UNIVERSIDAD ESTATAL
PENINSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

EXAMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

ANALISÍS E IMPLANTACIÓN DE TÉCNICAS Y HERRAMIENTAS DE ETHICAL HACKING PARA LA CIBERSEGURIDAD

AUTOR

GARCÍA PERERO FREDDY GIANCARLO

LA LIBERTAD- ECUADOR
2021

APROBACIÒN DEL TUTOR

En mi calidad de tutor/tutora del trabajo de componente práctico del examen de carácter complexivo: “ANALISÍS E IMPLANTACIÓN DE TECNICAS Y HERRAMIENTAS DE ETHICAL HACKING PARA LA CIBERSEGURIDAD”., elaborado por el/la sr/ta. (a) GARCÍA PERERO FREDDY GIANCARLO, de la carrera de Tecnología de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes.

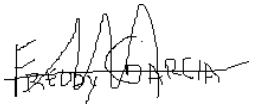
La libertad, **10 de marzo del 2021.**

……..

Ing. Iván Alberto Coronel Suárez, MSIA.

DECLARACIÓN

El contenido del presente componente práctico del examen de carácter complexivo es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.



.....
Freddy Giancarlo García Perero

AGRADECIMIENTO

En primera instancia agradezco a Dios por brindarme entendimiento para llegar al punto en donde me encuentro, a mis docentes que son personas de gran sabiduría que me han formado para hoy llegar al punto donde me encuentro, a familiares, amigos y personas especiales de mi vida este nuevo logro es en gran parte gracias a ustedes y que sin su ayuda no podría haber culminado una meta más en mi vida.

García Perero Freddy

DEDICATORIA

A mis padres por haberme formado como la persona que soy; a mi esposa e hija ya que muchos de mis logros se los debo a ellas incluido este y a todas las personas que me han apoyado; y además de ser una parte importante durante mi formación académica

García Perero Freddy

TRIBUNAL DE GRADO

Ing. Samuel Bustos Gaibor, Mgt.
DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

LSI. Daniel Quirumbay Yagual, MSIA.
DOCENTE ESPECIALISTA

Ing. Iván Alberto Coronel Suárez, MSIA
DOCENTE TUTOR

Ing. Alicia Andrade Vera, Mgt.
DOCENTE GUÍA UIC

RESUMEN

Este presente proyecto pretende determinar el uso de la herramienta correcta para mitigar ataques cibernéticos mediante un laboratorio implantado en una red local, además de dar a conocer la mejor técnica para resolver ciertas amenazas, que se estudiarán a continuación.

Actualmente en el mundo existe un elevado incremento de delitos informáticos, ya que estos cibercriminales no tan solo atacan a empresas particulares o privadas, sino que también lo hacen a usuarios específicos, entre los principales ataques a estudiar están los malware, phishing y los ataques de suplantación de identidad, estas amenazas son en la actualidad una de las principales causas de la sustracción de información con el fin de perjudicar al usuario.

Además, estudio brindara la información necesaria para conocer que herramienta debemos aplicar para la mitigación de los ataques analizados en ambientes simulados, las principales herramientas a evaluar se las escogió de acuerdo al grado de popularidad entre los usuarios.

También se utilizó los estándares basados en la metodología PTES, los cuales nos ayudan a estructurar de mejor manera nuestros ciberataques y así dar mejor entendimiento a nuestro proyecto; conjuntamente también se usará la investigación de carácter longitudinal que permitirá estudiar el comportamiento de la amenaza durante el periodo de ejecución del mismo.

Tabla de contenido

Índice de figuras

Índice de tablas

Índice de anexos

INTRODUCCIÓN

La presente investigación tiene como objetivo a ayudar a los usuarios a tener una herramienta y una técnica, las cuales se puedan implementar en cualquier ambiente de real permitiendo así la mitigación de los ciberataques realizados por personas inescrupulosas que tiene como fin la obtención de información confidencial de las víctimas, los cuales en su gran porcentaje son vulnerable.

El aumento de los ciberataques a nivel mundial está en crecimiento, el objetivo de estos cibercriminales va más allá del simple hecho de la obtención de información; ya además usan los datos obtenidos para causar algún tipo de daño a la víctima para beneficio propio, entre los principales ataques a nivel nacional e internacional tenemos el popular malware que se viene usando desde tiempos atrás y sigue mejorando su estructuración de ataque, el phishing una de las técnicas que usa la ingeniería social como aliado para esta proceso y por ultimo los ataque de suplantación de identidad entre los cuales tenemos Mide in the Middel(MitM).

Además, está basado en los estándares de la metodología PTES los cuales nos brindarán un mejor entendiendo de los procesos y pasos a ejecutar para la implantación de los ciberataques dentro de nuestro laboratorio informático obteniendo como resultado la herramienta y técnica más optima que permitirán llevar a cabo los ciberataques.

CAPÍTULO I

1. FUNDAMENTACIÓN

1.1.ANTECEDENTES

Uno de los principales problemas del uso del Internet es la inseguridad a la cual se enfrentan los internautas. Con respecto aquello, el progreso que ha experimentado la "gran red de redes" ha sido tan acelerada como el incremento de las amenazas informáticas que se difunden por este medio [1].

Actualmente vivimos una era digital en donde entidades gubernamentales, asociaciones, empresas o usuarios son vulnerables a los ataques cibernéticos, donde personas oportunistas con un pequeño o amplio conocimiento informático tienen como objetivo principal obtener información confidencial dañando la integridad del objetivo y obteniendo un beneficio económico o sencillamente se puede convertir en juego para aquella persona [1].

Con la ayuda de técnicas y herramientas de ethical hacking podemos realizar un análisis profundo y darle una pronta solución al problema realizando simulaciones de los posibles casos donde se producen los ataques cibernéticos.

Según lo observado en la investigación de carácter exploratoria de los portales web de ataques cibernéticos en tiempo real, los ciberataques en el Ecuador van creciendo de manera paulatina, teniendo como un común denominador al usuario como principal amenaza ante estos ataques, y para garantizar la seguridad de la información se necesita de un conjunto de metodologías, sistemas, y herramientas (Ver Anexo1).

Además, según el estudio realizado por cisco en el año 2019; en su reporte de amenazas señala que a partir del año 2016 el uso de ransomware era unos de los principales métodos de ciberataque; y que a principios del 2018 este método está quedando para la historia, pero esto no quiere decir que se tiene que pasar por alto.

Actualmente la principal amenaza para los administradores de redes sería el robo de información a través de phishing, suplantación de identidad y malwares en general, bajo función de los altos índices de transacciones de información; estos códigos maliciosos pueden ser instalado por agente externos o por la propia víctima de manera sencilla ya que tienden a funcionar en segundo plano y pasan desapercibido para el usuario [2].

Por este motivo se desea realizar un análisis de las herramientas y técnicas que permitan estudiar los diferentes ataques que existen actualmente y como contrarrestarlo, guiados bajo un estándar

de pruebas de penetración, y así tener un mejor control de los procesos realizados por el usuario permitiendo llevar un seguimiento de las actividades realizadas y crear conciencia del uso correcto de las TICs.

La universidad politécnica de valencia llevo a cabo el desarrollo e implementación de un PENTEST, en donde su objetivo principal es pretender esbozar las fases que toda auditoria de seguridad informática debe tener, dentro de las cuales se usaron diversas herramientas y técnicas para la ejecución de este proyecto basándose en los estándares de PTES [3].

En Latinoamérica, la universidad católica de Colombia realizó un proyecto basado en la definición de una metodología de hacking ético para empresas públicas específicas, el principal alcance del este proyecto está en desarrollar un análisis de las vulnerabilidades encontradas logrando entregar un informe detallado de como mitigar las vulnerabilidades basados en las buenas prácticas para mantener una infraestructura informática segura [4].

En la universidad privada del norte en Perú se llevó a cabo la aplicación de una auditoria de Pentesting para la contribución de las medidas de seguridad de la información de los sistemas informáticos manteniendo la viabilidad, integridad, disponibilidad [5].

En Ecuador, la Universidad católica del Ecuador con sede en Esmeraldas estudio la propuesta de una metodología para la realización de pruebas de penetración logrando implementar una metodología que permita realizar pruebas de penetración en ambientes virtuales [6].

Los estudios realizados con anterioridad y las implantaciones ejecutadas fueron diseñadas bajo diferentes metodologías o sin ellas, la cual en a la actualidad no nos permiten saber que herramientas o técnicas son las adecuadas para el control de la ciberseguridad y como aplicarlas.

Luego del estudio realizado y basándonos como guía en los análisis hechos con anterioridad, se logró determinar que el estudio además de darnos unas pautas de cómo realizar un correcto manejo de la ciberseguridad también nos darán como resultado saber cuál es la mejor técnica y las mejores herramientas para la aplicación de la ethical hacking en la ciberseguridad.

1.2. DESCRIPCIÓN DEL PROYECTO

Este presente proyecto surge desde la idea de tener un mejor manejo y control sobre la ciberseguridad de las entidades, basadas en los estándares de la metodología PTES que permitan una buena gestión al momento de aplicar las pruebas de penetración, además de conocer herramientas y técnicas orientadas correctamente para el manejo de la ethical hacking. El presente estudio aplicara de referencia los ataques más concurridos a nivel nacional e internacional, entre los cuales tenemos:

El conocido phishing delito de engañar a las personas para que compartan información confidencial; los malware, por ejemplo: troyanos estos se camuflan como un software legítimo, para intentar acceder a los sistemas de los usuarios y finalmente el Ataques del Hombre en el Medio (MitM) se trata del ataque en dónde el atacante en este caso, posee la habilidad de controlar o desviar las comunicaciones entre dos partes.

Para la realización del presente proyecto, se llevará a cabo el desarrollo de las siguientes fases detalladas a continuación:

- **Fase de recolección de información:** Comprende la preparación del ambiente simulado y la recopilación de información necesaria para realizar los diferentes ataques a nuestros objetivos.
- **Fase de modelado de amenaza:** En esta fase se realiza el modelado y la búsqueda de herramientas necesarias, para ejecutar los ataques seleccionados en la implantación en el ambiente simulado.
- **Fase de análisis de vulnerabilidades:** En la siguiente fase se usan los datos recolectados de la primera fase, para encontrar vías o métodos de ataques que permitan vulnerar el sistema.
- **Fase de explotación:** Hace refiera a la ejecución del ataque a través de las diferentes herramientas seleccionadas en el modelado de la amenaza.
- **Fase de informe**: Una vez terminada las fases anteriores, se procede a documentar el proceso de cada ataque; además de seleccionar la herramienta más óptima para mitigar los ciberataques.

1.2.1. Hardware

Para el presente proyecto de análisis se requiere de la implantación de un laboratorio para el estudio de las herramientas y las técnicas, se utilizará una máquina Hp notebook 14 de procesador AMD A6-7310 APU con una tarjeta gráfica de Radeon R4 y una memoria RAM de 8 GB, además del uso de máquinas virtuales realizadas en virtual box con las siguientes descripciones: una estación para el hacker con un mínimo de 2 GB de RAM y un disco duro de 20 GB mínimo, 2 equipos victimas con 2GB de RAM con una mínimo de 20GB disco duro,1 router de wifi de marca Huawei Hg-8245H, 1 equipo servidor con un mínimo de 2GB de RAM y disco duro de 20GB.

1.2.2. Software

El software base a utilizar, es el sistema operativo Kali Linux en su versión 2020 para la ejecución de la mayoría de los ataques; además de otras diversas herramientas como: HTTrack Website Copier, Armitage, Ettercap.

Para la parte de análisis de vulnerabilidad se emplearán la herramienta: Wireshark; finalmente para la parte de detención de los ciberataques se usarán herramientas de antivirus en su versión free entre los cuales tenemos: Avast, AVG, ESET-NOD32; los cuales servirán para mitigar ciertos ataques.

Adicionalmente, las maquinas consideradas con víctimas de los ciberataques utilizaran como sistema operativo base Windows 10 y Windows server 2016 respectivamente virtualizados con la herramienta VirtualBox.

- **Kali Linux:** Es una distribución de Linux basada en Debian destinada a las pruebas de penetración avanzadas y la auditoría de seguridad, contiene varias herramientas que están orientadas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa [7].
- **VirtualBox:** Es una potente herramienta de virtualización para uso empresarial y doméstico. Además, no solo es un producto extremadamente rico en funciones y de alto rendimiento para clientes empresariales, sino que también es la única solución profesional que está disponible gratuitamente como software de código abierto bajo los términos de la General Public License (GPL) [8].
- **Windows server 2016:** Es un sistema operativo tipo servidor desarrollado por Microsoft como parte de la familia de sistemas operativos Windows NT, desarrollado simultáneamente con Windows 10. La primera versión preliminar estuvo disponible el

1 de octubre de 2014. Windows Server 2016 se lanzó el 26 de septiembre de 2016 en la conferencia Ignite de Microsoft y estuvo disponible en general el 12 de octubre de 2016 [9].

- **Windows 10**: Es la última versión de sistema operativo desarrollado por Microsoft como parte de la familia de Windows NT, la empresa la dio a conocer en el año 2014 y se lanzó al público en julio del 2015, lo distinto de esta versión es que Microsoft ofrece gratuitamente para aquellos usuarios que cuenten con copias originales de Windows 7 y Windows 8.1 update. Esta versión es una edición súper completa diseñado para toda la familia de los productos Microsoft tales como: laptops, tabletas, teléfonos inteligentes, Xbox One, entre otros. Esto se da gracias a su código casi idéntico que le permite tener tal compatibilidad [10].
- **Wireshark:** Es el analizador de protocolos de red más importante y más utilizado del mundo, que permite ver lo que está sucediendo en su red a un nivel microscópico en muchas empresas comerciales y sin fines de lucro, agencias gubernamentales e instituciones educativas. El desarrollo de Wireshark prospera gracias a las contribuciones voluntarias de expertos en redes de todo el mundo y es la continuación de un proyecto iniciado por Gerald Combs en 1998 [11].
- **Armitage:** Es una Herramienta que permite el uso de scripts para metasploit que permite visualizar objetivos, recomienda exploits y expone las características avanzadasde post-explotación que tiene el framework [12].
- **Avast Free Antivirus:** Es una herramienta proporcionada por una de las empresas de seguridad más grandes del mundo, utiliza tecnologías de última generación para hacer frente a los ciberataques en tiempo real; lo que la diferencia de otras compañías de última generación es que cuentan con un gigantesco motor de aprendizaje automático en la nube que recibe un flujo constante de datos de cientos de millones de usuarios, lo cual permite aprender a velocidades inusitadas y convierte a nuestro motor de inteligencia artificial en el más rápido e inteligente del mundo. [13].
- **HTTrack:** Esta herramienta permite descargar un sitio World Wide Web desde Internet a un directorio local, creando de forma recursiva todos los directorios, obteniendo HTML, imágenes y otros archivos desde el servidor a su computadora, además organiza la estructura de enlaces relativa del sitio original, también puede actualizar un sitio duplicado existente y reanudar las descargas interrumpidas. HTTrack es completamente configurable y tiene un sistema de ayuda integrado [14].

- **Stripo**: Es una herramienta que sirve para crear plantillas de correo electrónico gratuito, además de tener todas las plantillas de correo electrónico diseñadas con el editor de correo electrónico HTML. Por otra parte, nuestro editor le permite habilitar los botones VML para Outlook en sus correos electrónicos mediante un solo clic, también permite tener una previa visualización del correo electrónico antes de ser enviado [15].
- **ESET-NOD32:** En un antivirus protegido por la tecnología multipremiada ESET NOD32, en la que confían más de 110 millones de usuarios en todo el mundo para detectar las amenazas digitales, como ransomware, rootkits, gusanos y spyware. Además, te brinda seguridad ante técnicas que buscan evadir los métodos de detección habituales y bloquea ataques dirigidos y exploits. El módulo Anti-Phishing te protege de sitios web falsos que buscan acceder a tu información, como nombres de usuario y contraseñas. [16].
- **AVG:** Es un software para detener y eliminar los programas maliciosos. Fue desarrollado gracias a una empresa checa llamada AVG Technologies. Y se ha puesto disponible para distintos sistemas operativos. Por ejemplo, Linux, Windows, iOS, Android y Windows Phone [17].
- **Mi arroba:** es un hosting que ofrece un servicio gratuito de creación de foros, blogs, estadísticas, clasificados, alojamiento de fotos [18].

1.3. OBJETIVO

1.3.1. OBJETIVO GENERAL

Implantar técnicas y herramientas de ethical hacking para la ciberseguridad basado en las fases de la metodología PTES.

1.3.2. OBJETIVO ESPECIFICO

- Identificar las principales herramientas para la práctica de ciberseguridad.
- Plantear las fases de la metodología PTES que permita manejar de manera ordenada y secuencial el uso de las herramientas escogidas.
- Describir las mejores técnicas para el manejo y control de las amenazas.
- Recomendar el uso especifico de la técnica y herramienta de acuerdo a la problemática presentada.

1.4. JUSTIFICACIÓN

La propagación acelerada de los equipos tecnológicos, el amplio acceso al servicio de Internet han sido los principales factores para que el usuario sea participe de manera directa e indirecta de los delitos informáticos, donde la información personal o institucional es obtenida de manera indebida por personas inescrupulosas buscando el beneficio propio sin importarle el daño generado [19].

Cabe recalcar que a medida que se genera la evolución tecnológica, los delitos informáticos empiezan a incrementarse a cada minuto ocasionando que sea un tema importante y que en algunos casos tenga que buscarse soluciones inmediatas para remediar el daño obtenido sin importar el tamaño o tipo de negocio [19].

Por tal motivo surge la necesidad de realizar un análisis de la herramientas y técnicas del hacking ético basados en la metodología PTES, la cual permite identificar y analizar los respectivos controles que fortalecen los niveles de seguridad permitiendo así la mitigación de los riesgos informáticos a los que estamos expuestos cuando navegamos en la gran red de redes [20].

El presente tema propuesto está alineado a los objetivos del Plan Nacional de Desarrollo del buen vivir en el siguiente eje.

Objetivo 5

Impulsar la productividad y competitividad para el crecimiento económico sostenible de manera redistributiva y solidaria [21].

Política 5.6 Promover la investigación, la formación, la capacitación, el desarrollo y la transferencia tecnológica, la innovación y el emprendimiento, la protección de la propiedad intelectual, para impulsar el cambio de la matriz productiva mediante la vinculación entre el sector público, productivo y las universidades [21].

1.5. ALCANCE

Fase de recolección de información:

- Estructurar el ambiente simulado para la ejecución del análisis de amenazas.
- Investigar diferentes ataques según la frecuencia de uso para su respectiva selección en el ambiente simulado.

- Utilización de las herramientas informáticas para detectar puertos abierto y servicios vulnerables de las víctimas.

Fase de modelado de amenaza:

- Búsqueda de las herramientas necesarias para la creación de los ciberataques.
- Modelado de los diferentes tipos de ciberataque seleccionados en la primera fase.

Fase de análisis de vulnerabilidades:

- Exploración de vulnerabilidades de las víctimas para así lograr el acceso que permita vulnerar el sistema.
- Monitorear los eventos suscitados dentro de la red simulada.

Fase de explotación:

- Implantar los diferentes tipos de ciberataque seleccionados.
- Ejecutar los diferentes ataques seleccionados que permitan vulnerar el sistema.
- Probar las diferentes herramientas que ayudan a mitigar los ciberataques.

Fase de informe:

- Obtención de los resultados de la diferentes técnicas y herramientas escogida para la mitigación de las amenazas.
- Elaboración de cuadros sobre las técnicas y herramientas usadas.
- Elección de la técnica y herramienta óptima para reducir los ciberataques.
- Sugerencias y recomendaciones a seguir en base a los resultados obtenidos.

CAPÍTULO 2

2. MARCO TEORÍCO Y METODOLOGÍA DEL PROYECTO

2.1. MARCO TEÓRICO

2.1.1. Seguridad de la informática

La seguridad de la informática en términos básicos comprende en un parte los cimientos de una disciplina muy compleja la cual tiene como concepto brindar un bienestar a una organización además de mitigar la ausencia y presencia de riegos dentro de la misma. Existen países donde la seguridad es prioridad en muchos aspectos como lo son seguridad ambiental, seguridad pública, seguridad económica que tienen como privilegio evitar el robo, daño, manipulación de bienes [22].

La seguridad siempre tomara en cuenta la forma de evitar o prevenir, acciones que permitir causar algún tipo de daño a la entidad he involucra los siguientes procesos:

- Prevención del riesgo
- Transferir el riesgo
- Mitigar el riesgo
- Aceptar el riesgo

Para entender lo que con lleva la seguridad de la informática debemos de entender cuál es la diferencia entre seguridad informática y seguridad de la información esta última mantiene bajo sus parámetros el manejo de pérdida o fuga de información, en cambio la seguridad informática se encarga de los medios por los cuales esta información se transmite o se almacena [22].

2.1.2. Ciberseguridad

Las redes de información forman una gran parte integral de nuestra vida, ya que la mayoría de las entidades ya sean estas financieras, educativas, o medicas funcionan atreves de una red, es por ello que nace la ciberseguridad un tema donde su concepto esta fomentado en el esfuerzo que regir el deber de proteger estos sistemas ante algún uso no debido o autorizado [23].

A medida que pasan los años la población supera en gran porcentaje el deseo de mantenerse más tiempo en línea, esto puede ocasionar severas consecuencias para las organizaciones ya que el punto más débil para la misma es el usuario final.

"Las ciberamenazas mundiales siguen desarrollándose a un ritmo rápido, con una cantidad cada vez mayor de filtraciones de datos cada año. En un informe de RiskBased Security, se

reveló que unos alarmantes 7900 millones de registros han sido expuestos por filtraciones de datos solo en los primeros nueve meses del 2019. Esta cifra es más del doble (112 %) de la cantidad de registros expuestos en el mismo período durante el 2018" [23].

2.1.3. Tipos de ciberataques.

- **Códigos maliciosos o malware:** Este tipo de ciberamenaza hace referencia a un ataque directo al sistema que puede ocasionar daños muy graves al intentar modificar código base de nuestro sistema en estos ataques esta incluidos, gusanos, ransomware o troyano, el objetivo de estos ataques es impregnarse en el sistema para así causarle debilidad a el mismo [24].
- **Ciber-espionaje:** Esta técnica se usa más en las organizaciones gubernamentales, esto no quiere decir que no se lo use con otros fines su objetivo principal es obtener información [24].
- **Ransomware:** Consiste en introducir un conjunto de código malicioso dentro de un sistema, el cual tiene como finalidad encriptar los datos, pedir una recompensa.
- **Phishing:** se enfoca en el redireccionamiento de páginas o de sistemas atreves de sitios web o correos falsos [24].
- **Malware spam:** Conjuntos de correos que se envían a la víctima y tienen como finalidad dañar el sistema [24].
- **Criptojacking:** Este ataque en los últimos años ha aumentado en un gran nivel, consiste en la creación y obtención de la criptomoneda para apoderarse de ella teniendo el control de la máquina [24].

2.1.4. Clasificación de las amenazas

Amenazas de seguridad internas

Estos ataques son los que principalmente se generan dentro de una organización, estos pueden ser ejecutado por los empleados de la empresa ya sean de planta o contratados, además de que pueden ser ocasionas de manera accidental o de manera intencional.

"Las amenazas internas también tienen el potencial de generar mayor daño que las amenazas externas, porque los usuarios internos tienen acceso directo al edificio y a sus dispositivos de infraestructura. Los empleados también tienen conocimiento de la red corporativa, sus recursos

y sus datos confidenciales, así como diferentes niveles de usuario o privilegios administrativos" [25].

Amenazas de seguridad externas

Estas amenazas son unas de las más comunes dentro de las entidades empresariales, uno de sus principales objetivos es encontrar vulnerabilidades dentro de la red, y usas distintas técnica o métodos para conseguir el acceso a la misma [25].

2.1.5. Hacking ético.

Podemos entender que el hacking ético son un conjunto de técnicas utilizadas por profesionales de la seguridad informática para ayudar a mitigar diversos tipos de ciberamenazas. A diferencia del hacker informático, podríamos diferenciar que el Hacking ético se basa en buscar soluciones en seguridad informática, realizando pruebas en redes y buscando vulnerabilidades, para después reportarlas y que se tomen medidas necesarias para reducir el impacto del ataque [26].

El hacker ético tiene que conocer lo que un hacker no ético hace, además de saber las técnicas que utilizan, cómo actúan y también mantenerse siempre actualizado porque día a día aparecen nuevas técnicas [26].

La manera correcta de describir a un hacker ético, está en decir que es el encargado de encontrar vulnerabilidades, dando esto como resultado el desarrollo de aplicaciones para la explotación de las mismas; esto conlleva a que la información de millones de personas alojada en la nube se encuentre vulnerable [26].

Descrito en lo anterior, podemos decir que el hacking ético es realizado por un hacker; de la misma manera este puede ser ético o no dependiendo de cómo se realice el hackeo. El papel fundamental del hacker ético se basa en la ejecución de ataques informáticos para la búsqueda de vulnerabilidades e implementar posibles medidas de prevención ante estas amenazas.

2.1.6. Metodología PTES (Penetration Testing Execution Standard)

Es una metodología que sirve como guía técnica para los procesos de test de intrusión ya que define los pasos y herramientas requeridas en cada fase del ciclo de pruebas de vulnerabilidades, está comprendida por una cadena de estándares los cuales permiten el fácil entendimiento y

comprensión del estudio de vulnerabilidades [27].

Los objetivos de un test de penetración varían dependiendo del cliente, ya que se le puede solicitar al pentester la comprobación de una aplicación web, intentar ejecutar ataques de ingeniería social y adicionalmente aquello el actuar como un atacante interno etc.

2.1.7. Diferentes metodologías para realizar pruebas de Pentesting.

OWASP: Es una metodología de código abierto dedicado a la identificación y mitigación de aplicaciones inseguras, además contiene pruebas de seguridad periódicas en varias fases. Su enfoque principal es basado en pruebas de penetración de caja negra y se compone de 2 fases:

- Fase pasiva: En esta el tester entiende la lógica del sistema evaluado.
- Fase activa: El tester prueba todas las herramientas recomendadas por la metodología [28].

ISSAF: Es una metodología estructurada para el análisis de seguridad en múltiples dominios y detalles específicos de las pruebas. Su objetivo es proporcionar procedimientos muy detallados para la comprobación de sistemas de información, aplicaciones web o redes de trabajo; pero no permiten evaluar todos los aspectos requeridos actualmente [28].

OSSTMM: Es un estándar profesional utilizado para el testeo de seguridad en cualquier entorno, esta metodología en conjunto representa un modelo de referencia en el área de testeo de seguridad. Además de también incluir lineamientos, ética del auditor de seguridad, legislación sobre el testeo de seguridad y un conjunto integral de testeo al igual que los otros [28].

2.1.8. Fases del Pentesting.

El Pentesting está conformado por una serie de fases las cuales se encuentran comprendidas desde la planeación hasta el reporte.

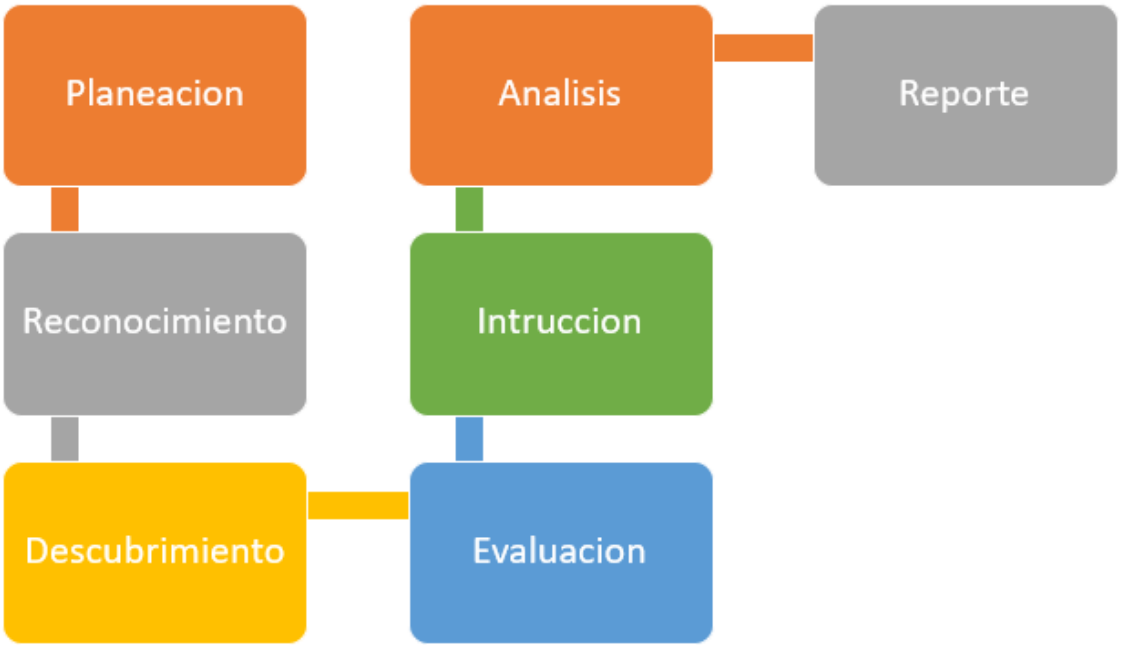


Fig. 1 Fases del Pentesting

Planeación: Dentro de esta fase el pentester y el cliente definen los límites y objetivos de la prueba, de modo que ambas partes estén de acuerdo ya que estos límites marcan una frontera de legalidad dentro de cada prueba [29].

Reconocimiento: En esta segunda fase se analiza de forma detallada el cómo se va a recolectar información del objetivo, para obtener una mejor visión de los mecanismos de seguridad que emplea la víctima. Además, la información disponible debe ser proporcionada, completa y clara [29].q

Descubrimiento: Dentro de esta fase se encuentra comprendida la obtención o recolección de datos a través de herramientas de análisis de vulnerabilidades, en donde el pentester busca: rangos de direcciones IP, dirección física de la empresa, datos personales de la empresa: números de teléfonos, nombres del personal y cuentas de correo electrónico entre otra cosa [29].

Evaluación: Dentro de esta fase se analiza los diferentes datos encontrados dentro de las anteriores fases, para así determinar cuál es la mejor herramienta para afectar al sistema y determinar sus puntos de vulnerabilidad [29].

Instrucción: Esta fase se centra en la explotación de las posibles puertas o entradas, encontradas en la fase de evaluación; las cuales son aprovechadas por un exploit o cualquier otro tipo de ciberataque que permita el ingreso al sistema [29].

Análisis: Evalúa las posibles vulnerabilidades que se encuentren dentro del sistema que afecten

o comprometan la entidad [29].

Reporte: En esta fase se desarrolla un informe detallado de cada uno de los procedimientos o pruebas realizadas y así determinar sugerencias para una seguridad futura [29].

2.1.9. Ciberataques más frecuentes.

Según el portal web welivesecurity, los ataques más frecuentes en primer lugar son los tipos malware dejando por detrás a los phishing y por último a otros tipos de ataques.

"De acuerdo con el Antiphishing Working Group, durante el segundo trimestre de 2018, alrededor del 35% de los ataques de phishing registrados se alojaron en sitios web con el protocolo HTTPS, cifra que significa un importante incremento en comparación con el casi 5% de los casos de sitios falsificados con certificados SSL, reportados hacia finales de 2016" [30].

Los códigos maliciosos continúan siendo una de las principales amenazas, a esto se suma su uso para llevar a cabo varios ataques; según el ESET security report 2018 los ataques de malware son la principal causa de incidencias de seguridad en empresas latinoamericanas.

"Entre las familias con más altos niveles de propagación, se encuentra la llamada Win32, cuyos primeros registros se hicieron presentes durante 2016, y que valiéndose de un lenguaje de scripting como AutoIt, estaba diseñado en sus inicios para tomar capturas de pantalla. Hoy, esta amenaza evolucionó y ya cuenta con funcionalidades de keylogger, robo de información de sitios de comercio electrónico y contraseñas almacenadas en los buscadores y, más recientemente, la capacidad de minar criptomonedas" [31].

"Antes del COVID-19, los ataques cibernéticos ya estaban aumentando, y la pandemia y la cuarentena resultante no hicieron más que incrementar aún más este riesgo. Desde las estafas de phishing hasta el malware relacionado con el COVID-19, los ciberdelincuentes se han abalanzado sobre las vulnerabilidades que se desprenden del trabajo descentralizado y los sistemas de TI para encontrar grietas por donde filtrarse" [32].

Según los conceptos anteriores podemos determinar que el aumento de los ataques va en incremento, además que consecuentemente a la pandemia del 2020 por covid-19 no solo elevo su crecimiento, sino que también aceleró los ciberataques.

Como último ataque tenemos el conocido Man in the Middle que actualmente se lo considera como una amenaza de mando y control o también como suplantación de identidad según el portal web akamai.

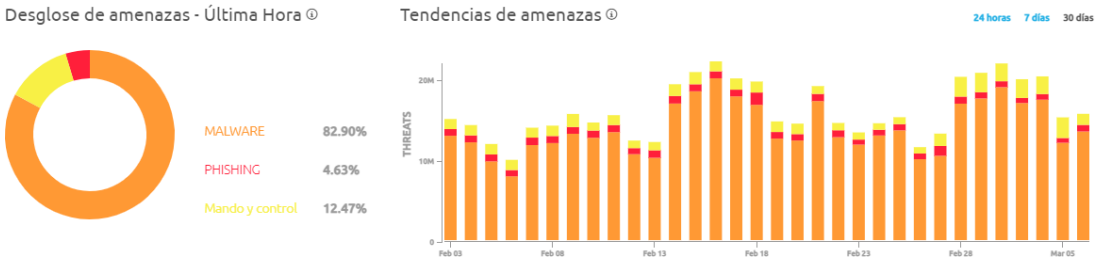


Fig. 2 Estadísticas de amenazas en tiempo real

fuente: www.akamai.com

2.2. METODOLOGÍA DEL PROYECTO

2.2.1. Metodología de la investigación

Se realizará una investigación longitudinal, con ayuda de la recopilación de información relevante y de estudios relacionado con el uso de los estándares de PTES en la ejecución de análisis de Pentesting. Con la información obtenida de la literatura se procederá a levantar un laboratorio de hacking ético para la implantación de las herramientas y técnicas para contra restar los ataques informáticos (Ver anexo2).

En base a la metodología aplicada se detectó una variable dependiente e independiente:

Variable independiente: Hacking Ético.

Variable dependiente: Identificación de las herramienta y técnicas para la mitigación de ciberataques.

2.2.2. Técnicas de recolección de información

Para realizar la búsqueda de la información se tendrá en cuenta la técnica de recolección conocida como recopilación documental y bibliográfica, la cual tiene como finalidad obtener datos a través de fuentes documentales que permitirán proporcionar la obtención de información; posteriormente se analizará y se presentaran los resultados obtenidos. Además, se tendrá como propósito el cumplimiento de los objetivos propuestos en esta investigación.

2.2.3. Metodología de desarrollo del proyecto

Las siguientes fases detalladas a continuación están basadas según la metodología PTES y acopladas a la búsqueda de la herramienta más optima y técnica para la mitigación de los ciberataques respectivamente:

Fase I: Recolección de información

Se llevará a cabo un análisis de la estructura de la organización en el ambiente simulado, tomando en consideración la información obtenida de los diferentes ciberataques a ejecutar y de las herramientas a utilizar.

Fase II: Modelado de la amenaza

Se buscará e instalará las herramientas necesarias para el modelo de las amenazas de una manera correcta y controlada.

Fase III: Análisis de Vulnerabilidades

En esta etapa se buscará obtener las vulnerabilidades de las víctimas para producir los ciberataques dentro ambiente simulado, además de monitorizar los eventos sucitado dentro laboratorio implantado.

Fase IV: Fase de explotación

En esta fase se ejecutar los diferentes ataques seleccionados para obtener el acceso al sistema, además de detectar el ataque para una pronta respuesta y continua protección.

Fase V: Informe

Evidenciar las pruebas realizadas dentro de la implantación de cada herramienta y técnica, luego de los resultados obtenidos se realizará la selección de las optima.

CAPÍTULO 3

3. PROPUESTA

3.1. Introducción.

La propuesta presentada a continuación permitirá obtener un nivel adecuado de ciberseguridad que permitirá prevenir riesgos de ciberataques a las redes de datos y a la información que transita por ellos, siendo esencial para el funcionamiento de las organizaciones.

Con la adopción de nuevas tecnologías digitales se incrementa la dependencia de las mismas, creando un ambiente de vulnerabilidad para nada despreciable, convirtiéndose en un peligro potencial.

Con el fin de evitar facilidades al incremento de los ciberataques, las infraestructuras tecnológicas existentes deben establecer un proceso de seguridad de naturaleza técnica, por lo que se vuelve necesario reconocer los recursos intangibles a proteger, para así poder precisar cuál será la trascendencia de la seguridad para que la protección de dichos recursos sea de forma eficaz y controlada.

3.2. Desarrollo de la propuesta

3.2.1. Fase I: Recolección de información

Estructuración del laboratorio de hacking ético implantado en una red local para la ejecución de los ciberataques.

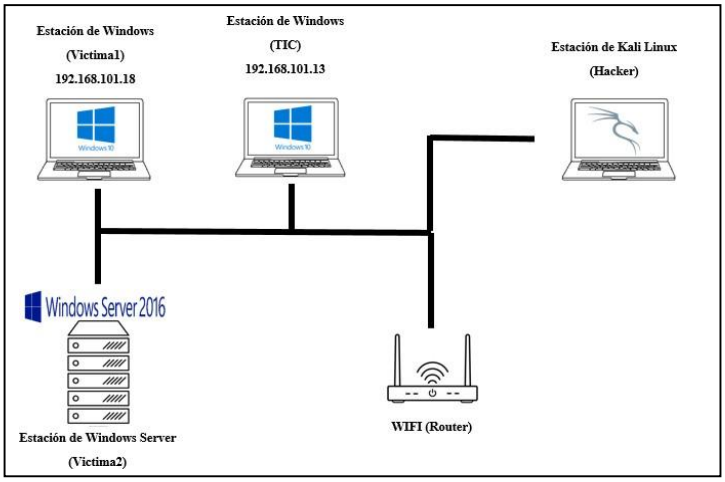


Fig. 3 Estructura del laboratorio de hacking ético

Según los investigado con anterioridad se escogió los ataques de malware, phishing, y por último un ataque de control y dominio (MitM).

Malware

Con el comando nmap buscamos alguna vulnerabilidad del sistema para la ejecución de nuestro ataque.

Comando a ejecutar: nmap –A –T4 192.168.101.18

Comando a ejecutar: nmap –A –T4 192.168.101.24

Comando a ejecutar: nmap –A –T4 192.168.101.13

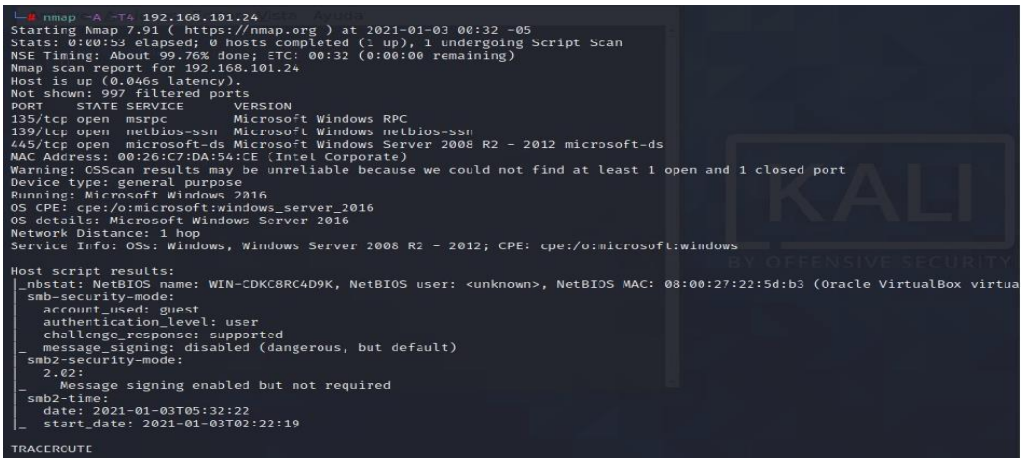


Fig. 4 Información obtenida de la maquina 192.168.101.24

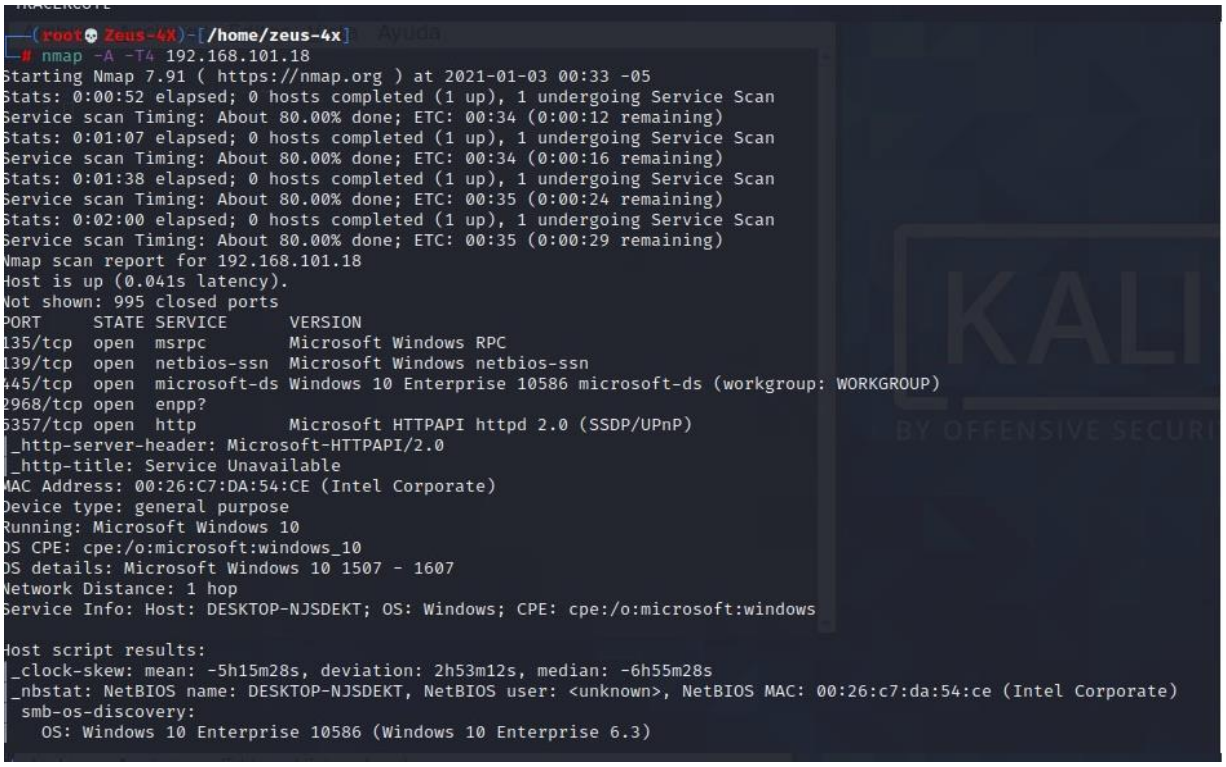


Fig. 5 Información de la maquina 192.168.101.18

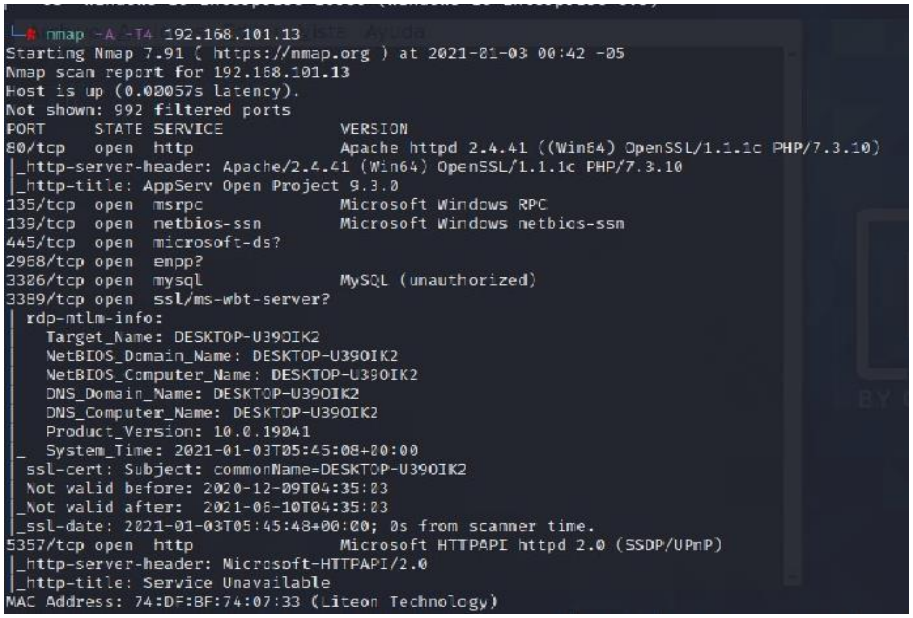


Fig. 6 Información de la maquina 192.168.101.13

También con el comando: [Nmap -O Dirección del Gateway] determinamos si existe alguna vulnerabilidad.

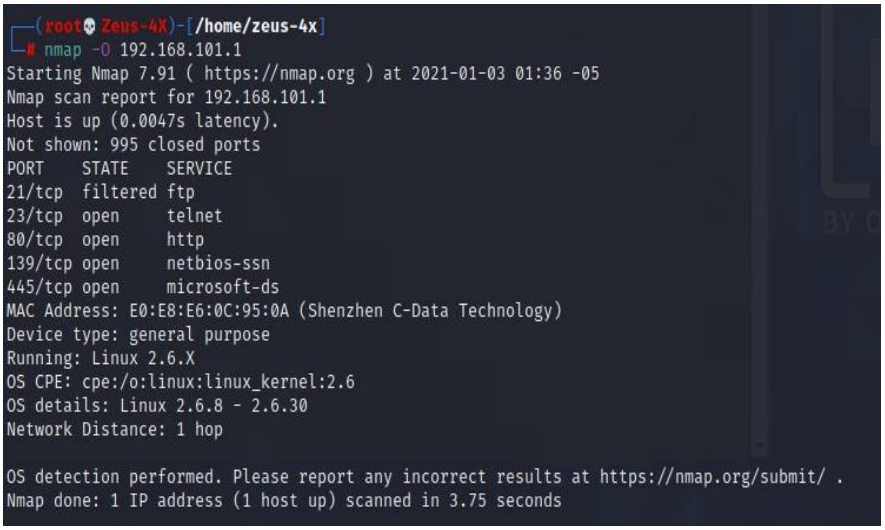


Fig. 7 Información obtenida del Gateway

Por último, ejecutamos un script de la herramienta nmap para buscar posibles vulnerabilidades dentro de nuestro laboratorio controlado.

Comando a ejecutarse: nmap –script vuln [Dirección IP].

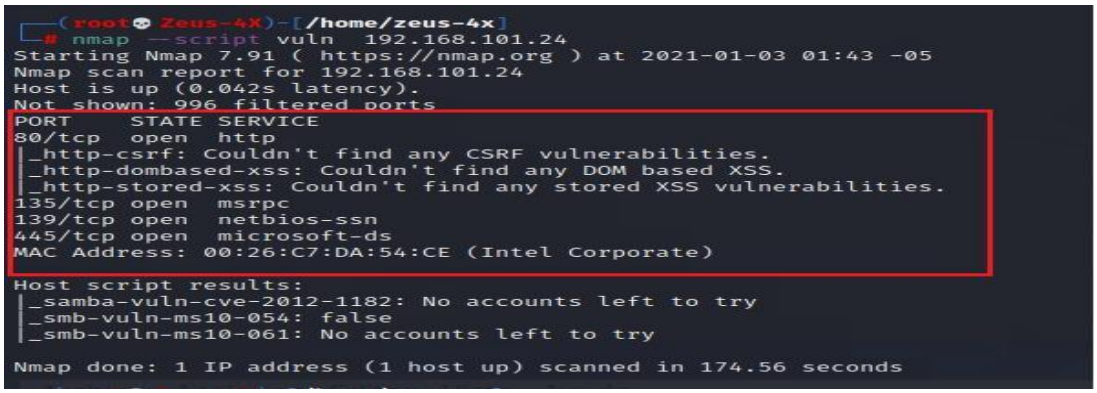


Fig. 8 Vulnerabilidades obtenidas de la dirección IP 192.168.101.24

Para su elaboración se usará la herramienta Armitage la cual nos permitirá crear el Payload que nos ayudará a penetrar el sistema y en la detención se usará la herramienta wireshark para verificar si existe algo inusual en la red.

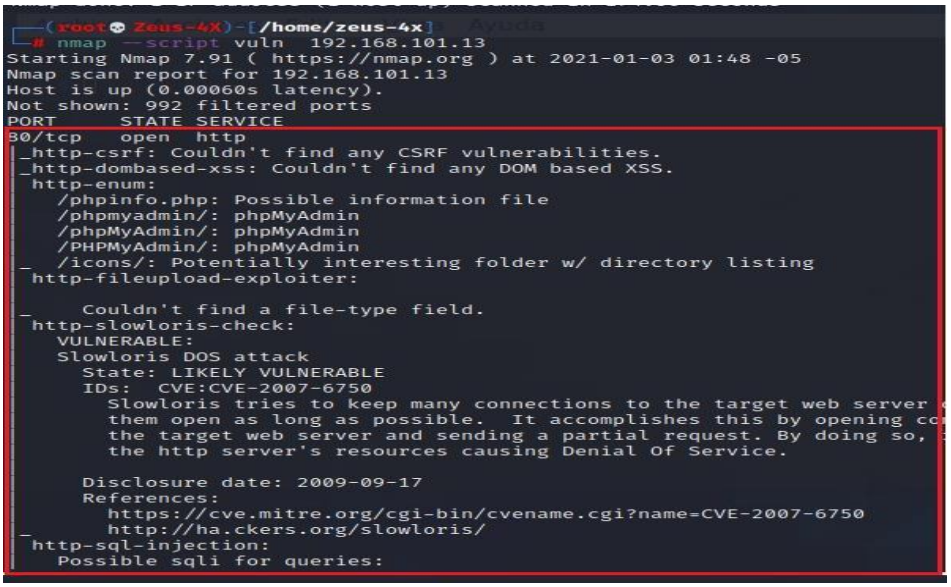


Fig. 9 Vulnerabilidades de la IP 192.168.101.13

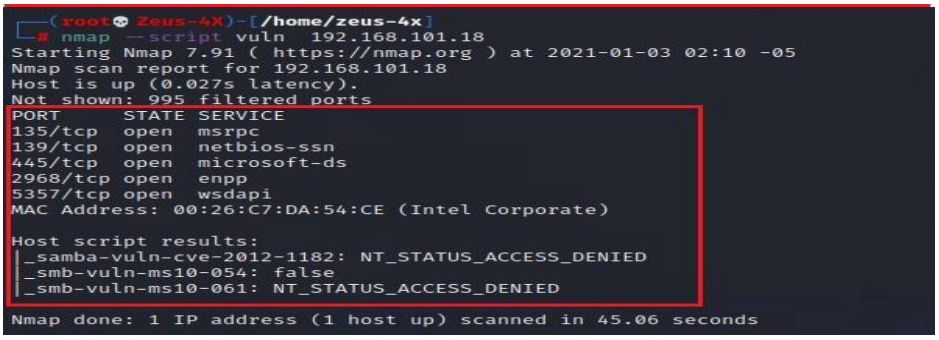


Fig. 10 Vulnerabilidades de la IP 192.168.101.18

Phishing

Atreves de Google hacking obtenemos el correo de la víctima.

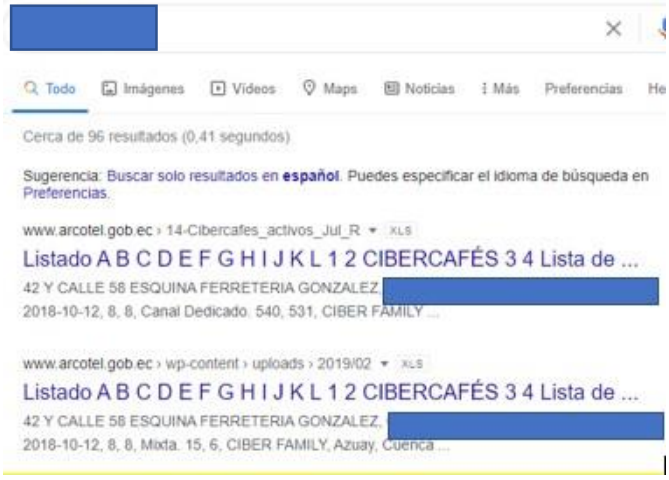


Fig. 11 Obtención de información de la victima

- Se utilizará la herramienta HTTrack web copier para el clonado del sitio web.
- Para la detención se aplicará conceptos básicos de prevención de páginas fraudulentas.

Main in the Middle (MitM)

Ejecutamos el comando **ipconfig** para verificar las MAC y IP de las maquinas víctimas.

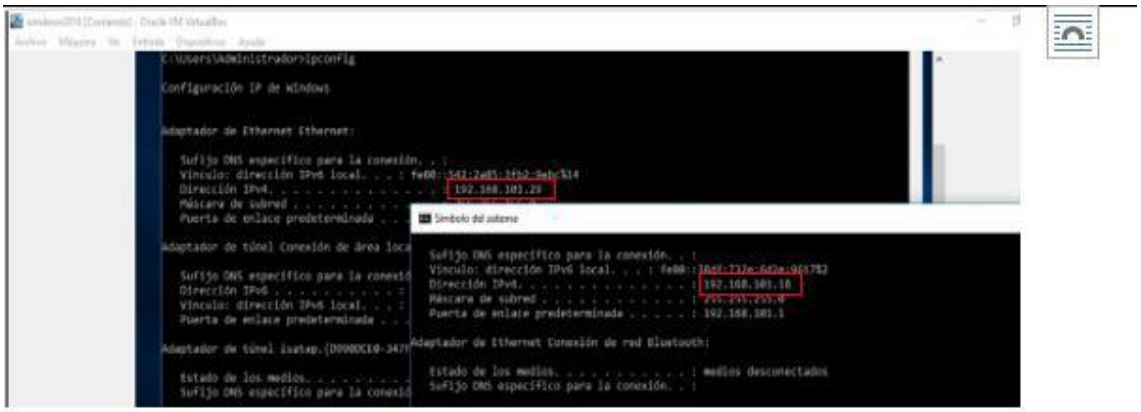


Fig. 12 IP de máquinas victimas

Ejecutamos el comando **arp -a** para revisar asignaciones de direcciones físicas a las direcciones **IPv4** conocidas.

- Una vez detectadas las direcciones físicas procedemos a realizar el ataque desde Kali Linux
- Para la ejecución de este ataque se empleará la herramienta ettercap.
- Además de la herramienta nmap para conocer puertos abierto, MAC address, IP de las maquinas víctimas.

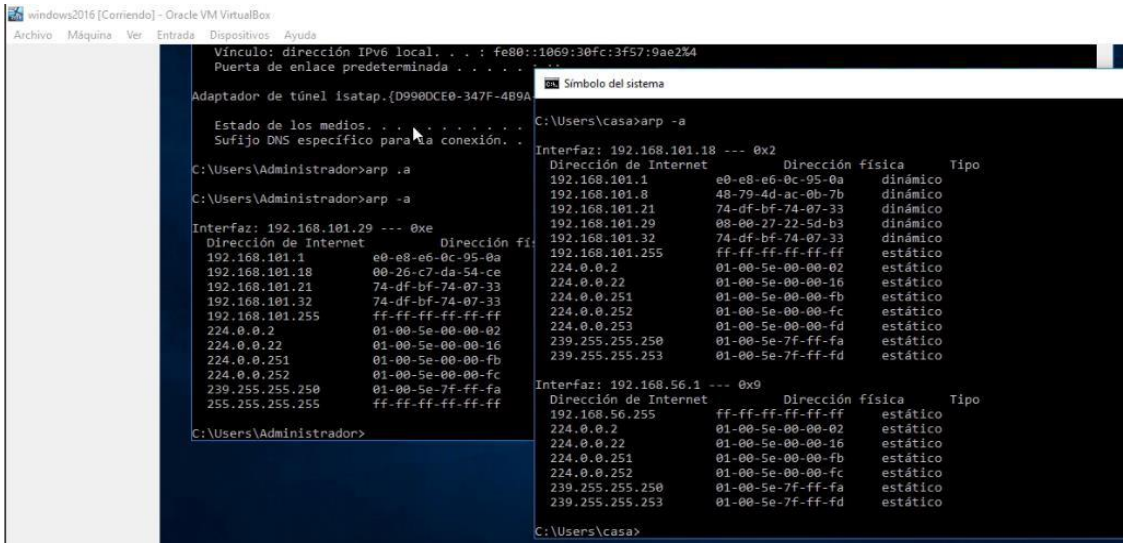


Fig. 13 MAC address de las maquinas victimas

En los ataques detallados con anterioridad se ejecutó las mismas herramientas de detención para

evaluar su comportamiento ante cada amenaza, estos softwares fueron escogido de acuerdo al grado de popularidad según el portal web Computer Hoy [33]:

- **ESET Internet Security 13.2**
- **Avast Premium Security**
- Norton 360
- Bit defender Internet Security 25.0
- Panda Dome Complete
- Kaspersky Internet Security 21.0
- McAfee Total Protection
- G Data Internet Security 2021
- Avira Internet Security 2021
- **AVG Internet Security 2021**

Tomando como referencia los dos primeros lugares y el ultimo de la lista para su estudio respectivo.

3.2.2. Fase II: Modelados de amenazas

Malware.

Primero instalamos la herramienta Armitage que nos ayudara a crear el malware tipo troyano para su ejecución.

Comando a ejecutarse: apt-get install Armitage.

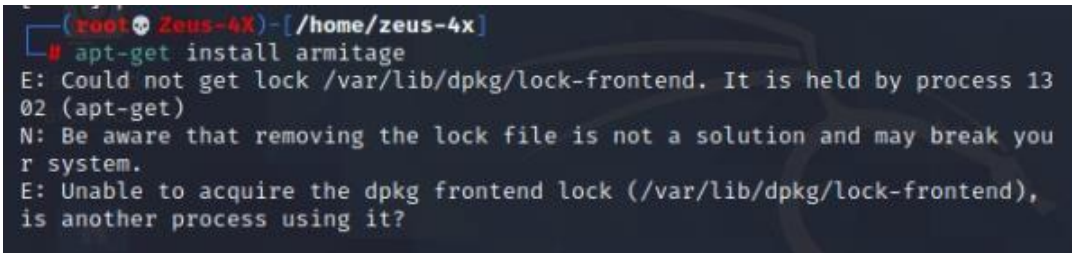


Fig. 14 Proceso de instalación de la herramienta Armitage

Luego ejecutamos el comando **service postgresql start** este nos ayudara a iniciar el servicio de SQL para la ejecución de la herramienta.

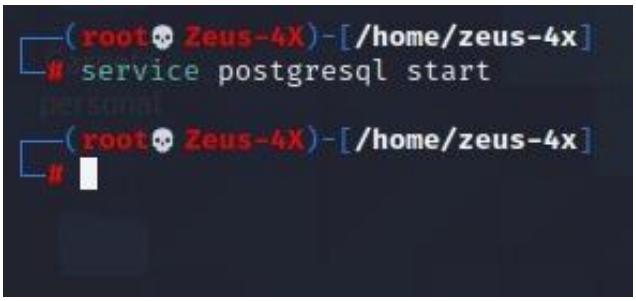


Fig. 15 Inicio de servicio SQL

Con el comando Armitage ejecutamos la herramienta a utilizar.

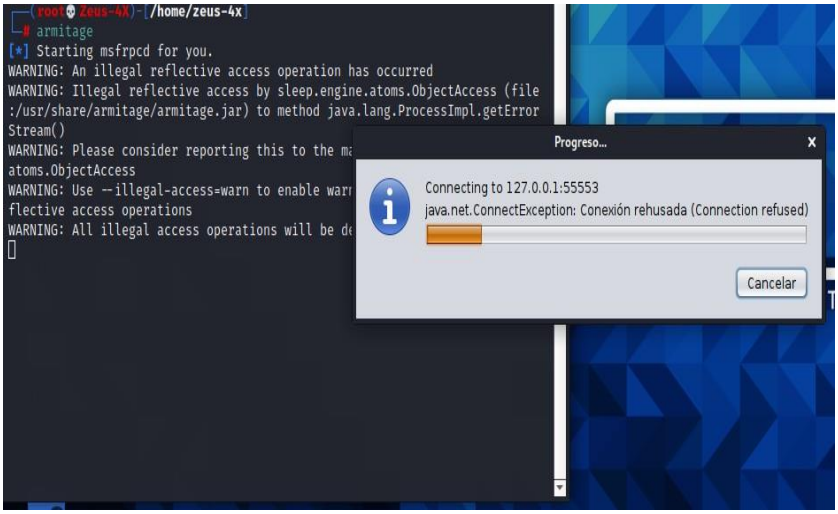


Fig. 16 Ejecución del programa

Phishing

De manera inicial obtenemos la copia del sitio web, en este caso clonamos para nuestra simulación la página de la red social Facebook para esto utilizamos la aplicación HTTRACK.

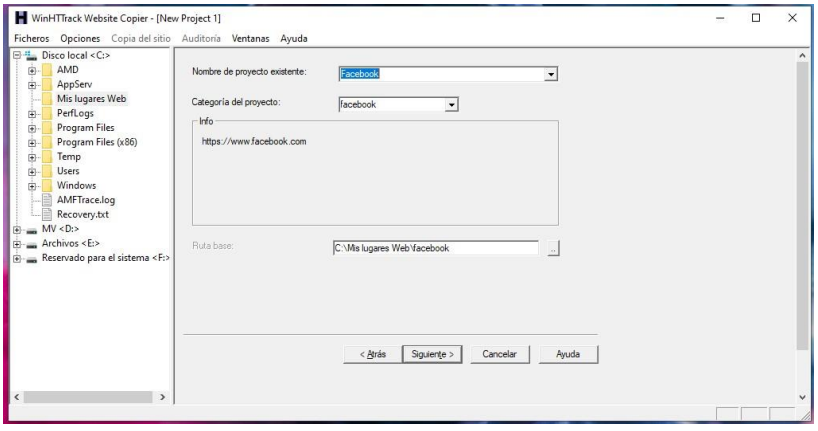


Fig. 17 Elaboración de clonamiento de página web

Configuramos los parámetros iniciales para dar inicio a la clonación.

- En el apartado de acción dejamos por defecto copiar sitio de la web
- En dirección web colocamos la URL del sitio que deseamos copiar y damos clic en siguiente.

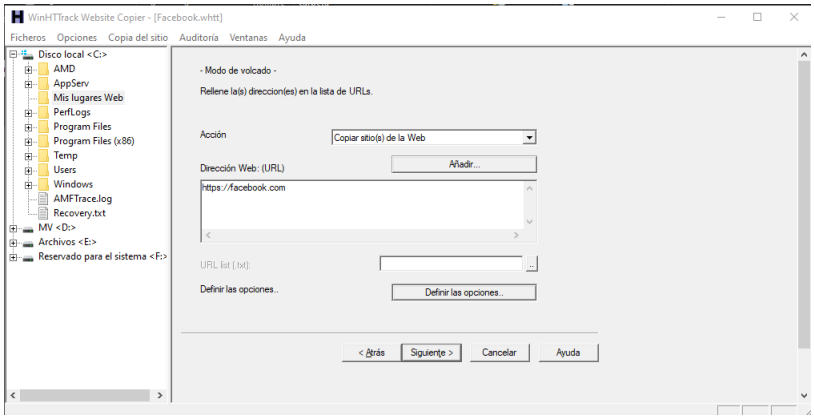


Fig. 18 Configuración de la herramienta de clonación

Dejamos la configuración por defecto y damos clic en finalizar.

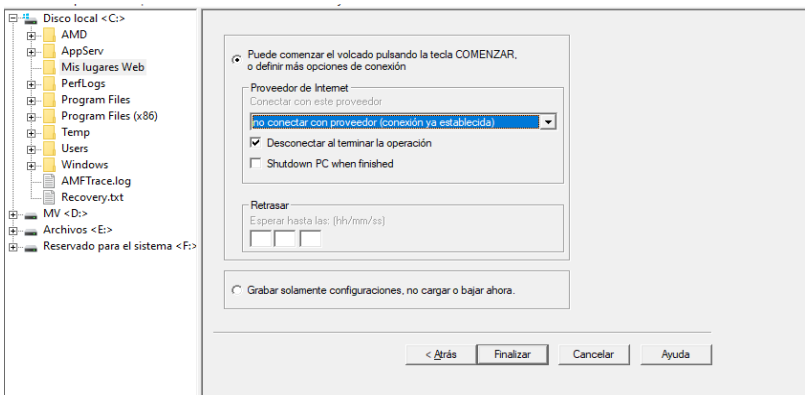


Fig. 19 Configuración final para la clonación

A continuación, comienza la ejecución de la clonación del sitio web en cual debemos esperar hasta que finalice dicho proceso, el tiempo de ejecución puede variar dependiendo de la característica físicas del computador.

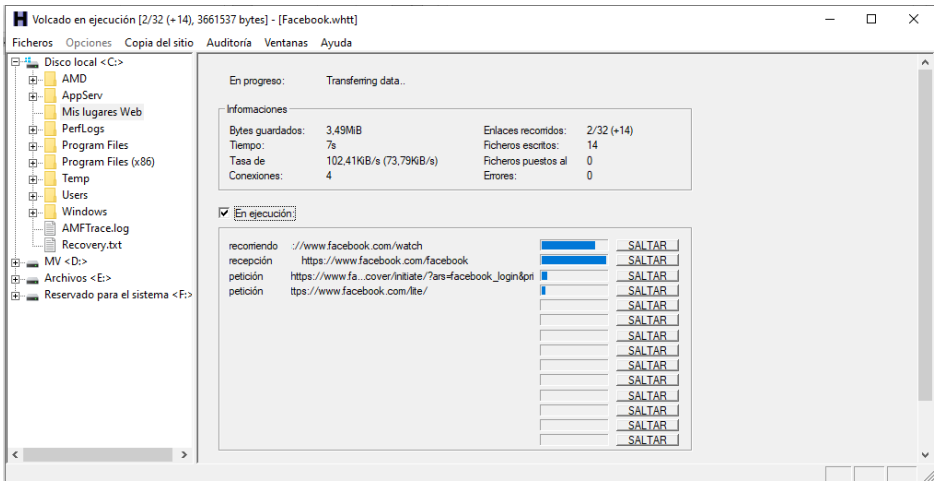


Fig. 20 Proceso de clonado de página web

Una vez finalizada la clonación nos dirigimos a la carpeta creada y buscamos dentro el archivo llamado index.html.

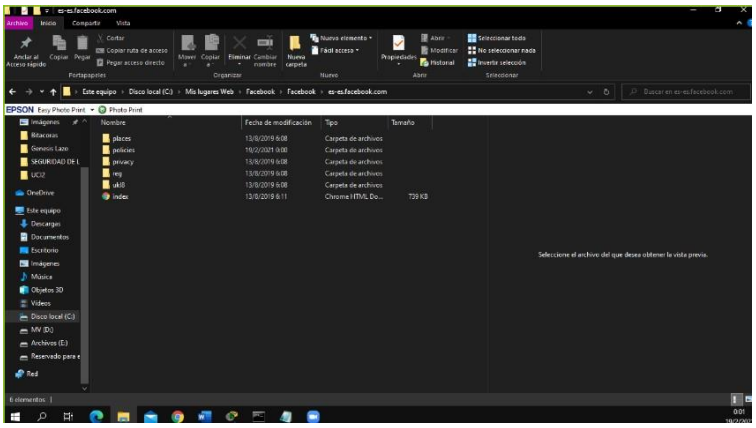


Fig. 21 Ubicación del archivo index.html

Una vez encontrado el archivo index.html, damos doble clic y a continuación se abrirá la página clonada; en la cual hacemos clic derecho y en menú de secundario seleccionamos la opción "**ver código fuente de la página"** y ejecutamos los siguientes pasos:

- Dentro del código fuente de la página presionamos CTRL+F para buscar.
- En el cuadro de búsqueda digitamos la palabra **login_form.**
- Una vez encontrado nos dirigimos donde nos muestra la sentencia:

action= "https://facebook.com/login/?"

- Luego la remplazamos por la sentencia:

action= "post.php"

Fig. 22 Proceso de modificación de página clonada

Luego procedemos a crear el archivo post.php:

- De manera inicial creamos un archivo en cualquier editor de texto, para la simulación usaremos bloc de notas; dentro del cual detallamos el siguiente código que nos permitirá obtener los datos de registro de la víctima.
- Una vez culminado procedemos a cambiar la extensión del archivo a **post.php.**

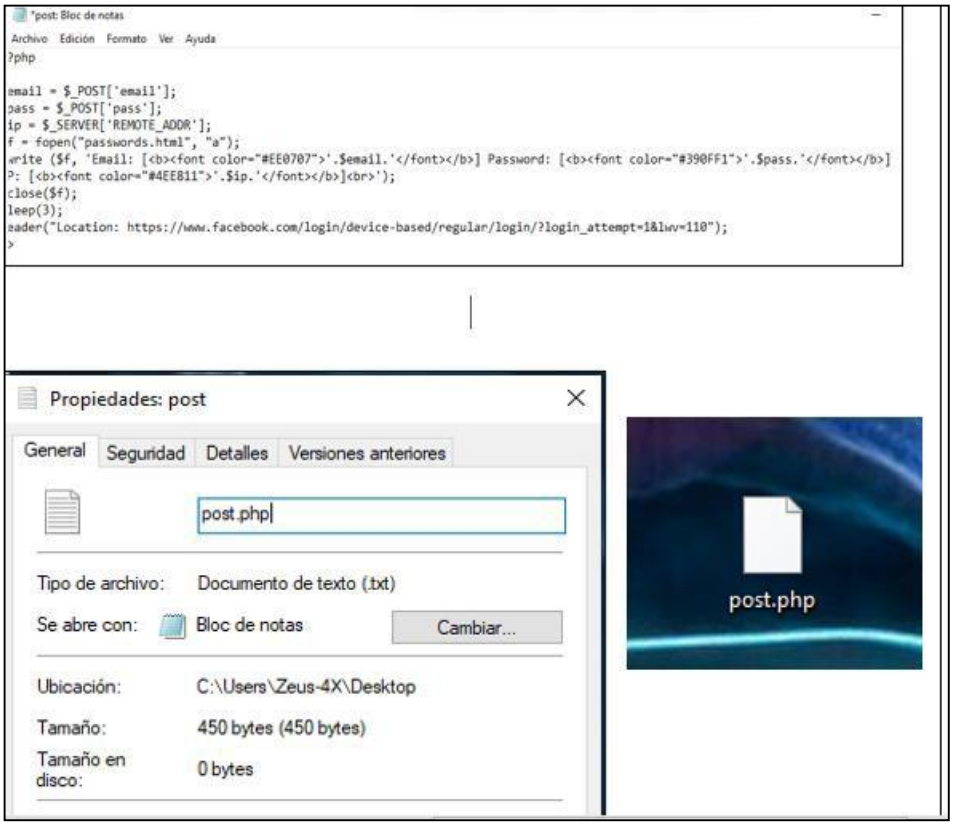


Fig. 23 Configuración del archivo PHP

Una vez cambiada la extensión copiamos el archivo **post.php** y lo pegamos dentro de la carpeta donde esta alojada nuestra página clonada.

Luego procedemos a cargar en un hosting pagado o gratuito la carpeta que contiene los archivos resultantes de la clonación de la página incluido el archivo post.php que creamos para la

simulación.

Para nuestra simulación usaremos el hosting gratuito **“miarroba.com”.**

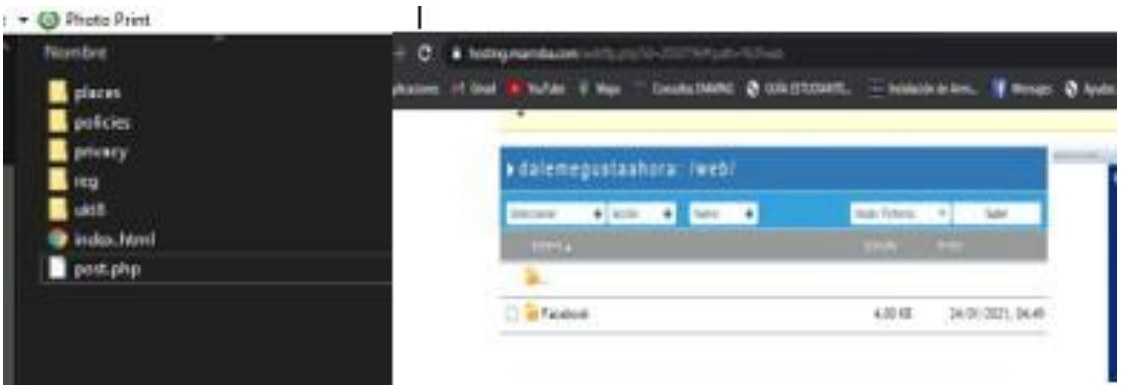


Fig. 24 Subida de la amenaza a la red

A continuación, procedemos a diseñar nuestra plantilla que puede ser creada de forma nativa o usando herramientas para la creación de las misma, para nuestra simulación usamos la herramienta “**stripo. email”.**

Una vez creada la plantilla del correo, esta será enviada a la víctima; donde colocará los datos solicitados.

Fig. 25 Diseño del correo falso que se enviara

Main the Middel (MitM)

Dentro del Kali Linux ejecutamos la aplicación de nombre ettercap.

- Activamos la opción **sniffing startup** y seleccionamos la red.
- Luego buscamos los hosts que se encuentran en la red.

- Dentro de la lista de host verificamos si nuestras IP se encuentran con sus respectivas direcciones físicas.

Fig. 26 Host encontrados en la red

3.2.3. Fase III: Análisis de vulnerabilidades.

Malware

Con el programa wireshark se describe una anomalía dentro del sistema de red de la empresa presentado a continuación.

Al momento de realizar una petición **nmap -sT [dirección IP]** a el servidor o la maquina victima notamos las peticiones [SYN]. Para luego recibir un [SYN, ACK] y cerrar con un [ACK], adicionalmente nos percatamos que se está preguntando si el servidor esta activo o no; además a través de su **dirección IP** deduciríamos de donde o quien está haciendo esas peticiones a nuestro servidor o maquina víctima.

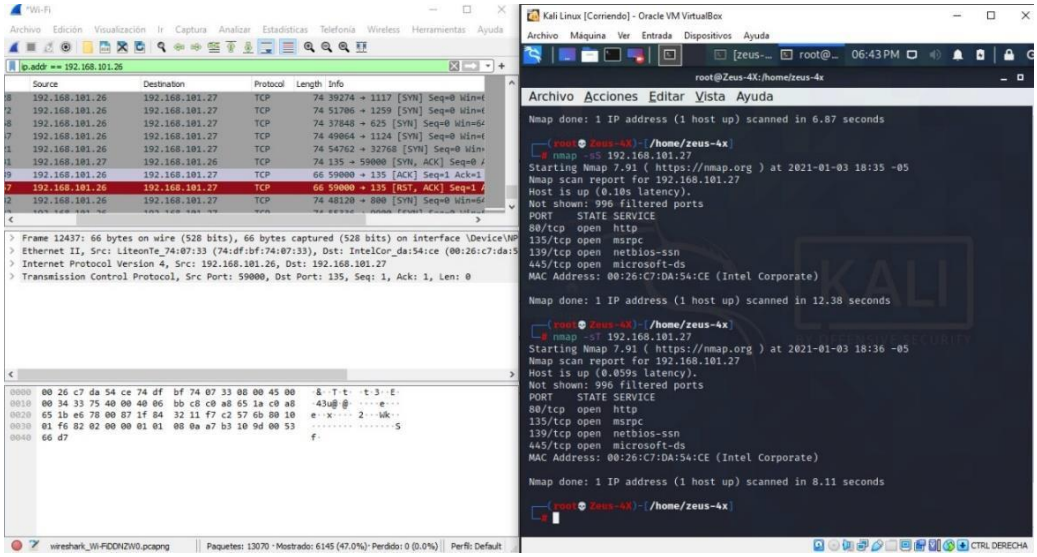


Fig. 27 Detección de peticiones al servidor

Si un ciberdelincuente se encuentra en nuestra red debemos de deducir peticiones al servidor de forma sigilosa por medio de un comando **nmap -sS y la [dirección IP]** del objetivo, se lo puede ejecutar y obtener información muy valiosa para el atacante.

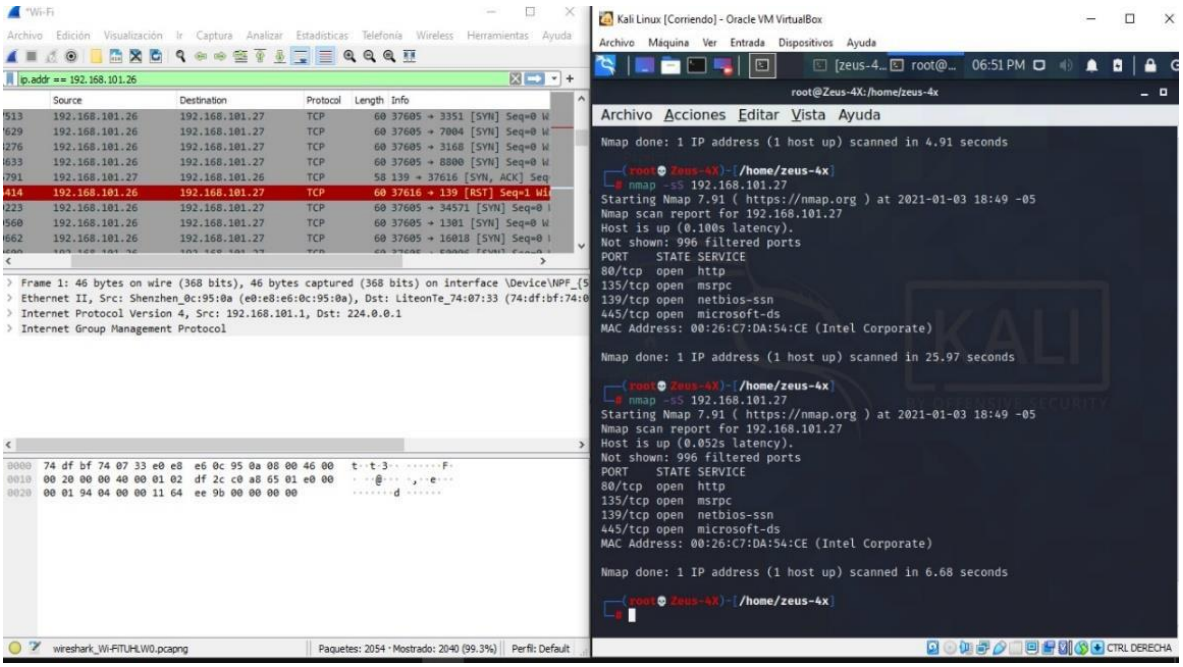


Fig. 28 Detección de peticiones al servidor de forma sigilosa

Phishing

Nos percatamos que el correo fue recibido sin ninguna sospecha del servidor de archivos ni del equipo víctima.

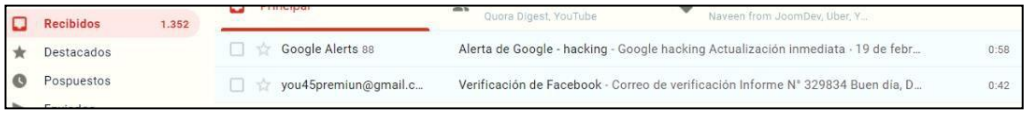


Fig. 29 Correo malicioso recibido

3.2.4. Fase IV: Fase de explotación

Malware

En la opción nmap que se encuentra ubicada en el apartado host de la barra de tareas, nos sirve para detectar las maquinas que se encuentran dentro de nuestro laboratorio controlado, en caso de que no detecte la maquina en la red se lo puede realizar manualmente.

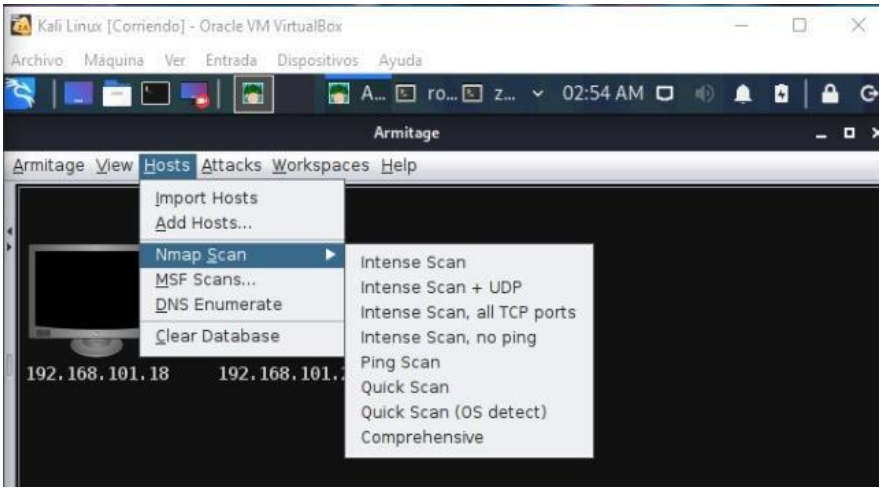


Fig. 30 Ejecución del apartado nmap scan

Fig. 31 Introducción manual de IP no detectada

A continuación, seleccionamos en la barra de tareas la opción [Payload], seguidamente la opción [Windows] y finalmente en la carpeta con el nombre de **meterpreter.**

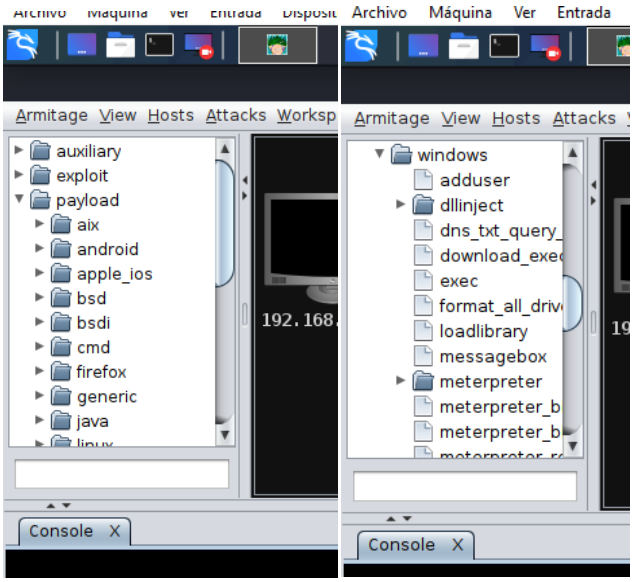


Fig. 32 Ejecución del apartado meterpreter

Dentro de la carpeta meterpreter escogemos la opción [reverse_tcp], también debemos verificar que la dirección IP y puerto sea los correctos, posterior damos clic en launch.

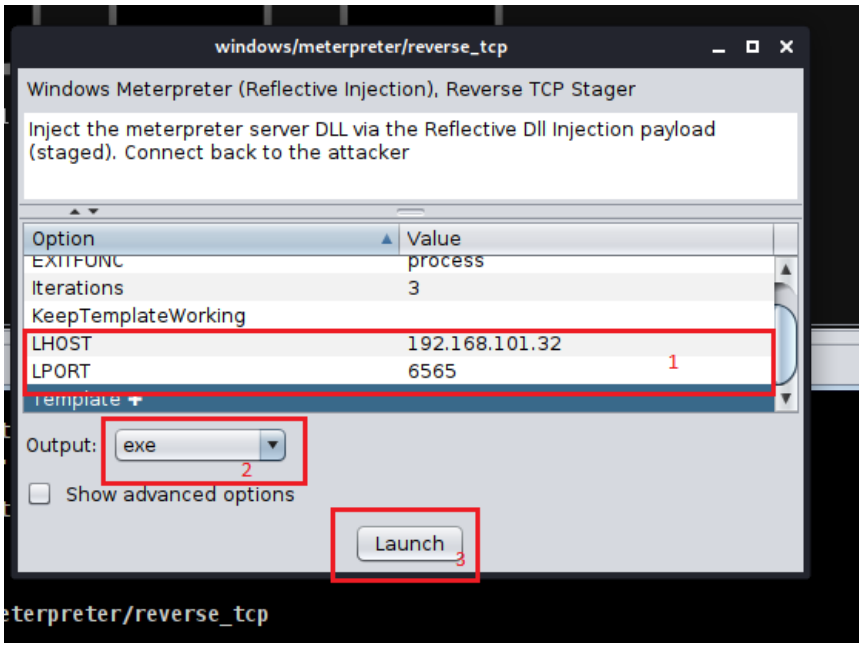


Fig. 33 Ejecución de la función reverse_tcp

En la siguiente ventana que aparece automáticamente debemos de colocar la ubicación y nombre a nuestro archivo malicioso para el ejemplo lo llamaremos [Prueba1].

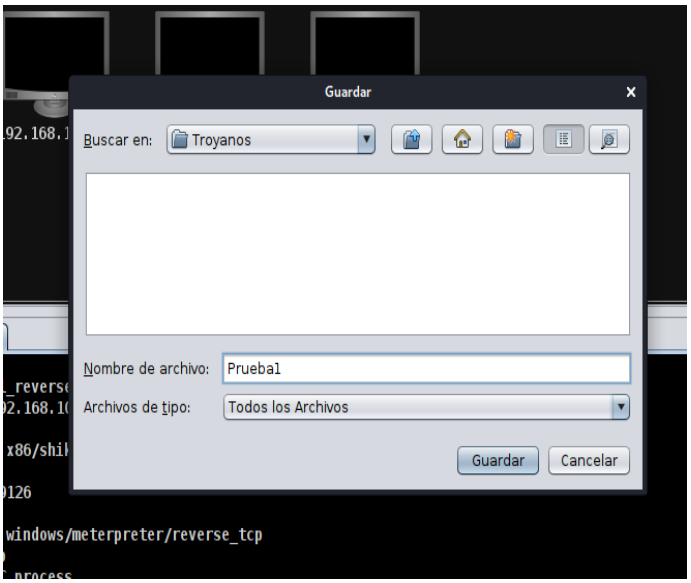


Fig. 34 Nombre de nuestro archivo troyano

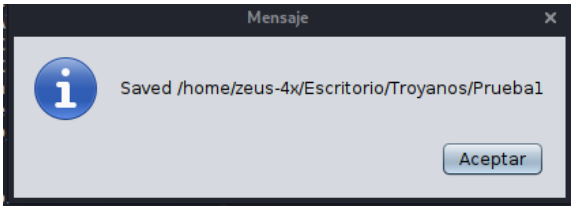
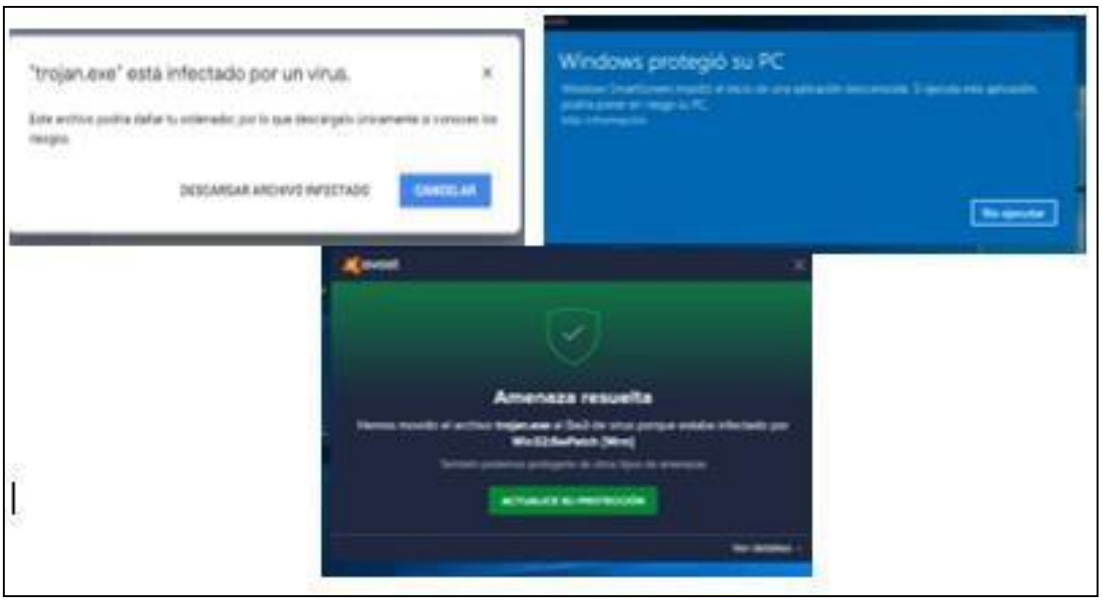


Fig. 35 Mensaje de confirmación de creación de Payload

Como podemos observar Google drive detecta los archivos infectados, pero de igual manera no protege nuestra magina porque a la final nos permite la opción de descarga.

Fig.



36 Detección de la amenaza.

Phishing

Una vez abierto el enlace observamos que los antivirus Avast Free y AVG instalados no lo reconocen como ataque de phishing al igual que tampoco lo hace el navegador.

Para nosotros poder saber si es o no un correo real, en el enlace verificamos a donde nos direcciona.

Fig. 37 Detección de enlaces extraños

Fig. 38 Ejecución del ataque de phishing

El antivirus Avast free y AVG no detectaron el ataque de phishing, pero ESET NOD 32, que contiene un apartado de detención de anti- phishing lo detecto y no permitió la ejecución del ataque.

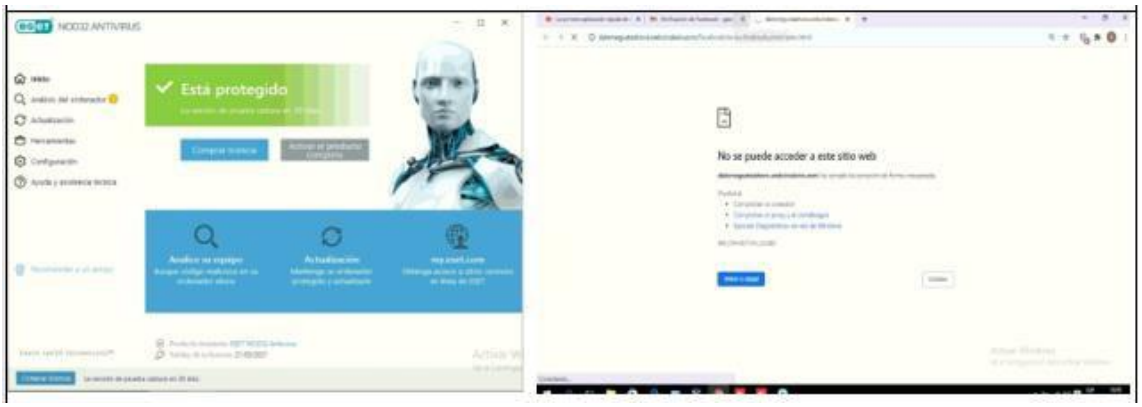


Fig. 39 Detección del ataque de phishing

Man in the middle (MitM).

Una vez encontrado los hosts, seleccionamos y hacemos clic en add target 1 y target 2. Finalmente, en el menú de MitM damos clic en ARP poisoning.

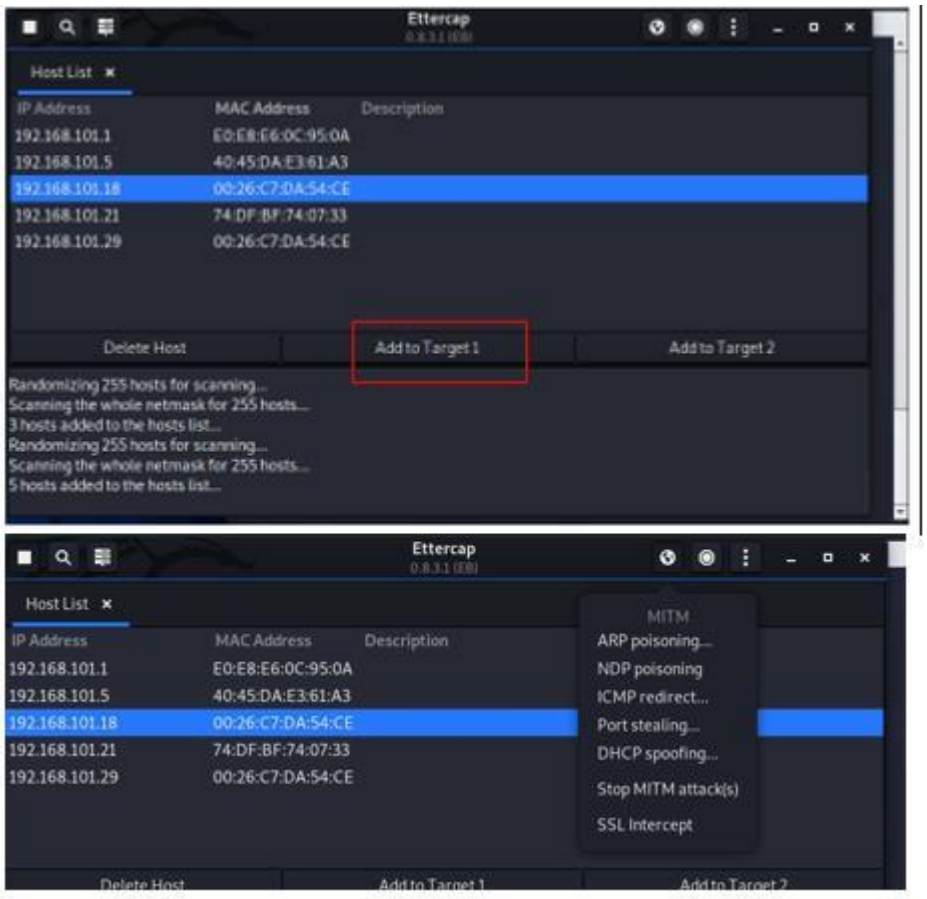


Fig. 40 Ejecución del ataque ARP poisoning

El ataque es detectado por el antivirus **ESET NOD 32** en su versión Smart Security, ya que las demás versiones detectan otros ataques exceptos los que son directo a la red.

Fig. 41 Detección del ataque MitM

3.2.5. Fase V: Fase de informe

Ataque	Herramienta	Técnica
Malware (Troyano)	**Software antivirus** • Avast Free. • AVG Antivirus free. • ESET NOD32 Antivirus (Versión de prueba).	• Pruebas de penetración. • Instalación de IDS
	Escáner de vulnerabilidades • Wireshark	
	Firewall de red • Firewall de Microsoft Defender	
Phishing	**Software antivirus** • Avast Free. • AVG Antivirus free. • ESET NOD32 Antivirus (Versión de prueba).	• Análisis estático de código. • Análisis dinámico de código. • Pruebas de penetración • Instalación de IDS
	Firewall de red • Firewall de Microsoft Defender.	

MitM (Hombre en el medio)	**Software antivirus** • Avast Free. • AVG Antivirus free. • ESET NOD32 Antivirus (Versión de prueba).	• Instalación de IDS. • Pruebas de penetración.
	Firewall de red • Firewall de Microsoft Defender	

Tabla 1 Cuadro de análisis de técnicas por cada herramienta de mitigación

Software Antivirus	Ventajas	Desventajas
Avast Free	• Tiene una versión con licencia free. • Bloquea cualquier tipo de virus. • Contiene un cortafuegos avanzado.	• La versión free trae mínimas herramienta de mitigación de seguridad informática. • No elimina virus ni software maliciosos. • El cortafuego que contiene solo detecta ciertos ataques informáticos.
AVG	• Navegación privada. • Bloqueador de anuncios. • Te protege contra script.	• El bloqueador de anuncios en versión free es limitado. • El cifrado HTTPS es vulnerable en la versión free. • Requiere de otros complementos para mejorar seguridad informática.
ESET NOD32	• La versión de mecanismo antirrobo es muy avanzada. • Evita la emisión de anuncio de amenazas en su mayoría. • Utiliza pocos recursos de la PC.	• Solo ofrece una versión free por 30 días. • El alto costo en sus diferentes versiones.

Tabla 2 Cuadro comparativo entre (Intrusion Detection System) IDS

Ataque	Herramienta	Observación
Malware	✓ Avast Free.	Detecta el ataque en primera instancia.
	✓ AVG Antivirus free.	Detecta el ataque en primera instancia.
	✓ ESET NOD32 Antivirus (Versión de prueba).	Detecta el ataque en primera instancia.
Phishing	✓ Avast Free.	No detecta el ataque ni en primera ni en segunda instancia
	✓ AVG Antivirus free.	No detecta el ataque en primera instancia, pero una vez ejecutado el robo de información lo detecta en segunda instancia.
	✓ ESET NOD32 Antivirus (Versión de prueba).	Detecta el ataque en primera instancia.
MitM	✓ Avast Free.	No detecta el ataque ni en primera ni en segunda instancia
	✓ AVG Antivirus free.	No detecta el ataque ni en primera ni en segunda instancia
	✓ ESET NOD32 Antivirus (Versión de prueba).	Lo detecta en primera instancia.

Tabla 3 Comportamiento de las herramientas según los ataques

Ataque	Sugerencias y Recomendaciones
Malware	• Para la mitigación de este ataque se recomienda el uso de algún antivirus de versión free de los analizados con anterioridad • Actualización del software. • Desinstalación de aplicaciones que se usan. • Estar atento antes cualquier actitud sospechosa.
Phishing	• Verificar procedencia de las páginas web. • Revisar las URL de las páginas web. • Reforzar la seguridad de la PC con algún antivirus. • Evitar ingresar información confidencial en sitios web no seguros.
MitM	• Evitar conectarse a rede públicas y abiertas • Utilizar VPN para la conexión. • Usar software de antivirus de mejor robusticidad para la mitigación del ataque. • Mantener sistemas actualizados.

Tabla 4 Recomendaciones especifica de cada amenaza

De acuerdo al análisis y a los resultados obtenidos de las diferentes técnicas y herramientas usadas en nuestro laboratorio controlado se puede determinar que la herramienta más óptima para la mitiga de los ciberataques presentados es ESET NOD 32, y mejor técnica para detectar intrusos es la instalación de IDS.

CONCLUSIONES

- ✓ Se identifico y aplico las herramientas principales para llevar a cabo las pruebas de penetración además del estudio de cada una de ellas.
- ✓ Se aplico y modifico los estándares de la metodología PTES de acuerdo al estudio a realizar con cada ciberataque.
- ✓ Se diseño un cuadro comparativo de cada técnica a usar dependiendo de la amenaza a implantar.
- ✓ Se especifico las recomendaciones de técnicas y herramientas a usar antes las amenazas estudiadas.

RECOMENDACIONES

- ✓ Para la mitigación de estos ciberataques realizados, se recomienda el uso de software de antivirus ESET Security en su versión free.
- ✓ Tener cuidado con sitios fraudulentos donde descarguemos cualquier tipo de archivo desconocido.
- ✓ Educar a los usuarios de manera que sepan identificar correos fraudulentos.
- ✓ Estar atentos a correos de dudosa procedencia los cuales soliciten información confidencial.
- ✓ Mantener el sistema actualizado permitiendo agregar mejoras que ayuden a mitigar los ciberataques.

GLOSARIO

PTES: El estándar de ejecución de pruebas de penetración consta de secciones principales. Estos cubren todo lo relacionado con una prueba de penetración, desde la comunicación inicial y el razonamiento detrás de un pentest.

Malware: es un término general para referirse a cualquier tipo de software malicioso diseñado para infiltrarse en su dispositivo sin su conocimiento.

Phishing: métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta.

Main in the middle: Es un método de ataque informático que sólo necesita que el atacante se sitúe entre las dos partes que intentan comunicarse; interceptando los mensajes enviados e imitando al menos a una de ellas.

Metasploit: Es una herramienta desarrollada en Perl y Ruby en su mayor parte, que está enfocada a auditores de seguridad

Exploits: Es un programa informático, una parte de un software o una secuencia de comandos que se aprovecha de un error o vulnerabilidad para provocar un comportamiento no intencionado o imprevisto en un software, hardware o en cualquier dispositivo electrónico.

Sniffing: Es una aplicación especial para redes informáticas.

VPN: Es una red privada virtual que permite crear una conexión segura y cifrada hacia otra red a través de Internet.

Mitigación: Moderar, aplacar, disminuir o suavizar algo riguroso o áspero

URL: Dirección que es dada a un recurso único en la Web

Free: Es un vocablo anglosajón que significa “libre” o “gratis”.

IDS (Intrusion Detection System): Es un software de seguridad cuya función es detectar accesos no autorizados en un sistema o una red de ordenadores.

HTTPS: es un protocolo que permite establecer una conexión segura entre el servidor y el cliente, que no puede ser interceptada por personas no autorizadas.

Nmap: Es una herramienta de escaneo de puertos y descubrimiento de hosts que existe actualmente.

Payload: Es la carga que se ejecuta en esa vulnerabilidad

Script: Se trata de un código de programación, usualmente sencillo, que contiene comandos u ordenes que se van ejecutando de manera secuencial y comúnmente se utilizan para controlar el comportamiento de un programa en específico o para interactuar con el sistema operativo.

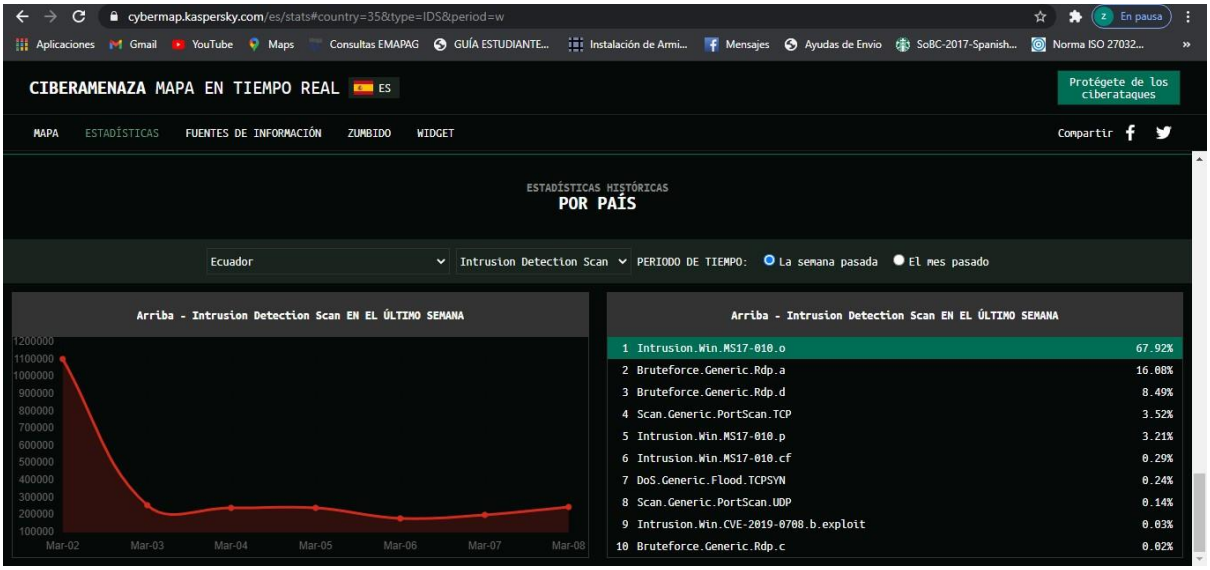
Launch: Es un término anglosajón que significa “lanzamiento”**.**

Post: Es típicamente enviada por un formulario HTML y resulta en un cambio en el servidor

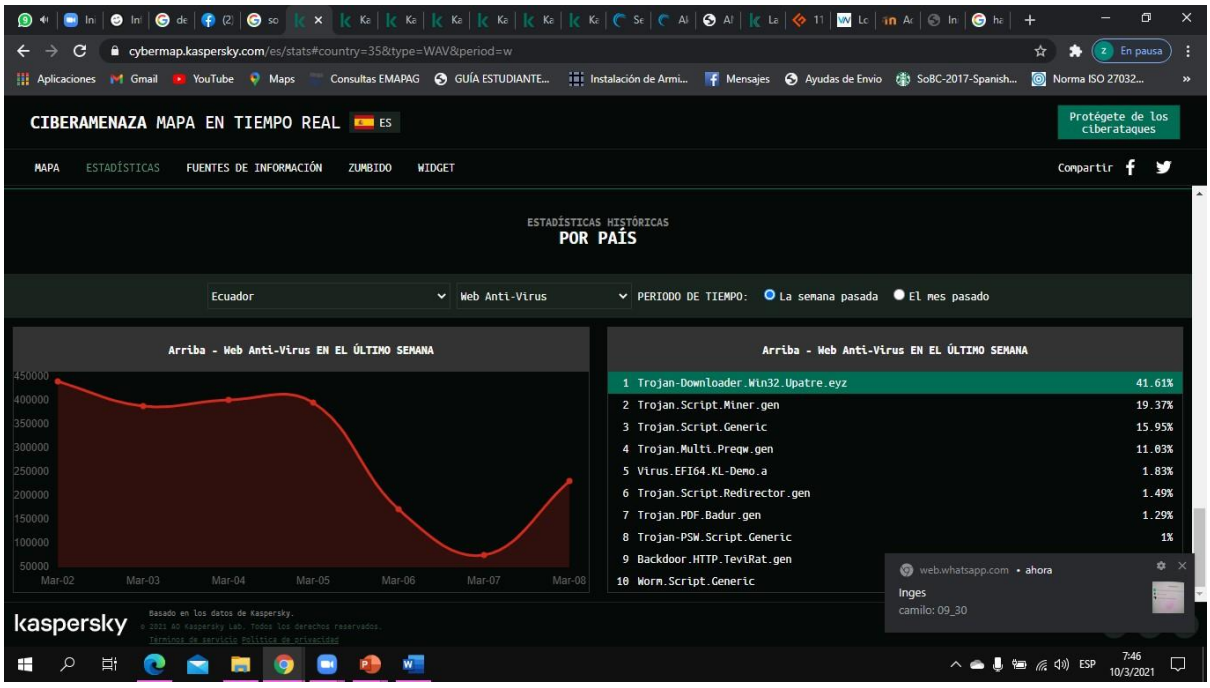
Host: protocolo IP identifica a cada ordenador que se encuentre conectado a la red mediante su correspondiente dirección.

TICs: Abreviatura de Tecnologías de la información y comunicación.

ANEXOS



Anexo 1: Los ataques de intrusión se encuentran dentro de los más ejecutados su función es intentar explotar aplicaciones, servicios y sistemas operativos vulnerables.



Anexo 2: Dentro de los ataques de troyanos más populares está el de tipo win32.

BIBLIOGRAFÍA

[1] OHMY GEEK, «OHMY GEEK,» 17 Mayo 2013. [En línea]. Available: https://ohmygeek.net/2013/05/17/los-principales-ataques-informaticos-de-la-actualidad/.

[2] Cisco cybersecurity, «Cisco,» 2 Abril 2019. [En línea]. Available: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/cybersecurity-series-threat.pdf. [Último acceso: 3 Marzo 2021].

[3] M. T. R. Manuel, «m.riunet.upv.es,» 6 Marzo 2016. [En línea]. Available: https://m.riunet.upv.es/bitstream/handle/10251/70164/MART%C3%8D%20-%20Desarrollo%20e%20implementaci%C3%B3n%20pr%C3%A1ctica%20de%20un%20PENTEST.pdf?sequence=2&isAllowed=y. [Último acceso: 3 Marzo 2021].

[4] S. A. W. ANDRÉS, «repository.ucatolica.edu.co,» 15 Junio 2019. [En línea]. Available: https://repository.ucatolica.edu.co/bitstream/10983/23377/1/Trabajo%20de%20Grado%20Seg.%20de%20la%20Informacion%20Final.pdf. [Último acceso: 4 Marzo 2021].

[5] C. S. W. Gonzalo, «Universidad privada del Norte,» 23 Agosto 2014. [En línea]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwisn-3w7ZXvAhVhpVkKHXP6AjoQFjAFegQIBRAD&url=https%3A%2F%2Frepositorio.upn.edu.pe%2Fbitstream%2Fhandle%2F11537%2F10239%2FCruz%2520Saavedra%2520Walter%2520Gonzalo.pdf%3F. [Último acceso: 4 Marzo 2021].

[6] B. A. C. ALEXANDRA, «repositorio.pucese.edu.ec,» 22 Abril 2019. [En línea]. Available: https://repositorio.pucese.edu.ec/bitstream/123456789/1890/1/BURBANO%20ANGULO%20CAROLINA%20ALEXANDRA.pdf. [Último acceso: 4 Marzo 2021].

[7] g0tmi1k, «kali.org,» 2020. [En línea]. Available: https://www.kali.org/docs/introduction/what-is-kali-linux/. [Último acceso: 24 Noviembre 2020].

[8] Oracle, «VirtualBox.org,» 2020. [En línea]. Available: https://www.virtualbox.org/. [Último acceso: 24 Noviembre 2020].

[9] Microsoft, «https://www.microsoft.com/,» 2020. [En línea]. Available: https://www.microsoft.com/es-es/windows-server. [Último acceso: 24 Noviembre 2020].

[10] Adrián y Yirda, « Definición de Windows 10,» 30 07 2019. [En línea]. Available: https://conceptodefinicion.de/windows-10/. [Último acceso: 2 11 2020].

[11] Gerald Combs , «www.wireshark.org,» 16 Octubre 2020. [En línea]. Available: https://www.wireshark.org/. [Último acceso: 20 Diciembre 2020].

[12] DragonJAR, «DragonJAR,» 12 Junio 2011. [En línea]. Available: https://www.dragonjar.org/manual-de-armitage-en-espanol.xhtml. [Último acceso: 24 Diciembre 2020].

[13] avast, «Avast.com,» 2 Enero 2020. [En línea]. Available: https://www.avast.com/es-ww/about. [Último acceso: 20 Diciembre 2020].

[14] X. R. y. o. colaboradores, «HTTrack website copier,» 20 Mayo 2020. [En línea]. Available: https://www.httrack.com/page/1/en/index.html. [Último acceso: 2 Febrero 2021].

[15] Stripo.email, «Stripo.email,» 31 Diciembre 2020. [En línea]. Available: https://stripo.email/es/. [Último acceso: 2 Febrero 2021].

[16] Enjoy Safer Technology, «eset.com,» 2021. [En línea]. Available: https://www.eset.com/fileadmin/ESET/LATAM/Overviews/Hogar/ESET-NOD32-Antivirus-Overview.pdf. [Último acceso: 8 Febrero 2021].

[17] Top mejores antivirus, «Top mejores antivirus,» 6 Noviembre 2020. [En línea]. Available: https://topmejoresantivirus.com/avg-antivirus/. [Último acceso: 3 Marzo 2021].

[18] M. Javier, «Loogic,» 20 Enero 2007. [En línea]. Available: https://loogic.com/miarrobacom/#:~:text=Mi%20arroba%20ofrece%20servicio%20de,tipo%20m%C3%A1s%20usado%20en%20espa%C3%B1ol.. [Último acceso: 9 Marzo 2021].

[19] L. H. DÍAZ, «El delito informático,» Diciembre 2019. [En línea]. Available: https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf. [Último acceso: 24 Noviembre 2020].

[20] G. G. Morales, «Gestión de la Ciberseguridad según el ISO/IEC 27032:2012,» 10 Marzo 2017. [En línea]. Available: https://es.linkedin.com/pulse/gesti%C3%B3n-de-la-ciberseguridad-seg%C3%BAn-el-isoiec-gianncarlo-g%C3%B3mez-morales. [Último acceso: 24 Noviembre 2020].

[21] Consejo nacional de planificacion (CNP), «Plan Nacional de Desarrollo 2017-2021-Toda una Vida,» 2017. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/downloads/2017/10/PNBV-26-OCT-FINAL_0K.compressed1.pdf. [Último acceso: 24 Noviembre 2020].

[22] Irene, Liliana, Soraya, Efraín, Roberto, Christian, Ángel y Miriam, INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES, Manabi: Área de Innovación y Desarrollo,S.L., 2018.

[23] Kaspersky, «Latam kaspersky,» 2021. [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Último acceso: 25 12 2020].

[24] ViewNext, «ViewNext,» 16 Abril 2020. [En línea]. Available: https://www.viewnext.com/tipos-de-ciberataques-a-empresas/. [Último acceso: 10 Marzo 2021].

[25] Telefonica Fundacion , CIBERSEGURIDAD,LA PROTECCIÓN DE LA INFORMACIÓN EN UN MUNDO DIGITAL, Madrid: Ariel, S.A, 2016.

[26] C. &. R. J. Dias, «Universitat Oberta de Catalunya UOC,» 7 Junio 2014. [En línea]. Available: http://openaccess. uoc. edu/webapps/o2/bitstream/10609/34501/7/cdiasTFC0614me moria. pdf.. [Último acceso: 05 Enero 2021].

[27] M. C. A. Leonardo, «Respositorio UNISEK,» 21 Marzo 2019. [En línea]. Available: https://repositorio.uisek.edu.ec/bitstream/123456789/3348/1/Tesis-AndresMeza.pdf. [Último acceso: 05 Marzo 2021].

[28] B. González y M. Raydel, «Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web,» *Revista Cubana de Ciencias Informáticas*, vol. 12, nº 4, pp. 52-65, 2018.

[29] M. H. Ander, «Laboratorio de Pentesting con GNS3,» 26 Septiembre 2019. [En línea]. Available: https://repositorio.unican.es/xmlui/bitstream/handle/10902/16949/419449.pdf?sequence=1&isAllowed=y. [Último acceso: 6 Marzo 2021].

[30] M. M. Ángel, «Welivesecurity,» 14 Diciembre 2018. [En línea]. Available: https://www.welivesecurity.com/la-es/2018/12/14/cibercrimen-ataques-comunes/. [Último acceso: 06 Marzo 2021].

[31] Welivesecurity, «ESET SECURITY REPORT,» 15 Diciembre 2018. [En línea]. Available: https://www.welivesecurity.com/wp-content/uploads/2018/06/ESET_security_report_LATAM2018.pdf. [Último acceso: 6 Marzo 2021].

[32] ESET Security , «Tendencia en ciberseguridad para el 2021,» 3 Enero 2021. [En línea]. Available: https://www.welivesecurity.com/wp-content/uploads/2020/12/Cybersecurity_Trends_2021_ES.pdf. [Último acceso: 7 Marzo 2021].

[33] AXEL SPRINGER ESPAÑA, «Computer hoy,» 2 Enero 2021. [En línea]. Available: https://computerhoy.com/antivirus. [Último acceso: 8 Marzo 2021].

[34] E. D. R. C. F. D. B. LARRY ANDRES SILVA CASTRO, «http://repositorio.utp.edu.co/,» 2 Octubre 2011. [En línea]. Available: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2518/0058S586.pdf?sequence=1&isAllowed=y. [Último acceso: 23 Noviembre 2020].