UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TÍTULO DE ANTEPROYECTO DE TITULACIÓN

Análisis de la Seguridad de la Red del Ministerio de Inclusión Económica y Social mediante técnicas de Hacking Ético para Identificar Vulnerabilidades y Amenazas.

AUTOR

Torres Lara Mayerli Johanna

MODALIDAD: EXAMEN COMPLEXIVO

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

ING. IVÁN CORONEL SUÁREZ, MSIA

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
JOSE MIGUEL SANCHEZ AQUINO

Ing. Jose Sanchez A. Mgt.
DIRECTOR DE LA CARRERA

Firmado electrónicamente por:
IVAN ALBERTO CORONEL SUAREZ

Ing. Iván Coronel Suarez, Mgt.
TUTOR

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andradre V. Mgt.
DOCENTE ESPECIALISTA

Firmado electrónicamente por:
MARJORIE ALEXANDRA CORONEL SUAREZ

Ing. Marjorie Coronel S. Mgt.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Mayerli Johanna Torres Lara, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 11 días del mes de diciembre del año 2023

TUTOR

Ing. Iván Coronel Suarez, Mgt.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, MAYERLI JOHANNA TORRES LARA

DECLARO QUE:

El trabajo de Titulación Análisis de la Seguridad de la Red del Ministerio de Inclusión Económica y Social mediante técnicas de Hacking Ético para Identificar Vulnerabilidades y Amenazas. Previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los XX días del mes de XXXX del año 2023

EL AUTOR

MAYERLI JOHANNA TORRES LARA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado Análisis de la seguridad de la red del ministerio de inclusión económica y social mediante técnicas de hacking ético para identificar vulnerabilidades y amenazas, presentado por el estudiante, Mayerli Johanna Torres Lara fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 5%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


CERTIFICADO DE ANÁLISIS
magister

INTRODUCCIÓN

5%
Textos sospechosos

5% Similitudes
< 1% similitudes entre comillas
< 1% Idioma no reconocido
0% Textos potencialmente generados por la IA

Nombre del documento: INTRODUCCIÓN.docx
ID del documento: 7a9cc9ee7ee6bc2314dd3eb4bd7f0435fd13d851
Tamaño del documento original: 452,18 kB

Depositante: IVAN ALBERTO CORONEL SUAREZ
Fecha de depósito: 11/12/2023
Tipo de carga: interface
fecha de fin de análisis: 11/12/2023

Número de palabras: 13.247
Número de caracteres: 92.779

TUTOR

Ing. Iván Coronel Suarez, Mgt.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, MAYERLI JOHANNA TORRES LARA

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del trabajo de titulación con fines de difusión pública, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los XX días del mes de XXXX del año 2021

EL AUTOR

Mayerli Torres L.

MAYERLI JOHANNA TORRES LARA

AUTORIZACIÓN DE LA INSTITUCIÓN

Gobierno del Ecuador

Oficio Nro. MIES-CZ-5-DDSAL-2023-0545-OF

Salinas, 08 de junio de 2023

Asunto: Autorización a realizar trabajo de titulación "ANÁLISIS DE VULNERABILIDADES Y AMENAZAS EN LA RED DE UNA EMPRESA PÚBLICA MEDIANTE TÉCNICAS DE HACKING ÉTICO" de la Universidad Península de Santa Elena

Ing
Jose Miguel Sanchez Aquino
En su Despacho

De mi consideración:

En atención al Oficio No. UPSE-CTI-150-2023-OF, de fecha 30 de Mayo del 2023, suscrito por el Ing. José Sánchez Aquino, Mgt. en calidad de Director de la carrera de Tecnologías de la Información, en el que se solicita se autorice realizar el trabajo de titulación "Análisis de vulnerabilidades y amenazas en la red de una empresa pública mediante técnicas de Hacking Ético" de la estudiante Srta. Mayerli Johanna Torres Lara cédula No. 0956771745 de la Universidad Estatal Península de Santa Elena.

Por lo antes expuesto, se autoriza a la estudiante antes mencionada a recolectar la información necesaria para desarrollar su proyecto de titulación, cabe indicar que por cuestiones de seguridad a la información sensible que maneja nuestra entidad como organismo público solo se le permitirá el acceso a la estudiante autorizada para el ingreso a la Dirección Distrital en el tiempo propuesto, debiendo registrarse en la bitácora de ingreso portando su credencial o documento de identidad, al mismo tiempo se indica que estará sujeta a la normativa y políticas establecidas en el acceso a la información obtenida.

Del proyecto emprendido en este establecimiento se hace conocer que el trabajo a realizar por parte de la estudiante es de carácter informativo y no de implementación que pudiere ocasionar algún incidente de denegación a los servicios de nuestra plataforma de red y continuidad operativa. Bajo estas directrices se le autoriza a la estudiante de la carrera de TIC's empezar en su proceso de recopilación de datos desde el 08 de junio del presente.

Con sentimientos de distinguida consideración.

Atentamente,

Gobierno del Ecuador

Oficio Nro. MIES-CZ-5-DDSAL-2023-0545-OF

Salinas, 08 de junio de 2023

Documento firmado electrónicamente

Mgs. Doris Lisseth Mazzini Illescas
DIRECTORA DISTRITAL SALINAS

Copia:
Mayerli Johanna Torres Lara

Señor Economista
Roy Andres Mora Oyola
Analista de Administración de Recursos Humanos (2) - Distrito Salinas

jm

DORIS LISSETH MAZZINI ILLESCAS

AGRADECIMIENTO

Primero agradezco a Dios, mi guía constante, por darme la fortaleza y la dirección para completar este trabajo de titulación.

A mis padres, les dedico mi más profundo agradecimiento. Su apoyo incondicional y sacrificio han sido el faro que ilumina mi camino académico.

A mis amigos, compañeros y seres queridos, gracias por estar siempre presentes. Su aliento y amistad han sido un regalo invaluable a lo largo de este proceso.

Al Ing. Iván Coronel Suarez cuya guía experta y dedicación han sido cruciales en la realización de este proyecto. Su sabiduría ha dejado una huella imborrable en mi desarrollo académico.

Mayerli Johanna, Torres Lara

DEDICATORIA

Dedico este trabajo principalmente a Dios, por permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mis padres, quienes siempre me han brindado su apoyo incondicional y han sido mi fuente constante de inspiración. Agradezco su amor, sabiduría y paciencia a lo largo de este viaje académico.

A mis amigos y seres queridos, cuyo ánimo y compañía han iluminado los días más desafiantes. Gracias por creer en mí cuando yo dudaba.

Mayerli Johanna, Torres Lara

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE IMÁGENES

RESUMEN

Este trabajo se centró en realizar un análisis de seguridad de la red del Ministerio de Inclusión Económica y Social (MIES) con el propósito de identificar vulnerabilidades y amenazas, empleando la metodología OSSTMM que permite comprender diversas fases para emplear el enfoque investigativo, diagnóstico y evaluativo.

Se llevaron a cabo simulaciones de ataques informáticos con el objetivo de comprender el contexto e intenciones de potenciales piratas informáticos. El resultado fue la generación de un reporte detallado que presenta datos específicos obtenidos durante las pruebas, además de un informe final que correlaciona los problemas sustentados a través del (CVE). Además, se propuso una guía técnica de buenas prácticas para fortalecer la seguridad en el área de red y establecer mecanismos de defensa contra intrusiones futuras.

En conclusión, este estudio proporciona una evaluación exhaustiva y práctica de seguridad, sentando las bases para mejoras técnicas y estrategias de protección más robustas en el futuro.

Palabras claves: Seguridad, Ataques Informáticos, OSSTMM, CVE

ABSTRACT

This work focused on carrying out a security analysis of the network of the Ministry of Economic and Social Inclusion (MIES) with the purpose of identifying vulnerabilities and threats, using the OSSTMM methodology that allows understanding various phases to use the investigative, diagnostic and evaluative approach.

Simulations of computer attacks were carried out with the aim of understanding the context and intentions of potential hackers. The result was the generation of a detailed report that presents specific data obtained during the tests, in addition to a final report that correlates the problems supported through the (CVE). In addition, a technical guide of good practices was proposed to strengthen security in the network area and establish defense mechanisms against future intrusions.

In conclusion, this study provides a comprehensive and practical security assessment, laying the foundation for technical improvements and more robust protection strategies in the future.

Keywords: Security**,** Computer Attacks, OSSTMM, CVE.

INTRODUCCIÓN

CAPÍTULO 1. FUNDAMENTACIÓN

1.1 Antecedentes

En los últimos años se han recibido más reportes cibernéticos que detienen operaciones por días, tanto de instituciones públicas y privadas, debido a programas maliciosos denominados ransomware, durante la pandemia este ataque tuvo un crecimiento significativo siendo este del 27 % ha comparación con el periodo previo a la conocida emergencia Sanitaria [1].

De acuerdo con el grafico presentado, se evidencia un notable aumento en las vulnerabilidades informadas en productos y fabricantes durante el año 2022, siendo este de 25.226, esta cifra representa un crecimiento de un 26,5 % de vulnerabilidades reportadas a comparación con el 2021 y equivale al menos a unas 70 vulnerabilidades por día, situación que si se sigue manteniendo se puede proveer un aumento de detecciones para el 2023 [2].

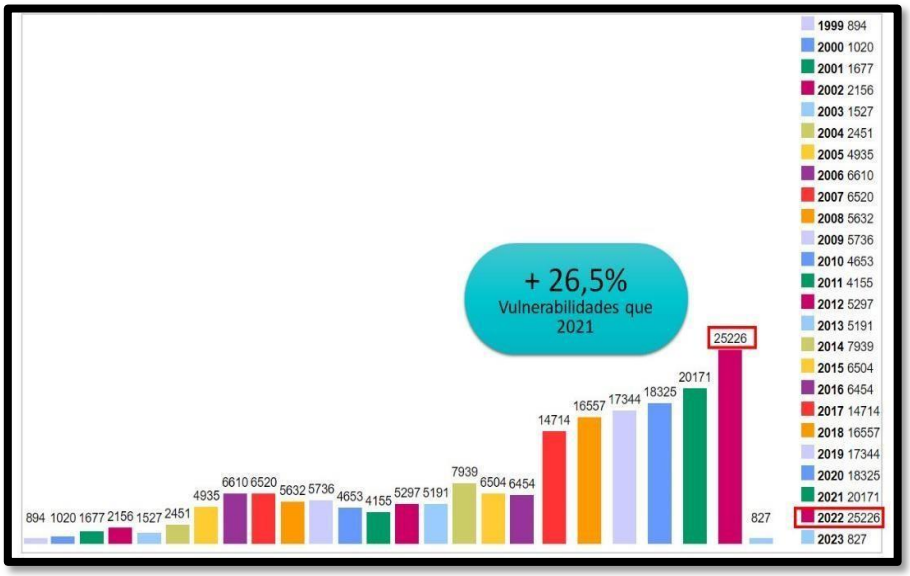


Figura 1: Vulnerabilidades por año

El estudio de amenazas y vulnerabilidades a lo largo de la historia tecnológica se ha visto influenciado por la gran capacidad de información que son transportados por la red para beneficiar al internauta con el fin de comunicarse, almacenar, y enviar datos de un punto a otro. La investigación titulada “Vulnerabilidades reportadas en 2022 aumentaron un

26% y alcanzaron récord histórico", menciona como en el año mencionado se presentó un pico histórico de 25.226 vulnerabilidades reportadas en diferentes puntos de productos y fabricante, que en porcentaje representa un 26,5% como número de vulnerabilidades reportadas a diferencia del año anterior. A continuación, se presenta las vulnerabilidades presentadas por welivesecurity en referencia a temas de seguridad cibernética [3].

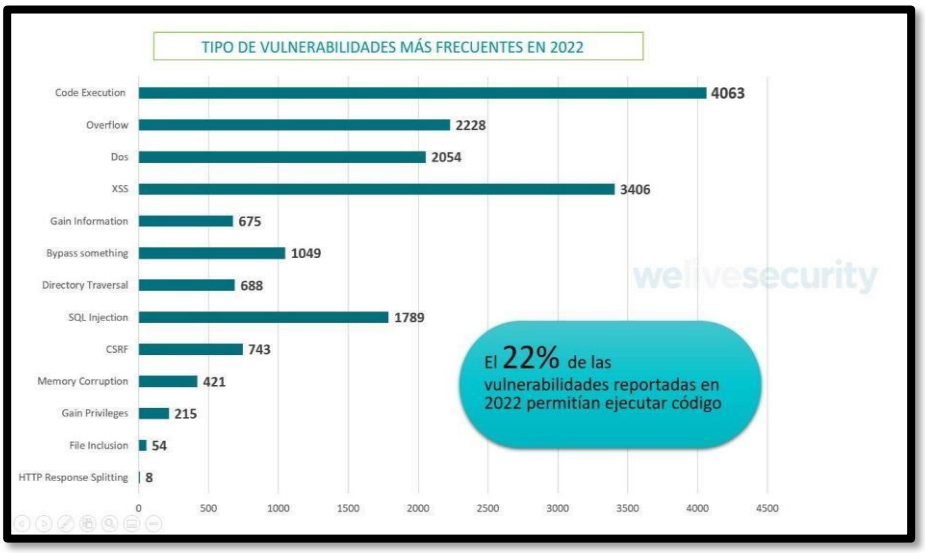


Figura 2: Tipo de vulnerabilidades más comunes Frecuentes en 2022 [2]

Las instituciones son estructuras organizativas que desempeñan un papel fundamental en la sociedad, estableciendo normas, regulaciones y patrones de comportamiento que guían las interacciones entre individuos. Estas entidades como el Ministerio de Inclusión Económica y Social (MIES) en el Ecuador se dedican a promover la inclusión social y económica a nivel nacional. Con presencia en distintos distritos, como Salinas, esta sucursal enfoca su estudio en modernizar su infraestructura tecnológica, sistemas antivirus avanzados y conexiones remotas, con el propósito de mejorar la eficacia en la atención a grupos vulnerables y fomentar la igualdad de oportunidades [4].

El malware basado en VBA (Visual Basic for Applications), también conocido como macro malware, ha experimentado un aumento sostenido en la cantidad de variantes desde su detección inicial en 2014. Su crecimiento fue particularmente notorio, llegando a niveles sin precedentes en el año 2018 [5], junto con la creciente actividad en Ecuador, subraya la importancia de la vigilancia continua y las medidas de seguridad robustas en toda la región (Anexo 1).

La institución ha experimentado ciberataque, donde hubo una mínima perdida de información, correos comprometidos, secuestro de datos e inserción de malware. Estos ataques pueden volver a darse de forma dirigida, arbitrario o esporádicos, la institución puede caer en un estado de soborno provocado por ransomware que en algunos casos suelen pedir que el pago sea a través de criptomoneda (Anexo 2).

Las técnicas de recolección de información a utilizar será la entrevista mediante la cual se va a poder tomar los datos directamente de la población a estudiar [6], mediante su forma de aplicación, siendo un cuestionario (Anexo 3).

En el presente análisis, se considerarán los diversos estudios similares llevados a cabo a lo largo de los años, tanto a nivel internacional, nacional como local. Esta revisión abarcará investigaciones relevantes que hayan abordado problemáticas similares en distintos contextos geográficos y socioculturales.

A nivel mundial se realizó una introducción a la seguridad informática y el análisis de vulnerabilidades, el trabajo realizado por el área de innovación y desarrollo, S.L, menciona que es importante tener en claro los conceptos de seguridad informática y seguridad de la información, que a simple viste suenan parecidos tienen puntos clave que demuestran una diferencia. Siendo el primero el encargado de la seguridad de los medios informáticos mediante procesos y técnicas. [7].

Dentro del nivel nacional se aplicó, Hacking Ético para mejorar la seguridad en la infraestructura informática del grupo electrodata, el presente trabajo de titulación da a conocer las necesidades del grupo Electrodata que surgen a raíz de un crecimiento acelerado en cuanto al desarrollo de su negocio, por lo cual requieren adquirir un conjunto mínimo de mecanismo de control de seguridad para proteger sus sistemas informáticos, es por esto que tienen la necesidad de implementar políticas de seguridad basadas en estándares (ISO/IEC 27001) el cual les va a permitir controlar y regular servicio que ofrecen atreves de sus equipos informáticos [8].

En Ecuador se ejecutó el trabajo denominado, Diagnóstico de las vulnerabilidades informáticas en los sistemas de información para proponer soluciones de seguridad a la rectificadora Gabriel Mosquera S.A, en este trabajo da a conocer que debido a las nuevas tecnologías se dio la aparición de nuevas amenazas tecnológicas que ponen en riesgo los activos de información, de lo cual surge la necesidad de realizar un

diagnóstico de las vulnerabilidades informáticas, para que así los responsables de la seguridad junto con la directiva de la empresa concienticen y contrarresten los riesgos a los que se someten sus activos [9].

Dentro del nivel local tenemos, Análisis de seguridad controlado en aplicaciones web de una institución financiera utilizando herramientas de ciberseguridad y buenas prácticas de OWASP, en el siguiente trabajo se da a conocer que los sectores financieros aumentan sus servicios digitales, debido al incremento de usuarios que realizan transacciones a través de internet con un 72.42 % y a través de dispositivos móviles, es por esto que se deben prevenir para evitar futuros ataques o situaciones que exponen la seguridad de la entidad y sus diferentes usuarios. Dando en conclusión que la aplicación era vulnerable a 5 de los 10 riesgos de seguridad de la lista de OWASP y a su vez presenta cuatro vulnerabilidades de riesgo [10].

Por todo lo anterior expuesto, el presente trabajo es pertinente ante una realidad problemática expuesta, este busca determinar debilidades o huecos que se encuentran dentro de los sistemas utilizados por dicha institución y a su vez dar solución ante la problemática ya expuesta haciendo uso de técnicas de Hacking Ético dando como resultado un informe de sus posibles debilidades.

1.2 Descripción del proyecto

El poco conocimiento de seguridad de la red de datos en instituciones públicas o privada hace inestable la calidad, integridad y confiabilidad de activos de información que circulan en la red, provocando la tediosa tarea de poder detectar a tiempo las anomalías o acciones malintencionadas que son incitadas por piratas informáticos. Por ende, surge el axioma de presentar una estructura de propuesta de testeo de seguridad basado en la metodología OSSTMM (Open Source Security Testing Methodology Manua), que indica un esquema estructurado de especificaciones de seguridad que son comprobados mediante técnicas de seguridad de una forma precisa, concreta y eficiente.

Los testeos de seguridad están conectados a escenarios que frecuentemente ocurren los incidentes de seguridad, ejerciendo una investigación detallada sobre los sistemas y

servicios identificados en la metodología de estudio para desarrollar las pruebas de penetración como; vulnerabilidades, falta de políticas de seguridad, activo de información en peligro, modo de ataque, nivel de criticidad, entre otros aspectos que el pirata informático emplea para comprometer el entorno o sistema red. Por lo cual, el estudio de esta rama de seguridad informática y Ethical Hacking es conciso, útil y necesario para identificar posibles mejoras.

El presente proyecto se guía con la metodología OSSTMM (Open Source Security Testing Methology Manual).

Fase I: Preparación

- Entrevista al encargado del departamento de TI de la institución MIES (Ministerio de Inclusión Económica y Social) para conocer la importancia de la seguridad tecnológica de internet.

Fase II: Interacción

- Escaneo de puertos con Nmap
- arp-scan para conocer dispositivos conectados a la red.
- Advanced Ip Scann

Fase III: Investigación

- Agrupar ataques de penetración a las vulnerabilidades
- Ponderar el nivel de criticidad

Fase IV: Intervención

- Explotación de vulnerabilidades conocidas presente en el estudio de red mediante técnicas de hacking ético

Fase V: Reporte

- Alcance de intrusión
- Evaluación de resultados

- Recomendaciones y observaciones

Las herramientas para utilizar en el desarrollo del proyecto son las siguientes:

wireshark: Se trata de un analizador de protocolos de red que permite revisar lo que sucede en su red a un nivel microscópico y sin fines de lucro. [11]

NetworkMiner: Nos permite capturar datos que se transportan en la red de forma activa o pasiva, o analizar una captura de datos realizados con otra herramienta, se enfoca en recolección de información y así mismo analizarla [12]

Nmap: Es una utilidad gratuita que sirve para el descubrimiento de redes que a su vez es gratuita y de código abierto, utiliza paquetes de ip sin procesar para determinar que host está disponible en la red. [13]

Nessus: es un administrador de vulnerabilidades más implementado debido a que ayuda a reducir la superficie de ataques en una organización. [14]

Metasploit: Metasploit proporciona una amplia variedad de módulos de explotación, payloads y herramientas para llevar a cabo pruebas de seguridad, investigaciones y simulaciones de ataques. [15]

Masscan: Masscan es una herramienta de escaneo de puertos de red de alta velocidad. A diferencia de otras herramientas de escaneo de puertos. [16]

Arp-scan: se utilizará para mapear direcciones IP a direcciones MAC en una red local. [17]

La línea de investigación en la que se encuentra direccionado este proyecto es Tecnología y Sistemas de la información, unido a la sub línea de investigación TSI en las organizaciones y en la sociedad, debido a que la propuesta está relacionada con temas de seguridad. [18]

1.3 Objetivos del Proyecto

Objetivo general

Analizar las vulnerabilidades y amenazas presentes en la red mediante técnicas de hacking ético, para evaluar el nivel de seguridad de la institución MIES, y proponer

medidas de mitigación.

Objetivo específico

- Conocer el contexto real de la seguridad informática de la institución mediante la aplicación de una entrevista para recolectar información.
- Identificar puntos débiles mediante el uso de técnicas de Hacking para conocer el nivel de seguridad informática.
- Elaborar un informe sobre los datos recolectados para salvaguardar la información.
- Proponer una guía de recomendaciones de buenas prácticas de seguridad informática y seguridad de la información para brindar una sólida protección de datos.

1.4 Justificación del Proyecto

La seguridad informática empezó a tomar más auge en los últimos años, ya que dentro de la misma existe información de suma importancia. Para lograr una relación entre cada una de las áreas del negocio existen documentos que logran mantenerlas conectadas, aumentando así la productividad para cumplir con cada objetivo propuesto, es por esta razón que la información es valiosa y debe de estar protegida de forma adecuada [19].

Una de estas es permitir creación de barreras de protección mediante herramientas como: antivirus o anti-espías, para delimitar las vulnerabilidades informáticas se debe tener en cuenta que existen varios tipos de seguridad informática, entre ellos se encuentra la seguridad para la red, software y hardware.

Actualmente, las instituciones optan por mantener su información segura haciendo uso de protocolos y normativas de seguridad, como puede ser uso de firewall o poner restricciones en la red, aplicando así la seguridad informática debido a que esta radica en la prevención, evitando así robos de información de las institucione [20]. Este también ayuda a identificar cuando hay riesgos de sistemas de información y amenazas de virus. De la misma forma, no se encuentra orientado netamente a proteger solo activos de una institución, sino también a la información crítica y personal de sus empleadores.

La ley orgánica de protección de datos personales menciona que su principal objetivo es garantizar el derecho a la protección de los datos. Donde establece que los responsables del manejo los datos deben garantizar la seguridad de la información ante cualquier

riesgo, aplicando todas las medidas posibles, como adoptar estándares u otros mecanismos para el manejo de los datos [21]. Por esta razón, se contempla realizar un análisis de vulnerabilidades mediante técnicas de hacking. Esto permitirá detectar vulnerabilidades y evaluar la exposición a riesgos. El objetivo es poner de manifiesto los posibles puntos débiles, comprender las amenazas a las que están expuestos y determinar si los servidores son susceptibles a solicitudes de peticiones falsas.

En la realización de este proyecto la detección de vulnerabilidades es de gran importancia, ya que mediante este los miembros del departamento de TI donde se realizara este análisis tomarán decisiones importantes con respecto a las medidas de seguridad que deberán ser aplicadas, evitando así el ingreso de personas mal intencionadas a la red que tienen como fin atentar contra la seguridad y privacidad que se encuentra en dicha institución pública, el presente trabajo, permitirá obtener una idea clara sobre el impacto de una posible intrusión y al realizar una evaluación de las técnicas de Hacking Ético va a permitir proporcionar o brindar posibles soluciones de cómo evitar y mitigar en caso de que llegue a presentarse dentro de la organización.

El diagnóstico de vulnerabilidades mediante técnicas de Hacking Ético orientado en los procesos del área de tecnología de una institución pública, es por esto por lo que surge la necesidad de analizar, conocer y realizar la detección de vulnerabilidades dirigida a la seguridad informática. Esta es una de las medidas que actualmente es utilizada en varias organizaciones por profesionales dedicados al Ethical Hacking aplicándolas en instituciones, publicaciones o privadas. Cada año existe incremento en las vulnerabilidades y en su mayoría son detectadas en organizaciones que han dado la apertura a realizar investigaciones como el presente trabajo, con la finalidad de lograr determinar el grado de vulnerabilidad, puertos abiertos, archivos maliciosos y así logra conocer que tan vulnerables son.

El presente trabajo se encuentra alienado a los objetivos del Plan de Creación de Oportunidades, específicamente en el siguiente eje:

Eje 3: Seguridad Integral

Objetivo 10: Garantizar la soberanía nacional, integridad territorial y seguridad del estado.

Política 10.1: Fortalecer al Estado para mantener la confidencialidad, integridad y disponibilidad de la información frente a amenazas provenientes del Ciberespacio y Proteger su infraestructura crítica. [22]

1.5 Alcance del Proyecto

La introducción de un estudio de seguridad informática en una institución pública posibilitará llevar a cabo un análisis exhaustivo de las vulnerabilidades más comunes y las amenazas presentes en la red, debido a la falta de seguridad o control al proteger los activos de información.

El presente proyecto presenta una visión detallada de las problemáticas derivadas de las vulnerabilidades en la seguridad de la red informática. Se destaca especialmente la preocupante exposición de datos de usuarios debido a la falta de cifrado, lo cual constituye una brecha significativa en la ciberseguridad de la institución. Esta situación plantea riesgos sustanciales para los activos de información, incluyendo la amenaza de intrusiones por parte de piratas informáticos y la presencia de códigos maliciosos. La magnitud de estas amenazas no solo compromete la integridad de la red, sino que también podría desencadenar consecuencias severas, incluso hasta el punto de poner en riesgo la continuidad de la institución si no se abordan adecuadamente las deficiencias en la gestión de la seguridad de los datos.

Para ejecutar el proyecto deberá incluirse las fases mencionadas a continuación:

Fase I: Preparación

Se realiza la entrevista al encargado del departamento de TI de la Institución MIES (Ministerio de Inclusión Económica y Social) para comprender la importancia de la seguridad tecnológica de internet en las instituciones públicas, métodos, entre otros.

Fase II: Interacción

Implica interactuar con el entorno de la red de la institución objeto de estudio para obtener información detallada. Se llevarán a cabo actividades como el escaneo de puertos, el mapeo de la red y la identificación de los dispositivos conectados en la red.

Fase III: Investigación.

En esta etapa, se lleva a cabo una investigación exhaustiva que detalla las posibles vulnerabilidades conocidas en los sistemas o servicios disponibles. El objetivo es estudiar ataques preliminares que posteriormente serán utilizados en la fase de intervención. Además, se realiza una evaluación del nivel de criticidad de cada uno de los puntos débiles identificados. Esta información es crucial para categorizar adecuadamente las vulnerabilidades y planificar la siguiente fase del proceso.

Fase IV: Intervención

En esta fase del proceso, se ejecuta la etapa de explotación, la cual implica realizar ataques en los escenarios pertinentes para comprometer la seguridad. Esto se basa en la fase previa de identificación de vulnerabilidades conocidas. El propósito es llevar a cabo una prueba exhaustiva de seguridad en los sistemas bajo estudio, para luego elaborar el correspondiente informe y reporte de resultados.

Fase V: Reporte

En el desarrollo del reporte se toma en cuenta los resultados obtenidos en la fase de intervención que cumple la acción de explotación mediante técnicas de hacking, en donde se explica de manera detallada de los objetivos y consignación de valoración de la seguridad de la red informática. El presente documento esta estructura con la información de la institución de objeto, objetivo de estudio, alcance de intrusión, evaluación de resultados y observaciones.

El estudio centrado en la evaluación de la red mediante técnicas de hacking ético brindará un punto de vista favorable en la seguridad de los activos de la información emitido en la red. Por ende, el estudio estará centrado en el testeo de seguridad de las redes de datos según la metodología de estudio, en donde se contará la visualización de un contexto real de ejecución de intrusión con precaución y contar con información detallada como; archivos de configuración, usuarios, entre otros con la finalidad de entender el arte de los incidentes de seguridad presente en una red pública.

Por consiguiente, El estudio investigativo debe ser amplio a un entorno más sutil para experimentar las otras categorías de seguridad que la metodología OSSTMM

proporciona, con el fin de tener más amplio enfoque de análisis con todo el tema de vulnerabilidades y amenazas

CAPÍTULO 2. MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1 Marco contextual

2.1.1 Instituciones Públicas

Las instituciones públicas representan pilares fundamentales en la estructura gubernamental de cualquier sociedad. Estas entidades desempeñan un papel esencial en la implementación y ejecución de políticas públicas, asegurando el funcionamiento efectivo de los servicios gubernamentales y el cumplimiento de las obligaciones del Estado. [23].

El ministerio de Inclusión Económica y Social (MIES) es una institución gubernamental a nivel nacional en Ecuador, encargada de implementar políticas de inclusión social y económica en todo el país. Su objetivo es brindar apoyo a grupos vulnerables y promover la igualdad de oportunidad. Cuenta con diversos distritos como en la provincia de Santa Elena, Guayas, Quito, Una de las sucursales del MIES cuenta como objetivo primordial de este estudio – Salinas, dentro de su infraestructura tecnológica cuenta con servidores virtuales de antivirus, gestores de archivos, conexiones remotas, entre otros [4].

2.1.2 Base legal

La Ley Orgánica de Protección de Datos Personales es una regulación legal cuyo propósito principal es salvaguardar el procesamiento de datos personales, las libertades públicas y los derechos fundamentales de los individuos, especialmente su honor, intimidad personal y familiar [24]. En el contexto de esta ley, se consideran los artículos más importantes para el trabajo actual.

Capítulo I.- Ámbito de aplicación integral

Art. 1.- Objeto y finalidad. - El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela [24].

Art. 25.- Categorías especiales de datos personales.

Se considerarán categorías especiales de datos personales, los siguientes [24].

a) Datos sensibles; -

b) Datos de niñas, niños y adolescentes:

c) Datos de salud; y,

d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.

Art. 38.- Medidas de seguridad en el ámbito del sector público.- El mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deban

implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier nesgo, amenaza., vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los daros conforme al principio de seguridad de datos personales [24].

Art. 40.- Análisis de riesgo, amenazas y vulnerabilidades.- Para el análisis de riesgos, amenazas y vulnerabilidades, ¡el responsable y el encargado del tratamiento de los datos personales deberán utilizar una metodología que considere, entre otras [24];

1) Los resultados del análisis de riesgos, amenazas y vulnerabilidades;

2) La naturaleza de los datos personales;

3) Las características de las partes involucradas; y,

4) Los antecedentes de destrucción de datos personales, la pérdida, alteración,

divulgación o impedimento de acceso a los mismos por parte del titular, sean

accidentales e intencionales, por acción u omisión, así como los antecedentes de transferencia, comunicación o de acceso no autorizado o exceso de autorización de tales datos.

Art. 43.- Notificación de vulneración de seguridad.- El responsable del tratamiento deberá notificar la vulneración de la seguridad de datos personales a la Autoridad de

Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones, tan pronto sea posible, y a más tardar en el término de cinco (5) días después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la Autoridad de Protección de Datos no tiene lugar en el término de cinco (5) días, deberá ir acompañada de indicación de los motivos de la dilación [24].

2.2 Marco contextual

2.2.1 Hacking ético

El objetivo principal del Ethical Hacking o hackeo ético consiste en detectar las debilidades existentes en el sistema de interés a través de pruebas de intrusión, las cuales permiten comprobar y evaluar la seguridad física y lógica de los sistemas de información, redes informáticas, aplicaciones web, servidores, bases de datos, entre otros [25].

2.2.2 Ethical Hackers

Los hackers éticos emplean técnicas y conocimientos de la rama de seguridad informática para emplear intrusión y proponer buenas prácticas tras una brecha tecnológica, para muchas personas su definición se iguala a los piratas informáticos.

Los piratas informáticos, en realidad, son muy diferentes de las personas responsables de los ataques informáticos y los virus de hoy. Un hacker puede definirse como una "persona que disfruta aprendiendo los detalles de los sistemas informáticos y cómo ampliar sus capacidades. El hacking ético puede definirse como la “metodología adoptada por hackers éticos para descubrir las vulnerabilidades existentes en los entornos operativos de los sistemas de información” [26]

2.2.3 Tipos de Hacking Ético

Los distintos tipos de hacking ético se diferencian en la forma en que llevan a cabo la realización de pruebas de análisis de vulnerabilidades y su posterior explotación. Cuando una empresa solicita los servicios de un hacker ético, el profesional encargado de realizar estas actividades debe definir junto con la institución si se llevarán a cabo sin tener acceso a ninguna información previa, lo que se conoce como hacking ético Black Box; si la

empresa proporcionará información, como direcciones IP o credenciales, entonces se trata de un hacking ético White Box; y si solo proporciona cierta información, pero en menor medida que en el caso del White Box, entonces se trata de un hacking ético Gray Box [27].

2.2.4 Elementos que cubren la seguridad informática

2.2.4.1 Confidencialidad

Se refiere a la protección de los datos y la información contra el acceso no autorizado. Esto implica que solo las personas que tienen el permiso adecuado pueden acceder a la información, y que se toman medidas para evitar la divulgación o el acceso no autorizado a la misma [28].

2.2.4.2 Disponibilidad

Se refiere a la capacidad de los sistemas y la información para estar disponibles y accesibles para los usuarios autorizados cuando sea necesario. Esto significa que los usuarios deben poder acceder a la información y los sistemas de manera confiable y sin interrupciones [29].

2.2.4.3 Integridad

Se refiere a la garantía de que los datos y la información son precisos, completos y confiables. Esto implica que se deben tomar medidas para prevenir cualquier modificación o alteración no autorizada de los datos y garantizar que los datos no sean manipulados o dañados de ninguna manera [30].

2.2.5 Metodología del hacking ético

Una metodología de Hacking Ético es un grupo de procedimientos organizados que le permitirán al Hacker Ético desarrollar de forma secuencial y ordenada el logro de sus objetivos. Toda la información obtenida y procesada por los Hackers Éticos debe tener un orden para no entrar en redundancia de información y no desgastar mayor tiempo del que le debería tomar, para ello existen diversas metodologías que le permitirán al Ethical Hacker llevar a cabo sus consultorías. Entre la más conocida tenemos a ISSAF [27].

2.2.5.1 Metodología ISAAF

Esta metodología puede ser aplicada para analizar la seguridad de dispositivos de red, sistemas de auditoría de bases de datos, sistemas operativos y aplicaciones. Además, ISSAF destaca la importancia de cumplir con los requisitos normativos y las buenas prácticas en la implementación de medidas de seguridad. Cabe señalar que ISSAF es una metodología específica para llevar a cabo pruebas de "pentesting" [31].

2.2.5.2 Metodología OSSTMM

Open Source Security Testing Methodology Manual (OSSTMM) es una metodología de hacking ético que se centra en la evaluación de la seguridad física, lógica y social de los sistemas de información. OSSTMM se enfoca en la identificación de vulnerabilidades mediante pruebas que se realizan en diferentes niveles, desde la evaluación de políticas y procedimientos hasta la realización de pruebas de penetración [32].

2.2.5.3 Metodología OWASP

Es una comunidad global que se enfoca en la seguridad de las aplicaciones web y proporciona una metodología de hacking ético para realizar pruebas de seguridad de aplicaciones web. La metodología de OWASP cubre todas las fases del ciclo de vida de las aplicaciones web, desde la planificación hasta la fase de mantenimiento [33].

2.2.6 Técnicas hacking ético

se refieren a un conjunto de prácticas y metodologías utilizadas por expertos en seguridad informática para evaluar la seguridad de un sistema de manera ética y con el objetivo de detectar vulnerabilidades y debilidades que puedan ser aprovechadas por atacantes malintencionados [34].

2.2.7 Seguridad informática

Se refiere a un conjunto de técnicas, tácticas y herramientas que tienen como objetivo asegurar la confidencialidad, disponibilidad e integridad de la información. Estos métodos y herramientas están diseñados para proteger los sistemas informáticos de posibles amenazas, y se llevan a cabo con la participación de personas en un proceso de protección de la información [35].

2.2.8 Vulnerabilidad

Se entiende como vulnerabilidad cualquier punto débil de un sistema que puede ser aprovechado para causar daño o pérdida. Por lo tanto, el punto más vulnerable de seguridad de un sistema es el más propenso a ser explotado. Un ataque, por su parte, es cualquier tipo de acción que busque aprovechar una vulnerabilidad en un sistema [35].

2.2.9 Amenazas

Las amenazas son situaciones que tienen la capacidad de provocar daños o pérdidas en un sistema, tales como ataques perpetrados por seres humanos, desastres naturales, errores involuntarios cometidos por personas, o fallas internas en el hardware o software [36].

2.2.10 Mitigación

La mitigación se refiere a la acción de reducir o minimizar los efectos negativos de un riesgo o una amenaza. Consiste en implementar medidas preventivas para disminuir la probabilidad de que se produzca un evento indeseado o para reducir su impacto en caso de que ocurra. La mitigación puede ser aplicada en diferentes ámbitos, como la seguridad informática, la gestión de riesgos naturales, la salud pública, entre otros [37].

2.2.11 Tipos de pentesting

2.2.11.1 Black box (caja negra)

La técnica en cuestión implica llevar a cabo todos los procedimientos propios del hacking ético, sin tener acceso a ningún tipo de información previa, salvo la identidad de la organización que se someterá a la consulta. Esta técnica imita todas las artimañas y habilidades que podría emplear un atacante malintencionado, con el propósito de obtener acceso a la empresa y vulnerar información confidencial [27].

2.2.11.2 White box (caja blanca)

La técnica se centra en identificar los recursos críticos de la institución y, con la información proporcionada por esta, intenta detectar y demostrar las posibles deficiencias de configuración o insuficiencias en los controles de seguridad implementados [27].

2.2.11.3 Gray box (caja gris)

La prueba de penetración es la técnica más utilizada y requiere un esfuerzo significativo para obtener información importante. La comunicación efectiva entre el equipo de pruebas y la institución en evaluación es crucial para su éxito [38].

2.2.12 Informe de hallazgos

Documento detallado que registra las vulnerabilidades descubiertas, su impacto potencial, las pruebas realizadas y las recomendaciones para remediar los problemas identificados durante el análisis de vulnerabilidades y el hacking ético [38].

2.2.13 Gestión de riesgos

Examinar y evaluar las posibilidades de sufrir pérdidas y los efectos secundarios derivados de desastres, así como de tomar medidas preventivas, correctivas y mitigadoras correspondientes. El riesgo se ve influenciado por dos variables principales: la amenaza y la vulnerabilidad. Ambas condiciones son necesarias para determinar el nivel de riesgo, que se define como la probabilidad de sufrir pérdidas en un lugar específico y durante un período de tiempo determinado. Mientras que los eventos naturales no siempre son controlables, la vulnerabilidad puede ser gestionada y reducida [39].

2.2.14 Cumplimiento de normas

Asegurarse de que la institución pública cumple con las regulaciones y estándares de seguridad aplicables, como las leyes de protección de datos y las normativas específicas del sector [40].

2.2.15 Ciberataques

Los ataques cibernéticos son acciones con el propósito de obtener acceso no autorizado a sistemas informáticos y sustraer, alterar o dañar datos. Aprende cómo salvaguardarte frente a estas amenazas [41].

2.2.16 Amenazas internas

Las amenazas provenientes de fuentes internas tienen un potencial de generar daños más significativos en comparación con las amenazas externas debido al acceso directo que los usuarios internos tienen a las instalaciones y dispositivos de infraestructura. Los atacantes

internos suelen estar familiarizados con la red corporativa, sus recursos y los datos confidenciales. Además, es posible que posean conocimiento sobre las medidas de seguridad implementadas, las políticas establecidas y los privilegios administrativos de mayor nivel [42].

2.2.17 Amenazas externas

Las amenazas externas, tanto por parte de aficionados como de expertos en ataques, pueden aprovechar las vulnerabilidades presentes en los dispositivos conectados a la red o recurrir a técnicas de ingeniería social, como el engaño, para obtener acceso. Estos ataques externos se valen de las debilidades o vulnerabilidades existentes con el fin de acceder a los recursos internos [42].

2.2.18 Ciberataques más comunes

2.2.18.1 Ransomware

El ransomware es un tipo de malware avanzado que aprovecha las vulnerabilidades del sistema y utiliza una encriptación robusta para secuestrar datos o bloquear la funcionalidad del sistema como una forma de chantaje. Los delincuentes cibernéticos emplean el ransomware con el objetivo de exigir un pago a cambio de restaurar el acceso al sistema. Una tendencia reciente en el ámbito del ransomware es la aplicación de tácticas de extorsión. [43]

2.2.18.2 Inyección SQL

Los ataques de inyección SQL implican la inserción de código malicioso en aplicaciones que presentan vulnerabilidades, lo que provoca la generación de consultas a la base de datos de backend y la ejecución de comandos o acciones similares sin el consentimiento del usuario. [43]

2.8.18.3 Malware

El malware, conocido también como software malicioso, utiliza técnicas de camuflaje al presentarse como programas legítimos o archivos adjuntos de correo confiables, como por ejemplo una carpeta de archivos o un documento cifrado. Su objetivo es permitir a

los hackers acceder a una red de computadoras y comprometer su seguridad. Este tipo de ciberataque puede afectar gravemente toda una infraestructura de TI. Algunos ejemplos comunes de malware incluyen troyanos, spyware, gusanos, virus y hardware. [44]

2.2.18.4 Ataque de denegación de servicio distribuido (DDoS)

Un ataque de Denegación de Servicio Distribuido (DDoS) ocurre cuando múltiples equipos comprometidos apuntan hacia un sitio web o red en particular con el objetivo de dificultar o denegar la experiencia del usuario en esa plataforma. Por ejemplo, cientos de ventanas emergentes, anuncios o incluso el bloqueo completo de un sitio pueden contribuir a un ataque DDoS en un servidor vulnerable. [44]

2.2.18.5 Phishing

Otro tipo de ataque cibernético es el phishing, el cual se trata de estafas diseñadas para engañar a los usuarios y hacerlos revelar sus credenciales u otra información confidencial. Este tipo de amenaza cibernética utiliza tanto tecnología como técnicas de ingeniería social para persuadir a las personas a proporcionar datos sensibles que luego serán utilizados de manera fraudulenta. [45]

2.2.18.6 Mitm o man-in-the-middle

En un ataque de Man in the Middle o Hombre en el Medio (MitM), un atacante interfiere de manera secreta en la comunicación entre dos personas e incluso puede manipularla.

Este tipo de ataque es posible cuando la conexión se realiza a través de un punto de acceso wifi no cifrado. Es importante destacar que las personas involucradas en la conversación no son conscientes de que el atacante está interceptando o modificando la información compartida. [45]

2.2.18.7 Ataque de troyanos

Este tipo de troyano es considerado uno de los más simples, pero también potencialmente el más peligroso. Esto se debe a que tiene la capacidad de cargar diversos tipos de malware en tu sistema, funcionando como una puerta de entrada, o al menos asegurando que tu sistema sea vulnerable a ataques. Con frecuencia, se utiliza como una puerta trasera para establecer botnets. Sin que tú lo sepas, tu computadora se convierte en parte de una red zombi que se utiliza para llevar a cabo ataques. [46]

2.2.18.8 Rootkits

Los rootkits son una forma de software utilizada por criminales con el fin de tomar el control de una computadora o incluso de una red. Aunque pueden aparecer como una sola aplicación, la mayoría de los rootkits están compuestos por varias herramientas que, cuando se utilizan en conjunto, permiten obtener un acceso privilegiado al dispositivo. [47]

2.3 Marco teórico

2.3.1 Seguridad de la información como proceso continuo

Esta teoría se basa en la idea de que la seguridad de la información es un proceso continuo y dinámico. Se sostiene que es necesario evaluar y analizar las vulnerabilidades y amenazas en la red de una institución para garantizar la confidencialidad, integridad y disponibilidad de la información. El hacking ético se considera una técnica efectiva para descubrir y remediar estas vulnerabilidades. "Fundamentos de seguridad de redes" es un libro escrito por Behrouz A. Forouzan y Mohammad A. Mazidi en 2014 y publicado por McGraw-Hill Interamericana.

Este libro proporciona una comprensión básica de los principios de seguridad de redes y los fundamentos necesarios para proteger la información en un entorno de red. Además, se analizan las amenazas más comunes que enfrentan las redes, como el malware, los ataques de denegación de servicio (DoS), el phishing y el spoofing. Se examinan las medidas de seguridad necesarias para proteger los componentes clave de una red, como routers, switches, firewalls y servidores. [48]

2.3.2 Hacker ético utilizado como medio para remediar vulnerabilidades

Esta teoría se centra en la importancia de utilizar habilidades de hacking ético para identificar y remediar vulnerabilidades en la red. Se sostiene que, al simular los métodos y técnicas utilizados por los hackers maliciosos, los hackers éticos pueden descubrir y corregir las debilidades en los sistemas de información, fortaleciendo así la seguridad de la red. "Ethical Hacking: Técnicas de seguridad ofensiva" es un libro escrito por Alejandro Hernández en 2016.

Este libro se centra en proporcionar información y técnicas relacionadas con el hacking ético y la seguridad ofensiva, aborda el concepto de hacking ético y explica cómo los profesionales de la seguridad pueden utilizar estas técnicas para identificar y prevenir vulnerabilidades en los sistemas. Se enfoca en las metodologías y herramientas utilizadas por los hackers éticos para evaluar la seguridad de los sistemas informáticos y las redes, presenta una amplia gama de temas relacionados con el hacking ético, como la recolección de información, el escaneo de puertos, la explotación de vulnerabilidades, el acceso no autorizado, el análisis de malware y la protección de los sistemas. [49].

2.3.3 Análisis de riesgo cibernético, evaluación de amenazas y vulnerabilidades en la red corporativa

Esta teoría se basa en la idea de que el análisis de vulnerabilidades y amenazas en la red es fundamental para evaluar y gestionar los riesgos asociados con las operaciones de una institución. El hacking ético se utiliza como una técnica para identificar las vulnerabilidades y evaluar su impacto potencial en la organización. Con esta información, la institución puede tomar medidas proactivas para mitigar los riesgos identificados. "Análisis y gestión de riesgos en sistemas de información" es un libro escrito por J. A. en 2013 y publicado por la Universidad Politécnica de Madrid. Este libro se centra en proporcionar una comprensión profunda del análisis y la gestión de riesgos en los sistemas de información, aborda los conceptos fundamentales relacionados con la gestión de riesgos en sistemas de información y ofrece una metodología estructurada para identificar, evaluar y mitigar los riesgos en estos sistemas. Se enfoca en los procesos y técnicas utilizadas para proteger la confidencialidad, integridad y disponibilidad de la información en un entorno de sistemas de información [50].

2.3.4 Mejora continua en un enfoque para la mejora de procesos operativos

Esta teoría sugiere que el análisis de vulnerabilidades y amenazas en la red de una institución pública debe ser un proceso continuo y constante. Se sostiene que las amenazas y las vulnerabilidades evolucionan con el tiempo, por lo que es necesario realizar evaluaciones periódicas utilizando técnicas de hacking ético para mantener la seguridad de la red actualizada y adaptada a los cambios del entorno tecnológico. "Gestión de la seguridad de la información y ciberseguridad" es un libro escrito por Richard Solms en 2017 y publicado por Ediciones Díaz de Santos.

Este libro se centra en proporcionar una comprensión integral de la gestión de la seguridad de la información y la ciberseguridad, habla sobre conceptos fundamentales relacionados con la seguridad de la información y la ciberseguridad, ofreciendo una visión holística de los desafíos y las estrategias necesarias para proteger la información en un entorno digita, explora los aspectos clave de la gestión de la seguridad de la información, como la identificación de activos de información, la evaluación de riesgos, la implementación de controles de seguridad, la gestión de incidentes y la planificación de la continuidad del negocio [51].

2.3.5 Seguridad informática en instituciones públicas

En 2018, había 130 instituciones gubernamentales con portales web, de los cuales el 80% contaba con características de accesibilidad y solo el 9% tenía aplicaciones móviles para la gestión de trámites ciudadanos. Actualmente, se puede gestionar el 73% de los trámites en línea, lo que ha llevado a un aumento en la vulnerabilidad de la gestión gubernamental y ha destacado la importancia de la ciberseguridad para proteger contra los riesgos derivados del uso de internet [52].

Para abordar de manera efectiva las necesidades actuales de la sociedad en términos de protección de los diferentes servicios electrónicos manejados por las organizaciones, el estado tiene previsto implementar un Plan Nacional entre 2018 y 2021. Las principales iniciativas incluyen la gestión del Esquema Gubernamental de Seguridad de la Información (EGSI), la creación del Centro de Respuesta ante Incidentes Informáticos EcuCERT y la incorporación de delitos informáticos en el Código Orgánico Integral [52].

Aplicación de seguridad informática en el ámbito institucional

La seguridad informática es crucial para las instituciones, ya que la explotación malintencionada de los sistemas de información y recursos internos puede tener graves consecuencias en todas las áreas de la organización, afectando tanto la productividad como las finanzas. Por lo tanto, es importante que la seguridad informática esté enfocada en prevenir amenazas y riesgos a los sistemas de información internos. Actualmente, para garantizar una buena seguridad de la información, se necesita personal experto en

tecnologías informáticas que puedan prever y enfrentar estas amenazas y riesgos. Según la Southern New Hampshire University [53].

- El 62% de los responsables de seguridad informática en las instituciones se siente medianamente seguro o nada seguro respecto a los sistemas de información de las organizaciones en las que trabajan, mientras que solo el 7% se siente extremadamente seguro.
- En consecuencia, las instituciones están asignando más fondos a la seguridad informática para combatir los constantes ataques informáticos. Las herramientas de seguridad informática deben enfocarse en el análisis constante y la ejecución proactiva para detectar vulnerabilidades en los ambientes de TI de las instituciones.

La detección de vulnerabilidades y la seguridad informática son fundamentales para mantener segura la información privada de las instituciones, por lo que invertir en este tipo de herramientas es necesario y una inversión a corto, mediano y largo plazo [53].

2.4 Metodología del Proyecto

2.4.1 Metodología de Investigación

La metodología exploratoria sirve para investigar una temática poco conocida donde existe poca información sobre el objeto de estudio [54]. El presente trabajo de titulación ha sido desarrollado en la institución pública a estudiar, debido a esto es necesario indagar la información de trabajos relacionados con respecto a la línea de investigación, comparando así las diferencias frente al trabajo propuesto, por tal motivo se va a aplicar dicha investigación para la recolección de información bibliográfica.

La investigación diagnóstica [54] se realizará a través de una entrevista direccionada al personal del departamento de TI para obtener conocimientos sobre la situación actual de la institución, permitiendo conocer la situación actual, identificando las necesidades y mejoras que se pueden aplicar en el proyecto.

Variable

- ✓ Nivel de acceso a la red de la institución pública al hacer la prueba de intrusión con técnicas de hacking Ético

2.4.2 Técnicas e instrumentos de recolección de datos

Técnicas

- **Observación:** Es la técnica para ejecutarse por medio de una previa observaciónde campo.
- **Entrevista:** Esta técnica va a permitir entrevistar al personal encargado del departamento de TI de la institución pública.

Instrumentos

Cuestionario: Es el instrumento que se ejecutará para encuestar al personal encargado del departamento de TI de una institución pública para determinar el nivelde conocimiento sobre la seguridad informática.

Población

- La población por estudiar está conformada por un miembro directivo del departamento deTI, considerando también diversas técnicas que se obtuvieron mediante la revisión bibliográfica que son las más utilizadas para detectar las vulnerabilidades en la actualidad.

2.4.3 Metodología de desarrollo

El presente trabajo se establece con base a la metodología OSSTMM, debido a que se trata de un manual de metodologías de código abierto, donde se realiza análisis y medición de la seguridad llevando a cabo pruebas exhaustivas, se ejecutará de acuerdo con una serie de procedimientos ya sea cuando se esté desarrollando, administrando y gestionando sus sistemas para que estos se encuentren seguros empleando rigor en cada proceso [55].

La metodología OSSTMM se encuentra dividida en cinco fases donde permiten identificar y tomar medidas para evitar futuros inconvenientes, esta metodología está direccionado con la identificación de errores y vulnerabilidades.

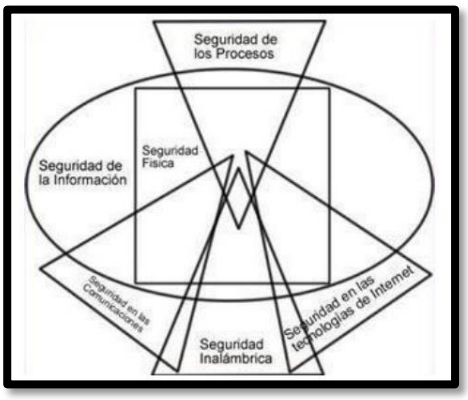


Figura 3: Esquema de Metodología OSSTMM

Es necesario escoger sesiones con mayor énfasis al proyecto, como lo es la seguridad de las redes de datos.

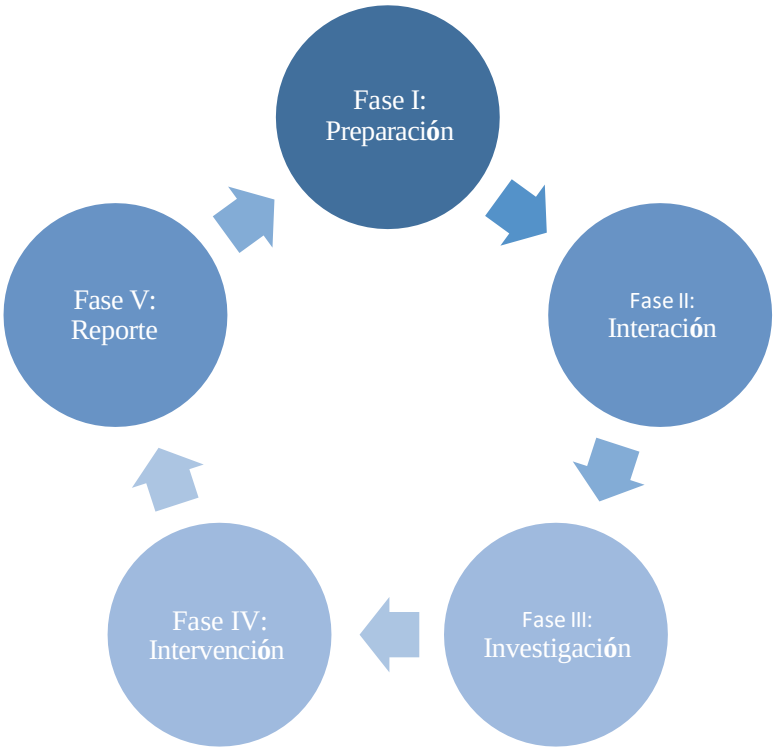


Figura 4 Fases Metodología OSSTMM

CAPÍTULO 3. PROPUESTA

3.1 REQUERIMIENTOS

Código	Especificación de requerimiento
RQ1	Autorización del permiso para la realización del proyecto al departamento de TI del MIES.

RQ2	Entrevista al encargado del departamento de TI para la recopilación de información y conocer el contexto real de vulnerabilidades y amenazas en redes informáticas.
RQ3	Reconocimiento de la infraestructura de la red y desarrollo de la topología.
RQ4	Investigar las amenazas comunes de la red informática moderna para el análisis, identificación y selección para el desarrollo de evaluación de la metodología.
RQ5	Se hará la configuración e instalación de las aplicaciones necesarias para el proyecto en bases a los requerimientos.
RQ6	Preparación del entorno virtual de la instalación de la máquina Kali Linux
RQ7	Se ejecutará la fase de evaluación con el primer paso de exploración mediante la utilización de la herramienta de Kali Linux para conocer las características de la red.
RQ8	Para el segundo criterio de la fase de evaluación, se identificará las vulnerabilidades mediante el análisis de la red por herramientas centradas en el área.
RQ9	Reconocer los puertos vulnerables de la red y determinar sus brechas de seguridad.
RQ10	Preparación de diseños de ataques según las amenazas usuales de la red moderna clasificadas por técnicas de hacking ético.
RQ11	Se requiere saber el objetivo, modo de realización, dificultad y tiempo del ataque a ejecutarse al objeto
RQ12	Se requiere conocer herramientas para la ejecución y creación de ataques (códigos maliciosos, virus, ficheros malintencionados, entre otros)

RQ13	Se pretende examinar los entornos, sistemas o dispositivos enlazados de la red, de tal forma para escalar privilegio y tener control por las pruebas de penetración
RQ14	Basado a la realización de la fase de evaluación se debe recolectar la información para el desarrollo informe preliminar.
RQ15	Se requiere estructurar el informe preliminar con los datos de la institución, objetivo, alcance, clasificación del nivel de riesgo, entre otras.
RQ16	Contar con un análisis e interpretación de los datos recolectados en la prueba de penetración y presentar observaciones.

3.2. COMPONENTE DE LA PROPUESTA

FASE 1- PREPARACIÓN

Comprende en la obtención de la información muy relevante y concisa de la institución para el desarrollo investigativo. Así como también contar con el permiso para ejercer la práctica. El diagnóstico de vulnerabilidades y amenazas de la red informática que no debe ser comprometida y divulgada. Uno de los primeros puntos a desarrollar de la fase fue la realización de entrevista al encargado del departamento TI, para recolectar datos esenciales sobre la situación actual de la institución referente a las amenazas y vulnerabilidades que son presentados en la tecnología evolutiva (Anexo 3).

La recopilación de datos de la topología de la red, mediante la observación como técnicas de datos, identificación de equipos físicos que se encuentra conectado en la propia red. Adicional se utilizó la herramienta Advanced Ip Scanner para tener el número de dispositivos activos de la red (Anexo 4).

RESULTADO	
Red Principal	190.152.215.85
Topología	Anillo
Red distrital	192.168.5.0/24
Red interna	10.2.98.0./24
DNS preferido	192.168.21.20
DNS alternativo	192.168.21.21
Departamentos	4 unidades
Vlans Administrativas	Si
Servidor	Si
Acceso Remoto	Si

Tabla 1. Datos obtenidos de entrevista

Por otro lado, al contar con la información, también se cuenta con un análisis de las amenazas de las redes informáticas modernas, para tener en claro que tan impactante puede ser la amenazas, como vulnerarlas con diversos tipos de ataques, y entre otros aspectos que será crucial para el desarrollo de la siguiente fase de la metodología de desarrollo OSSTMM. A continuación, se muestra las herramientas empleadas en la primera fase.

HERRAMIENTAS	DESCRIPCIÓN	VENTAJAS	OBJETIVO	NIVEL DE ANÁLISIS

NESSUS	Es un administrador de vulnerabilidades más implementado debido a que ayuda a detecta la superficie de ataques en una organización.	Identifica las vulnerabilidades que necesitan atención con un escaneo preciso de alta velocidad	Reconocimiento exhaustivo de la red 10.2.98.1-255/24	MEDIO
NMAP	Es una herramienta de código abierto utilizada para la exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes.	Permite conocer los puertos abiertos de la red, con sus respectivos nombres y estados.	Analizar la red, para determinar los puertos, el estado, nombre del servicio y versión del mismo	ALTO
MASSCAN	Es una herramienta que permite escanear puertos de una red de datos.	Utiliza técnicas complejas y exhaustivas, se enfoca en escaneo asincrónico.	Escaneo completo de red de datos, para su comparación con otras herramientas	MEDIO
ARP-SCAN		Se realiza de forma muy		MEDIO

	Identifica los hosts conectados a la red de datos.	rápida para entornos con diversos dispositivos.	Identificar las IP conectadas a la red.	
ADVANCED IP SCANN	Escáner de red que identifica los hosts conectados con sus respectivas MAC.	Permite conocer las direcciones MAC de cada dispositivo conectado a la red.	Identificar las MAC de los dispositivos conectados a la red.	MEDIO
NETWORK MINER	Es utilizada para realizar ataques de Man-In-The-Middle, permite leer archivos de otras herramientas.	Analiza la captura de datos de manera activa como pasiva.	Analizar y capturar datos de los sistemas informático	ALTO
WIRESHARK	Analizador de protocolos de red que permite revisar lo que sucede en su red a un nivel microscópico. [12]	Permite capturar datos que se transportan en la red de datos, de manera sigilosa.	Capturar datos de la red, para identificar datos sensibles.	ALTO
				ALTO

METASPLOIT	Es un marco de código abierto que utilizan los profesionales de la seguridad de la información y los ciberdelincuentes para encontrar, explotar las vulnerabilidades del sistema	Permite realizar pruebas de seguridad en entornos reales y controlados.	Creación de virus informático, para evaluar el nivel de seguridad de los dispositivos de la institución.	

Tabla 2. Herramientas utilizadas

FASE II – INTERACCIÓN

Comprende en la recuperación de datos esenciales mediante el reconocimiento de la red a través de herramientas especiales que tienen como objetivo presentar datos de manera masiva sobre el contexto del hacking ético, y pruebas de intrusión.

Por ende, para ello se tomaron en cuenta herramientas de análisis de seguridad de red como Nmap, Nessus, Advanced Ip Scanner, masscan, arp-scan para la recopilación de datos como; hosts activos, descubrimientos de puertos abiertos, dispositivos conectados, servicios, todo referente a la infraestructura de la red de estudio.

Además, mediante nmap y crackmapexec se involucró un poco la indagación de encontrar máquinas vulnerables y servicios de ejecución para la prueba de penetración y lograr comprometer.

Ejecución de herramienta Nmap

El uso de la herramienta en cuestión permite escanear direcciones Ip y puerto sobre una red para obtener información crucial, para posteriormente controlar y lograr gestionar una seguridad. Para el reconocimiento de dispositivos conectados en la red se estableció el siguiente comando **"nmap –sn 10.2.98.0/24"** llegando obtener como resultado un total

de 42 dispositivos en posesión de la red con la información de la Mac, latencia y modelo (Ver anexo: Descubrimiento Nmap Ima2-Ima14)

Además, se realizó el descubrimiento de puertos y servicios sobre los 42 dispositivos en cuestión de la red (Ver anexo: Puertos, servicios y versiones)

Y para finalizar el desarrollo de ejecución de la herramienta, se estableció la indagación sobre máquinas vulnerables con el siguiente comando **"nmap –script "vuln and safe" –p445 dirección Ip"** llegando a encontrar de los 42 dispositivos 5 direcciones vulnerables al eternalblue - CVE-2017-0143 (Ver anexo: Máquinas Vulnerables)

Ejecución de herramienta Nessus

Esta herramienta se utiliza en prácticas de pruebas de penetración debido a que nos va a permitir escanear posibles vulnerabilidades encontradas en distintos sistemas operativos de la red. (Ver anexo: Análisis Nessus)

Ejecución de masscan

Herramienta de código abierto con la cual se realizó escaneo de posibles puertos abiertos dentro de la red de forma eficiente y rápida.

Comando por utilizar: masscan -p80 10.2.x.x/24c (Ver anexo: Masscan)

Ejecución de arp-scan

Herramienta implementada para descubrir dispositivos activos en la red mediante un envío de consultas ARP que dan como resultado direcciones MAC.

Comando ejecutado: arp-scan -I eth0 –localnet (Ver anexo: arp–scan)

Ejecución de Advanced Ip Scanner

La ejecución de la herramienta permite descubrir todos los dispositivos conectados a la red, computadoras, impresoras, cámara, Ip, enrutadores, servidores, entre otros. También dar la información detallada de direcciones Ip, nombre del host, fabricante del dispositivo, dirección MAC, nombre del equipo, datos relevantes. (Ver anexo: Ip Scanner)

Ejecución de crackmapexec

La ejecución de la herramienta permite escanear y enumerar toda la red para obtener la información de usuarios, grupos, recursos compartidos, políticas de seguridad, entre otros, para ejercer el análisis de vulnerabilidades y explotar sistemas Windows en entornos de la red. Como resultado se encontró 21 dispositivos en relación con SAMBA, dominio, y versiones de Windows en uso (Ver anexo: Crackmapexec)

FASE III – INVESTIGACIÓN

ANÁLISIS DE AMENAZAS CÓMUNES SOBRE REDES INFORMÁTICAS

AMENAZAS	OBJETIVO	TIPOS	EXPLOTACIÓN	NIVEL DE CRITICIDAD
INTERPRETACIÓN	Leer la ruta de datos, leer la red y supervisar el tráfico	• Captura de tráfico por Wireshark • Inyección de comandos • Inyección de código	Análisis de tráfico de red y protocolos de servicios	MEDIO
SUPLANTACION DE IDENTIDAD E INGENIERIA SOCIAL	Comprometer la seguridad de la información personal y realizar acciones malintencionadas	• Phishing por correo • Clonación de sitio • SMS falsos • Spear phishing	Entorno inseguro (HTTP)	ALTO

MAN IN THE MIDDLE	Redirigir la comunicación y analizarel tráfico de datos	• ARP Spoofing • Envenenamientode Caché DNS • Ataque de Wifi • Ataque de enrutamiento BGP	Protocolo WEP/WPA2	ALTO
MALWARE	Comprometer el objetivo y escalar privilegio para obtenerdatos	• Virus • Gusanos • Troyanos • Spyware	Crear virus mfsconsole	ALTO
ACCESO NO AUTORIZADO	Obtener acceso a sistemas o informaciónsin permiso	• Fuerza bruta • Explotación de vulnerabilidades • Robo de credenciales	• Ataque de diccionario • Recopilación de Cookie	MEDIO
DEBILIDAD EN SISTEMAS OPERATIVOS	Aprovechar los erroresde seguridad y configuraciones incorrectas para tener acceso no autorizado	• Exploits • Escalas de privilegio • Ejecución remota de código • Inyección de código	• Reverse_Shell • Desarrollo de ficheros maliciosos	MEDIO

Tabla 3. Amenazas de seguridad comunes [71]

ANÁLISIS DE VULNERABILIDADES DE AMENAZAS CÓMUNES EN REDES

NOMBRE	VENTAJAS	DESVENTAJAS	SISTEMAS	IMPACTO	CRITICIDAD
INYECCIÓN DE CÓDIGO	Se desarrolla la manipulación de configuraciones de seguridad para acceder a la información mediante código anómalos para ser camuflados y direccionado al objetivo del sistema como lo es el servidor, formulario web, database, entre otros	Se requiere de conocimiento técnico de desarrollo y programación para emplear el análisis del entorno a doblegar, debido a que diversos sistemas pueden contar con parametrización de procesos, políticas y tener estrategias alternas para instruir es clave	Entorno web Sistemas Operativos	Revisión de confidencialidad de usuarios potente	MEDIO

PHISHING	Está directamente relacionado en engañar para obtener acceso no autorizado a datos confidenciales con el uso técnico de camuflar correos, sitios web, formularios para extraer lo desea sin que la víctima sepa	Debido a ser un ataque común en instituciones la seguridad es correspondido, por ello se requiere de ideas para doblegar la seguridad y saltar la seguridad	Navegadores Correo Electrónico	Contraseñas de usuarios potenciales y datos financieros, entre otros activos valiosos	ALTO
ATAQUE DE HOMBRE EN EL MEDIO	Comprende en el uso constante de un punto de acceso a red para ejercer la manipulación del medio y lograr interceptar el tráfico y encontrar datos importantes en acción.	Pueden ser detectados por los administradores de sistemas, y así mismo no siempre es efectivo debido a que si la red en donde se comunica se encuentra cifrada en complejo, que el atacante pueda leer o	Redes Inalámbricas	Red de comunicación	ALTO

		modificar los datos que se transmiten			
INFECCIÓN DE MALWARE	Es un proceso estrictamente complejo debido a que se requiere de desarrollo de un software malicioso para ejercer la manipulación, control y dañar el sistema objeto para así robar datos considerables.	Debido a su complejidad puede contar con el riesgo de ser detectado si este deja rastros y precisamente puede ser eliminado inmediatamente y otra es el riesgo al fracaso si no cumple lo establecido	Servidores Sistemas operativos Red	Bloquear acceso a datos y dañar sistemas	ALTO
ACCESO NO AUTORIZADO	Permite el acceso a sistemas de información de una red sin la necesidad de tener la autorización pertinente, en pocas palabras sobrepasar la seguridad y ejercer el robo	Riesgo de ser detectado y rastreado	Gestores administrativos como base de datos, correo, mensajería	Credenciales de usuarios	MEDIO

	de datos esenciales y privados				
CONFIGURACIÓN ERRÓNEA DE SEGURIDAD	Tras la falta de seguridad o la incorrecta se proporciona la eminente utilización de códigos anómalos, virus informáticos, bots de ataques, entre otros, para comprometer el sistema y robar información crucial.	Riesgo de ser detectado y rastreado	• Firewalls • Servidores web • Gestores de data base	Desactualización de parches de seguridad y actualización de servicios y sistemas operativos	MEDIO

Tabla 4. Análisis de vulnerabilidades de amenazas comunes en redes

FASE IV- INTERVENCIÓN

ACCIÓN	TÉCNICA	ATAQUE	DESCRIPCIÓN	RESULTADO	RIESGO	DETALLE
#1	Fuzz Testing	MAIN IN THE MIDLE	Interceptar y ejercer la posible modificación de una de las dos partes sin que se den cuenta.	Hallar protocolos y host de enviados de datos y de recibido	**MEDIO**	**Ejecución 1**
#2	Fuzz Testing	NETWORKMINER	Examinar el tráfico de la red en tiempo real	Extracción de archivos, host, imágenes, credenciales	**MEDIO**	**Ejecución 2**
#3	Prueba de Penetración	SAMBA RELAY	Aprovechar vulnerabilidad de autenticación que ejecuten servicio de Samba	Capturar hash por protocolo NTLMv2	**MEDIO**	**Ejecución 3**

#4	Prueba de Penetración	FUERZA BRUTA	Descubrir contraseñas, usuarios, claves de acceso por combinaciones hasta encontrar la correcta	Contraseñas descifradas por diccionarios	**MEDIO**	**Ejecución 4**
#5	Explotaciones de Vulnerabilidades	MALWARE VIRUS	Infectar sistemas con software malicioso	Robo de información	**ALTA**	**Ejecución 5**
#6	Explotación de vulnerabilidades	MALWARE BACKDOOR	Ejercer una puerta trasera para tener acceso no autorizado	Robo de información	**ALTA**	**Ejecución 6**

Tabla 5. Fase intervención

V. REPORTE

Luego de ejercer las fases anteriores y emplear la recolección de resultados en la red y ejecución de pruebas para comprometer el objeto de la fase intervención. Se comienza a realizar el reporte correspondiente en donde separa cada técnica desarrollada, prueba, intrusión, resultado, objetivo, evaluación, observaciones y recomendaciones. (Ver Reporte).

INFORMACIÓN GENERAL			
NOMBRE	REPORTE DE RESULTADOS		
FECHA	20 DE JULIO 2023		
AUTOR	MAYERLI TORRES LARA		
ORGANIZACIÓN	MIES – MINISTERIO DE INCLUSIÓN SOCIAL Y ECONÓMICA		
OBJETO DE ESTUDIO	INFRAESTRUCTURA DE LA RED INFORMÁTICA		
RESUMEN			
PROCESOS	**DESCRIPCIÓN**	**RESULTADOS**	**DETALLE**
ESCANEO DE RED	Uso de herramientas para explorar la topología de red.	Identificación de puertos y servicios abiertos.	Puerto 80: HTTP - Puerto 443: HTTPS - Puerto 25: SMTP - Puerto 139: SMB - Puerto 445: SMB - Se identificó que el servicio SMB estaba expuesto a la red pública,

			representando un riesgo de seguridad.
FUZZ TESTING	Se realizo pruebas de fuzzing para evaluar la resistencia de los servicios informáticos a entradas no válidas.	- Identificación de vulnerabilidades significativas en servicios informáticos.	- Se llevaron a cabo pruebas exhaustivas de fuzzing, revelando vulnerabilidades críticas en la seguridad de los servicios informáticos.
EXPLOTACIÓN DE VULNERABILIDAD	Utilización de exploits para aprovechar vulnerabilidades previamente identificadas.	Se logró obtener toma de control de dispositivos informática a través la creación de virus para doblegar la seguridad	Se destaca la importancia de corregir de inmediato las vulnerabilidades explotadas para prevenir accesos no autorizados y pérdida de datos.
ACCESO NO AUTORIZADO	Evaluación de la resistencia de las cuentas de usuario a ataques de fuerza bruta y otros métodos de acceso no autorizado.	Se logró obtener acceso no autorizado a la red interna mediante un ataque de fuerza bruta.	Se incita a mejorar las políticas de contraseñas y la implementación de medidas adicionales de seguridad para evitar accesos no autorizados.

DEBILIDAD EN SISTEMAS OPERATIVOS	- Identificación de sistemas operativos desactualizados y susceptibles a vulnerabilidades conocidas.	-Se detectó que los sistemas operativos de los servidores están desactualizados.	- Se recomienda realizar actualizaciones inmediatas para fortalecer la seguridad de los sistemas operativos y prevenir ataques potenciales.

Tabla 6. Ficha técnica

3.3. GUÍA DE BUENAS PRÁCTICAS

11.

CONTROLES DE SEGURIDAD

CONTROL	DESCRIPCIÓN
Política de seguridad de la información	Se establece una política de seguridad de la información, donde se organizan las directrices generales para la gestión de la seguridad de la información
Organización de la seguridad de la información	En este control se centra la organización de información en la institución, se define roles y responsabilidades.
Gestión de activos	Se basa en gestión de activos de información de la institución, incluye inventario, propiedad y clasificación de la información

Seguridad de recursos humanos	Se centra en la seguridad de los recursos humanos presentes en la organización, tales como la contratación, formación y concienciación de la seguridad de la información.
Seguridad física y del entorno	Se basa en la seguridad de la infraestructura, incluyendo un control de acceso a personas autorizadas.
Gestión de comunicaciones y operaciones	Gestiona las comunicaciones, red y servicios a terceros.
Control de accesos	Se centra en el control de acceso a la información de la institución, autenticación, y autorización
Adquisición, desarrollo y mantenimiento de sistemas de información	Se basa en la seguridad de adquisiciones, desarrollo y mantenimientos de los sistemas informáticos.
Gestión de incidentes de seguridad de la información	Seguridad de la información, identifica, evalúa y da respuesta a los incidentes de seguridad de la información
Gestión de la continuidad del negocio	Incluye la planificación y preparación para la recuperación en caso de interrupciones.

Conformidad	Conformidad con requisitos legales, políticas internas y compromisos institucionales.
Gestión de la seguridad de la información de terceros	Se encarga de garantizar la información compartida con terceros.
Seguridad de las comunicaciones	Se centra en la seguridad de las comunicaciones electrónicas, protección de información compartida en redes públicas.
Operaciones de la seguridad	Se realizan auditorias y revisiones de seguridad de la información.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

RESPONSABILIDAD DEL USUARIO Y CONCEPTOS GENERALES

- Los sistemas informáticos utilizados por la institución deben garantizar la privacidad de la información,
- Los sistemas informáticos deben ser utilizados con prudencia para cumplir objetivos.
- La seguridad de la información no solo es tarea de los administradores.
- El acceso a los sistemas debe ser controlado y autorizado, mediante autenticación.
- Garantizar el correcto funcionamiento de sistemas informáticos, manteniendo así la disponibilidad, integridad, confidencialidad y autenticación.
- Sancionar a los trabajadores que utilicen los sistemas informáticos y equipos físicos de forma incorrecta.

SEGURIDAD FÍSICA Y LÓGICA

SEGURIDAD FÍSICA	RECOMENDACIONES
Equipamiento	• Los equipos informáticos de la institución deben ser utilizados para fines institucionales, no para pasatiempos. • Deben recibir mantenimiento preventivo concurrente para garantizar el correcto funcionamiento de estos. • Ante cualquier perdida o destrucción de hardware debe ser informado al departamento de TICS • Prohibir la ingesta de alimentos en centros de control o en estación de trabajo. • Colocar contraseñas en equipos como Pc, Laptops para evitar acceso de personas no autorizadas a los equipos. • Comunicar a los encargados de sistemas si algún equipo presenta fallas, se recomienda hacerlo desde el momento que causa molestias
Cableado	• Mantener una correcta instalación eléctrica, con moduladores de energía, para evitar el agravio de los equipos electrónicos por cortes de luz, o diferencia de voltaje. • Realizar mantenimientos preventivos y correctivos. • Etiquetar los cables de red. • Revisar frecuentemente los conectores Rj45.

SEGURIDAD LÓGICA

Aspectos generales

- Las estaciones de trabajo deben estar bloqueadas, con sus respectivas contraseñas.
- Las cuentas de personas que ya no prestan sus servicios en la institución deben ser desactivadas.
- Las contraseñas deben ser cambiadas mínimas cada dos meses
- Limitar acceso de archivos y programas.
- Instalación de aplicaciones, archivos.
- Revisar los permisos solicitados antes de la instalación de un programa.
- Establecer sistemas alternativos para enviar información en caso de que el sistema principal falle.
- Se debe mantener la privacidad, autenticación, disponibilidad e integración de la información.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

ORGANIZACIÓN	RECOMENDACIÓN
FUNCIÓN Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN	• Se debe definir los roles y responsabilidades de cada empleado. • Dar acceso a información que necesita el usuario, dependiendo de su rol asignado. • Clasificar la información según su nivel de confidencialidad.
SEGREGACIÓN DE TAREAS	• Evitar el uso incorrecto de los sistemas informáticos. • Evitar el acceso no autorizado a programas externos, o sistemas informáticos no perteneciente al rol asignado

	• Designar perfiles a los usuarios. • Designar tareas específicas a cada usuario.
CONTACTO CON LAS AUTORIDADES	• Se basa en caso la información se vea comprometida, mantener la comunicación con las autoridades de la institución para buscar una solución. • Este control puede ser implementado en todo tipo de institución desde la pequeña hasta la más grande.
SEGURIDAD DE LA INFORMACIÓN EN PROYECTOS	• Se debe considerar la seguridad de la información en todos los proyectos que se realicen. • Garantizar la integridad de la información. • Garantizar la disponibilidad de la información, cuando los gestores del proyecto la necesiten. • Garantizar la autenticación para el acceso de información, según su clasificación y el perfil asignado al usuario. • Garantizar la seguridad y evitar que la información se filtre a personas no autorizadas

SEGURIDAD DE LOS ACTIVOS

CONTROL	**RECOMENDACIÓN**
Inventario de activos	• Identificar la cantidad de activos presentes en la institución. • Clasificar los activos según su funcionalidad.

	• Clasificar los activos según su importancia- • Clasificar los activos basados en información.
Propiedad de los activos	• El dueño del activo no es solo quien lo creo o el propietario, es quien tiene responsabilidades sobre este. • Definir periódicamente las restricciones de acceso. • Se clasifica teniendo en cuenta la política de control de acceso. • Garantizar la manipulación del activo cuando este es eliminado o destruido.
Uso aceptable de los activos	• Se debe realizar un informe sobre el uso correcto de los activos, es importante describir los requisitos de seguridad de estos. • Se debe capacitar a los usuarios sobre el uso correcto de los activos.
Devolución de los activos	• Este control es utilizado por varios ejes de la institución, cuando finaliza el contrato del activo.
Clasificación de la información	• Se debe clasificar según la importancia. • Se clasifica según su fecha de creación o modificación. • Se clasifica en 4 niveles, nivel 0,1,2,3-
Etiquetado de la información	• La información debe ser etiquetada según su nivel de importancia establecida en el control anterior.

	• Se debe etiquetar la información ya sea en estado físico o electrónico. • Las etiquetas deben ofrecer simplicidad y ser entendibles.
Manipulación de soportes	• Proteger la información, tanto en papel o medios de almacenamiento extraíbles

CONTROL DE ACCESO

Tiene como objetivo requisitos de negocio para el control de acceso y gestión de acceso de usuarios.

CONTROL	**RECOMENDACIONES**
Política de control de acceso	• Establecer, documentar y revisar las políticas de acceso y control. • Asignar privilegios según los perfiles. • Asignar tiempo a los privilegios dados. • Asignar roles
Gestión de acceso a los usuarios en red	• Gestionar la autorización de los usuarios que accedan a diversos servicios en la red informática. • Gestionar requisitos de autenticación y supervisar el uso. • Implementar un sistema de identificación. • Establecer autenticación en los sistemas. • Red y servicios al que usuario accede. • Medios por el cual el usuario accede.
	• Generar un registro Ids, o de cuentas de usuario, donde este se identifique.

Registro de usuarios y cancelación del registro	• Los Ids o cuentas de usuarios deben desactivarse una vez que el usuario deje la organización. • Controlar la creación de usuarios, para no cometer errores de redundancia. • Mantener un proceso de cancelación de cuenta.
Gestión de acceso a los usuarios	• Debe ser autorizado por las máximas autoridades de la institución. • Toda nueva cuenta creada debe cumplir con las políticas de acceso definidas por la institución. • Modificar los accesos y privilegios a personas que han cambiado de estación de trabajo. • El acceso a nuevos usuarios debe completarse una vez que el periodo de autorización haya concluido.
Gestión de derechos de acceso privilegiados	• Deben identificarse cada acceso privilegiado de los sistemas. • Se debe establecer normas de caducidad.
Gestión de derechos de acceso privilegiados	• Verificar las competencias de cada usuario. • Definir diferentes ID, para cuentas con accesos privilegiados. • Utilizar técnicas para mantener la confidencialidad de información de los usuarios-

	• Reforzar el mecanismo de cambio de contraseñas.
Gestión de la información de autenticación secreta de los usuarios	• Cambio obligatorio cambiar contraseñas después de su primer uso. • Los contratos deben incluir cláusulas importantes sobre la confidencialidad. • Utilización de medios seguros de comunicación. • Cifrar datos • Cambiar contraseñas en un determinado periodo. • Emplear diferentes técnicas de autenticación.

SEGURIDAD DE LAS COMUNICACIONES

CONTROL	RECOMENDACIÓN
Controles de red	• Designar responsabilidades dentro de la red. • Gestionar elementos físicos y dar soporte en la red. • Se debe considerar controlar la transmisión de datos. • Debe considerarse la disponibilidad y confidencialidad de la información, sin importar el tipo de red que se esté utilizando.

	• Control de acceso, control de privilegios y monitoreo de red deben ser fundamentales en esta sección.
Seguridad de los servicios de red	• Se deben definir requisitos de calidad y seguridad, sin importar el servicio de red. • Con auditorias de calidad de servicio es el único modo que se puede tener visibilidad sobre la disponibilidad de la red.
Separación en redes	• Acceso restringido a la red. • Subdivisión de redes. • Mantener dominios activos.
Políticas y procedimiento de intercambio de información	• Establecer medios de transmisión. • Almacenamiento externo • Almacenamiento en la nube • Respaldo de la información. • Uso de encriptación de datos al intercambiar información dentro y fuera de la red.
Acuerdos de intercambios de información	• Compartir responsabilidad en protección y custodia de la información. • Controles de acceso a la información • Requisitos de cifrado. • Cumplir las normas técnicas y legales.
Mensajería electrónica	• Protección de accesos no autorizados- • Confiabilidad y disponibilidad del servicio. • Firmas digitales.

	• Autorización para la utilización de servicios.
Acuerdos de confidencialidad	• Importancia de la información. • Nivel de confidencialidad de los datos. • Duración del acuerdo. • Cláusulas de rescisión. • Derecho de autor. • Responsabilidades. • Confidencialidad de los procesos. • Autenticación, autorización y disponibilidad. • Clausulas en caso de existir infracción del acuerdo.

PRACTICA DE SEGURIDAD	RECOMENDACIONES
Disponibilidad	• Identificar los riesgos que ponen en peligro la disponibilidad de información. • Realizar respaldo de la información. • Tener acceso a la información en todo momento sin importar donde se almacene. • Utilizar firewall • Implantación de cluster en el sistema. • Proteger las conexiones de los dispositivos.
	• Cambiar las contraseñas durante un periodo determinado. • No establecer las mismas contraseñas para diferentes sistemas.

Confidencialidad	• Proteger las redes de datos. • Establecer controles de autenticación. • Asignar perfiles para dar acceso a los usuarios, a información que necesiten en su función. • Monitoreo constante de cuentas electrónicas. • Establecer contraseñas y cifrado de datos a la información considerada de alto riesgo. • Bloquear puertos que no se utilicen.
Integridad	• Realizar validaciones con base en riesgos • Tener en cuenta todas las ubicaciones donde se almacena la información. • Dar acceso solo de lectura a los usuarios, para evitar modificaciones en la información. • Seleccionar sistemas y proveedores adecuados • Se debe analizar las normas de los proveedores. • Actualizar software. • Utilizar software con licencia. • Realizar backup de la información • Utilizar VPN • Utilizar IDS. • Utilizar firma electrónica

Autenticación y no repudio	• Utilizar métodos de identificación, demostrar ser quien dice ser. • Utilizar credenciales de acceso. • Verificar si los correos son enviados por fuentes confiables. • Analizar correos sospechosos por medios de herramientas. • Bloquear páginas que realizan spam. • No abrir links sospechosos • No brindar información sensible solicitada por correos no confiables. • Crear verificación de dos pasos antes de ingresar a alguna red social o sistema de institución.

CONCLUSIONES

- Se implementó la técnica de entrevista como método integral para recopilar información, ofreciendo una visión detallada del panorama de seguridad informática de la institución en el contexto de las amenazas y vulnerabilidades asociadas a la tecnología en constante evolución. La recolección de datos proporcionó una apertura completa hacia la topología de la red, incluyendo la identificación de equipos físicos conectados, servicios y otros detalles cruciales. Este enfoque no solo reveló información valiosa sobre las estrategias de seguridad existentes, sino que también destacó aspectos relevantes para comprender el entorno tecnológico de la institución.
- La aplicación de técnicas de hacking fue esencial para descubrir puntos débiles en el sistema de seguridad. Este enfoque proactivo proporcionó información valiosa sobre vulnerabilidades existentes, permitiendo una evaluación realista del nivel de seguridad informática. Se desarrollaron

simulaciones de ataques, abarcando main the midle, networminer, samba relay, fuerza bruta, malware virus y malware backdoor. Estos escenarios ofrecieron una evaluación exhaustiva de la seguridad de la red, estableciendo una base sólida para mejoras futuras y estrategias de protección informática más robustas.

- El informe resultante se posiciona como una herramienta vital para la protección de la información. Al consolidar los datos recolectados, no solo identifica claramente las vulnerabilidades, sino que también ofrece un análisis detallado del alcance, interpretación de resultados y recomendaciones técnicas fundamentadas en referencias específicas, como Common Vulnerabilities and Exposures (CVE). Este enfoque integral proporciona una guía efectiva para la toma de decisiones informadas y la implementación de medidas correctivas.

- La propuesta de una guía de buenas prácticas emerge como un pilar esencial para potenciar la seguridad informática y de la información. Esta guía no solo señala áreas de mejora, sino que también presenta recomendaciones concretas y prácticas, configurando un sólido marco que no solo resguarda los datos, sino que también implementa mecanismos eficaces para mitigar intrusiones informáticas y fortalecer la resistencia ante posibles amenazas cibernéticas.

RECOMENDACIONES

- Implementar actualizaciones continuas en las estrategias de seguridad, tomando en cuenta las amenazas emergentes y la evolución tecnológica. Esto garantizará una postura defensiva más robusta ante nuevas vulnerabilidades.
- Regularmente realizar simulaciones de ataques como los descritos en los escenarios prácticos, manteniendo así una evaluación continua de la

resiliencia del sistema. Estas pruebas prácticas proporcionan una comprensión más profunda de las debilidades y áreas críticas de mejora.

- Siguiendo las recomendaciones detalladas en el informe, implementar medidas correctivas específicas para abordar las vulnerabilidades identificadas. Esta acción directa ayudará a cerrar brechas y fortalecer la seguridad en áreas específicas.
- Considerar la adopción de prácticas y controles establecidos en la norma ISO 27001 para la gestión de la seguridad de la información. Esta norma proporciona un marco reconocido internacionalmente que facilita la implementación de un sistema de gestión de seguridad efectivo.
- Promover una cultura de seguridad dentro de la organización, donde la conciencia y las mejores prácticas se integren en las operaciones diarias. Esto involucra a todos los niveles de la organización en la responsabilidad de la seguridad de la información.

REFERENCIAS

[1] «Kasperskuy,» Hernan Diazgranados, 19 01 2022. [En línea]. Available: https://latam.kaspersky.com/blog/el-ransomware-dirigido-a-empresas-aumenta-mas-de-un-200-en-latinoamerica/23784/. [Último acceso: 15 11 2022].

[2] M. Micucci, «welivesecurity,» 12 junio 2023. [En línea]. Available: https://www.welivesecurity.com/la-es/2023/01/12/vulnerabilidades-reportadas-2022-aumentaron-record-historico/.

[3] M. Micucci, «welivesecurity,» 12 junio 2023. [En línea]. Available: https://www.welivesecurity.com/la-es/2023/01/12/vulnerabilidades-reportadas-2022-aumentaron-record-historico/.

[4] «Gobierno del Ecuador,» [En línea]. Available: https://www.inclusion.gob.ec/.

[5] E. S. Gallardo, «Revista Seguridad,» Mayo 2018. [En línea]. Available: https://revista.seguridad.unam.mx/print/2192. [Último acceso: 2022].

[6] M. Torres, «METODOS DE RECOLECCION DE DATOS PARA UNA INVESTIGACIÓN,» [En línea]. Available: https://fgsalazar.net/LANDIVAR/ING-PRIMERO/boletin03/URL_03_BAS01.pdf. [Último acceso: 11 2022].

[7] M. I. R. Castro, «ÁREA DE INNOVACIÓN Y DESARROLLO, S.L.,» 10 2018. [En línea]. Available: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf. [Último acceso: 11 2022].

[8] L. M. T. Romero, «Ingeniería de Seguridad y Auditoría Informática,» febrero 2020. [En línea]. Available: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/3095/Luis%20Tovar_Trabajo%20de%20Suficiencia%20Profesional_Titulo%20Profesional_2020.pdf?sequence=1&isAllowed=y. [Último acceso: noiembre 2022].

[9] K. A. Pintado, «Universidad Politecnica Salesiana,» Abril 2015. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/10349/1/UPS-GT001276.pdf. [Último acceso: Noviembre 2022].

[10] A. L. C. ORRALA, «INGENIERA EN TECNOLOGÍAS DE LA INFORMACIÓN,» 07 2022. [En línea]. Available: https://repositorio.upse.edu.ec/bitstream/46000/8646/1/UPSE-TTI-2022-0030.pdf. [Último acceso: 11 2022].

[11] «Wireshark,» [En línea]. Available: https://www.wireshark.org/. [Último acceso: 22 11 2022].

[12] M. J. M. Díaz, «Hacking Etico,» 9 Abril 2009. [En línea]. Available: https://hacking-etico.com/2014/04/09/networkminer/. [Último acceso: 10 Abril 2023].

[13] «nmap.org,» [En línea]. Available: https://nmap.org/. [Último acceso: 22 Noviembre 2022].

[14] «Tenable,» [En línea]. Available: https://es-la.tenable.com/products/nessus. [Último acceso: 2022].

[15] «metasploit,» [En línea]. Available: https://www.metasploit.com/. [Último acceso: 2023].

[16] «Keecode,» 25 Mayo 2023. [En línea]. Available: https://keepcoding.io/blog/que-es-masscan-y-como-funciona/.

[17] «Ionos,» 4 septiembre 2019. [En línea]. Available: https://www.ionos.es/digitalguide/servidores/know-how/arp-resolucion-de-direcciones-en-la-red/.

[18] U. E. P. d. S. Elena, «Resolucion RCF-FST-SO-09,» No. 03-2021, La libertad, 2021.

[19] Skillnet, «IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA EN LAS EMPRESAS,» 04 Agosto 2021. [En línea]. [Último acceso: Diciembre 2022].

[20] U. Unila, «¿Por qué es importante la seguridad informática en las empresas?,» 2021. [En línea]. Available: https://www.unila.edu.mx/por-que-es-importante-seguridad-informatica/#:~:text=La%20importancia%20de%20la%20seguridad,los%20sistemas%20de%20informaci%C3%B3n%20internos.. [Último acceso: Diciembre 2022].

[21] A. N. d. l. R. d. Ecudor, «Ley Orgánica de Protección de Datos Personales, Quito,» 2021. [En línea].

[22] S. N. d. Planificación, «Plan de Creación de Oportunidades 2021-2025,Quito: Secretaría Nacional de Planificación,» 2021. [En línea].

[23] «Empresas de servicio,» 20 Mayo 2022. [En línea]. Available: https://actualicese.com/definicion-de-una-empresa-de-servicios/#:~:text=Las%20empresas%20de%20servicios%20ejecutan,sector%20terciario%20de%20la%20econom%C3%ADa.. [Último acceso: 2023].

[24] C. d. l. R. d. Ecuador, «Ley orgánica de protección de datos personales,» Quito, 2021. [En línea].

[25] J. R. Vera, «ETHICAL HACKING,» BAGUA, 2018.

[26] R. Hartley, «ResearchGate,» Diciembre 2015. [En línea].

[27] L. M. T. Romero, «HACKING ÉTICO PARA MEJORAR LA SEGURIDAD EN LA INFRAESTRUCTURA INFORMÁTICA,» Lima, 2020.

[28] E. Mifsud, «Introducción a la seguridad informática - Seguridad de la información / Seguridad informática,» 26 marzo 2012. [En línea]. Available: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1.

[29] «Unir,» 03 03 2021. [En línea]. Available: https://www.unir.net/ingenieria/revista/disponibilidad-seguridad-informatica/#:~:text=La%20disponibilidad%20de%20la%20informaci%C3%B3n,los%20individuos%20o%20personas%20autorizadas..

[30] «ISOTools,» 01 02 2018. [En línea]. Available: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/.

[31] D. A. G. S. Roberto Javier Chango Saavedra, «Salesiana,» 2023. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/24450/1/TTS1228.pdf.

[32] «CIBERSEGURIDAD,» [En línea]. Available: https://ciberseguridad.com/guias/desarrollo-seguro/osstmm/#:~:text=OSSTMM%20(Open%20Source%20Security%20Testing,evita%20suposiciones%20y%20evidencia%20anecd%C3%B3tica.. [Último acceso: 2023].

[33] «OWASP,» 12 2013. [En línea]. Available: owas.org.

[34] «Unir,» 22 11 2022. [En línea]. Available: https://ecuador.unir.net/actualidad-unir/hacking-etico/#:~:text=El%20hacking%20%C3%A9tico%20o%20pirater%C3%ADa,sean%20explotados%20por%20los%20ciberdelincuentes..

[35] L. M. Q. Valarezo, «UNIVERSIDAD TÉCNICA DE AMBATO,» Agosto 2019. [En línea]. Available: https://repositorio.uta.edu.ec/bitstream/123456789/30108/1/Tesis_t1637si.PDF. [Último acceso: Mayo 2023].

[36] J. M. M. Pérez Porto, «Definicion,» 07 Marzo 2022. [En línea]. Available: https://definicion.de/amenaza/.

[37] «Estudiario,» 30 Mayo 2023. [En línea]. Available: https://estuario.org/mitigacion/.

[38] Deloitte, «Auditoria de Gestion,» 28 Enero 2015. [En línea].

[39] «Gestión del riesgo,» Febrero 2019. [En línea]. Available: https://www.eird.org/cd/toolkit08/material/proteccion-infraestructura/gestion_de_riesgo_de_amenaza/8_gestion_de_riesgo.pdf.

[40] H. A. Ángel, «Opirani,» Octubre 2022. [En línea].

[41] Microsoft. [En línea]. Available: https://www.microsoft.com/es-ww/security/business/security-101/what-is-a-cyberattack.

[42] J. R. Lara. [En línea]. Available: https://sites.google.com/site/maestrojuanrodriguezlara/topicos-selectos/1-4-1-la-propagacion-del-lado-obscuro/1-4-1-1-amenazas-internas-y-externas.

[43] «IBM,» [En línea]. Available: https://www.ibm.com/es-es/topics/cyber-attack.

[44] Microsoft. [En línea]. Available: https://www.microsoft.com/es-ww/security/business/security-101/what-is-a-cyberattack.

[45] D. Jaimovich, «Invgate,» Octubre 2022. [En línea]. Available: https://blog.invgate.com/es/tipos-de-ciberataque.

[46] «KASPERSKY,» [En línea]. Available: https://latam.kaspersky.com/resource-center/threats/trojans.

[47] Kaspersky. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-rootkit.

[48] B. A. F. y. M. A. Mazidi, Fundamentos de seguridad de redes, McGraw-Hill Interamericana, 2014.

[49] A. Hernández, Ethical Hacking: Técnicas de seguridad ofensiva, RA-MA, 2016.

[50] J. A, Análisis y gestión de riesgos en sistemas de información, Universidad Politécnica de Madrid, 2013.

[51] R. Solms, Gestión de la seguridad de la información y ciberseguridad, Díaz de Santos, 2017.

[52] N. M. Maldonado, «Estado de la ciberseguridad en las empresas,» abril 2021. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/20243/1/UPS-GT003204.pdf. [Último acceso: 2023].

[53] «hacknoid,» Julio 2019. [En línea]. Available: https://www.hacknoid.com/hacknoid/importancia-de-la-seguridad-informatica-de-las-empresas/.

[54] C. F. C. y. P. B. L. R. H. Sampieri, Metodología de la investigación, Mexico : ISBN: 978-1-4562-2396-0, 1998.

[55] V. Gasteiz, «CyberSecurity,» Julio 2022. [En línea]. Available: https://www.ciberseguridad.eus/ciberpedia/vulnerabilidades/open-source-security-testing-methodology-manual-osstmm#:~:text=OSSTMM%20es%20el%20acr%C3%B3nimo%20de,realizar%20auditor%C3%ADas%20t%C3%A9cnicas%20de%20seguridad..

[56] MITRE, «Common Vulnerabilities and Exposures (CVE) - CVE-2018-6789,» [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6789. [Último acceso: 10 Diciembre 2023].

[57] MITRE. [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6340. [Último acceso: 10 Diciembre 2023].

[58] MITRE, «Common Vulnerabilities and Exposures (CVE) - CVE-2009-3960,» [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3960. [Último acceso: 10 Diciembre 2023].

[59] MITRE, «Common Vulnerabilities and Exposures (CVE) - cve-2014-0224,» [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0224. [Último acceso: 10 Diciembre 2023].

[60] N. N. V. Database, «NVD - CVE-2017-0144,» [En línea]. Available: https://nvd.nist.gov/vuln/detail/cve-2017-0144. [Último acceso: 2023 Diciembre 2023].

[61] MITRE, «Common Vulnerabilities and Exposures (CVE) - CVE-2020-1472,» [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472. [Último acceso: 10 Diciembre 2023].

[62] MITRE, «Common Vulnerabilities and Exposures (CVE) - CVE-2019-0708,» [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708. [Último acceso: 10 Diciembre 2023].

[63] MITRE, «Common Vulnerabilities and Exposures (CVE) - CVE-2022-1111,» [En línea]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1111. [Último acceso: 10 Diciembre 2023].

[64] N. N. V. Database, «NVD - CVE-2022-34042,» [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2022-34042. [Último acceso: 10 Diciembre 2023].

[65] N. N. V. Database, «NVD - CVE-2020-9876,» [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2020-9876. [Último acceso: 10 Diciembre 2023].

[66] N. N. V. Database, «NVD - CVE-2022-27194,» [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2022-27194. [Último acceso: 10 Diciembre 2023].

[67] N. N. V. Database, «NVD - CVE-2022-3456,» [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2022-3456. [Último acceso: 10 Diciembre 2023].

[68] N. N. V. Database, «NVD - CVE-2016-7890,» [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2016-7890. [Último acceso: 10 Diciembre 2023].

[69] N. N. V. Database, «NVD - CVE-2022-41694,» [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2022-41694.

[70] N. N. V. Database, «NVD - CVE-2022-32596,» [En línea]. Available: https://nvd.nist.gov/vuln/detail/CVE-2022-32596. [Último acceso: 10 Diciembre 2023].

[71] «Microsoft,» 23 Mayo 2022. [En línea]. Available: https://learn.microsoft.com/es-es/skypeforbusiness/plan-your-deployment/security/common-threats.

ANEXOS

ANEXOS

Anexo 1 Detección de Macro Malware en América Latina

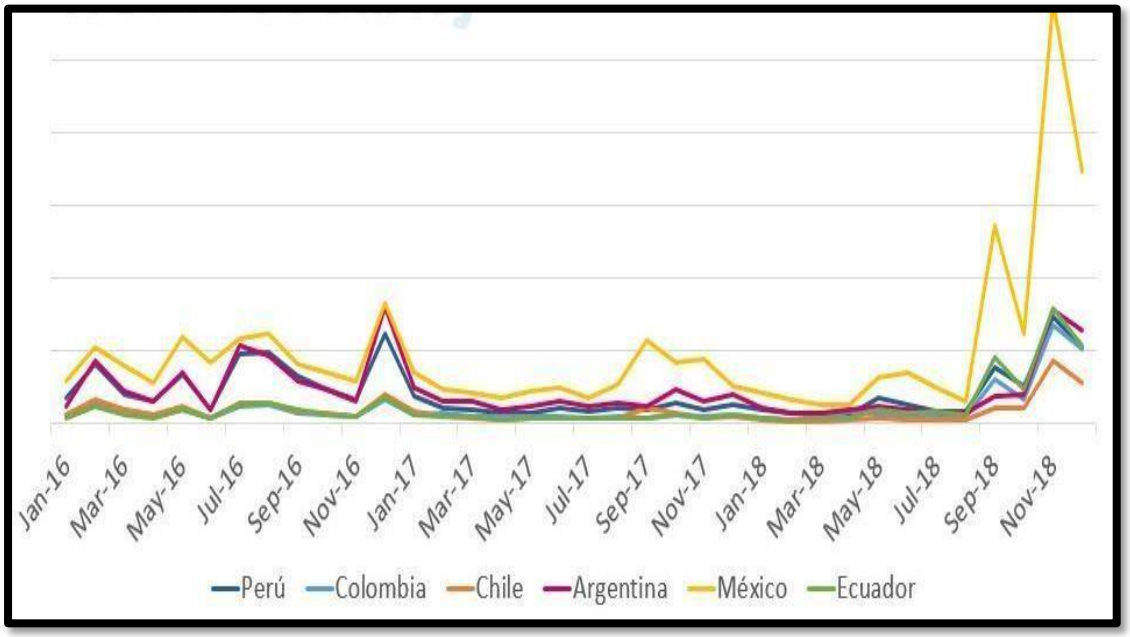


Figura 5: Fuente estadístico de Malware en Latino América

Anexo 2. Ataques Cibernéticos más frecuentes en 2021

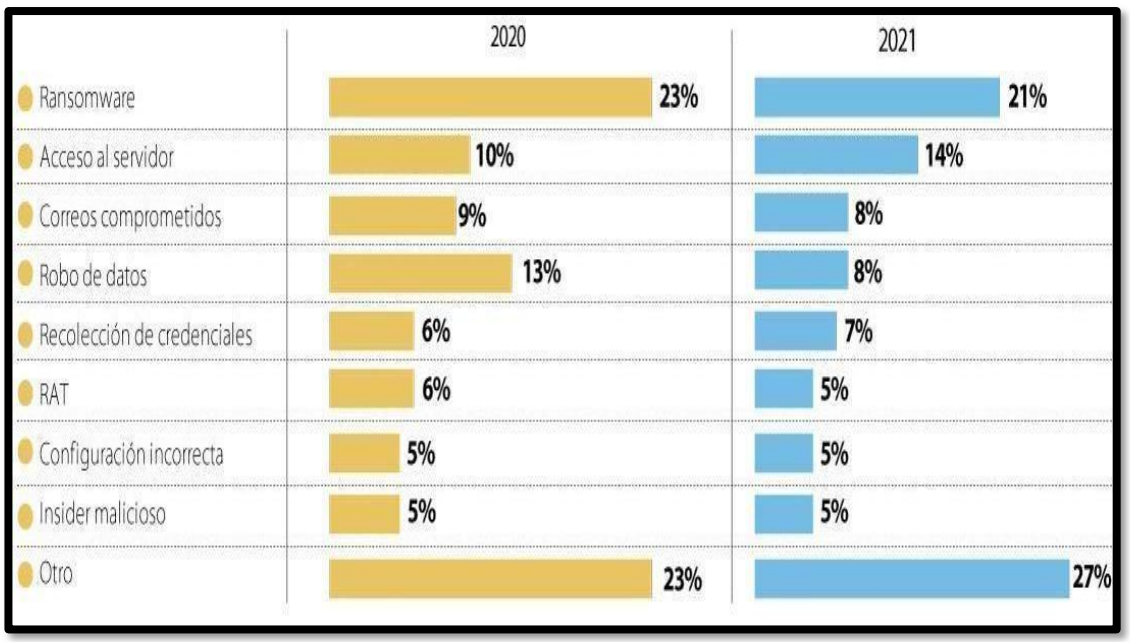


Figura 6: Ciberataques comunes en el año 2021

Anexo 3. Formato de entrevista desarrollada al director del departamento de TI – MIES – Salinas

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA FACULTAD DE SISTEMAS Y TELECOMUNICACIONES TECNOLOGÍAS DE LAINFORMACIÓN
Entrevista al Ing. José medina – director del Departamento de TI – MIES - SALINAS
Objetivo: Conocer la situación actual de la seguridad en las redes informáticas de laorganización
¿Porque es importante la seguridad informática en una institución?
la seguridad informática es considerada bueno para nuestra institución como ministerio de inclusión económica y social es un activo que se guarda con mucha seguridad aquí porquenormalmente en la institución se maneja formación bien sensible información pública quese tiene almacenada en equipos informáticos como servidores y qué en la mayoría de los casos cuente con la seguridad necesaria para que esta no pueda desvincularse de las áreas responsables y que pueda ser mal utilizada por personas externas
¿Qué tipos de herramientas y tecnologías utilizan para el análisis de la red?
Como institución utilizamos varias herramientas, primeramente los equipos están conectados a una red de dominio que tiene ciertas políticas de seguridad aparte de eso también tenemos un cortafuego a nivel nacional para protección de los paquetes de datosque se manejan a través de la red y aparte también tenemos software licenciado de seguridad que en este caso sería el antivirus que constan todos los equipos informáticos y aparte también tenemos las políticas institucionales del uso debido de acceso a los sitios de internet y acceso a la información de cada uno de los equipos informáticos

¿Cuáles son las vulnerabilidades más comunes que se enfrentan en las redes informáticas en las organizaciones?
Hablando por nuestra institución a la que no hemos visto sometido últimamente es a travésdel correo electrónico, hemos tenido demasiadas amenazas de spam es lo único que se ha monitoreado y se ha reportado a cada uno de los funcionarios, cuando recibimos esta clasede amenazas que de cierta manera cuando una persona no tiene el conocimiento necesariode lo que es y de lo que recibe se ve expuesto a esta amenaza que podría ocasionar una pequeña o gran dificultad en el manejo de la información que tiene almacenada en sus equipos de los que son custodios
¿Cuáles son las medidas de seguridad implementadas actualmente para proteger la redes informáticas de la institución?
en el caso de nosotros como distritos estamos conectados a una red institucional, nuestrasredes controladas desde planta central ya está red se han implementado ciertas seguridadesen el caso del cortafuegos sophos que tenemos implementado que maneja el tráfico de paquete de datos, el otro es el antivirus que tiene cada equipo informático que hace un antivirus con licencia y aparte las restricciones por políticas de seguridad que tenemos entodos los equipos que están conectados bajo el dominio Mies, en este caso vendría a haceresto como una de las medidas de seguridad que nosotros seamos implementado para proteger la información.
¿Como evalúa la efectividad de las medidas de seguridad implementadas y como se mantienen actualizadas ante las nuevas amenazas?
A nivel de departamento de tecnología de información ninguna medida que se pueda implementar por un corto o largo plazo es segura, porque las amenazas son recurrentes y cada vez las amenazas son nuevas porque de pronto nosotros podemos tener controladas las amenazas actuales pero de pronto desconocemos las amenazas futuras por ende se ha visto la necesidad de que en todos los equipos de la institución hayan políticas de seguridad incluso para ingresar memorias extraíbles u extraer información o ingresar información a los equipos, hay políticas que se han implementado que

conocen todos losservidores en el cual se conoce a ciencia cierta directrices que hay de lo que se puede y no se puede hacer en un equipo informático con información netamente institucional.
¿Cuál es la estrategia principal para educar y concientizar al personal de la institución sobre amenazas cibernéticas y cómo evitarlas?
Nosotros tenemos implementado un canal de mesa de servicios a nivel nacional por mediodel cual a través de lo que es el correo institucional nos llegan documentos, manuales queson como cuentas de intrusión para todo el personal y aparte de eso también recibimos constantemente boletines de lo que se debe evitar y lo que no se debe hacer en los equiposinformáticos y en los lugares a los cuales no se puede acceder en nuestra red interna, apartede eso también tenemos un control estricto por cada servidor de acuerdo a las competencias que tiene cada servidor accede solamente a páginas a nivel de red a las cuales está autorizada y las que vayan a necesitar no todo el personal tiene acceso total a información que pueda obtener de la red eso se realiza mediante niveles, estrategia y que están implementadas en las políticas de seguridad en este caso nosotros la consideramos como una manera de educar porque los servidores actualmente tienen conciencia de las amenazas que hay a través de la red y constantemente amenaza que se ve detectada en algún equipo institucional es remitida a través de correo por mesa de servicios a todos losservidores de la institución para que ellos tengan conocimiento de la amenaza presente y cuáles son mecánicos que tienen que utilizar para evitar.
¿Cuál ha sido el incidente de seguridad más significativo que ha presentado el departamento de TI y que lecciones se han aprendido del?
Hay varios eventos pero en el caso personal tengo un incidente siempre tengo presente como lección de un equipo que no tenía instalado todas las seguridades debidas y directrices de instalar un equipo no tenía todo eso y hubo en cierta ocasión de que al funcionario a través de correo le llegó un spam y ese spam ocasionarte que al abrir toda lainformación del funcionario fuera encriptado y por desacreditar la información pedían valores exorbitantes por esa razón debido a que no se pudo recuperar la información desdeahí se mantiene una de las políticas de que cada funcionario y también por parte del área de tecnología respaldar la información constantemente para que en el momento

que se presente una amenaza y por dar conocimiento del usuario que sea manejando su equipo
informático se presenta este incidente o sea poder tener protegida la información

¿Qué estándares internacionales se han aplicado a la red interna?

Hoy por cuestiones de presupuesto y por cuestiones de autoridad a nivel nacional en todaslas instituciones públicas, en estos últimos años en hemos omitido aplicar alguna seguridades con por medio de la contratación de empresas externas que se dediquen específicamente a la seguridad de las redes informáticas de instituciones públicas sin embargo hemos contado con un apoyo en nivel medio de políticas y procesos itil que de cierta manera nos han ayudado a coadyuvar ciertas amenazas de seguridad que se han presentado, bueno en mi distrito no se han presentado ninguna en estos últimos años perosí tenemos conocimiento que en otros distritos a nivel de institución sí se han presentado y para esto se ha tenido que realizar intervenciones de auditoría informática para verificarcuál sido en las falencias o la dificultad que han tenido los equipos informáticos o la persona que ha estado responsable del área de tecnología en no haber implementado
alguna de las seguridades que por exigencia de la institución.

¿Cuáles son las medidas de seguridad recomendadas que una institución pública puede implementar para proteger su red contra vulnerabilidades y amenazas?

Lo primero que tendría que ser una institución pública sería la educación de todos los servidores públicos que pertenecen a esa entidad, esa sería la primordial porque la personaque maneja el equipo informático son justamente los servidores que hacen han sido contratados previamente por las entidades públicas, sería concientizar de qué manera en las amenazas que hay a través de la red pueden afectar de una u otra forma la informaciónde la cual nosotros somos custodios porque aquí como institución nosotros tenemos que toda la información digital es como un bien intangible no tanto un bien físico sino como un bien intangible que conlleva a mucha responsabilidad, incluso nosotros tenemos aquí firmado un acuerdo de confidencialidad de toda la información que manejamos.
Es decir toda la información que está en los equipos no se la puede distribuir o no se

las puedes egresar por algún medio o dispositivo externo, entonces el concientizar eso en losservidores públicos que trabajan aquí ha sido una de las primeras normativas que hemos inculcado, la segunda es que todos debemos acostumbrarnos a las medidas de seguridad que ha implementado la institución entre ellas están las políticas que de cierta manera restringen a un funcionario el acceso a la información que se puede o no compartir de un equipo a otro o de una red a otra y aparte de eso también están las medidasde seguridad de las que planta central implementa a través de la red interna a todos los equipos de la institución esa es una de las tres cosas que hemos valorado acá.
¿Cómo evoluciona constantemente el análisis de vulnerabilidades y amenazas en el runcontexto actual de la ciberseguridad?
Como analista de tecnología de la información estoy consciente de que las vulnerabilidades ya amenazas que se presentan cada día el campo informático son mucha; sin embargo, a medida que nosotros nos vamos capacitando y experimentando más en estarama vamos buscando mecanismos y estrategias que de una u otra manera podríamos implementar o dar a conocer a nuestros inmediatos superiores para que ellos puedan con base en los recursos disponibles que tienen que una institución poderlos implementar y de esta forma poder tener medidas de seguridad que protejan la información sensible que se maneja, verdad que normalmente las amenazas que se presenta en el campo informático van apareciendo constantemente, sin embargo, la preparación y las pruebas de contingenciaque se tenga en una institución van de cierta manera ayudar a que estas vulnerabilidades y amenazas que se puedan presentar se los pueda tratar en el menor tiempo posible y con éxito para que no puedan afectar la vida

Anexo 4

Reconocimiento

Descubrimiento de dispositivos por Nmap

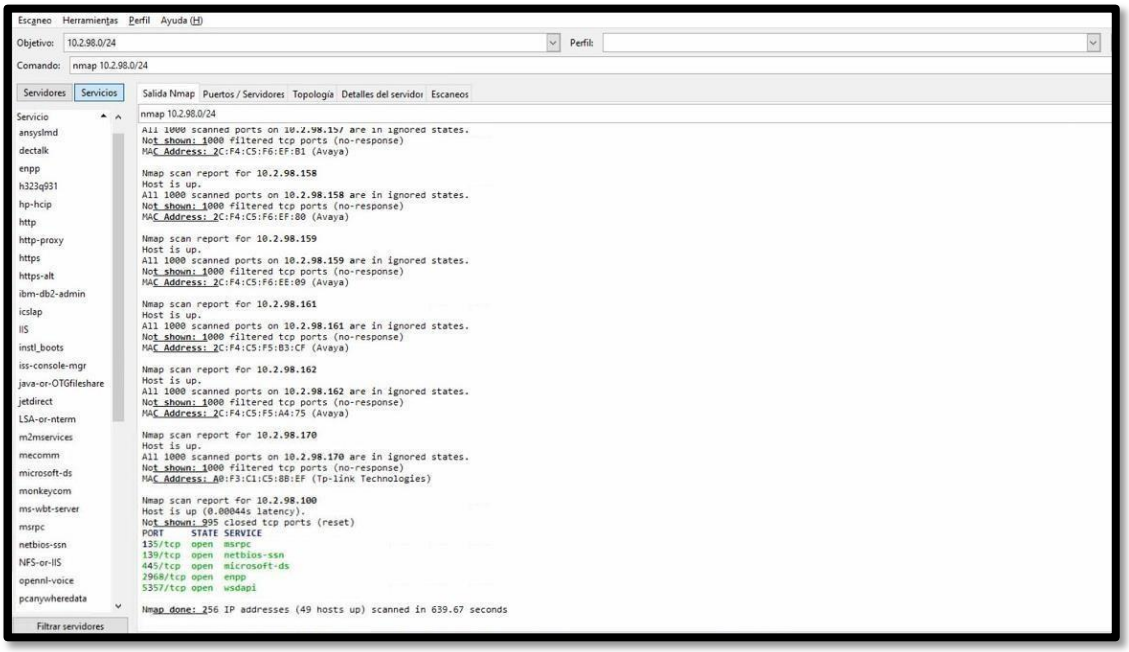


Imagen 1: Dispositivos por Nmap

Descubrimiento de puertos, servicios y versiones de los dispositivos por Nmap

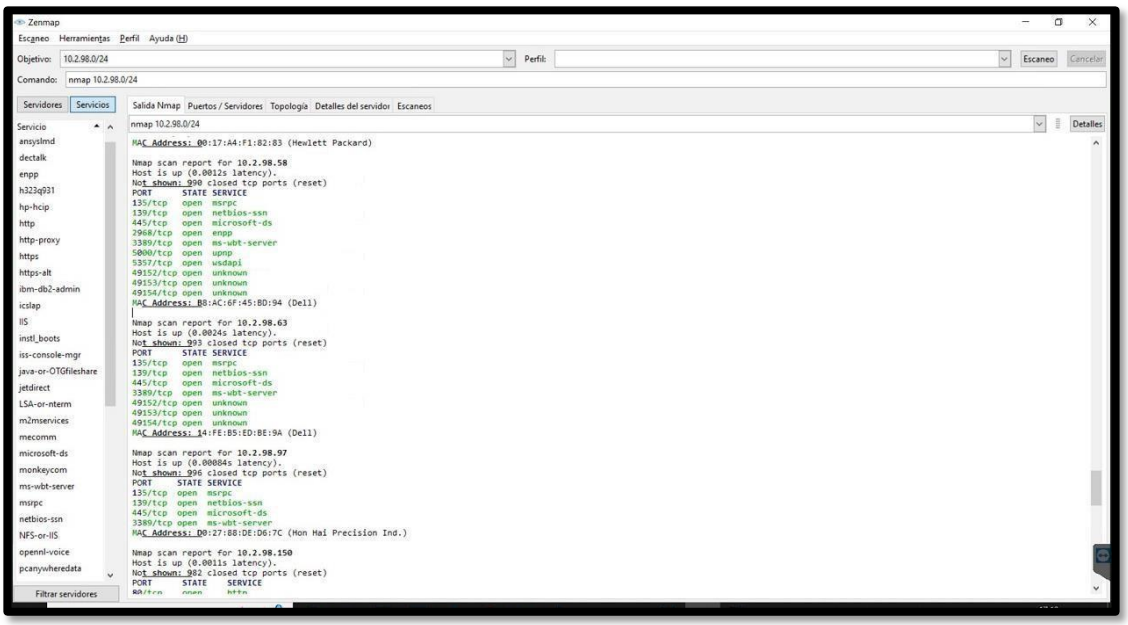


Imagen 2: Escaneo de la red Mies – Parte 1

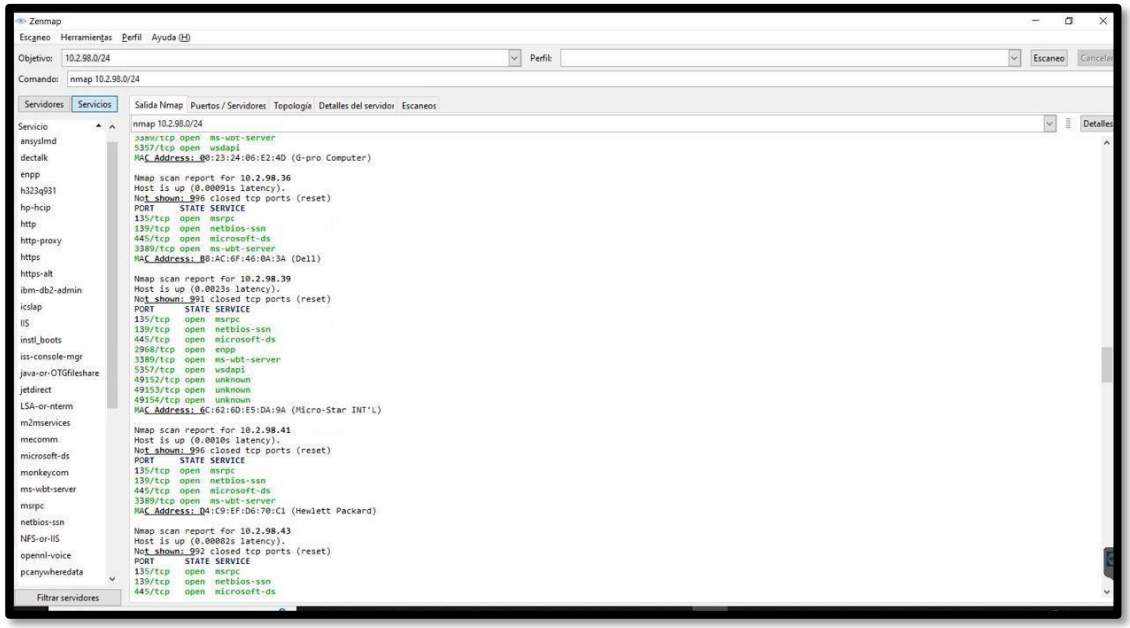


Imagen 3: Escaneo de la red Mies – Parte 2

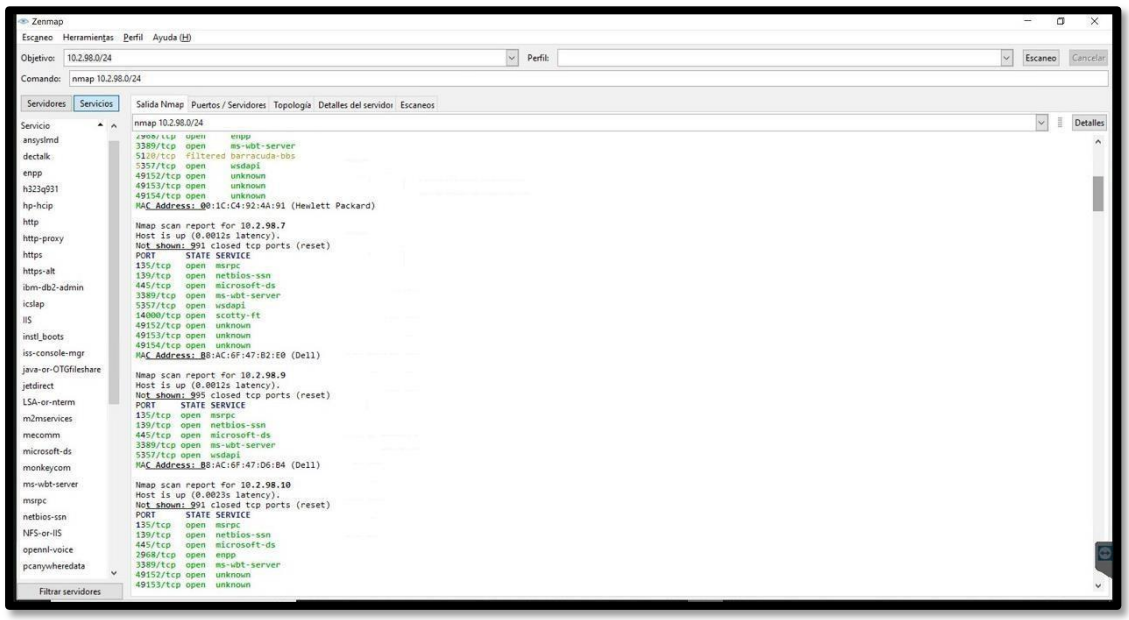


Imagen 4: Escaneo de la red Mies – Parte 3

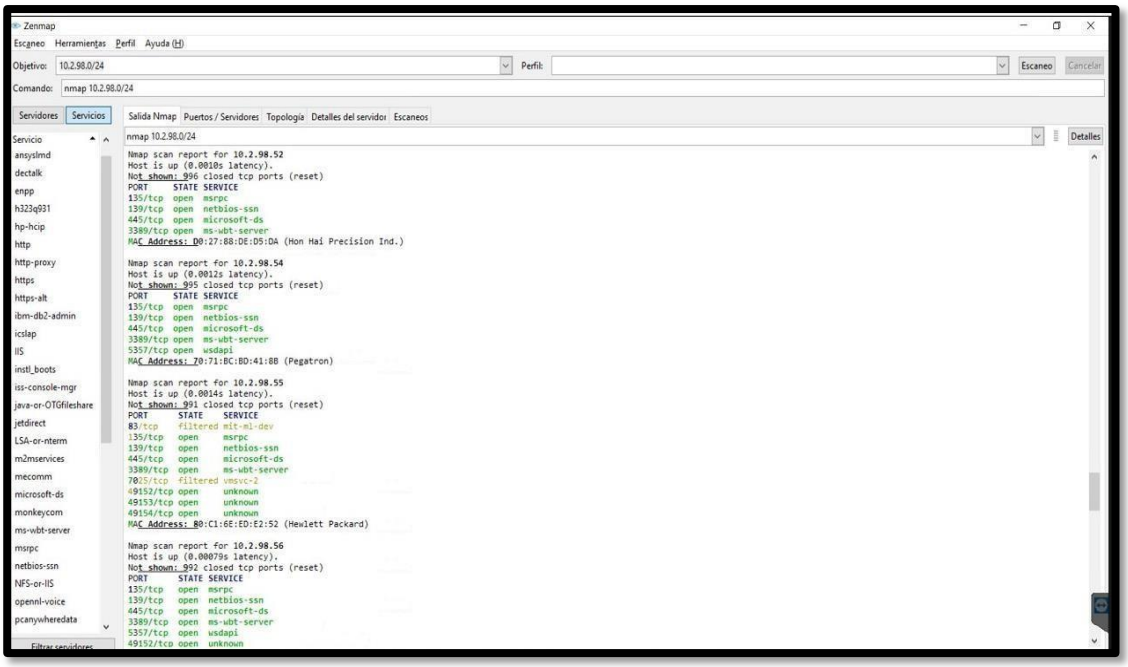


Imagen 5: Escaneo de la red Mies – Parte 4

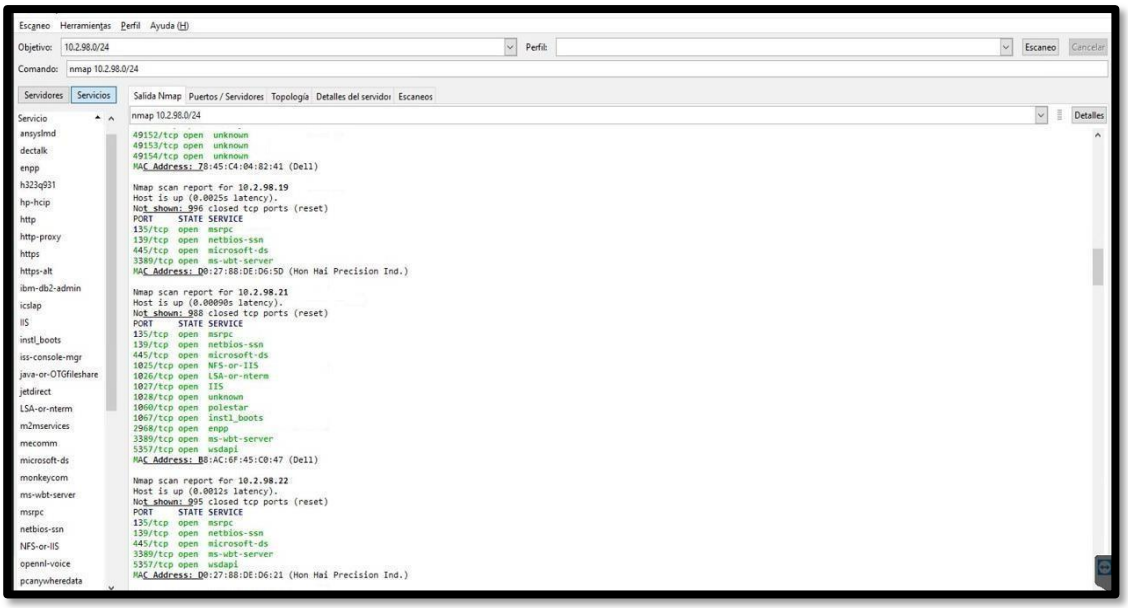


Imagen 6: Escaneo de la red Mies – Parte 5

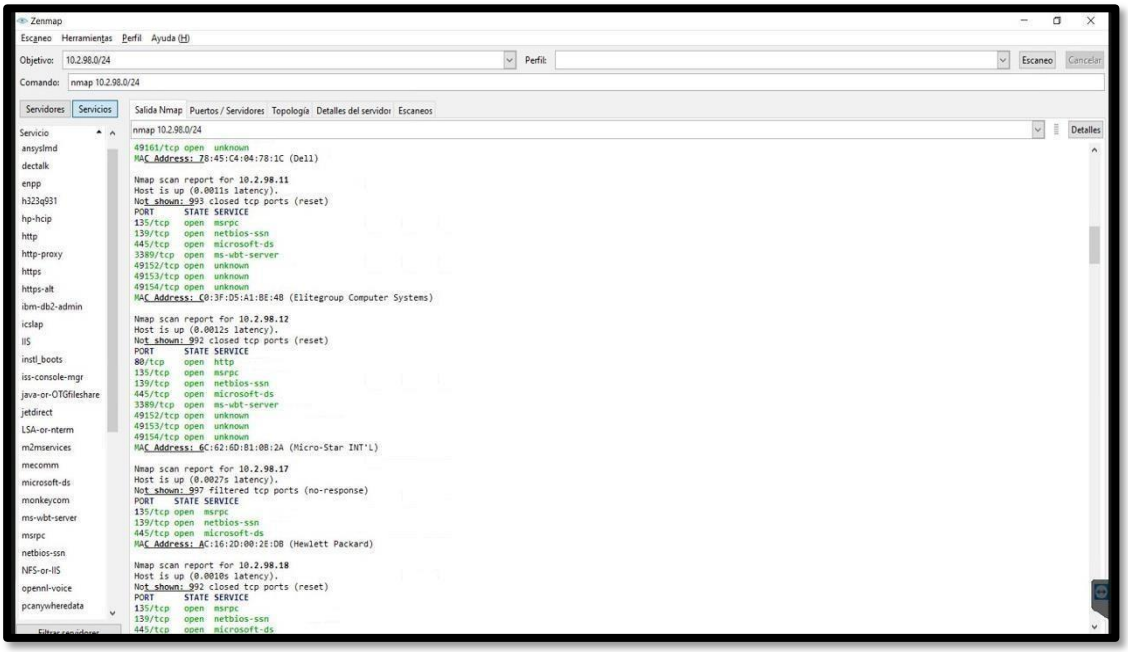


Imagen 7: Escaneo de la Red Mies – Parte 6

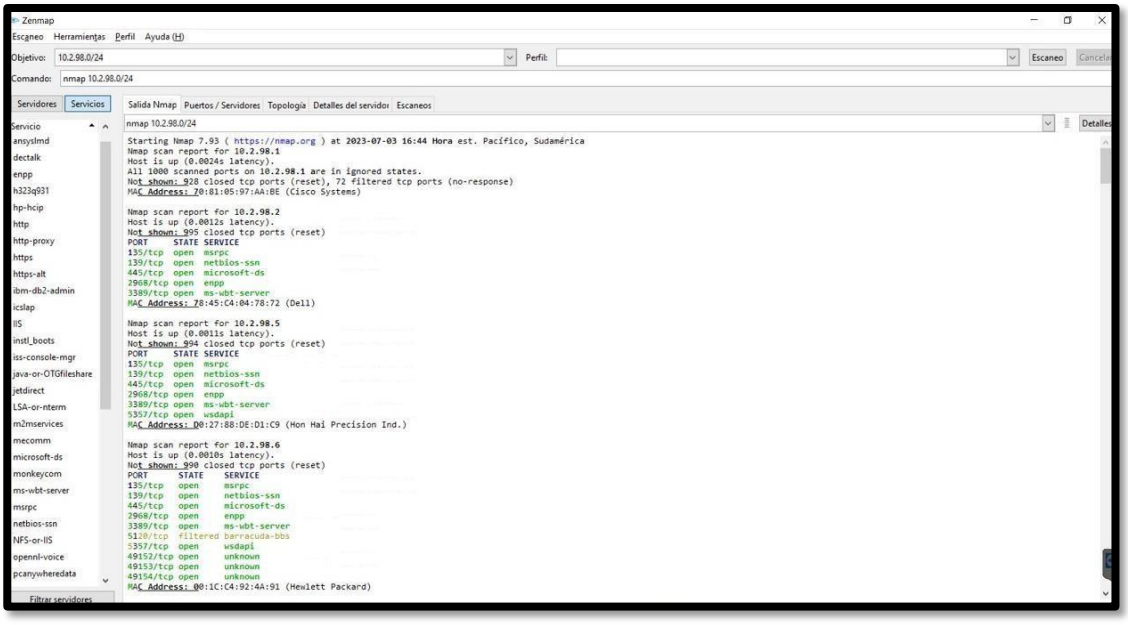


Imagen 8: Escaneo de la red Mies – Parte 7

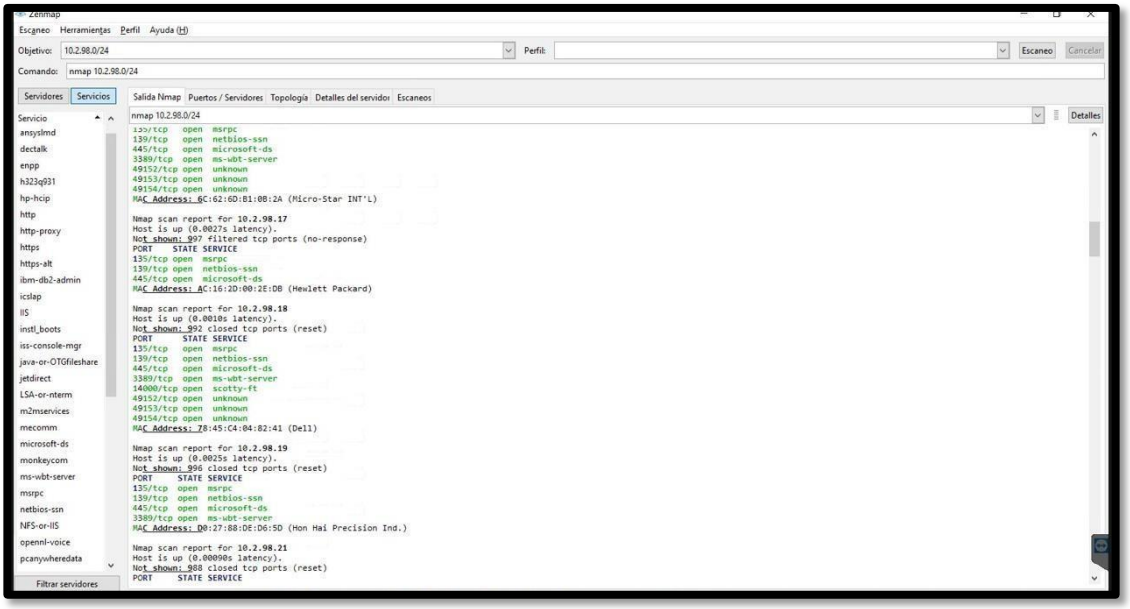


Imagen 9: Escaneo de la red Mies – Parte 8

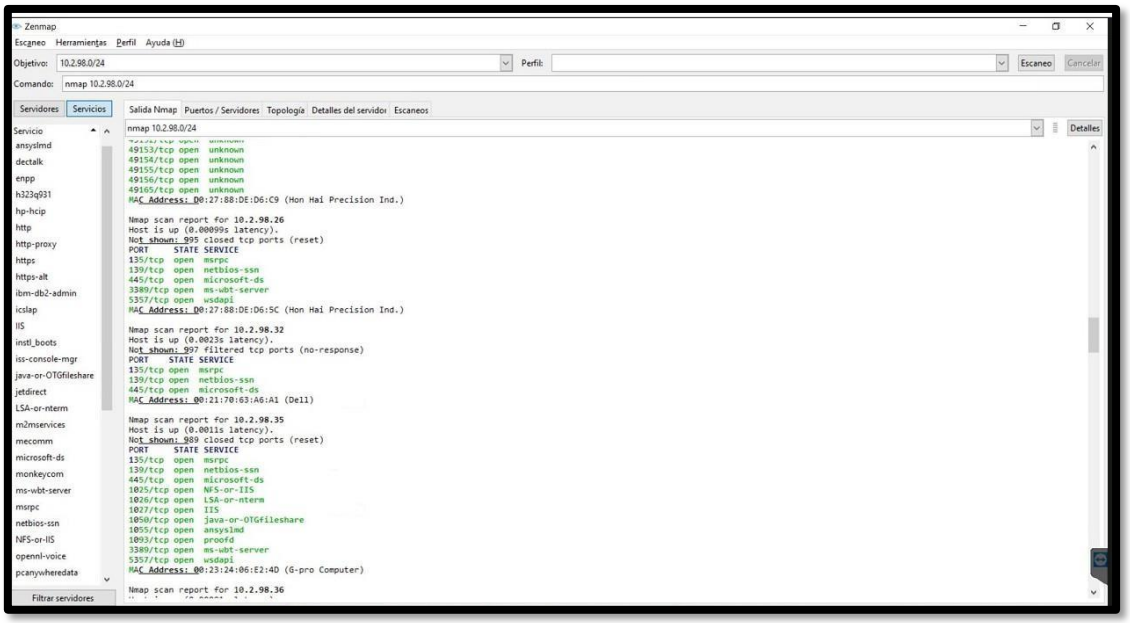


Imagen 10: Escaneo de la red Mies – Parte 9

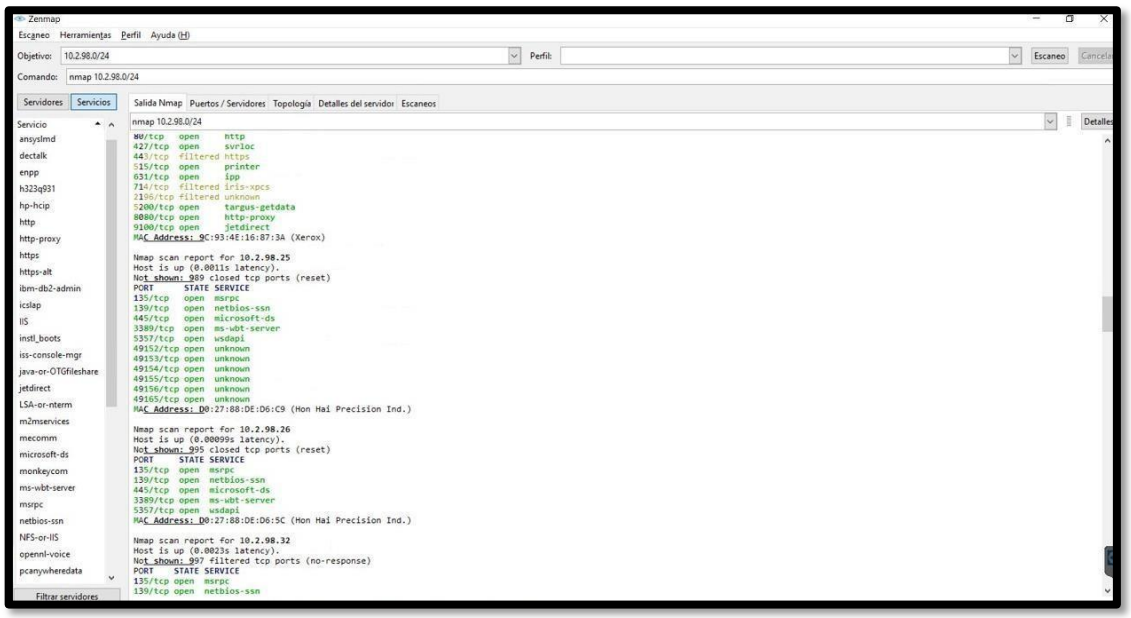


Imagen 11: Escaneo de la red Mies – Parte 10

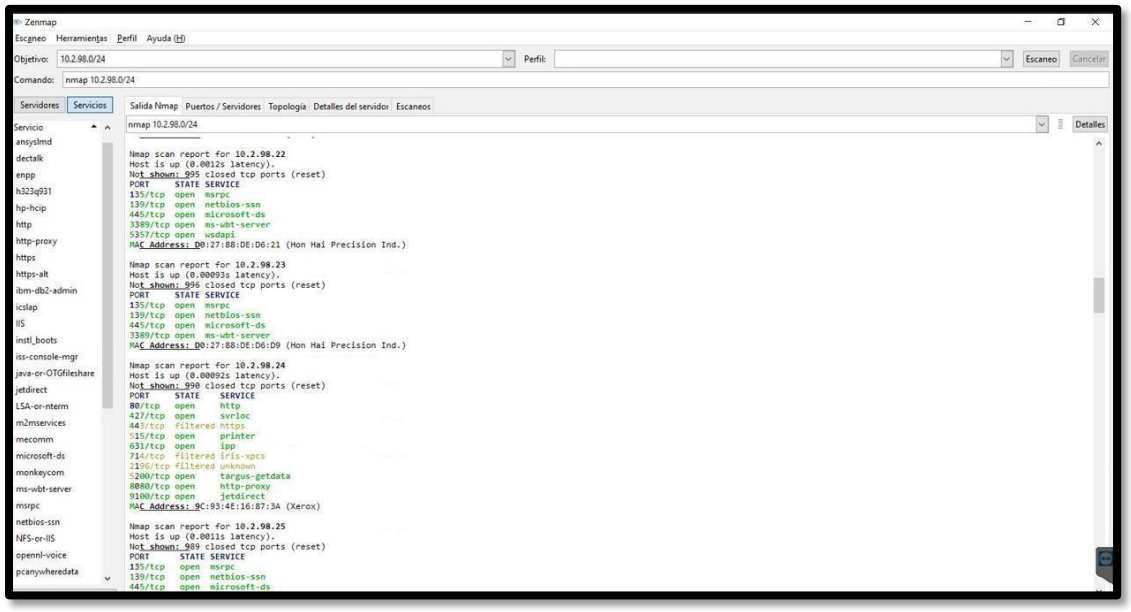


Imagen 12: Escaneo de la red Mies – Parte 11

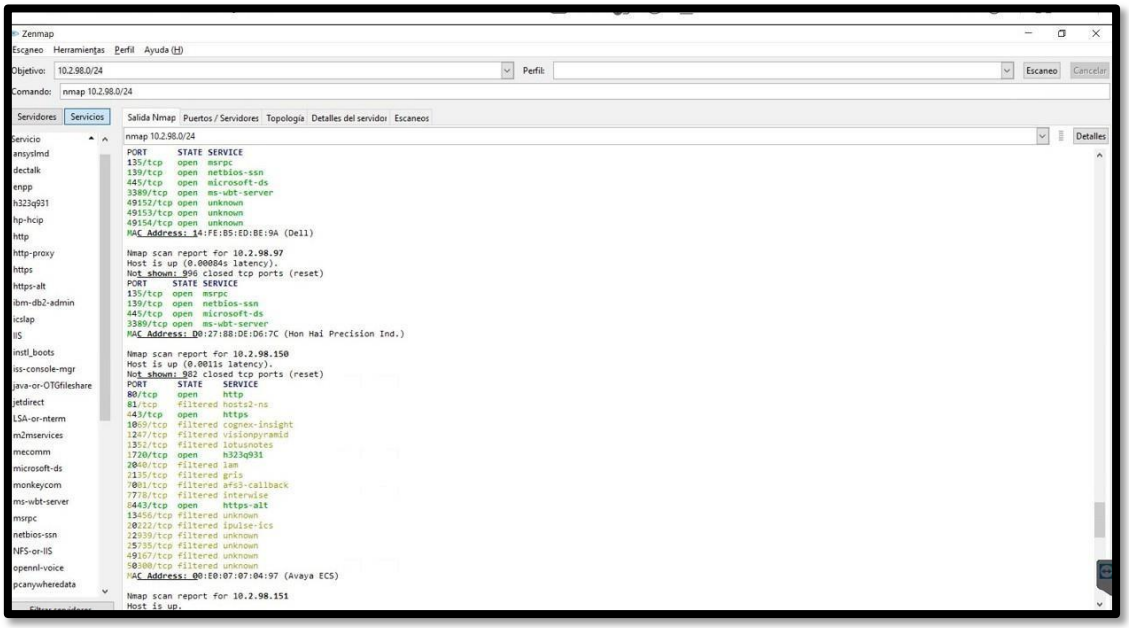


Imagen 13: Escaneo de la red Mies – Parte 12

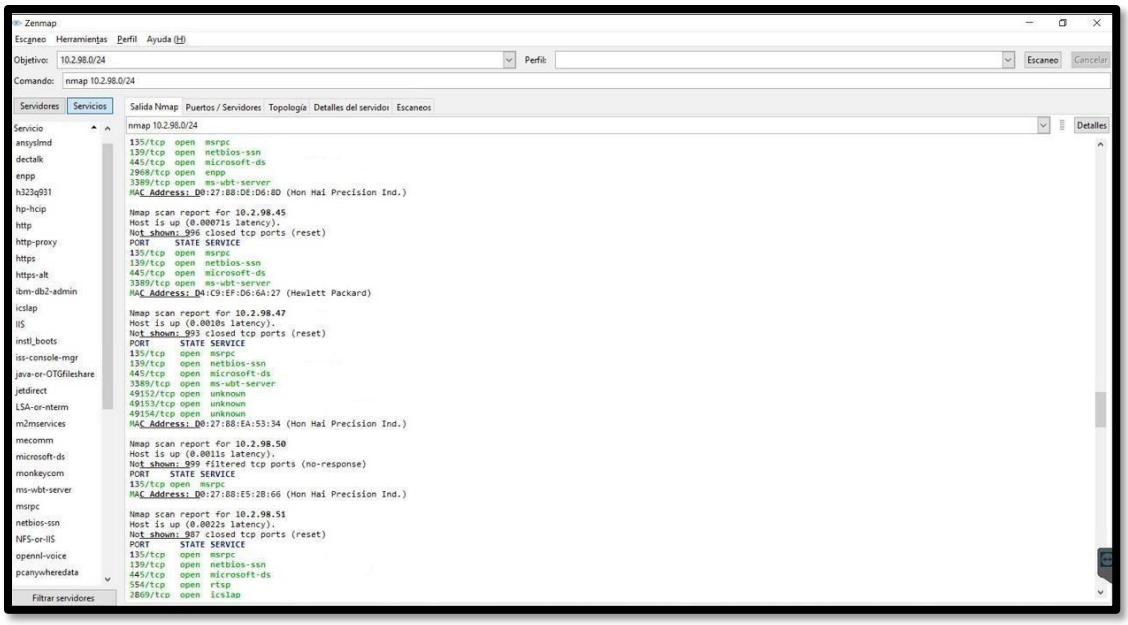


Imagen 14: Escaneo de la red Mies – Parte 13

Descubrimiento de máquinas vulnerables por Nmap

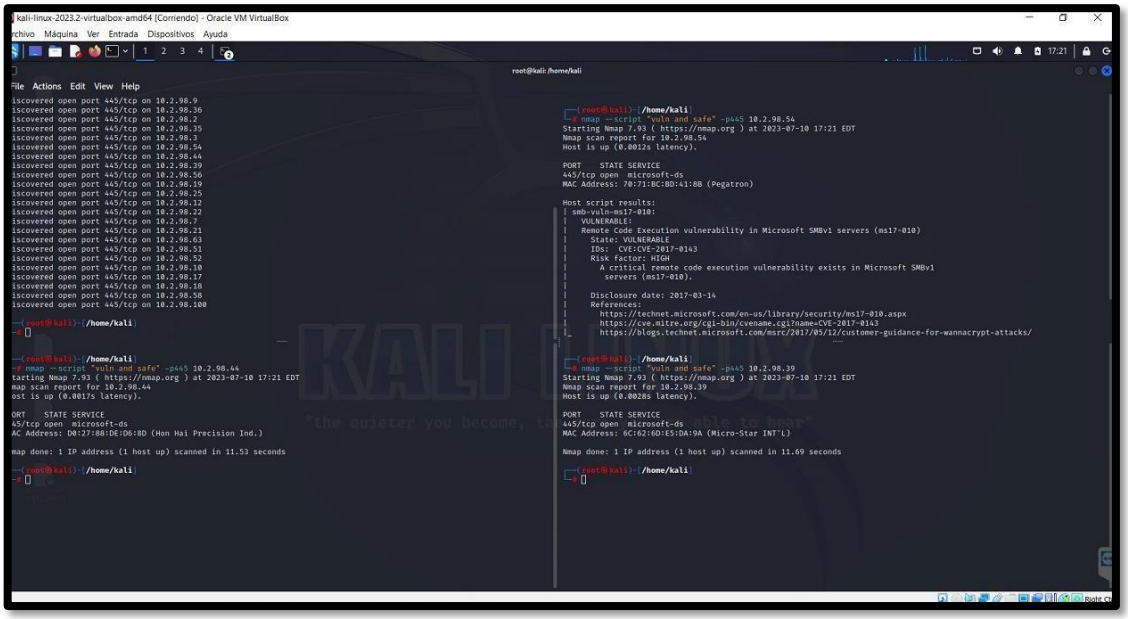


Imagen 15: Máquina vulnerable #1– 10.2.x.x

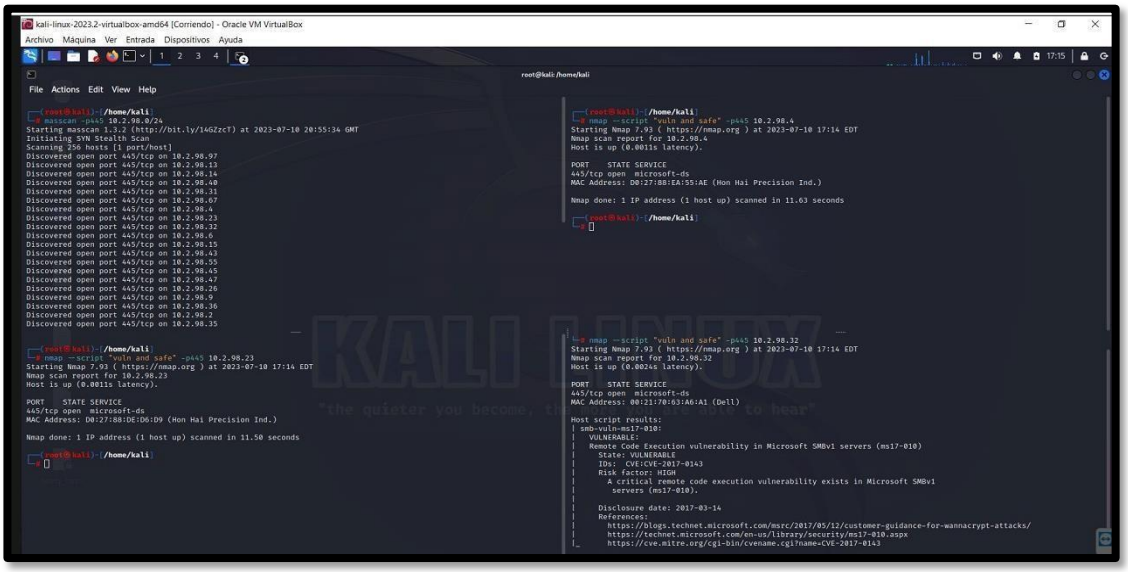


Imagen 16: Máquina Vulnerables #2 – 10.2.x.x

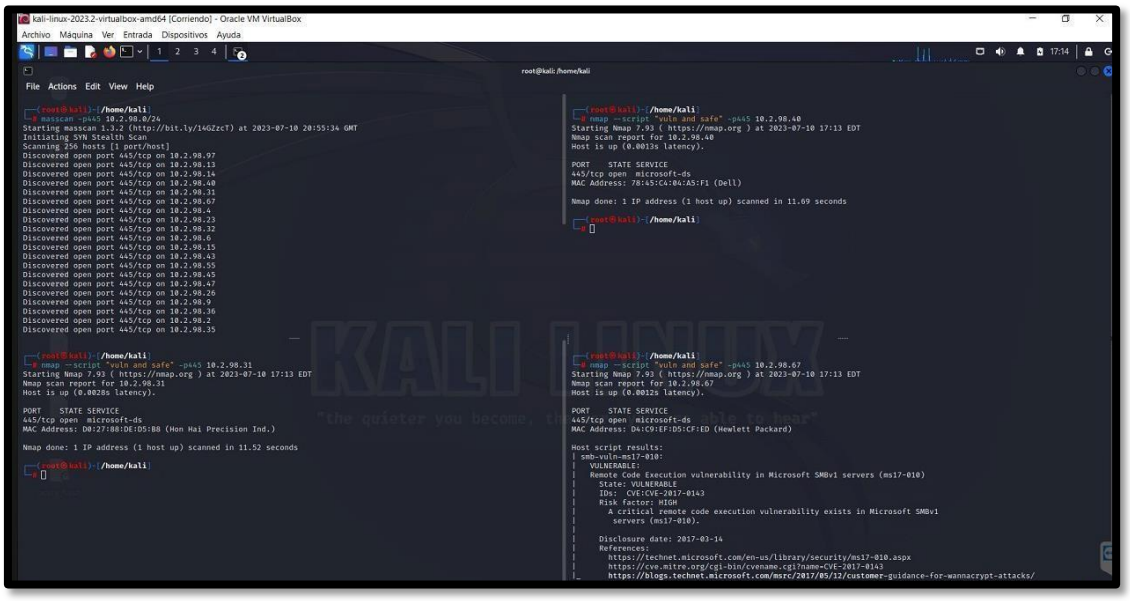


Imagen 17: Máquina Vulnerables #3 – 10.2.x.x

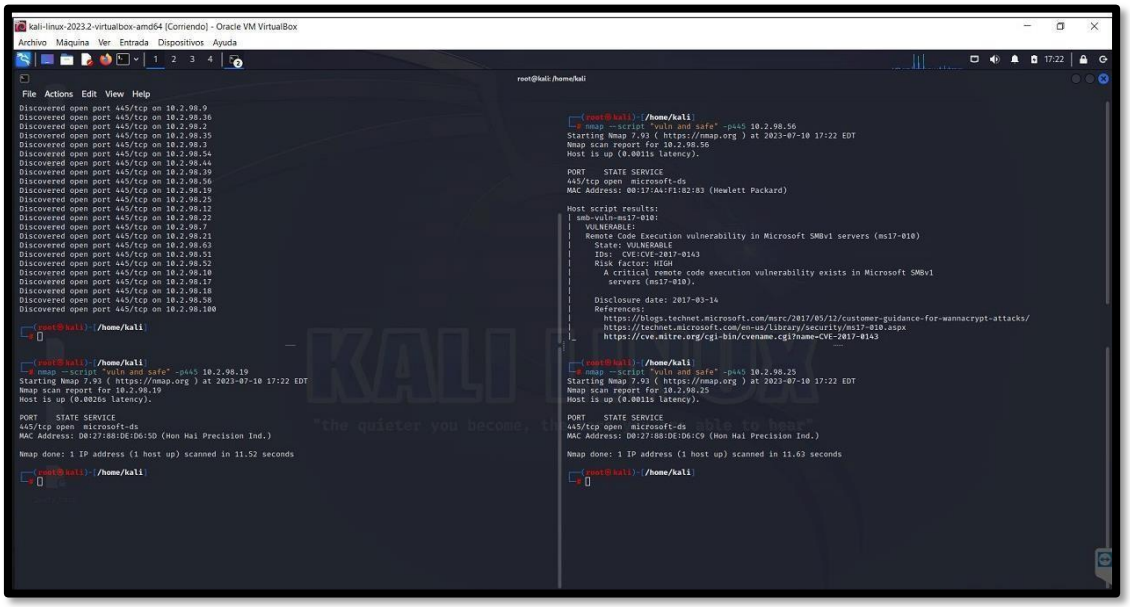


Imagen 18: Máquina Vulnerables #4 – 10.2.x.x

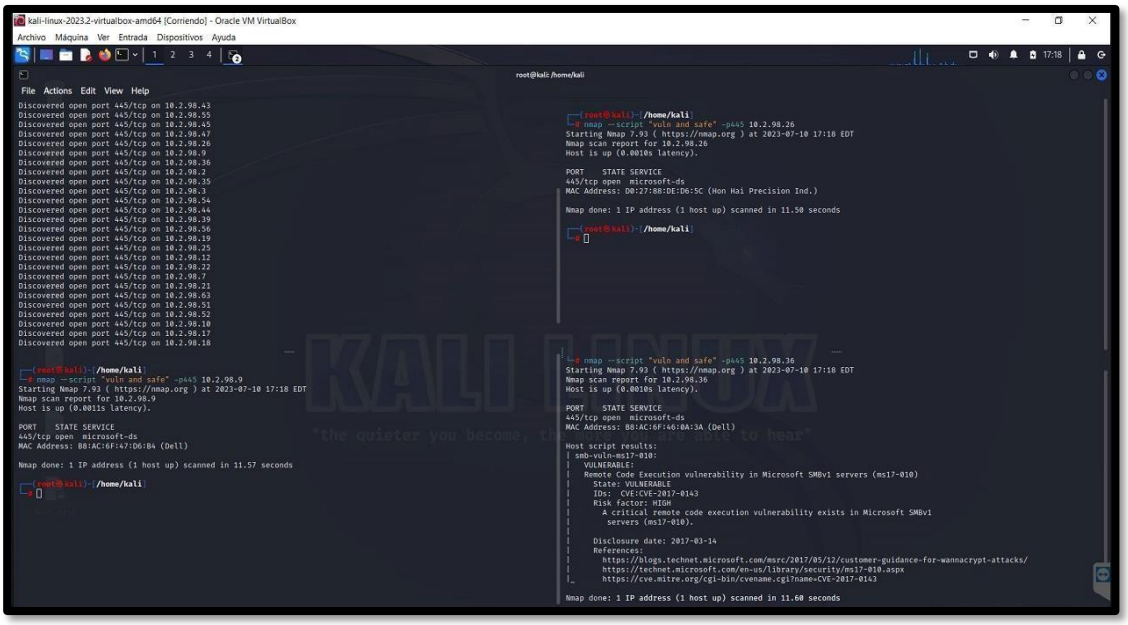


Imagen 19: Máquina Vulnerables # 5 – 10.2.x.x

Análisis de la red por Nessus

Hallazgos

- El escaneo encontró 22 vulnerabilidades en la red. Las vulnerabilidades se clasifican en tres niveles de gravedad:
- Crítica: 1 vulnerabilidad
- Alta: 4 vulnerabilidades
- Media: 6 vulnerabilidades
- Baja: 11 vulnerabilidades

Detalles sobre Nessus

Nessus es una herramienta de evaluación de vulnerabilidades que se utiliza para identificar y remediar vulnerabilidades en redes y sistemas informáticos. Nessus es una herramienta poderosa y flexible que puede ser utilizada por organizaciones de todos los tamaños.

Nessus utiliza una base de datos de plugins para detectar vulnerabilidades. Los plugins son pequeños programas que se ejecutan en los sistemas informáticos objetivo para verificar la presencia de vulnerabilidades conocidas.

Las vulnerabilidades críticas y altas son las más graves y requieren atención inmediata. Las vulnerabilidades medias y bajas también son importantes y deben abordarse en el futuro.

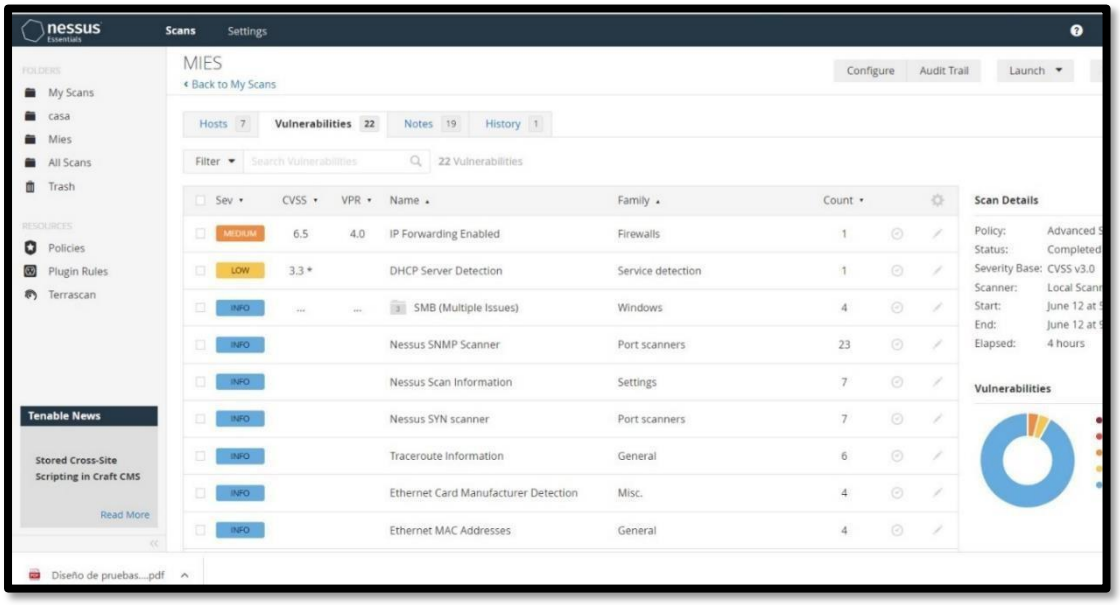
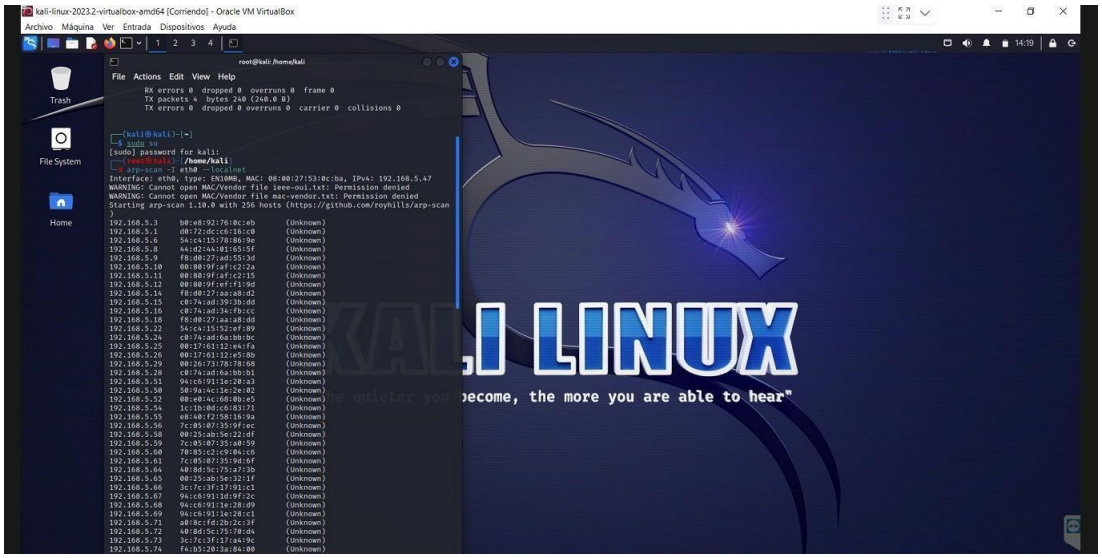


Imagen 20: Vulnerabilidades encontradas en Nessus

Dispositivos por masscan

Imagen 21: Dispositivos encontrados por MasScan



Dispositivos por arp-scan

Imagen 22: Direcciones ip encontradas por Arq-Scan

Descubrimiento de datos de la red y dispositivos por Advanced Ip Scanner

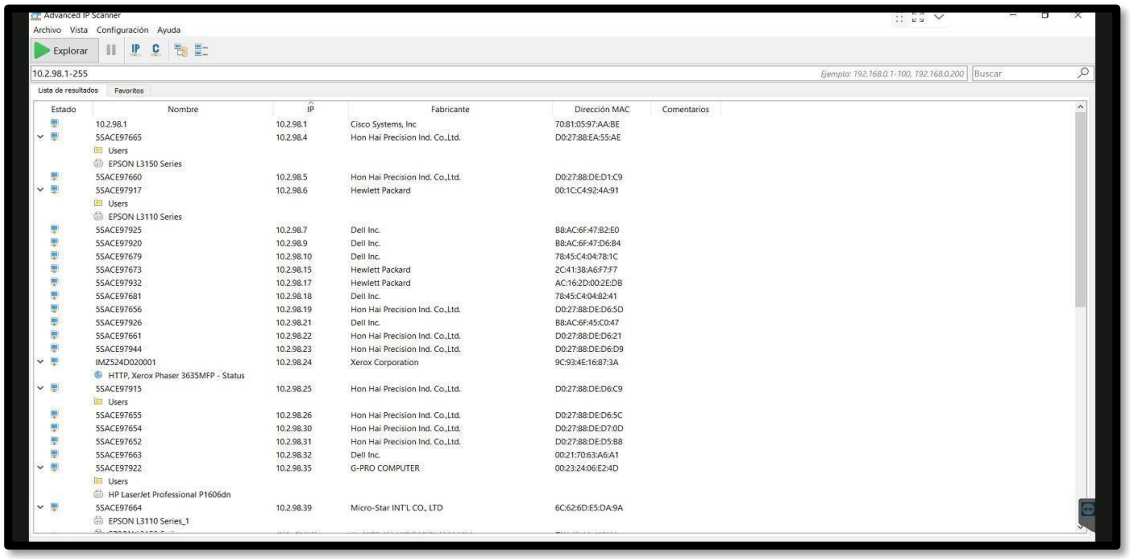


Imagen 23: Descubrimiento de la red por Advanced Ip Scanner – Parte 1

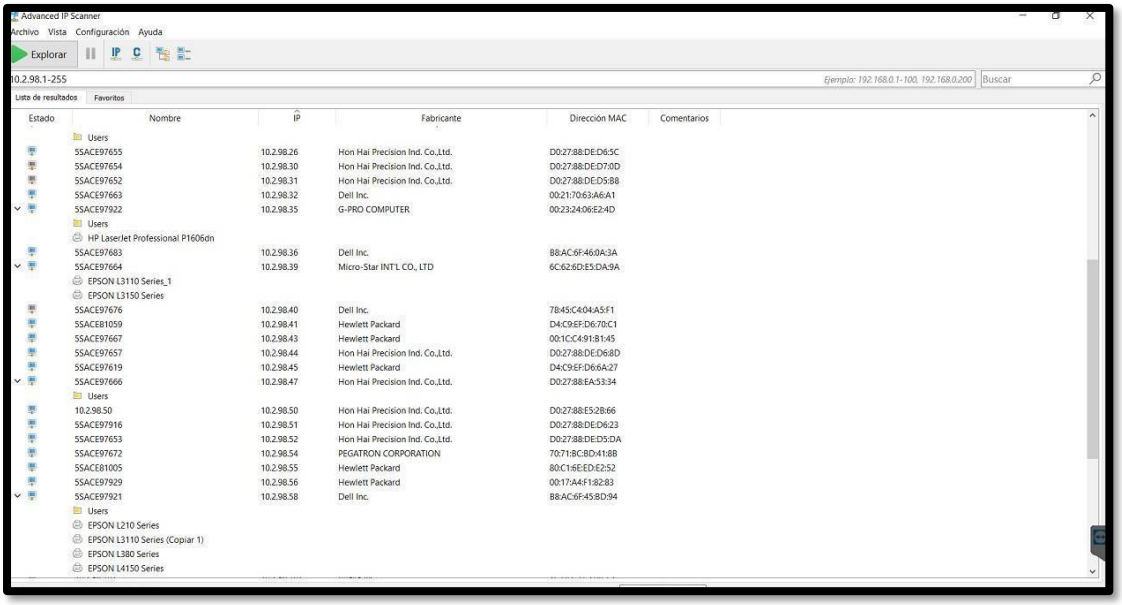


Imagen 24: Descubrimiento de la red por Advanced Ip Scanner – Pare 2

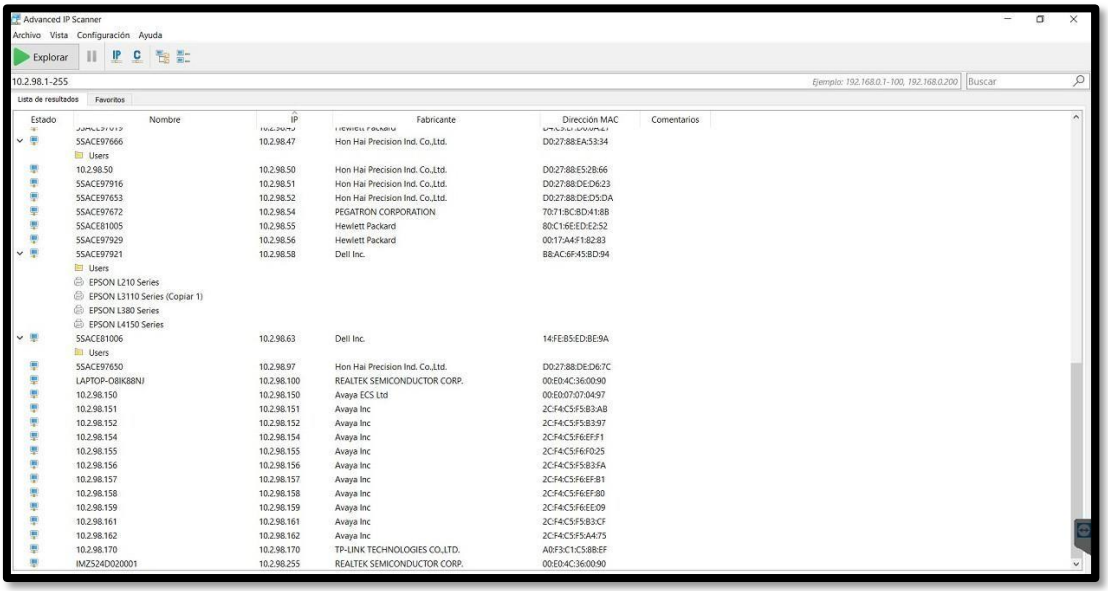


Imagen 25: Descubrimiento de la red por Advanced Ip Scanner – Parte 3

Descubrimiento por crackmapexec

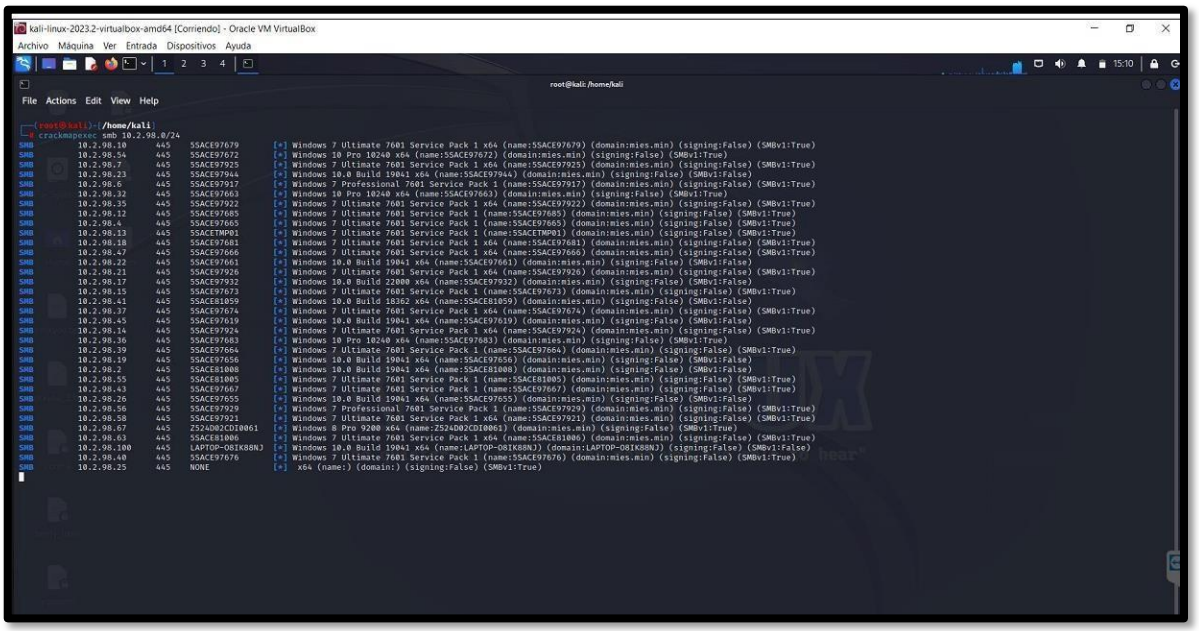


Imagen 26: Descubrimiento de direcciones ip por crackmapexec para hallar; S.O, dominio

Anexo 4

Intervención

TÉCNICA FUZZ TESTING

Ataque: Main The Midle

Objetivo: Analizar de la red para conocer el tráfico de envío de datos

El análisis de la red encontró lo siguiente:

- Se produjo un intercambio de paquetes TCP entre dos hosts, uno con la dirección IP 131.100.1.169 y el otro con la dirección IP 10.2.98.100.
- El primer host envió un paquete TCP de 78 bytes al segundo host.
- El segundo host envió un paquete TCP de 242 bytes al primer host.

1. Envió de paquetes

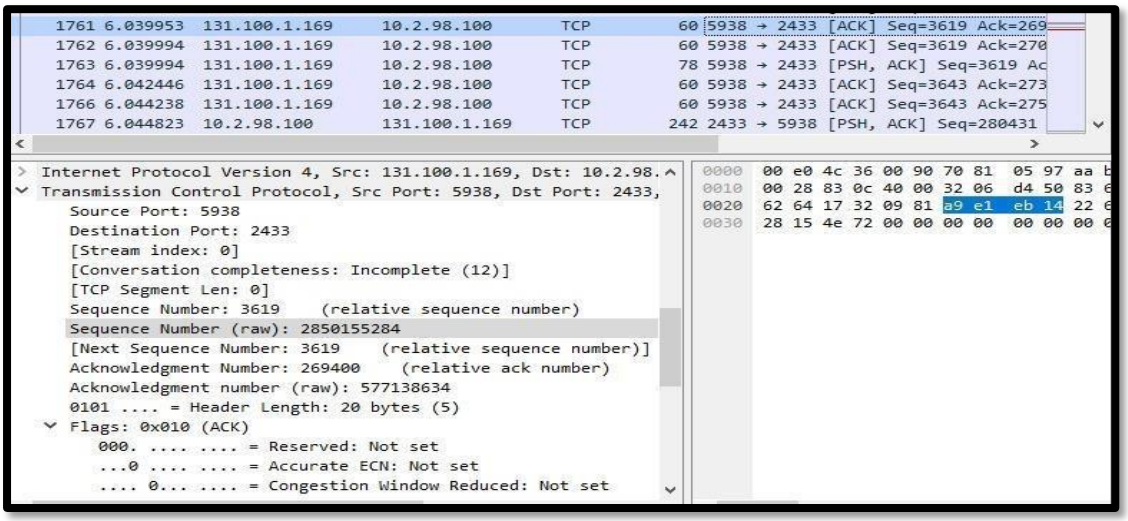


Imagen 27: Envió de paquetes por Wireshark

2. Capitulación de diseño de la página web

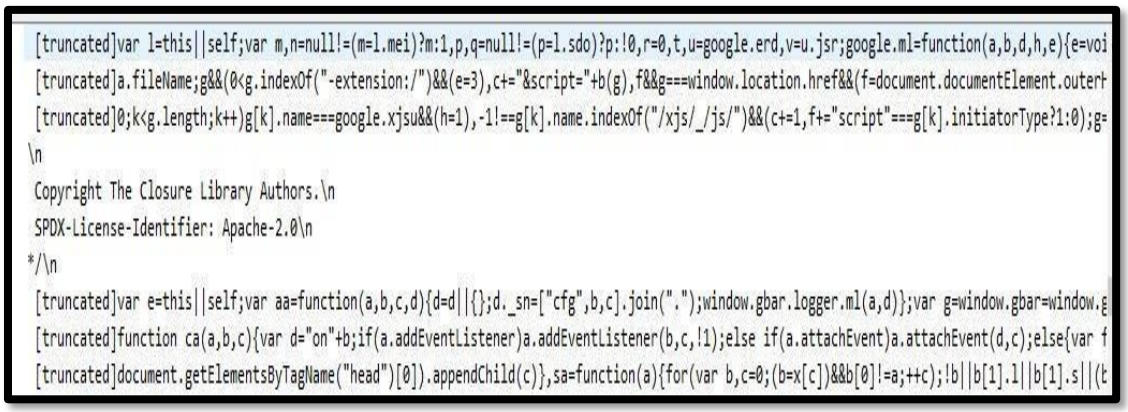


Imagen 28: código de diseño de código Web

3. Redirige a index.html por ip 10.2.98.100

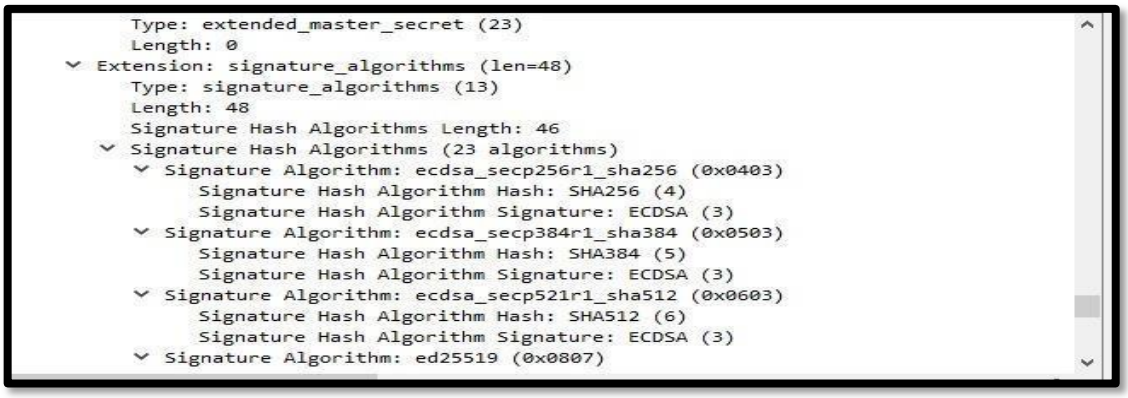
```
\t//AddNode( gTheTree, HEAD_NODE, " Phaser 3635MFP");\n
\tAddNode( gTheTree, ROOT_NODE, "General", "/status/general.dhtml");\n
\tAddNode( gTheTree, ROOT_NODE, "Alerts", "/status/statusAlerts.dhtml");\n
\tAddNode( gTheTree, ROOT_NODE, "Trays", "/status/trays.dhtml" );\n
\tAddNode( gTheTree, ROOT_NODE, "Consumables", "/status/consumables.dhtml" );\n
\tAddNode( gTheTree, ROOT_NODE, "SMart eSolutions ", "/status/smartesolutions.dhtml" );\r
\n
function LinkHitAndGotoPage( inMainTabPage, inUrlToHighlight )\n
```

Imagen 29: Index.html

4. Se logro visualizar código de página web index.html

Imagen 30: Cogido Index.html

5. Se observa tipo de hash



```
        Type: extended_master_secret (23)
        Length: 0
    Extension: signature_algorithms (len=48)
        Type: signature_algorithms (13)
        Length: 48
        Signature Hash Algorithms Length: 46
      Signature Hash Algorithms (23 algorithms)
        Signature Algorithm: ecdsa_secp256r1_sha256 (0x0403)
            Signature Hash Algorithm Hash: SHA256 (4)
            Signature Hash Algorithm Signature: ECDSA (3)
        Signature Algorithm: ecdsa_secp384r1_sha384 (0x0503)
            Signature Hash Algorithm Hash: SHA384 (5)
            Signature Hash Algorithm Signature: ECDSA (3)
        Signature Algorithm: ecdsa_secp521r1_sha512 (0x0603)
            Signature Hash Algorithm Hash: SHA512 (6)
            Signature Hash Algorithm Signature: ECDSA (3)
        Signature Algorithm: ed25519 (0x0807)
```

Imagen 31: Hashes

6. Descubrimiento de servicio de dominio

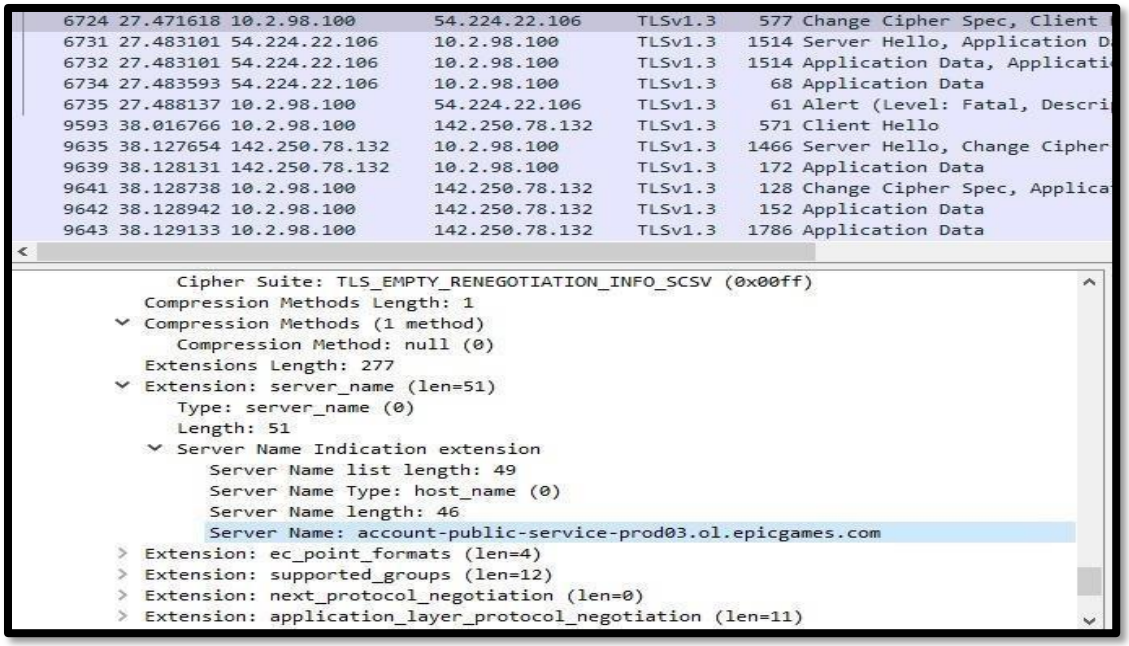


Imagen 32: Dominio

Herramienta - Networminer

Objetivo: Lectura de saturación de datos de Wireshark

7. En anomalías, se encontró errores de comunicación entre host, durante un tiempo determinado, se llegó a la conclusión según lo analizado, que fue por la múltiple cantidad de solicitudes que se recibió el host, luego de esto, funciono con normalidad

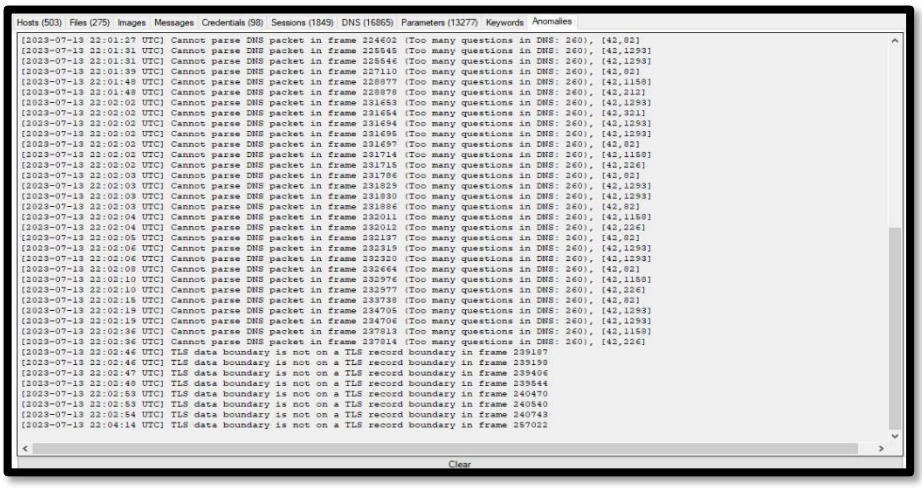


Imagen 33: Anomalías encontradas

10.2.98.58 [5SACE97921] (Windows)	RDP Cookie	mstshash=PAESSLERG	
10.2.98.54 [5SACE97672.local]	SNMPv1	SNMP community	public
10.2.98.44 [5SACE97657.local] [5SACE97657]	RDP Cookie	mstshash=PAESSLERG	
10.2.98.2 [5SACE81008.local] [5SACE81008]	RDP Cookie	mstshash=PAESSLERG	
10.2.98.10 [5SACE97679] (Windows)	RDP Cookie	mstshash=PAESSLERG	
10.2.98.7 [5SACE97925] (Windows)	RDP Cookie	mstshash=PAESSLERG	
10.2.98.40 [5SACE97676] (Windows)	RDP Cookie	mstshash=PAESSLERG	
10.2.98.43 [5SACE97667] (Windows)	RDP Cookie	mstshash=PAESSLERG	
10.2.98.63 [5SACE81006] (Windows)	RDP Cookie	mstshash=PAESSLERG	
10.2.98.23 [5SACE97944.local] [5SACE97944]	RDP Cookie	mstshash=PAESSLERG	
10.2.98.49	SNMPv1	SNMP community	public
10.2.98.36	SNMPv1	SNMP community	public
10.2.98.4 [5SACE97665] (Windows)	RDP Cookie	mstshash=PAESSLERG	

Imagen 34 Protocolos Encontrados

PRUEBA DE PENETRACIÓN

Ataque: Samba Relay

Objetivo: Retransmisión SMB para capturar proceso en tiempo real de solicitud de autenticación y obtener el protocolo NTLMv2 que contiene el hash para descifrar y obtener la contraseña.

8. Se efectuó la búsqueda de la herramienta Responder.py en el directorio, para ejecutar y envenenar la red para capturar peticiones

Imagen 35: Ejecución de Responder

9. Luego se inserta el comando de ejecución

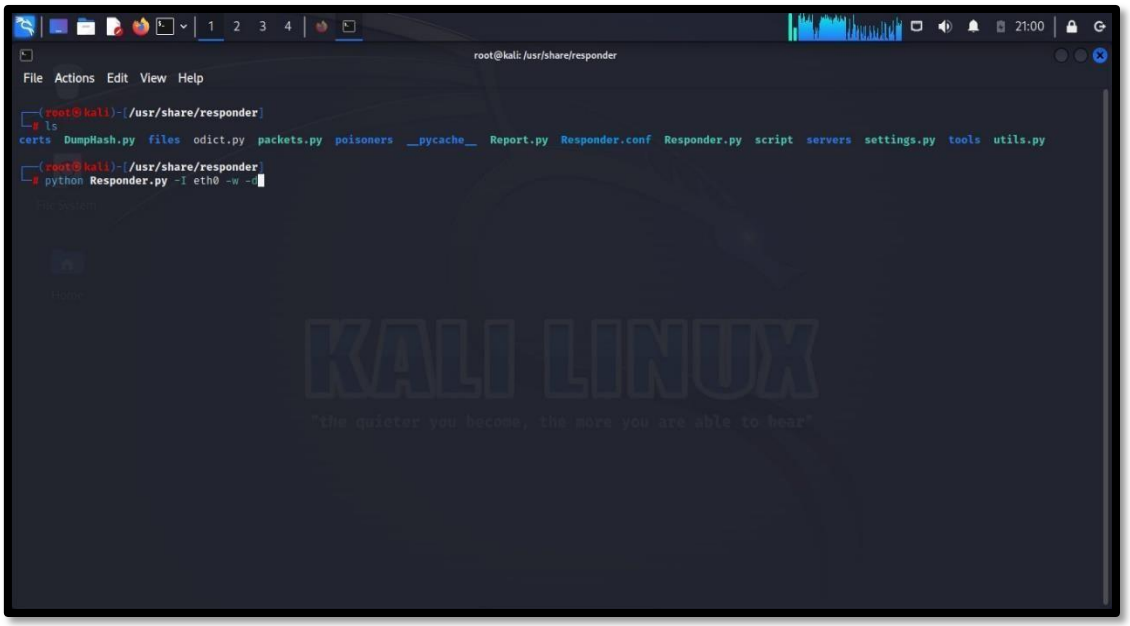


Imagen 36: Ejecución de Responder con el siguiente comando

10. Empieza a desarrollar hasta que encuentre algo

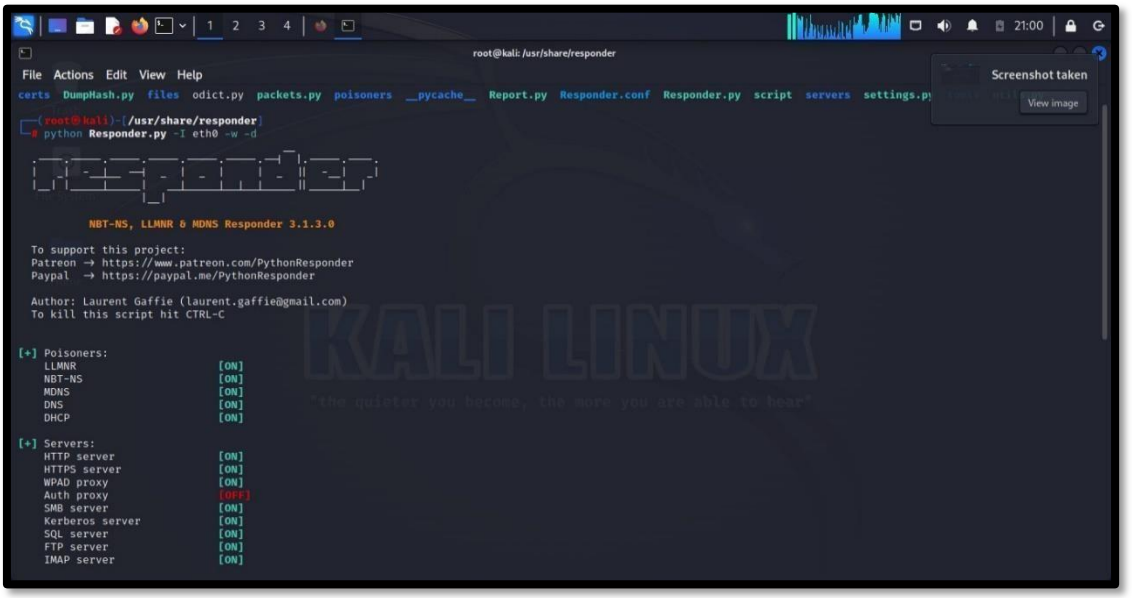


Imagen 37: Ejecución de responder envenenando la red

11. Al ejercer el envenenamiento con de la red por media hora se encontró el primer resultado.

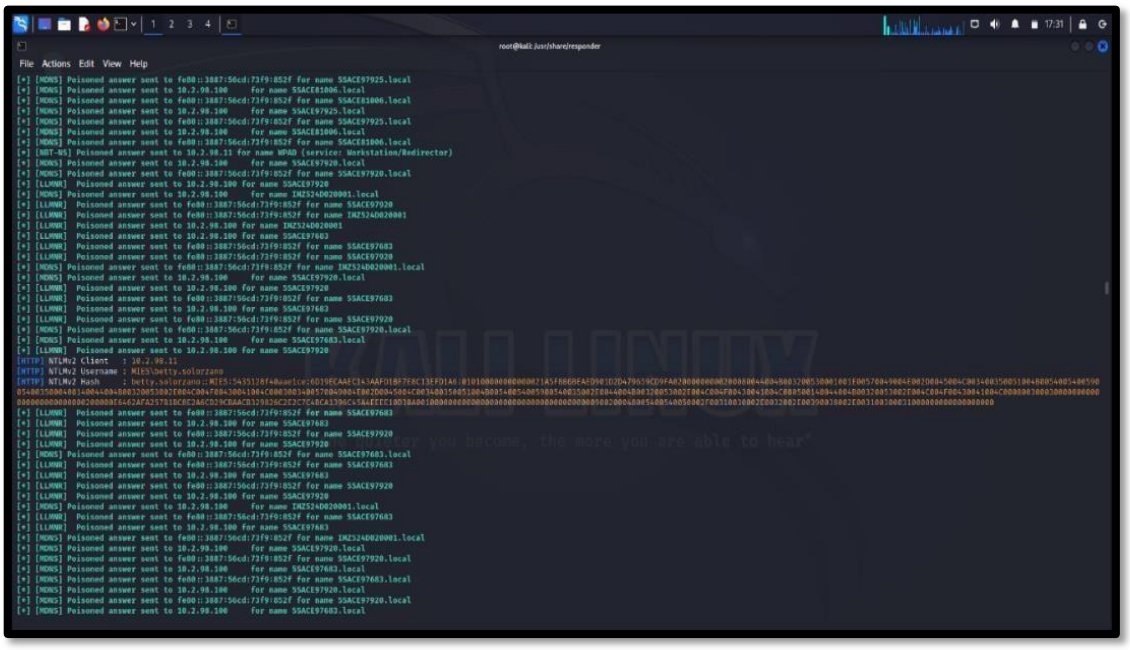


Imagen 38: Primer hash encontrado

12. Se halló el segundo hash de otra máquina

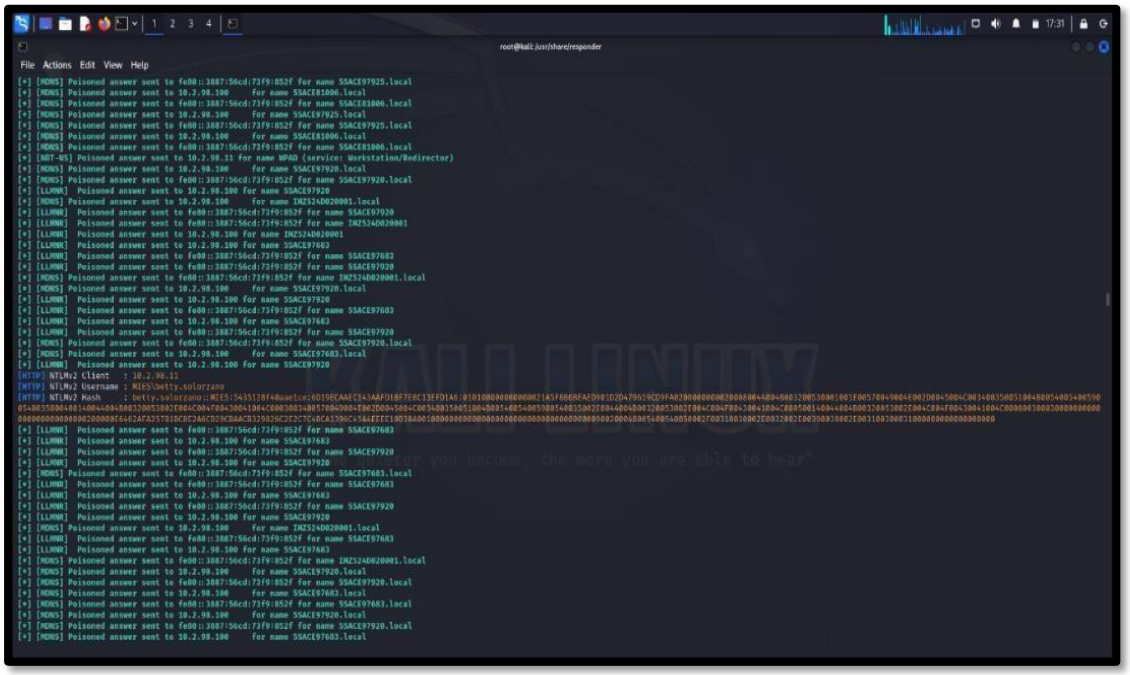


Imagen 39: Segundo hash encontrado

13. Se halló el tercer hash

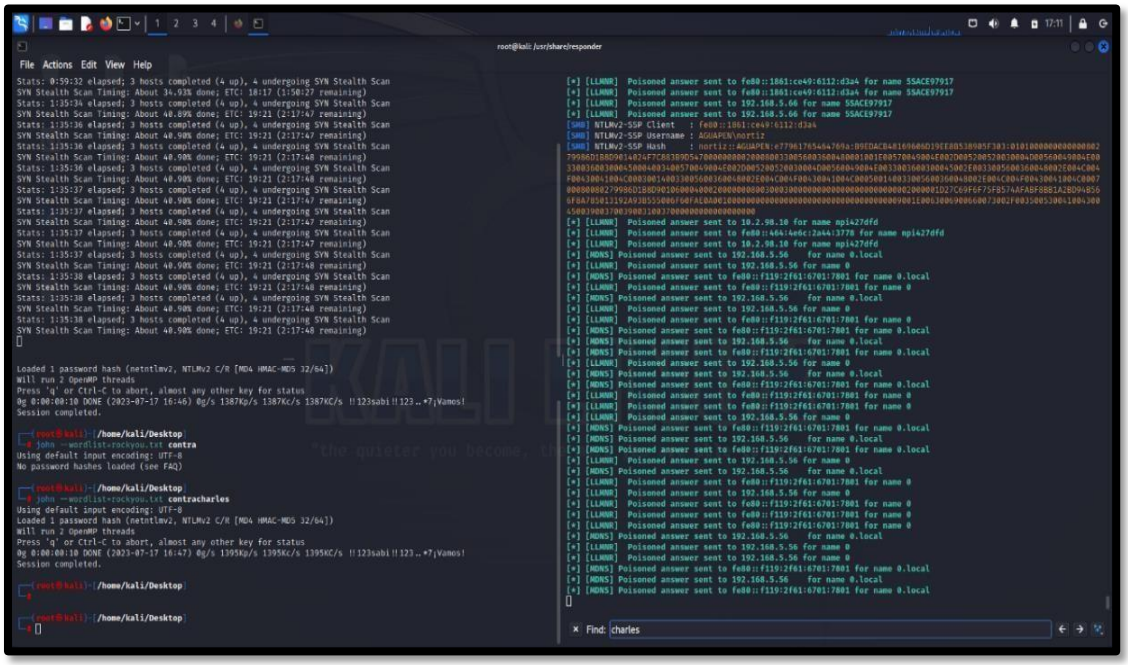


Imagen 40: Tercer hash encontrado

14. Se halló el cuarto hash

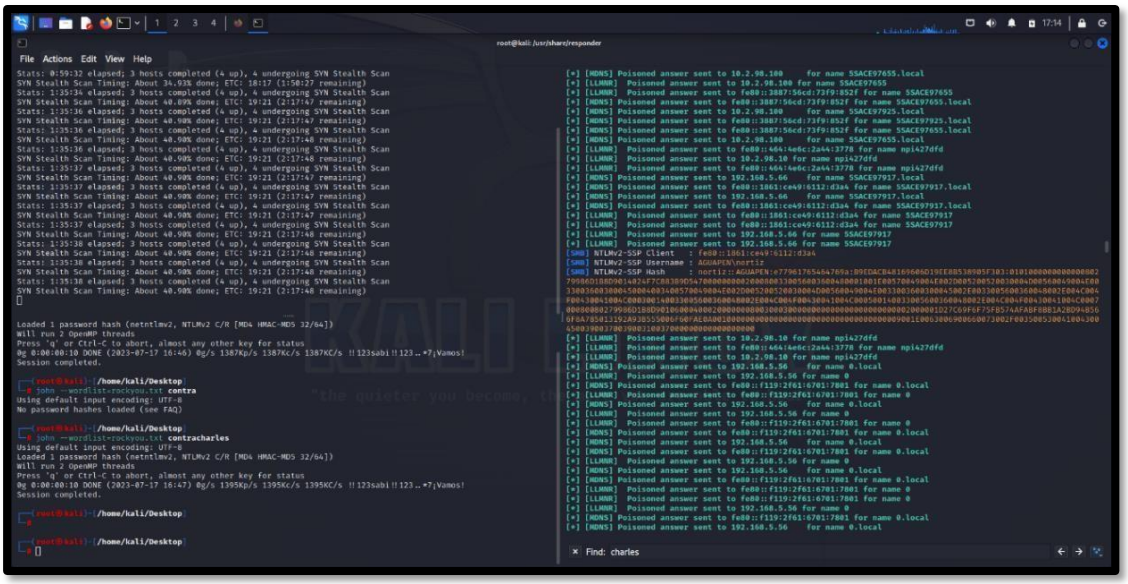


Imagen 41: Cuarto hash encontrado

15. Se halló el quinto hash

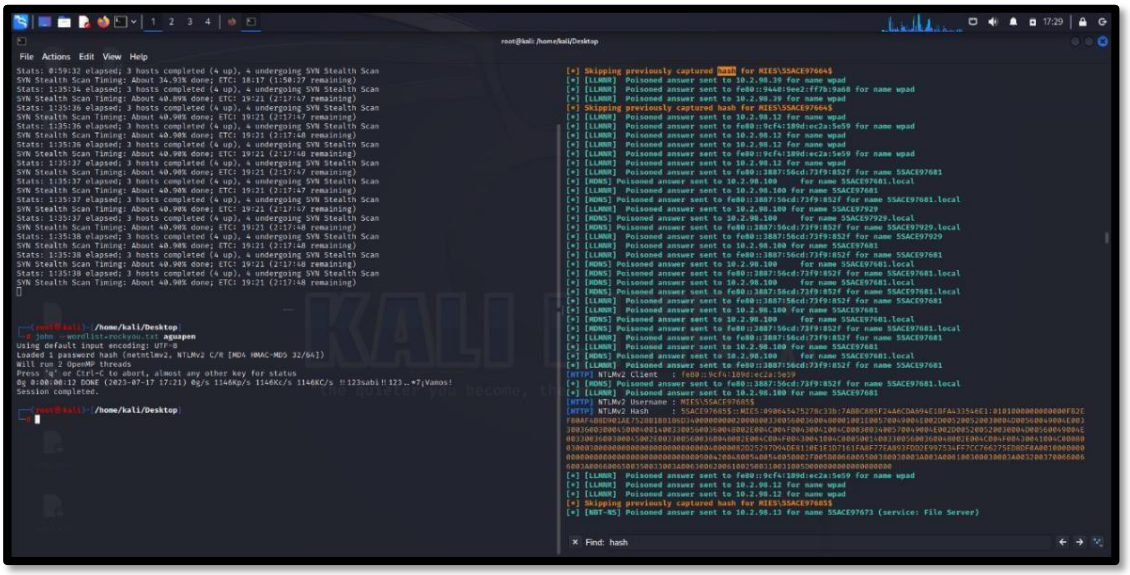


Imagen 42: Quinto hash encontrado

16. Hashes guardados

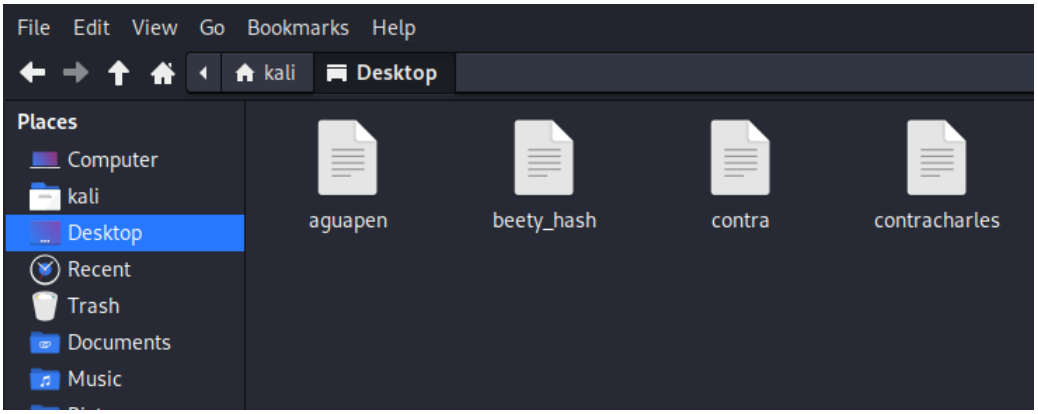


Imagen 43: Hashes almacenados

Ataque: Fuerza Bruta

Objetivo: Descifrar las contraseñas del hash capturado por Samba Relay por diccionario avanzados y comunes de contraseñas

17. Descifrado del primer hash con Jhon Reaper

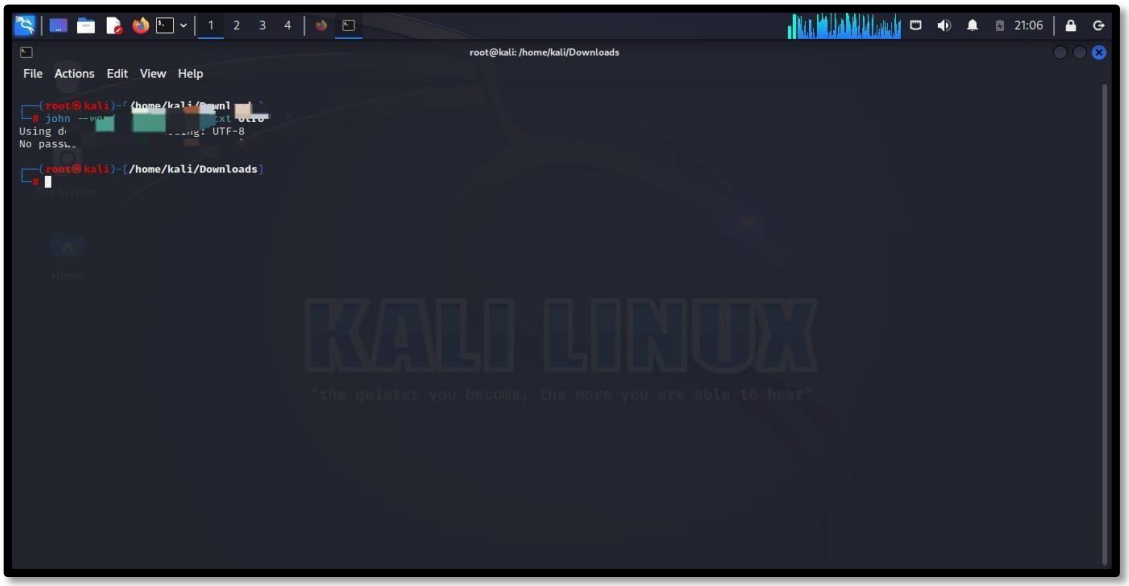


Imagen 44:Descifrado de primer hash

18. Descifrado del segundo hash con Jhon Reaper

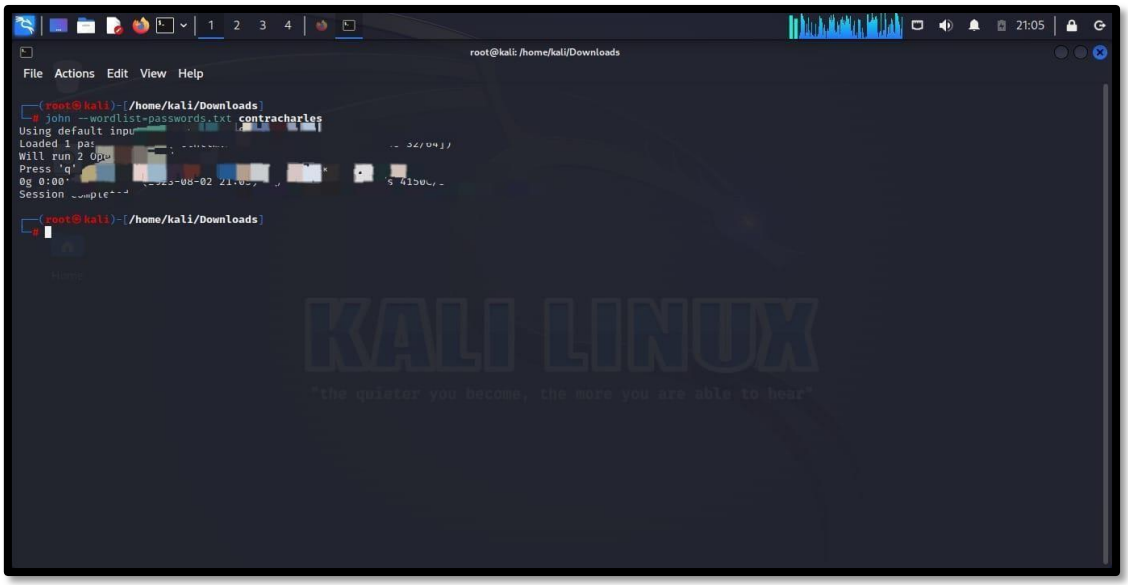


Imagen 45: Descifrado de segundo hash

19. Descifrado del tercero hash con Jhon Reaper

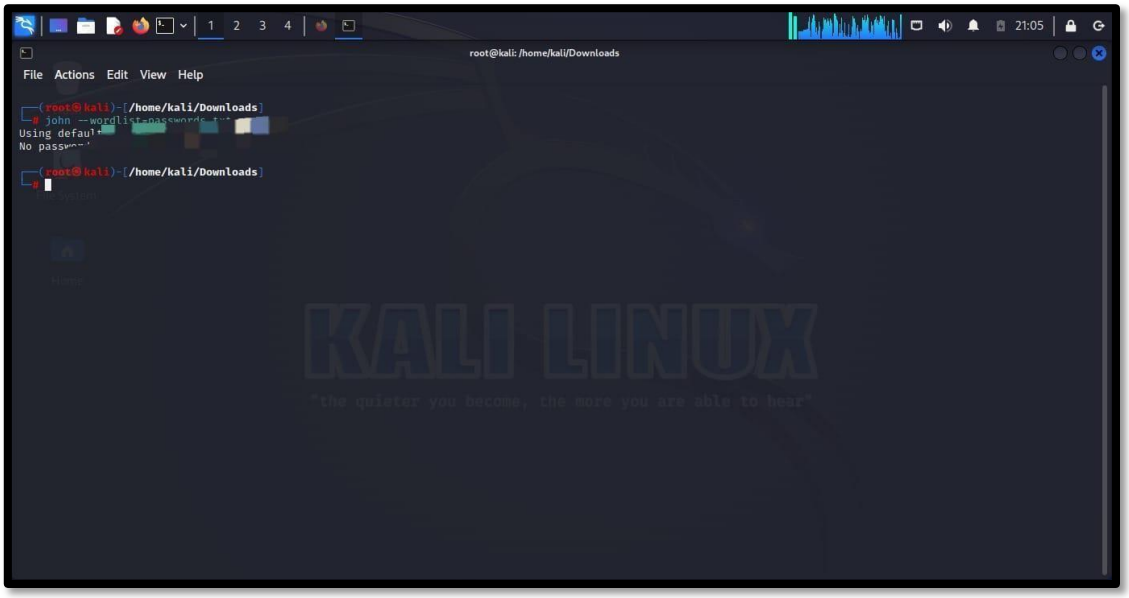


Imagen 46: Descifrado de tercer hash

20. Descifrado del cuarto hash con Jhon Reaper

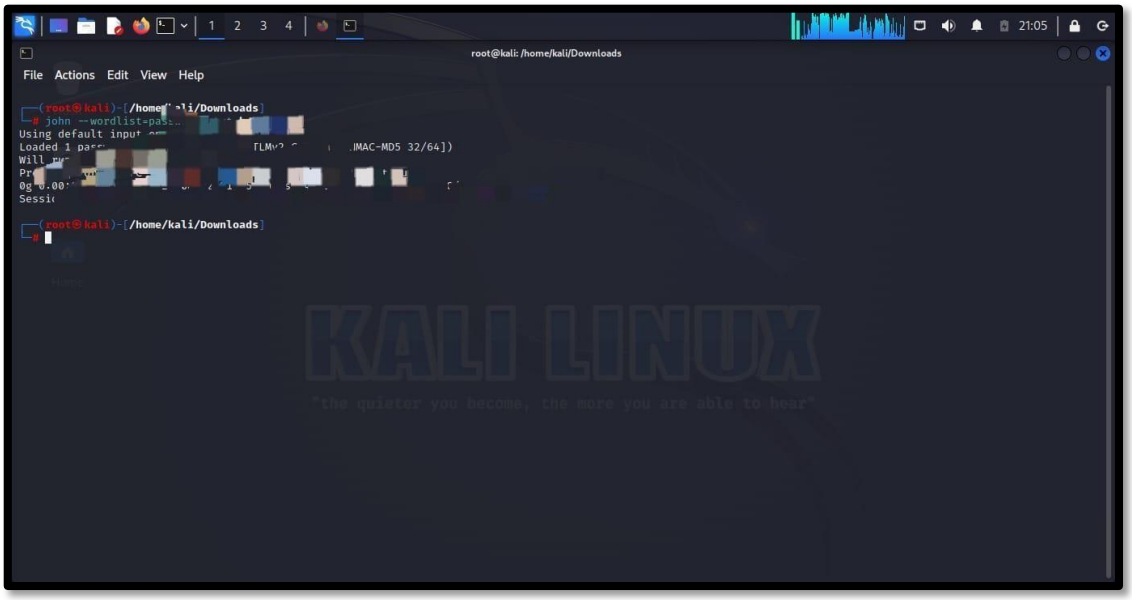


Imagen 47: Descifrado de cuarto hash

21. Descifrado del quinto hash con Jhon Reaper

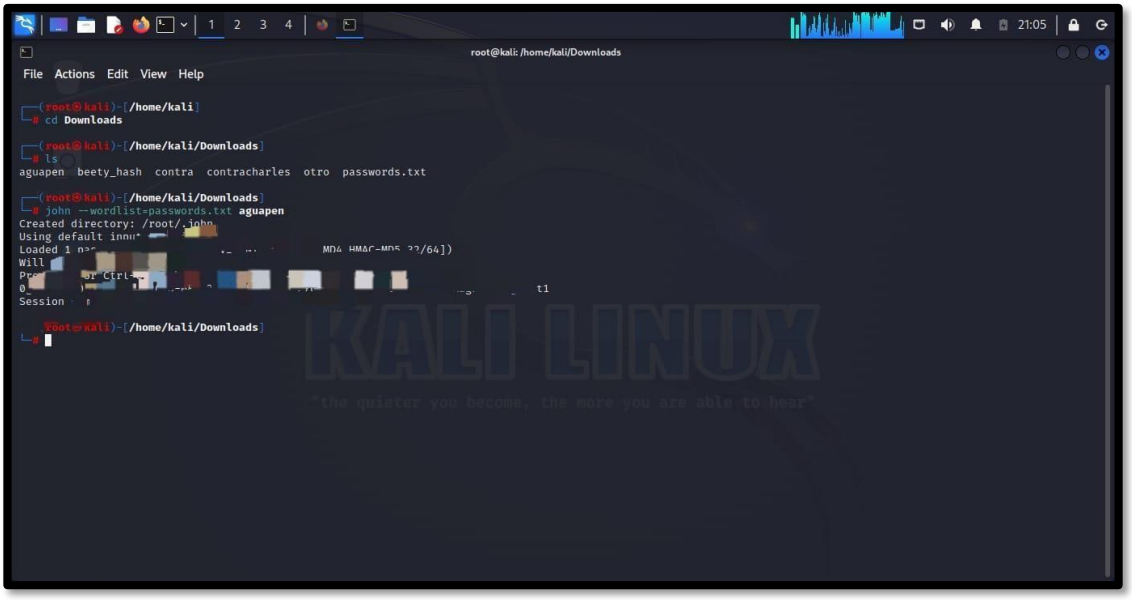


Imagen 48: Descifrado de quinto hash

- Se logro romper 5 hash encontrados

EXPLOTACIÓN DE VULNERABILIDADES

Simulación de ataque: Virus Informático – msfvenom

Objetivo: Inserción de virus informático a una máquina de la institución.

22. Una vez preparado el entorno se comenzó con la creación del payload(virus) para esto se debe encontrar como usuario root en Kali, luego se inicia Metasploit Framework.

Imagen 49: Entorno Msfconsole

23. Para el ejecutable de payload se ubicó el comando a continuación, logrando activar la herramienta Msfvenom,

    -p: sirve para especificar el payload a utilizar

    -a; que arquitectura utilizara el virus

    -platform: en que plataforma va a actuar el virus

    -o: Dirección donde el virus se guardará

    -f: formato del virus

    Lhost: se estable la dirección ip del atacante

    Lport: puerta local

Imagen 50: Comando de creación de virus

24. Virus creado exitosamente para soportar Windows

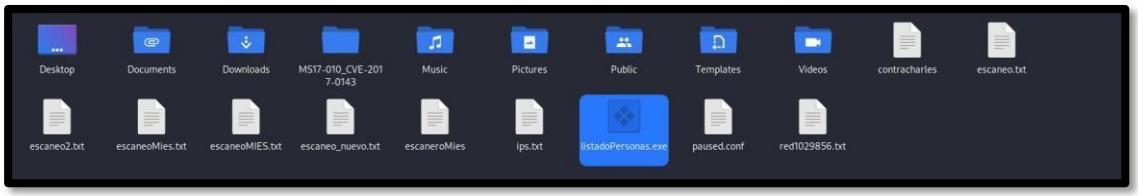


Imagen 51: Virus creado exitosamente

25. Luego se usó un exploit de tipo handler como se muestra a continuación para dar inicio al proceso multi/handler.

Imagen 52: Multi/Handler

26. Se definió la carga útil para que así sea un Shell inverso de Windows y lograr su adaptación con el ejecutable ya creado mediante msfvenom, indicamos el LHOST y el LPORT para escucha y estaría listo para ser ejecutado.

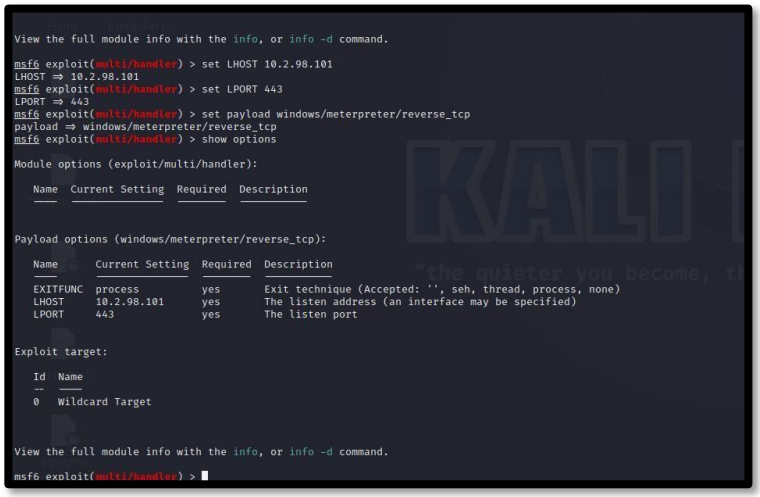


Imagen 53: Modificación de dirección y puerto para la escucha

27. Para finalizar se ejecutó el comando run para así poder quedar en escucha de lo que ocurra en el puerto configurado.

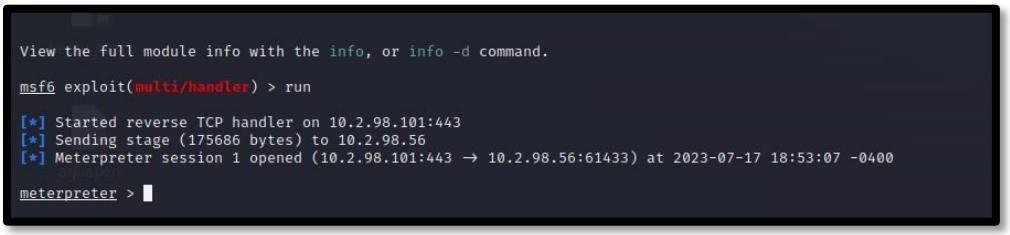


Imagen 54: Ejecución del virus

28. Una vez ejecutado el archivo en la máquina víctima se observará como se activa el payload de Meterpreter en la consola Metasploit obteniendo así control total sobre la máquina vulnerada.

Imagen 55: Control toral de la máquina con meterpretar

29. Documentos extraídos

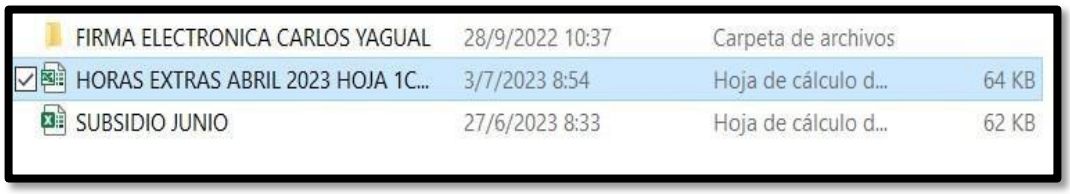


Imagen 56: Información extraída de la máquina víctima

Ataque: Puerta Trasera – Backdoor – villain

Objetivo: Crear una puerta trasera la máquina víctima para efectuar una rever_shell

30. Descargar Villain del repositorio de GitHub

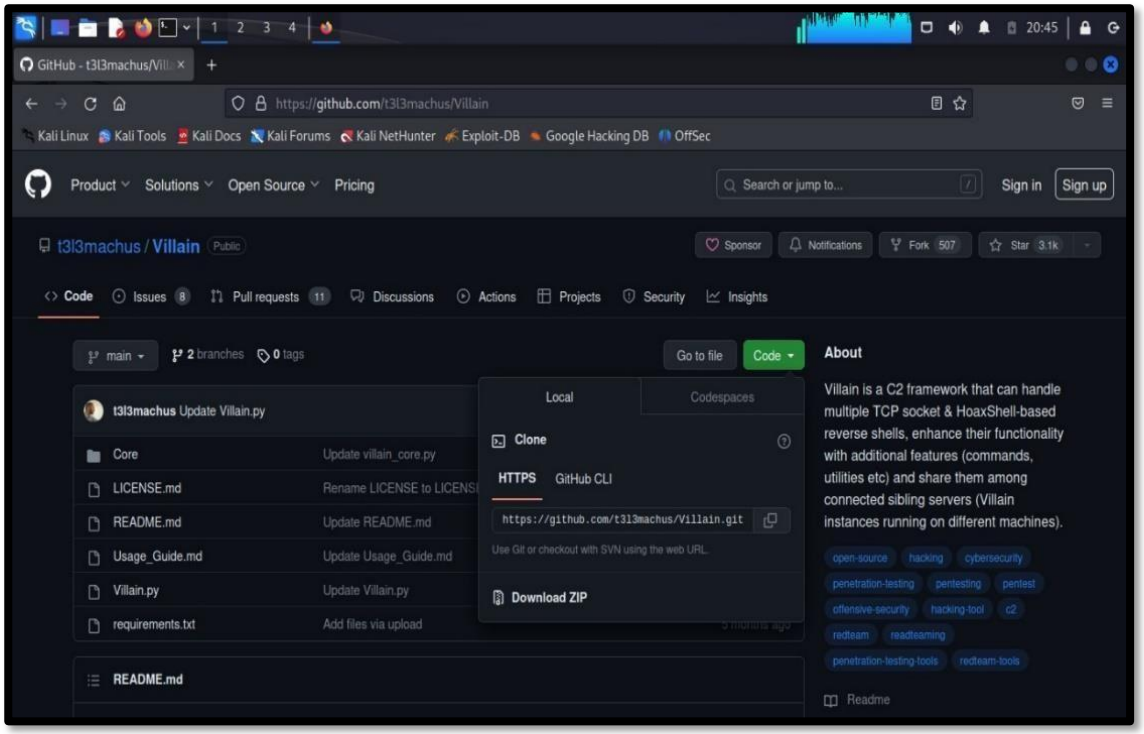


Imagen 57: Búsqueda de Villain por Github

31. Ejecutar la clonación del repositorio

Imagen 58: Clonación del repositorio de Villain

32. Ubicar dentro de la carpeta

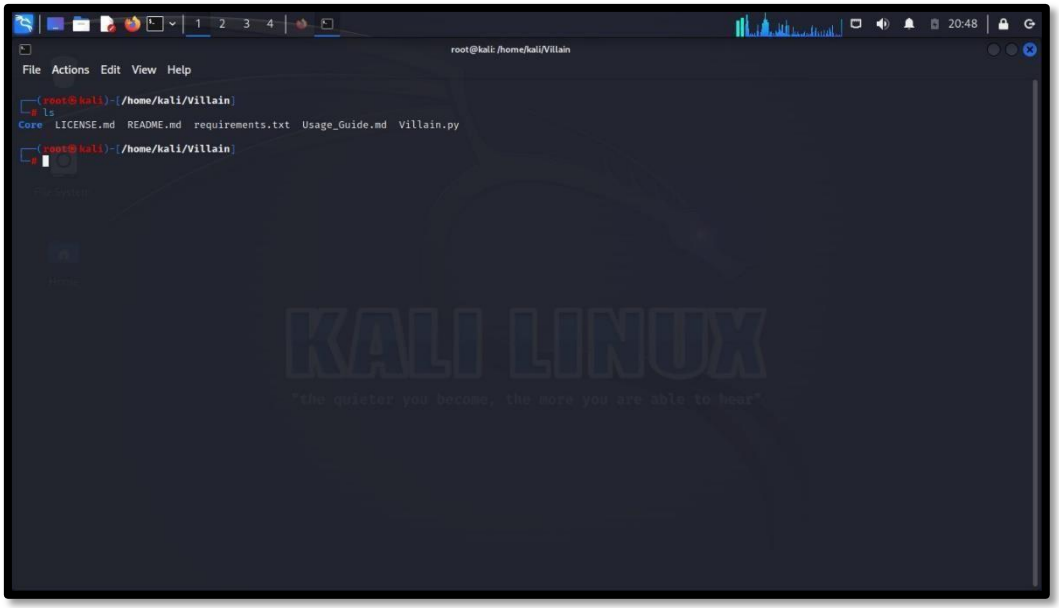


Imagen 59: Direccionarse a la carpeta Villain

33. Efectuar el cambio de permiso del archivo con chmod +x para dar permiso de ejecución

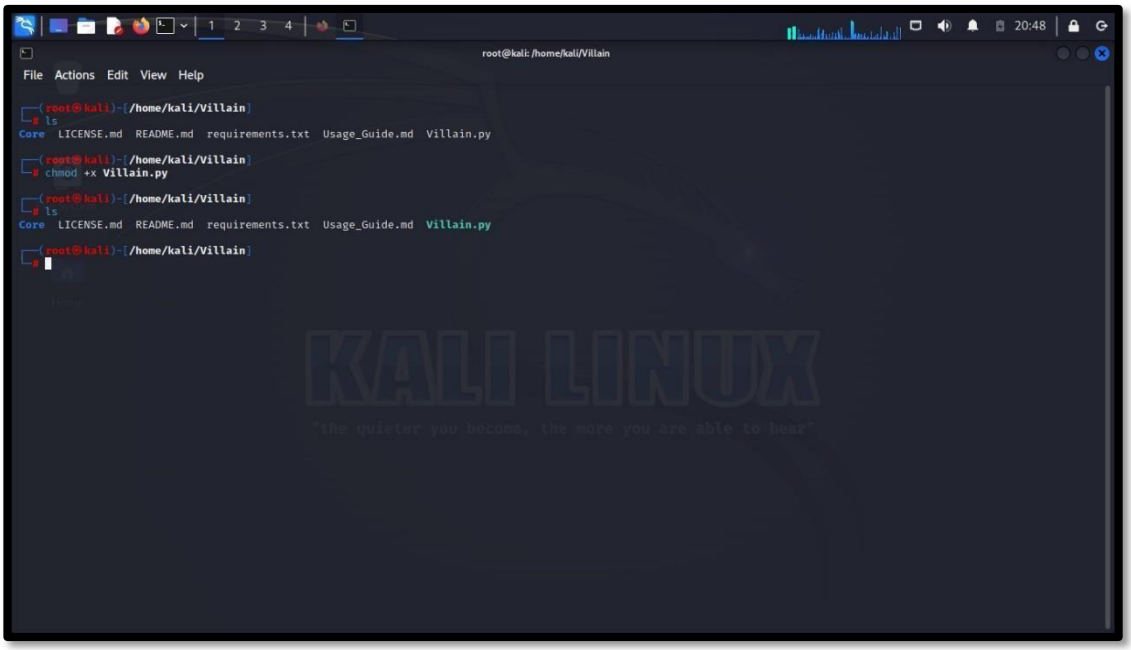


Imagen 60: Cambio de permiso al Script Villain

34. Instalar los requerimientos de Python del archivo requeriments.txt que contiene liberas necesarias para ejecutar el script

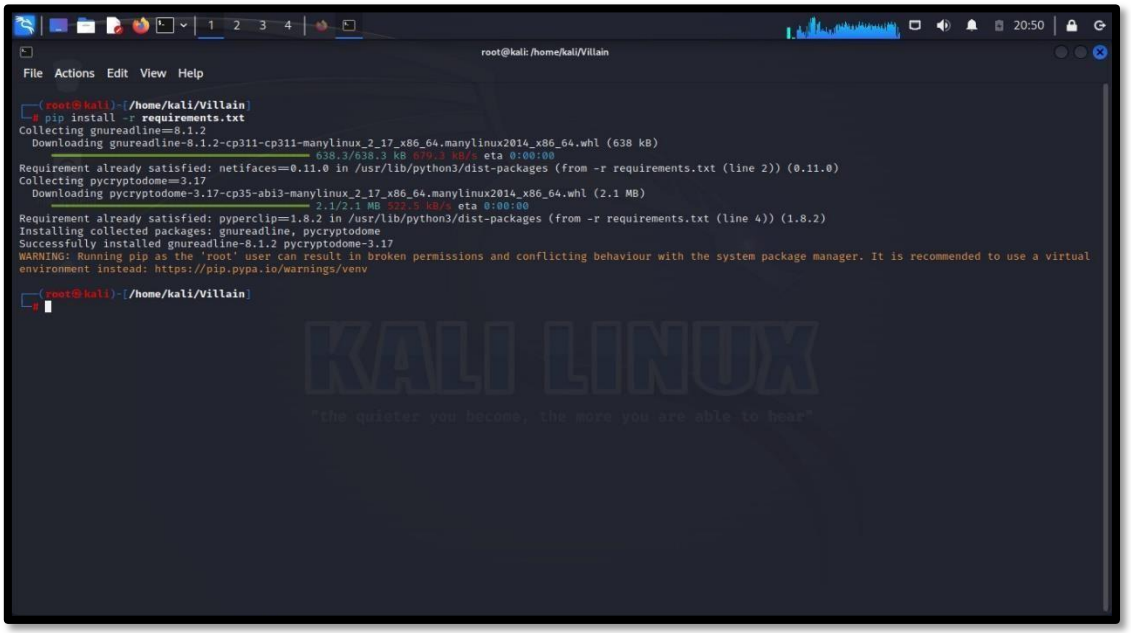


Imagen 61: Instalación de paquetes del archivo requeriments.txt

35. Ejecución de la herramienta python3 Villain.py

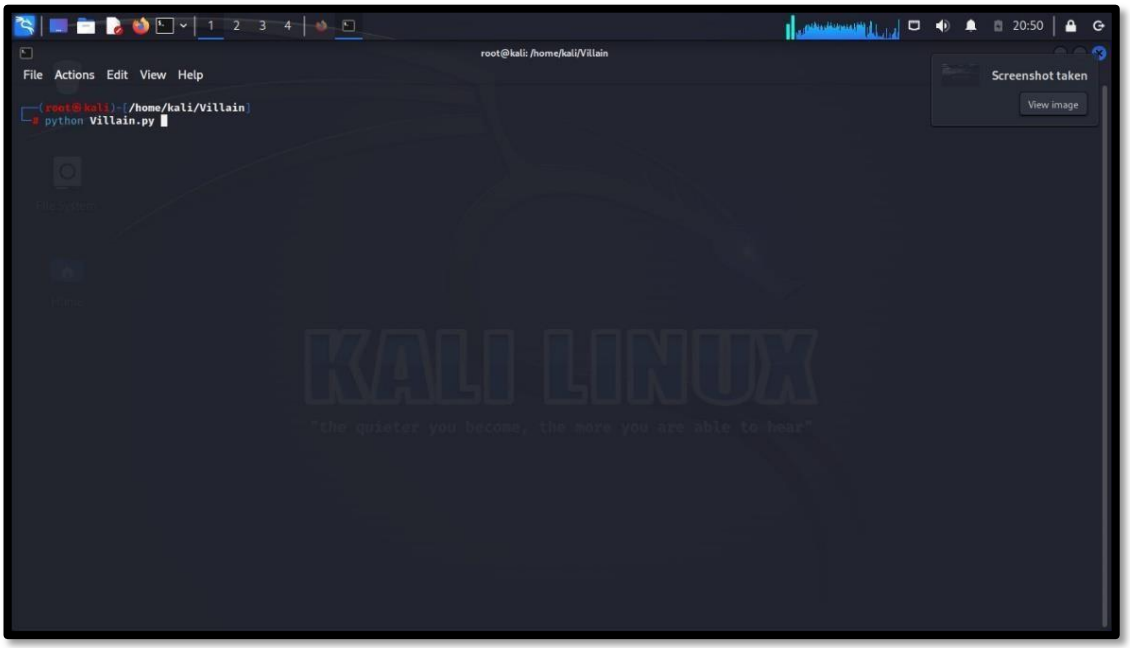


Imagen 62: Comando de inicio de script

36. Generar el payload respectivo para el sistema operativo Windows

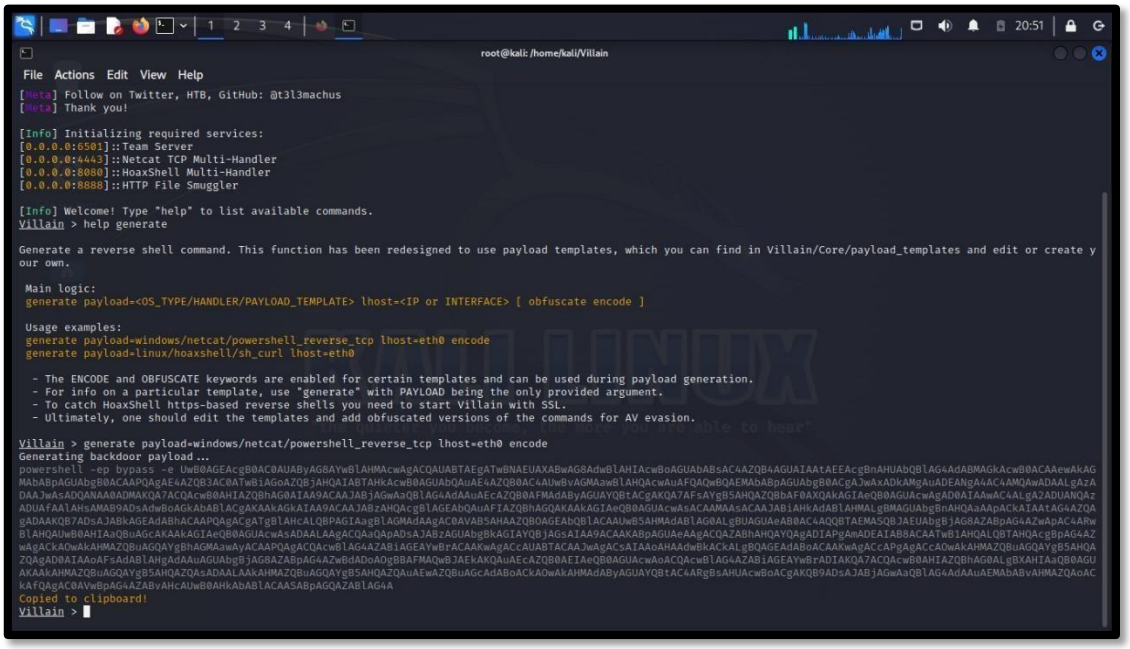


Imagen 63: Paylod generado exitosamente

37. Iniciar el servidor de Python para poder efectuar la descarga del archivo txt

Imagen 64:Inicio del servidor Python

38. Descargar el archivo por el servidor.

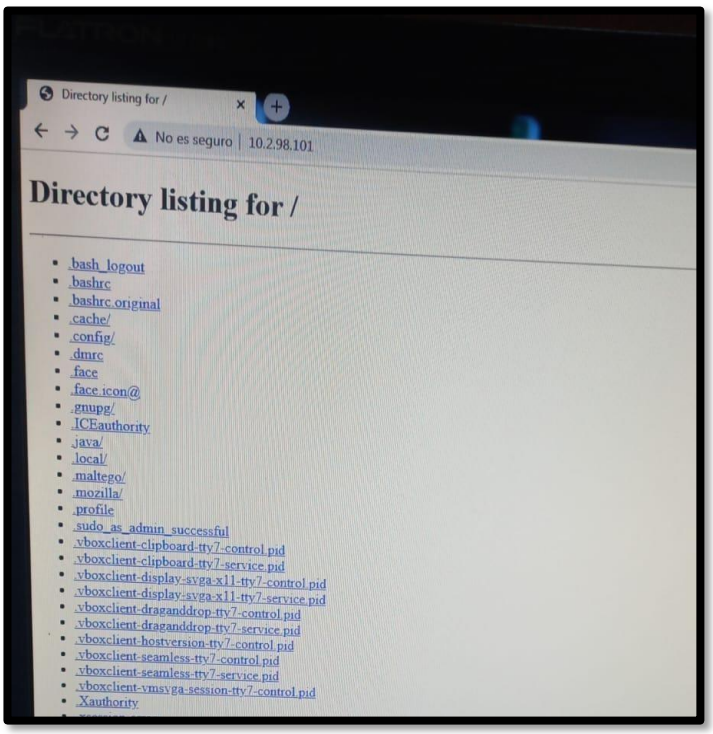


Imagen 65: Descarga del archivo txt

39. Copiar el contenido para insertar en la terminal de la máquina y ejecutar

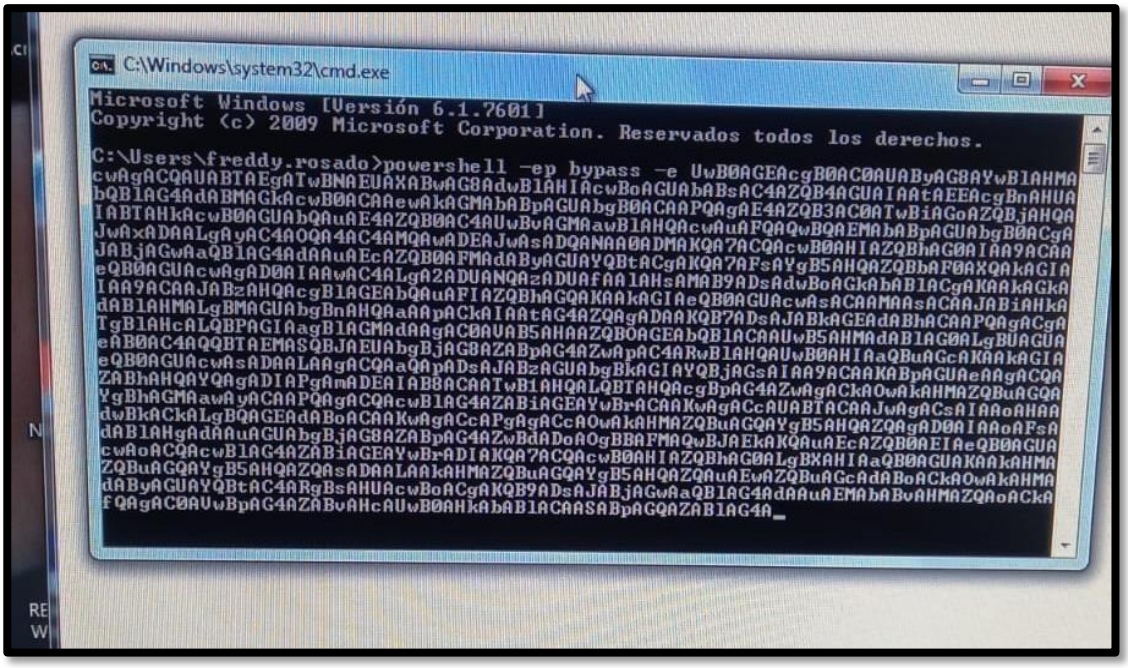


Imagen 66: Inserción de Payload en el terminal Víctima

40. Máquina vulnerada y presenciado en Villain

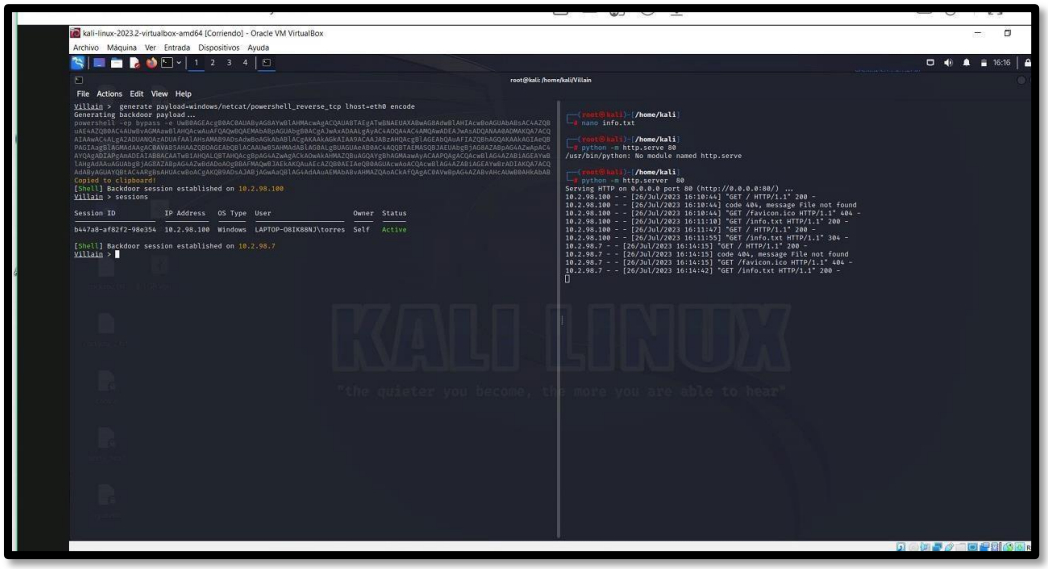


Imagen 67: Payload ejecutado exitosamente

41. Insertar el comando sessions y luego el comando Shell de la session se da la reverse_shell

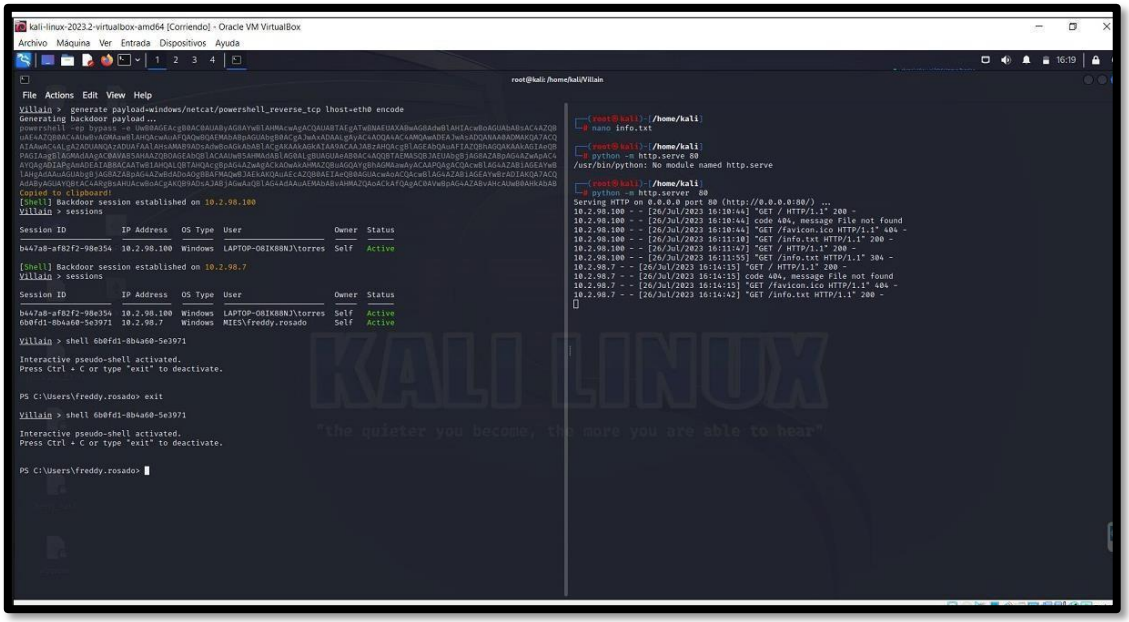


Imagen 68: Ejecución de reverse_shell

42. Con el comando net user se ve la información del usuario Windows

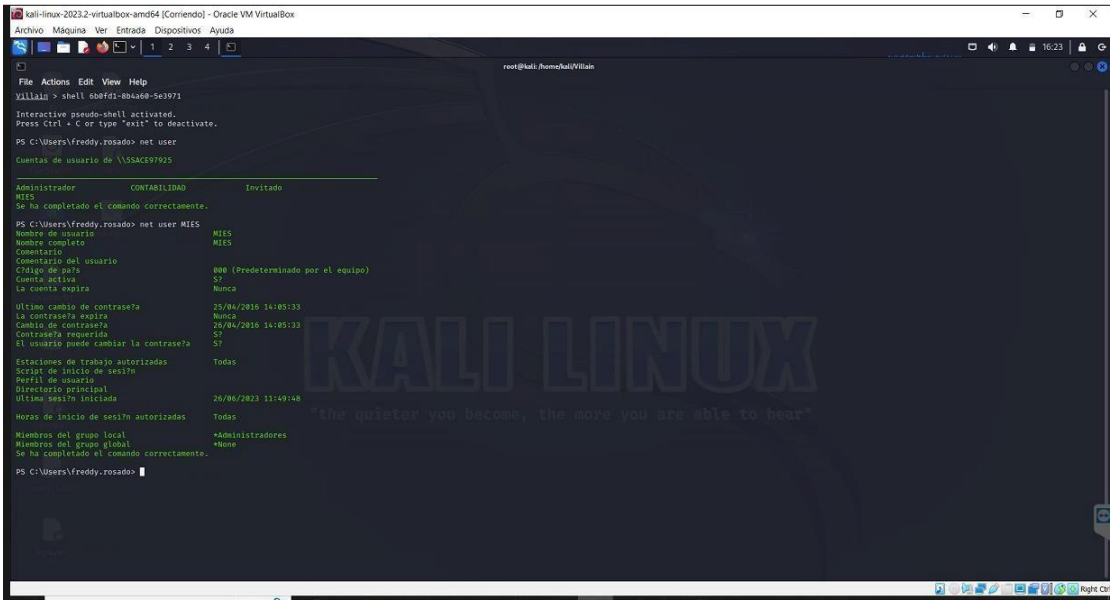


Imagen 69: Información de usuario

Anexo 5

Reporte

REPORTE

INDICE

2. PENTESTING A LA RED

3. DATOS DE LA INSTITUCIÓN

Objetivo: Red MIES – Salinas (Ministerio de Inclusión Económica y Social)

Fecha: 20- Julio-2023

Preparado por: Torres Lara Mayerli

Periodo: 2023

4. ALCANCE DE INTRUSION

El test de pentesting en el objeto mencionado consiste en la identificación, análisis de vulnerabilidades y amenazas que se encuentran presenten en la red. El enfoque es centrado con la metodología OSSTMM en la base de la seguridad en la red informática para la realización de la fase de intervención que corresponde en el desarrollo de los ataques seleccionado las amenazas como; Denegación de Servicio, Interpretación, Man In The Midle, Malware, Acceso no Autorizado, Debilidad en Sistemas Operativos. Aquellos que permitirán entender el arte de hacking ético en un contexto real y presentar los fallos para desarrollar una propuesta de mitigación.

5. EVALUACIÓN DE RESULTADOS

5.1. ESCANEO DE RED

5.1.1. ESCANEO DE PUERTOS Y SERVICIOS

La evaluación de seguridad permite la indagación de procesos claves para la intrusión, el escaneo de puertos y la enumeración de información son dos aspectos principales para desarrollar pruebas de penetración. Con la ayuda de nmap y crackmapexec la identificación de host activos vulnerables esenciales para doblegar la seguridad.

NMAP

Análisis: El desarrollo de escaneo de puerto sobre el objeto red dio como resultado el hallazgo de diversos servicios sobre los dispositivos conectado a la red.

Por lo tanto, el escaneo permite indagar y conocer los estados de puertos para así ejercer el correspondiente estudio de vulnerabilidades para comprometer

Interpretación: Se halló 21 dispositivos en la red tras el escaneo de la red mediante, encontrando servicios en común como Msrpc, Netbios-ssn, Micrsoft-ds servicio proveniente de samba. Todos con la finalidad de ejercer comparticiones de recursos de un lugar a otro(dispositivos)

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.2 CISCO SYSTEM	135	Msrpc	Sirve para el servicio remote procedu call en S.O Windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	2968	Enpp	Servicios particulares
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota

DIRECCIÓN	PUERTO	SERVICIO	USO

10.2.98.5 HON HAI PRECISION	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	2968	Enpp	Servicios particulares
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	5357	wsdapi	Sirve para descubrir y compartir funciones, capacidades a otros dispositivos que estén en la red

DIRECCIÓN	PUERTO	SERVICIO	USO
	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.

10.2.98.6 HEWLETT PACKARD	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	2968	Enpp	Servicios particulares
	3389	ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	5120	Barracuda-bbs	Funciones de sistemas BBS tradicionales
	5357	wsdapi	Sirve para descubrir y compartir funciones, capacidades a otros dispositivos que estén en la red
	49152	Unknown	Puertos efímeros
	49153	Unknown	Puertos efímeros
	49154	Unknown	Puertos efímeros

DIRECCIÓN	PUERTO	SERVICIO	USO

10.2.98.7 DELL LNC	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	2968	Enpp	Servicios particulares
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	5357	wsdapi	Sirve para descubrir y compartir funciones, capacidades a otros dispositivos que estén en la red
	14000	Scotty-ft	SCOTTY High-Speed File transfer
	49152	Unknown	Puertos efímeros
	49153	Unknown	Puertos efímeros
	49154	Unknown	Puertos efímeros

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.8	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
DELL LNC	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	2968	Enpp	Servicios particulares
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	5357	wsdapi	Sirve para descubrir y compartir funciones, capacidades a otros dispositivos que estén en la red
	14000	Scotty-ft	SCOTTY High-Speed File transfer
	49152	Unknown	Puertos efímeros

	49153	Unknown	Puertos efímeros
	49154	Unknown	Puertos efímeros

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.9	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
DELL LNC	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	2968	Enpp	Servicios particulares
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	5357	wsdapi	Sirve para descubrir y compartir funciones, capacidades a otros dispositivos que estén en la red

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.10	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
DELL LNC	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	2968	Enpp	Servicios particulares
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	49152	Unknown	Puerto efímero

DIRECCIÓN	PUERTO	SERVICIO	USO
	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un

10.2.98.11			programa se ejecute un proceso en otra que se encuentra en propia red.
	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	2968	Enpp	Servicios particulares
DELL LNC	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	49152	Unknown	Puerto efímero
	49153	Unknown	Puerto efímero
	49154	Unknown	Puerto efímero

DIRECCIÓN	PUERTO	SERVICIO	USO
	80	HTTP	Es usado para realizar peticiones de datos y recursos en un entorno web
	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un

10.2.98.12			programa se ejecute un proceso en otra que se encuentra en propia red.
	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
DELL LNC	2968	Enpp	Servicios particulares
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	49152	Unknown	Puerto efímero
	49153	Unknown	Puerto efímero
	49154	Unknown	Puerto efímero

DIRECCIÓN	PUERTO	SERVICIO	USO
	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un

10.2.98.17			programa se ejecute un proceso en otra que se encuentra en propia red.
HEWLETT PACKARD	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.18	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
DELL LNC	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	49152	Unknown	Puerto efímero

	49153	Unknown	Puerto efímero
	49154	Unknown	Puerto efímero

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.19	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
DELL LNC	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	2968	Enpp	Servicios particulares
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.21	135	Msrpc	Sirve para el servicio remote procedu call en S.O Windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
DELL LNC	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	1025	NFS -or- IIS	Servicios particulares
	1026	LSA-or-nterm	Servicios particulares
	1027	IIS	Servicios particulares
	1028	Uknown	Servicios particulares
	1060	Polestar	Servicios particulares
	1067	Instal_bots	Servicios particulares

	2968	Enpp	Servicios particulares
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	5357	wsdapi	Sirve para descrubir y compartir funciones, capacidades a otros dispositivos que estén en la red

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.22 DELL LNC	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota

	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	5357	Wsdapi	Sirve para descrubir y compartir funciones, capacidades a otros dispositivos que estén en la red

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.26	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
HON HAI PRECISIONLND CO.LTD	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota

	5357	Wsdapi	Sirve para descrubir y compartir funciones, capacidades a otros dispositivos que estén en la red

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.32	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
HON HAI PRECISIONLND CO.LTD	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.35	139	Netbios-ssn	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.

DELL LNC	445	Microsoft-ds	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	1025	NFS -or- IIS	Servicio Particular
	1026	LSA-or- nterm	Servicio Particular
	1027	IIS	Servicio Particular
	1050	Java-or-otgfileshare	Servicio Particular
	1055	Ansyslmd	Servicio Particular
	1093	Proofd	Servicio Particular
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	5357	Wsdapi	Sirve para descrubir y compartir funciones, capacidades a otros dispositivos que estén en la red

DIRECCIÓN	PUERTO	SERVICIO	USO
	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un

10.2.98.58 HON HAI PRECISIONLND CO.LTD			programa se ejecute un proceso en otra que se encuentra en propia red.
	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	2968	enpp	Servicios particulares
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	5000	upnp	Sirve para construir diversas aplicaciones y servicios
	5357	wsdapi	Sirve para descubrir y compartir funciones, capacidades a otros dispositivos que estén en la red
	49152	Uknown	Puerto efímero
	49153	Uknown	Puerto efímero

	49154	Uknown	Puerto efímero

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.63	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
XEROX CORPORTION	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota
	49152	Uknown	Puerto efímero
	49153	Uknown	Puerto efímero
	49154	Uknown	Puerto efímero

DIRECCIÓN	PUERTO	SERVICIO	USO
10.2.98.97 **DELL LNC**	135	Msrpc	Sirve para el servicio remote procedu call en S.O windows. Permite que un programa se ejecute un proceso en otra que se encuentra en propia red.
	139	Netbios-ssn	Es el servicio de NetBIOS que permite una aplicación de red se comunique con otra para ejercer acciones de recursos compartidos: como impresoras, entre otras acciones.
	445	Microsoft-ds	Es conocido como Server Message Block, permite ejercer acciones de recursos compartidos utilizando la red local o remota
	2968	Enpp	Servicio particular
	3389	Ms-wbt-server	Sirve para conexión y control remoto de un ordenador desde otra máquina, sirve para manejar servidores de manera remota

DIRECCIÓN	PUERTO	SERVICIO	USO
	80	Http	Es usado para realizar peticiones de datos y recursos en un entorno web

10.2.98.150 HON HAI PRECISIONLND CO.LTD	81	Hosts2-ns	Puerto alterno para enviar contenido a la web
	443	Https	Sirve para cifrar la comunicación de HTTP transformar a HTTPS
	1069	Cognex-insight	Servicio Particular
	1247	Visionpyramid	Servicio Particular
	1352	Lotusnotes	Servicio Particular
	1720	H233q931	Servicio Particular
	2040	1am	Servicio Particular
	2135	Gris	Servicio Particular
	7001	afs3-callback	Servicio Particular
	7778	interwise	Servicio Particular
	8443	Https-alt	Sirve para comunicarse al Https de servidores
	13456	Uknown	Puerto efimero
	20222	Ipulse-ics	Puerto efimero
	22939	Uknown	Puerto efimero
	25735	Uknown	Puerto efimero
	49167	Uknown	Puerto efimero

	50300	Uknown	Puerto efimero

5.1.2. CRACKMAPEXEC – ENUMERACI ÓN DE HOST – SAMBA

Análisis: El desarrollo del mapeo de la red cuenta con diversos enfoques y otro punto esencial es el hallazgo de recursos compartidos, host activos, usuarios válidos, entre otros que se relacionen a la seguridad en redes y sistemas Windows. El enfoque fue centrado en la dirección red de estudio para encontrar información relevante para ejercer la identificación de vulnerabilidades para dar paso a intrusión a una puerta trasera.

Interpretación: Se halló 35 dispositivos relacionados con el servicio Samba emitido por el puerto 445 y a su vez se dio al hallazgo de los nombres de los dispositivos dominio y el sistema operativo Windows en uso.

crackmapexec smb 10.2.98.0/24	DIRECCIÓN	PUERTO	NOMBRE	DOMINIO	S.O
SMB	10.2.98.10	445	55ACE97679	mies.min	Windows 7 ultimate
SMB	10.2.98.54	445	55ACE97672	mies.min	Windows 10 Pro
SMB	10.2.98.7	445	55ACE97925	mies.min	Windows 7 Ultimate
SMB	10.2.98.23	445	55ACE97944	mies.min	Windows 7 Ultimate

SMB	10.2.98.6	445	55ACE97917	mies.min	Windows 7 Professional
SMB	10.2.98.32	445	55ACE97663	mies.min	Windows 7 Ultimate
SMB	10.2.98.35	445	55ACE97922	mies.min	Windows 7 Ultimate
SMB	10.2.98.12	445	55ACE97685	mies.min	Windows 7 Ultimate
SMB	10.2.98.4	445	55ACE97665	mies.min	Windows 7 Ultimate
SMB	10.2.98.13	445	55ACETMP01	mies.min	Windows 7 Ultimate
SMB	10.2.98.18	445	55ACE97681	mies.min	Windows 7 Ultimate
SMB	10.2.98.47	445	55ACE97666	mies.min	Windows 10.0 Build
SMB	10.2.98.22	445	55ACE97661	mies.min	Windows 7 Ultimate
SMB	10.2.98.21	445	55ACE97926	mies.min	Windows 10.0 Build
SMB	10.2.98.17	445	55ACE97932	mies.min	Windows 7 Ultimate
SMB	10.2.98.15	445	55ACE97673	mies.min	Windows 10.0 build

SMB	10.2.98.41	445	55ACE81059	mies.min	Windows 7 Ultimate
SMB	10.2.98.37	445	55ACE97674	mies.min	Windows 7 Ultimate
SMB	10.2.98.45	445	55ACE97619	mies.min	Windows 10.0 Build
SMB	10.2.98.14	445	55ACE97924	mies.min	Windows 7 Ultimate
SMB	10.2.98.36	445	55ACE97683	mies.min	Windows 10 pro
SMB	10.2.98.39	445	55ACE97664	mies.min	Windows 7 Ultimate
SMB	10.2.98.19	445	55ACE7656	mies.min	Windows 10.0 Build
SMB	10.2.98.2	445	55ACE81008	mies.min	Windows 10.0 Build
SMB	10.2.98.55	445	55ACE81005	mies.min	Windows 7 Ultimate
SMB	10.2.98.43	445	55ACE97667	mies.min	Windows 7 Ultimate
SMB	10.2.98.26	445	55ACE97655	mies.min	Windows 10.0 Build

SMB	10.2.98.56	445	55ACE97929	mies.min	Windows 7 Professional
SMB	10.2.98.58	445	55ACE97921	mies.min	Windows 7 Ultimate
SMB	10.2.98.67	445	Z524D02CDI0061	mies.min	Windows 8 Pro
SMB	10.2.98.63	445	55ACE81006	mies.min	Windows 7 Ultimate
SMB	10.2.98.100	445	LAPTOP-08IK88NJ	mies.min	Windows 10.0 Build
SMB	10.2.98.40	445	55ACE97676	mies.min	Windows 7 Ultimate
SMB	10.2.98.25	445	NONE	mies.min	X64

Por otro lado, tras un análisis más profundo se obtuvo como la herramienta nmap tras el desarrollo del comando nmap –script “vuln and safe” –p445 ip proporciono el hallazgo de 5 dispositivos vulnerables al conocido CVE 2017-0143 conocido como vulnerabilidad EternalBlue

RESULTADOS OBTENIDOS					
IP	**MAC**	**PUERTO**	**SERVICIO**	**VULNERABLE**	**CVE**
10.2.98.56	00:17:A4:F1:B2:83	445/tcp	Microsoft-ds	Mircrosoft SMBv1 servers	CVE-2017-0143

10.2.98.51	D0:27:88:DE:D6:23	445/tcp	Microsoft-ds	Mircrosoft SMBv1 servers	CVE-2017-0143
10.2.98.54	70:71:BC:BD:41:8B	445/tcp	Microsoft-ds	Mircrosoft SMBv1 servers	CVE-2017-0143
10.2.98.36	B8:AC:6F:46:DA:3A	445/tcp	Microsoft-ds	Mircrosoft SMBv1 servers	CVE-2017-0143
10.2.98.32	00:21:70:63:A6:A1	445/tcp	Microsoft-ds	Mircrosoft SMBv1 servers	CVE-2017-0143

5.1.3. MASSCAN

Análisis: Analizar la red desde un modo eficaz y rápida para conocer los puertos posibles de la red objeto, como es el caso del puerto 80 y 445. Herramienta esencial para recolección de información y datos primarios

Interpretación: Se halló 39 direcciones en modo On en donde se distribuye en 4 direcciones con puerto 80 y 35 con puerto 445

RESULTADOS OBTENIDOS CON MASSCAN			
IP	**PUERTO**	**PROTOCOLO**	**ESTADO**
10.2.98.12	80	tcp	On
10.2.98.24	80	tcp	on
10.2.98.150	80	tcp	on

10.2.98.14	80	tcp	on
10.2.98.67	445	tcp	on
10.2.98.47	445	tcp	on
10.2.98.40	445	tcp	on
10.2.98.36	445	tcp	on
10.2.98.44	445	tcp	on
10.2.98.100	445	tcp	on
10.2.98.43	445	tcp	on
10.2.98.31	445	tcp	on
10.2.98.55	445	tcp	on
10.2.98.97	445	tcp	on
10.2.98.22	445	tcp	on
10.2.98.54	445	tcp	on
10.2.98.56	445	tcp	on
10.2.98.51	445	tcp	on
10.2.98.14	445	tcp	on
10.2.98.10	445	tcp	on
10.2.98.21	445	tcp	on
10.2.98.25	445	tcp	on

10.2.98.39	445	tcp	on
10.2.98.6	445	tcp	on
10.2.98.52	445	tcp	on
10.2.98.19	445	tcp	on
10.2.98.13	445	tcp	on
10.2.98.35	445	tcp	on
10.2.98.18	445	tcp	on
10.2.98.45	445	tcp	on
10.2.98.4	445	tcp	on
10.2.98.17	445	tcp	on
10.2.98.32	445	tcp	on
10.2.98.58	445	tcp	on
10.2.98.12	445	tcp	on
10.2.98.9	445	tcp	on
10.2.98.26	445	tcp	on
10.2.98.2	445	tcp	on
10.2.98.63	445	tcp	on
10.2.98.7	445	tcp	on

5.1.4. ARP-SCAN

Análisis: La realización de la evaluación de la red, identificar los hosts del objeto es punto esencial de partida para comprender al fondo los diversos dispositivos para comprometer y que servicios puede contar.

Interpretación: Se halló 35 dispositivos conectado a la red con su respectivo dirección MAC

RESULTADOS OBTENIDOS CON ARP-SCAN		
IP	**MAC**	**SERVICIO**
10.2.98.1	70:81:05:97: AA:BE	Unknown
10.2.98.2	78:45:C4:04:78:72	Unknown
10.2.98.5	D0:27:88:DE:DI:C9	Unknown
10.2.98.7	B8:AC:6F:47: B2:E0	Unknown
10.2.98.10	78:45:C4:04:78:1C	Unknown
10.2.98.17	AC: 16:2D: 00:2E:DB	Unknown
10.2.98.18	78:45:C4:04:82:41	Unknown
10.2.98.23	D0:27:88:DE: D6:D9	Unknown
10.2.98.25	D0:27:88:DE: D6: C9	Unknown
10.2.98.26	D0:27:88: DE: D6:5C	Unknown
10.2.98.24	9C: 93:4E: 16:87:3A	Unknown
10.2.98.31	D0:27:88: DE: D5: B8	Unknown
10.2.98.32	00:21:70: 63:46: A1	Unknown

10.2.98.39	6C: 62:6F: DE: 70: C1	Unknown
10.2.98.41	D4:C9:EF:DE:D6:8D	Unknown
10.2.98.44	D0:27:88:DE:D6:8D	Unknown
10.2.98.52	80: C1:6E:ED:E2:52	Unknown
10.2.98.56	00:17: A4:F1:82:83	Unknown
10.2.98.58	B8:AC:6F:45:BD:94	Unknown
10.2.98.97	DO:27:88:DE:D6:7C	Unknown
10.2.98.100	B6:F6:85:43:F7:C9	Unknown
10.2.98.150	00: E0:07:07: 04:97	Unknown
10.2.98.151	2C:F4:C5:F5:B3:AB	Unknown
10.2.98.152	2C:F4:C5:F5:B3:97	Unknown
10.2.98.154	2C: F4:C5: F6: E:F1	Unknown
10.2.98.155	2C: F4:C5:F6:F0:25	Unknown
10.2.98.156	2C: F4:C5: F5:B3: FA	Unknown
10.2.98.157	2C:F4:CS: F6:EF:B1	Unknown
10.2.98.158	2C:F4: C5:F6: EF:80	Unknown
10.2.98.159	2C: F4:C5: F6: EE :09	Unknown
10.2.98.161	2C:F4: C5:F5: B3:CF	Unknown
10.2.98.162	2C:F4:C5:F5:A4:75	Unknown

10.2.98.170	A0:F3: C1:C5:8B: EF	Unknown

5.1.5. NESSUS

Análisis: El enfoque de desarrollo del análisis, utilizando OSINT (Open Source Intelligence), ha permitido obtener una comprensión exhaustiva del comportamiento de la red, utilizando fuentes abiertas para recopilar información. Nessus ha sido una herramienta clave en la realización de escaneos de seguridad integrales.

Nessus ha sido esencial para realizar escaneos de seguridad en diversos aspectos, como redes, Su versatilidad ha permitido adaptarse a diferentes contextos y tipos de sistemas, proporcionando resultados detallados sobre vulnerabilidades presentes en la red analizada.

Interpretación: Tras la ejecución de la herramienta sobre la red ofuscada en modo avanzado dio como resultado 22 vulnerabilidades, diversos tipos de servicios como es el más común SMB distribuido por SAMBA, sistemas operativos, entre otros**.**

RESULTADOS OBTENIDOS CON NESSUS	
Vulnerabilidades encontradas	22
Tipo de servicios web	SMB CIFS
Puertos escaneados	6
Tipo de terminal	Microsoft Windows
Vulnerabilidades de alto riesgo	0
Vulnerabilidades de Riesgo medio	11

Vulnerabilidades de bajo riesgo	11
Tipo de análisis	Análisis avanzado
Tiempo inicial	13:00
Tiempo final	17:00
DNS	inclusion.gob.ec
Ip	192.168.x.x
Nivel de gravedad	Medio
Sistema Operativo del Host	Windows Server 2019
Detalles de los Puertos Escaneados	Puertos 135, 139, 445, 3389, 8080, 8443
Vulnerabilidades de Riesgo Medio	MS17-010: Vulnerabilidad de ejecución remota de código
Acciones Recomendadas	Aplicar el parche MS17-010, desactivar servicios no necesarios
Contexto sobre el Análisis Avanzado	Utilizó técnicas de escaneo exhaustivas y análisis profundo
Consideraciones de Seguridad Adicionales	Firewall en funcionamiento, políticas de seguridad implementadas. Se recomienda una revisión continua de configuraciones de seguridad.

Entorno de Red	Red corporativa con segmentación de subredes. Se recomienda una revisión de la topología de red para identificar posibles puntos de vulnerabilidad.

5.2. FUZZ TESTING

5.2.1. MAIN THE MIDLE

Análisis:

El enfoque en interceptar y manipular datos destaca como un aspecto crítico para la potencial sustracción de información sensible. La investigación se centró en la identificación de variantes con el propósito de evaluar la seguridad de las redes, destacando la importancia de proteger la integridad de la línea de comunicación. Se buscó comprender el impacto que podría derivarse de la falta de seguridad, permitiendo a un tercero ofuscar, robar y manipular datos de manera no autorizada.

Interpretación:

La aplicación de fuzz testing reveló la posibilidad de dirigir flujos de datos desde una IP de inicio hacia una IP de destino, aprovechando el tamaño de la información transmitida en tiempo real. Se identificaron protocolos en uso, fragmentos de código, páginas web, y se constató que la institución emplea métodos de cifrado robustos como MD5 y SHA256 para resguardar la integridad y confidencialidad de sus datos. Este hallazgo resalta la importancia de implementar medidas de seguridad proactivas y la adopción de estándares criptográficos sólidos para mitigar posibles riesgos en la manipulación y robo de información.

Detalles de Tráfico:

PROTOCOLO	IP ORIGEN	IP DESTINO	TAMAÑO
HTTP	10.2.98.100	10.2.98.150	268

HTTP	10.2.98.150	10.2.98.100	76
HTTP	10.2.98.100	10.2.98.150	278
HTTP	10.2.98.150	10.2.98.100	332
HTTP	10.2.98.100	142.250.78.132	271

Análisis de Tráfico:

TIPO DE ANALISIS	DURACION DEL ANALISIS
Análisis avanzado	45 minutos

Protocolos Identificados:

#	PROTOCOLO
1	HTTP
2	ARP
3	ICMP
4	LLMNR
5	TCP
6	BROWSER
7	CDP
8	DCERPC
9	MDNS

10	SMB2
11	SSDP
12	TLSv1.3
13	UDP

Hosts con Mayor Actividad:

Datos Enviados:

#	IP
1	10.2.98.100
2	10.2.98.150
3	10.2.98.64
4	10.2.98.65
5	10.2.98.24

Datos Recibidos:

#	IP
1	10.2.98.100
2	142.250.78.132
3	131.100.1.169
4	00:17:a4:f1:82:83
5	10.2.98.150

Observaciones y Conclusiones:

1. **Tráfico HTTP Intenso:**

   - Se detecta tráfico HTTP entre 10.2.98.100 y 10.2.98.150 con variados tamaños, indicando intercambio de datos web significativo

2. **Destacados:**

   - 10.2.98.100 es el principal emisor y receptor de datos, sugiriendo una alta actividad en la red.
   - Otros hosts involucrados: 10.2.98.150, 10.2.98.64, 10.2.98.65, 10.2.98.24, 10.2.98.25.

3. **Diversidad de Protocolos:**

   - Se identifican múltiples protocolos (HTTP, ARP, ICMP, etc.), indicando una variedad de actividades en la red.

Recomendaciones:

- Realizar un monitoreo continuo de tráfico para identificar patrones y posibles amenazas.
- Verificar la seguridad de las comunicaciones HTTP entre 10.2.98.100 y 10.2.98.150.
- Evaluar la configuración de seguridad de los hosts destacados**.**

5.2.2. NETWORKMINER

Análisis: La saturación previa de datos sobre el tráfico de la red en tiempo real dio como resultado el hallazgo sobre servicios en uso y host en comunicación. Por lo tanto, se capturo archivos, tablas, entre otros.

Interpretación: Tras el análisis de trafico de red se encontró 205 Host interpretado credenciales de servicios en común de protocolos.

Análisis de Seguridad de la Red:

Aspecto	Detalles
Tipo de Análisis	Medio
Duración	45 minutos
Número de Hosts	205
Análisis de Imagen	No aplicable
Archivos Analizados	No aplicable
Credenciales Utilizadas	SNMPv1, SNMPv2c
Comunidades SNMP	Public

Datos Adicionales:

Categoría	Cantidad
DNS	774
Parámetros Analizados	4200
NetBIOS	Sí (Detalles Adicionales Necesarios)
Protocolos Utilizados	SNMP, DHCP
Información sobre SNMP	Detalles Necesarios

Observaciones:

- El análisis se llevó a cabo con un enfoque de nivel medio durante un período de 45 minutos, explorando 205 hosts en la red.
- No se realizó un análisis de imágenes ni se examinaron archivos específicos durante esta sesión.
- Se emplearon credenciales SNMPv1 y SNMPv2c con la comunidad "public" para obtener información del equipo de red.
- Se generaron 774 consultas DNS para evaluar la resolución de nombres en la red.
- Se analizaron 4200 parámetros, detallando la complejidad y el alcance del análisis.
- Se detectaron consultas NetBios, se requieren detalles adicionales para una evaluación más precisa.
- Se identificaron protocolos como SNMP y DHCP, señalando la diversidad de servicios en la red**.**

5.3. EXPLOTACION DE VULNERABILIDAD

La implantación de virus o troyano sobre un sistema tiene como objetivo escalar privilegios y proporcionar los permisos correspondientes, para aquello se conoció el previo reconocimiento de puertos, servicios por donde ofuscar y ejercer una puerta trasera.

5.3.1. BACKDOOR

Análisis: La correcta elaboración de script malicioso se relaciona con el sistema operativo, payload y el modo de ejecución. El código Villain permite ejercer un encode para ser insertado en el terminal de la víctima y ejercer la reverse_shell, pero para ello es necesario desactivar la opción de antivirus tanto el que se usa como el defender.

Interpretación: La inserción del payload malicioso sobre el objeto permitió recolectar información valiosa como la opción de crear, modificar, o eliminar cualquier archivo y a su vez ver que archivos cuenta datos interesantes. Como

resultado se encontró archivos comprometedores y a su vez la data del usuario.

Resultado:

Resultado: Por motivo de confiabilidad no es permitido mostrar la información de los archivo y nombres. Punto a resaltar, la cantidad de activos fue hallado mediante la ruta del usuario vulnerado principal mediante comando y y efectivamente se realizó la previa de la desactivación de antivirus cuando el usuario se descuido

TIPO ARCHIVO	CANTIDAD
DOC	10
XLSX	5
PDF	10
TXT	5
LNK	10
EXE	2
TOTAL	32

5.3.2. VIRUS- MSFVENOM

Análisis: El desarrollo de una carga útil se ve influenciado a través del conocimiento sobre el objeto a comprometer, vulnerabilidad. Msfvenom permite crear el payload o carga útil malicioso que permite comprometer la seguridad para desarrollar intrusiones de escala de privilegio ya sea en comando como el famoso reverse_shell o petición de un playload relacionado a su exploits.

Interpretación: La correcta ejecución del virus informático o carga útil maliciosa en termino técnico fue oculto mediante un archivo pdf que cualquier usuario pueda observar con la única diferencia que cuenta con el ejecutable para doblegar la seguridad. Como resultado permitió encontrar archivos muy comprometedores y

algunos fáciles de eliminar, copiar y sacar uso

Resultado: Por motivo de confiabilidad no es permitido mostrar la información de los archivo y nombres. Punto a resaltar, la cantidad de activos fue hallado mediante la ruta del usuario vulnerado principal en donde se ejecutó la carga maliciosa y efectivamente se realizó la previa de la desactivación de antivirus cuando el usuario se descuido

TIPO ARCHIVO	CANTIDAD
DOC	10
XLSX	5
PDF	10
TXT	5
LNK	10
EXE	2
TOTAL	32

5.4. ACCESO NO AUTORIZADO

5.4.1. ATAQUE DE FUERZA BRUTA JOHN REPAER

Análisis: El hallazgo de credenciales mediante ataque de fuerza bruta es desarrollado desde el punto de vista de obtener conjunto necesario para doblegar la seguridad encriptada de una contraseña mediante una herramienta necesaria y obtener el resultado esperado.

Interpretación: Para ello se utilizado el conocido ataque de fuerza brute de diccionario mediante la obtención del hash de los usuarios que desarrollaron acción en la red envenado para recuperar el hash de formato NNTLMV2 logrando corromper 5 usuarios que se detalla a continuación.

USUARIO	HASH	RESULTADO
MIES\betty.solorzano	betty.solorzano::MIES:5435128f40aae1ce: 6D19ECAAEC143AAFD1BF7E8C13EFD1A6:0 101000000000000021A5F8B6BEAED901D2D479659CD9FA02000000000	Por confiabilidad no se puede mostrar
MIES\charles.zambrano	charles.zambrano::MIES:8827d0062f0be906: AD3B86D89321A79D4ADF0596586EB608: 0101000000000000152D080EEB8D9014014E4680F9B0CF1000000000	Por confiabilidad no se puede mostrar

AGUAPEN\nortiz	nortiz::AGUAPEN:e77961765464769a: B9EDACB48169606D19EE8B538905F303 :0101000000000000080279986D1B8D9014024F7C883B9D5470000000	Por confiabilidad no se puede mostrar
MIES\55ACE97685	5SACE97685$::MIES:090645475278c33b: 7ABBC885F24A6CDA694E1BFA433546E1: 0101000000000000FB2EF80AF4B8D901AE7528B1B8186D340000000002	Por confiabilidad no se puede mostrar
MIES\5SACETMP01	5SACETMP01$::MIES:35bcea4ea34155ee: 42988F56C0CD4D74F09CF76AB4EA2950: 0101000000000000022EDE2DFB4AED90126C077B771649588000	Por confiabilidad no se puede mostrar

5.5. DEBILIDAD EN SISTEMAS OPERATIVOS

5.5.1. SAMBA RELAY

Análisis: Es notorio como la debilidad de los sistemas operativos es otro punto esencial que poco tomado en cuenta, El ataque Samba Relay permite capturar la intercepción de acciones y sesiones mediante el protocolo SMB que se utiliza para compartir archivos y recursos en la red sobre los Sistemas Windows.

Interpretación: Se halló el hash en formato NTLMV2 de 5 usuarios gracias al envenenamiento de la red producto de responder para así luego descifrar el usuario con sus credenciales y acceder a la máquina.

IPV4	DIRECCION MAC	USERNAME	HASH
10.2.98.11	00:80:9F:AF:C2:2A	MIES\betty.solorzano	betty.solorzano::MIES:5435128f40aae1ce: 6D19ECAAEC143AAFD1BF7E8C13EFD1A6: 0101000000000000021A5F8B6BEA
10.2.98.12	00:80:9F:AF:C2:15	MIES\charles.zambrano	charles.zambrano::MIES:8827d0062f0be906: AD3B86D89321A79D4ADF0596586EB608: 0101000000000000152D080EEB8D
	fe80::1861:ce49:6112:d3a4	AGUAPEN\nortiz	nortiz::AGUAPEN:e77961765464769a: B9EDACB48169606D19EE8B538905F303: 0101000000000000802799866D
10.2.98.12	fe80::9cf4:189d:ec2a:5e59	MIES\55ACE97685	5SACE97685$::MIES:090645475278c33b: 7ABBC885F24A6CDA694E1BFA433546E1: 0101000000000000FB2EF80AF4B8D901AE

10.2.98.13	B8:AC:6F:46:C4:AC	MIES\5SACETMP01	5SACETMP01$::MIES:35bcea4ea34155ee:42988F56C0CD4D74F09CF76AB4EA2950:0101000000000000022EDE2DFB4AED90126

OBSERVACIONES

- Los resultados obtenidos mediante el análisis de seguridad en la red mediante la herramienta nmap y crackmapexec para mapear y enumerar hosts, servicios, entre otros, dio como enfoque que ciertos servicios no deben existir en modo open ya que es muy perjudicial su estado. Debido a que se puede realizar la explotación correspondiente por versiones, modo ataque, inserción de exploit, malware que convenga del arte de hacking ético
- A continuación del punto uno, es muy importante tener en cuenta la actualización de los sistemas operativos. Puesto que crackmapexec es responsable de hacer conocer aquellos dispositivos obsoletos desactualizado para poder ejercer el cometido de ataque por desactualizaciones como es el famoso ataque de eternal blue del CVE 2017-0143.
- La utilización de la herramienta Advanced Ip Scanner sobre el objeto red, permitió encontrar un total de 48 activos que hace mención a dispositivos conectados a la red conocer la MAC, nombre, Fabricante, entre otros puntos. Así mismo las herramientas Masscan, Arp-Scan
- La apertura Fuzz Testing sobre el enfoque víctima dio como resultado los siguientes puntos a observar:

    - Se pudo observar fragmentos de código, de páginas web, que eran modificados, script de JavaScript, diseño web con css

- Durante el análisis realizado, se pudo determinar que los hosts con más interacciones fueron 10.2.98.100, 10.2.98.150, 10.2.98.164.
- La cantidad de datos presentes en la red fue muy grande, durante la cantidad de tiempo empleada.
- La institución cifra sus datos con MD5 SHA256, entre 16 a 64 bits, recordando que entre más alto sea el número de bits en el cifrado, más difícil es descifrarlo.
- Las conexiones establecidas en red muestran protocolos como ICMP, es decir, correo electrónico, utilizan Zimbra/Admin

- Mediante NetworkMiner para analizar el tráfico de la red se llegó a los siguientes resultados:

  - 503 host que interactuaron entre sí, al momento de enviar o recibir información, se determinó también que, dentro de estos, se encontraron direcciones ip de servidores y páginas externas
  - Se obtuvo 275 archivos, entre ellos certificados SSL, html con fragmentos de códigos de páginas web, xls y archivos txt
  - 98 credenciales de inicio de cesión, entre públicas y cifradas con NTLM
  - Cuando se habla de sesión en la aplicación se refiere al registro de actividad del host hallado también el puerto por donde se realiza a comunicación
  - Determinó diferentes parámetros como NeTBios query, SNMP community, txt

- El resultado mostrado por la implementación de malware para crear puerta trasera como es el backdoor, permitió doblegar la seguridad fácilmente por el descuido del usuario, ya que en ocasiones tener sesión abierta o descargar algo sospechoso es clave para romper la seguridad. Por ello, es factible

concientizar a los usuarios. Se insertó el payload efectivamente en el terminal y con el virus se ejecutó de sin falla alguna.

- Los resultados encontrados por ataque de fuerza bruta por diccionario en John repaer, dio la efectividad de como tener contraseñas débiles, un simple diccionario regado por el internet es esencial para desencintar una contraseña y el modo de uso. Por ende, se dio la apertura de robar las credenciales de los usuarios victimas que son usuarios potenciadores y se evidenció activos para ser hurtados.
- El resultado evidenciado del ataque de samba relay permitió encontrar los hash de los usuarios víctimas para así luego ejercer el ataque de fuerza bruta para encontrar la contraseña. El modo de realización fue tan sencillo con solo envenena a la red con responder herramienta potencial para capturar peticiones por acciones y con espera el resultado de ataque puede ser completado, se halló debilidad por contraseña, usuarios, dirección
- El estudio de los exploits sobre las versiones obsoletas de S.O son cruciales y tener Windows antiguo provocaría ejercer el ataque de eternalblue. Por ello se observa como existe en la mayoría máquinas Windows 7 profesional y Windows 7 Ultímate sistemas operativos potenciales para comprometer y robar información

INFORME

INFORMACIÓN GENERAL

Fecha de Análisis: 20-Julio-2023

Responsable: Torres Lara Mayerli

Entidad Analizada: MIES-Salinas (Ministerio de Inclusión Económica y Social)

RESUMEN EJECUTIVO

El estudio consiste en indagar la infraestructura de la red de la entidad MIES – ministerio de inclusión social y económica distrital salinas que imparte servicios correspondientes a la inclusión social y atención durante el ciclo de vida. Por ende, imparte relevancia importante de información de datos que deben ser protegido en todo su aspecto físico y tecnológico.

Las entidades tanto pequeñas, grandes y de instituciones públicas deben arraigarse a un control de administración de ciberseguridad que permita evaluar y conocer los eventos ocurrentes para conocer los puntos débiles y en problemas que deben ser solucionados de manera inmediata

Por lo tanto, el análisis de esta magnitud debe contar con la investigación de vulnerabilidades y amanzanas frecuentes presente en las redes informáticas y reflejado con la ayuda de CVE que consiste en la catalogación de vulnerabilidades de seguridad conocidas y publicas en la red para gestionar de forma correcta y eficiente los problemas de seguridad tanto como lo es software y hardware.

METODOLOGÍA

Todo estudio de ciberseguridad relacionado con hacking ético y seguridad informática cuenta con una metodología referencial como pautas para el cumplimiento de lo requerido. La metodología OSSTMM es la esencial y elegida para el estudio de la seguridad en la red informática MIES en donde permite centrar la correcta gestión seguridad de los activos de información correspondiente a sus fases encerradas principalmente en el proceso de intervención que corresponde en la estructuración de los eventos de ataques correspondiente a las amenazas y vulnerabilidades que es; denegación de servicio, intrusión de servicios por samba relay, acceso no autorizado, entre otros que son comunes en redes informáticas.

HALLAZGOS

PROBLEMAS ENCONTRADOS	NUMERO DE CVE	DESCRIPCION	SEVERIDAD	POTENCIAL DE IMPACTO
Interrupción de servicios operacionales importantes	CVE-2018-6789	Se descubrió un problema en la función base64d en el escucha SMTP en Exim antes de 4.90.1. Al enviar un mensaje elaborado a mano, puede producirse un desbordamiento de búfer. Esto se puede utilizar para ejecutar código de forma remota [56].	ALTA	Daño de reputación correspondiente a la interrupción grave a los servicios
Acceso no autorizado a información confidencial	CVE-2019-6340	En versiones de Drupal 8.5.x a 8.5.11 y Drupal 8.6.x a 8.6.10,	ALTA	Posesión completa del sistema que permite el

		hay una vulnerabilidad que afecta a ciertos campos, permitiendo la ejecución arbitraria de código PHP si se cumplen condiciones específicas. Se recomienda actualizar a las versiones mencionadas para mitigar el riesgo. En Drupal 7, el módulo de Servicios no requiere una actualización, pero deben aplicarse otras actualizaciones asociadas si se utilizan los Servicio [57].		objetivo de manipular los datos sensibles
Robo de identidad del personal colaborativo como activos importantes como financieros y políticos	CVE-2009-3960	Vulnerabilidad no especificada en BlazeDS 3.2 y versiones anteriores, usadas en LiveCycle 8.0.1, 8.2.1 y 9.0, LiveCycle Data Services 2.5.1, 2.6.1 y 3.0, Flex	MEDIO	La divulgación de datos cruciales del personal colaborativo como así mismos datos financieros como la suplantación de identidad

		Data Services 2.0.1 y ColdFusion 7.0.2, 8.0, 8.0.1 y 9.0. Permite a atacantes remotos obtener información confidencial mediante solicitudes y manipulación de documentos XML [58].		
Manipulación de datos emitidos en el tráfico de la red por ambas partes	CVE-2014-0224	OpenSSL antes de 0.9.8za, 1.0.0 antes de 1.0.0m y 1.0.1 antes de 1.0.1h permite ataques intermedios que activan el uso de una clave maestra de longitud cero, exponiendo sesiones y datos confidenciales en ciertas comunicaciones OpenSSL a OpenSSL, conocida como la vulnerabilidad de "inyección CCS" [59].	MEDIO	Manipulación de datos en la trasmisión de comunicación permitiendo el acceso no autorizado al sistema
Bajo rendimiento del sistema	CVE-2017-0144	El servidor SMBv1 en Microsoft Windows Vista	MEDIO	Bajo rendimiento del sistema provocando así

		SP2; Servidor de Windows 2008 SP2 y R2 SP1; Windows 7 SP1; Ventanas 8.1; Servidor Windows 2012 Gold y R2; Windows RT 8.1; y Windows 10 Gold, 1511 y 1607; y Windows Server 2016 permite a atacantes remotos ejecutar código arbitrario a través de paquetes manipulados, también conocido como "Vulnerabilidad de ejecución remota de código de Windows SMB". Esta vulnerabilidad es diferente de las descritas en CVE-2017-0143, CVE-2017-0145, CVE-2017-0146 y CVE-2017-0148 [60].		la debilidad de seguridad para robo de datos críticos
	CVE-2020-1472	Existe una vulnerabilidad de elevación de privilegios	ALTA	Debilidad a la integridad de la información, confiabilidad y

Compromiso en la privacidad de la confidencialidad de los datos		cuando un atacante establece una conexión de canal seguro de Netlogon vulnerable a un controlador de dominio, utilizando el protocolo remoto de Netlogon (MS-NRPC), también conocido como 'vulnerabilidad de elevación de privilegios de Netlogon' [61].		disponibilidad y posibles interrupciones a los servicios emergentes
Exposición de información sensible presentando riesgo de seguridad informática	CVE-2019-0708	La vulnerabilidad de ejecución remota de código existe en los Servicios de Escritorio remoto, anteriormente conocidos como Servicios de Terminal Server, cuando un atacante no autenticado se conecta al sistema de destino mediante RDP y envía solicitudes especialmente diseñadas,	ALTA	Brechas de seguridad dando paso a vulnerabilidades abiertas que permiten el ataque informático para exponer los datos sensibles de la identidad

		también conocida como 'Vulnerabilidad de ejecución remota de código de los Servicios de Escritorio remoto' [62].		
Escalada de privilegios en sistemas operativos	CVE-2022-1111	Se descubrió una vulnerabilidad que permite la escalada de privilegios en sistemas operativos populares. Un atacante local podría aprovechar esta vulnerabilidad para obtener privilegios elevados en el sistema, comprometiendo la seguridad global del entorno [63].	ALTA	Posibilidad de manipulación y control indebido del sistema operativo
Vulnerabilidad en el protocolo de cifrado	CVE-2022-34042	Se encontró una vulnerabilidad en el protocolo de cifrado utilizado por una aplicación crítica para la comunicación segura. Esta vulnerabilidad	ALTA	Riesgo de exposición de datos confidenciales durante la transmisión

		podría permitir a atacantes realizar ataques de tipo man-in-the-middle y acceder a datos confidenciales transmitidos entre el cliente y el servidor [64].		
Debilidad en la autenticación de usuarios	CVE-2020-9876	Una debilidad en el proceso de autenticación de usuarios permite ataques de fuerza bruta exitosos, comprometiendo la seguridad de las cuentas de usuario. Los atacantes podrían obtener acceso no autorizado a sistemas y servicios sensibles mediante la adivinanza de contraseñas débiles [65].	ALTA	Riesgo de acceso no autorizado y compromiso de la confidencialidad de cuentas de usuario
Vulnerabilidad en el servicio de autenticación	CVE-2022-27194	Una vulnerabilidad crítica fue identificada en el servicio de autenticación utilizado en la infraestructura. Esta falla podría permitir a	ALTA	Riesgo de acceso no autorizado y compromiso de la confidencialidad de datos

		atacantes eludir la autenticación y ganar acceso no autorizado a sistemas y datos protegidos [66].		
Vulnerabilidad en el control de acceso de archivos	CVE-2022-3456	Una vulnerabilidad en el sistema de control de acceso de archivos permite a usuarios no autorizados leer, modificar o eliminar archivos críticos. Esto podría conducir a la pérdida de datos importantes y afectar la integridad del sistema [67].	ALTA	Riesgo de pérdida de datos críticos y compromiso de la integridad del sistema
Vulnerabilidad en el control de acceso a la red	CVE-2016-7890	Una vulnerabilidad en las políticas de control de acceso a la red permite a dispositivos no autorizados conectarse a la red corporativa. Esto podría facilitar ataques internos y comprometer la seguridad de la	ALTA	Riesgo de acceso no autorizado a la red interna y compromiso de la seguridad de la red

		red, permitiendo a intrusos obtener acceso no autorizado a sistemas y datos internos [68].		
Fallo en la gestión de contraseñas	CVE-2022-41694	Un fallo en la gestión de contraseñas en una aplicación empresarial permitió la exposición de contraseñas almacenadas en texto plano. Esto representa un riesgo significativo, ya que los atacantes podrían obtener acceso no autorizado a cuentas y sistemas que utilizan estas contraseñas [69].	ALTA	Riesgo de acceso no autorizado y compromiso de la confidencialidad de contraseñas
Exploits conocidos no parcheados	CVE-2022-6789	La presencia de exploits conocidos no parcheados en sistemas críticos expone el sistema a amenazas persistentes. Estos exploits podrían ser utilizados por atacantes para	ALTA	Riesgo de explotación persistente y compromiso continuo de la seguridad del sistema

		comprometer la seguridad del sistema y realizar acciones maliciosas sin ser detectados [70].		

RECOMENDACIONES

Se dará a continuación recomendaciones técnicas que deben ser tomadas en cuenta acorde a los resultados.

- Es recomendable filtrar los servicios como en pocas maquinas se observa, así permite aumentar la seguridad que ningún atacante puede conocer el servicio y por donde atacar**.**
- Se debe incorporar los parches de seguridad en los servicios, actualizaciones debido que en si caso es ignorado provocaría fallas y apertura para que cualquier malware, virus, troyano puede explotar la debilidad.
- Tener mucho en cuenta el tratamiento de los activos de información como emplear seguridad de claves sobre aquellos tipos de archivos potenciadores que cuenta información sensible como cuentas, firmas electrónicas, contraseñas.
- Emplear un administrador de contraseña para que en ocasiones la contraseña no sea la misma y cuente con una estructura diferente, con qué fin. Fácil tener una buena gestión de credenciales de usuarios.
- Es súper recomendable tener las contraseñas de su user bien privado y no dejarlo en cualquier lugar de la oficina o puesto de trabajo porque caso omiso punto fácil de intrusión.
- Emplear actualizaciones de Sistemas operativos, debido que sistemas operativos anteriores pueden traer fallas y por esas fallas comprometer toda

la data que cuenta el usuario actualizar es una opción muy optima y amigable por seguridad.

- No ingresar a direcciones sospechosa y peor descargar archivos desconocidos. La utilización de antivirus es esencial para evitar descarga desconocida.
- Es recomendable emplear firewall en la red y administrar los sitios accesibles, así la seguridad de la red es más fuerte y así comprometer sería complicado.
- Emplear políticas de seguridad de contenido (CSP).
- Ejerce búsqueda de problemas encontrados en CVE, NSIT que corresponde temas de ciberseguridad