identificaron los dispositivos (host) entre los cuales se encuentra equipos de cómputo, impresoras, cámaras IP, servidor DMZ que contiene como un firewall que actúa como mecanismo de protección de la red.

Figura 4. Diagrama fases 1 y 2 de metodología PTES aplicadas al objetivo.



Fuente: Elaboración propia.

Con el desarrollo de este objetivo se concluyó la importancia que tiene siempre limitar los objetivos de la prueba de intrusión con el fin que sean alcanzables y estén de acuerdo con los intereses de la empresa que solicita la prueba. Por eso, es de vital importancia para el éxito de la prueba de intrusión estas dos primeras fases propuestas en la metodología PTES.

De acuerdo con los resultados obtenidos al finalizar la prueba de intrusión expuesta en este trabajo y teniendo en cuenta los datos recolectados en este punto, se harán las recomendaciones necesarias para aumentar la ciberseguridad en la empresa Colombia Leds SAS.

6.2 ESTRUCTURAR EL ATAQUE SOBRE LA INFRAESTRUCTURA TECNOLÓGICA DE LA PYME COLOMBIA LEDS SAS QUE PERMITA HALLAR LOS PUNTOS MÁS VULNERABLES PARA SU POSTERIOR EXPLOTACIÓN.

Para el desarrollo de este objetivo se toma la tercera fase de la metodología PTES "Modelado de amenazas" y la fase 4 "Análisis de vulnerabilidades". Para la fase 3 de la metodología aplicada se sugiere realizar el proceso de modelado de amenazas de alto nivel en los siguientes pasos:

6.2.1 Obtención de documentación relevante: La obtención de información que permitió la elaboración del inventario fue obtenida por el escaneo de la red y la información suministrada por el encargado del área de sistemas que indicó la utilización de un NAS administrado por el servidor.

6.2.2 Identificación y categorización de los activos TI: De acuerdo con la relevancia que tiene los activos TI para el negocio, estos se catalogaron entre primarios y secundarios, donde los primarios son lo que son indispensables para la operación y los secundarios los que no son tan relevantes y que son sistemas de apoyo el cual se resumen en el Cuadro 1.

Cuadro 1. Categorización de activos TI.

Activo	Categorización	Descripción	Propietario	Custodio
Servidor	Primario	Equipo con sistema operativo Linux Fedora con los servicios: HTTP, SSH y SMB. Repositorio y base de datos Siigo.	Líder sistemas.	Líder sistemas.
NAS	Primario	Servidor para el almacenamiento de información con los servicios FTP y SMB.	Líder sistemas.	Líder sistemas.
Switch	Primario	Administra el enrutamiento de la red LAN y la salida al internet.	Líder sistemas.	Líder sistemas.
Router ISP	Primario	Proporciona la conexión a internet.	ISP.	Líder sistemas.

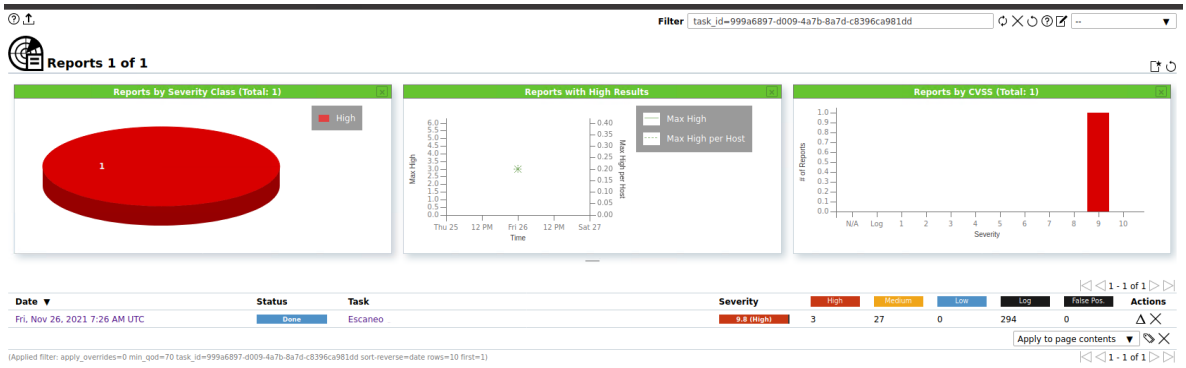
Router inalámbrico	Primario	Proporciona señal inalámbrica para salida internet de los visitantes y acceso a la red LAN para los empleados.	Líder sistemas.	Líder sistemas.
Equipos PCs	Primario	Equipos con sistemas operativos Windows 8.1 y Windows 10. Conectados a la red LAN por cable.	Líder sistemas.	Personal a cargo.
Equipo Virtual	Secundario	Máquina virtual con sistema operativo Windows 10 y con servicio de HTTP.	Líder sistemas.	Líder sistemas.
Cámaras IP 2	Secundario	Cámaras de seguridad ubicadas en las instalaciones de la empresa.	Líder sistemas.	Líder sistemas.
Cámara IP 2	Secundario	Cámaras de seguridad ubicadas en las instalaciones de la empresa.	Líder sistemas.	Líder sistemas.
Impresora 1	Secundario	Impresoras multifuncional con administración web. Puerto HTTP habilitado.	Líder sistemas.	Subge-rente.
Impresora 2	Secundario	Impresora Láser.	Líder sistemas.	Subge-rente.
Impresora 3	Secundario	Impresora multifuncional.	Líder sistemas.	Subge-rente.
Wink Hub	Secundario	Dispositivo IoT para control de luces y cámaras IP.	Líder sistemas.	Líder sistemas.

Fuente: Elaboración propia.

6.2.3 Identificación y categorización de las vulnerabilidades: Siguiendo con la fase 4 de la metodología PTES “Análisis de vulnerabilidades” esta sugiere realizar una prueba de vulnerabilidad con el fin de identificar fallas en los sistemas. En este punto, se hace uso de una prueba activa donde se utiliza la manera automática utilizando la herramienta Greenbone (openVAS) el cual nos arrojará el análisis de las vulnerabilidades de los hosts de la red. De acuerdo con los resultados, se realiza la identificación y posterior categorización de las vulnerabilidades en la red de la empresa.

En la figura 5 se visualiza el resumen del resultado del escaneo con la herramienta GreenBone donde la tarea de escaneo es llamada “Escaneo XX” encontrando 3 vulnerabilidades catalogadas como altas, 27 medianas y de esta manera alertándonos de las fallas de seguridad en la red local de Colombia Leds SAS.

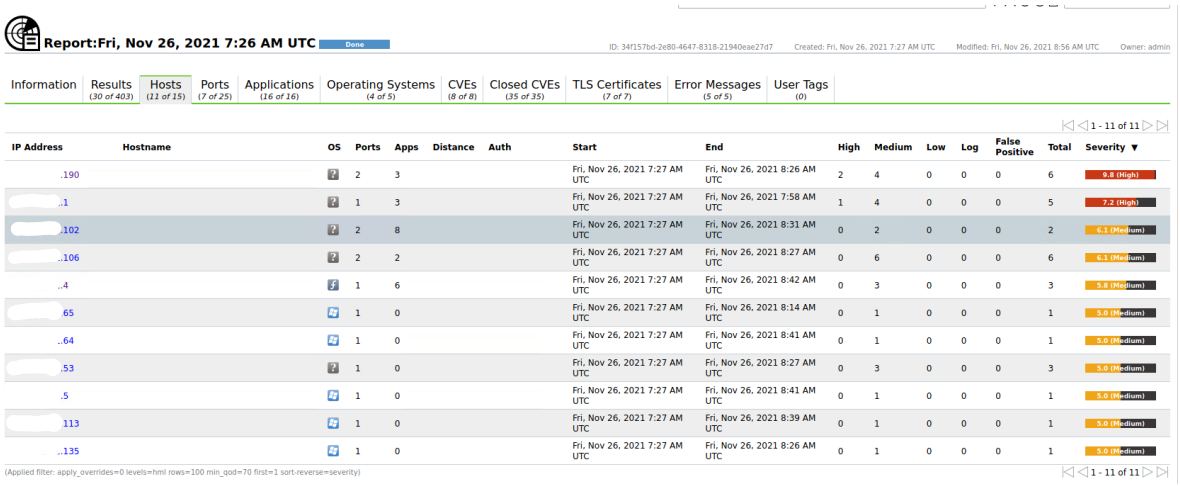
Figura 5. Reporte general de escaneo de vulnerabilidades.



Fuente: Elaboración propia.

Análisis de vulnerabilidades: La herramienta de escaneo de vulnerabilidades permite la posibilidad de ver por host las vulnerabilidades halladas, en el resultado como se puede apreciar en la figura 6 se encuentra que la dirección que corresponde a la cámara IP con 6 vulnerabilidades entre las cuales 2 son altas y el servidor de la DMZ con 5 vulnerabilidades entre las cuales 1 es alta.

Figura 6. Resultado de escaneo de vulnerabilidades por host.



Report:Fri, Nov 26, 2021 7:26 AM UTC — Done

ID: 34f157bd-2e80-4647-8318-21940eae27d7 Created: Fri, Nov 26, 2021 7:27 AM UTC Modified: Fri, Nov 26, 2021 8:56 AM UTC Owner: admin

Information | Results (30 of 403) | Hosts (11 of 15) | Ports (7 of 25) | Applications (16 of 16) | Operating Systems (4 of 5) | CVEs (8 of 8) | Closed CVEs (35 of 35) | TLS Certificates (7 of 7) | Error Messages (5 of 5) | User Tags (0)

1 - 11 of 11

IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive	Total	Severity ▼
.190			2	3			Fri, Nov 26, 2021 7:27 AM UTC	Fri, Nov 26, 2021 8:26 AM UTC	2	4	0	0	0	6	9.8 (High)
.1			1	3			Fri, Nov 26, 2021 7:27 AM UTC	Fri, Nov 26, 2021 7:58 AM UTC	1	4	0	0	0	5	7.2 (High)
.102			2	8			Fri, Nov 26, 2021 7:27 AM UTC	Fri, Nov 26, 2021 8:31 AM UTC	0	2	0	0	0	2	6.1 (Medium)
.106			2	2			Fri, Nov 26, 2021 7:27 AM UTC	Fri, Nov 26, 2021 8:27 AM UTC	0	6	0	0	0	6	6.1 (Medium)
.4			1	6			Fri, Nov 26, 2021 7:27 AM UTC	Fri, Nov 26, 2021 8:42 AM UTC	0	3	0	0	0	3	5.8 (Medium)
.65			1	0			Fri, Nov 26, 2021 7:27 AM UTC	Fri, Nov 26, 2021 8:14 AM UTC	0	1	0	0	0	1	5.0 (Medium)
.64			1	0			Fri, Nov 26, 2021 7:27 AM UTC	Fri, Nov 26, 2021 8:41 AM UTC	0	1	0	0	0	1	5.0 (Medium)
.53			1	0			Fri, Nov 26, 2021 7:27 AM UTC	Fri, Nov 26, 2021 8:27 AM UTC	0	3	0	0	0	3	5.0 (Medium)
.5			1	0			Fri, Nov 26, 2021 7:27 AM UTC	Fri, Nov 26, 2021 8:41 AM UTC	0	1	0	0	0	1	5.0 (Medium)
.113			1	0			Fri, Nov 26, 2021 7:27 AM UTC	Fri, Nov 26, 2021 8:39 AM UTC	0	1	0	0	0	1	5.0 (Medium)
.135			1	0			Fri, Nov 26, 2021 7:27 AM UTC	Fri, Nov 26, 2021 8:26 AM UTC	0	1	0	0	0	1	5.0 (Medium)

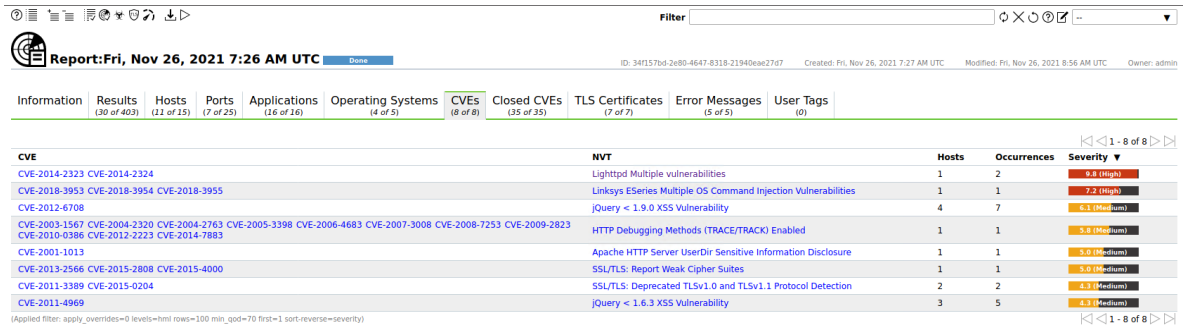
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 11 of 11

Fuente: Elaboración propia.

Ahora se hace uso del filtro por vulnerabilidades, encontrando que la vulnerabilidad de Lighthttpd Multiple vulnerabilities es la que más ocurrencias tiene con 2 como se ve en la figura 7 y 8.

Figura 7. Vulnerabilidades encontradas.



Filter

Report:Fri, Nov 26, 2021 7:26 AM UTC — Done

ID: 34f157bd-2e80-4647-8318-21940eae27d7 Created: Fri, Nov 26, 2021 7:27 AM UTC Modified: Fri, Nov 26, 2021 8:56 AM UTC Owner: admin

Information | Results (30 of 403) | Hosts (11 of 15) | Ports (7 of 25) | Applications (16 of 16) | Operating Systems (4 of 5) | CVEs (8 of 8) | Closed CVEs (35 of 35) | TLS Certificates (7 of 7) | Error Messages (5 of 5) | User Tags (0)

1 - 8 of 8

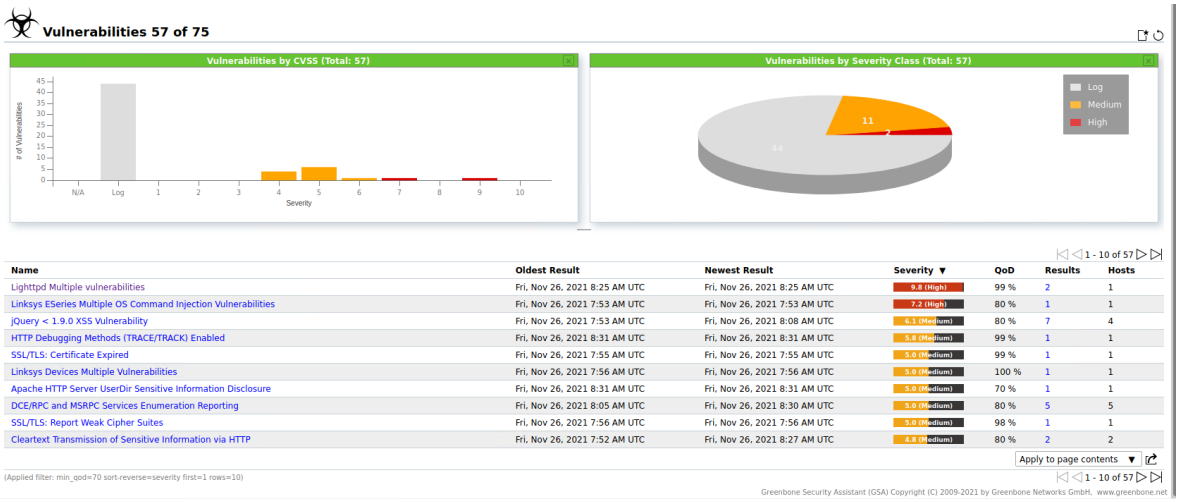
CVE	NVT	Hosts	Occurrences	Severity ▼
CVE-2014-2323 CVE-2014-2324	Lighttpd Multiple vulnerabilities	1	2	9.8 (High)
CVE-2018-3953 CVE-2018-3954 CVE-2018-3955	Linksys ESeries Multiple OS Command Injection Vulnerabilities	1	1	7.2 (High)
CVE-2012-6708	jQuery < 1.9.0 XSS Vulnerability	4	7	6.1 (Medium)
CVE-2003-1567 CVE-2004-2320 CVE-2004-2763 CVE-2005-3398 CVE-2006-4683 CVE-2007-3008 CVE-2008-7253 CVE-2009-2823 CVE-2010-0386 CVE-2012-2223 CVE-2014-7883	HTTP Debugging Methods (TRACE/TRACK) Enabled	1	1	5.8 (Medium)
CVE-2001-1013	Apache HTTP Server UserDir Sensitive Information Disclosure	1	1	5.0 (Medium)
CVE-2013-2566 CVE-2015-2808 CVE-2015-4000	SSL/TLS: Report Weak Cipher Suites	1	1	5.0 (Medium)
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	2	2	4.3 (Medium)
CVE-2011-4969	jQuery < 1.6.3 XSS Vulnerability	3	5	4.3 (Medium)

(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)

1 - 8 of 8

Fuente: Elaboración propia.

Figura 8. Reporte de vulnerabilidades encontradas.



Fuente: Elaboración propia.

6.2.4 Mapeo de vulnerabilidades comunes contra activos primarios y secundarios. Para esta actividad, basados en la información obtenida en el escaneo de vulnerabilidades se organizará la información para obtener una información clara que permita identificar con mayor claridad los objetivos más vulnerables en los cuales se puedan basar las pruebas de intrusión o pentest. Con la información recolectada se elabora el Cuadro 2 en el cual se puede identificar las vulnerabilidades y de esta manera organizar la información para facilitar el análisis.

Cuadro 2. Mapeo de Activos, Categorización y criticidad de vulnerabilidades.

Activo	Categorización	Vulnerabilidades	Criticidad	Referencia
Servidor	Primario	Ejecución remota de código para Samba versiones anteriores de 3.5.0, 4.6.4, 4.5.10 y 4.4.14.	Alto 9.8	CVE-2017-7494 CVE-2020-10745 CVE-2017-14746
Cámara IP 1	Secundario	Lighttpd Multiple vulnerabilities	Alta 9.8	CVE-2014-2323 CVE-2014-2324
Cámara IP 2	Secundario	lighttpd antes de 1.4.33 permite que atacantes remotos obtengan privilegios	Alto 7.6	CVE-2013-4559 CVE-2014-2323

Switch	Primario	Linksys ESeries Multiple OS Command Injection Vulnerabilities	Alto 7.2	CVE-2018-3953 CVE-2018-3954 CVE-2018-3955
Router inalámbrico	Primario	jQuery < 1.9.0 XSS Vulnerability	Medio 6.1	CVE-2012-6708
Impresora	Secundario	phpMyAdmin 2.6.4 and 2.6.4-pl1, permite ataques remotos.	Medio5.0	CVE-2005-3299
PC Virtual	Secundario	El servidor HTTP Apache 1.x y 2.x permite a atacantes remotos provocar una denegación de servicio.	Media 5.0	CVE-2007-6750
Router ISP	Primario	Ninguna detectada	N/A	N/A
Equipos PCs	Primario	Ninguna detectada	N/A	N/A
Wink Hub	Secundario	Ninguna detectada	N/A	N/A

Fuente: Elaboración propia.

6.2.5 Identificación de puntos vulnerables. De acuerdo con las vulnerabilidades encontradas, la categorización de los activos TI de la empresa y la criticidad de las vulnerabilidades halladas, las pruebas de intrusión se centrarán en aquellas en las cuales la criticidad sea alta y el activo sea primario, por tanto, el servidor y el switch serían los objetivos de esta prueba, quedando como posible alternativa una de las cámaras IP que a pesar de que es catalogada como un activo secundario, tiene un criticidad de vulnerabilidad alta, permitiéndole al intruso a través de este acceder a los demás recursos de la red y la posibilidad de escalar privilegios en los mismo, quedando comprometida la información y la seguridad del sistema.

Un vector de ataque es la ruta que se elige para aprovechar una vulnerabilidad en un sistema para realizar un ataque informático que permita ingreso al sistema para ejecutar algún tipo de malware para conseguir el objetivo propuesto [32] . Ya teniendo

[32] GRUPO ATICO 34. [Sitio web]. Madrid: ¿Qué son los vectores de ataque en ciberseguridad? Disponible en: https://protecciondatos-lopd.com/empresas/vectores-ataque-ciberseguridad/

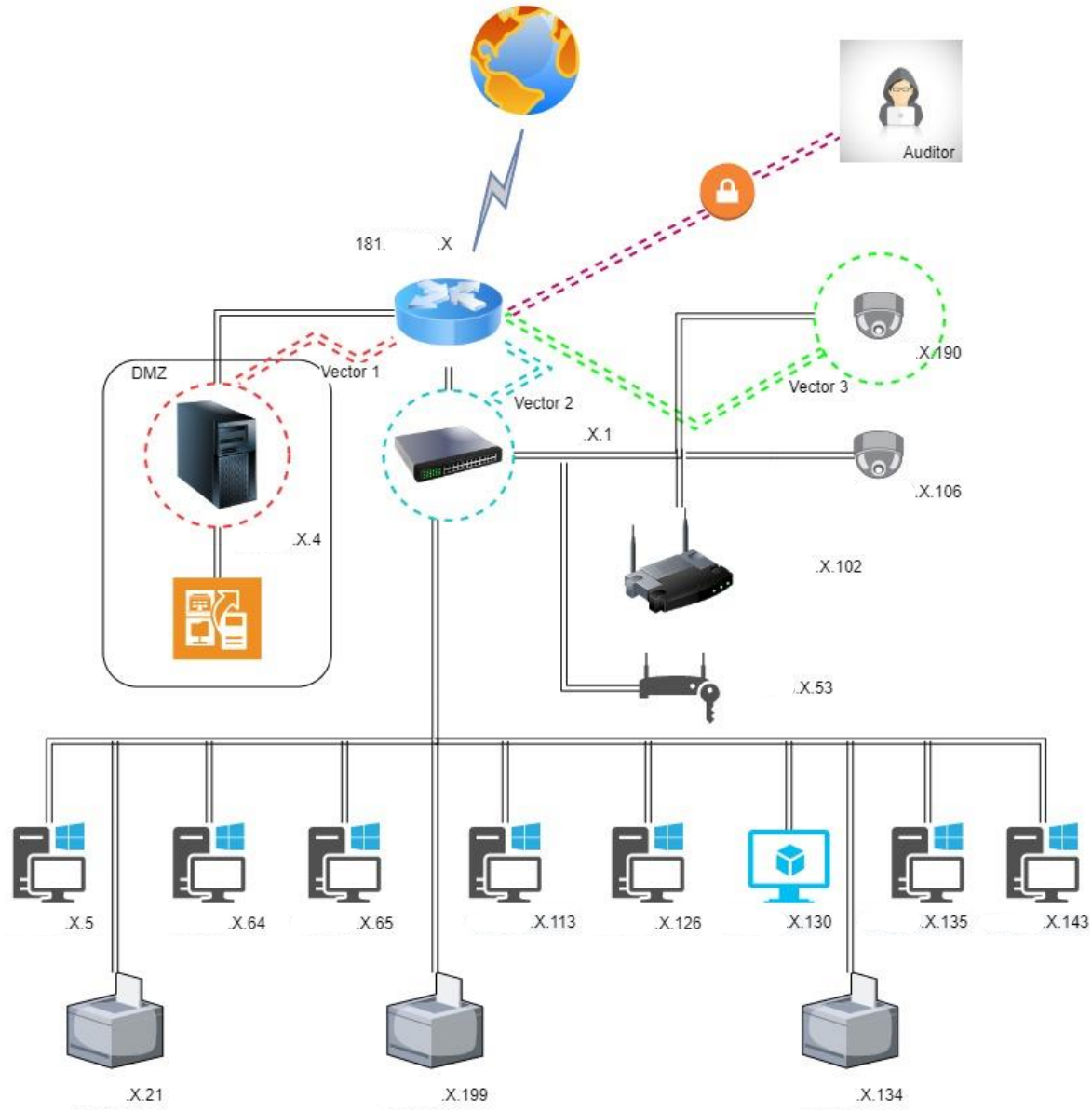
establecido los posibles objetivos del ataque, se establecen las rutas que se debe seguir para alcanzar el ingreso a estos objetivos.

Dentro de los vectores de ataque se encuentran dos tipos, el primero es el vector de ataque pasivo que cuyo objetivo es ganar acceso al sistema y el segundo es el vector de ataque activo que su objetivo es alterar el correcto funcionamiento del sistema [33].

En la Figura 9 se ve algunos de los vectores de ataque que se pueden realizar en la explotación de las vulnerabilidades encontradas. En primer corresponde al servidor que se encuentra en la DMZ y que para llegar a él es solamente conectarse al router del ISP, el segundo es el Switch capa 3 también conectado el router y por último la cámara IP que, para llegar a él, toca pasar por el rotuer y el switch.

[33] Ibid..

Figura 9. Diagrama de posibles vectores de ataque a puntos vulnerables.



Fuente: Elaboración propia.

Debido a su gran impacto que tiene el servidor dispuesto en la DMZ debido a que allí se centraliza todos los servicios necesarios para el funcionamiento de la infraestructura tecnológica de la empresa Colombia Leds SAS como lo es la página web de la intranet, el repositorio de documentación sensible e importante, el almacenamiento de la base de datos de la herramienta Siigo y que desde ahí se administran los servicios de red y el acceso desde internet y el hecho que se

encontró una vulnerabilidad crítica, se estableció como principal objetivo de la prueba de intrusión.

Teniendo en cuenta que ya se tiene acceso a la red para realizar la prueba de intrusión, se procede entonces a la explotación de las vulnerabilidades que se encuentran en servidor DMZ para ganar acceso al sistema y de esta manera tener control de toda la red y de la información que se encuentra en el repositorio, simulando de esta manera un posible ataque cibernético a la red de la empresa de estudio Colombia LEDS SAS, desarrollando de esta manera un vector de ataque pasivo.

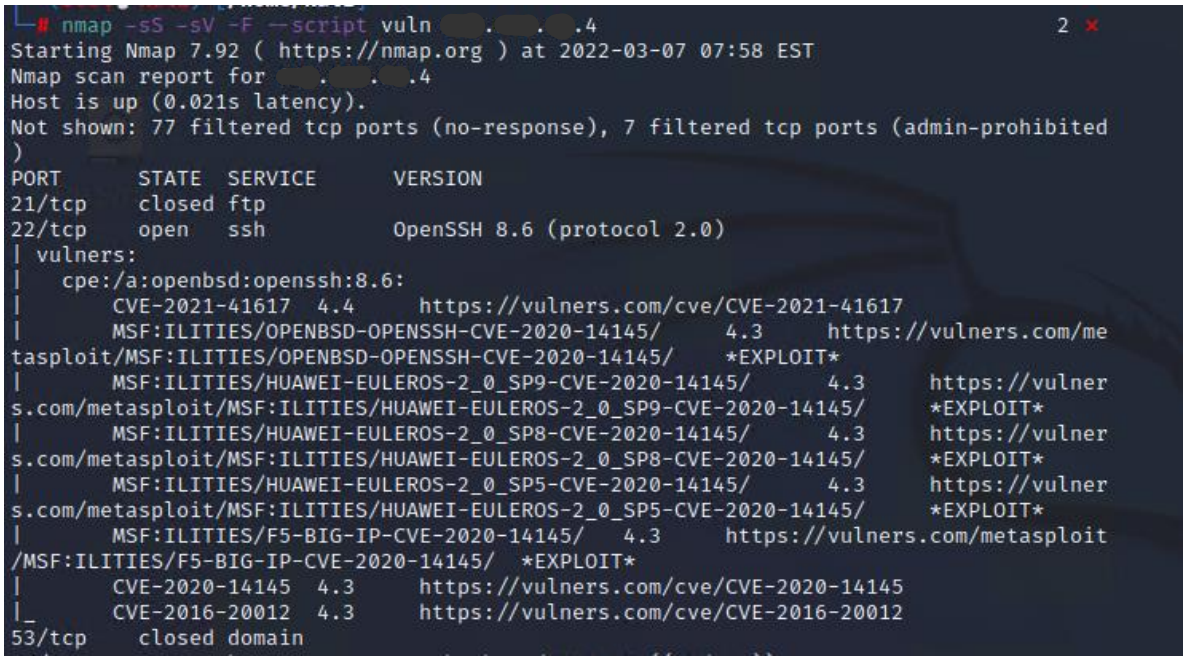
6.3 DEMOSTRAR LAS VULNERABILIDADES ASOCIADAS A LA INFRAESTRUCTURA TECNOLÓGICAS DE LA PYME COLOMBIA LEDS SAS, MEDIANTE LA APLICACIÓN DE LA METODOLOGÍA PTES CON EL FIN CONOCER LAS CONDICIONES DE CIBERSEGURIDAD.

Basados en las fases de la metodología PTES explotación y post-explotación que corresponden a las fases 5 y 6, se desarrollará este objetivo. Teniendo en cuenta que en la fase de explotación se busca tener acceso al sistema evitando restricciones de seguridad se explotará la vulnerabilidad hallada en el servidor DMZ y que corresponde al vector de ataque 1 (ver figura 9) ya que este es el activo con más valor.

6.3.1 Vulnerabilidades en servidor DMZ. De acuerdo con el análisis de vulnerabilidades realizado en el punto 6.2.3 “Identificación y categorización de vulnerabilidades” se halló que cuenta con una vulnerabilidad crítica. Haciendo uso de la herramienta “nmap” ejecutamos comando “nmap -sS -sV -F --script vuln X.X.X.4” para revisar de nuevo las vulnerabilidades en el servidor al cual se realiza la prueba de intrusión y con esto confirmar que esté disponible un exploit para aprovechar dicha vulnerabilidad. El resultado obtenido se ve en las figuras 10 a la 12.

Se encuentra vulnerabilidades en el puerto 22/tcp, 139/tcp y 445/tpc en donde estos dos últimos son los más críticos aprovechan una vulnerabilidad en la aplicación Samba 4.6.2 se identificó la vulnerabilidad CVE-2017-7494.

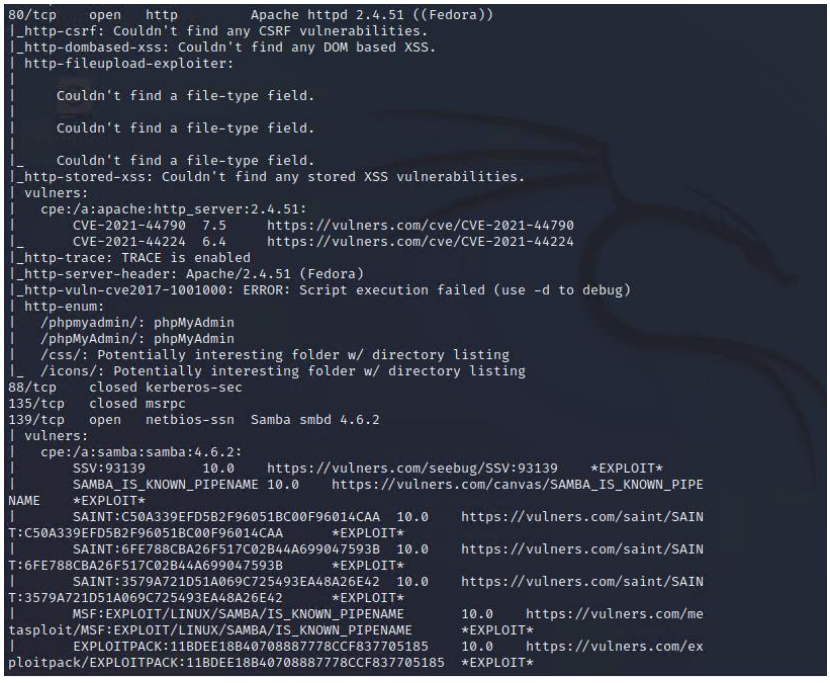
Figura 10. Revisión vulnerabilidades Servidor DMZ.



```
└─# nmap -sS -sV -F --script vuln [redacted].4                                2 ×
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-07 07:58 EST
Nmap scan report for [redacted].4
Host is up (0.021s latency).
Not shown: 77 filtered tcp ports (no-response), 7 filtered tcp ports (admin-prohibited
)
PORT      STATE  SERVICE      VERSION
21/tcp    closed ftp
22/tcp    open   ssh          OpenSSH 8.6 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:8.6:
|       CVE-2021-41617  4.4     https://vulners.com/cve/CVE-2021-41617
|       MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/     4.3     https://vulners.com/me
tasploit/MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/    *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/      4.3     https://vulner
s.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/     *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/      4.3     https://vulner
s.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/     *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/      4.3     https://vulner
s.com/metasploit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/     *EXPLOIT*
|       MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/   4.3     https://vulners.com/metasploit
/MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/  *EXPLOIT*
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|_      CVE-2016-20012  4.3     https://vulners.com/cve/CVE-2016-20012
53/tcp    closed domain
```

Fuente: Elaboración propia.

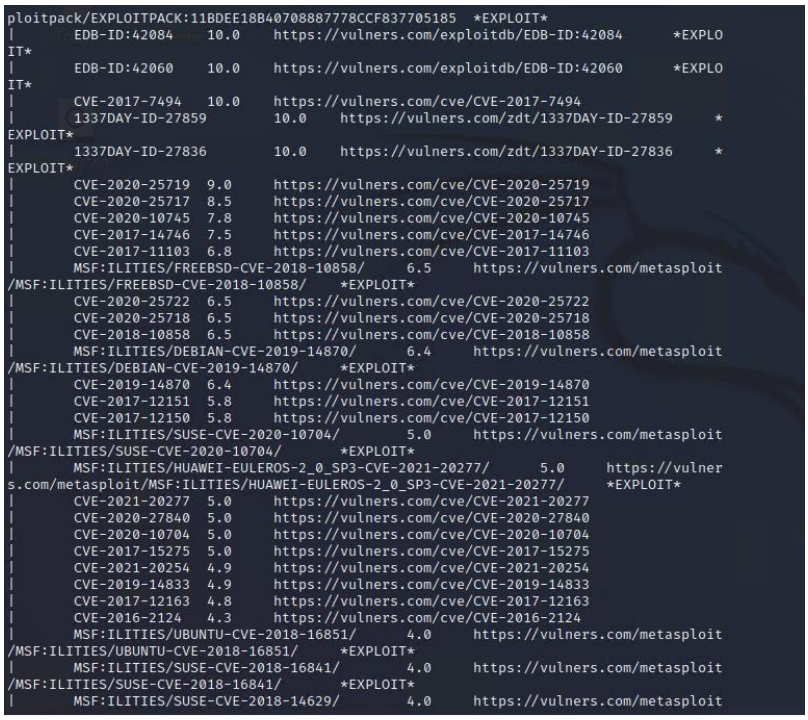
Figura 11. Resultados escaneo vulnerabilidades servidor DMZ.



```
80/tcp    open   http         Apache httpd 2.4.51 ((Fedora))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-fileupload-exploiter:
|
|     Couldn't find a file-type field.
|
|     Couldn't find a file-type field.
|
|_    Couldn't find a file-type field.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| vulners:
|   cpe:/a:apache:http_server:2.4.51:
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|_      CVE-2021-44224  6.4     https://vulners.com/cve/CVE-2021-44224
|_http-trace: TRACE is enabled
|_http-server-header: Apache/2.4.51 (Fedora)
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-enum:
|   /phpmyadmin/: phpMyAdmin
|   /phpMyAdmin/: phpMyAdmin
|   /css/: Potentially interesting folder w/ directory listing
|_  /icons/: Potentially interesting folder w/ directory listing
88/tcp    closed kerberos-sec
135/tcp   closed msrpc
139/tcp   open   netbios-ssn  Samba smbd 4.6.2
| vulners:
|   cpe:/a:samba:samba:4.6.2:
|       SSV:93139       10.0    https://vulners.com/seebug/SSV:93139    *EXPLOIT*
|       SAMBA_IS_KNOWN_PIPENAME 10.0    https://vulners.com/canvas/SAMBA_IS_KNOWN_PIPE
NAME    *EXPLOIT*
|       SAINT:C50A339EFD5B2F96051BC00F96014CAA  10.0    https://vulners.com/saint/SAIN
T:C50A339EFD5B2F96051BC00F96014CAA      *EXPLOIT*
|       SAINT:6FE788CBA26F517C02B44A6990475938  10.0    https://vulners.com/saint/SAIN
T:6FE788CBA26F517C02B44A6990475938      *EXPLOIT*
|       SAINT:3579A721D51A069C725493EA48A26E42  10.0    https://vulners.com/saint/SAIN
T:3579A721D51A069C725493EA48A26E42      *EXPLOIT*
|       MSF:EXPLOIT/LINUX/SAMBA/IS_KNOWN_PIPENAME       10.0    https://vulners.com/me
tasploit/MSF:EXPLOIT/LINUX/SAMBA/IS_KNOWN_PIPENAME      *EXPLOIT*
|       EXPLOITPACK:11BDEE18B4070888778CCF837705185     10.0    https://vulners.com/ex
ploitpack/EXPLOITPACK:11BDEE18B4070888778CCF837705185   *EXPLOIT*
```

Fuente: Elaboración propia.

Figura 12. Resultado escaneo servidor DMZ: CVE.



Fuente: Elaboración propia.

La vulnerabilidad más crítica es la CVE-2017-7494 (Figura 12) la cual presenta los siguientes detalles:

Descripción: Afecta a los sistemas con Samba con versiones 3.5.0 y anteriores y 4.6.4, 4.5.10 y 4.4.14 y anteriores [34]. Permite al atacante ejecutar código remoto cargándolo en un recurso compartido con permisos de lectura y escritura, luego el servidor ejecuta este código, dándole acceso al servidor con privilegios elevados.

Severidad: 9.8 Crítico. NVD (National Vulnerability Database).

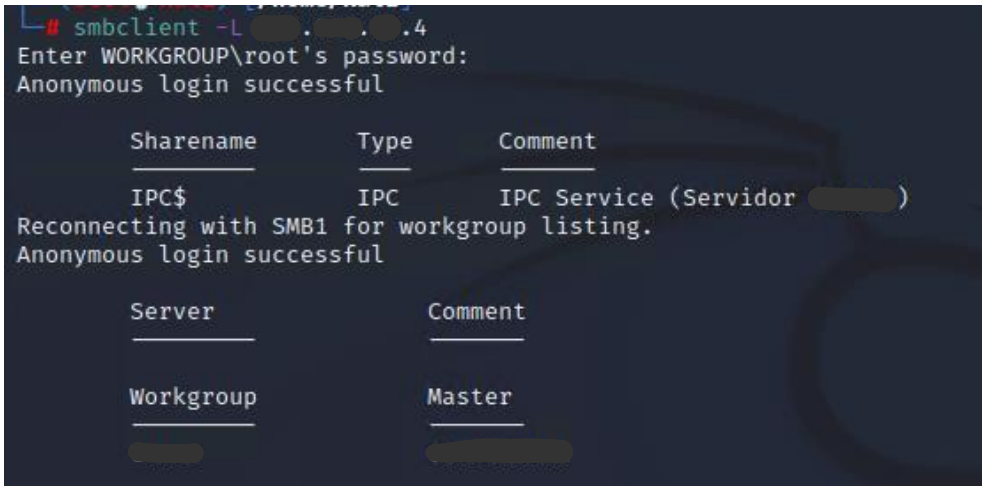
Exploit: is_know_pipename() [35].

[34] NATIONAL VULNERABILITY DATABASE. CVE-2017-7494 Detail. Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2017-7494

[35] EXPLOIT DATABASE BY OFFENSIVE SECURITY. Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipename()' Arbitrary Module Load (Metasploit). Disponible en: https://www.exploit-db.com/exploits/42084

6.3.2 Explotación de vulnerabilidad CVE-2017-7494 en servidor DMZ. Para la explotación de esta vulnerabilidad se debe tener acceso a una carpeta compartida en el servidor y que esta carpeta tenga permisos de lectura y escritura [36]. Haciendo uso de la herramienta del cliente de Samba, se ejecuta el comando "smbclient -L IP" listamos los recursos compartidos. El resultado en la Figura 13.

Figura 13. Revisión de carpetas compartidas en servidor DMZ.

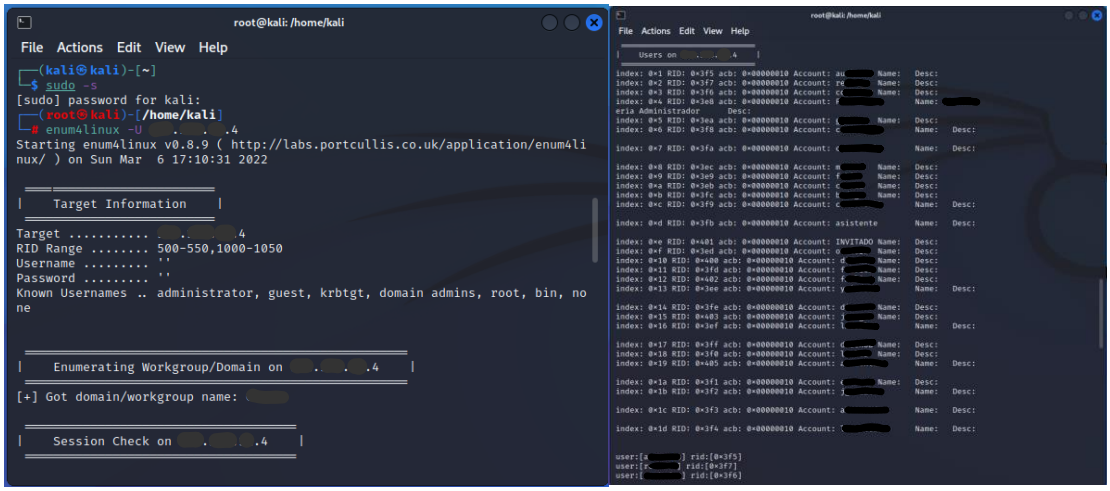


Fuente: Elaboración propia.

Con el usuario "Anonymous" no se encontró ninguna carpeta compartida, es decir que no hay recurso compartido, se hace entonces necesario revisar los usuarios registrados, para ello se puede utilizar la herramienta de escaneo enum4linux aplicando el comando "enum4linux -U IP". En la figura 14 se puede identificar los usuarios que tienen acceso a los recursos compartidos en el servidor.

[36] MILTON SECURITY. [Sitio web]. California: Milton Security Inc, EternalRed - CVE-2017-7494. Disponible en: https://www.miltonsecurity.com/company/blog/eternalred-cve-2017-7494

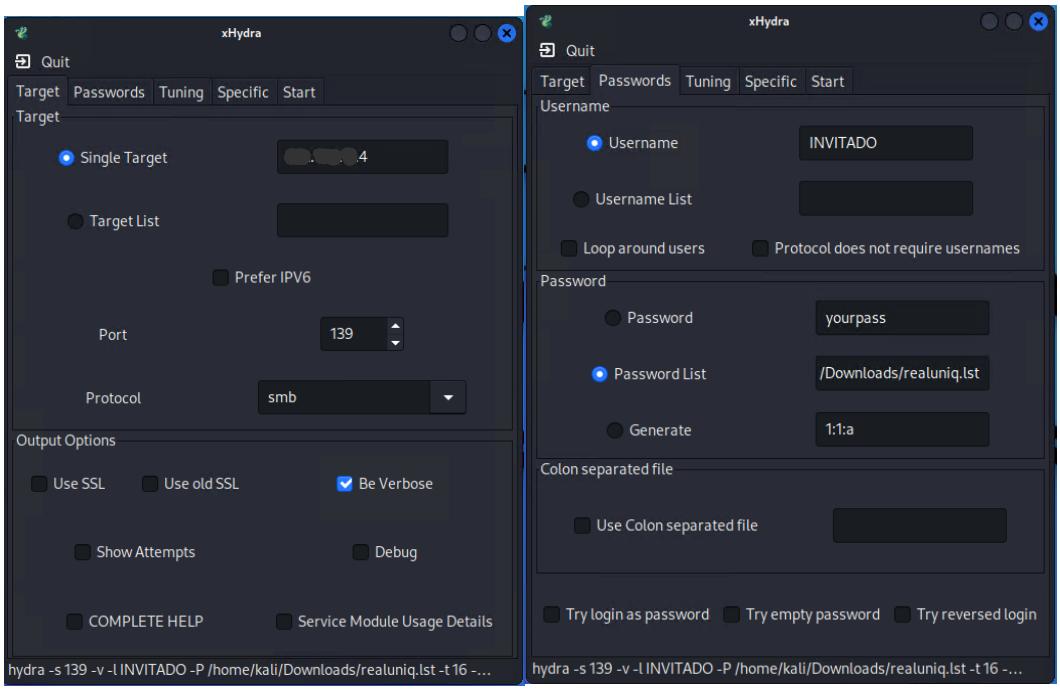
Figura 14. Revisión de usuarios con enum4linux.



Fuente: Elaboración propia.

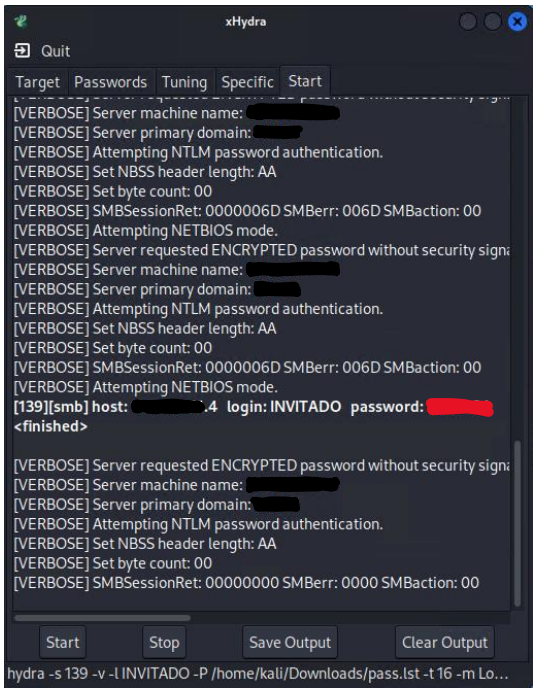
El escaneo (Figura 14) nos arroja que hay un usuario “INVITADO” el cual se puede tratar de encontrar la contraseña haciendo uso de fuerza bruta para ello utilizaremos la herramienta xHydra y con la ayuda de un diccionario de contraseñas configuraremos la herramienta como se puede ver en la Figura 15.

Figura 15. Utilización de xHydra para contraseña smb.



Fuente: Elaboración propia.

Figura 16. Resultado de extracción contraseña SMB.



Fuente: Elaboración propia.

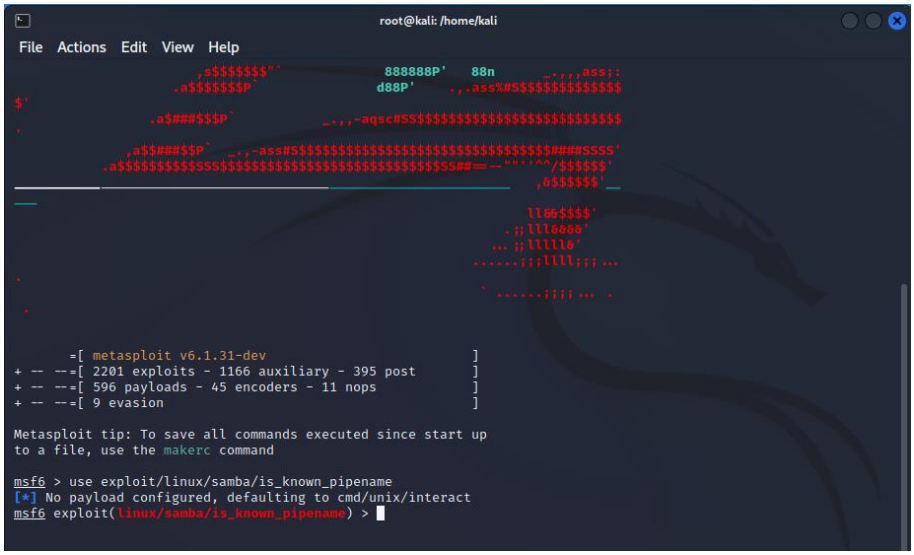
En la Figura 16 se ve el resultado el cual arroja la contraseña del usuario que se ha identificado. Con la obteniendo el usuario y la contraseña se procede a realizar la conexión por cliente de smb para revisar el nombre del recurso compartido como se muestra en la Figura 17.

Figura 17. Conexión a carpeta compartida.

Fuente: Elaboración propia.

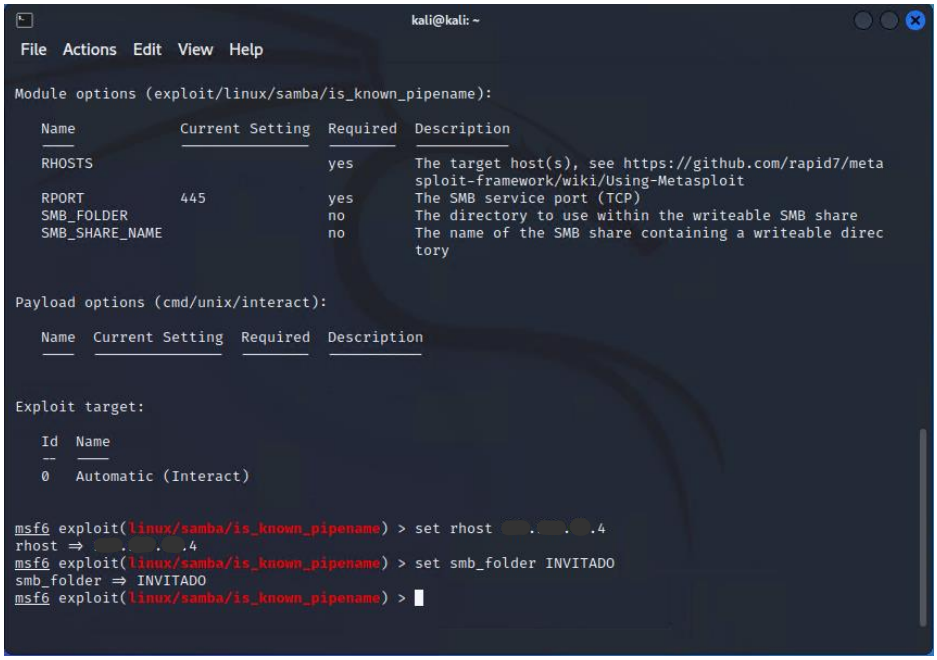
Ya temiendo todos los datos para poder explotar la vulnerabilidad, se procede a iniciar el FrameWork de MetaSploit y se selecciona el exploit (Figura 17) correspondiente. Luego se parametriza con los datos obtenidos (Figuras 19 y 20).

Figura 18. Inicio de metasploit.



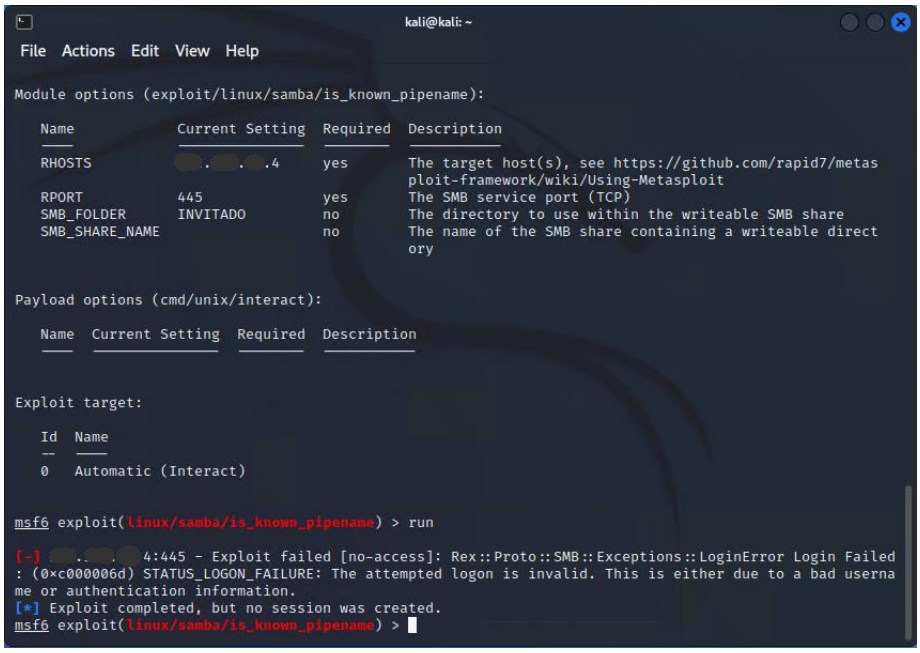
Fuente: Elaboración propia.

Figura 19. Configuración de exploit.



Fuente: Elaboración propia.

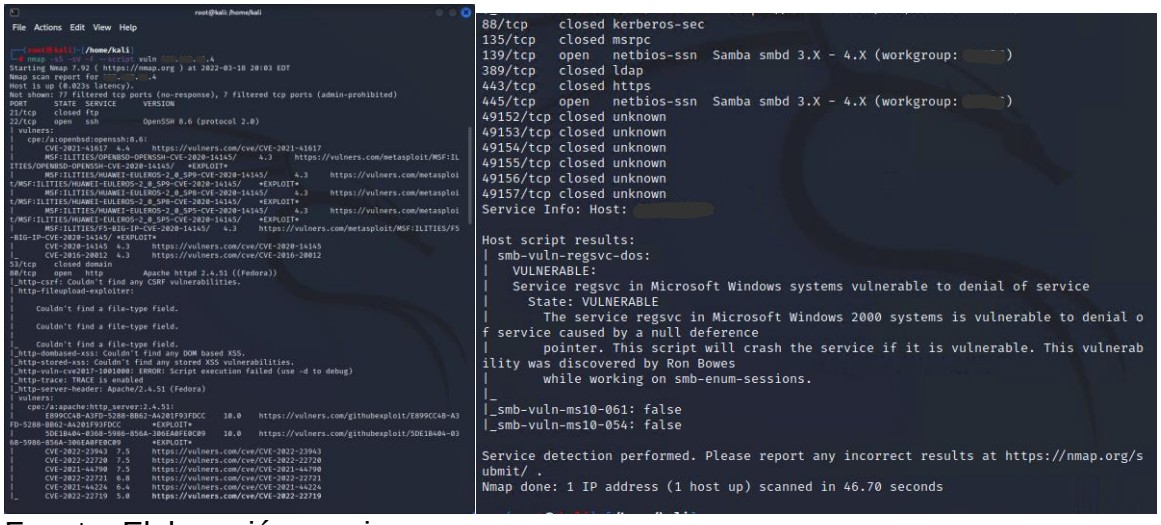
Figura 20. Ejecución de exploit CVE-2017-7494.



Fuente: Elaboración propia.

El exploit se ejecuta sin embargo no establece ninguna conexión porque no puede validar las credenciales. Se realiza una nueva validación de la vulnerabilidad en el equipo detectando que está ya no está disponible como se puede ver en la Figura 21.

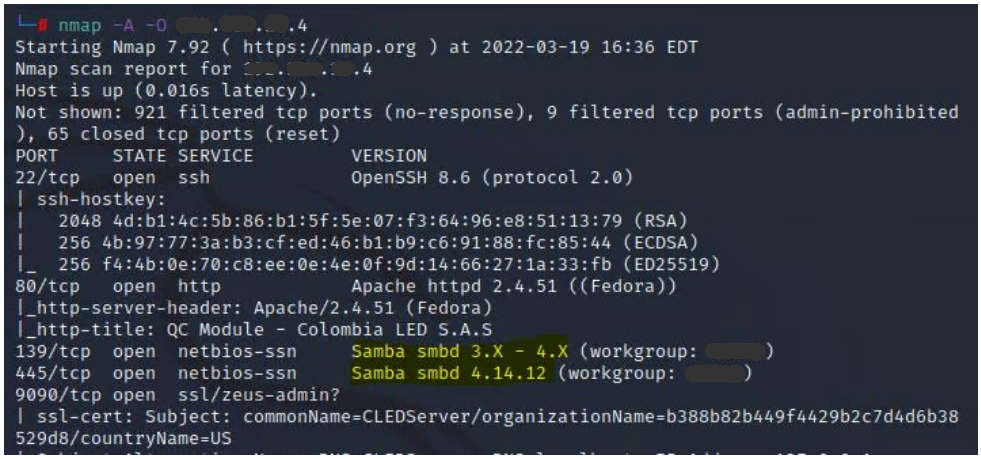
Figura 21. Resultado de nuevo escaneo de vulnerabilidades servidor DMZ.



Fuente: Elaboración propia.

Haciendo un escaneo de los puertos abierto, la versión del smb fue actualizada a la versión 4.14.12 (Figura 22) y por tanto ya la vulnerabilidad ha sido solventada quedando de esta manera mitigado el riesgo.

Figura 22. Revisión versión SMB en servidor DMZ.



Fuente: Elaboración propia.

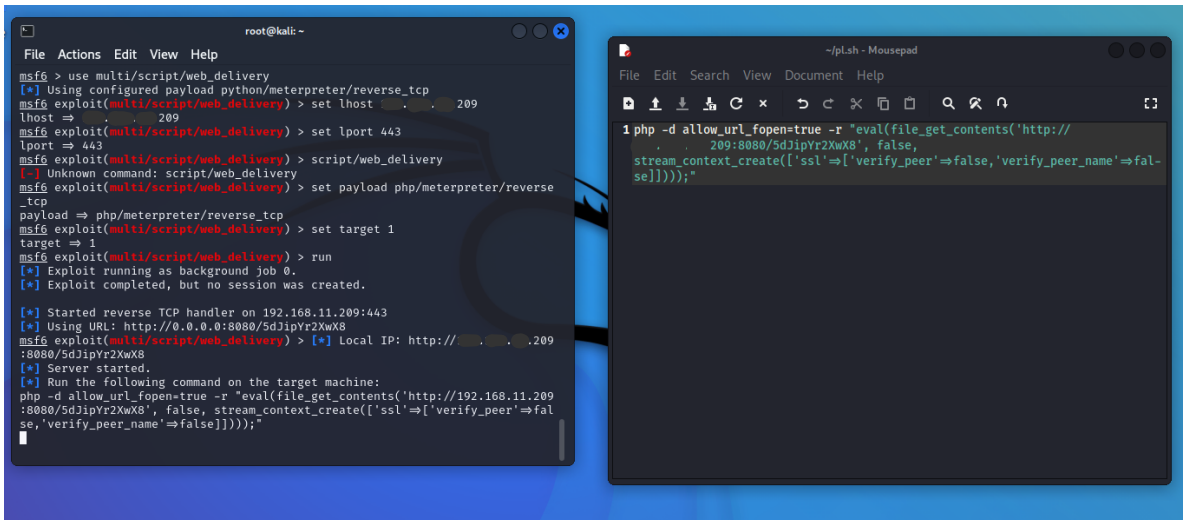
Concluida la actividad, se encontró que la vulnerabilidad más crítica que afectaba a la infraestructura tecnológica de la empresa Colombia Leds SAS que fue hallada en su servidor principal y que se categorizaba con el CVE-2017-7494, fue solventada con la actualización del Samba a la versión 4.14.12. Se realizó la consulta con el encargado del área de sistemas quien indicó que tiene como política realiza la actualización del servidor con una frecuencia de una vez por semana. Al no estar documentado esta política y tener limitada información sobre los sistemas de la empresa (con se plantea en un test de caja gris), no se tuvo presente al momento de establecer la explotación de la vulnerabilidad.

Aunque no se logró realizar la explotación exitosa de la vulnerabilidad, se pudo demostrar que esta estaba presente en el sistema. Adicionalmente, se encontró una vulnerabilidad con uno de los usuarios del servicio de Samba, que a través de un ataque de fuerza bruta se logró identificar su contraseña, quedando así demostrada la vulnerabilidad.

6.3.3 Prueba de concepto sobre vulnerabilidad en servidor DMZ. Para la fase 6 “Post-Explotación” de la metodología PTES su principal objetivo es validar el valor del recurso comprometido y mantener el acceso para que posteriormente se pueda ingresar de nuevo, se requiere haber explotado la vulnerabilidad encontrada, para ello se propuso al administrador de sistemas realizar esta prueba de concepto para validar el alcance que un intruso hubiera podido tener si la vulnerabilidad hubiera sido explotada exitosamente.

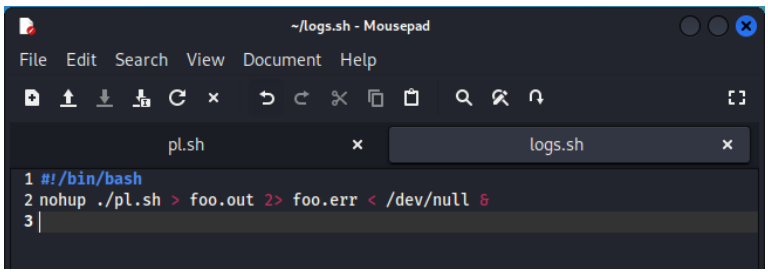
Haciendo uso de MSF (MetaSploit Framework) se genera un payload como se muestra en la figura 22 para para luego generar un archivo que se ejecutará en la máquina víctima (Figura 24).

Figura 23. Generación de payload con Metaesploit FrameWork.



Fuente: Elaboración propia.

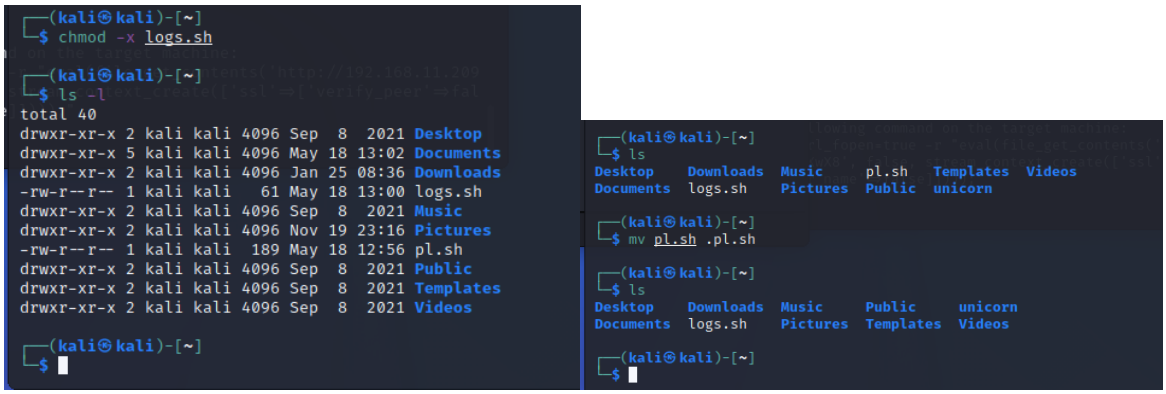
Figura 24. Creación de archivo con payload.



Fuente: Elaboración propia.

Ya teniendo el archivo creado, se cambian las propiedades del archivo para que sea oculto como se puede ver en la Figura 25.

Figura 25. Cambio de propiedades en archivo con payload.



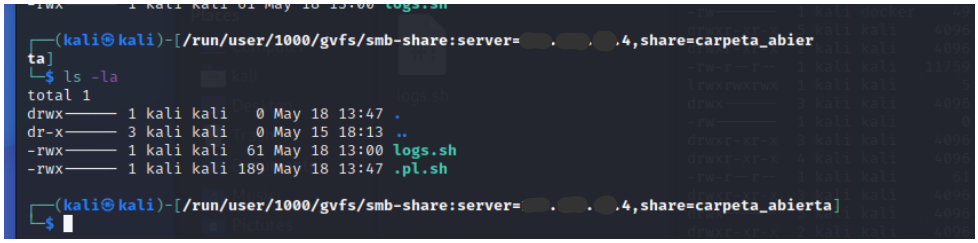
Fuente: Elaboración propia.

Ya teniendo el archivo, se copia al servidor Samba en la ruta compartida del servidor usando las credenciales que en el paso anterior habíamos encontrado, tal como se muestra en la Figura 26 y validamos que haya pasado bien (Figura 27).

Figura 26. Copia de archivos con payload.

Fuente: Elaboración propia.

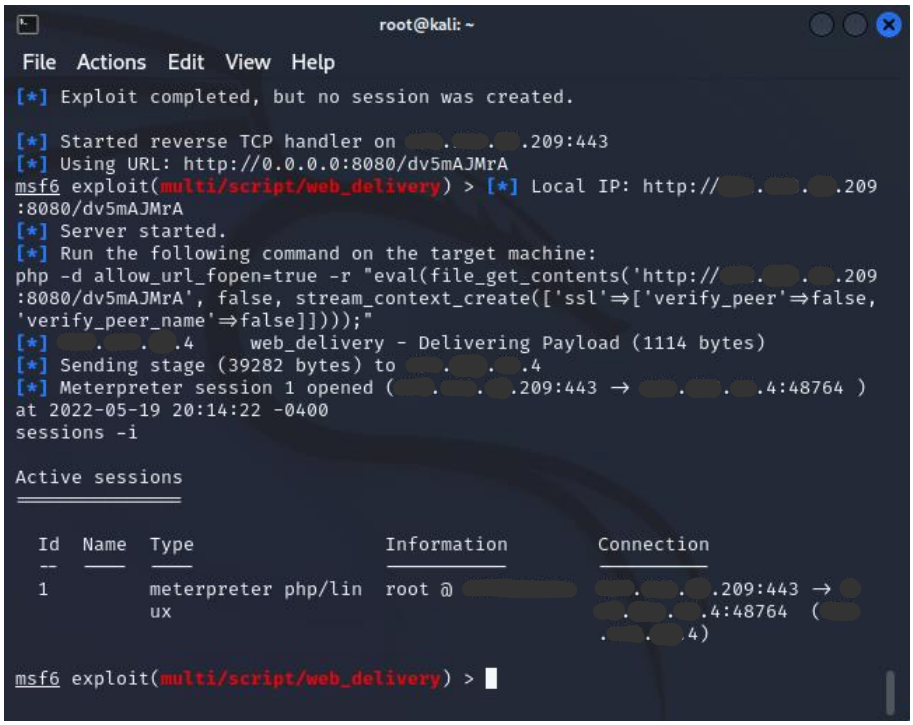
Figura 27. Revisión de archivos en carpeta destino.



Fuente: Elaboración propia.

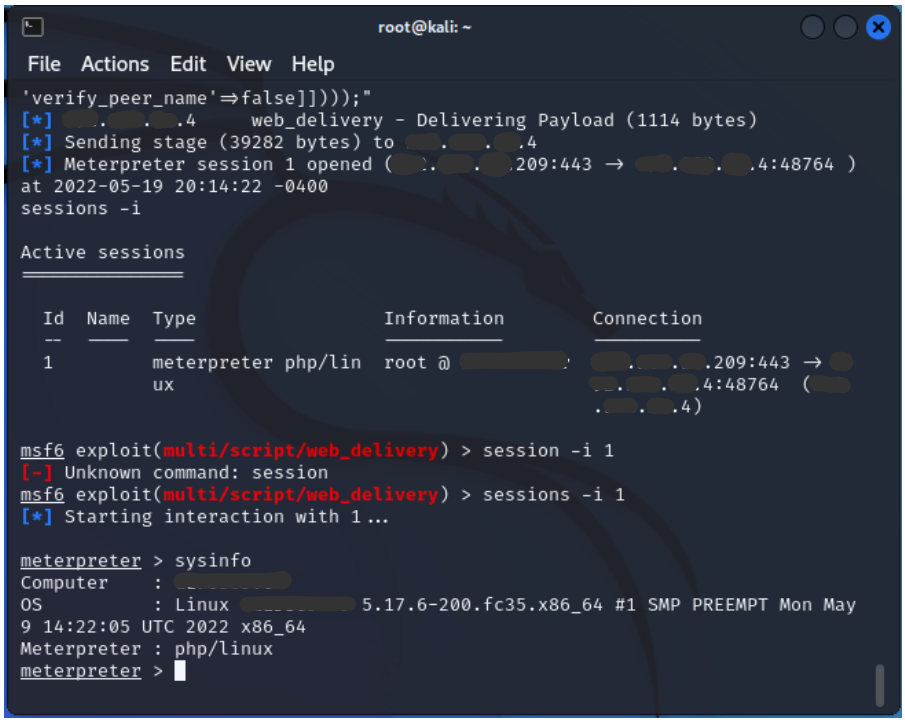
Ahora se abre el MSF y se carga el exploit esperando que en la máquina víctima se inicie el payload (Figura 28), cuando el archivo es abierto en la máquina destino el payload se carga abriéndose una sesión de meterpreter (Figura 29) en la cual iniciamos sesión remota.

Figura 28. Ejecución de payload.



Fuente: Elaboración propia.

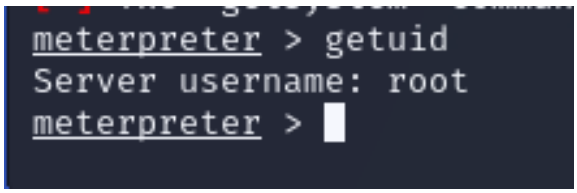
Figura 29. Inicio de sesión remota con Meterpreter.



Fuente: Elaboración propia.

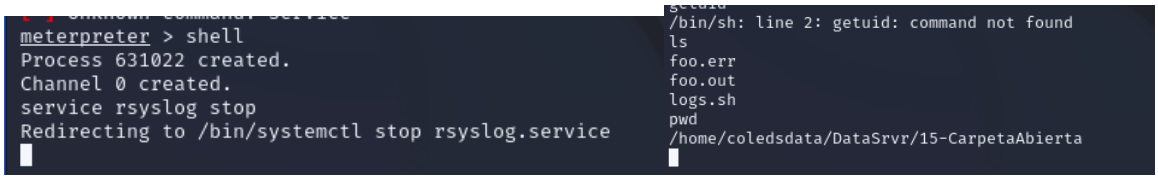
Una vez iniciada la sesión se revisa los privilegios que se tiene en la máquina (Figura 30) y con esto saber con qué acciones se puede contar. Como se ha iniciado sesión con usuario “root” por tanto se tiene el máximo de privilegios. Para evitar dejar rastro se de tienen los logs del sistema con el comando “service rsyslog stop” como se muestra en la Figura 31.

Figura 30. Revisión privilegios de usuario.



Fuente: Elaboración propia.

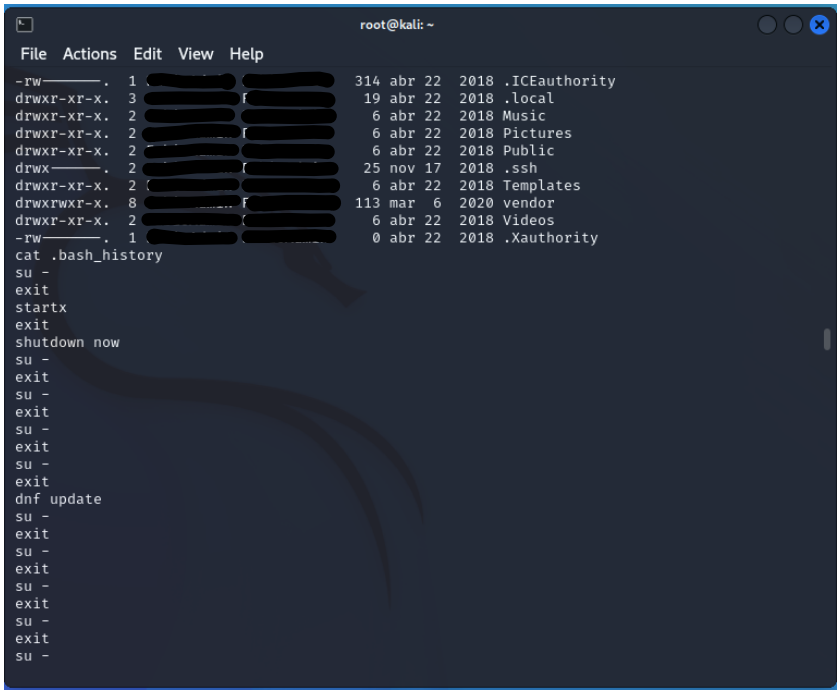
Figura 31. Detención de logs del sistema. Comando service rsyslog stop.



Fuente: Elaboración propia.

Terminado lo anterior, se puede validar el historial de los comandos ejecutados en la Shell del administrador con el archivo ".bash_history" (Figura 32) a ver si se encuentra algo interesante que ayude con la intrusión.

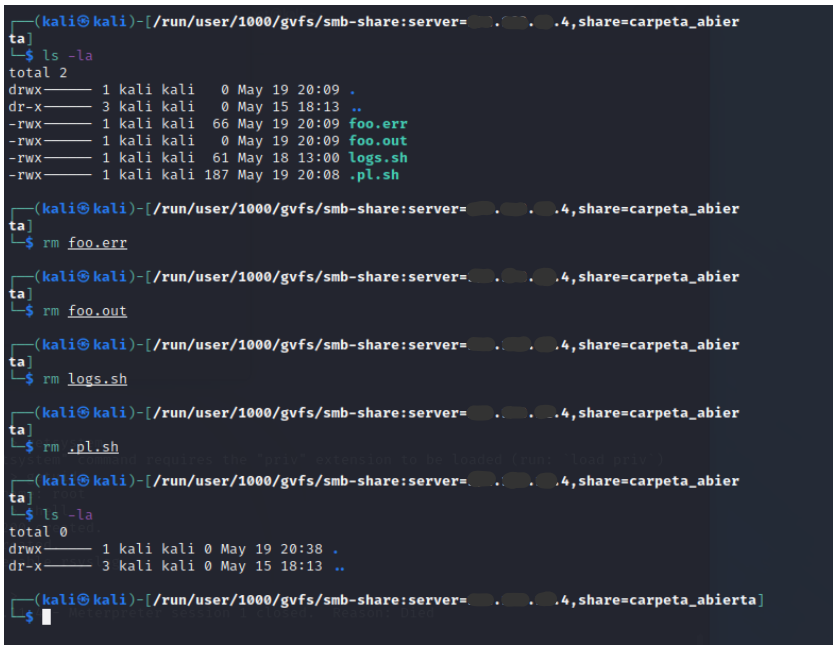
Figura 32. Revisión de historial de la shell.



Fuente: Elaboración propia.

Una vez terminado el ejercicio, se procede a eliminar los archivos generados al ejecutar el payload antes de salir del sistema como se ve en la Figura 33.

Figura 33. Eliminación de huellas.



Fuente: Elaboración propia.

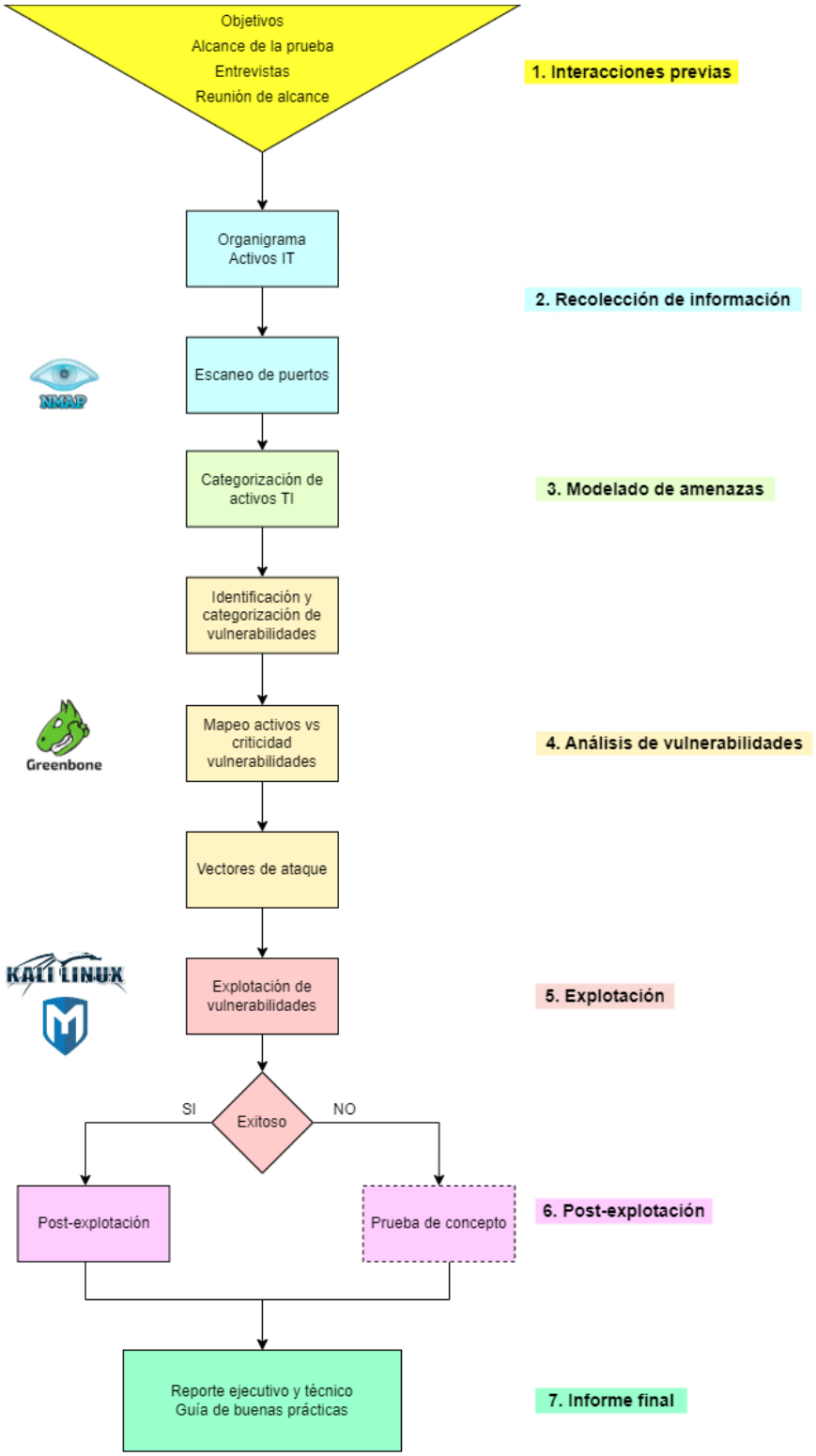
Con esto queda finalizado la prueba de concepto sobre el servidor DMZ en la cual se pude revisar el grado de vulnerabilidad que se llega a tener si se llegase a presentar un incidente de seguridad sobre este. Se logró escalar privilegios y llegar a ser administradores del sistema con lo cual se tuvo acceso a información sensible para la empresa consiguiendo de esta manera una post-explotación exitosa.

Se concluye entonces que una intervención temprana y oportuna por parte de los administradores en la actualización de los parches de seguridad en los sistemas operativos y las versiones de los programas evita en gran medida que se comprometan los sistemas.

La utilización de contraseñas débiles aumenta la posibilidad que los intrusos ganen acceso a la red y puedan vulnerar los sistemas. Se ha demostrado como una contraseña débil puede ser inicio de lograr el acceso e ir escalando en los privilegios que le permitan al intruso la instalación de puertas traseras para que le permita más adelante seguir contando con el acceso.

En la figura 34 se ve el resumen de la aplicación de la prueba de intrusión bajo la metodología PTES realizada en la empresa Colombia LEDS S.A.S donde se puede aprecias las siete fases de la metodología, las principales actividades realizadas en cada fase y las principales herramientas usadas durante la prueba de intrusión.

Figura 34. Resumen desarrollo prueba intrusión bajo PTES.



Fuente: Elaboración propia.

6.4 PROPONER RECOMENDACIONES A PARTIR DE LAS VULNERABILIDADES ENCONTRADAS MEDIANTE EL USO DE LINEAMIENTOS DE BUENAS PRÁCTICAS DE SEGURIDAD CON EL FIN DE SALVAGUARDAR LA INFORMACIÓN.

Las vulnerabilidades encontradas en los dispositivos de infraestructura tecnológica en la pyme Colombia Leds SAS se asocian con sistemas operativos y aplicaciones desactualizadas y contraseñas débiles donde los servicios SMB, HTTP, FTP y SSH son los más débiles y crean un punto para crear un vector de ataque contra la infraestructura de la empresa. De las vulnerabilidades halladas se hacen las siguientes recomendaciones enfocadas en tres aspectos: Procesos, personas y tecnología.

6.4.1 Recomendaciones orientadas a procesos: De acuerdo con la información recolectada en el punto 6.1.2 “Estructura T.I” se encontró que la empresa Colombia Leds SAS no cuenta con un sistema alterno para eventualidades que puedan surgir y que ponen en riesgo la continuidad del negocio como cortes de energía eléctrica, interrupción de servicio de internet, algún desastre natural o algún evento de orden público. Así como algún la posibilidad que los sistemas de la empresa queden inhabilitados por causas humanas. A este mecanismo se le conoce como “Plan de recuperación de desastres” o DRP (Disaster Recovery Plan) donde su principal objetivo es proporcionar los procedimientos detallados en caso de requerir recuperar la instalación, servicios o la capacidad de operar en un lugar alterno [37].

Contar con un DRP permite continuar con las actividades más importantes para la empresa mitigando o minimizando las pérdidas. Al iniciar el DRP es un proyecto que al concluirse hará parte de un Plan de Continuidad del Negocio (BCP por sus siglas en inglés). En la figura 35 se puede apreciar los pasos para poder realizar un DPR que permite además de continuar con el negocio y minimizar las pérdidas por inactividad, se minimiza el estrés generado por la toma de decisiones y asegura la información.

Figura 35. Pasos creación DRP.

Fuente: Elaboración propia.

[37] AREITIO BERTOLIN, Javier. Seguridad de la información Redes, informática y sistemas de información. p. 262.

Por otro lado, se detectó que la empresa Colombia Leds SAS no cuenta con política de manejo de la información en medios físicos como respaldo ante ataques de malware como podría ser ramsomware, así como la carencia de un inventario de los activos de la infraestructura tecnológica que le permitan definir su valor para el negocio. El inventario de activos informáticos es considerado el primer elemento que permite implementar un sistema de gestión de seguridad [38] con lo cual es vital su realización.

Recogiendo las consideraciones de tener un inventario de activos informáticos, un análisis de las amenazas y vulnerabilidades que nos permiten aumentar la ciberseguridad en la empresa, se hace necesario tener una política de ciberseguridad. Esto está planteado en lo que se denomina “Plan Director de Seguridad” PDS cuyo fin principal es reducir los riesgos a que se ve expuesta una organización a un nivel aceptables de seguridad de la información a partir de un análisis de situación actual [39].

En la figura 35 se ve las 6 etapas que componen este PDS donde se puede apreciar que es un plan cíclico que depende de la maduración de la empresa y el objetivo que se desea lograr de acuerdo con las necesidades del negocio.

[38] INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. Madrid: INCIBER-CERT, Inventario de activos y gestión de la seguridad en SCI. [Consultado el 17 de abril de 2023]. Disponible en: https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci
[39] INSTITUTO NACIONAL DE CIBERSEGURIDAD. Plan Director de Seguridad. p. 4.

Figura 36. Fases Plan Director de Seguridad.

Fuente: INSTITUTO NACIONAL DE CIBERSEGURIDAD. Plan Director de Seguridad. p. 5.

De acuerdo con lo anterior, se recomienda:

6.4.1.1 Política de seguridad de la información:

- Definir, diseñar e implementar una política de seguridad de la información como un Plan Director de Seguridad que permita alinear los activos informáticos a la estrategia de la empresa, desarrollando un inventario de los activos, un análisis de riesgos y vulnerabilidades.

- Desarrollar plan de recuperación en caso de desastres (DRP):

- Analizar posible sitio alterno de operación en caso de emergencia.
- Contar con contingencia en proveedor de internet.
- Contar con sistema de respaldo de energía eléctrica.
- Sistema de respaldo de la información a medios físicos con copia.
- Revisar al menos una vez al año el DRP.

Una vez realizado la implementación de estas recomendaciones, se espera mejoras notables en las condiciones de ciberseguridad a partir de una directriz promovida desde la alta gerencia de la empresa que permite evaluar las condiciones actuales de ciberseguridad y el nivel donde se desea llegar, dándole a la empresa una guía que le permite una mejora continua en las condiciones de ciberseguridad y con ello la continuidad del negocio haciendo frente a los constantes ataques cibernéticos que se ven expuestas las pymes en Colombia, la región y el mundo.

6.4.2 Recomendaciones orientadas a personas: Es sabido que el eslabón más débil en la cadena de ciberseguridad son las personas [40], por eso es de vital importancia que dentro de las recomendaciones que se planteen para mejorar la ciberseguridad en las empresas es hacer conciencia a las personas que hacen parte de ella sobre las conductas y hábitos cotidianos que pueden tener dentro y fuera de sus actividades laborales para crear un lugar más seguro para todos.

En una investigación realizada por el diario experto en tecnología ComputerWeekly.com y replicado por Kaspersky en su artículo “Concienciación sobre ciberseguridad: 7 maneras en las que sus empleados dejan a su empresa vulnerable a ciberataques” [41] atribuyen que el 84% de víctimas de ciberataques en parte es ocasionado por un error humano. Es aquí donde trabajar en el recurso humano junto con una política de seguridad impulsada desde la alta gerencia de las empresas se vuelve fundamental.

Las capacitaciones para las personas en temas de ciberseguridad se deben tocar temas como el manejo de correo electrónico ya que a través de este medio es uno de los más usados para realizar estafas y propagar virus según se indica Kaspersky el manejo de contraseñas, el control de acceso entre los temas más relevantes. Tal como se pudo evidenciar en el punto 6.3.1 “Vulnerabilidades en servidor DMZ” donde se encontró un mal manejo en un usuario con una contraseña débil y sin acceso limitado.

Por lo que se recomienda:

[40] TERÁN, David. Administración y seguridad en redes de computadoras. p. 222.
[41] KASPERSKY. [Sitio web]. Moscú: Concienciación sobre ciberseguridad: 7 maneras en las que sus empleados dejan a su empresa vulnerable a ciberataques. Disponible en: https://www.kaspersky.es/resource-center/preemptive-safety/7-ways-to-cyberattack-vulnerability

6.4.2.1 Campañas de concienciación y capacitación en ciberseguridad.

- Realizar periódicamente boletines de ciberseguridad con consejos prácticos al personal de la empresa y proveedores.
- Capacitar anualmente a los empleados en temas de ciberseguridad.
- Hacer campañas de concienciación de forma periódica.
- Realizar pruebas de ingeniería social utilizando medios como el correo electrónico para analizar el grado de concienciación de ciberseguridad.

Con la aplicación de esta recomendación se mitigará en gran medida la falta de conciencia en temas de ciberseguridad, los empleados y altos directivos de la empresa serán capaces de tomar medidas como la generación de contraseñas más robustas para el ingreso a los sistemas, el uso adecuado de los recursos tecnológicos de acuerdo a sus funciones y la importancia de estar prevenidos ante posibles ataques de ingeniería social por medio de medios de comunicación como correo electrónico, llamadas telefónicas y redes sociales.

6.4.3 Recomendaciones orientadas a tecnología: Después de realizada la prueba de intrusión donde se evidenciaron las vulnerabilidades que se encontraron en los dispositivos de la red interna de la empresa Colombia Leds SAS en el punto 6.2.3 "Identificación y categorización de las vulnerabilidades" donde se hallaron vulnerabilidades críticas que se deben mitigar con la actualización de los programas según las recomendaciones de cada fabricante. Adicionalmente a esto, se requiere también la actualización de parches de seguridad en los sistemas operativos de los equipos de usuario final y del servidor DMZ.

Dentro del análisis realizado a partir del mapeo de la red realizado en el punto 6.1.2.2 "Escaneo de red y puertos" se encontró que el servidor DMZ se encuentra expuesto a varias fallas de seguridad como el tener conexión a la red LAN de la empresa y ser accesible desde internet, por lo que se requiere el aseguramiento del servidor. Otros dispositivos como el switch y el NAS cuentan con fallas críticas que deben ser solucionadas con la actualización de software o con su remplazo ya que representan un punto que se puede utilizar para un vector de ataque por parte de un intruso.

Por otro lado, en cuanto a los equipos de usuario final, aunque no contaban con alguna vulnerabilidad conocida, si se hace necesario aplicar recomendaciones de buenas prácticas como sistema de protección frente amenazas [42] tanto en software como en hardware para evitar fuga de información e instalación de software malicioso. En cuanto a las cámaras IP, se evidenció en el análisis de vulnerabilidades la necesidad de actualizar su software. Es conveniente que la red para las cámaras esté aislada de la red principal de la empresa.

[42] ORTEGA CANDEL, José Manuel. Ciberseguridad: Manual práctico. [En línea]. p. 85.

Dentro del análisis realizado, no se encontró algún mecanismo para controlar y monitorear el acceso a internet y que nos ayude a tener una navegación en internet más segura, para evitar ejecución de código malicioso, interceptación y manipulación de las comunicaciones, la descarga de ficheros no confiables entre otros. Ya que los navegadores gestionan gran cantidad de información personal y de la empresa, este se convierte en un objetivo de los ciberdelincuentes según indica INCIBE en su blog “Navegación segura y privada para ti y tu empresa” [43].

Teniendo en cuenta los hallazgos que se evidenciaron en el análisis de vulnerabilidades, se recomienda realizar las siguientes actividades a la infraestructura tecnológica de la empresa Colombia Leds SAS:

6.4.3.1 Actualización de sistema operativo y aplicaciones: Se evidenció que la vulnerabilidad CVE-2017-7494 que hace referencia a una debilidad en el servicio de SMB en una versión antigua pone en riesgo crítico el equipo servidor ubicado en la DMZ al permitir al atacante puede acceder al sistema con privilegios altos haciendo posible un ataque de tipo ramsomware y la inyección de código malicioso en el servicio HTPP al contar con la vulnerabilidad CVE-2014-2323/2324 del servicio Lighttpd. Por tanto, se recomienda:

- Realizar la actualización de las aplicaciones desde los repositorios oficiales. La instalación desde sitios no oficiales implica un posible alto riesgo.
- Mantener los repositorios actualizados:
    - Para servidor GNU/Linux: “sudo dnf update”.
    - Para equipos Windows: Activar en “Windows Update” la búsqueda automática de actualizaciones.
- Utilizar las herramientas del fabricante del sistema operativo para realizar las actualizaciones.
    - Windows: Posibilidad de implementar el WSUS (Windows Server Update Services). Activar las actualizaciones automáticas en los equipos de usuario final con Windows.

[43] INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. Madrid: INCIBER-CERT, Navegación segura y privada para ti y tu empresa. Parte I. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/navegacion-segura-y-privada-ti-y-tu-empresa-parte-i

6.4.3.2 Aseguramiento de servidor DMZ.

- Actualización de parche de seguridad del servicio de Samba a la versión más reciente desde el repositorio oficial del sistema operativo del servidor [44].
- Aislar el servidor ubicado en la DMZ de la red LAN.
- Restringir el acceso al servidor desde la red de invitados.
- Se recomienda la implementación de un sistema IDS/IPS.
- Utilizar protocolo HTTPS en lugar de HTTP.

6.4.3.3 Dispositivo de almacenamiento de red NAS.

- Actualizar la versión de lighttpd de 1.4.20 a una versión igual o superior a la 1.4.35 [45].
- De ser posible cambiar el NAS por obsolescencia.
- Deshabilitar usuario Anonymous para visualizar las carpetas.

6.4.3.4 Aseguramiento Switch.

- Actualizar el firmware a la versión 2.0.10 [46].
- Segmentar la red de invitados, restringiendo el acceso a la red LAN.

6.4.3.5 Aseguramiento de equipos de usuario final.

Hardware:

- Asignación de clave de ingreso a BIOS/UEFI.
- Deshabilitar menú de boot.
- Bloquear puertos USB y unidades de CD/DVD.
- Implementar control de acceso físico al servidor.
- Colocar PIN para el uso de las impresoras.

Software:

---

[44] SAMBA ORG. [Sitio web]. USA: Samba Security Releases. Disponible en: https://www.samba.org/samba/history/security.html

[45] INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. Madrid: INCIBER-CERT, Vulnerabilidad en lighttpd (CVE-2014-2323). Disponible en: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-2323

[46] CISCO. [Sitio web]. USA: Talos Vulnerability Report: Linksys ESeries multiple OS command injection vulnerabilities. Disponible en: https://talosintelligence.com/vulnerability_reports/TALOS-2018-0625

- Política de escritorio limpio.
- Deshabilitar carpetas compartidas en equipos locales.
- Utilizar contraseñas fuertes: Combinación de letras, números y caracteres especiales. Se recomienda cambiarlas cada 30 días.
- Habilitar los archivos ocultos y extensiones de los archivos.
- Restringir privilegios de administrador.
- Contar con software original y licenciado.
- Desinstalar de los equipos software no necesario para las funciones del empleado.
- No tener en los equipos y en los recursos de red información personal.
- Implementar un sistema de categorización de la información: Documento interno, privado, restringido y público.
- Implementar política de contraseñas fuertes.

6.4.3.6 Seguridad de navegación.

- Mantener las actualizaciones automáticas en los navegadores de internet.
- Se debe controlar la navegación de internet a través de un servidor proxy.
- Limitar la navegación a los usuarios a páginas no relacionadas con sus funciones.
- Bloquear los puertos de conexión P2P.
- Bloquear la instalación de barras en el navegador de internet.

Al finalizar de implementar las recomendaciones dadas para aumentar la ciberseguridad en la infraestructura tecnológica de Colombia Leds SAS, se espera que todas las vulnerabilidades catalogadas como críticas y que se encuentran en los activos informáticos más relevantes para la empresa se eliminen (ver Cuadro 2. Mapeo de Activos, Categorización y criticidad de vulnerabilidades). Al eliminar estas vulnerabilidades el sistema queda protegido ante posibilidades de un ciberataque explotando un fallo en el sistema.

Con la aplicación de las recomendaciones para el aseguramiento del servidor DMZ proporciona mayores niveles de seguridad para los servicios que este presta a la red corporativa de la empresa, evitando que desde internet se pueda ingresar a la red interna.

Al asegurar los equipos de usuario final se disminuye el riesgo de ser un vector de ataque donde se pueda instalar software malicioso y se pueda propagar con mayor facilidad dentro de la red.

Figura 37. Guía de buenas prácticas de ciberseguridad.

Fuente: Elaboración propia.

En la figura 37 se ve un resumen de las recomendaciones dadas para aumentar la ciberseguridad en la empresa como una guía de buenas prácticas. Con estas recomendaciones dadas con base a los hallazgos encontrados durante la aplicación del test de intrusión PTES se logrará aumentar la ciberseguridad en la pyme Colombia Leds SAS y de esta manera salvaguardar la información de la empresa, clientes y proveedores. Dando así un mayor nivel de confianza a las partes interesadas y por ende aumentando el valor de la empresa.

7 CONCLUSIONES

Mediante el uso de las herramientas de recolección de información que sugiere la metodología PTES se seleccionó la información más relevante referente a la estructura organizacional e infraestructura tecnológica de la pyme Colombia LEDS SAS con lo cual se pudo establecer el punto de partida para la realización de la prueba de intrusión bajo la metodología PTES. Este paso es fundamental ya que es el punto de partida para poder realizar una prueba de intrusión exitosa que permita a la organización conocer las vulnerabilidades de ciberseguridad a las que se ve expuesta.

De acuerdo con el análisis realizado sobre el levantamiento de información sobre la infraestructura tecnológica de la pyme Colombia Leds SAS, se logró estructurar los posibles ataques sobre los puntos más vulnerables aplicando la metodología de hacking ético PTES. Con esto, el vector de ataque queda diseñado de tal manera que se puede seguir avanzando en la prueba de intrusión con el fin de poder explotar las vulnerabilidades encontradas.

Siguiendo el vector de ataque diseñado a partir del levantamiento de información, se demostró las vulnerabilidades asociadas a la infraestructura tecnológicas de la pyme Colombia LEDS SAS, mediante la aplicación de la metodología PTES con el fin conocer las condiciones de ciberseguridad aunque sin llegar a explotar con éxito la vulnerabilidad más crítica identificada porque fue mitigada (con la actualización del servicio vulnerable) antes de la realización de la prueba de intrusión ya que por el riesgo de ser explotada por un intruso era muy alto.

Por otro lado, se logró demostrar otras vulnerabilidades que con herramientas de identificación de vulnerabilidades como nmap y GreenBone (OpenVas) no se lograron detectar como lo son usuarios con contraseñas débiles en los recursos compartidos en el servidor de archivo al cual se le estaba haciendo la prueba de intrusión. Por tanto, en la realización de este tipo de pruebas es aconsejable la utilización de varias herramientas para ampliar el campo de aplicación del test.

Con los resultados obtenidos y siguiendo algunas recomendaciones de buenas prácticas en ciberseguridad aplicadas en los estándares y en la metodología PTES, se propuso recomendaciones a partir de las vulnerabilidades encontradas mediante el uso de lineamientos de buenas prácticas de seguridad con el fin de aumentar los niveles de ciberseguridad y de esta manera salvaguardar la información del negocio, clientes y proveedores.

Con el informe presentado a la gerencia de Colombia Leds SAS, se obtuvo una opinión muy positiva sobre la prueba de intrusión realizada ya que les permitió

conocer el estado real de la ciberseguridad de su infraestructura tecnológica y tomar correctivos a tiempo para mitigar los riesgos a los que estaban expuestos, por ejemplo, la vulnerabilidad de eternal blue (CVE-2017-7494) que se encontraba en su servidor principal. Por otro lado, solicitaron los servicios de quien realizó esta prueba para implementar las recomendaciones dadas en el informe final.

8 RECOMENDACIONES

- Se recomienda seguir realizando periódicamente la actualización de los parches de seguridad en el servidor principal de la empresa (servidor DMZ) al encargado del área de sistemas. Si bien la vulnerabilidad CVE-2017-7494 fue mitigada durante una actualización de software en el servidor, esta se encontraba desde hace bastante tiempo en el sistema.
- Se hace importante revisar las vulnerabilidades en el NAS actualizando la versión del Ligthhpd a la versión 1.4.35 o superior o realizar el remplazo por obsolescencia tecnológica. Esta solicitud se hace al encargado del área de sistemas de la empresa.
- Actualizar la versión del firmware del switch a la versión 2.0.10 o superior, cuya responsabilidad es el encargado del área de sistemas.
- La realización del inventario de los activos informáticos ayuda de gran manera en la administración y gestión de tecnología por tanto se sugiere a la gerencia de la pyme Colombia Leds SAS realizar un levantamiento de información de toda la infraestructura tecnológica de la empresa haciendo la documentación respectiva.
- Es importante realizar un análisis de riesgos de los activos para asignarles un valor dentro de las necesidades de la empresa. Esta importante labor debe estar respaldada por los accionistas y la alta gerencia de la empresa.
- Se recomienda a la gerencia de la empresa tener un plan de recuperación del negocio que pueda mitigar algunas vulnerabilidades como el hecho de contar con un único proveedor de internet y la ausencia de control de acceso a zonas restringidas.
- Se recomienda que desde el área de sistema la adopción de política de contraseñas, eliminación de permisos de administrador a usuarios finales.
- Se recomienda que la red inalámbrica de visitantes no tenga acceso a la red local y se maneje el control de contenidos.
- Se hace la recomendación al encargado del área de sistemas, de aislar el servidor que se encuentra en la DMZ de la red local.
- Se sugiere a la gerencia de la empresa el estudio de la implementación de un IDS/IPS para la red local y la configuración de un VLAN para el sistema de cámaras.

BIBLIOGRAFÍA

ANAYA MORENO, Javier Alexander. Impacto de las vulnerabilidades cibernéticas en la evaluación de la gestión del riesgo para las pymes. [En línea]. Proyecto de grado especialización en seguridad informática. Bogotá D.C: Universidad Nacional Abierta y a Distancia UNAD. Facultad de Ingeniería, 2021. [Consultado el 18 de septiembre de 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/41343/jaamayam.pdf?sequence=3&isAllowed=y

ALCALDÍA DE BOGOTÁ. Guardianes de la información: Penetration Testing. [En línea]. [Consultado el 18 de septiembre de 2021]. Disponible en: https://tic.bogota.gov.co/sites/default/files/seguridad-de-la-informacion/ambito2.pdf

ARBOLEDAS BRIHUEGA, David. BackTrack 5: Hacking de redes inalámbricas. [En línea]. Editorial RA-MA. Madrid, 2014. [Consultado el 1 de septiembre de 2021]. Disponible en: https://books.google.com.co/books?id=mo2fDwAAQBAJ&printsec=frontcover&dq=aircrack+espa%C3%B1ol&hl=es&sa=X&redir_esc=y#v=onepage&q&f=false

ARCHLINUX. [Sitio web]. Berlín: Levente Polyak & team, OpenVAS (español). [Consultado el 28 de octubre de 2021]. Disponible en: https://wiki.archlinux.org/title/OpenVAS_(Espa%C3%B1ol)

AREITIO BERTOLIN, Javier. Seguridad de la información Redes, informática y sistemas de información. [En línea]. Editorial Ediciones Parainfo S.A. Madrid, 2008. [Consultado el 17 de abril de 2023]. Disponible en: https://www.google.com.co/books/edition/Seguridad_de_la_informaci%C3%B3n_Redes_infor/_z2GcBD3deYC?hl=es-419&gbpv=1&pg=PA254&printsec=frontcover

BOISSON MORALES, Natalia. Aplicación de la metodología PTES en la clínica Medellín para la identificación de vulnerabilidades en historia clínica electrónica. [En línea]. Proyecto de grado especialización en seguridad informática. Medellín: Universidad Nacional Abierta y a Distancia UNAD. Facultad de Ingeniería, 2020. [Consultado el 18 de septiembre de 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/40837/nboissonm--.pdf?sequence=3&isAllowed=y

BLOGSPOT. Metodología PTES (Penetration Testing Execution Standard). [Consultado el 18 de septiembre de 2021]. Disponible en http://blogdeauditoriadeseguridad.blogspot.com/2017/09/metodologia-ptes-penetration-testing.html

CADAVID ROMERO, DIEGO FERNANDO. Hallazgos de vulnerabilidades en los sistemas operativos y base de datos de la empresa Aldim Acciones Logísticas En Distribución De Mercancías S.A.S. [En línea]. Proyecto de grado especialización en seguridad informática. Guadalajara de Buga: Universidad Nacional Abierta y a Distancia UNAD. Facultad de Ingeniería, 2018. [Consultado el 18 de septiembre de 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/17412/94477303.pdf?sequence=1&isAllowed=y

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias del cibercrimen en Colombia 2019-2020. [En línea]. [Consultado el 18 de septiembre de 2021]. Disponible en: https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

CASTRO, Carlos. Pruebas de Penetración e Intrusión. [En línea]. Bogotá D.C: Universidad Piloto de Colombia. Facultad de Ingeniería, 2018. [Consultado el 18 de septiembre de 2021]. Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6273/00005218.pdf?sequence=1&isAllowed=y

CISCO. [Sitio web]. USA: Talos Vulnerability Report: Linksys ESeries multiple OS command injection vulnerabilities. [Consultado el 18 de septiembre de 2021]. Disponible en: https://talosintelligence.com/vulnerability_reports/TALOS-2018-0625

CYBERSECURITY EDUCATION GUIDES. [Sitio web]. USA: What Is The PTES (Penetration Testing Execution Standard)? [Consultado el 12 de septiembre de 2022]. Disponible en: https://www.cybersecurityeducationguides.org/what-is-the-ptes-penetration-testing-execution-standard/

CYBERSECURE. FORTINET informa vulnerabilidades detectadas en sus productos. [Consultado el 18 de septiembre de 2021]. Disponible en https://portal.cci- entel.cl/Threat_Intelligence/Boletines/361/

COLOBRAN HUGUET, Miguel; ARQUÉS SOLDEVILLA, José María y GALINDO, Eduardo Marco. Administración de sistemas operativos en red. [En línea]. Editorial UOC. Barcelona, 2008. [Consultado el 1 de septiembre de 2021]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/56468?page=214

COMMON VULNERABILITIES AND EXPOSURES. [Sitio web]. McLean: CVE-MITRE. [Consultado el 10 de septiembre de 2021]. Disponible en: https://cve.mitre.org/index.html

CONGRESO DE COLOMBIA. [Sitio web]. Bogotá D.C.: CONGRESO DE LA REPÚBLICA, Ley 1273 de 2009. [Consultado el 18 de septiembre de 2021]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

EXPLOIT DATABASE BY OFFENSIVE SECURITY. Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipename()' Arbitrary Module Load (Metasploit). [En línea]. [Consultado el 7 de marzo de 2022]. Disponible en: https://www.exploit-db.com/exploits/42084

FUENTE MAESTRO, Antonio. Elaboración de una metodología de test de intrusión dentro de la auditoria de seguridad. [En línea]. Trabajo fin de master en seguridad informática. Universidad Internacional de La Rioja, 2014. [Consultado el 10 de septiembre de 2021]. Disponible en: https://reunir.unir.net/bitstream/handle/123456789/2331/AntonioFuertesMaestroTFM.pdf?sequence=3&isAllowed=y

FLOREZ MARTÍNEZ, José Luis y RENTERÍA MOSQUERA, José Mario. Conocer el valor de la información (activo económico) para valorar la necesidad de la ciberseguridad. [En línea]. Trabajo de grado para ingeniero de sistemas. Medellín: Tecnológico de Antioquia. Facultad de Ingeniería, 2020. [Consultado el 18 de septiembre de 2021]. https://dspace.tdea.edu.co/handle/tdea/1395

FRANCO, David A; PEREA, Jorge y PUELLO, Plinio. Metodología para la Detección de Vulnerabilidades en Redes de Datos. [En línea]. Cartagena: Universidad de Cartagena. Facultad de Ingeniería, 2012. [Consultado el 18 de septiembre de 2021]. Disponible en: https://scielo.conicyt.cl/scielo.php?pid=S0718-07642012000300014&script=sci_arttext

FUNCIÓN PÚBLICA GOBIERNO DE COLOMBIA. [Sitio web]. Bogotá D.C: Ley Estatutaria 1581 De 2012. [Consultado el 12 de septiembre de 2022]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

GESTIOPOLIS. [Sitio web]. Bogotá D.C.: Teoría de la organización y estructuras organizacionales. [Consultado el 9 de noviembre de 2022]. Disponible en: https://www.gestiopolis.com/teoria-organizacion-estructuras-organizacionales/

GREENBONE. [Sitio web]. Osnabrück: Greenbone Networks GmbH, OpenVAS – Open Vulnerability Assessment Scanner. [Consultado el 28 de octubre de 2021]. Disponible en: https://www.openvas.org/

GONZALEZ DÍAS, David Alejando y PULIDO SAINEA, Saúl Sebastián. La ciberseguridad política clave dentro de las organizaciones. [En línea]. Trabajo de grado especialización en Auditoría y Aseguramiento de la información. Tunja: Universidad Santo Tomás. Facultad de Ingeniería, 2021. [Consultado el 10 de octubre de 2021]. Disponible en: https://repository.usta.edu.co/handle/11634/37635

GONZALEZ LÓPEZ, Juan Camilo y RAMÍREZ MESA, Cristian. Guía de Controles y Buenas Prácticas de Ciberseguridad para MiPymes. [En línea]. Medellín: Tecnológico de Antioquia. Facultad de Ingeniería, 2020. [Consultado el 18 de septiembre de 2021]. https://dspace.tdea.edu.co/bitstream/handle/tdea/1394/Informe%20Controles.pdf?sequence=1&isAllowed=y

GRUPO ATICO 34. [Sitio web]. Madrid: ¿Qué son los vectores de ataque en ciberseguridad? [Consultado el 9 de diciembre de 2022]. Disponible en: https://protecciondatos-lopd.com/empresas/vectores-ataque-ciberseguridad

HERNÁNDEZ MARÍN, Yesid. Análisis y diseño de un mecanismo de cifrado de correo electrónico para garantizar y proteger la información enviada de las pymes. [En línea]. Proyecto de grado especialización en seguridad informática. Bogotá D.C: Universidad Nacional Abierta y a Distancia UNAD. Facultad de Ingeniería, 2020. [Consultado el 18 de septiembre de 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/36604/yhernandezmar.pdf?sequence=1&isAllowed=y

HMONG.ES. [Sitio web]. Madrid: HMONG.ES, Prueba de penetración. [Consultado el 1 de diciembre de 2021]. Disponible en: https://hmong.es/wiki/Penetration_test

INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. Madrid: INCIBER-CERT, vulnerabilidades. [Consultado el 10 de septiembre de 2021]. Disponible en: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades

INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. Madrid: INCIBER-CERT, Inventario de activos y gestión de la seguridad en SCI. [Consultado el 17 de abril de 2023]. Disponible en: https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci

INSTITUTO NACIONAL DE CIBERSEGURIDAD. Plan Director de Seguridad. [En línea]. Madrid: INCIBER-CERT. [Consultado el 17 de abril de 2023]. Disponible en: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. Madrid: INCIBER-CERT, Vulnerabilidad en lighttpd (CVE-2014-2323). [Consultado el 17 de abril de 2023]. Disponible en: https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2014-2323

INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. Madrid: INCIBER-CERT, Buenas prácticas para navegar seguros por la red. [Consultado el 17 de abril de 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/buenas-practicas-navegar-seguros-red

INSTITUTO NACIONAL DE CIBERSEGURIDAD. [Sitio web]. Madrid: INCIBER-CERT, Navegación segura y privada para ti y tu empresa. Parte I. [Consultado el 17 de abril de 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/navegacion-segura-y-privada-ti-y-tu-empresa-parte-i

KASPERSKY. [Sitio web]. Moscú: Concienciación sobre ciberseguridad: 7 maneras en las que sus empleados dejan a su empresa vulnerable a ciberataques. [Consultado el 17 de abril de 2023]. Disponible en: https://www.kaspersky.es/resource-center/preemptive-safety/7-ways-to-cyberattack-vulnerability

LAGOS FLORES, Eduardo. Análisis de vulnerabilidades y pruebas de penetración a la infraestructura
tecnológica de empresas. [En línea]. Proyecto de grado para obtener el título de ingeniero en computación. México: Universidad Nacional Autónoma de México. Facultad de Ingeniería, 2018. [Consultado el 18 de septiembre de 2021]. Disponible en:
http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/15381/%20Informe.pdf?sequence=1

LOPEZ PARRA, Miguel Ángel. Diseño de procedimientos de seguridad basados en pruebas de pentesting aplicadas a la empresa Cjt&T Ingeniería de Software. [En línea]. Proyecto de grado especialización en seguridad informática. San Juan de Pasto: Universidad Nacional Abierta y a Distancia UNAD. Facultad de Ingeniería, 2017. [Consultado el 18 de septiembre de 2021]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/14929/1085285379.pdf?sequence=1&isAllowed=y

MARTÍNEZ ROMERO, Jhon Alexander y BLANCO MEDINA, Leidy Xiomara. Recomendaciones de buenas prácticas de ciberseguridad en Pymes para la generación de soluciones de detección de intrusos usando Snort. [En línea]. Trabajo de grado para ingeniero de sistemas. Bucaramanga: Universidad Autónoma de Bucaramanga. Facultad de Ingeniería, 2020. [Consultado el 18 de septiembre de 2021]. Disponible en: https://repository.unab.edu.co/handle/20.500.12749/13911

MARTÍ TALÓN, Rafael Manuel. Desarrollo e implementación práctica de un PENTEST. [En línea]. Proyecto de grado ingenierio de sistemas de telecomunicaciones, sonido e imagen. Gandia: Universidad Politécnica de Valencia. Facultad de Ingeniería, 2016. [Consultado el 18 de septiembre de 2021]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/70164/MART%C3%8D%20-%20Desarrollo%20e%20implementaci%C3%B3n%20pr%C3%A1ctica%20de%20un%20PENTEST.pdf?sequence=2

MELO, Dubán Mauricio y MORENO RUIZ, Roger Fabián. Seguridad Perimetral Pymes. [En línea]. Proyecto de grado ingeniería en telecomunicaciones. Bogotá D.C: Universidad Distrital Francisco José de Caldas. Facultad de Ingeniería, 2015. [Consultado el 18 de septiembre de 2021]. Disponible en: https://repository.udistrital.edu.co/bitstream/handle/11349/4847/MeloDub%c3%a1nMauricio2015.pdf?sequence=1&isAllowed=y

MILTON SECURITY. [Sitio web]. California: Milton Security Inc, EternalRed - CVE-2017-7494. [Consultado el 7 de marzo de 2022]. Disponible en: https://www.miltonsecurity.com/company/blog/eternalred-cve-2017-7494

MINTRABAJO. [Sitio web]. Bogotá D.C.: MINISTERIO DE TRABAJO, “MiPymes representan más de 90% del sector productivo nacional y generan el 80% del empleo en Colombia”: ministra Alicia Arango. [Consultado el 10 de septiembre de 2021]. Disponible en: https://www.mintrabajo.gov.co/prensa/comunicados/2019/septiembre/mipymes-representan-mas-de-90-del-sector-productivo-nacional-y-generan-el-80-del-empleo-en-colombia-ministra-alicia-arango

MONSALVE PULIDO, Julián; APONTE NOVOA, Fredy & CHAVES TAMAYO, David. Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). [En línea]. Tunja, Boyacá: Universidad Pedagógica y Tecnológica de Colombia UPTC. Facultad de Ingeniería, 2014. [Consultado el 18 de septiembre de 2021]. Disponible en: https://doi.org/10.19053/01211129.2791

NATIONAL INSTITUTE OF STANDAR AND TECHNOLOGY NIST. Technical Guide to Information Security Testing and Assessment. [En línea]. [Consultado el 18 de septiembre de 2021]. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

NATIONAL VULNERABILITY DATABASE. CVE-2017-7494 Detail. [En línea]. [Consultado el 7 de marzo de 2022]. Disponible en: https://nvd.nist.gov/vuln/detail/CVE-2017-7494

ORTEGA CANDEL, José Manuel. Ciberseguridad: Manual práctico. [En línea]. Ediciones Parainfo S.A. Madrid, 2021. [Consultado el 17 de abril de 2023]. Disponible en: https://www.google.com.co/books/edition/Ciberseguridad_Manual_pr%C3%A1ctico/QsROEAAAQBAJ?hl=es-419&gbpv=1&dq=eslabon%20debil%20en%20seguridad%20inform%C3%A1tica&pg=PA85&printsec=frontcover

ORTEGA CANDEL, José Manuel. Hacking ético con herramientas Python. [En línea]. Editorial RA-MA. Madrid, 2018. [Consultado el 1 de septiembre de 2021]. Disponible en: https://books.google.com.co/books?id=wo6fDwAAQBAJ&lpg=PA1&dq=Sqlmap%20espa%C3%B1ol&hl=es&pg=PA3#v=onepage&q&f=false

PALACIOS GALLARDO, Margaret Lesly. Aplicación de Pentesting en el análisis de vulnerabilidades del sistema web de gestión administrativa de la Empresa DEVHUAYRA SAC Huancayo. [En línea]. Proyecto de grado para optar el título de Bachiller en ingeniería de sistemas e informática. Huancayo: Universidad Continental. Facultad de Ingeniería, 20121 [Consultado el 18 de septiembre de 2021]. Disponible en: https://repositorio.continental.edu.pe/bitstream/20.500.12394/9560/4/IV_FIN_103_TI_Palacios_Gallardo_2021.pdf

PAEZ PIRAZAN, Miguel Camilo. Propuesta de procedimiento para la ejecución de pentest dentro del esquema de pruebas de las fábricas de software para aplicaciones web. [En línea]. Proyecto de grado especialización en seguridad informática. Bogotá D.C: Universidad Piloto de Colombia. Facultad de Ingeniería, 2014. [Consultado el 18 de septiembre de 2021]. Disponible en: http://polux.unipiloto.edu.co:8080/00002027.pdf

PENETRATION TESTING EXECUTION STANDARD. PTES Technical Guidelines. [En línea]. [Consultado el 18 de septiembre de 2021]. Disponible en: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

PORTO SOLANO, Andrés. Estructuras organizacionales: Nuevas tendencias. [En línea]. Proyecto de grado para optar el título Máster en ingeniería industrial. Barranquilla: Universidad del Norte. Facultad de Ingeniería, 2017. [Consultado el 9 de noviembre de 2022]. Disponible en: https://publicaciones.americana.edu.co/index.php/adgnosis/article/view/192/209

POSTIGO PALACIOS, Antonio. Seguridad informática. [En línea]. Editorial Ediciones Parainfo S.A. Madrid, 2020. [Consultado el 1 de septiembre de 2021]. Disponible en: https://books.google.com.co/books?id=UCjnDwAAQBAJ&lpg=PA195&dq=Metodolog%C3%ADas%20intrusi%C3%B3n&hl=es&pg=PP1#v=onepage&q=Metodolog%C3%ADas%20intrusi%C3%B3n&f=false

RAMIREZ MONTEALEGRE, Benjamín José. Medición de madurez de ciberseguridad en pymes colombianas. [En línea]. Trabajo de grado maestría. Bogotá D.C: Universidad Nacional de Colombia. Facultad de Ingeniería, 2016. [Consultado el 18 de septiembre de 2021]. Disponible en: https://repositorio.unal.edu.co/handle/unal/57956

SAMBA ORG. [Sitio web]. USA: Samba Security Releases. [Consultado el 17 de abril de 2023]. Disponible en: https://www.samba.org/samba/history/security.html

SANTOS ORCERO, David. Kali Linux. [En línea]. Editorial RA-MA. Madrid, 2018. [Consultado el 1 de septiembre de 2021]. Disponible en: https://books.google.com.co/books?id=to6fDwAAQBAJ&printsec=frontcover&dq=kali+linux+espa%C3%B1ol&hl=es&sa=X&redir_esc=y#v=onepage&q=kali%20linux%20espa%C3%B1ol&f=false

TAMAYO VENTIMILLA, Oswaldo Alejandro. Desarrollo de una guía técnica estándar para aplicar herramientas de Ethical hacking en redes de datos, dirigido a pymes. [En línea]. Proyecto de grado para optar el título de ingeniero de sistemas. Quito: Universidad Pontificia Católica del Ecuador. Facultad de Ingeniería, 2016. [Consultado el 18 de septiembre de 2021]. Disponible en: http://repositorio.puce.edu.ec/bitstream/handle/22000/12612/disertaci%c3%b3ndegrado%20OswaldoTamayo.pdf?sequence=1&isAllowed=y

TERÁN, David. Administración y seguridad en redes de computadoras. [En línea]. Editorial Alfa y Omega. Madrid, 2008. [Consultado el 17 de abril de 2023]. Disponible en: https://www.google.com.co/books/edition/Administraci%C3%B3n_y_seguridad/8H14EAAAQBAJ?hl=es-419&gbpv=1&pg=PA222&printsec=frontcover

TORRES ORTÍZ, Luis Miguel. Implementación de metodología PTES en auditorías de seguridad informática. [En línea]. Proyecto de grado para obtener el título de ingeniero en computación. México: Universidad Nacional Autónoma de México. Facultad de Ingeniería, 2019. [Consultado el 18 de septiembre de 2021]. Disponible en: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/17015/informe.pdf?sequence=5&isAllowed=y

VAYONES MOSQUERA, Amancio. Ciberseguridad en Colombia. [En línea]. Seminario (SIA). Bogotá D.C: Universidad Piloto de Colombia. Facultad de Ingeniería, 2019. [Consultado el 18 de septiembre de 2021]. Disponible en: http://repository.unipiloto.edu.co/handle/20.500.12277/6370

VILLA MESA, Sara. Impacto del Riesgo Cibernético en el Bienestar del Segmento Mipyme. [En línea]. Trabajo de Grado para Optar al Título de Magíster en Economía Aplicada. Medellín: Universidad EAFIT. Facultad de Economía, 2018. [Consultado el 12 de septiembre de 2022]. Disponible en: http://hdl.handle.net/10784/12890

ANEXOS

Figura 38. Carta entrega resultados prueba de intrusión PTES.

Bogotá D.C., 25 de febrero de 2023

Señor:
Carlos Arturo Feria
Gerente

Asunto: Entrega reporte de prueba de intrusión bajo la metodología PTES como resultado del proyecto aplicado realizado.

Cordial saludo estimado Gerente,

Se hace entrega del resultado de la prueba de intrusión realizada en la empresa Colombia Leds SAS correspondiente a la ejecución del proyecto "Aplicación de la metodología PTES en la pyme Colombia Leds SAS para la identificación de vulnerabilidades de ciberseguridad".

Se agradece a Colombia Leds SAS por permitir realizar este proyecto el cual busca aplicar los conocimientos adquiridos durante los estudios de la especialización en seguridad informática de la Universidad Nacional Abierta y a Distancia UNAD de la cual se espera aportar a mitigar los riesgos existentes en ciberseguridad y llevar a mejorar las condiciones de actuales de seguridad informática en base de ejecución de buenas prácticas de ciberseguridad.

Firman en Bogotá D.C., a los (25) días del mes de (febrero) de 2023

Cordialmente,

Ing. Eduard Andrés Fernández Peralta
Estudiante UNAD

Carlos Arturo Feria
Gerente

Fuente: Elaboración propia.