UACM

Universidad Autónoma
de la Ciudad de México

NADA HUMANO ME ES AJENO

COLEGIO DE CIENCIA Y TECNOLOGÍA
LICENCIATURA EN INGENIERÍA EN SISTEMAS
ELECTRÓNICOS Y DE TELECOMUNICACIONES

Implementación de análisis de red a través de Kali Linux sobre plataforma Raspberry Pi

T E S I S

QUE PARA OPTAR POR EL TÍTULO DE

LICENCIADO EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

P R E S E N T A :

MICHAEL RAMÍREZ RAMÍREZ

D I R E C T O R : **M. EN I. LUIS ENRIQUE ARANDA MELO**

C O D I R E C T O R : **ING. OSCAR ABRAHAM OCAMPO ROJAS**

Ciudad de México, mayo de 2024.

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

Dedicatoria.

A mis padres, quienes me apoyaron en esta trayectoria de conocimiento, sobre todo a mi madre quien estuvo siempre presente. Este trabajo es dedicado a su inquebrantable apoyo, elemento fundamental que han sido el cimiento de mi trayectoria académica. A mi familia, por su comprensión, gracias por ser el refugio en cada desafío.

Este logro está también dedicado a aquellos que han creído en mí. A mis amigos, cuya amistad ha sido fundamental en los momentos difíciles.

Agradecimiento.

Expreso mi agradecimiento a todos aquellos que, de diversas maneras, han contribuido a la realización de este proyecto académico. A mis profesores cuya guía ha sido esencial para mi desarrollo académico. Este logro lleva consigo la influencia de sus enseñanzas y la responsabilidad.

Objetivo.

El objetivo principal de este proyecto de investigación es el análisis de la seguridad de protocolos y servicios de red para identificar posible vulnerabilidad y establecer estrategias de seguridad efectivas que permitan proteger los datos y recursos de una organización. Para lograr este objetivo, se realizará una evaluación de profundidad de los protocolos y servicios utilizados en la red, con la finalidad de identificar la vulnerabilidad presente y se analizar los riesgos asociados.

Una vez identificado la vulnerabilidad, se realizará un análisis de los posibles vectores de ataque para desarrollar estrategias de mitigación adecuadas para minimizar el riesgo de ataques. Estas estrategias consideran en incluir parches de seguridad, así como el fortalecimiento de la configuración de seguridad y la orientación de los usuarios para que sean conscientes de las mejores prácticas de seguridad en la red.

Los objetivos que se persiguen en este proyecto de investigación es mejorar la seguridad de los protocolos y servicios de red para proteger los datos y recursos de una organización. La investigación de la importancia de elaboración e implementación de un laboratorio en un entorno controlado para implementar acciones. Como también satisfacer los requerimientos para poder implementar las herramientas de hacking ético necesarias en la plataforma Raspberry Pi. Al identificar las vulnerabilidades y establecer estrategias efectivas de seguridad, se logrará mitigar el riesgo de ataques y mejorar la confiabilidad y disponibilidad de los servicios en la red.

Introducción.

En la actualidad, el *hacking* ético ha experimentado un crecimiento importante en el campo de la seguridad informática. Esto se debe a la necesidad de proteger la infraestructura y los datos de empresas y organizaciones, así como a la sofisticación de los ciberataques y la necesidad de cumplir con regulaciones y cumplimiento de estándares.

Las diferentes amenazas que existen en las formas en que nos conectamos a Internet, han llevado a un refuerzo en las áreas de ciberseguridad, como:

- **La seguridad de datos:** medidas y prácticas implementadas para proteger la confidencialidad, integridad y disponibilidad de la información almacenada, procesada y transmitida en un sistema o una organización.
- **Seguridad de software:** las medidas y prácticas implementadas para proteger los sistemas y las aplicaciones de software contra amenazas y ataques cibernéticos.
- **Seguridad de red:** medidas y prácticas implementadas para proteger una red de computadoras y los datos que se transmiten a través de ella contra amenazas y ataques cibernéticos.
- **Seguridad física:** medidas y prácticas implementadas para proteger los activos físicos de una organización, como los edificios, equipos, instalaciones y personas, contra amenazas físicas y riesgos.
- **Seguridad social:** las medidas y prácticas implementadas para proteger la información y la privacidad de los usuarios en las plataformas.

La ciberseguridad es fundamental en la actualidad, ya que cada vez más empresas y organizaciones dependen de la tecnología para realizar sus operaciones diarias, y los ciberataques pueden causar graves daños financieros y de reputación.

Por esta razón, las empresas están incrementado su interés en ciberseguridad y contratando expertos en la materia. Las áreas de ciberseguridad están en constante evolución debido a que los ciberdelincuentes también están modificando y creando nuevas formas más elaboradas de acceder y vulnerar sistemas. Por lo tanto, es necesario que los expertos en ciberseguridad estén actualizados y tengan conocimientos avanzados en seguridad informática.

Este trabajo se enfoca en la identificación de vulnerabilidades a nivel de protocolos de red y servicios, así como en la exploración de cómo algunas de estas vulnerabilidades pueden ser

explotadas. Con la finalidad de realizar recomendaciones de seguridad para la mejor de los protocolos y servicios de la red.

Glosario.

Activos: Elementos valiosos, como datos y sistemas, que requieren protección.

Activos digitales: Elementos valiosos almacenados en formato digital, como datos, sistemas y aplicaciones.

Amenazas cibernéticas: Peligros para sistemas y datos digitales.

Aspectos físicos y digitales: Incluye medidas de seguridad en formatos físicos y en línea.

Autenticación: Proceso de verificar la identidad de un usuario o entidad.

Botnet: Red de dispositivos comprometidos controlados por un atacante.

Capas del modelo OSI: Niveles de funciones en el modelo OSI.

Cifrado: Proceso de convertir información en un formato ilegible para protegerla.

Cliente-servidor: Modelo donde los clientes se conectan a un servidor para realizar operaciones.

Criptomonedas: Monedas digitales que se consideran seguras y anónimas.

Credenciales de inicio de sesión: Datos para acceder a cuentas.

Continuidad del negocio: Planificación para mantener operaciones esenciales en caso de interrupciones o desastres.

Controles de seguridad: Medidas técnicas y administrativas para reducir vulnerabilidades y mitigar riesgos en la seguridad de la información.

Contraseñas o claves de cifrado: Datos utilizados para autenticar y proteger el acceso a sistemas o datos cifrados.

Consecuencias de reputación: Daño a la imagen o percepción pública.

Cookies: Pequeños archivos que almacenan información sobre la navegación web.

Criptomonedas: Monedas digitales que se consideran seguras y anónimas.

Credenciales de inicio de sesión: Datos para acceder a cuentas.

COBIT: Control Objectives for Information and Related Technologies, marco para gobernar y gestionar tecnologías de la información.

CVE: Common Vulnerabilities and Exposures, una lista pública de vulnerabilidades.

Descifrar: Proceso de revertir un cifrado para obtener información legible.

DNS Spoofing: Suplantación de la tecnología DNS para redirigir tráfico.

Dominio: Nombre que identifica un sitio web.

Emular: Proceso mediante el cual un sistema virtual simula el comportamiento de otro sistema, como si estuviera ejecutando su propio hardware y software.

Extensiones: Partes finales de los nombres de archivo.

FreeBSD: Sistema operativo de código abierto basado en Unix, diseñado para ser seguro, rápido y eficiente, utilizado en servidores y sistemas integrados.

Filtración: Divulgación no autorizada de información.

Gestión de parches y actualizaciones: Estrategias para aplicar correcciones de seguridad y mejoras en el software.

Gestión de riesgos: Identificación, evaluación y control de amenazas con controles y políticas.

Hacking: Acceso no autorizado a sistemas informáticos.

Interrupción de servicios: Bloqueo o desactivación de servicios en sistemas o redes.

Internet Engineering Task Force (IETF): Organización que desarrolla estándares de Internet.

Instituto Nacional de Estándares y Tecnología (NIST): Entidad que promueve estándares y tecnología.

Inyección de paquetes maliciosos: Introducción de datos dañinos en la comunicación.

IP Spoofing: Suplantación de dirección IP de origen en paquetes de red.

ITU (Unión Internacional de Telecomunicaciones): Organización que establece estándares y regulaciones para las tecnologías de la información y la comunicación a nivel global.

Informática forense: Disciplina que se enfoca en recuperar y analizar pruebas digitales en investigaciones legales y criminales, involucrando la recuperación de información de dispositivos electrónicos.

Latencia: Tiempo que transcurre entre un estímulo y la respuesta que produce.

libpcap: La biblioteca libpcap (Packet Capture Library) es una biblioteca de software de código abierto que proporciona capacidades de captura y filtrado de paquetes en sistemas Unix-like (como Linux y macOS).

Linux: Sistema operativo de código abierto basado en el kernel del mismo nombre, utilizado en una variedad de dispositivos y plataformas.

Mac OS X: Sistema operativo desarrollado por Apple para sus dispositivos Macintosh (Mac), conocido por su diseño elegante y su enfoque en la experiencia del usuario.

Malware: Software malicioso diseñado para dañar o acceder a sistemas y datos.

Máquina Virtual: Un software que emula un sistema operativo dentro de otro sistema, funcionando de manera aislada con sus propios recursos y configuraciones.

Medidas de mitigación: Acciones para reducir la exposición a riesgos.

NIST: National Institute of Standards and Technology, un instituto estadounidense que mantiene una base de datos de vulnerabilidades.

Npcap: Npcap es una bifurcación (fork) del proyecto WinPcap, que es una implementación de la biblioteca libpcap para sistemas Windows.

OpenBSD: Sistema operativo de código abierto basado en Unix, conocido por su enfoque en la seguridad y sus características avanzadas de seguridad.

Organización Internacional de Normalización (ISO): Entidad que establece normas internacionales.

Phishing: Táctica de engaño para obtener información sensible.

Plan de respaldo: Estrategia para mantener la operación ante fallos o interrupciones.

Plan de contingencia: Estrategia para afrontar situaciones de emergencia y mantener la operación.

Potencia computacional: Capacidad de procesamiento de una computadora.

Privacidad: Protección de la información personal y sensible de individuos y entidades.

Protocolo de Control de Transmisión (TCP): Protocolo que garantiza la entrega confiable de datos en redes.

Protocolo de Usuario de Datagrama (UDP): Protocolo que permite la transmisión de datos sin garantía de entrega confiable.

X

Prueba sistemática: Método organizado de probar todas las combinaciones una por una o de manera aleatoria.

Red de spoofing: Red inalámbrica falsa diseñada para engañar a usuarios.

Router: Dispositivo que conecta redes y dirige el tráfico entre ellas.

Secretaría de la Defensa Nacional (SEDENA): Organismo gubernamental de defensa.

Servidores: Dispositivos que almacenan y gestionan información.

Script: Pequeño programa o código utilizado para realizar tareas específicas de forma automatizada.

Sistemas de información abiertos: Sistemas interconectados con redes y que interactúan con otros sistemas externos, lo que aumenta la importancia de la seguridad de la información.

SSID: Nombre de red inalámbrica.

Solaris: Sistema operativo desarrollado por Oracle, originalmente creado por Sun Microsystems, diseñado para servidores y estaciones de trabajo de alto rendimiento.

Técnicas de compresión: Métodos para reducir el tamaño de los datos.

Tokens: Dispositivos físicos o de software que autentican a los usuarios y les dan acceso a recursos protegidos.

VBScript: Lenguaje de programación usado en scripts de Windows.

Vulnerabilidades: Puntos débiles en sistemas o redes que pueden ser explotados en un ataque.

Web Spoofing: Suplantación de una página web real con una falsa.

WikiLeaks: Sitio web que publica información confidencial.

Windows: Sistema operativo desarrollado por Microsoft, ampliamente utilizado en entornos personales y empresariales.

Índice de Contenido

Contenido

DEDICATORIA III

AGRADECIMIENTO. IV

OBJETIVO. V

INTRODUCCIÓN. VI

GLOSARIO. VIII

ÍNDICE DE CONTENIDO XIII

ÍNDICE FIGURAS XVII

ÍNDICE DE TABLAS XIX

Capítulo 1: La importancia de la seguridad y sus elementos.

1.1 SEGURIDAD DE LA INFORMACIÓN 2

1.2 CIBERSEGURIDAD 3

1.2 RELACIÓN ENTRE SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD. 4

1.3 AMENAZAS Y ATAQUES. 5

1.3.1 Ataques a contraseñas 5

1.3.2. Ataques a las conexiones. 8

1.3.3. Ataque por Malware. 11

1.3.4 Ingeniería social 13

1.4. ANTECEDENTES DE ATAQUES A NIVEL INTERNACIONAL. 14

1.4.1. Ataque: I love you (2000) 15

1.4.2. Caso: WikiLeaks (2007) 15

1.4.3. Ataque: Stuxnet (2010) *15*

1.4.4. Caso: Play Station Network (2011) *16*

1.4.5. Caso: Yahoo! (2013-2014) *16*

1.4.6. Caso: Netflix y Disney (2017) *16*

1.4.7. Caso: SEDENA (2022) *16*

REFERENCIAS 17

Capítulo 2: Seguridad de la red y herramientas para evaluar la seguridad.

2.1. ¿QUÉ ES UNA RED? 20

2.2 MODELO OSI 21

2.3 MODELO TPC/IP 22

2.4 PROTOCOLOS DE RED 22

2.4.1 FTP *24*

2.4.2. MySQL *25*

2.4.3 Telnet *25*

2.5 SEGURIDAD EN LAS REDES 26

2.5.1. Cualidades de la seguridad de la información *27*

2.5.2 Plan de seguridad en una red. *27*

2.5.3 Seguridad física en una red *28*

2.5.4 Seguridad lógica en una red. *30*

2.5.5 POLÍTICA DE SEGURIDAD BASADA EN REGLAS 31

2.5.6 MECANISMOS DE CONTROL DE ACCESO 31

2.5.6 AUDITORÍA DE SEGURIDAD 32

2.5.7 CONFIDENCIALIDAD DEL FLUJO DE TRÁFICO 34

2.6 NORMAS Y ESTÁNDARES PARA LA SEGURIDAD DE LA INFORMACIÓN 35

2.6.1 Norma X.800 .....*36*

2.6.2 ISO 27000 e ISO 27001 .....*37*

2.7 HERRAMIENTAS PARA EVALUAR SEGURIDAD. 37

2.7.1 Kali Linux *37*

2.7.2 Nmap.....*39*

2.7.3 Wireshark *40*

2.7.5 Metasploit *41*

2.7.4 Metasploitable. *42*

2.7.7 VirtualBox......*43*

REFERENCIAS. 45

Capítulo 3: Instalación de Kali en Raspberry Pi 4 y máquina virtual de Metasploitable 2.

3.1. INSTALACIÓN DE KALI EN RASPBERRY PI 4 48

3.1.1. ¿Por qué Kali Linux? *48*

3.1.2. Raspberry Pi para instalar Kali Linux......*51*

3.1.3. Raspberry Pi Imager. *52*

3.2 INSTALACIÓN DE VIRTUALBOX.....53

3.3 INSTALACIÓN DE METASPLOITABLE. 55

REFERENCIAS 60

Capítulo 4: Análisis de red y explotación de vulnerabilidades.

4.1 SISTEMA CON KALI EN LA RED 62

4.2 ESCANEO CON NMAP 63

4.2. EXPLOTACIÓN DE VULNERABILIDADES 67

4.2.1. Vulnerabilidad 1. Telnet puerto 23 68

4.2.2. Vulnerabilidad 2. MySQL puerto 3306 70

4.2.3. Vulnerabilidad 3. FTP puerto 21 74

Capítulo 5: Resultados.

5.1 REPORTE 79

Conclusiones

CONCLUSIONES. 85

BIBLIOGRAFÍA Y REFERENCIAS 89

REFERENCIAS CAPÍTULO 1 89

REFERENCIAS CAPÍTULO 2. 89

REFERENCIAS CAPÍTULO 3 91

Índice Figuras

Figura 1.1: Contraseñas más comunes en 2019-2021 según NordPass. 7

Figura 2.1: Capas de modelo OSI. 22

Figura 2.2: Triángulo de la seguridad informática. 27

Figura 3.1. Plataformas con soporte oficial de Kali. 50

Figura 3.2: Versión 2022.3 Kali Linux en Raspberry. 51

Figura 3.3: Raspberry Pi 4 Model B. 51

Figura 3.4. Interfaz de Raspberry Pi imager de la versión v1.7.3. 52

Figura 3.5: Pantalla de inicio del sistema Kali. 53

Figura 3.6. Página oficial de VirtualBox. 54

Figura 3.7: Interfaz de VirtualBox 54

Figura 3.8: Página de descarga de Metasploitable 2. 55

Figura 3.9: Parámetros de tipo de sistema para máquina virtual. 56

Figura 3.10: Tamaño de memoria de máquina virtual. 57

Figura 3.11: Unidad Virtual de Metasploitable 2. 57

Figura 3.12: Máquina virtual de Metasploitable 2. 58

Figura 3.13. Configuración de red de máquina virtual. 59

Figura 4.1: Comando ifconfig para Kali Linux. 63

Figura 4.2.A: Escaneo con nmap comando nmap 192.168.100.0/24 64

Figura 4.2.B: Escaneo con nmap comando nmap 192.168.100.0/24. 65

Figura 4.3: Comando ifconfig en Metasploitable 2. 66

Figura 4.4. Determinación del sistema operativo del objetivo. 67

Figura 4.5: Acceso al sistema de Metasploitable 2 por medio del protocolo Telnet. 69

Figura 4.6. Consola de metasploit en Kali Linux. 70

Figura 4.7. Exploits disponibles para la vulnerabilidad de MySQL. 71

Figura 4.8: Parámetros para configurar ataque por diccionario. 71

Figura 4.9. Resultados del ataque de directorio. 72

Figura 4.10: Tráfico de red para el caso de ataque de diccionario 73

Figura 4.11: Búsqueda de la herramienta para ataque al puerto 21 74

Figura 4.12: Parámetros para ataque al puerto 21. 75

Figura 4.13: Registro del ataque al puerto 21. 75

Figura 4.14: Directorio del servidor ftp de Metasploitable 2. 76

Índice de tablas

TABLA 5.1. EQUIPOS DETECTADOS EN EL ESCANEO DE RED. 79

TABLA 5.2: SERVICIOS Y PUERTOS DE EQUIPO 1. 80

TABLA 5.3: SERVICIOS Y PUERTOS DE EQUIPO 2. 81

TABLA 5.4: VULNERABILIDADES Y POSIBLES SOLUCIONES. 82

TABLA 6.1 COMPARACIONES DE VERSIONES DE KALI LINUX. 87

Capítulo 1:

La importancia de la seguridad y sus elementos.

Introducción de capítulo.

En los últimos años, la ciberseguridad ha adquirido una importancia cada vez mayor debido al aumento exponencial del uso de la tecnología en nuestras vidas cotidianas, el entorno académico y empresarial. El acceso a internet, el almacenamiento en la nube mediante el uso generalizado de dispositivos de acceso a través de redes de comunicaciones ha ampliado las posibilidades de ataques informáticos. Además, la digitalización de la mayoría de los procesos empresariales y la creciente dependencia de los servicios en línea han aumentado la vulnerabilidad de las empresas a los ciberataques.

Los ciberdelincuentes, aprovechando esta vulnerabilidad, pueden acceder a información confidencial, interrumpir servicios críticos, secuestrar sistemas o realizar actividades delictivas como el robo de identidad o el fraude financiero. El impacto financiero y de reputación de los ciberataques puede ser devastador para las empresas, y en algunos casos, puede llevar a la quiebra.

Por lo tanto, es fundamental que las empresas y las organizaciones lleva a cabo medidas sólidas de ciberseguridad para protegerse contra los ciberataques y minimizar el riesgo de sufrir daños. Esto implica una desarrollan estrategia de seguridad de múltiples capas, que incluya no solo tecnología de seguridad, sino también la educación y concientización del personal en ciberseguridad, la realización de políticas y procedimientos de seguridad sólidos y la realización de auditorías y pruebas de penetración regulares para identificar su vulnerabilidad.

1.1 Seguridad de la información

El autor Whirman M. en su publicación "*Principles of Information"*, menciona que: La seguridad de la información se refiere a las medidas y prácticas diseñadas para proteger la confidencialidad, integridad y disponibilidad de la información, tanto en formato electrónico como en formato físico. La seguridad de la información busca prevenir que la información sea revelada, modificada, destruida o acceda de manera no autorizada.[1]

Conceptos clave relacionados con la seguridad de la información incluyen:

- Confidencialidad; Se refiere a la protección de la información sensible para evitar su divulgación no autorizada. Implica el control de acceso a la información y el cifrado de datos para mantenerlos privados.
- Integridad; Consiste en mantener la exactitud, integridad y fiabilidad de la información. Esto implica prevenir modificaciones no autorizadas, garantizar la precisión de los datos y mantener la consistencia de la información a lo largo del tiempo.

- Disponibilidad; Se refiere a garantizar que la información esté accesible y utilizable cuando sea necesario. Esto implica proteger contra interrupciones, fallos del sistema o ataques que puedan causar la indisponibilidad de la información.
- Autenticidad; Se refiere a la verificación de la autenticidad de la información y de los usuarios que acceden a ella. Esto puede involucrar la aplicación de mecanismos de autenticación, como contraseñas, certificados digitales o biometría.
- Respaldo y recuperación; La cual implica realizar copias de seguridad de la información y tener planes de recuperación ante desastres para garantizar la continuidad del negocio y la recuperación de datos en caso de pérdida o daño.
- Gestión de riesgos; La seguridad de la información también implica identificar y evaluar los riesgos asociados con la información y tomar medidas para mitigarlos. Esto puede incluir el desarrollo de controles de seguridad, políticas y procedimientos para reducir los riesgos a un nivel aceptable.
- Concientización y capacitación; La seguridad de la información requiere la participación de los usuarios. Es importante brindar capacitación y conciencia sobre las mejores prácticas de seguridad, como el manejo de contraseñas, la detección de ataques de phishing y el uso seguro de la tecnología.

La seguridad de la información es esencial en todos los ámbitos, incluyendo organizaciones, gobiernos y usuarios individuales, para proteger los activos y la privacidad de la información frente a las constantes amenazas y riesgos en el entorno digital.

1.2 Ciberseguridad

La ciberseguridad es un conjunto de medidas y prácticas destinadas a proteger los sistemas informáticos, redes, dispositivos y datos de ataques, daños, robo o acceso no autorizado. La ciberseguridad se enfoca en la prevención, detección y respuesta a los riesgos y amenazas cibernéticas, y busca garantizar la confidencialidad, integridad y disponibilidad de la información y de los sistemas en línea.

Este conjunto de medidas abarca una amplia variedad de áreas, incluyendo la protección de datos personales y empresariales, la seguridad de las redes y los dispositivos, la prevención de ataques informáticos y el desarrollo de planes de contingencia en caso de incidentes de seguridad cibernética. También se enfoca en la educación y la concientización de los usuarios sobre las amenazas cibernéticas y las mejores prácticas para protegerse.

La ciberseguridad es una disciplina basada en la computación que involucra tecnología, personas, información y procesos para permitir operaciones seguras en el contexto de los

adversarios. Se basa en los campos fundamentales de seguridad de la información y garantía de la información. [2]

Es un desafío constante debido a la evolución de las amenazas y la sofisticación de los ataques cibernéticos. Por lo tanto, es esencial mantenerse actualizado con las mejores prácticas de seguridad, seguir las recomendaciones de expertos y utilizar herramientas de seguridad adecuadas para protegerse contra las amenazas digitales.

“Por otro lado, en la publicación de *International Federation for Information Processing Technical Committee on Information Security Education* (Comité Técnico de Educación en Seguridad de la Información de la Federación de Procesamiento de Información) se menciona que: la ciberseguridad es una disciplina basada en la computación que involucra tecnología, personas, información y procesos para permitir operaciones seguras en el contexto de los adversarios. Se basa en los campos fundamentales de seguridad de la información y garantía de la información.” [3]

1.2 Relación entre seguridad de la información y la ciberseguridad.

La seguridad de la información y la ciberseguridad están estrechamente relacionadas y se consideran dos aspectos fundamentales para proteger los activos digitales en el entorno tecnológico. Si bien los términos a menudo se utilizan indistintamente, hay una diferencia sutil pero importante entre ellos.

La seguridad de la información se centra en proteger la confidencialidad, integridad y disponibilidad de la información en general, tanto en formato digital como físico. Esto implica establecer medidas para prevenir la divulgación, modificación o destrucción no autorizada de la información y asegurarse de que esté disponible cuando se necesite. Por otro lado, la ciberseguridad se enfoca específicamente en proteger los sistemas y datos digitales contra amenazas cibernéticas. Esto incluye la protección de sistemas informáticos, redes, dispositivos y datos contra ataques maliciosos, como *malware*, *hacking*, *phishing* y otras formas de ciberdelincuencia.

La seguridad de la información abarca aspectos físicos y digitales de la información, mientras que la ciberseguridad se enfoca en proteger los activos digitales y los sistemas de información contra amenazas cibernéticas.

Es importante destacar que la ciberseguridad es esencial para proteger la información en la era digital, ya que la mayoría de las amenazas provienen del entorno digital y requieren medidas específicas para mitigar los riesgos.

1.3 Amenazas y ataques.

En la seguridad informática, una amenaza se refiere a cualquier actividad, evento, proceso o estado que pueda dañar o dañar la integridad, disponibilidad o confidencialidad de los sistemas de información o de la infraestructura informática. Una amenaza puede ser intencional o accidental y puede ser causada por factores internos o externos.

En el libro “Fundamentos de Seguridad en la Red” el autor Stallings [4] define estos términos como:

Amenaza; Una posibilidad de violación de la seguridad, que existe cuando se da una circunstancia, capacidad, o evento que pudiera romper la seguridad y causar perjuicio.

Ataque; Un asalto a la seguridad del sistema derivado de una amenaza inteligente; es decir un acto inteligente y deliberado (especialmente en el sentido de métodos o técnicas) para eludir los servicios de seguridad y violar la política de seguridad de un sistema. [4]

Los ataques informáticos son acciones maliciosas llevadas a cabo por individuos o grupos con el objetivo de explotar vulnerabilidades en sistemas, redes o aplicaciones para obtener acceso no autorizado, robar información, interrumpir servicios o causar daños. Estos ataques pueden ser devastadores tanto para usuarios individuales como para organizaciones, y pueden tener consecuencias financieras, legales y de reputación.

La clasificación de los tipos de ataques informáticos se basa en diferentes criterios, como la intención del atacante, la técnica utilizada o el objetivo del ataque. A continuación, se presenta una introducción a la clasificación de los ataques informáticos en función de su objetivo principal:

- Ataques de contraseñas.
- Ataques a las Conexiones.
- Ataques por *malware*.
- Ataques de ingeniería social.

1.3.1 Ataques a contraseñas

Los ciberdelincuentes tienen diversas técnicas y herramientas con para atacar nuestras credenciales (conjunto de datos utilizados para identificar y autenticar a un usuario, proceso o dispositivo). Los usuarios suelen caer en malas prácticas que ponen en peligro la seguridad como utilizar contraseñas “débiles”, que facilitan la efectividad de las siguientes técnicas implementadas por el atacante.

Fuerza bruta; Un ataque de fuerza bruta es un método utilizado por los atacantes para descubrir credenciales de acceso a un sistema mediante la prueba de todas las combinaciones posibles de contraseñas o claves de cifrado hasta encontrar la correcta. Es un ataque simple pero efectivo que se basa en la premisa de que, aunque el número de combinaciones posibles puede ser muy grande, eventualmente se encontrará la contraseña correcta si se prueba suficientes veces. El atacante utiliza un programa automatizado para generar milles o incluso millones de intentos de inicio de sesión en un corto período de tiempo.

El funcionamiento exacto de un ataque de fuerza bruta implica lo siguiente:

- Recopilación del objetivo: El atacante identifica el sistema o servicio que desea comprometer, como una cuenta de usuario, un servidor o una aplicación en particular.
- Generación de combinaciones: Se generan todas las posibles combinaciones de caracteres que podrían formar una contraseña o clave de cifrado. Esto puede incluir letras mayúsculas y minúsculas, números, caracteres especiales y diferentes longitudes de contraseñas.
- Prueba sistemática: El atacante utiliza una herramienta automatizada o un script para probar cada combinación de forma secuencial o aleatoria. Por cada combinación probada, se verifica si coincide con la contraseña o clave real.
- Duración del ataque: La duración de un ataque de fuerza bruta puede variar dependiendo de la complejidad de la contraseña, la potencia computacional utilizada y las medidas de seguridad implementadas. Puede llevar desde segundos hasta años en casos extremos.

En un ataque de fuerza bruta, se prueban todas las combinaciones posibles de caracteres, comenzando desde combinaciones simples hasta llegar a combinaciones más complejas. Este proceso se lleva a cabo utilizando herramientas automatizadas que generan las combinaciones y las prueban una tras otra hasta encontrar la contraseña correcta.

Los ataques de fuerza bruta pueden ser extremadamente intensivos en términos de recursos computacionales y tiempo, ya que tienen que probar un gran número de combinaciones. Sin embargo, pueden tener éxito si la contraseña objetivo es débil o está compuesta por combinaciones predecibles.[5]

Ataque de diccionario; Un ataque de diccionario es una técnica utilizada en seguridad informática para descifrar contraseñas o claves de cifrado mediante el uso de una lista predefinida de palabras comunes o términos que podrían ser utilizados como contraseñas. A diferencia de un ataque de fuerza bruta, donde se prueban todas las combinaciones posibles,

un ataque de diccionario se basa en probar una lista de palabras comunes o predefinidas en un intento de encontrar la contraseña correcta.

Un ataque de diccionario es una técnica utilizada en seguridad informática para descifrar contraseñas o claves de cifrado mediante la prueba de palabras comunes o términos predefinidos en lugar de probar todas las combinaciones posibles. En lugar de agotar todas las opciones, este tipo de ataque se basa en la premisa de que muchas personas eligen contraseñas débiles o utilizan palabras comunes como contraseñas. Durante un ataque se utiliza una lista predefinida de palabras comunes o términos que podrían ser utilizados como contraseñas. Esta lista, conocida como diccionario, incluye palabras comunes del idioma, nombres populares, palabras relacionadas con el objetivo o términos que los usuarios suelen utilizar como contraseñas.

Los atacantes utilizan herramientas automatizadas (software) que prueban cada palabra del diccionario como contraseña, verificando si coincide con la contraseña real. Además, algunos atacantes personalizan el diccionario agregando palabras específicas relacionadas con el objetivo o utilizando técnicas de variaciones de palabras comunes.

Es una técnica en la que se utiliza un software que, de forma automática, trata de averiguar nuestra contraseña. Para ello, realiza diferentes comprobaciones. Estas contraseñas pueden estar basadas en estudios como el que llevo a cabo la empresa NordPass (Figura 1.1).

	2019		2020		2021	
	Contraseña	Número de usuarios	Contraseña	Número de usuarios	Contraseña	Número de usuarios
1	12345	2,812,220	123456	2,543,285	123456	103,170,552
2	123456	2,485,216	123456789	961,435	123456789	46,027,530
3	123456789	1,052,268	picture1	371,612	12345	32,955,431
4	test1	993,756	password	360,467	qwerty	22,317,280
5	password	830,846	12345678	322,187	password	20,958,297
6	12345678	512,560	111111	230,507	12345678	14,745,771
7	zinch	483,443	123123	189,327	111111	13,354,149
8	g_czechout	372,278	12345	188,268	123123	10,244,398
9	asdf	359,520	1234567890	171,724	1234567890	9,646,621
10	qwerty	348,762	senha	167,728	1234567	9,396,813

Figura 1.1: Contraseñas más comunes en 2019-2021 según NordPass.

$Figura\ 1.1$ Estudio de datos NordPass., "https://nordpass.com/es/most-common-passwords-list/ ", (consultado 20 de enero 2023)

Diferencia entre ataque de fuerza bruta y ataque de diccionario:

La principal diferencia entre un ataque de fuerza bruta y un ataque de diccionario radica en la forma en que se prueban las combinaciones. Mientras que un ataque de fuerza bruta prueba todas las combinaciones posibles, un ataque de diccionario se basa en una lista predefinida de palabras comunes. Algunos puntos para poder diferenciar estos ataques:

- En un ataque de fuerza bruta, se prueban todas las posibles combinaciones de caracteres para descifrar la contraseña o clave.
- En un ataque de diccionario, se utiliza una lista predefinida de palabras comunes o términos que podrían ser utilizados como contraseñas.
- En términos de eficacia, un ataque de fuerza bruta tiene más probabilidades de tener éxito si la contraseña es compleja y no está en el diccionario utilizado. Por otro lado, un ataque de diccionario tiene más probabilidades de éxito si la contraseña es débil o se basa en palabras comunes.

1.3.2. Ataques a las conexiones.

Los ataques a las conexiones son aquellos que buscan aprovechar la vulnerabilidad en la comunicación entre dos dispositivos o redes, con el objetivo de acceder a información confidencial o tomar el control de los sistemas involucrados. Estos ataques pueden incluir la intercepción de datos transmitidos en una red, la suplantación de identidad para obtener acceso no autorizado, la inyección de paquetes maliciosos para interrumpir la comunicación, entre otros. En general, los incluso ataques a las conexiones pueden ser muy peligrosos y pueden permitir que un atacante tenga acceso a información sensible o al control total de los sistemas afectados.

Redes Trampa; La creación de redes wifi falsas es una práctica muy utilizada por los ciberdelincuentes. Consiste en la creación de una red wifi idéntica a otra legítima y segura, con un nombre igual o muy similar a la original, que crean utilizando software y hardware. Luego, la configuran con los mismos parámetros que la original.

Las redes wifi falsas (también conocidas como "redes wifi de spoofing") son una técnica de ataque en la que un atacante crea una red inalámbrica falsa que parece legítima para atraer a las víctimas a conectarse a ella. Esta red falsa puede tener un nombre de red (SSID) similar al de una red wifi real cercana, lo que puede engañar a los usuarios para que se conecten sin saberlo a la red falsa en lugar de la red real. Una vez que un usuario se conecta a la red falsa, el atacante puede interceptar y espiar su tráfico de red, y posiblemente incluso robar

información confidencial como contraseñas, información de inicio de sesión y datos personales.

Los ataques de redes wifi falsas son especialmente peligrosos en lugares públicos como cafeterías, aeropuertos, hoteles y centros comerciales, donde los usuarios pueden estar preparados para conectarse a una red wifi abierta para acceder a Internet. Para evitar este tipo de ataques, es importante verificar el nombre de la red wifi a la que se está conectando y asegurarse de que sea legítimo antes de ingresar información confidencial en línea.

IP Spoofing; "*IP spoofing*" (suplantación de IP) es una técnica utilizada por los atacantes para falsificar la dirección IP de origen en un paquete de red con el objetivo de ocultar su identidad o para engañar a un sistema o usuario para que crea que el paquete es de una fuente confiable.

La técnica de *"IP spoofing"* funciona cambiando la dirección IP de origen en los paquetes de datos para hacer que parezca que se originan desde una dirección IP diferente. Esto se hace para ocultar la verdadera dirección IP del atacante y hacer que parezca que los paquetes provienen de otra fuente confiable o no sospechosa.

Web Spoofing; Es la suplantación de una página web real por otra falsa. La web falsa es una copia del diseño de la original, llegando incluso a utilizar una URL muy similar. El atacante trata de hacer creer que la web falsa es la original.

Web spoofing se puede llevar a cabo de varias formas, como por ejemplo mediante la suplantación de DNS o mediante la creación de un sitio web falso en un servidor comprometido y haciendo que el usuario acceda a él mediante un enlace o redireccionamiento malicioso.

DNS Spoofing; Se utiliza a través de software malicioso y explotando vulnerabilidades en las medidas de protección, los atacantes pueden infectar y acceder al router objetivo. Así, al acceder a una determinada web desde el navegador, este nos llevará a otra web seleccionada por el atacante. Para ello, los atacantes tienen que suplantar la DNS (*Domain Name System*), es decir, la tecnología utilizada para conocer la dirección IP del servidor donde está alojado el dominio al que quiere acceder.

Ataque a *Cookies*; Las *cookies* son pequeños archivos que contienen información de las páginas web que hemos visitado, así como otros datos de navegación, como pueden ser los anuncios vistos, el idioma, la zona horaria, si hemos proporcionado una dirección de correo electrónico, etc. Su función es ayudarnos a navegar de forma más rápida, recordando esta información para no tener que volver a procesarla.[6]

Las cookies se envían entre el servidor de la web y nuestro equipo, sin embargo, en páginas con protocolos http, este intercambio puede llegar a ser visible para los ciberdelincuentes. Los ataques a las cookies consisten en el robo o modificación de la información almacenada en una cookie.

Ataque de DDoS; Un ataque DDoS (*Distributed Denial of Service*) es un tipo de ataque cibernético en el que un atacante utiliza múltiples solicitudes (a menudo una botnet, que es una red de dispositivos comprometidos) para inundar un servidor o una red con una gran cantidad de tráfico malintencionadas, con el objetivo de hacer que el servicio o la red sean inaccesibles para los usuarios legítimos. El objetivo de un ataque DDoS es saturar el sistema o red objetivo con una tan grande de tráfico falso que no pueda manejarlo, lo que puede provocar una caída del servicio o una interrupción en el acceso a la red.

Inyección SQL; Las páginas web suelen estar vinculadas a bases de datos, basadas en un lenguaje de programación conocido como SQL. Este tipo de ataque permite a los ciberdelincuentes insertar líneas de código SQL en la propia aplicación web, obteniendo acceso parcial o completo a los datos, permitiendo ser monitorizados, modificados o robados por el atacante.

SQL es un lenguaje de programación utilizado para interactuar con bases de datos. Los ciberdelincuentes atacan a una aplicación web basada en este tipo de lenguaje, comprometiendo la base de datos mediante líneas de código malicioso. [6]

Man in the middle ; El ataque Man-in-the-Middle (MITM) es una técnica utilizada en seguridad informática en la que un atacante intercepta la comunicación entre dos partes legítimas y la manipula para poder espiar, modificar o falsificar información.

El objetivo principal del ataque MITM es obtener información sensible o realizar acciones maliciosas sin que las víctimas sean conscientes de la intervención del atacante.

El ataque MITM se lleva a cabo en tres fases:

1. Captura: el atacante intercepta la comunicación entre las dos partes legítimas, como un usuario y un servidor.
2. Manipulación: el atacante manipula la comunicación para realizar acciones maliciosas, como modificar los datos enviados por el usuario.
3. Reenvío: el atacante reenvía la comunicación modificada a su destino original, de modo que las partes legítimas no se dan cuenta de la manipulación.

Este ataque puede ser realizado en redes cableadas e inalámbricas. Para llevar a cabo este ataque, el atacante puede utilizar diversas técnicas, como el envenenamiento de ARP, DNS spoofing o el uso de redes WiFi-falsas.

1.3.3. Ataque por *Malware*.

Los ataques por *malware* usan programas maliciosos cuya funcionalidad consiste en llevar a cabo acciones dañinas en un sistema informático y contra nuestra privacidad. Generalmente, buscan robar información, causar daños en el equipo, obtener un beneficio económico a nuestra costa o tomar el control del equipo. Dependiendo del modus operandi, y de la forma de infección, existen distintas categorías de *malware.* [6]

Virus; Tipo de software malicioso o *malware* que se propaga a través de la inserción de su código en otros programas o archivos ejecutables. Los virus informáticos se caracterizan por tener la capacidad de autorreplicarse y propagarse a otros equipos y dispositivos, sin el conocimiento del usuario. Una vez que un virus infecta un sistema, puede llevar a cabo una variedad de acciones maliciosas, como dañar o destruir archivos, robar información, ralentizar o inutilizar el sistema, o incluso tomar el control completo del equipo.

Adware; Software malintencionado que muestra anuncios no deseados en la computadora o dispositivo móvil del usuario. Por lo general, el adware se instala junto con otro software descargado por el usuario y se ejecuta sin su conocimiento o consentimiento. El objetivo del adware es generar ingresos para sus creadores a través de la publicidad, lo que puede ralentizar la computadora y ser molesto para el usuario.

Spyware; *Malware* que se instala en un dispositivo sin el conocimiento del usuario y tiene como objetivo recopilar información del usuario sin su consentimiento. El spyware puede registrar las pulsaciones de teclas, capturar imágenes de la pantalla, grabar conversaciones o recopilar información del sistema, como contraseñas, direcciones de correo electrónico o información de tarjetas de crédito. Esta información puede ser utilizada por los atacantes con multas malintencionadas, como el robo de identidad, la extorsión o el espionaje.

Troyanos; También conocido como caballo de Troya, es un tipo de *malware* que se hace pasar como un programa legítimo para engañar a los usuarios y así poder infectar y tomar el control de su dispositivo. Los troyanos a menudo se propagan a través de correos electrónicos de phishing, descargas de software aprovechadas o aprovechadas vulnerabilidades de seguridad en el sistema operativo. Una vez que se instala en el dispositivo, el troyano puede permitir al atacante acceder a información personal, robar datos financieros, espiar al usuario y controlar el dispositivo a través de comandos remotos.

Backdoors; Es una puerta trasera o un método de acceso no autorizado a un sistema o red informática. En términos generales, se refiere a un mecanismo oculto utilizado por un atacante para acceder a un sistema, evadiendo las medidas de seguridad implementadas en él. El objetivo del backdoor es permitir que el atacante pueda realizar acciones maliciosas sin ser detectado, como la manipulación de datos, la obtención de información confidencial, el robo de contraseñas o la instalación de malware. Los backdoors pueden ser instalados intencionalmente por desarrolladores o administradores de sistemas para fines legítimos, pero también pueden ser utilizados por atacantes malintencionados para realizar actividades ilegales o dañinas. Este tipo de malware es capaz de monitorear, registrar y compartir la actividad con el atacante. También le permite la creación, eliminación, edición y copia de cualquier archivo.

Keylogger; Se utiliza para registrar y grabar todas las pulsaciones de teclas que se realizan en un dispositivo sin el conocimiento ni el consentimiento del usuario. El objetivo principal de un keylogger es recopilar información confidencial, como contraseñas, datos bancarios y otra información personal, y enviarla a terceros malintencionados. Los keyloggers pueden ser instalados en un dispositivo de forma manual o mediante el uso de otro malware, como un virus o un troyano. También pueden ser usados por padres o usuarios para monitorear las actividades en línea de sus hijos o empleados, pero en estos casos su uso debe ser legal y ético.

Stealers

Tipo de malware que se enfoca en robar información de un sistema sin que el usuario se dé cuenta. A menudo se utiliza para robar información financiera, como contraseñas de cuentas bancarias o tarjetas de crédito. Los stealers se ejecutan en segundo plano y envían la información robada a los atacantes, lo que permite que estos últimos accedan a la información personal o financiera del usuario.

Ransomware

El ransomware es un tipo de malware que bloquea el acceso a archivos o sistemas informáticos, y exige al usuario afectado un rescate o pago a cambio de restaurar el acceso. El ransomware puede cifrar los archivos del usuario o incluso bloquear todo el sistema operativo, mostrando una pantalla de advertencia o mensaje que exige el pago de un rescate en criptomonedas para recuperar los archivos o el control del sistema.

Los métodos de propagación del ransomware varían, pero comúnmente se distribuyen mediante correos electrónicos de phishing, descargas de software malicioso, explotación de vulnerabilidades de software o por medio de redes sociales. Una vez que se ejecuta en el

sistema, el ransomware busca archivos y la cifra o bloquea para que el usuario no pueda acceder a ellos. Luego, el malware muestra un mensaje de rescate que incluye instrucciones para pagar un rescate en criptomonedas a cambio de una clave de descifrado que permite al usuario recuperar el acceso a sus archivos o sistemas.

1.3.4 Ingeniería social

"La ingeniería social se puede definir como la práctica de obtener información confidencial, en la mayoría de los casos información de gran valor a través de la manipulación de las personas, donde los atacantes por medio del engaño intentan obtener información sensible o privilegios en algún sistema, se trata de engañar y confundir al usuario de un sistema informático para que acabe haciendo algo que realmente no quiere hacer, cómo ejecutar un software, facilitar sus claves de acceso, o acceder a determinados servicios". [7]

La ingeniería social es una técnica utilizada para engañar a las personas y persuadirlas para realizar ciertas acciones o divulgar información confidencial. Esta técnica no se basa en vulnerabilidades de la tecnología, sino en la explotación de la psicología humana y las debilidades emocionales y sociales. Algunos ejemplos de técnicas de ingeniería social incluyen la suplantación de identidad, la manipulación emocional, el engaño y la persuasión, el uso de pretextos falsos y la creación de falsos escenarios para obtener información confidencial o acceso no autorizado a sistemas informáticos. Los atacantes utilizan la ingeniería social en combinación con otras técnicas de hacking para obtener acceso no autorizado a sistemas informáticos o para robar información confidencial.

Phishing; "El phishing es una forma de ataque de ingeniería social en la que el atacante intenta acceder a las credenciales de inicio de sesión, obtener información confidencial o entregar malware." [8]

El phishing es un tipo de ataque de ingeniería social que se lleva a cabo a través de correos electrónicos, mensajes de texto o mensajes instantáneos fraudulentos que parecen ser legítimos y que buscan obtener información confidencial del usuario, como contraseñas, números de tarjetas de crédito o información personal. Los mensajes suelen contener enlaces a sitios web falsos que imitan a los sitios legítimos y engañan al usuario para que revelen información confidencial. El objetivo final del ataque de phishing es obtener acceso a información valiosa que puede ser utilizada para robar identidades, cometer fraudes financieros u otros delitos.

Vishing; Se puede decir que es un método similar al phishing, pero mediante el cual se utilizan llamadas telefónicas fraudulentas en lugar de correos electrónicos. El atacante finge ser representantes de bancos o compañías de seguros.

Smishing; Técnica de ingeniería social que se utiliza para engañar a las personas mediante el envío de mensajes de texto o SMS fraudulentos. El objetivo del smishing es hacer que el usuario revele información personal, financiera o confidencial. Los mensajes suelen incluir enlaces maliciosos que dirigen a sitios web fraudulentos o solicitudes para que el usuario llame a un número telefónico fraudulento.

Scareware; Se intenta asustar a los usuarios para que realicen alguna acción, como comprar un software falso o descargar un archivo malicioso. El scareware a menudo se presenta en forma de mensajes de alerta que afirman que el sistema ha sido comprometido con virus, y que se debe tomar una acción inmediata para solucionar el problema. A menudo, estos mensajes son falsos y están diseñados para engañar a los usuarios para que realicen acciones que beneficien al atacante, como proporcionar información personal o financiera, o descargar software malicioso.

1.4. Antecedentes de ataques a nivel internacional.

Los ataques de hacking a nivel internacional son aquellos realizados por hackers o grupos de hackers a nivel global, con el objetivo de obtener acceso no autorizado a sistemas informáticos y robar información valiosa o causar daños.

Estos ataques pueden ser realizados de diversas formas, como la explotación de vulnerabilidades en el software o hardware de los sistemas, el phishing o la ingeniería social para obtener credenciales de acceso, o la realización de ataques de denegación de servicio (DDoS) para inundar un sistema con tráfico malicioso y dejarlo fuera de línea.

Los motivos detrás de los ataques de *hacking* a nivel internacional pueden variar, desde la obtención de información para conseguir ganancias financieras, hasta la realización de ataques por motivos políticos o ideológicos.

Es importante destacar que los ataques de hacking a nivel internacional pueden tener un impacto significativo en la economía, la seguridad nacional y la privacidad de los usuarios, por lo que es crucial que las empresas y los gobiernos implementen medidas de seguridad adecuadas para protegerse contra estas amenazas.

Desafortunadamente, en la historia de la informática, ha habido muchos ataques informáticos notables que han tenido un impacto significativo en las empresas, los gobiernos y los

individuos. A continuación, se presentan algunos de los ataques informáticos más destacados y relevantes en la historia.

1.4.1. Ataque: *I love you* (2000)

Uno de los mayores ataques de *malware* de la historia fue el gusano *I love you*, que durante el mes de mayo del año 2000 infectó a más de 50 millones de computadoras en todo el mundo.

I love you se propagó a través de correos electrónicos, que incluían un archivo adjunto llamado "LOVE-LETTER-FOR-YOU.TXT.vbs". Cuando el usuario abría el archivo adjunto, el gusano se instalaba en el sistema y se propagaba a otros contactos del usuario a través del correo electrónico. El gusano también tiene la capacidad de copiar en archivos del sistema y reemplazaba archivos importantes con copias infectadas, causando daños significativos en los sistemas.

Se trataba de un *malware* que se replicaba y trasmitía por correo electrónico de las víctimas, donde el asunto del email era “ILOVEYOU”, éste eliminaba archivos con determinadas extensiones remplazándolos por otros con el mismo nombre, pero con sus propias extensiones de *VBScript*. [9]

1.4.2. Caso: *WikiLeaks* (2007)

WikiLeaks no es un ataque de *hacke*r en sí mismo, sino un sitio web que publica información confidencial que ha sido obtenida de diversas fuentes, incluyendo la de los *hackers*. En este portal se encuentran disponibles miles de documentos con información sensible para la opinión pública. La información publicada por *WikiLeaks* ha generado controversia y ha tenido impacto en gobiernos y empresas, revelando secretos y conductas cuestionables.

Su actividad se centra en denunciar acciones éticamente reprochables de un organismo y organizaciones, como gobiernos, empresas, etc. [9]

1.4.3. Ataque: *Stuxnet* (2010)

Stuxnet es un *malware* que infecta sistemas operativos Windows, y cuyo objetivo es controlar sistemas SCADA (*Supervisory, Control And Data Adquisition*) que monitorean el funcionamiento de estructuras industriales.

Fue descubierto en la central nuclear iraní de Natanz, donde ya había infectado a miles equipos. Tras la investigación posterior se comprobó que se había extendido a infraestructuras críticas de 13 países. [9]

1.4.4. Caso: *Play Station Network* (2011)

En abril de 2011, la compañía Sony sufrió un grave ataque en su plataforma de juegos y compras en línea de *Play Station*. Los atacantes lograron acceder a la información almacenada en las cuentas de aproximadamente 77 millones de usuarios, lo que representó un gran golpe para la empresa.

Además de comprometer la información personal y financiera de los usuarios de *PlayStation*, el ataque también interrumpió los servicios en línea de la plataforma durante varias semanas, lo que causó un gran malestar entre los clientes. El ataque fue atribuido a un grupo de hackers llamado "*Anonymous*", aunque algunos miembros del grupo negaron su participación. Como resultado del ataque, Sony tuvo que implementar nuevas medidas de seguridad y compensar a los usuarios afectados.

1.4.5. Caso: *Yahoo!* (2013-2014)

En 2014 *Yahoo!* sufrió el robo de información de las cuentas de unos 500 millones de usuarios de la plataforma, lo que obligó a la compañía a pedir que todos los usuarios cambiaran sus contraseñas, aunque su información ya había sido comprometida.

Un año antes había sufrido otro ataque que en el que también le fueron sustraídos los datos de los usuarios. En un primer momento se cifraron en 1,000 millones de cuentas afectadas, pero en las últimas auditorias llevadas a cabo por Verizon éstas podrían haber llegado hasta los 3,000 millones.[9]

1.4.6. Caso: Netflix y Disney (2017)

Los atacantes consiguieron colarse en los servidores de ambas compañías y hacerse de su contenido no publicado todavía, exigiendo grandes sumas de dinero para no hacerlos públicos en Internet antes de sus respectivos estrenos.[9]

1.4.7. Caso: SEDENA (2022)

El Gobierno de México sufrió un hackeo masivo por parte del grupo de activistas denominado "Guacamaya", quienes habrían logrado vulnerar la base de datos de la Secretaría de la Defensa Nacional (SEDENA). La información hackeada consiste en una filtración de aproximadamente 6 terabytes de información, que incluye decenas de miles de correos alojados en los servidores de la SEDENA, y que datan del año 2016 hasta septiembre de 2022.

Referencias

[1] Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. Cengage Learning.

[2] Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). (2017). Cybersecurity Curricular 2017.https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

[3] Cybersegurity Curricular (2017), Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS) , Association for Information Systems Special Interest Group on Information, Security and Privacy (AIS SIGSEC), International Federation for Information Processing Technical Committee on Information Security Education

[4] [Stallings, W. (2004). Fundamentos de Seguridad en la Red, Aplicaciones y Estándares. Pearson]

[5] Stuttard, D., & Pinto, M. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Wiley Publishing.

[6] Guía de ciberataques, España, Oficina de Seguridad del Internauta.

[7] K-oox seguridad informática. Sitio web. [Online]. Disponible: http://k-oox.blogspot.com/2016/05/ingenieriasocial-la-amenaza-invisible.html

[8] ESET. (sf). MANUAL DE INGENERIA SOCIAL: Cómo actuar correctamente.

[9] Fernández, M., & Andrés, J. (2021). Hackers: Técnicas y herramientas para atacar y defendernos. Ediciones de la U.

Capítulo 2:

Seguridad de la red y herramientas para evaluar la seguridad.

Introducción de capitulo

La seguridad de la red informática es de vital importancia debido a que las redes informáticas son cada vez más utilizadas en la actualidad para compartir información y recursos. Una red segura ayuda a proteger la información confidencial o no confidencial, a prevenir el acceso no autorizado a los recursos de la red, a reducir el riesgo de virus y malware, y asegurar la continuidad de los servicios.

La seguridad de la red informática implica la aplicación de medidas de seguridad adecuadas en diferentes niveles, como en los dispositivos de la red (routers, switches, firewalls, etc.), en los sistemas y aplicaciones que se ejecutan en la red, y en las políticas y procedimientos de seguridad que se implementan en la organización.

La seguridad de la red informática es esencial en cualquier organización, ya sea una pequeña empresa o una gran corporación, y es importante tener en cuenta que la seguridad es un proceso continuo y que debe ser revisado y actualizado regularmente para mantenerse al día con las amenazas y vulnerabilidades que puedan surgir.

2.1. ¿Qué es una red?

En la actualidad las redes de comunicaciones y los sistemas de información son un factor esencial del desarrollo económico y social. La informática y las redes son recursos indispensables.

Las redes de comunicación se definen como, "un conjunto de dispositivos interconectados que se utilizan para transmitir datos e información entre sí" [1]

La informática es manipular información de forma automática. Por un lado, las computadoras almacenan documentos, hojas de cálculo, imágenes, música, bases de datos con la información de usuarios, nóminas, pedidos, facturación, cuentas bancarias, y muchos otros datos de carácter público o privado. Por otra parte, las computadoras también se utilizan para transmitir información a través del correo electrónico, de la web, mensajería instantánea, y de muchas formas distintas. Entonces las computadoras crean, almacenan, manipulan, copian, comparten y transmiten información.

La red informática es un conjunto de dispositivos interconectados que utilizan un medio para intercambiar información y compartir recursos. En este proceso, los dispositivos conectados alternan dos roles: emisor y receptor, para entablar la comunicación. La estructura y el funcionamiento de las redes informáticas actuales se basan en varios estándares, entre los que destaca el modelo TPC/IP y el modelo teórico OSI.

El modelo TCP/IP (*Transmission Control Protocol/Internet Protocol, Protocolo de control de transmisión/Protocolo de Internet*) es el más utilizado y extenso de todos, y se basa en el modelo OSI *(Open Systems Interconnection, Interconexión de Sistemas Abiertos*). Este modelo define cómo se deben transmitir los datos a través de la red, establece la forma en que los dispositivos deben comunicarse y asegura la interoperabilidad entre diferentes dispositivos y sistemas. En resumen, el TCP/IP es un conjunto de protocolos que permite que los dispositivos de una red informática puedan comunicarse entre sí de manera efectiva y segura.

2.2 Modelo OSI

El modelo OSI es un marco teórico que se utiliza para describir cómo los datos se transmiten a través de una red de computadoras. Fue desarrollado por la Organización Internacional de Estándares (ISO) en 1984, y se convirtió en un estándar para las redes de computadoras.[2]

El modelo OSI describe cómo se comunican dos dispositivos a través de una red utilizando un conjunto de siete capas. Cada capa se encarga de una función específica y proporciona servicios a las capas superiores y utiliza servicios de las capas inferiores para enviar y recibir datos.

Las capas del modelo OSI se pueden describir brevemente de la siguiente manera:

1. Capa física: se encarga de la transmisión de datos a través del medio físico, como cables u ondas de radio.
2. Capa de enlace de datos: se encarga de dividir los datos en tramas para su transmisión y proporciona detección y corrección de errores.
3. Capa de red: se encarga de enrutar los paquetes de datos a través de la red y controlar el flujo de datos.
4. Capa de transporte: se encarga de la entrega de los datos de manera confiable y proporciona servicios de control de flujo y de congestión.
5. Capa de sesión: se encarga de establecer, mantener y finalizar las sesiones de comunicación entre dispositivos.
6. Capa de presentación: se encarga de la representación y el formato de los datos, como la codificación de caracteres y la compresión de datos.
7. Capa de aplicación: se encarga de proporcionar servicios de red a las aplicaciones y programas que se ejecutan en los dispositivos de la red.

El modelo OSI describe cómo se organizan y se relacionan las diferentes capas para permitir la comunicación efectiva entre dispositivos en una red de computadoras.

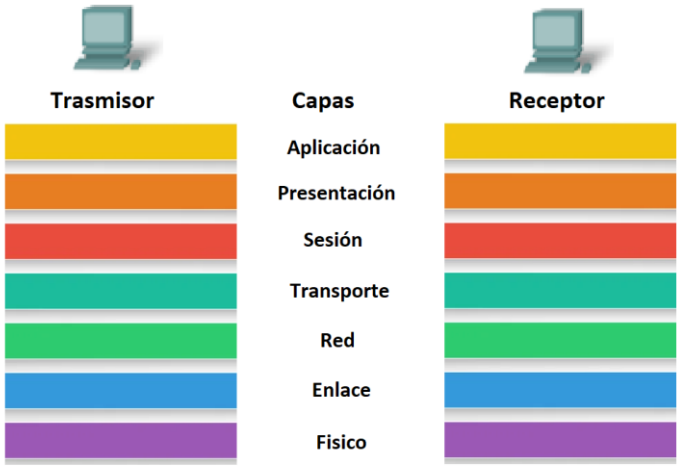


Figura 2.1: Modelo de capas OSI.

2.3 Modelo TPC/IP

Aunque el modelo OSI proporciona una estructura teórica sólida para el diseño y la implementación de redes, en la práctica se ha adoptado ampliamente el modelo TCP/IP debido a su simplicidad y su capacidad para adaptarse a diferentes tecnologías y entornos de red. El modelo de referencia TCP/IP, estableció por primera vez por Cerf y Kahn (1974); después se refinó y consideró como estándar en la comunidad de Internet (Braden, 1989). Clark (1988) describe la filosofía de diseño detrás de este modelo.[3]

El modelo TCP/IP es más fácil de mantener en comparación con el modelo OSI, que tiene una estructura más compleja y rígida. Además, el modelo TCP/IP se basa en una implementación más eficiente y escalable en comparación con el modelo OSI, lo que lo hace más adecuado para redes de gran tamaño y de alta velocidad.

Otra razón por la que se prefiere el modelo TCP/IP sobre el modelo OSI es que TCP/IP es la base de Internet y se ha convertido en el estándar en la mayoría de las redes, mientras que el modelo OSI nunca llegó a ser ampliamente adoptado en la industria de las redes.

2.4 Protocolos de red

Los protocolos de red son un conjunto de reglas y estándares que establecen la forma en que los dispositivos de una red se comunican y comparten información entre sí. Estas reglas y estándares establecen los formatos de los mensajes, los procedimientos de intercambio de información y las características técnicas de la comunicación. A continuación, se mencionan algunas de las reglas y estándares comunes utilizados en los protocolos de red: Estos protocolos permiten que los dispositivos puedan identificarse entre sí en la red, enviar y recibir datos de manera eficiente y asegurarse de que los datos lleguen sin errores o pérdidas.

Estos estándares son desarrollados y mantenidos por organizaciones como el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), la Organización Internacional de Normalización (ISO), la Internet Engineering Task Force (IETF) y el Instituto Nacional de Estándares y Tecnología (NIST).

- Estructura del mensaje: Los protocolos establecen la estructura y el formato de los mensajes que se intercambian entre los dispositivos. Esto incluye el orden y la forma en que se presentan los campos de información dentro de un mensaje, como las cabeceras, los datos y los campos de control.

- Codificación de datos: Los protocolos definen cómo se codifican los datos para su transmisión. Esto puede incluir técnicas de compresión para reducir el tamaño de los datos y técnicas de encriptación para proteger la confidencialidad de la información.

- Establecimiento y terminación de conexiones: Algunos protocolos requieren el establecimiento de una conexión antes de que se pueda realizar la comunicación. Estas reglas definen los procedimientos para establecer, mantener y terminar la conexión entre los dispositivos [4]

- Control de flujo: Los protocolos pueden incluir mecanismos de control de flujo para regular la velocidad de transmisión de datos y evitar la congestión en la red. Estas reglas permiten que el receptor informe al emisor sobre su capacidad de recepción, evitando la pérdida o la saturación de datos.

- Detección y corrección de errores: Los protocolos pueden incorporar técnicas para detectar y corregir errores en la transmisión de datos. Esto puede incluir el uso de bits de paridad, sumas de comprobación o algoritmos de detección y corrección de errores más complejos.

- Encaminamiento y enrutamiento: Algunos protocolos, como el Protocolo de Internet (IP), establecen reglas para el encaminamiento de los paquetes de datos a través de la red. Estas reglas determinan cómo se selecciona la ruta óptima y cómo se entregan los paquetes de un nodo a otro.

- Seguridad: Los protocolos pueden incluir mecanismos para proteger la integridad, la autenticidad y la confidencialidad de los datos. Estos mecanismos pueden incluir autenticación, encriptación y firmas digitales, entre otros.

Hay una gran variedad de protocolos de red, cada uno diseñado para realizar funciones específicas dentro de una red. Algunos ejemplos comunes de protocolos de red son el

Protocolo de Internet (IP), el Protocolo de Control de Transmisión (TCP), el Protocolo de Usuario de Datagrama (UDP), el Protocolo de Transferencia de Archivos (FTP), el Protocolo Simple de Correo (SMTP), entre otros. Cada uno de estos protocolos se utiliza para proporcionar servicios diferentes y se combinan para permitir la comunicación entre diferentes dispositivos y aplicaciones en una red.

A continuación, se hablará de algunos como FTP, MySQL y Telnet ya que en una red permite comprender la seguridad y la eficiencia de las transferencias de archivos, las consultas de bases de datos y la administración remota de sistemas. Esto ayuda a detectar posibles problemas, mejorar el rendimiento y garantizar la seguridad en la red.

2.4.1 FTP

FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos) es un servicio confiable orientado a conexión que utiliza TCP para transferir archivos entre sistemas que admiten FTP. El propósito principal de FTP es transferir archivos desde una computadora hacia otra copiando y moviendo archivos desde los servidores hacia los clientes, y desde los clientes hacia los servidores. Cuando los archivos se copian de un servidor, FTP primero establece una conexión de control entre el cliente y el servidor. [5]

Este es un protocolo estándar utilizado para la transferencia de archivos entre dispositivos en una red. Fue desarrollado originalmente en los años 70 y ha sido ampliamente utilizado desde entonces.

Cuando se establece una conexión FTP, el cliente se conecta al servidor a través del puerto 21 (puerto de control) y se autentifica proporcionando un nombre de usuario y una contraseña. Una vez que se establece la conexión, el cliente puede enviar comandos al servidor, así como listar el contenido de un directorio o descargar un archivo. Para descargar un archivo el servidor responde abriendo una conexión de datos en un puerto separado (mediante el puerto 20) y enviando el archivo solicitado a través de esta conexión. Una vez que se completa la transferencia de archivos, se cierra la conexión de datos y se devuelve el control al canal de control.

El protocolo FTP transfiere datos, incluyendo nombres de usuario y contraseñas, en texto sin cifrar. Esto significa que cualquier persona que tenga acceso a la red puede interceptar y leer fácilmente la información transmitida a través de FTP. Además, el FTP no proporciona mecanismos de autenticación robustos, lo que hace vulnerable la verificación de la identidad de los usuarios. [6]

Aunque FTP sigue siendo ampliamente utilizado, su uso ha disminuido en los últimos años debido a problemas de seguridad y a la aparición de alternativas más seguras y eficientes, como SFTP y FTPS.

2.4.2. MySQL

MySQL es un sistema de gestión de bases de datos relacional que utiliza un protocolo propio llamado Protocolo de Comunicación de MySQL (MySQL Communication Protocol). Este protocolo es utilizado por los clientes para conectarse a un servidor MySQL y realizar operaciones de bases de datos, como consultas, inserciones, actualizaciones y borrado de datos.

El protocolo de MySQL se basa en el modelo cliente-servidor, donde el servidor MySQL es el encargado de administrar y almacenar los datos de la base de datos, mientras que los clientes se conectan al servidor para realizar las operaciones en la base de datos. El protocolo permite que los clientes se autentiquen y se comuniquen de manera segura con el servidor, utilizando un conjunto de comandos y respuestas definidos en el protocolo.

2.4.3 Telnet

Telnet es un protocolo de red utilizado para acceder a servidores, dispositivos de red y otros equipos remotamente. El protocolo Telnet utiliza el puerto 23 para establecer una conexión entre el cliente y el servidor.

Telnet permite a un usuario conectarse a un servidor remoto y operar en él como si estuviera sentado frente a él. Una vez que se establece la conexión, el usuario puede enviar comandos y recibir respuestas a través de la red.

El protocolo Telnet no proporciona ningún tipo de seguridad, ya que toda la información, incluyendo las contraseñas y los comandos, se envían en texto plano, lo que significa que cualquier persona que tenga acceso a la red puede leer la información. Por esta razón, Telnet ya no se utiliza ampliamente y se ha reemplazado por protocolos más seguros como SSH (Secure Shell).

Es importante destacar que, si bien MySQL proporciona características de seguridad, su implementación adecuada y la configuración correcta son responsabilidad del administrador de la base de datos. Además, es recomendable mantenerse actualizado con las versiones y actualizaciones más recientes de MySQL, ya que estas suelen incluir mejoras de seguridad. [7]

2.5 Seguridad en las redes

El crecimiento de la informática y de las redes de comunicaciones, ha hecho que el número de incidentes de seguridad aumente y se incrementen contantemente. En este contexto el riesgo de pérdida, alteración o revelación de información aumenta a medida que se transmite y se procesa más información, porque a medida que la cantidad de información se incrementa, también lo hace la cantidad de puntos vulnerables en los que se puede producir un fallo de seguridad. Además, cuanta más información se transmite, mayor es la probabilidad de que alguien intente interceptar o acceder de manera no autorizada a la información, especialmente si se trata de información valiosa o sensible.

La seguridad de la información se basa en proteger a los sistemas informáticos frente a distintas amenazas que existen como ataques de *malware*, virus, troyanos, *spyware, hacking, phishing*, ataques de fuerza bruta, etc. Por lo cual, la aplicación de medidas de seguridad debe ser planeada y selectiva, para así dirigir esfuerzos donde solo hace falta o no destinar grandes recursos donde no hace falta. Para que estas medidas y mecanismos de protección sean eficientes, deben estar dentro de un sistema de gestión de la seguridad de la información.es decir debe existir un plan de acción que guíe los recursos de protección de los activos, estos elementos o recursos valiosos para la organización que requieren protección adecuada para garantizar la seguridad y continuidad de la organización.

La seguridad de las redes de comunicación y de los sistemas de información, y en particular su disponibilidad, es un asunto que toma mayor relevancia para la sociedad. Debido a que las vulnerabilidades en las redes y los sistemas pueden resultar en el robo de información confidencial, la interrupción de servicios críticos, el compromiso de la privacidad y la pérdida de la confianza de los usuarios. [8]

En una red, además de la seguridad lógica también se debe tomar en cuenta la seguridad física, lo cual restringe el acceso a ciertos sectores de la infraestructura. La seguridad en la red tiene como fin proteger la disponibilidad de la información y la confidencialidad, y proveer un mantenimiento continuo, que tiene como finalidad asegurar la comunicación.

Por lo tanto, la seguridad de los datos compartidos es un aspecto relevante, ya que la información se encuentra disponible en terminales e instalaciones específicas y es necesaria la implementación de medidas de seguridad que se deben considerar para evitar el acceso no permitido.

2.5.1. Cualidades de la seguridad de la información

La seguridad de la información puede ser comprometida y las tres características según el autor Pablo Gutiérrez en El libro blanco del hacker, para que se considere segura son :[5]

1. **Confidencialidad**: significa que solo la persona que tiene permiso de ver la información pueda verla.
2. **Integridad**: implica que solo debe de ser accedida o modificada por la persona con el permiso.
3. **Disponibilidad:** aspecto que considera que la información tenga la capacidad de acceder y utilizar la información cuando sea necesario, y es esencial para garantizar la continuidad del negocio y la productividad de la organización.

Esto conforma la triada de la seguridad, mostrada en la figura 2.2:

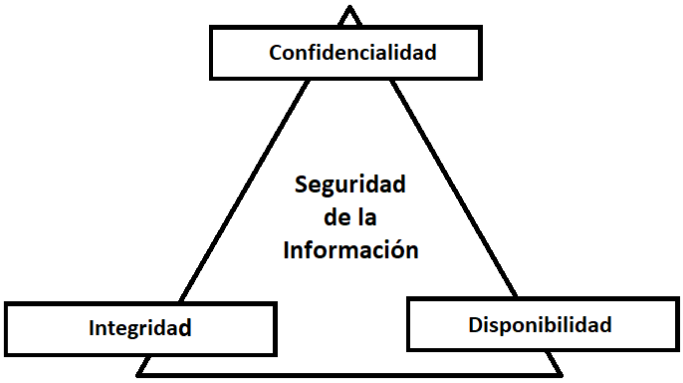


Figura 2.2: Triángulo de la seguridad informática.

2.5.2 Plan de seguridad en una red.

Un plan de seguridad es un documento estratégico que establece las políticas, procedimientos y controles necesarios para proteger los activos de información y garantizar la seguridad de una organización. Es una guía integral que aborda las medidas y acciones que se deben implementar para prevenir, detectar y responder a las amenazas y riesgos de seguridad.

COBIT (*Control Objectives for Information and Related Technologies, Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas*) proporciona reglas/instrucción para el gobierno y la gestión de la tecnología de la información en las organizaciones. Aunque COBIT no aborda directamente el plan de seguridad como un componente específico, incluye aspectos relacionados con la seguridad de la información y puede ayudar en su desarrollo.

En COBIT, el dominio "Asegurar, adquirir e implementar" y el dominio " entregar, dar soporte y monitorear" abordan los controles de seguridad de la información y ofrecen directrices sobre la planificación, implementación y monitoreo de la seguridad. Estos dominios se centran en aspectos como la gestión de riesgos, el diseño de controles, la gestión de accesos y la continuidad del negocio, que son fundamentales para un plan de seguridad sólido.[10]

Para implementar un plan de seguridad se deben considerar los siguientes aspectos:

- **Análisis de riesgos;** Se evalúan los recursos clave para el funcionamiento de la red, en el caso de que surja un incidente y el tiempo requerido para una rápida resolución.
- **Medidas preventivas;** Las personas tienen acceso a los servidores ya sea física o remotamente. Mediante estos filtros se establece que los usuarios puedan realizar determinadas acciones, por ejemplo: instalar software y acceder a los puertos de periféricos disponibles, realizar la actualización de antivirus o *service packs* del SO (Sistema Operativo).
- **Prevención ante accidentes de índole natural;** Tiene como fin establecer acciones que se deben realizar cuando se presente una catástrofe como una inundación o incendio.
- **Plan de respaldo;** Consiste en la evaluación de la situación al verse afectado un servicio para seguir trabajando. Por ejemplo, en el caso de que sean afectados uno o varios equipos en la red, la posibilidad de remplazarlos en un tiempo mínimo; en el caso en el que se pueda comprometer un servidor en el que se almacenan los datos del cliente, se deberá determinar el tiempo en que queda sin funcionamiento y realizar las tareas necesarias para poner en funcionamiento e implementar las soluciones tales como un servidor alternativo de *backup* (copia de los datos y archivos importantes en un sistema informático).

2.5.3 Seguridad física en una red.

La seguridad física en una red se refiere a la protección de los dispositivos y componentes que conforman la red, con el fin de evitar accesos no autorizados, daños y robos. Es importante implementar medidas de control de acceso, proteger los dispositivos de red, el cableado y tener planes de contingencia para situaciones de emergencia.

Es decir, cómo se menciona en el libre Physical Security Threats in Data Centers de los autores Al-Shehri, S., Khan, M. K., Al-Wabil, A., y Al-Dossari, H.:

“La seguridad física de una red se refiere a las medidas y controles implementados para proteger los recursos físicos que componen la infraestructura de red de una organización. Esto

incluye la protección de los equipos, dispositivos de red, servidores, centros de datos, cableado y otros elementos físicos necesarios para el funcionamiento de la red.

La seguridad física de una red abarca una serie de aspectos, como el acceso físico restringido a las instalaciones de red, la protección contra robos, daños físicos o vandalismo, la implementación de sistemas de detección y prevención de incendios, y la gestión adecuada del cableado y la infraestructura física para evitar fallas y daños.” [11]

Los controles y medidas de seguridad física pueden incluir:

- Control de acceso; Utilización de cerraduras, tarjetas de acceso, sistemas biométricos u otros métodos de autenticación para restringir el acceso a áreas críticas de la red.
- Vigilancia y monitoreo; Implementación de sistemas de videovigilancia, alarmas y sistemas de detección de intrusos para supervisar y registrar la actividad en las instalaciones de red.
- Protección contra incendios y desastres; Implementación de sistemas y protocolos para prevenir y mitigar incendios, inundaciones y otros desastres naturales que puedan dañar la infraestructura física de la red.
- Respaldo de energía; Uso de fuentes de alimentación ininterrumpida (UPS) y generadores de respaldo para garantizar la continuidad del suministro de energía y proteger contra interrupciones no planificadas.
- Gestión del cableado: Mantenimiento y organización adecuada del cableado para evitar interferencias, daños y problemas de seguridad.
- IDS; en el caso de que se realice la detección de un intruso, se debe notificar de inmediato al administrador de red. El IDS cumple muchas funciones de forma automática, entre las cuales cambiar configuración de firewall o bloquear algún acceso.
- Cableado; el cableado de una red se establece que debe ir por un lugar seguro, un techo falso, un sitio que no sea de muy fácil acceso, y lejos de las fuentes de interferencia. El cableado de la red debe ser protegido y etiquetado adecuadamente para que en caso de que exista un mal funcionamiento o un daño físico se pueda facilitar su identificación.

Estas medidas de seguridad física son fundamentales para proteger la integridad, la confidencialidad y la disponibilidad de los activos físicos de una red y garantizar su funcionamiento seguro y confiable.

2.5.4 Seguridad lógica en una red.

La seguridad lógica en una red se refiere a la protección de la información y los datos que se transmiten a través de la red, y la protección de los sistemas informáticos contra accesos no autorizados, uso indebido y manipulación malintencionada. La seguridad lógica es un aspecto fundamental de la seguridad de la red, ya que se enfoca en proteger la información y los datos que se transmiten a través de la red.

Los autores Fernández, D., & Bernal, D. mencionan que: “La seguridad lógica en una red se refiere a las medidas y controles implementados para proteger los recursos y datos de una red a nivel lógico, utilizando mecanismos de software y configuraciones. Estas medidas se centran en proteger la información, autenticar usuarios, gestionar el acceso, controlar los privilegios y detectar y prevenir intrusiones.” [12]

Algunos aspectos importantes de la seguridad lógica en una red incluyen:

- Autenticación y control de acceso. Implementación de mecanismos de autenticación, como contraseñas, tokens o sistemas biométricos, para verificar la identidad de los usuarios y controlar su acceso a los recursos de la red.
- Gestión de privilegios. Asignación de permisos y privilegios adecuados a los usuarios, limitando el acceso solo a las funciones y datos necesarios para realizar sus tareas, y evitando privilegios excesivos que puedan comprometer la seguridad.
- Encriptación de datos. Uso de algoritmos de encriptación para proteger la confidencialidad e integridad de los datos mientras se transmiten a través de la red, asegurando que solo los destinatarios autorizados puedan acceder a ellos.
- Detección y prevención de intrusiones. Implementación de sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) para monitorear el tráfico de red en busca de comportamientos maliciosos y tomar medidas para prevenir o detener ataques.
- Actualizaciones y parches. Mantenimiento regular del software y los sistemas de la red, aplicando actualizaciones y parches de seguridad para corregir vulnerabilidades conocidas y garantizar la protección contra amenazas conocidas.
- El factor humano. Se considera en las medidas de seguridad lógica en una red porque las personas son un componente clave en la protección de los sistemas informáticos. Aunque las medidas de seguridad técnicas, como los firewalls y los sistemas de detección de intrusos, pueden proporcionar una barrera efectiva contra las amenazas cibernéticas, no son infalibles y pueden ser vulnerables a las tácticas de ingeniería social utilizadas por los atacantes.

Las medidas de seguridad lógica también deben incluir la educación y capacitación de los usuarios para que puedan reconocer y evitar posibles amenazas. Los usuarios pueden ser capacitados en la creación y uso de contraseñas seguras, la identificación de correos electrónicos maliciosos, la protección de información confidencial y la utilización de aplicaciones y herramientas de seguridad. Además, es importante establecer políticas de seguridad claras y hacer cumplir las mismas para garantizar que todos los usuarios de la red cumplan con los estándares de seguridad establecidos.

2.5.5 Política de seguridad basada en reglas

Las políticas de utilizan en la seguridad informática son un conjunto de reglas y directrices que establecen las medidas de seguridad que deben seguirse en una organización para proteger su información y sistemas de posibles amenazas y riesgos de seguridad. Estas políticas establecen un marco de referencia que define los objetivos y estrategias para proteger la información, los recursos y los activos de la organización.

Las políticas en la seguridad informática pueden cubrir diferentes áreas, como la gestión de contraseñas, la autenticación y control de acceso, la gestión de parches y actualizaciones de software, la gestión de incidentes de seguridad, la seguridad en las comunicaciones y la gestión de riesgos.

Las políticas de seguridad pueden ser de carácter obligatorio y aplicarse a todos los empleados de la organización, incluyendo la alta dirección, y deben ser actualizadas y revisadas periódicamente para adaptarse a los cambios en el entorno de seguridad y amenazas que puedan surgir.

La política de seguridad basada en reglas globales impuestas a todos los usuarios, suelen depender de una comparación de la sensibilidad de los recursos a los que se accede con los atributos correspondientes de los usuarios, de un grupo de usuarios o de entidades que actúan en nombre de los usuarios. [9]

2.5.6 Mecanismos de control de acceso

Los mecanismos de control de acceso son los que se utilizan para aplicar una política de limitación del acceso a un recurso a los usuarios autorizados. Estas técnicas comprenden la implementación de listas o de matrices de control de acceso (que por lo general contienen las identidades de los hosts controlados y de los usuarios autorizados); estas técnicas utilizan también contraseñas y capacidades, etiquetas o testigos, cuya posesión puede emplearse para indicar derechos de acceso. [9]

Algunos de los mecanismos de control de acceso más comunes incluyen:

- Autenticación; proceso de verificación de la identidad del usuario a través de credenciales, como contraseñas, *tokens* (es un objeto físico o una pieza de software que se utiliza para autentificar la identidad de un usuario y proporcionar acceso a recursos protegidos, como sistemas informáticos, redes o aplicaciones) o biometría.
- Autorización; proceso que determina si un usuario tiene permiso para acceder a determinados recursos o realizar determinadas acciones.
- Control de acceso basado en roles (**RBAC**, *role-based access control*); técnica que permite la asignación de permisos y roles a los usuarios de acuerdo con su función en la organización.
- Mecanismo de control de Acceso (**MAC,** *Media Access Control*); técnica que se utiliza para restringir el acceso a los recursos basándose en políticas de seguridad predefinidas.
- Control de acceso discrecional (**DAC**, *discretionary access control*); técnica que permite que el propietario de los recursos decida quién tiene acceso a ellos y cómo.
- Control de acceso condicional (**CAC**, *Conditional Access Control*); técnica que permite la aplicación de políticas de seguridad en función de diferentes factores, como la hora del día o la ubicación física.

En general, los mecanismos de control de acceso son esenciales para garantizar la seguridad de la información y los recursos en una organización, y deben ser diseñados y aplicados adecuadamente para minimizar los riesgos de seguridad.

2.5.6 Auditoría de seguridad

Una auditoría de seguridad es un proceso de evaluación sistemática; los sistemas, redes y aplicaciones informáticas de una organización para determinar si cumplen con los estándares de seguridad y si están protegidos adecuadamente contra posibles amenazas y vulnerabilidades. El objetivo principal de una auditoría de seguridad es identificar y evaluar los riesgos de seguridad, y recomendar soluciones para mitigarlos.

“Una auditoría puede ser realizada por auditores internos dentro de la organización o por auditores externos independientes contratados para llevar a cabo la evaluación. El objetivo final de una auditoría es proporcionar una visión clara y objetiva de la situación actual de la organización o sistema auditado, identificar áreas de mejora y garantizar el cumplimiento de los requisitos de seguridad y cumplimiento establecidos.” [13]

Durante una auditoría de seguridad, se llevan a cabo diversas actividades, como la revisión de políticas y procedimientos de seguridad, el análisis de la infraestructura de seguridad, la evaluación de los controles de acceso y autenticación, la prueba de vulnerabilidades y la verificación del cumplimiento de los requisitos legales y reglamentarios.

En el libro "The Project Management Tool Kit" escrito por Tom Kendrick se mencionan las actividades comunes realizadas durante una auditoría: [14]

1. Planificación. Se establece el alcance, los objetivos y los criterios de auditoría. Se identifican los recursos necesarios, se elabora un plan de auditoría y se establece el cronograma de actividades.
2. Recopilación de información. Se recopila información relevante sobre el sistema o proceso a auditar, como políticas, procedimientos, manuales, registros, documentación técnica y normativa aplicable.
3. Entrevistas. Se llevan a cabo entrevistas con el personal clave de la organización para obtener información sobre el funcionamiento del sistema, los controles implementados y los procesos relacionados.
4. Revisión de documentación. Se analiza y revisa la documentación relacionada con el sistema auditado, como políticas, planes, manuales, registros y reportes de incidentes.
5. Evaluación de controles. Se examinan los controles de seguridad implementados en el sistema, se verifica su efectividad y se evalúa su cumplimiento con los requisitos establecidos.
6. Pruebas de cumplimiento. Se realizan pruebas y análisis de evidencia para verificar si se cumple con los requisitos establecidos, como normas, regulaciones y políticas internas.
7. Análisis de riesgos. Se evalúan los riesgos asociados al sistema o proceso auditado, identificando posibles amenazas, vulnerabilidades y brechas de seguridad.
8. Hallazgos y recomendaciones: Se documentan los hallazgos de la auditoría, se identifican las áreas de mejora y se formulan recomendaciones para fortalecer los controles y el cumplimiento de los requisitos.
9. Informe de auditoría. Se elabora un informe que resume los resultados de la auditoría, incluyendo los hallazgos, las recomendaciones y las acciones correctivas propuestas.
10. Seguimiento y cierre. Se realiza un seguimiento de las acciones correctivas implementadas en respuesta a los hallazgos de la auditoría, verificando su efectividad y cierre adecuado.

Los resultados de una auditoría de seguridad se presentan en un informe detallado que incluye una descripción de los hallazgos, las recomendaciones para mejorar la seguridad y la evaluación de los riesgos. El informe también puede incluir un plan de acción para implementar las recomendaciones y mejorar la seguridad de la organización.

Revisión y examen independientes de los registros y actividades del sistema para verificar la calidad de los controles del sistema, hay que asegurar que se cumplan la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos. [9]

2.5.7 Confidencialidad del flujo de tráfico

El análisis de tráfico se refiere al proceso de examinar y evaluar los datos de tráfico en una red de comunicaciones. Consiste en recopilar, inspeccionar y analizar los paquetes de datos que se transmiten a través de la red con el fin de obtener información y conocimientos sobre el tráfico de red.[15]

El análisis de tráfico puede llevarse a cabo con diversas herramientas y técnicas, que incluyen:

- Captura de paquetes. Consiste en utilizar software especializado para capturar y registrar los paquetes de datos que se transmiten en la red. Esto permite obtener una visibilidad completa del tráfico de red y analizar los paquetes en detalle.
- Filtrado y clasificación. Una vez capturados los paquetes, es posible filtrar y clasificar el tráfico según diferentes criterios, como direcciones IP, puertos, protocolos o tipos de paquetes. Esto facilita el análisis específico del tráfico que se desea examinar.
- Análisis de protocolos. Se examinan los protocolos utilizados en la red, como TCP/IP, DNS, HTTP, entre otros, para comprender cómo se comunican los dispositivos y las aplicaciones. Esto ayuda a identificar posibles problemas de rendimiento, anomalías o ataques en la red.
- Identificación de patrones. Mediante técnicas de análisis de tráfico, es posible identificar patrones de comportamiento, tendencias y anomalías en el tráfico de red. Esto puede revelar información valiosa sobre la utilización de la red, los flujos de datos y posibles eventos de seguridad.
- Detección de amenazas y problemas de rendimiento. El análisis de tráfico puede ayudar a identificar actividades maliciosas, como ataques de red, malware o comportamientos anómalos. También permite detectar problemas de rendimiento, como congestiones, cuellos de botella o latencia excesiva.

El análisis de tráfico es una práctica fundamental en la ciberseguridad y la gestión de redes. Proporciona información valiosa para optimizar el rendimiento de la red, detectar y responder a amenazas, y tomar decisiones informadas sobre la configuración y la seguridad de la infraestructura de red.[15]

La confidencialidad del flujo de tráfico se refiere a la capacidad de proteger la información que se transmite a través de una red, de manera que sólo las personas autorizadas puedan acceder a ella. Esto significa que la información que se transmite no puede ser vista o accedida por terceros no autorizados.

Para garantizar la confidencialidad del flujo de tráfico, se utilizan diferentes técnicas y herramientas de seguridad. Entre ellas se encuentran:

- Cifrado de datos: consiste en transformar los datos que se transmiten en un código ilegible para las personas no autorizadas. Esto se logra mediante el uso de algoritmos criptográficos y claves de cifrado.
- VPN (Virtual Private Network): es una red privada virtual que se establece sobre una red pública, como Internet. Las VPN permiten que las comunicaciones se realicen de forma segura y cifrada entre dos puntos de la red.
- Firewall: es un dispositivo de seguridad que se utiliza para controlar el tráfico de red y filtrar el tráfico no deseado.
- Control de acceso: se utilizan técnicas como la autenticación, la autorización y la auditoría para controlar el acceso a los datos y la información que se transmiten por la red.

La confidencialidad del flujo de tráfico es esencial para garantizar la privacidad y seguridad de la información que se transmite por la red. Sin ella, la información estaría expuesta a posibles ataques y vulnerabilidades que podrían poner en riesgo la integridad y disponibilidad de los datos.

2.6 Normas y estándares para la seguridad de la información

Se utilizan normas y estándares para la seguridad de la información porque proporcionan un marco común y reconocido internacionalmente para la gestión de la seguridad de la información en una organización. Estas normas y estándares ayudan a las organizaciones a asegurar que la información sea manejada de manera adecuada, confidencial y segura, y que se cumpla con las regulaciones y leyes aplicables.

Además, seguir estas normas y estándares permite a las organizaciones demostrar su compromiso con la seguridad de la información a los clientes, socios comerciales, reguladores y otras partes interesadas. Al seguir estas normas y estándares, se pueden minimizar los riesgos de seguridad, proteger la información valiosa y garantizar la continuidad operativa de instituciones y organizaciones.

2.6.1 Norma X.800

La norma X.800, también conocida como ISO/IEC 7498-2, es un estándar internacional de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) que proporciona un marco para la seguridad de la información en redes de computadora

“La norma X.800 se centra en la seguridad de los sistemas de información abiertos, es decir, aquellos sistemas que están conectados a redes y que interactúan con otros sistemas externos. Su objetivo principal es establecer una arquitectura de seguridad sólida que proteja la confidencialidad, integridad y disponibilidad de la información en estos entornos.” [16]

La norma X.800 se divide en cuatro partes principales:

Parte 1. Introducción y descripción general; en esta parte se presenta una visión general de la norma, se define la seguridad de la información y se describen los conceptos y principios fundamentales.

Parte 2. Arquitectura de seguridad para sistemas de comunicación abiertos; esta parte describe la arquitectura de seguridad de OSI que consta de siete capas y proporciona una estructura para la seguridad de la información en redes de computadoras.

Parte 3. Mecanismos de seguridad; en esta parte se describen los mecanismos de seguridad necesarios para implementar la arquitectura de seguridad de OSI, incluyendo la autenticación, la confidencialidad, la integridad, el control de acceso y la de no repudio.

Parte 4. Gestión de seguridad; esta parte describe los procesos y procedimientos necesarios para la gestión de la seguridad de la información en redes de computadoras, incluyendo la gestión de claves, políticas de seguridad, incidentes de seguridad y en sí de la seguridad en la red.

“La recomendación X.800 de la ITU (Unión Internacional de Telecomunicaciones) implementa la arquitectura de seguridad OSI, define este enfoque sistemático. La arquitectura de seguridad OSI es útil a los administradores de red para organizar la tarea de proporcionar seguridad. Además, debido a que esta arquitectura fue desarrollada como un estándar

internacional, los vendedores han desarrollado características de seguridad para sus productos y servicios conforme a esta definición estructurada de servicios y mecanismos.” [17]

2.6.2 ISO 27000 e ISO 27001

La ISO 27000 es una serie de estándares internacionales que se refieren a la gestión de la seguridad de la información. Esta serie de estándares fue desarrollada por la ISO y IEC para proporcionar un marco de buenas prácticas para la gestión de la seguridad de la información.

La serie ISO 27000 incluye diferentes estándares que abordan diferentes aspectos de la seguridad de la información, como la gestión de riesgos, la implementación de controles de seguridad, la continuidad del negocio y la gestión de incidentes de seguridad.

La implementación de la serie ISO 27000 ayuda a las organizaciones a proteger la privacidad, integridad y disponibilidad de la información de su negocio, así como a cumplir con los requisitos legales y regulatorios relacionados con la seguridad de la información.

Esta norma se enfoca en la gestión de riesgos de seguridad de la información, incluyendo la identificación, evaluación y tratamiento de los riesgos. Además, también establece un conjunto de controles de seguridad de la información que pueden ser implementados para proteger la información de la organización. [18]

La norma ISO 27001 es la norma central de la serie y establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Esta norma proporciona un marco para que las organizaciones desarrollen, implementen, mantengan y mejoren continuamente un SGSI efectivo.

2.7 Herramientas para evaluar seguridad.

Las herramientas de *pentesting* o prueba de penetración son aplicaciones informáticas utilizadas por los profesionales de seguridad informática para detectar y explotar vulnerabilidades en sistemas, redes y aplicaciones con el fin de mejorar la seguridad y evitar ataques maliciosos. Es importante recordar que estas herramientas deben ser utilizadas con ética y responsabilidad, y solo en sistemas y redes donde se tenga autorización explícita para realizar pruebas de seguridad.

2.7.1 Kali Linux

Kali Linux (anteriormente conocido como BackTrack Linux) es una distribución basada en Debian el cual es un sistema operativo libre y de código abierto con base en Linux, que se utiliza principalmente en servidores y estaciones de trabajo. Es una de las distribuciones más

populares y se caracteriza por su estabilidad, seguridad y por estar enfocado en la filosofía del software libre.

Kali Linux contiene modificaciones específicas de la industria, así como varios cientos de herramientas dirigidas a diversas tareas de seguridad de la información, como:

- Pruebas de penetración; las pruebas de penetración son un conjunto de técnicas y métodos utilizados para evaluar la seguridad de un sistema informático o de una red. El objetivo principal de una prueba de penetración es identificar posibles vulnerabilidades en el sistema que podrían ser explotadas por un atacante externo o interno.

  Durante una prueba de penetración, un equipo de profesionales en seguridad informática simula o intenta la simulación de un ataque real para descubrir debilidades en el sistema.
- Informática forense; también conocida como informática forense digital o ciberforense, es una disciplina que se enfoca en la recuperación, preservación, análisis y presentación de pruebas digitales en investigaciones legales y criminales.

  Se utiliza para investigar y analizar delitos informáticos, como la piratería informática, el robo de información, el fraude electrónico, el acoso cibernético, entre otros. Los especialistas en informática forense utilizan técnicas y herramientas para analizar discos duros, servidores, redes y otros dispositivos electrónicos en busca de información que pueda ser utilizada como evidencia en una investigación legal.
- Ingeniería inversa; es una técnica utilizada en seguridad informática para analizar y entender el funcionamiento interno de un software o sistema, descomponiendo sus componentes y estructuras para obtener información valiosa sobre su diseño, algoritmos y lógica. Es decir, se trata de tomar algo que ya está creado y desmontarlo para entender cómo funciona.

  La ingeniería inversa se utiliza tanto con fines legítimos como ilegales. En el ámbito de la seguridad informática, se utiliza para analizar y descubrir vulnerabilidades en software o sistemas, lo que permite a los expertos en seguridad diseñar contramedidas para evitar posibles ataques.
- Pruebas de *Red Team*; las pruebas de *Red Team* son un tipo de prueba de seguridad que simula un ataque realista en el que un equipo de profesionales en seguridad (el equipo de *Red Team*) intenta comprometer el sistema de una organización (el equipo *Blue Team*). El objetivo de estas pruebas es evaluar la capacidad de la organización para detectar, responder y mitigar un ataque realista.

El equipo de *Red Team* utiliza técnicas y herramientas de hacking para intentar infiltrarse en los sistemas de la organización, y una vez dentro, intenta mantener el acceso no detectado el mayor tiempo posible, mientras recopila información valiosa. Mientras tanto, el equipo *Blue Team* debe detectar la actividad del equipo de *Red Team* y responder a la amenaza de manera efectiva.

2.7.2 Nmap

Nmap (Network Mapper) es una herramienta de exploración de redes y escaneo de puertos de código abierto y gratuita, utilizada por profesionales de seguridad y administradores de sistemas para descubrir dispositivos en una red y determinar los servicios y puertos que están abiertos en esos dispositivos. Con Nmap, se pueden encontrar vulnerabilidades en la red y se pueden tomar medidas preventivas para proteger los sistemas contra ataques maliciosos. La herramienta también tiene capacidades avanzadas como la detección de sistemas operativos y la identificación de servicios y aplicaciones en ejecución en los dispositivos. Nmap se ejecuta en sistemas operativos como Windows, Linux, Mac OS X, FreeBSD, OpenBSD, Solaris y otros.

Entre las funciones de Nmap se incluyen:

- Escaneo de puertos TCP; Nmap envía paquetes TCP a los puertos de destino y analiza las respuestas para determinar si los puertos están abiertos, cerrados o filtrados por un firewall.
- Escaneo de puertos UDP; Similar al escaneo de puertos TCP, pero utiliza paquetes UDP para buscar servicios que podrían estar ejecutándose en puertos UDP.
- Detección de sistemas operativos (OS); Nmap envía una serie de paquetes al host de destino y analiza las respuestas para intentar identificar el sistema operativo que se está ejecutando en ese host.
- Detección de servicios; Nmap envía paquetes específicos a los puertos abiertos y analiza las respuestas para determinar qué servicios están disponibles en esos puertos.
- Escaneo de scripts; Nmap permite ejecutar scripts personalizados para realizar tareas adicionales, como la detección de vulnerabilidades o la recopilación de información adicional sobre los hosts objetivo.

En cuanto a los paquetes que Nmap envía, utiliza paquetes de bajo nivel para interactuar directamente con los protocolos de red, como TCP, UDP, ICMP y otros. Los paquetes enviados por Nmap pueden variar según la técnica de escaneo utilizada, pero generalmente incluyen

paquetes de solicitud y paquetes de respuesta para determinar el estado de los puertos y servicios en los hosts objetivo.[19]

2.7.3 Wireshark

Wireshark es una herramienta de análisis de paquetes de red. Es un software de código abierto que está disponible para su descarga y uso de forma gratuita en varios sistemas operativos, incluyendo Windows, Linux y macOS. Se utiliza para capturar, analizar y solucionar problemas en redes de computadoras. Permite a los usuarios capturar y ver el tráfico de red en tiempo real y también analizar el tráfico capturado para identificar problemas de red, errores de protocolo y posibles ataques de seguridad.

Wireshark se utiliza en la resolución de problemas de red, auditorías de seguridad, análisis de tráfico de red y muchas otras tareas relacionadas con la seguridad y el rendimiento de la red. Al capturar y analizar el tráfico de red, los usuarios pueden ver la información que se envía y recibe en una red, incluyendo detalles de los paquetes y los protocolos que se utilizan.

Entre las características de Wireshark se encuentran la capacidad de filtrar el tráfico capturado para examinar sólo los paquetes de interés, la visualización de los paquetes en diferentes formatos, la generación de informes y estadísticas y la capacidad de comparar diferentes capturas de tráfico para analizar los cambios y mejoras en la red. Como herramienta de análisis de tráfico de red de código abierto y ampliamente utilizada. Permite capturar y examinar paquetes de datos en una red con el fin de comprender y solucionar problemas relacionados con la red, la seguridad y el rendimiento. Wireshark es compatible con una amplia gama de protocolos de red y ofrece una interfaz gráfica de usuario intuitiva para analizar los paquetes capturados.

La captura los paquetes de datos que pasan a través de una interfaz de red seleccionada. Esto se logra utilizando libpcap o Npcap (bibliotecas y controladores de captura de paquetes de red dependiendo del sistema operativo), que son bibliotecas de captura de paquetes de bajo nivel. Una vez que los paquetes son capturados, Wireshark proporciona una interfaz gráfica de usuario donde los usuarios pueden analizar y filtrar los paquetes según sus necesidades.

Wireshark permite la aplicación de diversos filtros para examinar paquetes específicos, como filtros de dirección IP, puertos, protocolos y otros criterios. También ofrece la capacidad de realizar análisis avanzados, como seguimiento de flujo, estadísticas de protocolo y decodificación de protocolos específicos para obtener información detallada sobre el tráfico de red.

Aquí hay algunas razones por las que se necesita Wireshark:

- Solución de problemas de red. Wireshark permite analizar el tráfico de red para identificar problemas de rendimiento, errores de configuración, conflictos de protocolos y otros problemas relacionados con la conectividad de la red.
- Monitoreo de seguridad. Wireshark puede ayudar a detectar y analizar actividades sospechosas o maliciosas en una red, como ataques de intrusión, malware, fugas de información y comportamiento anómalo.
- Desarrollo y pruebas de protocolos. Los desarrolladores y probadores de protocolos pueden utilizar Wireshark para analizar la interacción entre diferentes componentes de una aplicación o sistema distribuido, validar la implementación de protocolos y depurar problemas de comunicación.
- Educación en redes. Wireshark se utiliza ampliamente en entornos educativos y de formación para enseñar los conceptos de redes, protocolos y análisis de tráfico de red. Permite a los estudiantes visualizar y comprender cómo funcionan los protocolos y cómo se intercambian los datos en una red.

2.7.5 Metasploit

Es una plataforma de código abierto la cual permite la ejecución y el desarrollo de exploits. Esta se encuentra instalada de forma predeterminada en Kali Linux. se utiliza para realizar pruebas de penetración y evaluaciones de vulnerabilidades, simulando ataques para detectar debilidades y vulnerabilidades en sistemas y aplicaciones. Los profesionales de seguridad informática y los investigadores de vulnerabilidades pueden utilizar Metasploit para probar y evaluar la seguridad de sus propias redes y sistemas, o para identificar vulnerabilidades en los sistemas de sus clientes o empleadores. También puede ser utilizado por los equipos de defensa para probar y mejorar la seguridad de sus sistemas.

Metasploit es un *framework* (es una estructura de software que proporciona un conjunto de herramientas y librerías para facilitar el desarrollo de aplicaciones) de pruebas de penetración (*penetration testing*) que se utiliza para evaluar la seguridad de los sistemas de información.

Está diseñado para ser modular y extensible, lo que permite a los usuarios personalizar y ampliar su funcionalidad según sus necesidades. El marco se compone de varios componentes clave: [20]

- Módulos. Metasploit utiliza módulos para realizar diversas tareas, como la enumeración de redes, la explotación de vulnerabilidades y la generación de payloads. Los módulos se pueden clasificar en módulos auxiliares, módulos de escaneo, módulos de explotación y más.

- Exploits. Los exploits son piezas de código o técnicas que aprovechan las vulnerabilidades en sistemas o aplicaciones para ganar acceso no autorizado. Metasploit proporciona una amplia biblioteca de exploits para una variedad de vulnerabilidades conocidas.
- Payloads. Los payloads son las cargas útiles que se ejecutan después de que se haya aprovechado una vulnerabilidad. Pueden ser utilizados para realizar diversas acciones, como obtener una shell remota, descargar y ejecutar archivos maliciosos, capturar contraseñas, entre otros.
- Handlers. Los handlers son componentes de Metasploit que reciben y gestionan las conexiones establecidas a través de los exploits. Pueden ser utilizados para interactuar con los sistemas comprometidos y realizar acciones adicionales.

Es una herramienta necesaria para profesionales de seguridad, investigadores y equipos de respuesta a incidentes por varias razones:

- Evaluación de seguridad: Metasploit permite realizar pruebas de penetración y evaluaciones de seguridad para identificar y corregir vulnerabilidades en sistemas y redes. Ayuda a determinar la efectividad de las defensas de seguridad existentes y a tomar medidas para fortalecerlas.
- Respuesta a incidentes: Metasploit puede ser utilizado para investigar y responder a incidentes de seguridad. Permite analizar y entender mejor las técnicas utilizadas por los atacantes y facilita la recuperación y mitigación de los sistemas comprometidos.
- Desarrollo y validación de seguridad: Metasploit se utiliza en el desarrollo de exploits y herramientas de seguridad. Los investigadores y desarrolladores pueden utilizar Metasploit para probar la eficacia de sus herramientas, validar parches de seguridad y contribuir a la comunidad de seguridad.

Es importante destacar que Metasploit debe ser utilizado de manera legal y ética, con el permiso del propietario de los sistemas y redes que se están probando. Su uso indebido puede tener consecuencias legales y éticas.

2.7.4 Metasploitable.

Metasploitable es una máquina virtual diseñada para ser utilizada como un objetivo de práctica para pruebas de penetración y evaluaciones de seguridad. Es una imagen de sistema operativo basada en Linux que incluye una serie de vulnerabilidades conocidas y explotables. Metasploitable es utilizada por profesionales de seguridad, investigadores y estudiantes para aprender y practicar técnicas de pruebas de penetración en un entorno controlado. La idea

detrás de Metasploitable es proporcionar un ambiente vulnerable y explotable que los investigadores de seguridad puedan usar para aprender y practicar técnicas de hacking ético.

Metasploitable se utiliza para aprender y practicar técnicas de pruebas de penetración y evaluaciones de seguridad en un ambiente controlado y seguro. Puede ser utilizado para aprender sobre vulnerabilidades comunes y cómo explotarlas, y para probar diferentes herramientas de pruebas de penetración. También es utilizado por empresas y organizaciones para entrenar y capacitar a sus equipos de seguridad en técnicas de hacking ético y pruebas de penetración.

Metasploitable se configura con diferentes servicios y aplicaciones, como servidores web, bases de datos y servicios de correo electrónico, que contienen vulnerabilidades conocidas. El objetivo es permitir a los usuarios practicar y desarrollar habilidades en pruebas de penetración y seguridad de redes.

Algunas razones para utilizar Metasploitable son:

- Educación y formación: Metasploitable ofrece un entorno seguro para que los estudiantes y profesionales de seguridad adquieran experiencia práctica en la identificación, explotación y mitigación de vulnerabilidades.
- Evaluación de la postura de seguridad: Las organizaciones pueden utilizar Metasploitable para evaluar la efectividad de sus defensas de seguridad. Al simular ataques en Metasploitable, pueden identificar posibles debilidades en sus sistemas y aplicar medidas correctivas para mejorar su postura de seguridad.
- Investigación y desarrollo: Los investigadores de seguridad y desarrolladores de herramientas pueden utilizar Metasploitable para probar exploits, desarrollar nuevas técnicas de ataque y realizar investigaciones sobre seguridad de redes.

2.7.7 VirtualBox.

VirtualBox es un software que se utiliza para crear y gestionar máquinas virtuales, una máquina virtual de un sistema es un software cuyo objetivo principal es emular un sistema operativo dentro de otro, con la característica que trabajan de forma independiente. Debido a que aísla los recursos de cada máquina virtual, de manera que el sistema principal no sea compatible.

Usos de las máquinas virtuales:

- Implementar varios sistemas operativos en un único equipo.
- Tener diferentes configuraciones de sistema.
- Distintas configuraciones de redes.

- Ejecución de programas como software antiguo que no son compatibles con sistemas actuales.
- Probar comportamiento de archivos sospechosos, en el caso de ser *malware* evitar la infección en un sistema real, la máquina virtual tiene un ambiente aislado y separado del sistema operativo principal.

VirtualBox es una herramienta de virtualización que puede ser utilizada para crear y manejar máquinas virtuales. En el campo de la seguridad informática, VirtualBox se utiliza para crear entornos virtuales de pruebas para realizar pruebas de penetración, auditoría de seguridad y para desarrollar y probar aplicaciones de seguridad.

Referencias.

[1] Tanenbaum, A. S., & Wetherall, D. J. (2011). Redes de computadoras (5a ed.). Pearson Educación

[2] [Peterson, L. L., & Davie, B. S. (2000). Computer Networks: A Systems Approach (Redes de Computadoras: Un Enfoque de Sistemas)]

[3] Tanenbaum, AS (2003). Redes de ordenadores (4.ª ed.). Pearson Educación.

[4] ["Computer Networking: A Top-Down Approach" por James F. Kurose y Keith W. Ross

[5] Cisco Systems, Inc. Cisco Networking Academy Program, CCNA 1 y CCNA 2.

[6] TechTarget. (s.f.). What is File Transfer Protocol (FTP)?. Recuperado el 16 de mayo de 2023, de https://searchsecurity.techtarget.com/definition/File-Transfer-Protocol-FTP

[7] MySQL. (s.f.). MySQL 8.0 Reference Manual. Recuperado el 16 de mayo de 2023, de https://dev.mysql.com/doc/refman/8.0/en/

[8] McClure, S., Scambray, J., & Kurtz, G. (2009). Seguridad de redes. En Hacking Exposed: Network Security Secrets & Solutions (6.a ed.). McGraw-Hill Education.

[9] Gutiérrez, P. (2019). El libro blanco del HACKER (2.ª ed.). Ra-Ma.

[10] [ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. Recuperado de https://www.isaca.org/-/media/isaca/cobit/cobit-2019/overview-and-introduction/overview-and-introduction-of-cobit-2019-framework.pdf]

[11] [Al-Shehri, S., Khan, M. K., Al-Wabil, A., & Al-Dossari, H. (2014). Physical Security Threats in Data Centers: A Case Study of Saudi Arabia. In 2014 9th International Conference for Internet Technology and Secured Transactions (ICITST)]

[12] Fernández, D., & Bernal, D. (2019). Seguridad lógica en redes: conceptos y mejores prácticas. Revista Avances en Sistemas e Informática

[13] Ramírez, J. A., & Zavaleta, E. (2018). Seguridad Lógica en Redes de Datos. Revista Ciencia e Ingeniería Neogranadina,

[14] Kendrick, T. (2016). The Project Management Tool Kit: 100 Tips and Techniques for Getting the Job Done Right (3rd ed.). AMACOM.

[15] Papp, L., & Varga, A. (2014). Traffic Analysis. En Traffic Analysis and Design of Wireless IP Networks (p. 1-13). Springer International Publishing

[16] ITU-T. (1991). ITU-T Recommendation X.800: Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Overview

[17] [6] Stallings, W. (2004). Fundamentos de Seguridad en Redes, Aplicaciones y Estándares. Pearson.

[18] [7] International Telecommunication Union. (1991). X.800: Security architecture for Open Systems Interconnection for CCITT applications. Disponible en https://www.itu.int/rec/T-REC-X.800-199103-I/es

[19] Lyon, G. F. (2009). Nmap Network Scanning: The Official Nmap Project Guide. San Francisco, CA: Insecure.Com LLC.

[20] David Kennedy,D., O'Gorman, J., Kearns D., & Aharoni, M.,

(2011) Metasploit: The Penetration Tester's Guide"

Capítulo 3: Instalación de Kali en Raspberry Pi 4 y máquina virtual de Metasploitable 2.

Introducción de capitulo.

En el presente capítulo, se aborda un tema de gran relevancia en el campo de la seguridad informática: la instalación de Kali Linux en una placa única Raspberry Pi y la configuración de una máquina virtual de Metasploitable 2. Estas dos herramientas son ampliamente utilizadas en el ámbito de las pruebas de penetración y el análisis de vulnerabilidad.

En primer lugar, se explorará el proceso de instalación de Kali Linux en una Raspberry Pi, aprovechando las ventajas de esta plataforma de bajo costo y su versatilidad en entornos de seguridad. Se analizarán los pasos necesarios, las consideraciones técnicas y las recomendaciones para lograr una instalación exitosa.

Posteriormente, se procederá a la configuración de una máquina virtual de Metasploitable 2, un entorno deliberadamente vulnerable diseñado para poner a prueba las habilidades de los profesionales de seguridad. Se explorarán los pasos necesarios para la configuración de la máquina virtual, así como las medidas de seguridad que deben implementarse para garantizar un entorno controlado y protegido.

A lo largo de este capítulo, se profundizará en los beneficios y las limitaciones de utilizar Kali Linux en una Raspberry Pi, así como en las posibilidades de aprendizaje y práctica que brinda la configuración de una máquina virtual de Metasploitable 2.

3.1. Instalación de Kali en placa Raspberry Pi 4

La instalación de Kali Linux en una Raspberry Pi permite a los profesionales de seguridad y los investigadores realizar tareas de seguridad sin tener que cargar con dispositivos más grandes y costosos. Además, la combinación de Kali Linux y Raspberry Pi ofrece una solución asequible y fácilmente transportable para las pruebas de seguridad en lugares donde se requiere un equipo más discreto o en espacios reducidos.

3.1.1. ¿Por qué Kali Linux?

Como ya se mencionó Kali Linux es una de las distribuciones de Linux más populares para la seguridad informática debido a que está diseñada específicamente para pruebas de penetración y auditorías de seguridad. Además, Kali Linux es muy versátil y cuenta con una amplia variedad de herramientas de seguridad preinstaladas, lo que la hace una opción conveniente y fácil de usar para los profesionales de seguridad informática y los entusiastas de hacking ético.

Además de Kali Linux, hay otros sistemas operativos para seguridad informática disponibles para Raspberry Pi, entre ellos:

1. Parrot Security OS: una distribución de Linux basada en Debian que se enfoca en seguridad informática, privacidad y análisis forense digital.
2. BlackArch Linux: una distribución de Linux basada en Arch Linux que está diseñada específicamente para pruebas de penetración y piratería ética.
3. PiBang Linux: una distribución de Linux basada en Raspbian que se enfoca en la seguridad y privacidad.
4. Fedora Security Lab: una distribución de Linux basada en Fedora que se enfoca en la seguridad informática y el análisis forense.
5. SELinux: una implementación de seguridad de Linux que proporciona un mecanismo para controlar el acceso a los recursos del sistema y proteger contra ataques maliciosos.

La elección de Kali Linux fue principalmente porque tiene una comunidad activa y una gran cantidad de documentación que ayuda a los usuarios a familiarizarse con las herramientas y la plataforma en general.

Cada uno de estos sistemas operativos tiene sus propias características y enfoques en cuanto a la seguridad informática, por lo que es importante investigar y elegir el que mejor se adapte a las necesidades de cada usuario.

Actualmente la página oficial de Kali Linux (Figura 3.1) ofrece cinco alternativas distintas para su instalación. Una de ellas es la versión ARM, diseñada específicamente para dispositivos que utilizan procesadores ARM. Estos procesadores se caracterizan por su conjunto reducido de instrucciones, lo cual les confiere una mayor eficiencia y un menor consumo energético en comparación con los procesadores que operan con conjuntos de instrucciones más amplios

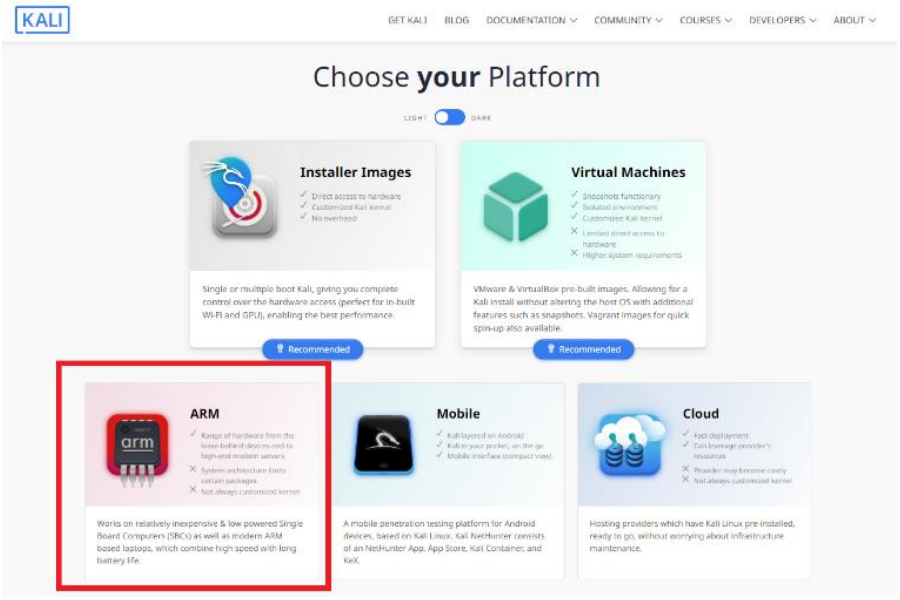


Figura 3.1. Plataformas con soporte oficial de Kali.

El archivo que contiene la imagen (copia completa de un sistema operativo, incluyendo todos los archivos, configuraciones y aplicaciones instaladas) del sistema operativo tiene una extensión **.xz** .

Cabe mencionar que esta versión oficial 2.1G tiene por defecto las credenciales:

Usuario: Kali

Contraseña: Kali

$figura\ 3.1$ Plataformas con soporte oficial de Kali, "https://www.kali.org/get-kali/", (consultado 5 de febrero 2023)

En cuanto la versión de Linux que trae la imagen del SO con el cual se trabajó, como se muestra en la figura 3.2.

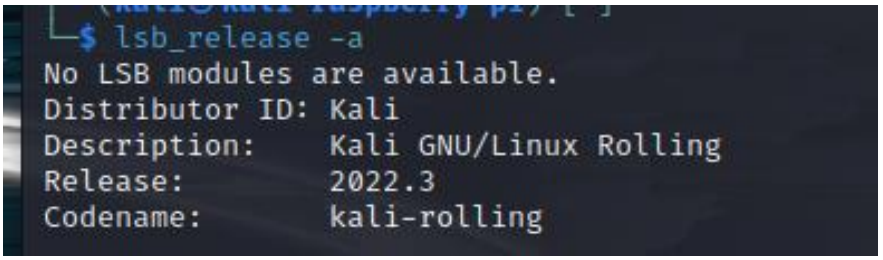


Figura 3.2: Versión 2022.3 Kali Linux en Raspberry.

3.1.2. Raspberry Pi para instalar Kali Linux.

Kali Linux es una distribución de Linux diseñada específicamente para pruebas de penetración y auditorías de seguridad. Con su amplia gama de herramientas de seguridad preinstaladas. La Raspberry Pi, por otro lado, es una pequeña computadora de placa única que se puede utilizar para una variedad de proyectos de electrónica, desde sistemas de automatización del hogar hasta robots. Juntos, Kali Linux y Raspberry Pi crean un dúo poderoso y portátil para la seguridad informática y el hacking ético, el modelo ocupado en este trabajo es Model B (Figura 3.3).

Figura 3.3: Raspberry Pi 4 Model B.

Para comenzar Raspberry Pi, necesitará los siguientes accesorios:

- Monitor.

La mayoría debería funcionar como una pantalla para Raspberry Pi, pero según la página oficial debe usar una pantalla con entrada HDMI. También necesitará un cable de pantalla apropiado para conectar el monitor a la Raspberry Pi.

- Teclado y mouse
- Alimentación

La página oficial de Raspberry recomienda una fuente de alimentación oficial de Raspberry Pi, que ha sido diseñada específicamente para proporcionar constantemente +5.1 V .

Para este caso que se ocupa Raspberry Pi 4 Model B debe usarse una fuente de alimentación tipo C.

- Almacenamiento

Tarjeta microSD de 8 GB como mínimo y usar Raspberry Pi Imager para instalar un sistema operativo en ella.

3.1.3. Raspberry Pi Imager.

Raspberry Pi Imager (Figura 3.4) es el método rápido y fácil para instalar un sistema operativo Raspberry Pi y otros sistemas operativos en una tarjeta microSD, lo cual se lleva a cabo montando un instalador dentro de la tarjeta SD que al ser insertada en el dispositivo raspberry Pi este iniciará su instalación.

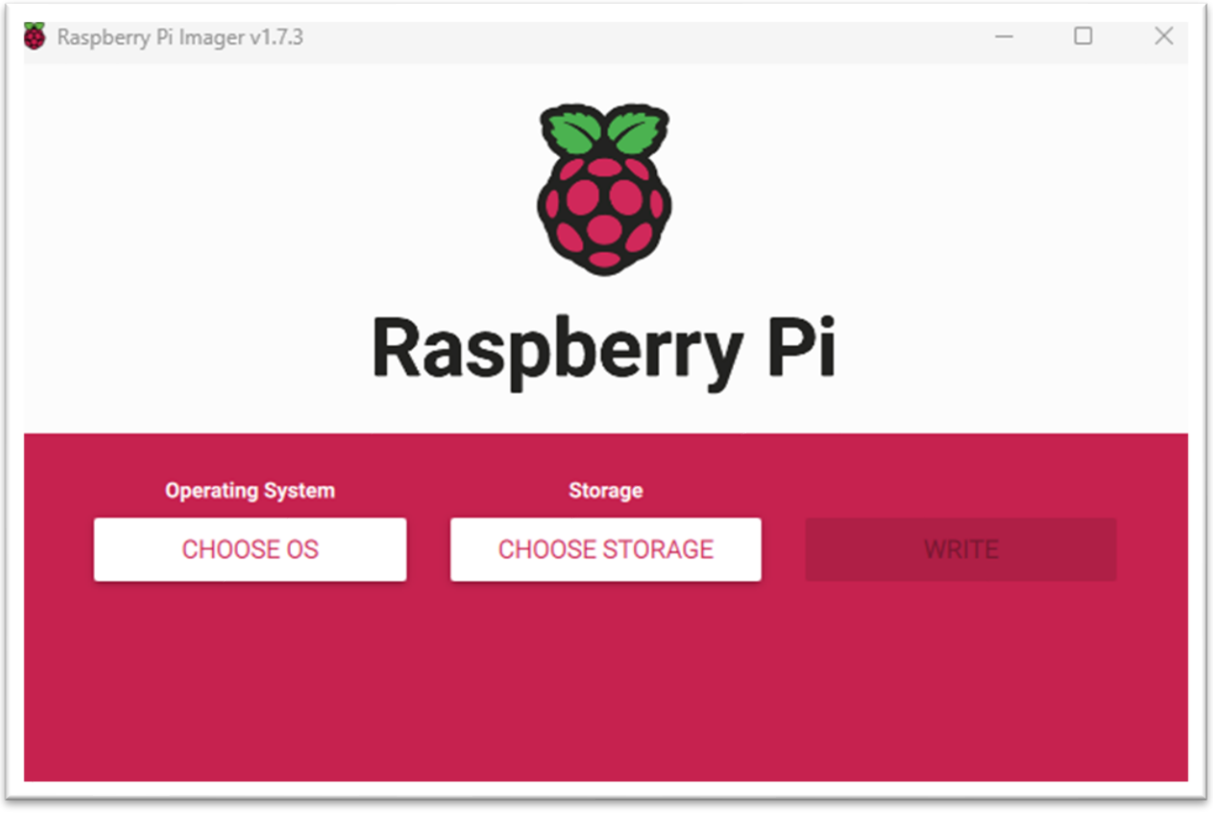


Figura 3.4. Interfaz de Raspberry Pi imager de la versión v1.7.3.

Este software se puede descargar de manera oficial desde la siguiente liga:

https://www.raspberrypi.com/software/

Después de que el instalador automático del sistema operativo Kali termine el proceso se mostrará la siguiente pantalla como se muestra en la Figura 3.5:

Figura 3.5: Pantalla de inicio del sistema Kali.

Como se mencionó anteriormente se podrá ingresar con las credenciales predeterminadas.

3.2 Instalación de VirtualBox

VirtualBox es compatible con diversos sistemas operativos, tales como Windows, Linux, macOS y Solaris, y admite una amplia gama de sistemas operativos invitados, como Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x y 4.x), entre otros. Por lo cual no es obligatorio alguno en especial, pero con respecto a los requisitos de hardware se puede decir que depende de que tan grande se busca un espacio virtualizado, pero más adelante se hablará de la necesidad de lo que se desea visualizar para esta aplicación.

En el sitio oficial de VirtualBox Figura 3.6 (https://www.virtualbox.org/) en el apartado de descargas se muestra la versión (7.0.6) y la plataforma en la cual se desea instalar en este caso Windows, el archivo .exe tiene un tamaño de 107.8 MB.

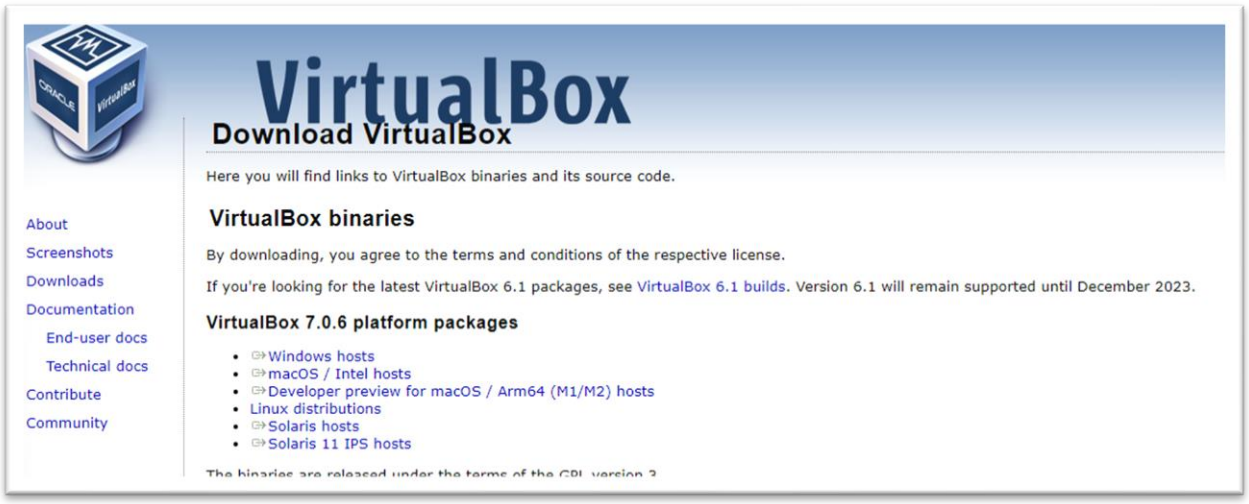


Figura 3.6. Página oficial de VirtualBox.

Al ejecutar el archivo, eligiendo la ruta de instalación y terminado la instalación se mostrará la ventana de la figura 3.7.

Figura 3.7: Interfaz de VirtualBox

En este punto VirtualBox ya estará disponible para trabajar.

NOTA: Cabe mencionar que el sistema base debe tener la opción habilitada de virtualización desde la BIOS (programa informático que se encuentra en una memoria de solo lectura en la placa base de una computadora).

3.3 Instalación de Metasploitable.

La razón para virtualizar Metasploitable 2 es para realizar pruebas de penetración o *testing* de seguridad en un entorno controlado y seguro. Al virtualizar Metasploitable 2, se puede crear un ambiente aislado en el que se pueda ejecutar el sistema sin afectar a otros sistemas en la red. Además, se pueden realizar diferentes tipos de pruebas de seguridad, como escaneo de puertos, análisis y explotación de vulnerabilidades, para evaluar la resistencia del sistema a posibles ataques. La virtualización también permite la fácil creación y eliminación de instancias de Metasploitable 2 para fines de pruebas y experimentación.

Es importante tener en cuenta que la realización de pruebas de penetración sin autorización previa puede ser considerado como un delito de intrusión informática y llevar a graves consecuencias legales. Este sistema ha sido diseñado para buscar vulnerabilidades o probar herramientas de ataque, lo que permitirá evitar ser acusado de piratería informática al acceder sin permiso al sistema. Es decir, estas pruebas y análisis se realizarán en entornos controlados, lo que hace imposible ser acusado por acceder a esta máquina.

Para fines prácticos se iniciará una instalación de Metasploitable 2 con la versión 2.0.0 como se muestra en la Figura 3.8.

En la siguiente liga se podrá descargar Metasploitable 2:

https://sourceforge.net/projects/metasploitable/files/Metasploitable 2/

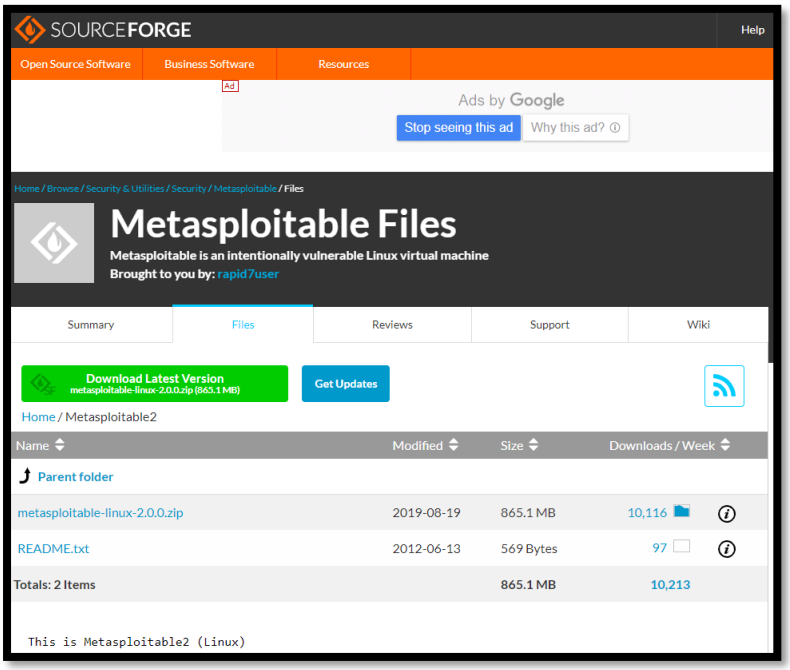


Figura 3.8: Página de descarga de Metasploitable 2.

Se descarga y descomprime el archivo extensión **.zip**, dentro de la carpeta habrá 5 archivos donde estará uno con extensión **.vmdk**, es el archivo necesario para instalar la máquina virtual en VirtualBox.

Agregar Metasploitable como una máquina virtual será muy fácil para este caso, ya que viene una imagen de sistema especial para máquinas virtuales para hacer más sencilla la instalación, para poder importar la máquina de Metasploitable en el botón de añadir se seleccionan los parámetros mostrados en la figura 3.9.

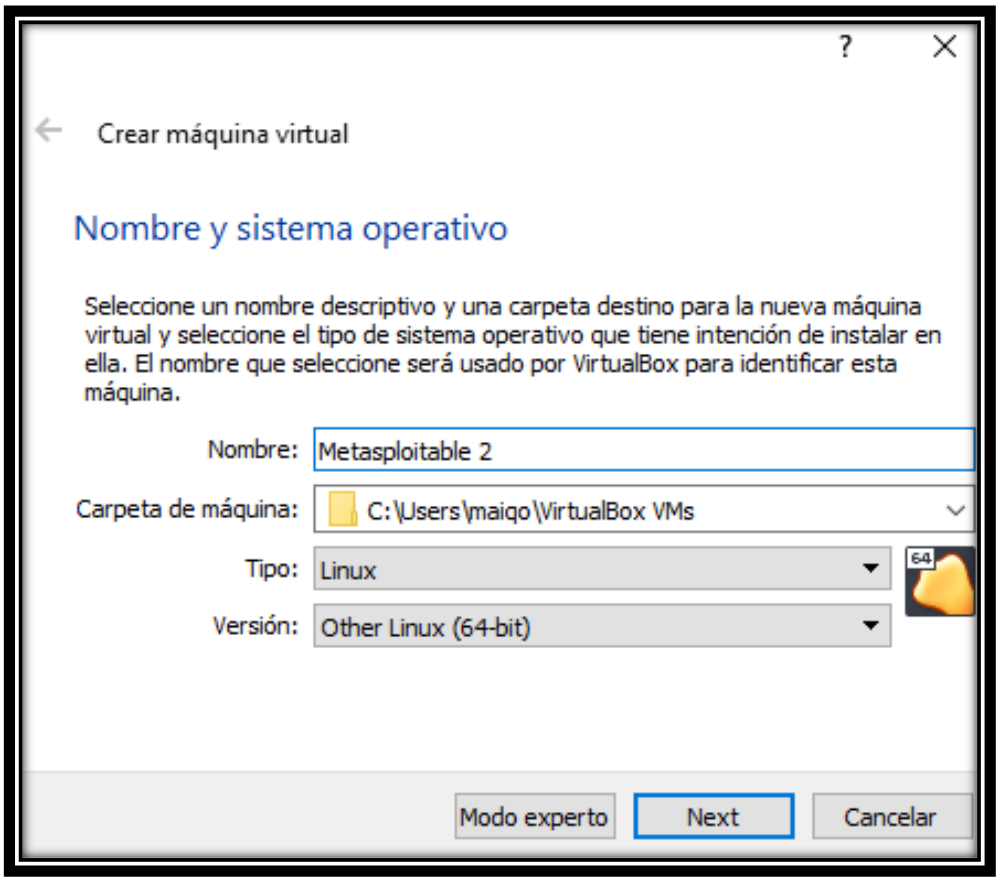


Figura 3.9: Parámetros de tipo de sistema para máquina virtual.

La siguiente ventana (Figura 3.10) será el tamaño de memoria; como Metasploitable es un sistema que solo trabaja sobre línea de comando, con 512 MB de memoria asignada será suficiente.

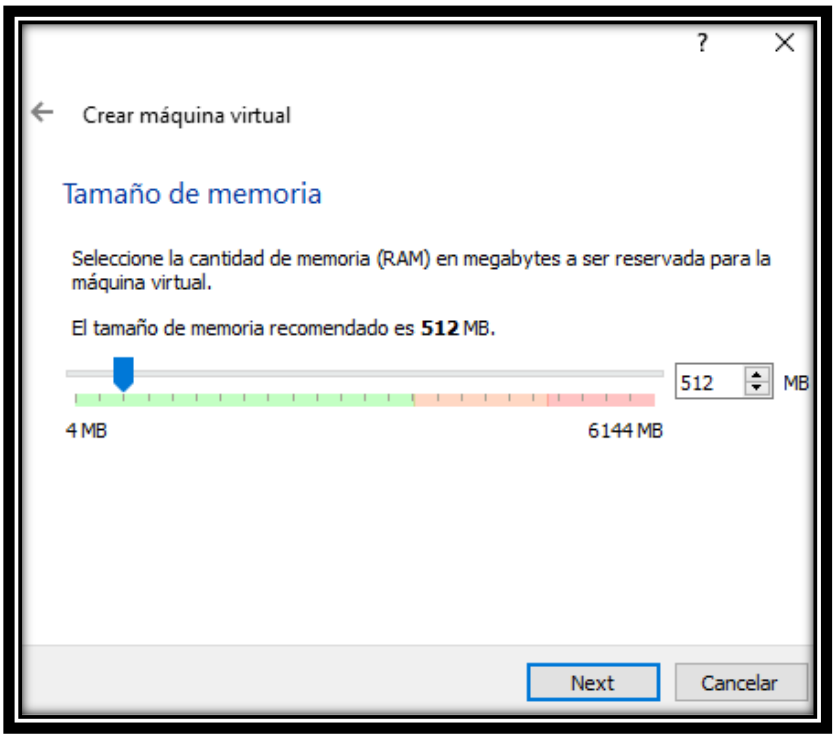


Figura 3.10: Tamaño de memoria de máquina virtual.

Por último en la ventana de la Figura 3.11 se muestran las opciones de disco virtual aquí se seleccionara "**usar una archivo de disco duro virtual**" y se agregará el archivo con la extensión **.vmdk .**

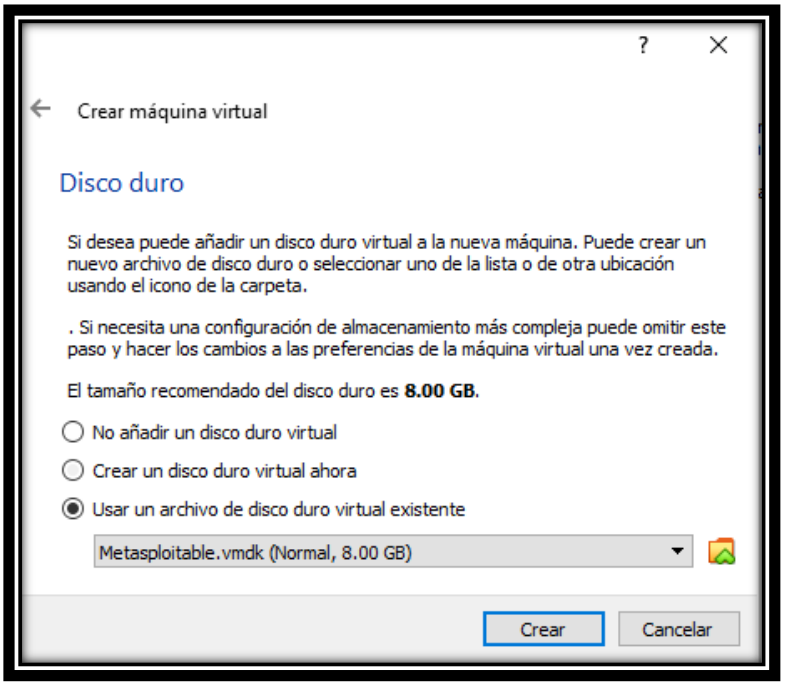


Figura 3.11: Unidad Virtual de Metasploitable 2.

Al presionar al botón **crear** se regresará la pantalla principal con Metasploitable agregada a lista de máquinas virtuales, al iniciar la máquina virtual se mostrará la siguiente ventana la cual indicará que el sistema objetivo ya está operando, como se muestra en la Figura 3.12.

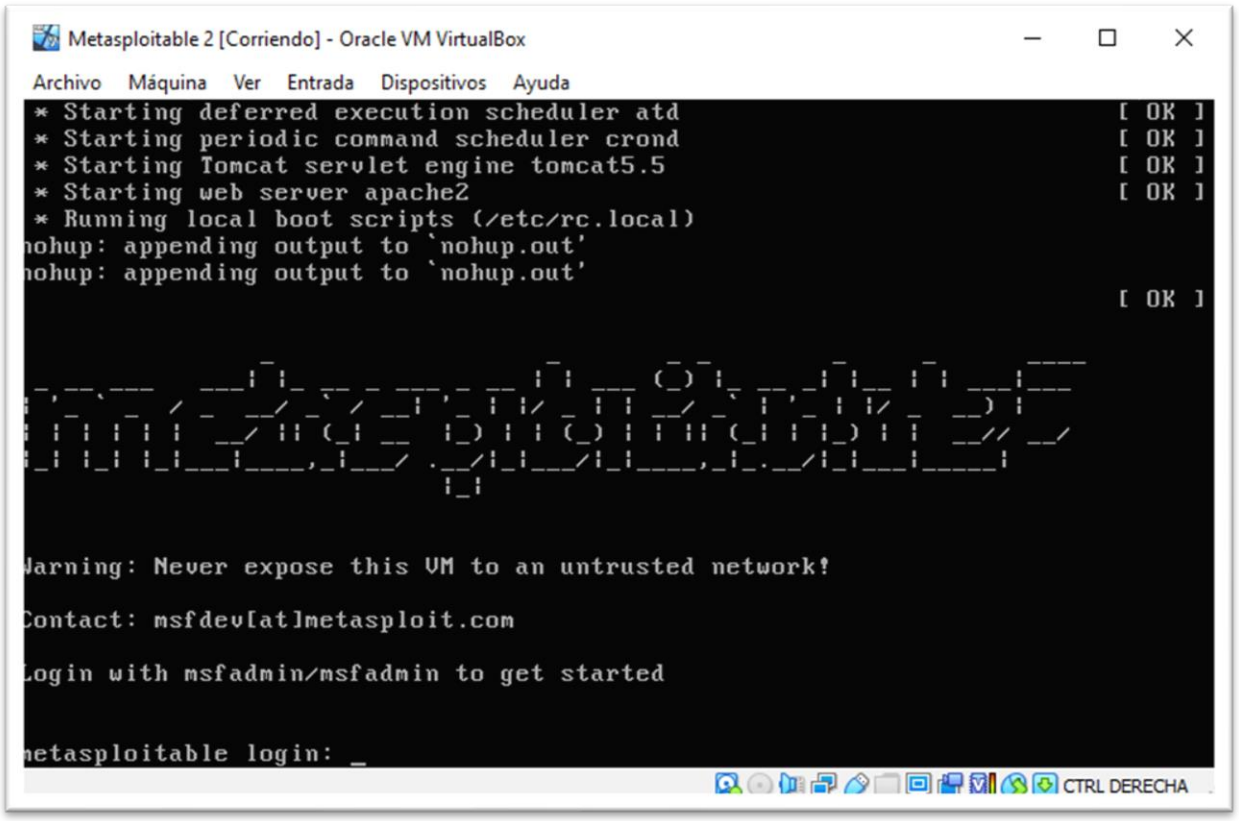


Figura 3.12: Máquina virtual de Metasploitable 2.

Metasploitable 2 tiene por defecto las siguientes credenciales.

Usuario: msfadmin

Contraseña: msfadmin

Cabe mencionar que esta máquina virtual debe estar en configuración de adaptador de red por “Puente” dentro de VirtualBox como se ve en la figura 3.13.

Una conexión puente (bridge) se utiliza a menudo en el ámbito de la virtualización para permitir que una máquina virtual comparta la conexión de red física del host. Esto es útil en situaciones en las que se desea que la máquina virtual tenga una conexión directa con la red, en lugar de a través de una conexión NAT (Network Address Translation) que puede limitar la funcionalidad de ciertas herramientas de seguridad y pruebas de penetración .

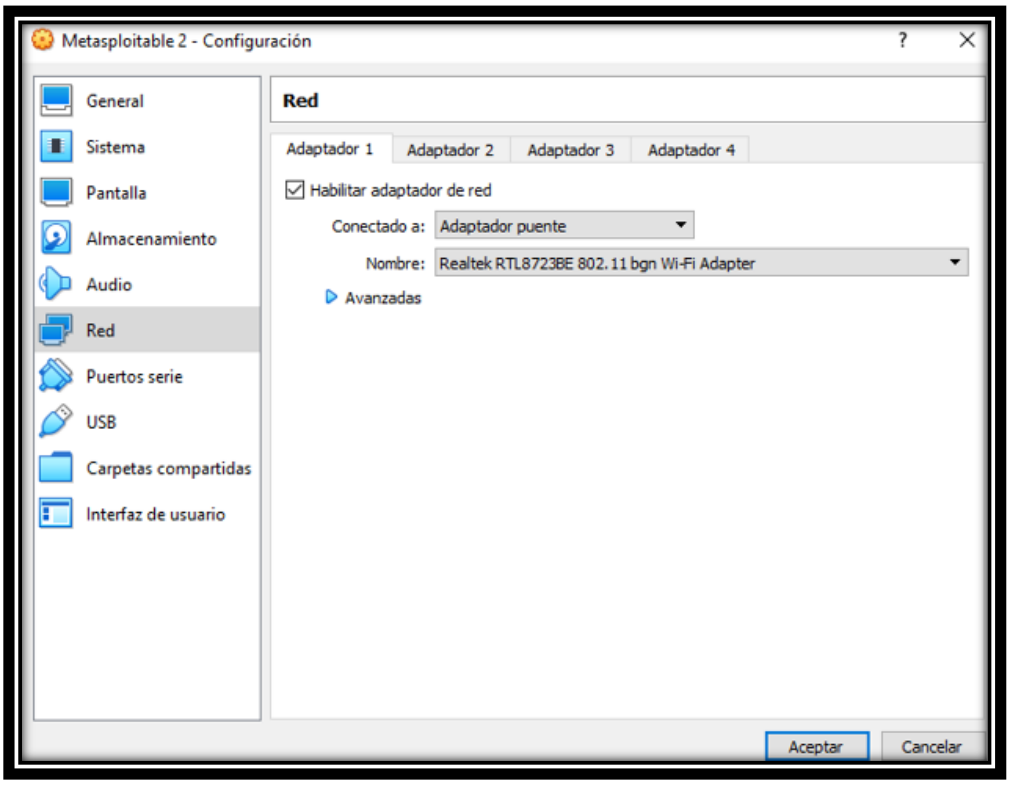


Figura 3.13. Configuración de red de máquina virtual.

Referencias

[1] Raspberry Pi Foundation. (s.f.). Raspberry Pi. https://www.raspberrypi.org/

[2] Kali Linux. (s.f.). Home of Kali Linux, an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments. https://www.kali.org/

[3] Oracle. (s.f.). VirtualBox. https://www.virtualbox.org/

Capítulo 4: Análisis de red y explotación de vulnerabilidades.

Introducción de capítulo

El análisis de red y explotación de vulnerabilidades es una técnica utilizada para evaluar la seguridad de una red informática. Consiste en identificar las vulnerabilidades en la red y en los sistemas informáticos que la conforman, y luego explotarlas para determinar el alcance del riesgo y la magnitud de las posibles amenazas.

En el análisis de red, se realiza una evaluación de los dispositivos de red, como routers, switches y firewalls, para determinar si tienen configuraciones de seguridad adecuadas y si hay vulnerabilidades conocidas que pueden ser explotadas. También se pueden analizar los protocolos de red, como TCP/IP, para identificar posibles debilidades.

Por otro lado, la explotación de vulnerabilidades se enfoca en aprovechar las debilidades encontradas en los sistemas informáticos para ganar acceso no autorizado, robar datos confidenciales, tomar control del sistema o causar daños. Esto se hace utilizando técnicas como la inyección de código, el uso de exploits, el phishing y otras tácticas.

La combinación de ambas técnicas es fundamental para garantizar la seguridad de una red y prevenir posibles ataques informáticos. Los resultados del análisis y la explotación de vulnerabilidades se utilizan para tomar medidas de seguridad, corregir vulnerabilidades y mejorar la protección de la red y sus sistemas.

4.1 Sistema con Kali en la red

Una vez conectada el sistema Raspberry Pi a la red, en Kali Linux se debe obtener la IP a la que se está asignada a través de la consola de Kali con el comando:

Ifconfig : es utilizado en sistemas operativos Unix y Unix-like (incluyendo Linux) para mostrar y configurar la información de las interfaces de red de un dispositivo

En la figura 4.1 nos muestra la respuesta del la terminal.

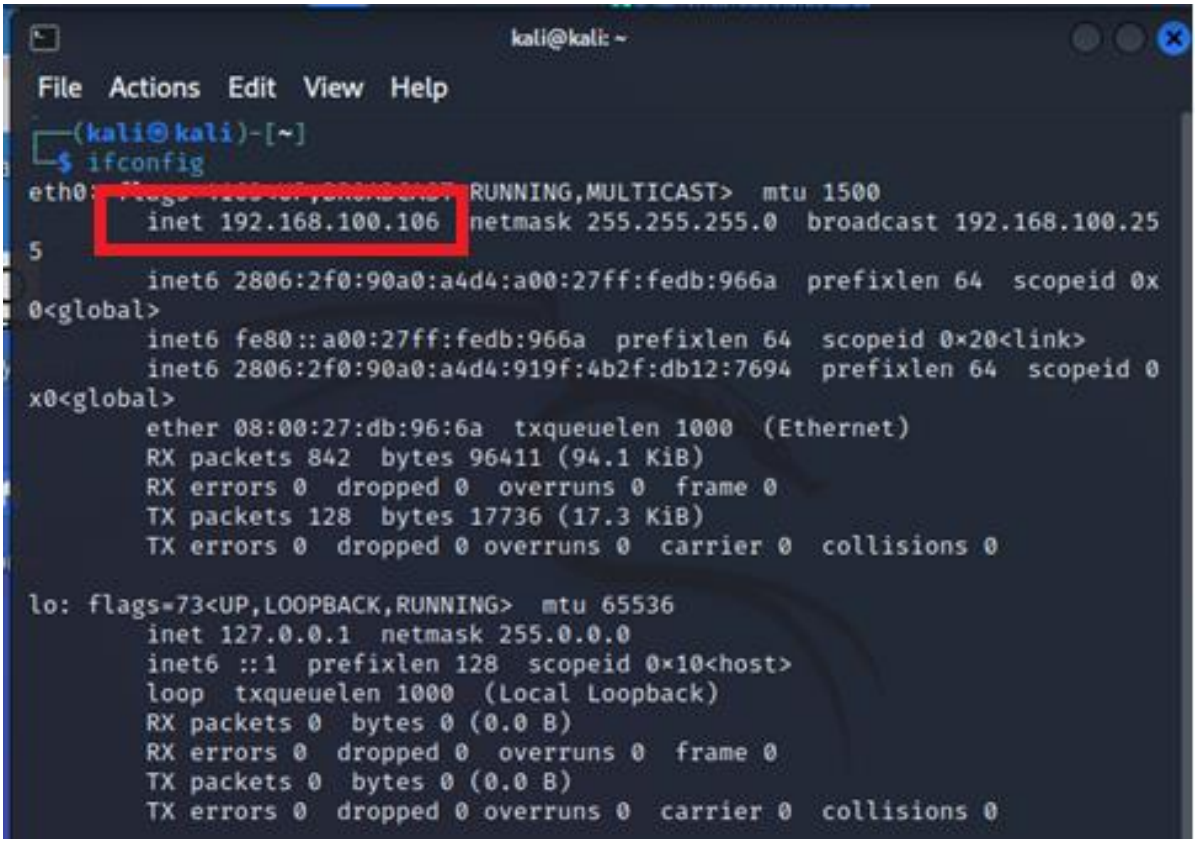


Figura 4.1: Comando ifconfig para Kali Linux.

La IP es: **192.168.100.106**

Se debe de tener en cuenta que en este caso el router administra las IP´s de forma dinámica así que cada que sea necesario se mencionará la IP que tendrá como el sistema con Kali como el sistema objetivo de Metasploitable 2.

4.2 Escaneo con Nmap

Para dar inicio al escaneo de una red, se puede utilizar la herramienta Nmap en la línea de comandos. A continuación, se muestra un ejemplo de una instrucción típica para iniciar el escaneo de una red utilizando Nmap. El uso del comando:

nmap 192.168.100.0/24 : el cual sirve para analizar todas las IP que corresponden a la red.

Se sabe que 192.168.100.x , por lo cual se hace un escaneo desde la IP 192.168.100.0 hasta la 192.168.100.254.

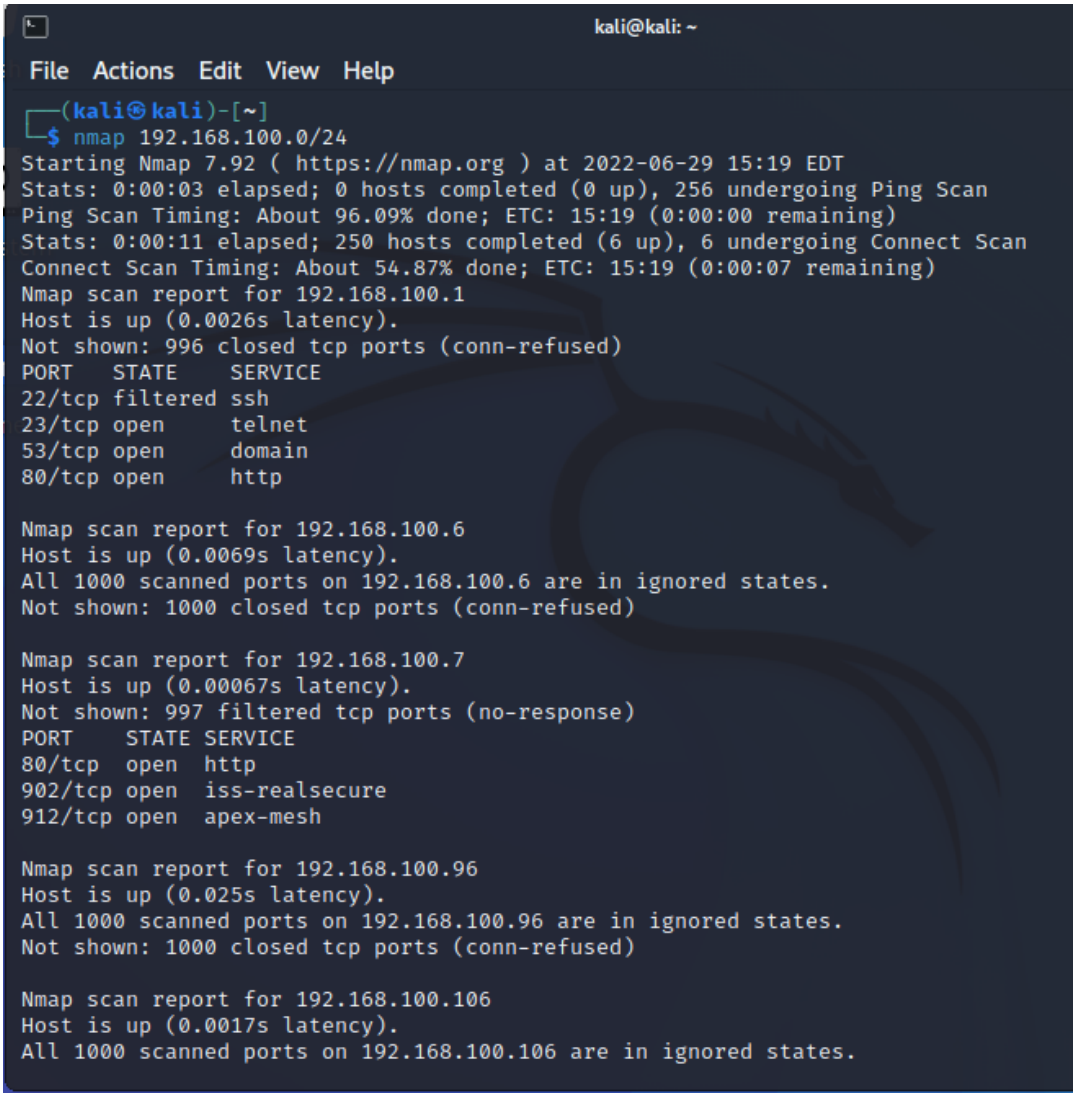


Figura 4.2.A: Escaneo con nmap comando nmap 192.168.100.0/24

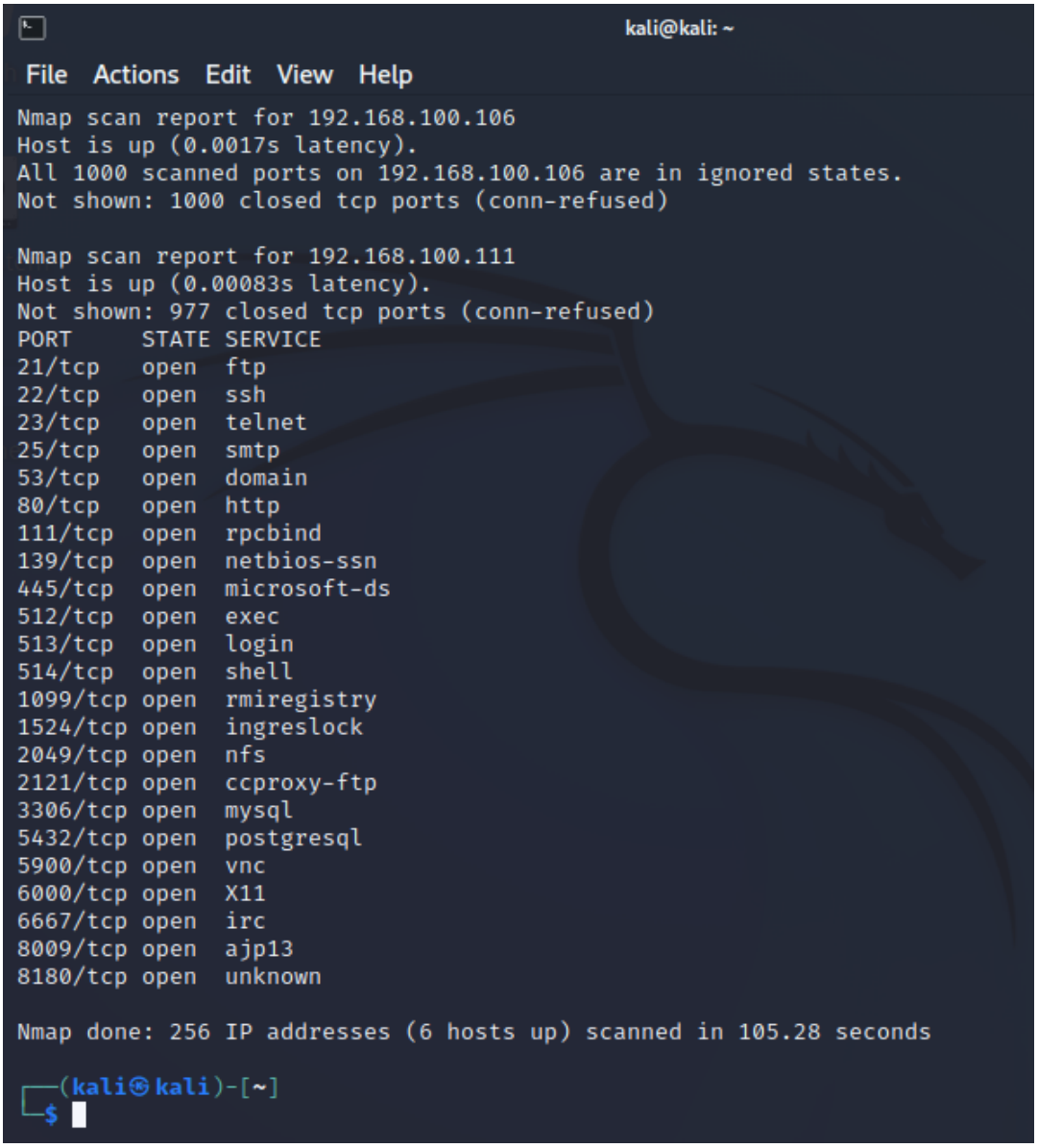


Figura 4.2.B: Escaneo con nmap comando nmap 192.168.100.0/24.

Se puede observar en las capturas A y B de la figura 4.2 el escaneo arroja respuesta de 6 host en la red, como también sus puertos de protocolos de red. En la figura B se registra el host con la IP **192.168.100.111,** tiene mayor cantidad de puertos abiertos entre los cuales están los puertos 21, 22, 23, 25, 53, 80, 111. Se sabe que estos puertos con estos protocolos tienen vulnerabilidades. Por lo tanto, se propone que el dispositivo con la IP **192.168.100.111** como sistema objetivo. Por otro lado, desde la máquina virtual de Metasploitable 2 se accede con las credenciales mencionadas en el capítulo anterior y utilizando el comando ***ifconfig*** (Figura 4.3) se puede observar que la IP de Metasploitable 2 (**192.168.100.111**) corresponde a la escaneada en el sistema de Kali Linux.

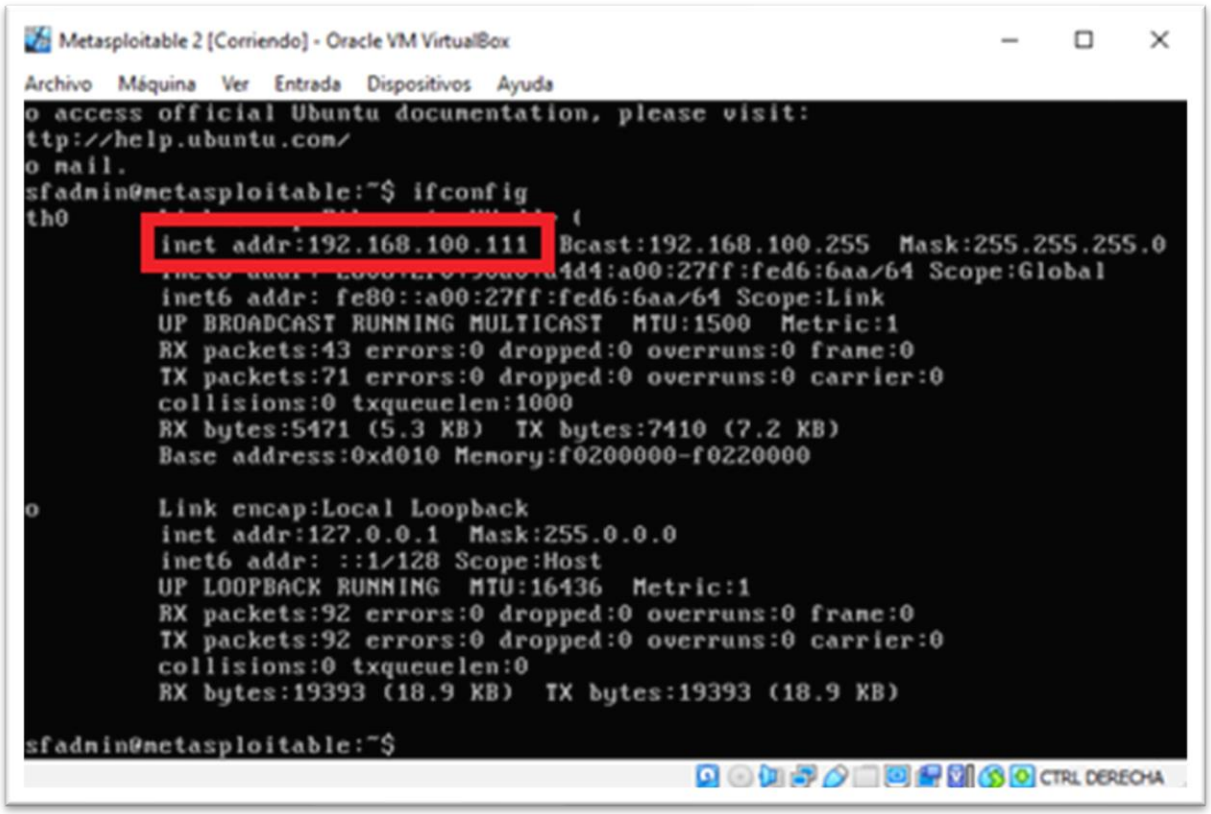


Figura 4.3: Comando ifconfig en Metasploitable 2.

La figura 4.4 nos muestra un escaneo de puertos a la IP objetivo con el comando:

nmap -O 192.168.100.111 : servirá para determinar el sistema operativo y si está disponible la versión de este.

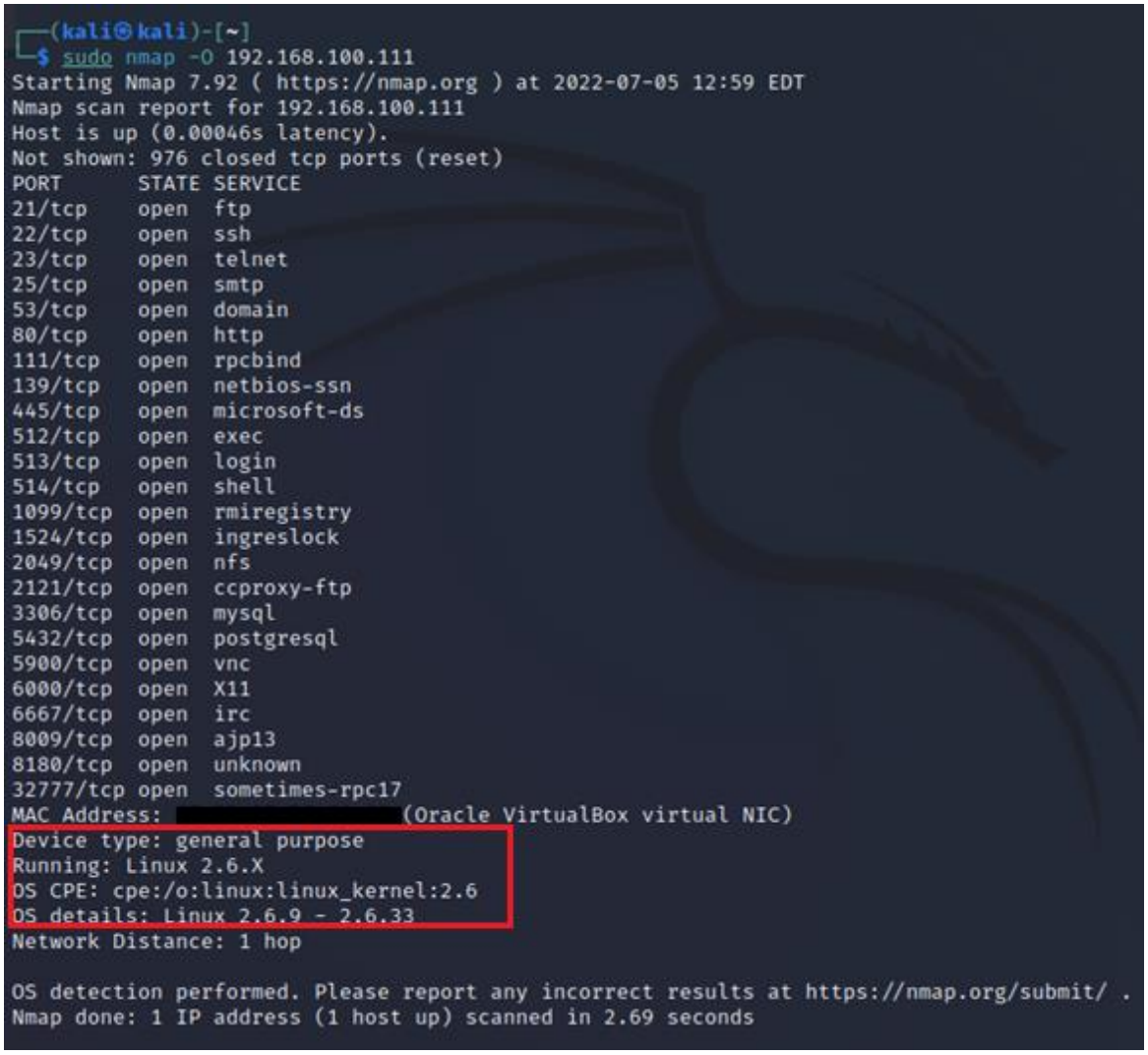


Figura 4.4. Determinación del sistema operativo del objetivo.

La respuesta se aproxima a que el sistema operativo objetivo es posible que sea una versión entre Linux 2.6.9 y Linux 2.6.33.

4.2. Explotación de vulnerabilidades.

La explotación de vulnerabilidades mediante puertos es una técnica utilizada por los atacantes para buscar y explotar vulnerabilidades en los servicios que se ejecutan en un puerto específico de un sistema remoto. Los puertos son una forma de identificar los servicios que se ejecutan en un sistema y permiten que los dispositivos se comuniquen entre sí.

Los atacantes pueden escanear puertos abiertos en un sistema y buscar vulnerabilidades en los servicios que se ejecutan en esos puertos. Una vez que se encuentra una vulnerabilidad, el atacante puede utilizarla para explotar el sistema y obtener acceso no autorizado al mismo.

Es importante tener en cuenta que muchas vulnerabilidades pueden ser corregidas mediante parches y actualizaciones de seguridad. Por lo tanto, mantener los sistemas actualizados y configurar adecuadamente los cortafuegos y otros mecanismos de seguridad puede ayudar a prevenir la explotación de vulnerabilidades mediante puertos.

4.2.1. Vulnerabilidad 1. Telnet puerto 23

Como se vio anteriormente el puerto 23 que da el servicio de telnet, se encuentra abierto, por eso se va a explorar esta vulnerabilidad. Para propósitos prácticos, se supondrá que se emplearon técnicas de ingeniería social con el fin de obtener el usuario y la contraseña, pero es importante destacar que dichas prácticas no se llevaron a cabo en un entorno real. El objetivo de este análisis de red no es realizar acciones invasivas ni comprometer la seguridad de usuarios legítimos. Más bien, se busca evaluar la efectividad de las medidas de seguridad del sistema objetivo y concientizar sobre las posibles vulnerabilidades en un entorno controlado. Es fundamental respetar los límites éticos y legales en todo momento y enfocarse en el aprendizaje y la mejora de las medidas de protección en un contexto seguro. Por lo tanto, se ejecuta el comando de **telnet** con la dirección objetivo el cual nos pedirá acceso al introducir el usuario y contraseña permitirá el acceso a distancia del sistema objetivo como se muestra la figura 4.5. Se debe mencionar que, debido a la asignación dinámica de IP debido al modem, la IP de Metasploitable 2 será **192.168.1.8** en esta ocasión.

Figura 4.5: Acceso al sistema de Metasploitable 2 por medio del protocolo Telnet.

4.2.2. Vulnerabilidad 2. MySQL puerto 3306

Para la explotación de esta vulnerabilidad se ejecutará la herramienta de Metasploit mediante el comando **msfconsole** (Figura4.6). Cabe mencionar que la IP objetivo cambio a **192.168.1.14**.

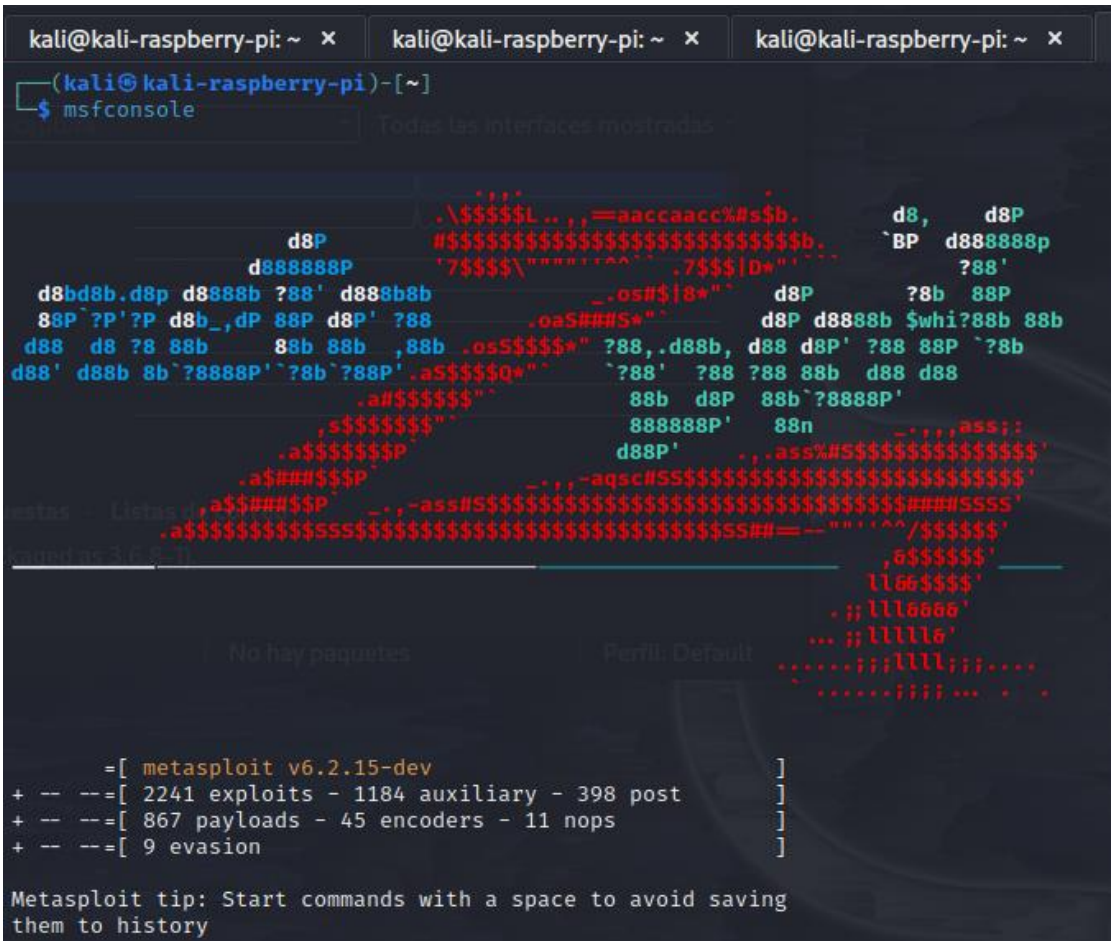
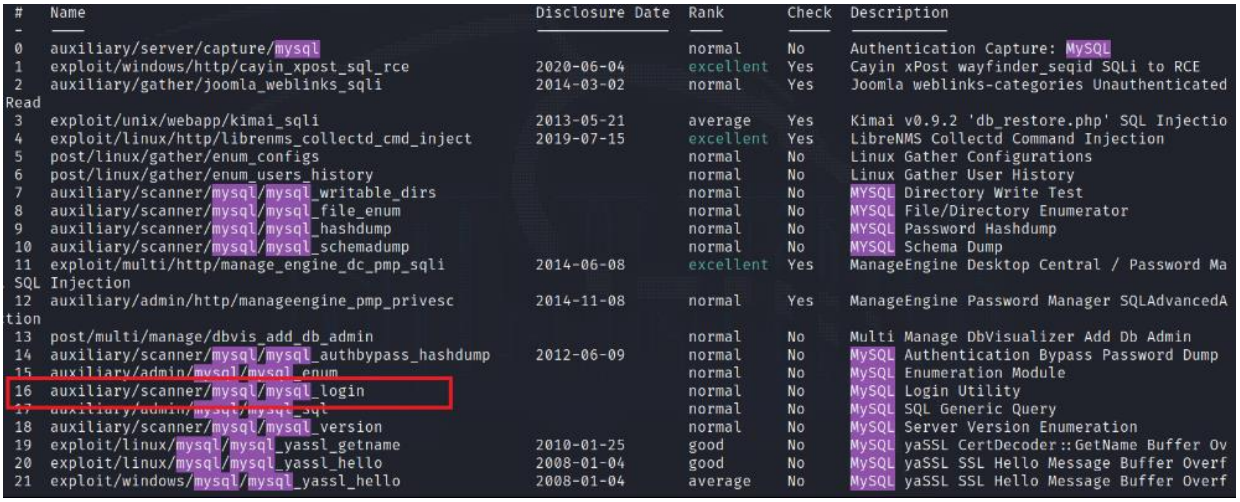


Figura 4.6. Consola de metasploit en Kali Linux.

Aquí nos muestra que esta versión la 6.2.15 cuenta con 2241 exploits que trabajan con distintos protocolos. En este caso el servicio que se busca vulnerar es de MySQL. Se puede buscar los exploits para este protocolo mediante ***search mysql***, como se muestra en la figura 4.7:

search mysql: Al ejecutar este comando, Metasploit buscará en su base de datos todos los módulos, exploits o payloads que estén diseñados específicamente para aprovechar vulnerabilidades o debilidades en sistemas o servicios relacionados con MySQL



#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/server/capture/mysql		normal	No	Authentication Capture: MySQL
1	exploit/windows/http/cayin_xpost_sql_rce	2020-06-04	excellent	Yes	Cayin xPost wayfinder_seqid SQLi to RCE
2	auxiliary/gather/joomla_weblinks_sqli	2014-03-02	normal	Yes	Joomla weblinks-categories Unauthenticated Read
3	exploit/unix/webapp/kimai_sqli	2013-05-21	average	Yes	Kimai v0.9.2 'db_restore.php' SQL Injectio
4	exploit/linux/http/librenms_collectd_cmd_inject	2019-07-15	excellent	Yes	LibreNMS Collectd Command Injection
5	post/linux/gather/enum_configs		normal	No	Linux Gather Configurations
6	post/linux/gather/enum_users_history		normal	No	Linux Gather User History
7	auxiliary/scanner/mysql/mysql_writable_dirs		normal	No	MySQL Directory Write Test
8	auxiliary/scanner/mysql/mysql_file_enum		normal	No	MySQL File/Directory Enumerator
9	auxiliary/scanner/mysql/mysql_hashdump		normal	No	MySQL Password Hashdump
10	auxiliary/scanner/mysql/mysql_schemadump		normal	No	MySQL Schema Dump
11	exploit/multi/http/manage_engine_dc_pmp_sqli	2014-06-08	excellent	Yes	ManageEngine Desktop Central / Password Ma SQL Injection
12	auxiliary/admin/http/manageengine_pmp_privesc	2014-11-08	normal	Yes	ManageEngine Password Manager SQLAdvancedA tion
13	post/multi/manage/dbvis_add_db_admin		normal	No	Multi Manage DbVisualizer Add Db Admin
14	auxiliary/scanner/mysql/mysql_authbypass_hashdump	2012-06-09	normal	No	MySQL Authentication Bypass Password Dump
15	auxiliary/admin/mysql/mysql_enum		normal	No	MySQL Enumeration Module
16	auxiliary/scanner/mysql/mysql_login		normal	No	MySQL Login Utility
17	auxiliary/admin/mysql/mysql_sql		normal	No	MySQL SQL Generic Query
18	auxiliary/scanner/mysql/mysql_version		normal	No	MySQL Server Version Enumeration
19	exploit/linux/mysql/mysql_yassl_getname	2010-01-25	good	No	MySQL yaSSL CertDecoder::GetName Buffer Ov
20	exploit/linux/mysql/mysql_yassl_hello	2008-01-04	good	No	MySQL yaSSL SSL Hello Message Buffer Overf
21	exploit/windows/mysql/mysql_yassl_hello	2008-01-04	average	No	MySQL yaSSL SSL Hello Message Buffer Overf

Figura 4.7. Exploits disponibles para la vulnerabilidad de MySQL.

La figura 4.8 nos muestra que esta versión de Metasploit tiene 21 herramientas, donde se muestra el nombre, la fecha de divulgación (si está disponible), la efectividad, la comprobación y la descripción del exploit para poner a prueba la seguridad de este puerto, como se propone hacer un ataque de diccionario y poder obtener acceso a la base de datos se utilizará el número 16 que tiene el nombre de ***auxiliary/scanner/mysql/mysql_login***. Para iniciar su configuración se ejecuta con el comando ***use 16*** (el número de la herramienta que se implementará). Y después, el comando ***show options***, el cual nos mostrará los parámetros modificables junto con su descripción.

Name	Current Setting	Required	Description
BLANK_PASSWORDS	true	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE		no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	3306	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	root	no	A specific username to authenticate as
USERPASS_FILE		no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE		no	File containing usernames, one per line

Figura 4.8: Parámetros para configurar ataque por diccionario.

Como se muestra en la figura 4.8 se configuraron 3 parámetros con el comando ***set***:

- ***set RHOSTS 192.168.1.14***: Por medio de este comando se indicó la dirección de ip de host objetivo.
- ***set user_file /home/Kali/Desktop/user***: Da la dirección de la ruta del archivo donde se encuentra la lista propuesta de posibles contraseñas.
- ***set user_as_pass true***: Prueba la combinación en que el nombre del usuario sea igual a la contraseña.

Terminada la configuración, se ejecutará el ataque de diccionario mediante el comando ***run***. La ventana mostrará el resultado de las pruebas. Se puede observar en la figura 4.9 que de los 12 intentos realizados solo 2 tuvieron acceso.

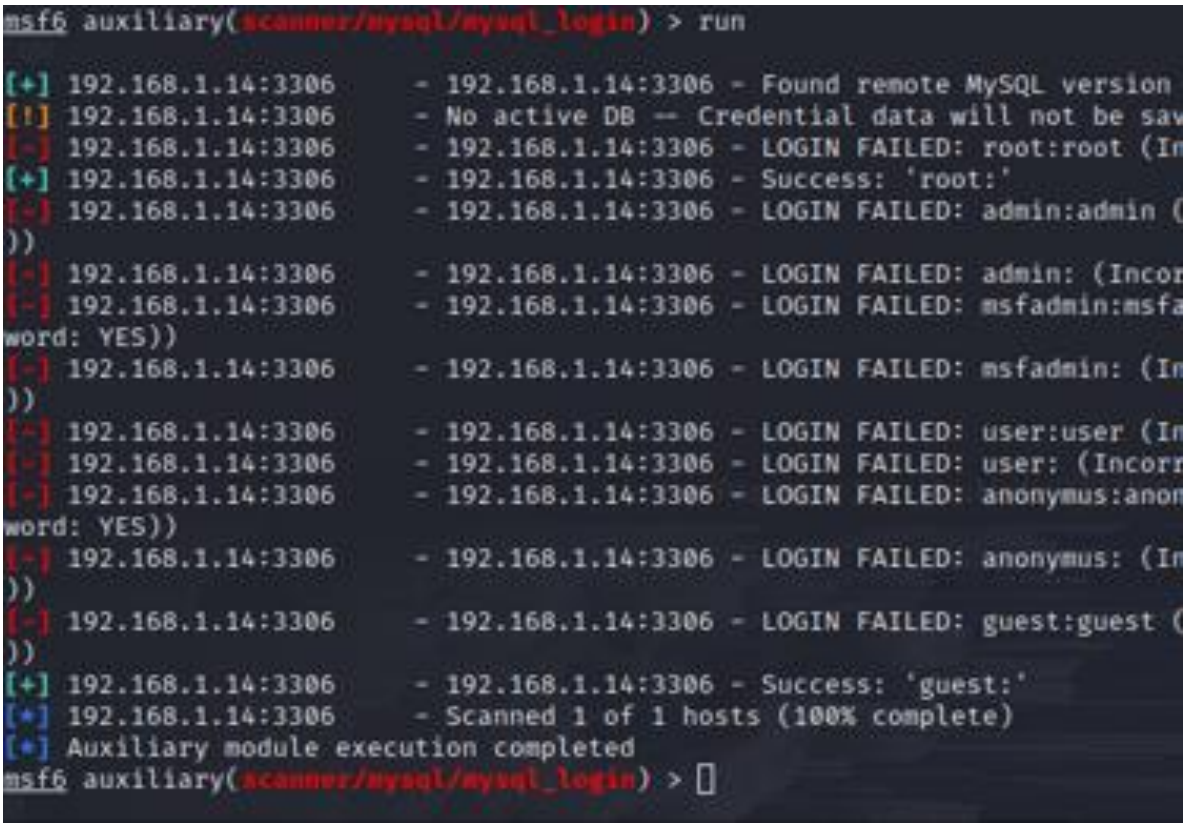


Figura 4.9. Resultados del ataque de directorio.

Si se analiza el tráfico de datos mediante Wireshark, en la figura 4.10 se puede ver el momento (registro 37) donde el sistema de Kali con la IP 192.168.1.13 manda la solicitud con el protocolo de MySQL con la información de usuario de nombre ***rot*** al sistema objetivo con la **IP 192.168.1.14**, y en el número de registro 39 el sistema objetivo acepta la petición de acceso.

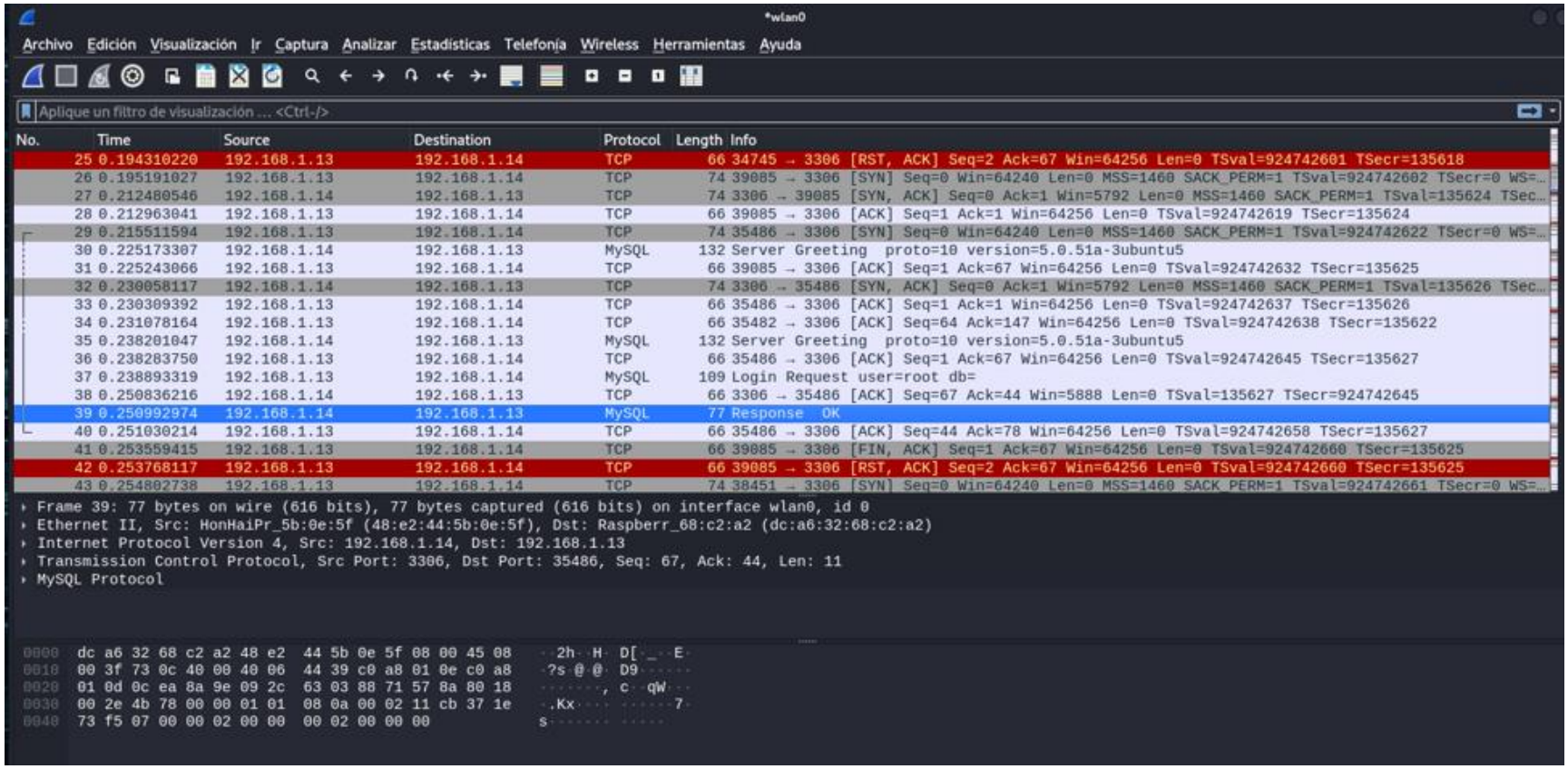


Figura 4.10: Tráfico de red para el caso de ataque de diccionario

4.2.3. Vulnerabilidad 3. FTP puerto 21

El puerto 21 con el protocolo de FTP (File Transfer Protocol) es conocido por su alta vulnerabilidad y en la gran mayor parte de los casos es recomendable que este se encuentre cerrado para evitar ser objeto de atacantes.

La figura 4.11 muestra que para poder explotar esta vulnerabilidad metasploit ofrece una única pero eficaz herramienta, cuando se busca en su base de datos con el comando ***search vsftp***

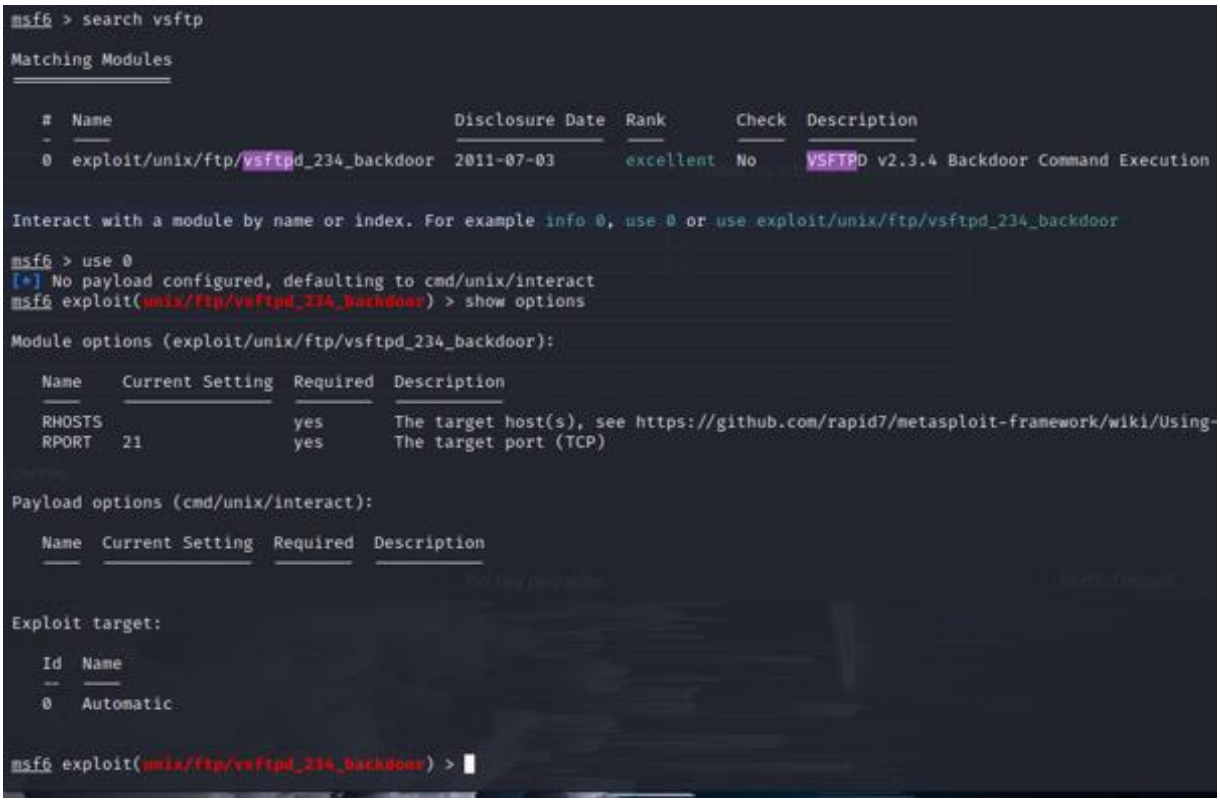


Figura 4.11: Búsqueda de la herramienta para ataque al puerto 21

La herramienta aparece con el nombre de ***exploit/unix/ftp/vsftpsd_234backdoor*** y se selecciona con el comando ***use 0***. De igual forma que en el ataque de diccionario se deben configurar parámetros los cuales se muestran con el comando ***show options*** y en este caso solo se debe dar la dirección IP que se mantiene en **192.168.1.14** con el comando ***set RHOSTS 192.168.1.14***, una vez configurado que daría de como se muestra en la figura 4.12.

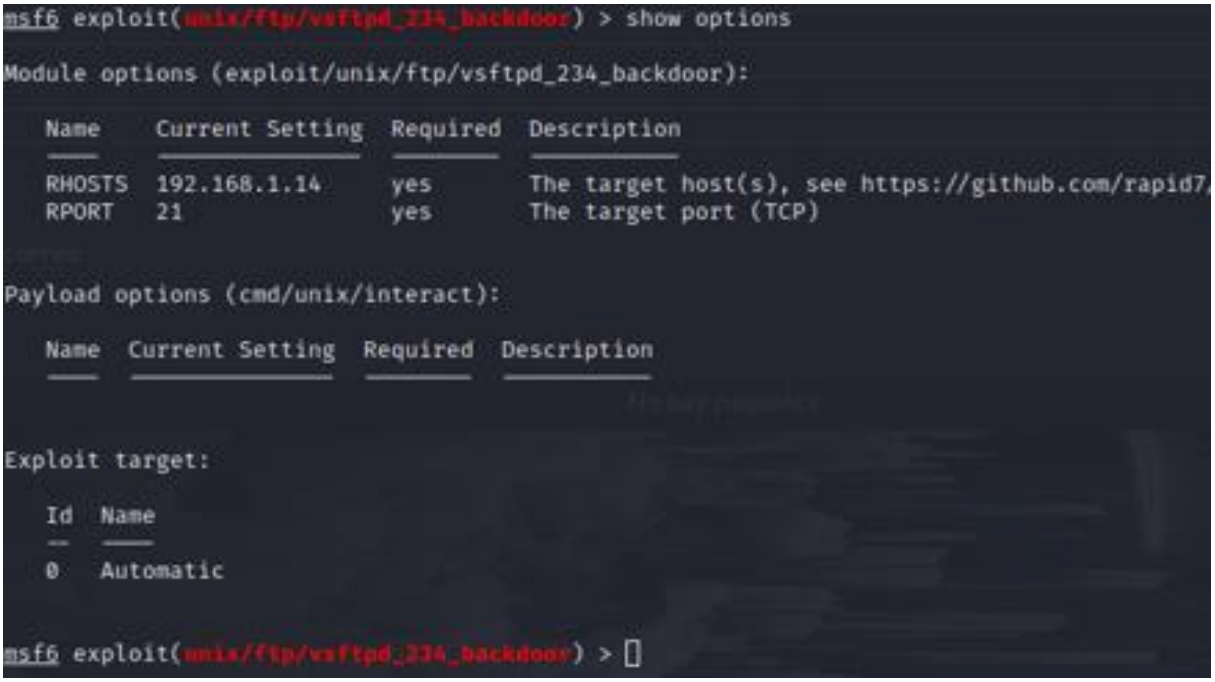


Figura 4.12: Parámetros para ataque al puerto 21.

Al ejecutar el exploit con el comando ***run*** mostrara el registro del proceso de la explotación de la vulnerabilidad se puede observar en la figura 4.13.

Figura 4.13: Registro del ataque al puerto 21.

Tras completar el proceso la terminal nos mandara directamente a la raíz de la carpeta del servidor ftp de la máquina de Metasploitable 2 Figura 4.14. Para poderlo comprobar sencillamente con el comando ***ls*** la terminal y despegara las carpetas contenidas.

Figura 4.14: Directorio del servidor ftp de Metasploitable 2.

Capítulo 5: Resultados.

Introducción de capítulo

Metasploitable 2 es un servidor vulnerable diseñado para pruebas de penetración y entrenamiento de seguridad. Como cualquier equipo real, tiene un conjunto de vulnerabilidades que podrían ser explotadas por atacantes malintencionados.

Este informe tiene como objetivo presentar una visión general de los servicios y puertos proporcionados por Metasploitable 2, así como las vulnerabilidades conocidas y las posibles soluciones. Y está basado en varias páginas donde se documentan las vulnerabilidades y posibles ataques.

A continuación, se presentan las páginas consultadas:

- La página oficial de Metasploit Project, que es el framework de pruebas de penetración utilizado en Metasploitable 2, tiene una lista de los módulos de explotación disponibles para Metasploitable 2 y otras máquinas virtuales similares. Esta página se actualiza con frecuencia y es una buena fuente para obtener información sobre las vulnerabilidades y posibles ataques.

  https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/
- El sitio web de vulnerabilidades de NIST (The National Institute of Standards and Technology), que es una base de datos de vulnerabilidades mantenida por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, también es una buena fuente para obtener información sobre las vulnerabilidades conocidas en Metasploitable 2 y otros sistemas.

  https://www.nist.gov/
- El sitio web de CVE (Common Vulnerabilities and Exposures), que es una lista pública de vulnerabilidades comunes y exposiciones, también puede proporcionar información útil sobre las vulnerabilidades en Metasploitable 2.

Es importante tener en cuenta que la evaluación de vulnerabilidades y la seguridad informática son campos complejos y cambiantes, por lo que es recomendable consultar fuentes actualizadas y confiables y siempre seguir las mejores prácticas y recomendaciones actualizadas para garantizar la seguridad y protección de los sistemas.

Metasploitable es una máquina virtual que se utiliza para prácticas de hacking ético y pruebas de penetración. Como tal, no es un servidor real y, por lo tanto, no puede ser atacado directamente a través de la ingeniería social.

Sin embargo, si se relaciona Metasploitable con un servidor real en un entorno empresarial, es posible que los atacantes utilicen la ingeniería social para obtener información sobre los sistemas, usuarios y contraseñas que podrían ser útiles en un ataque contra el servidor real. Esto podría incluir el uso de técnicas de phishing para engañar a los usuarios para que proporcionen información confidencial o el uso de técnicas de ingeniería social para manipular a los empleados para que realicen acciones que podrían comprometer la seguridad del servidor.

5.1 Reporte

Se llevó a cabo un análisis de vulnerabilidades en una red local, detectando un total de cuatro equipos. El objetivo de esta evaluación fue identificar posibles vulnerabilidades en los sistemas y servicios de red, para tomar medidas de corrección y prevención que reduzcan los riesgos de seguridad informática.

En el siguiente informe se presentarán los resultados obtenidos de cada equipo, describiendo las vulnerabilidades encontradas y las recomendaciones para su mitigación.

A continuación, se presenta la tabla 5.1 en la que se organizan los equipos según su nivel:

Consideración: Un equipo contendrá más de una IP debido a la asignación dinámica del router.

Equipo	Dirección IP	Nivel
Equipo 1	192.168.100.111 192.168.1.14 192.168.1.8	Critico
Equipo 2	192.168.100.1	Medio
Equipo 3	192.168.100.7	Bajo
Equipo 4	192.168.100.6	Bajo
Equipo 5	192.168.100.96	Bajo
Equipo 6	192.168.100.106	Bajo

Tabla 5.1. Equipos detectados en el escaneo de red.

En la tabla se muestran los cuatro equipos encontrados en el escaneo de red, indicando su dirección IP, sistema operativo y el nivel de criticidad asignado. El equipo 1 ha sido considerado crítico, lo que indica que presenta vulnerabilidades muy importantes que deben ser atendidas de forma prioritaria. por lo tanto, se analizó principalmente este equipo.

Servicios y puertos

A continuación, la tabla 5.2 y 5.3 presenta los servicios y puertos proporcionados por los equipos en la red que se consideran importantes debido a sus vulnerabilidades.

Equipo 1

Servicio	Puertos	Descripción
SSH	22	Protocolo de red utilizado para la conexión a sistemas remotos.
Telnet	23	Protocolo de red utilizado para la conexión a sistemas remotos.
FTP	21	Protocolo de red utilizado para la transferencia de archivos.
Samba (netbios-ssn/Microsoft-ds).	139, 445	Implementación del protocolo SMB/CIFS para compartir archivos e impresoras.
HTTP	80	Protocolo de la World Wide Web utilizado para la transferencia de datos.
mysql	3306	Sistema de gestión de bases de datos relacionales.
postgresql	5432	Sistema de gestión de bases de datos relacionales.
RPCBind/NFS	111, 2049	Servicio de red para compartir sistemas de archivos en una red.

Tabla 5.2: Servicios y puertos de equipo 1.

Equipo 2

Servicio	Puertos	descripción
SSH	22	Protocolo de red utilizado para la conexión a sistemas remotos.
Telnet	23	Protocolo de red utilizado para la conexión a sistemas remotos.
HTTP	80	Actualizar a un protocolo más seguro como HTTPS

Tabla 5.3: Servicios y puertos de equipo 2.

Vulnerabilidades y soluciones.

La seguridad de un sistema no sólo depende de la fortaleza de sus medidas de protección, sino también de la identificación y corrección de vulnerabilidades. En este sentido, se han identificado dos equipos, 1 y 2, que presentan vulnerabilidades similares en su infraestructura de seguridad. El objetivo de este informe es ofrecer una visión global de los problemas de seguridad que enfrentan estos equipos y presentar medidas concretas para solucionarlas y mejorar su protección contra posibles ataques.

A continuación, en la tabla 5.4, se presentan algunas de las vulnerabilidades más importantes que se han descubierto como una posible solución:

Servicio/Puerto	vulnerabilidad	Posible solución
SSH (22)	Contraseñas débiles y autenticación basada en contraseñas habilitada	Utilizar autenticación basada en llaves SSH y/o implementar políticas de contraseñas seguras

FTP (21)	Anónimo FTP habilitado Y Backdoor	Deshabilitar el acceso anónimo o configurar permisos adecuados en los archivos y carpetas compartidos y Actualizar a una versión más reciente
Telnet (23)	Autenticación basada en contraseñas habilitada y tráfico de red no cifrado	Utilizar SSH en su lugar para un acceso remoto seguro.
SMTP (25)	Servidor de correo vulnerable a ataques de relay abierto	Configurar restricciones en el servidor de correo para evitar el relay abierto
HTTP (80)	Versiones antiguas y vulnerables de aplicaciones web (por ejemplo, Apache, PHP, etc.)	Actualizar a un protocolo más seguro como HTTPS
HTTPS (443)	Certificados SSL auto firmados y versiones antiguas de OpenSSL	Utilizar certificados SSL emitidos por una autoridad de certificación confiable y actualizar OpenSSL a la última versión disponible
MySQL (3306)	Contraseñas de MySQL débiles y acceso remoto habilitado	Utilizar contraseñas fuertes y deshabilitar el acceso remoto si no es necesario
PostgreSQL (5432)	Contraseñas de PostgreSQL débiles y autenticación basada en contraseñas habilitada	Utilizar contraseñas fuertes y/o autenticación basada en llaves SSH
Samba (139, 445)	Configuración de permisos de archivo/ carpeta incorrectos	Configurar los permisos adecuados en los archivos y carpetas compartidos
SNMP (161)	Comunidad SNMP predeterminada configurada	Configurar una comunidad SNMP personalizada y utilizar autenticación basada en contraseñas o llaves.

Tabla 5.4: Vulnerabilidades y posibles soluciones.

Cabe mencionar que la ingeniería social puede ser una táctica utilizada por los atacantes para obtener acceso inicial al servidor y otras herramientas pueden ser utilizadas para explotar vulnerabilidades y realizar ataques posteriores.

Es importante destacar que la ingeniería social es una técnica de ataque muy efectiva y puede ser muy difícil de detectar y prevenir. Es fundamental que los usuarios sean conscientes de

los riesgos y estén capacitados para reconocer y evitar técnicas de ingeniería social para minimizar la posibilidad de que se produzca una brecha de seguridad.

Conclusiones.

Durante el desarrollo de esta tesis, se llevó a cabo una exhaustiva investigación sobre los conceptos fundamentales de la ciberseguridad. Se buscó comprender en profundidad los principios y técnicas utilizadas para proteger los sistemas y datos frente a posibles amenazas y ataques cibernéticos. Se exploraron temas como la identificación y gestión de riesgos, la seguridad de redes y sistemas, las políticas de seguridad, la concientización y educación en seguridad. Por lo que se concluye que es necesario la adquisición de conocimientos sólidos y actualizados en este campo en constante evolución, con el fin de desarrollar estrategias efectivas de protección y mitigación de riesgos en entornos digitales cada vez más complejos y amenazantes.

También se requiere de una amplia investigación de las herramientas y tecnologías utilizadas en este campo. Se investigaron a fondo herramientas populares como Kali Linux, Wireshark y Metasploit, las cuales son ampliamente reconocidas en la comunidad de seguridad informática. Se exploraron sus capacidades, funcionalidades y metodologías, análisis de tráfico de red y pruebas de penetración. aunque Kali Linux, Wireshark y Metasploitable son herramientas poderosas y útiles en el ámbito de la seguridad informática, su utilización puede presentar dificultades relacionadas con el conocimiento técnico requerido, la configuración adecuada, el uso responsable y ético, y la comprensión de los riesgos asociados. Superar estas dificultades y utilizar estas herramientas de manera adecuada puede proporcionar beneficios significativos en términos de evaluación de la seguridad y fortalecimiento de los sistemas.

Se identificaron las necesidades clave para contar con un espacio dedicado a las pruebas de seguridad, analizando la importancia de disponer de un entorno controlado y aislado. Este entorno permite llevar a cabo pruebas sin comprometer la seguridad de los sistemas reales. Aunque la virtualización ofrece numerosos beneficios, también es importante tener en cuenta que puede presentar algunas dificultades. Durante la investigación, se examinaron los requisitos de hardware y software necesarios para establecer un entorno de pruebas seguro y confiable, incluyendo consideraciones sobre la configuración de redes, sistemas operativos y herramientas especializadas.

Además, se exploró la virtualización de máquinas, centrándose específicamente en la creación y configuración de una máquina virtual de Metasploitable 2. Metasploitable 2 es una máquina virtual diseñada intencionalmente con vulnerabilidades conocidas, y su propósito es brindar un entorno de pruebas realista para evaluar y mejorar las habilidades de seguridad.

El presente trabajo ha abordado el análisis de Metasploitable 2 como si fuera un equipo real, identificando sus principales vulnerabilidades y proponiendo posibles soluciones para mitigar los riesgos asociados. Se ha demostrado que Metasploitable 2 es vulnerable a una serie de ataques comunes en entornos de redes, incluyendo el uso de contraseñas débiles, vulnerabilidades en servicios y aplicaciones desactualizadas y la falta de autenticación adecuada.

Por otro lado, la utilización de una Raspberry Pi para ejecutar Kali Linux ofrece tanto beneficios como desafíos. En primer lugar, la Raspberry Pi brinda una solución de bajo consumo energético y medianamente económica, lo que la convierte en una opción atractiva para implementar un entorno de pruebas y análisis de vulnerabilidades. Además, su tamaño compacto y portabilidad permiten realizar pruebas de seguridad en diferentes ubicaciones de manera conveniente, en este punto cabe mencionar que la portabilidad es si se llega a algún lugar donde se encuentren los periféricos ya instalados, si no la portabilidad se pierde por completo.

Sin embargo, el uso de una Raspberry Pi para ejecutar Kali Linux también presenta ciertos desafíos. Debido a las limitaciones de hardware y recursos de la Raspberry Pi, puede haber restricciones en cuanto a la potencia de procesamiento y la memoria disponible, lo que puede afectar el rendimiento y la eficiencia en tareas intensivas. Entre las más notables durante el uso de Kali Linux en Raspberry Pi fue los tiempos en que inicia el sistema operativo era mucho más prolongados a la versión de escritorio, al inicializar algunas herramientas como la consola de Metasploit, lentitud al abrir programas de interfaz gráfica como el propio navegador Firefox.

En los principales foros oficiales se mencionan estas principales

La tabla 6.1 es comparación de las diferencias entre Kali Linux en su versión de escritorio y Kali Linux en una Raspberry Pi:

Aspectos	Kali Linux de escritorio	Kali Linux en Raspberry Pi
Rendimiento	Mayor potencia de procesamiento y recursos disponibles	Limitaciones de hardware y recursos, lo que puede afectar el rendimiento en tareas intensivas

Compatibilidad	Amplia compatibilidad con diversas herramientas y funcionalidades	Algunas herramientas y funcionalidades pueden no ser completamente compatibles o funcionar de manera óptima en una plataforma con recursos limitados
Capacidad de almacenamiento	Capacidad de almacenamiento flexible y escalable	Capacidad de almacenamiento limitada en comparación con una computadora de escritorio
Conectividad	Conexión a una amplia gama de dispositivos y redes	Limitaciones en las opciones de conectividad y puertos disponibles
Experiencia de usuario	Interfaz de usuario gráfica y completa	Interfaz de usuario adaptada a la pantalla y recursos limitados de la Raspberry Pi
Portabilidad	Requiere una computadora de escritorio o portátil para su uso	Tamaño compacto y portabilidad de la Raspberry Pi para realizar pruebas de seguridad en diferentes ubicaciones

Tabla 6.1 Comparaciones de versiones de Kali Linux.

Con respecto al análisis de red donde el DHCP (Dynamic Host Configuration Protocol/ Protocolo de configuración dinámica de host) estaba activado presentó algunas dificultades, entre las cuales se pueden mencionar:

- Cambio frecuente de direcciones IP: El DHCP asigna direcciones IP de forma dinámica a los dispositivos en la red. Esto significa que las direcciones IP pueden cambiar con cierta frecuencia, lo que dificultó el seguimiento y la identificación del dispositivo objetivo en la red.
- Obtención de información limitada: Al utilizar DHCP, en algunos escaneos no se obtiene información detallada sobre los dispositivos conectados a la red, como nombres de host o información de identificación adicional.

En general, se ha demostrado que la seguridad en el entorno de las redes es una preocupación crítica en la actualidad y que la identificación y mitigación de vulnerabilidades en los sistemas es esencial para garantizar la protección de los datos y la privacidad de los usuarios. Se espera que este trabajo contribuya al desarrollo de estrategias efectivas para la prevención y mitigación de ataques informáticos, lo que resultará en una mayor seguridad y protección de la información, y que la implementación de todas estas herramientas.

Bibliografía y Referencias

Referencias Capítulo 1

[1] Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. Cengage Learning.

[2] Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC), International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). (2017). Cybersecurity Curricular 2017. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

[3] Cybersegurity Curricular (2017), Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS) , Association for Information Systems Special Interest Group on Information, Security and Privacy (AIS SIGSEC), International Federation for Information Processing Technical Committee on Information Security Education

[4] Stallings, W. (2004). Fundamentos de Seguridad en la Red, Aplicaciones y Estándares. Pearson.

[5] Stuttard, D., & Pinto, M. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. Wiley Publishing.

[6] Guía de ciberataques, España, Oficina de Seguridad del Internauta.

[7] K-oox seguridad informática. Sitio web. [Online]. Disponible: http://k-oox.blogspot.com/2016/05/ingenieriasocial-la-amenaza-invisible.html

[8] ESET. (sf). MANUAL DE INGENERIA SOCIAL: Cómo actuar correctamente.

[9] Fernández, M., & Andrés, J. (2021). Hackers: Técnicas y herramientas para atacar y defendernos. Ediciones de la U.

Referencias capítulo 2.

[1] Tanenbaum, A. S., & Wetherall, D. J. (2011). Redes de computadoras (5a ed.). Pearson Educación

[2] [Peterson, L. L., & Davie, B. S. (2000). Computer Networks: A Systems Approach (Redes de Computadoras: Un Enfoque de Sistemas)]

[3] Tanenbaum, AS (2003). Redes de ordenadores (4.ª ed.). Pearson Educación.

[4] "Computer Networking: A Top-Down Approach" por James F. Kurose y Keith W. Ross

[5] Cisco Systems, Inc. Cisco Networking Academy Program, CCNA 1 y CCNA 2.

[6] TechTarget. (s.f.). What is File Transfer Protocol (FTP)?. Recuperado el 16 de mayo de 2023, de https://searchsecurity.techtarget.com/definition/File-Transfer-Protocol-FTP

[7] MySQL. (s.f.). MySQL 8.0 Reference Manual. Recuperado el 16 de mayo de 2023, de https://dev.mysql.com/doc/refman/8.0/en/

[8] McClure, S., Scambray, J., & Kurtz, G. (2009). Seguridad de redes. En Hacking Exposed: Network Security Secrets & Solutions (6.a ed.). McGraw-Hill Education.

[9] Gutiérrez, P. (2019). El libro blanco del HACKER (2.ª ed.). Ra-Ma.

[10] ISACA. (2019). COBIT 2019 Framework: Introduction and Methodology. Recuperado de https://www.isaca.org/-/media/isaca/cobit/cobit-2019/overview-and-introduction/overview-and-introduction-of-cobit-2019-framework.pdf

[11] Al-Shehri, S., Khan, M. K., Al-Wabil, A., & Al-Dossari, H. (2014). Physical Security Threats in Data Centers: A Case Study of Saudi Arabia. In 2014 9th International Conference for Internet Technology and Secured Transactions (ICITST)

[12] Fernández, D., & Bernal, D. (2019). Seguridad lógica en redes: conceptos y mejores prácticas. Revista Avances en Sistemas e Informática

[13] Ramírez, J. A., & Zavaleta, E. (2018). Seguridad Lógica en Redes de Datos. Revista Ciencia e Ingeniería Neogranadina,

[14] Kendrick, T. (2016). The Project Management Tool Kit: 100 Tips and Techniques for Getting the Job Done Right (3rd ed.). AMACOM.

[15] Papp, L., & Varga, A. (2014). Traffic Analysis. En Traffic Analysis and Design of Wireless IP Networks (p. 1-13). Springer International Publishing

[16] ITU-T. (1991). ITU-T Recommendation X.800: Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Overview

[17] Stallings, W. (2004). Fundamentos de Seguridad en Redes, Aplicaciones y Estándares. Pearson.

[18] International Telecommunication Union. (1991). X.800: Security architecture for Open Systems Interconnection for CCITT applications. Disponible en https://www.itu.int/rec/T-REC-X.800-199103-I/es

[19] Lyon, G. F. (2009). Nmap Network Scanning: The Official Nmap Project Guide. San Francisco, CA: Insecure.Com LLC.

[20] (2011) Metasploit: The Penetration Tester's Guide" por David Kennedy, Jim O'Gorman, Devon Kearns y Mati Aharoni.

Referencias Capítulo 3

[1] Raspberry Pi Foundation. (s.f.). Raspberry Pi. https://www.raspberrypi.org/

[2] Kali Linux. (s.f.). Home of Kali Linux, an Advanced Penetration Testing Linux distribution used for Penetration Testing, Ethical Hacking and network security assessments. https://www.kali.org/

[3] Oracle. (s.f.). VirtualBox. https://www.virtualbox.org/