Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Dayan Stiven Solarte Lara

Asesor

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de ciencias básicas, tecnología e ingeniería - ECBTI

Especialización en seguridad informática

Popayán

2024

Resumen

El presente informe técnico recopila y sintetiza las actividades realizadas durante el seminario especializado en ciberseguridad, con un enfoque práctico y teórico en las tareas de Red Team y Blue Team. Este documento aborda conceptos fundamentales de seguridad informática, la importancia de la actuación ética y legal en las prácticas de pentesting, así como la ejecución de laboratorios orientados a la identificación y mitigación de vulnerabilidades en entornos controlados. Cada sección del informe refleja los aprendizajes y estrategias aplicadas para fortalecer la postura de seguridad de una organización en escenarios realistas de ciberataques.

Primeramente se desarrollaron los conceptos básicos de seguridad, abarcando principios como la confidencialidad, integridad y disponibilidad de la información. Además, se analizó el uso de herramientas y metodologías necesarias para realizar evaluaciones de seguridad efectivas.

Así mismo, se analiza la actuación ética y legal, destacando la importancia de cumplir con normativas nacionales e internacionales y la responsabilidad de los especialistas en ciberseguridad de garantizar la protección de los sistemas sin exceder los límites éticos.

Para finalizar, el informe presenta un laboratorio práctico donde se ejecuta un ataque controlado utilizando herramientas virtuales para explotar vulnerabilidades en un sistema. Además, se documentan estrategias para la contención de ataques informáticos, como el uso de firewalls, sistemas de detección de intrusos, y hardenización de sistemas. Estas estrategias buscan mitigar riesgos y fortalecer la infraestructura tecnológica, proporcionando recomendaciones concretas para garantizar la seguridad operativa de la organización.

Tabla de contenido

Lista de imágenes

Lista de tablas

1 Glosario

Blue Team: equipo responsable de la defensa activa de los sistemas y redes de una organización, enfocándose en prevenir, detectar y responder ante amenazas de ciberseguridad

Ciberseguridad: conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas informáticos, redes, y datos frente a accesos no autorizados, ataques cibernéticos y daños

Exploit: código o programa diseñado para aprovechar una vulnerabilidad informática con el fin de ejecutar acciones no autorizadas en un sistema

Firewall: dispositivo o software perimetral que filtra y controla el tráfico de red según reglas predefinidas, bloqueando accesos no autorizados y protegiendo la infraestructura de amenazas externas e internas

Hardenización: proceso de asegurar y fortalecer sistemas y aplicaciones mediante la eliminación de configuraciones inseguras, servicios innecesarios y vulnerabilidades conocidas

Pentesting: pruebas de penetración realizadas para identificar y explotar vulnerabilidades en sistemas, aplicaciones o redes, con el objetivo de evaluar su nivel de seguridad

Red Team: equipo que simula ataques reales para identificar vulnerabilidades en la infraestructura de una organización y evaluar la efectividad de las medidas de seguridad implementadas

Vulnerabilidad informática: debilidad o fallo en un sistema, aplicación o red que puede ser aprovechado por un atacante para comprometer la seguridad de la información o los servicios

2 Introducción

En un mundo cada vez más interconectado, la ciberseguridad se ha convertido en un componente esencial para proteger la información y los activos críticos de las empresas frente a un panorama creciente de amenazas cibernéticas. Las organizaciones enfrentan riesgos constantes, como robo de datos, interrupción de servicios y violaciones de privacidad, que pueden afectar su operación, reputación y sostenibilidad. En este contexto, los equipos Red Team y Blue Team desempeñan un papel fundamental: el primero, simulando ataques para identificar vulnerabilidades y evaluar la capacidad de respuesta de la organización, y el segundo, implementando estrategias de defensa y contención para mitigar los riesgos identificados. Este enfoque dual permite fortalecer la postura de seguridad de las empresas, alineando los esfuerzos ofensivos y defensivos en una estrategia integral. Este informe técnico documenta actividades prácticas y teóricas que ilustran cómo ambos equipos trabajan en conjunto para garantizar la protección de los sistemas, reflejando la importancia de combinar conocimientos técnicos, medidas preventivas y principios éticos en la gestión de la ciberseguridad empresarial.

3 Objetivos

3.1 Objetivo general

Realizar un informe técnico sobre el desarrollo de las fases del seminario especializado, con el fin de proponer estrategias de fortalecimiento en las infraestructuras informáticas, que permitan la contención y mitigación de ciberataques.

3.2 Objetivos específicos

- Analizar los conceptos básicos de los equipos de seguridad, mediante el conocimiento de la actuación ética y legal en el ámbito de la ciberseguridad, así como el uso de herramientas virtuales para la ejecución de pruebas de pentesting
- Ejecutar en un entorno controlado, las etapas de un proceso de pentesting, demostrando el paso a paso de la actuación de un equipo Red Team
- Proponer estrategias de endurecimiento de sistemas de ciberseguridad, que mediante un equipo Blue Team se permita contener o mitigar ciberataques en una organización

4 Desarrollo del informe

4.1 Conceptos equipos de seguridad

4.1.1 Actuación legal

Dentro del margen colombiano, existen varias leyes y decretos que buscan proteger los datos personales ante delitos informáticos, dentro de las principales normas se encuentran:

4.1.1.1 Ley 1273 de 2009 - Delitos Informáticos

Esta ley modifica el Código Penal colombiano y tipifica los delitos informáticos. Su objetivo es proteger la información y los datos almacenados en sistemas informáticos (Pública, 2009)

Principales características

- Crea el concepto de "bien jurídico" sobre la protección de la información.
- Establece delitos como el acceso abusivo a un sistema informático, la interceptación de datos, daño informático, uso de software malicioso, y suplantación de identidad.
- Establece sanciones penales que pueden incluir prisión, dependiendo de la gravedad del delito.

4.1.1.2 Ley 1581 de 2012 - Protección de Datos Personales

Esta ley establece el marco general para la protección de datos personales en Colombia. Su finalidad es garantizar que las personas puedan controlar la manera en que sus datos son recolectados, almacenados, usados, y compartidos (Pública, Función Pública, 2012)

Principales características

- Define qué se entiende por "datos personales" y clasifica los datos en categorías: públicos, semiprivados, privados y sensibles

- Establece los derechos de los titulares de los datos, como el derecho a conocer, actualizar y rectificar su información
- Introduce el principio de consentimiento, donde los responsables del tratamiento de datos deben obtener la autorización previa del titular
- Crea la Superintendencia de Industria y Comercio (SIC) como el organismo encargado de vigilar el cumplimiento de la ley

4.1.1.3 Decreto 1377 de 2013 - Reglamentación de la Ley 1581 de 2012

Este decreto reglamenta aspectos operativos de la Ley 1581 de 2012 y establece cómo las empresas y organizaciones deben tratar los datos personales (Pública, Función Pública, 2013)

Principales características

- Detalla cómo se debe solicitar la autorización para tratar datos personales
- Establece los mecanismos para que los titulares de los datos ejerzan sus derechos
- Fija obligaciones para los responsables y encargados del tratamiento de datos en cuanto a la implementación de medidas de seguridad

4.1.1.4 Ley 1928 de 2018 - Convenio de Budapest

Colombia ratifica el Convenio de Budapest sobre ciberdelincuencia, que busca fortalecer la cooperación internacional en la lucha contra los delitos cibernéticos (REPÚBLICA, 2018)

Principales características

- Fomenta la colaboración entre países para investigar y sancionar delitos cibernéticos
- Establece normas comunes para la recolección de evidencia electrónica
- Ayuda a combatir delitos como la pornografía infantil, fraudes en línea, ataques contra sistemas informáticos, y violación de derechos de autor en internet

4.1.1.5 Ley 2014 de 2020 - Delitos informáticos contra menores

Modifica el Código Penal para proteger a menores de edad en entornos digitales, creando sanciones más severas para los delitos cibernéticos que los afecten (MIRA, 2024)

Principales características

- Penaliza conductas como el "grooming" (acoso sexual a menores en línea) y la difusión de material pornográfico con participación de menores
- Refuerza la cooperación entre entidades para prevenir y combatir la explotación infantil en el ámbito digital

4.1.2 Pentesting

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting, dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting

El "Pentesting" o pruebas de penetración son evaluaciones de seguridad diseñadas para identificar vulnerabilidades en sistemas informáticos, redes, aplicaciones o infraestructuras mediante la simulación de ataques reales (Laprovittera, 2024). El objetivo de estas pruebas es descubrir y corregir debilidades en estas infraestructuras antes de que puedan ser explotadas por ciberdelincuentes o actores maliciosos. Este proceso suele ser llevado a cabo por equipos especializados (Red Teams) que simulan el comportamiento de los atacantes

4.1.3 Etapas del pentesting

El proceso de pentesting se divide en las siguientes etapas:

4.1.3.1 Etapa 1: Reconocimiento

Esta etapa inicial consiste en recopilar información sobre el objetivo. Existen dos tipos:

- Reconocimiento activo: El atacante interactúa directamente con el sistema objetivo, por ejemplo, mediante escaneos.
- Reconocimiento pasivo: Se recopila información sin interactuar directamente con el objetivo, usando fuentes públicas como bases de datos, redes sociales, etc

Herramienta

Maltego: es una herramienta útil para la recolección de información pasiva, permitiendo explorar relaciones en redes, dominios, personas, etc

4.1.3.2 Etapa 2: Escaneo

En esta etapa, se exploran los sistemas y redes para identificar puntos de acceso y vulnerabilidades específicas que pueden ser explotadas. El objetivo es detectar puertos abiertos, servicios activos, sistemas operativos y vulnerabilidades en estos sistemas

Herramienta

- **Nmap**: es una de las herramientas más populares en ciberseguridad para escanear redes y detectar servicios, puertos abiertos, y obtener detalles del sistema

4.1.3.3 Etapa 3: Enumeración y explotación

Después del escaneo, los pentesters intentaran explotar vulnerabilidades encontradas. Esta fase incluye el uso de exploits, técnicas de escalamiento de privilegios, y la explotación de fallos de seguridad en sistemas o aplicaciones

Herramienta

- **Metasploit**: es una plataforma de explotación ampliamente utilizada que permite realizar pruebas y ejecutar exploits para comprometer sistemas

4.1.3.4 Etapa 4: Mantenimiento del Acceso

Una vez que los pentesters logren acceder a la infraestructura, trataran de mantener el acceso al sistema durante el mayor tiempo posible para simular cómo un atacante podría persistir dentro de un sistema comprometido sin ser detectado. Esto puede incluir la instalación de puertas traseras (backdoors)

Herramienta

- **Cobalt Strike**: esta herramienta permite simular cómo mantener el acceso en un sistema comprometido, siendo muy útil para la persistencia y post-explotación

4.1.3.5 Etapa 5: Limpieza y Cierre

En esta fase, los pentesters eliminan cualquier evidencia de su actividad, como registros (logs) de sistema, archivos o accesos. Esto simula cómo los atacantes intentan borrar su rastro. Al final, se elabora un informe detallando los hallazgos y recomendaciones para corregir las vulnerabilidades encontradas (TECNEK, 2024)

Herramienta

- **Clearev (en Metasploit)**: un módulo dentro de Metasploit que permite limpiar rastros y registros del sistema

4.1.3.6 Etapa 6: Informe

Para finalizar el proceso de pentesting, se debe realizar un informe donde se detalle todos los hallazgos encontrados en las fases anteriores; describiendo las vulnerabilidades encontradas, los datos explotados y, demostrando el éxito del ataque simulado; proponiendo de esta manera recomendaciones que garanticen el endurecimiento de los sistemas vulnerables, todo esto con el fin de fortalecer los equipos, la red y toda la infraestructura del lugar ante posibles ataques de ciberseguridad.

4.1.4 Herramientas en ciberseguridad

Las herramientas de ciberseguridad son de vital importancia, además que existe un gran abanico de posibilidades de herramientas existentes y software especializado para desarrollar herramientas propias. Usted como futuro experto debe definir y explicar las siguientes herramientas:

4.1.4.1 Metasploit

Metasploit es una plataforma de pruebas de penetración que permite realizar exploits sobre vulnerabilidades conocidas, facilitando la tarea de pentesters y Red Teams. Es una de las herramientas más completas y populares para ataques y explotación de vulnerabilidades (CAMPUSCIBERSEGURIDAD, 2024)

Características

- Exploit Modules: incluye miles de módulos de explotación que permiten realizar ataques sobre diferentes tipos de sistemas y aplicaciones
- Payloads: permite insertar cargas útiles (payloads) como shell reverso o meterpreter para mantener acceso a los sistemas comprometidos
- Post-explotación: ofrece herramientas para explorar y mantener el control de los sistemas comprometidos
- Interfaz versátil: se puede utilizar a través de una interfaz gráfica (Armitage) o en modo de línea de comandos

4.1.4.2 Nmap

Nmap, (Network Mapper) es una herramienta de código abierto utilizada para el escaneo de redes y sistemas. Permite descubrir hosts y servicios en una red, identificando posibles puntos vulnerables (Jenifa, 2024)

Características

- Escaneo de puertos: Nmap permite identificar qué puertos están abiertos y qué servicios están siendo ejecutados en un host
- Detección de sistemas operativos: identifica el sistema operativo y versión que se ejecuta en los dispositivos escaneados
- Escaneos avanzados: ofrece opciones de escaneo de puertos específicos, detección de vulnerabilidades y scripts para pruebas adicionales mediante su motor NSE (Nmap Scripting Engine)

4.1.4.3 OpenVas

OpenVAS, (Open Vulnerability Assessment System) es una plataforma de análisis de vulnerabilidades de código abierto que permite detectar y gestionar vulnerabilidades en redes y sistemas (Cusi, 20024)

Características

- Escaneo de vulnerabilidades: permite detectar y evaluar vulnerabilidades conocidas en sistemas, utilizando una base de datos de vulnerabilidades actualizada
- Gestión de vulnerabilidades: ofrece reportes detallados con las vulnerabilidades encontradas y sus niveles de riesgo, facilitando la priorización de acciones correctivas
- Amplia cobertura: soporta una gran variedad de tipos de vulnerabilidades en sistemas operativos, redes, servidores y aplicaciones

Servicios en línea:

4.1.4.4 ExploitDB

Exploit Database, es una plataforma en línea que proporciona un repositorio de exploits verificados para diversas vulnerabilidades de software. Es una de las mayores bases de datos públicas de exploits y sirve como referencia para pruebas de seguridad (Cilleruelo, 2024)

Características

- Repositorio de exploits: contiene exploits para una amplia gama de aplicaciones, sistemas operativos y servicios vulnerables
- Colaboración comunitaria: es mantenido por la comunidad, con contribuciones regulares de investigadores y hackers éticos.
- Fácil búsqueda: los usuarios pueden buscar exploits específicos según el software, versión, tipo de vulnerabilidad, o fecha

4.1.4.5 CVE

El sistema CVE es una lista pública de vulnerabilidades de seguridad conocidas en software. Cada vulnerabilidad recibe un identificador único (CVE ID), que facilita la referencia y consulta en diferentes plataformas de seguridad (TARLOGIC, 2024)

Características

- Identificación única: cada vulnerabilidad tiene un código único (por ejemplo, CVE-2024-XXXX), facilitando su referencia en herramientas de análisis de vulnerabilidades y bases de datos
- Estándar global: es un estándar utilizado a nivel mundial, lo que permite a desarrolladores, administradores de sistemas y profesionales de seguridad hablar un lenguaje común sobre vulnerabilidades

- Vinculación con bases de datos: herramientas como OpenVAS o Metasploit están directamente vinculadas con la base de datos de CVE, lo que permite explotar o corregir vulnerabilidades de forma rápida

4.1.5 Banco de trabajo

Para finalizar esta actividad es importante que usted reconozca, analice y configure "banco de trabajo" lo solicitado en el anexo 1 – Escenario 1 sobre el cual deberá trabajar actividades que contienen un alto grado de tecnicidad. Lo solicitado en el anexo 1 – escenario 1 es lo siguiente:

4.1.5.1 Paso A:

Descargar la herramienta virtualizadora "VirtualBox" en su última versión

Imagen 1
VirtualBox

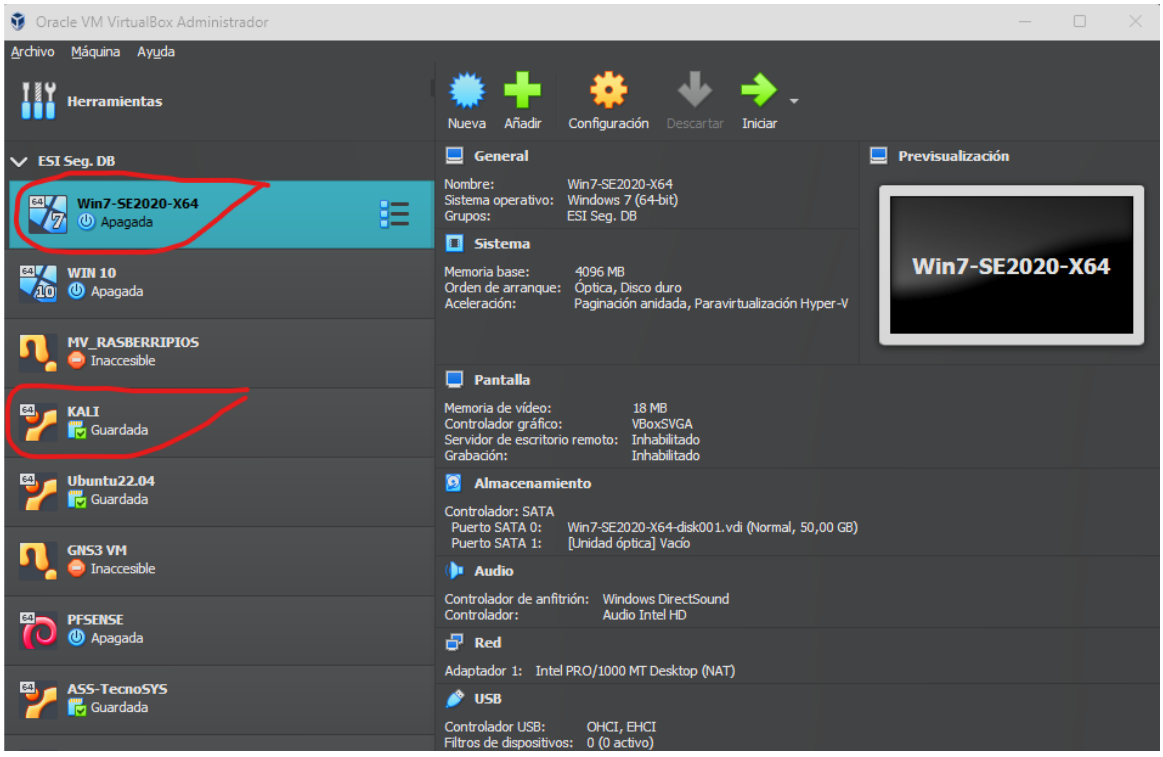
Nota. Fuente: autoría propia

Sistema Virtual Box instalado y operativo

4.1.5.2 Paso B:

Una vez se realice apertura del foro para el desarrollo de la actividad se procederá a compartir enlace de descarga de lo requerido para el montaje del banco de trabajo, las imágenes en formato. OVA las cuales se encuentran ya preconfiguradas para ser utilizadas en las actividades de carácter técnico. En las imágenes. OVA existe: Un sistema operativo windows y un sistema operativo Kali Linux

Imagen 2
Banco de Trabajo



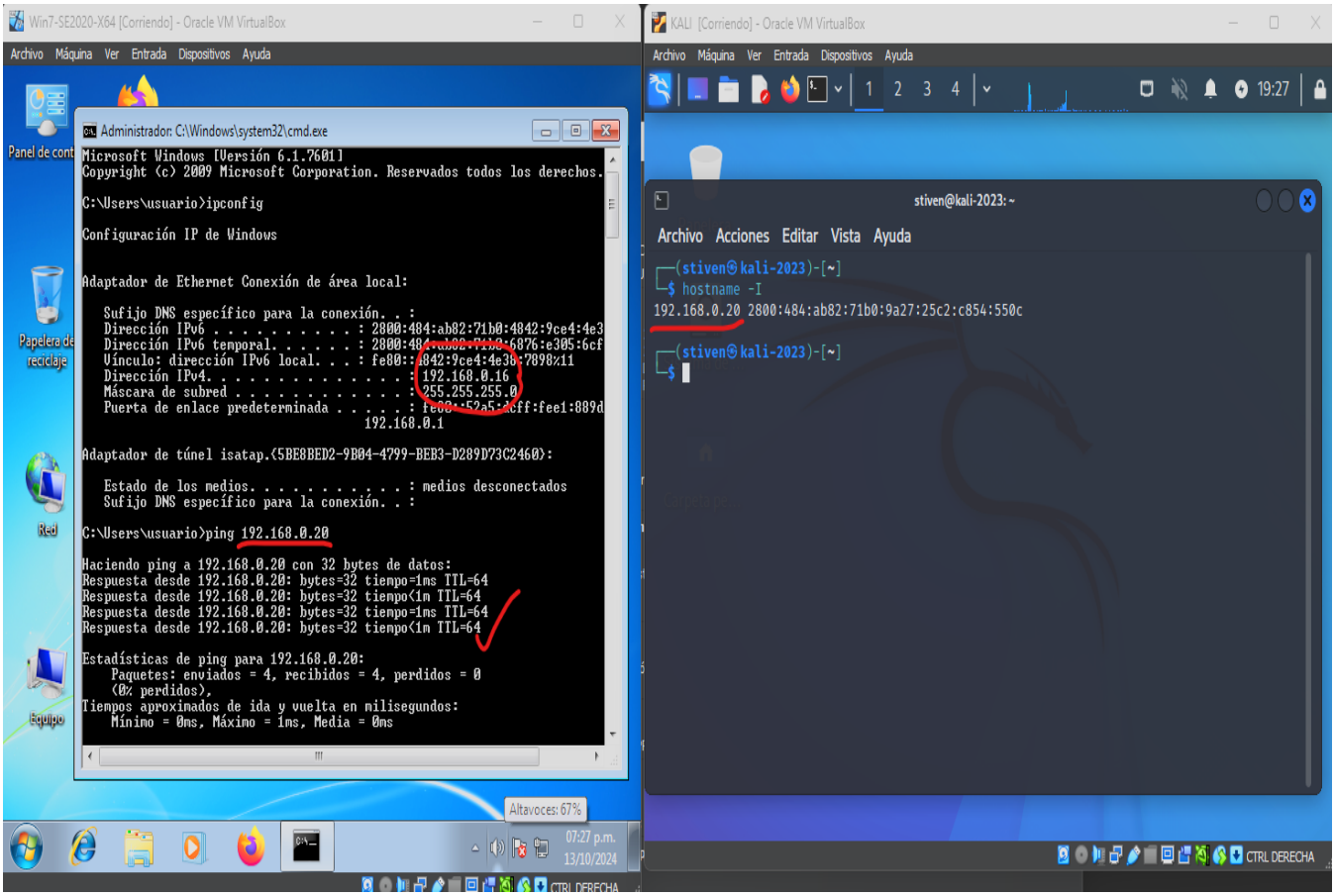
Nota. Fuente autoría propia

Sistemas operativos Kali Linux y Windows 7 instalados correctamente en VM

4.1.5.3 Paso C:

Debe validar que exista comunicación entre cada una de las máquinas Windows con la máquina de Kali Linux, recuerde por favor no encender las tres máquinas al tiempo ya que puede colapsar los recursos hardware de su equipo host, encienda primero una máquina Windows y posterior a ello encienda la máquina Kali Linux

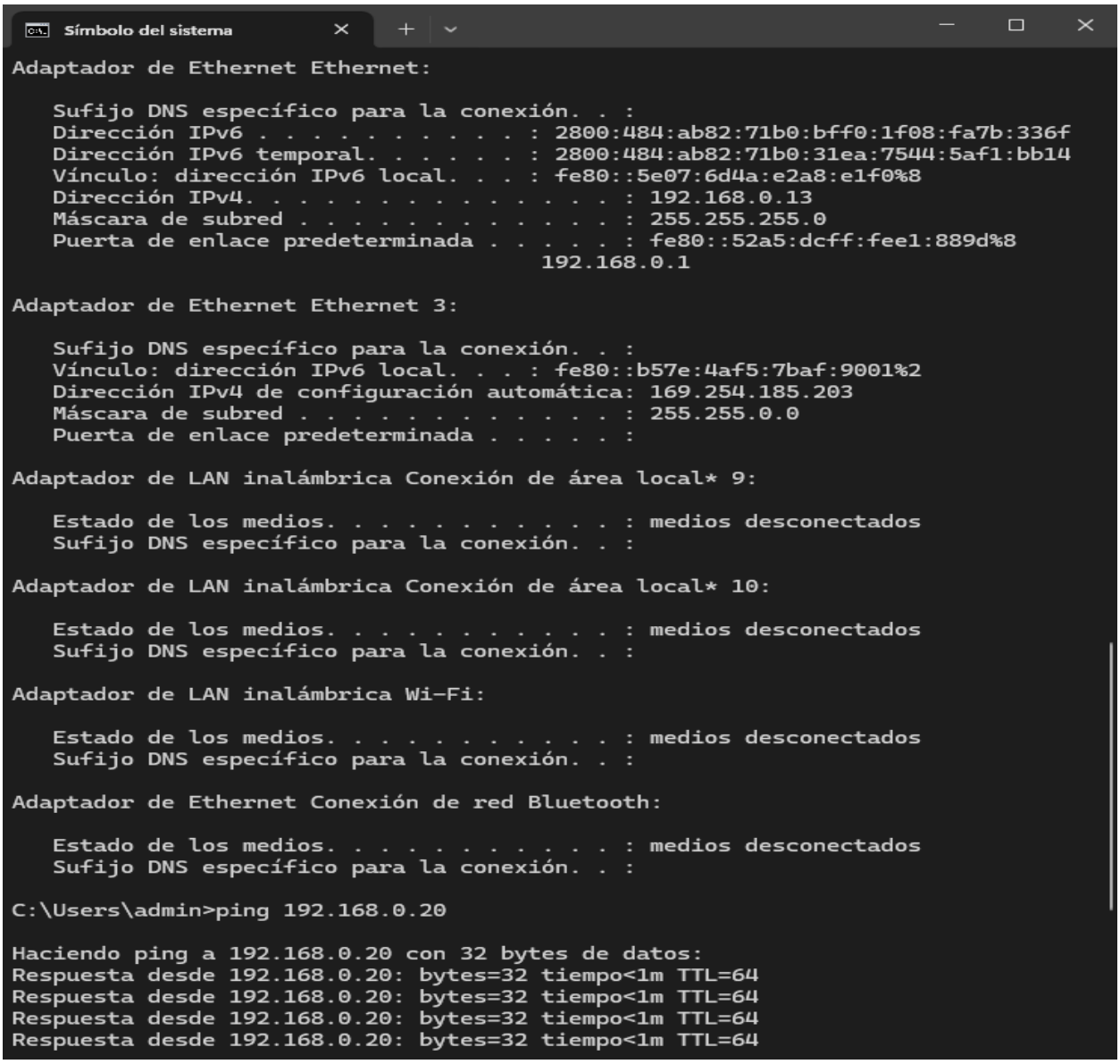
Imagen 3
Windows 7 Direccionamiento IP - PING



Nota. Fuente: autoría propia

Se valida en el direccionamiento IP del sistema operativo Windows 7 (192.168.0.16); así mismo se valida conexión hacia la maquina Kali Linux (192.168.0.20), mediante el comando ping y la dirección IP del host

Imagen 4
PC anfitrión Direccionamiento IP – PING



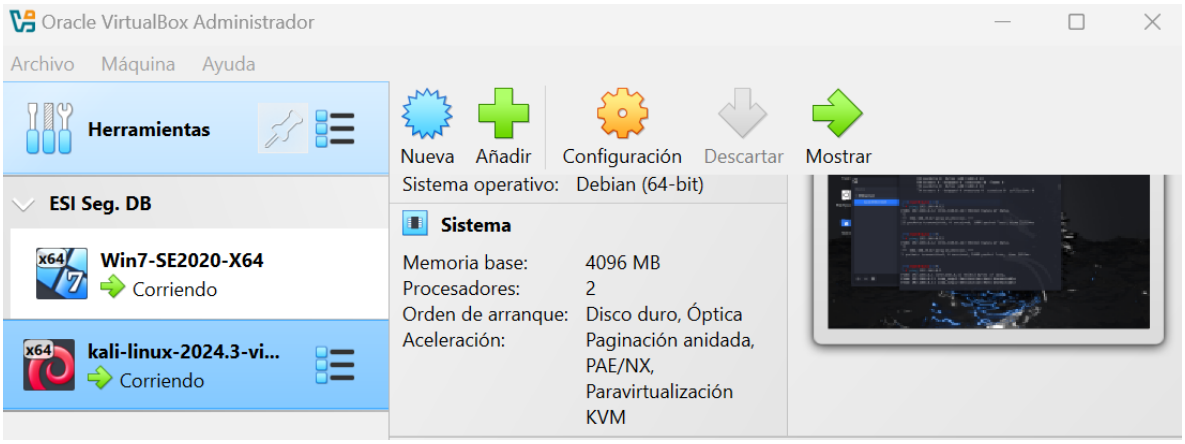
Nota. Fuente: autoría propia

Se valida direccionamiento IP del sistema operativo Anfitrión (192.168.0.13); asi mismo se valida conexión hacia la maquina Kali Linux (192.168.0.20), mediante el comando ping y la dirección IP del host

4.2 Proceso de un pentesting

El presente laboratorio, se ejecuta en un entorno controlado mediante del uso de herramientas virtuales. Dentro la herramienta de Virtual Box, se instala los sistemas operativos requerido para la práctica, los cuales son: Kali Linux, en versión 2024.3 como sistema operativo *atacante* y Windows 7 como sistema operativo *víctima*.

Imagen 5 Virtual box

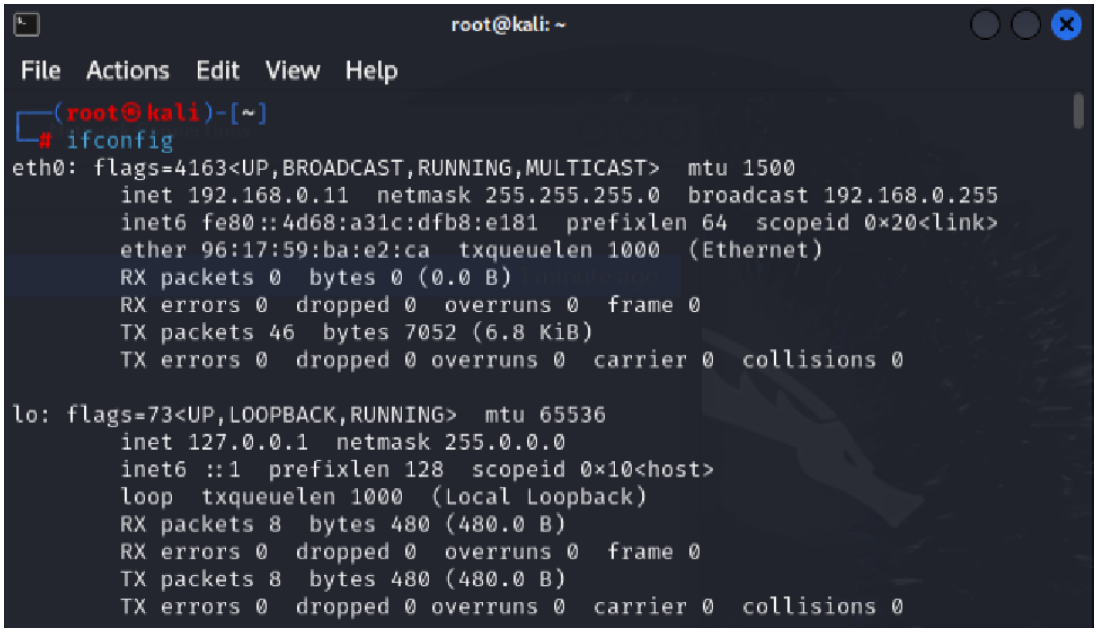


Nota. Fuente: autoría propia

Los hosts se encuentran en el mismo segmento de red, el direccionamiento configurado en las máquinas virtuales es el siguiente:

- Kali Linux: 192.168.0.11

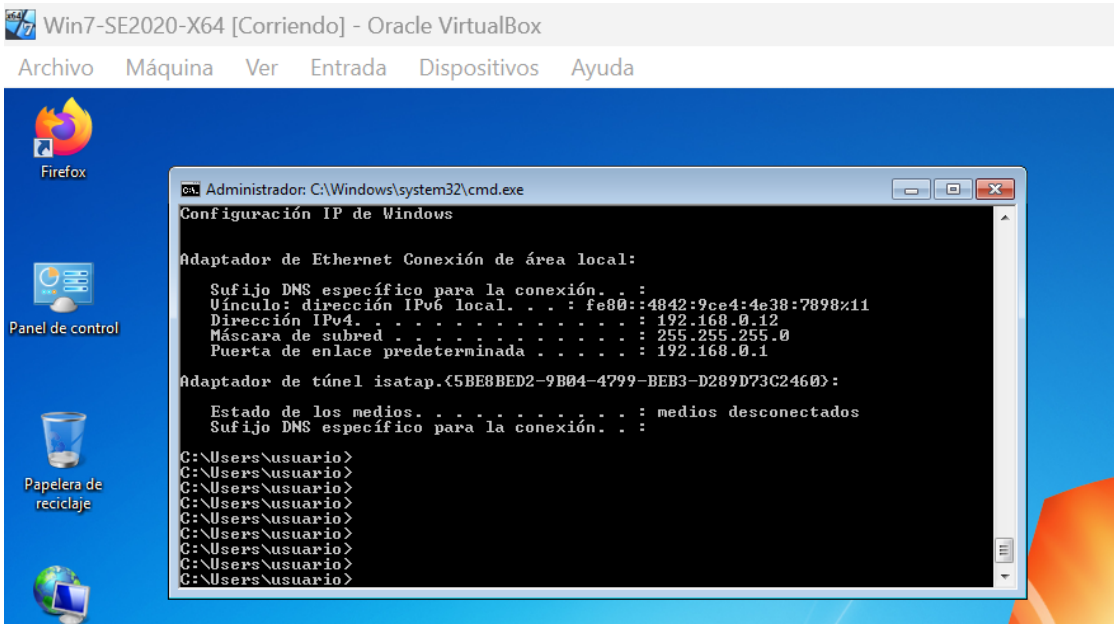
Imagen 6 Direccionamiento IP - Kali Linux



Nota. Fuente: autoría propia

- Windows 7: 192.168.0.12

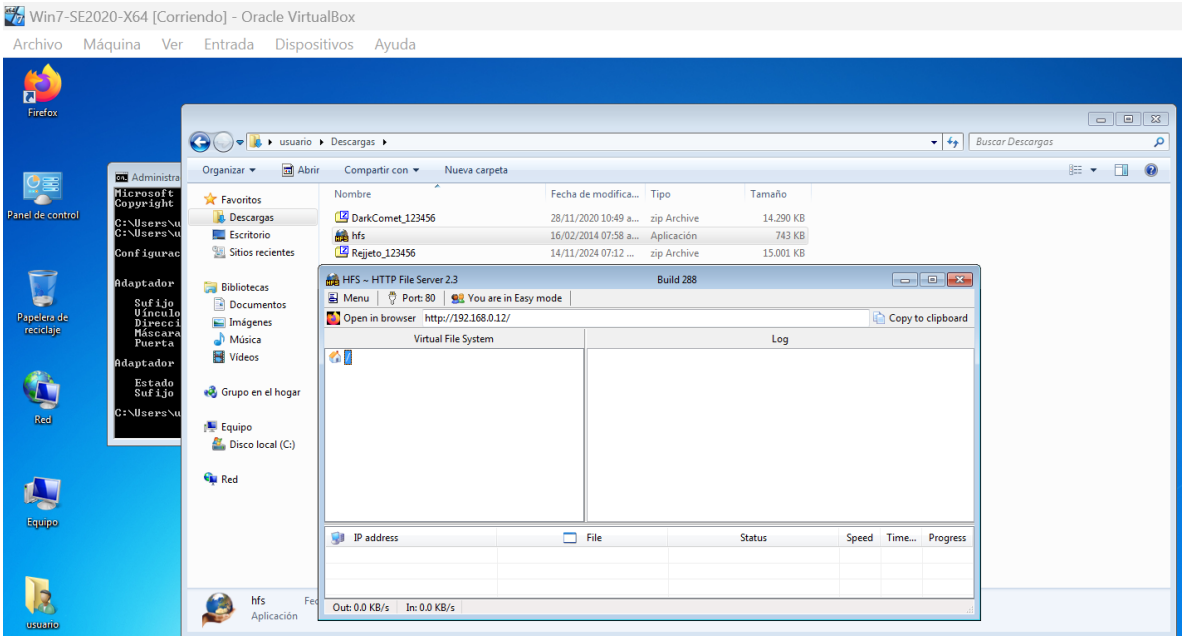
Imagen 7 Direccionamiento IP - Windows 7



Nota. Fuente: autoría propia

Igualmente se instala y ejecuta la aplicación HFS en el SO de Windows 7, la cual presenta un fallo de seguridad:

Imagen 8 HFS en Windows 7



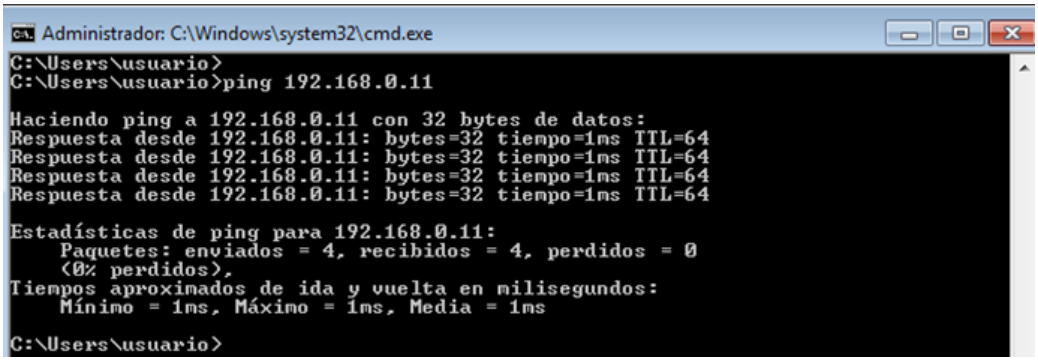
Nota. Fuente: autoría propia

4.2.1 Etapas del Pentesting

4.2.1.1 Etapa 1: Reconocimiento

Esta etapa inicial consiste en recopilar información sobre el objetivo. Para validar este reconocimiento en las maquinas debe haber conexión entre estas, por lo cual se realiza un ping desde la maquina *víctima* W7 192.1680.12 hacia la maquina *atacante* Kali 192.168.11

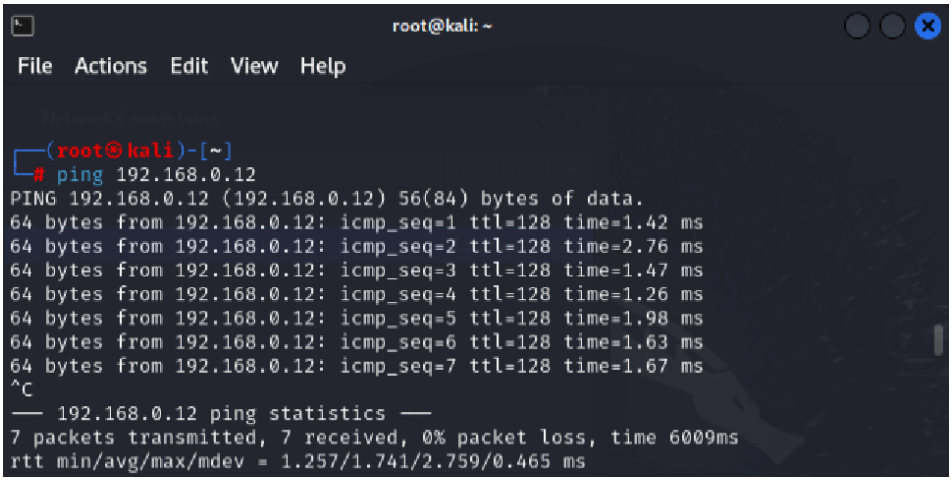
Imagen 9 Ping hacia Kali Linux



Nota. Fuente: autoría propia

Igualmente se valida conexión desde la maquina *atacante* Kali 192.168.0.11, hacia la maquina *victima* W7 192.168.0.12

Imagen 10 Ping hacia Windows 7



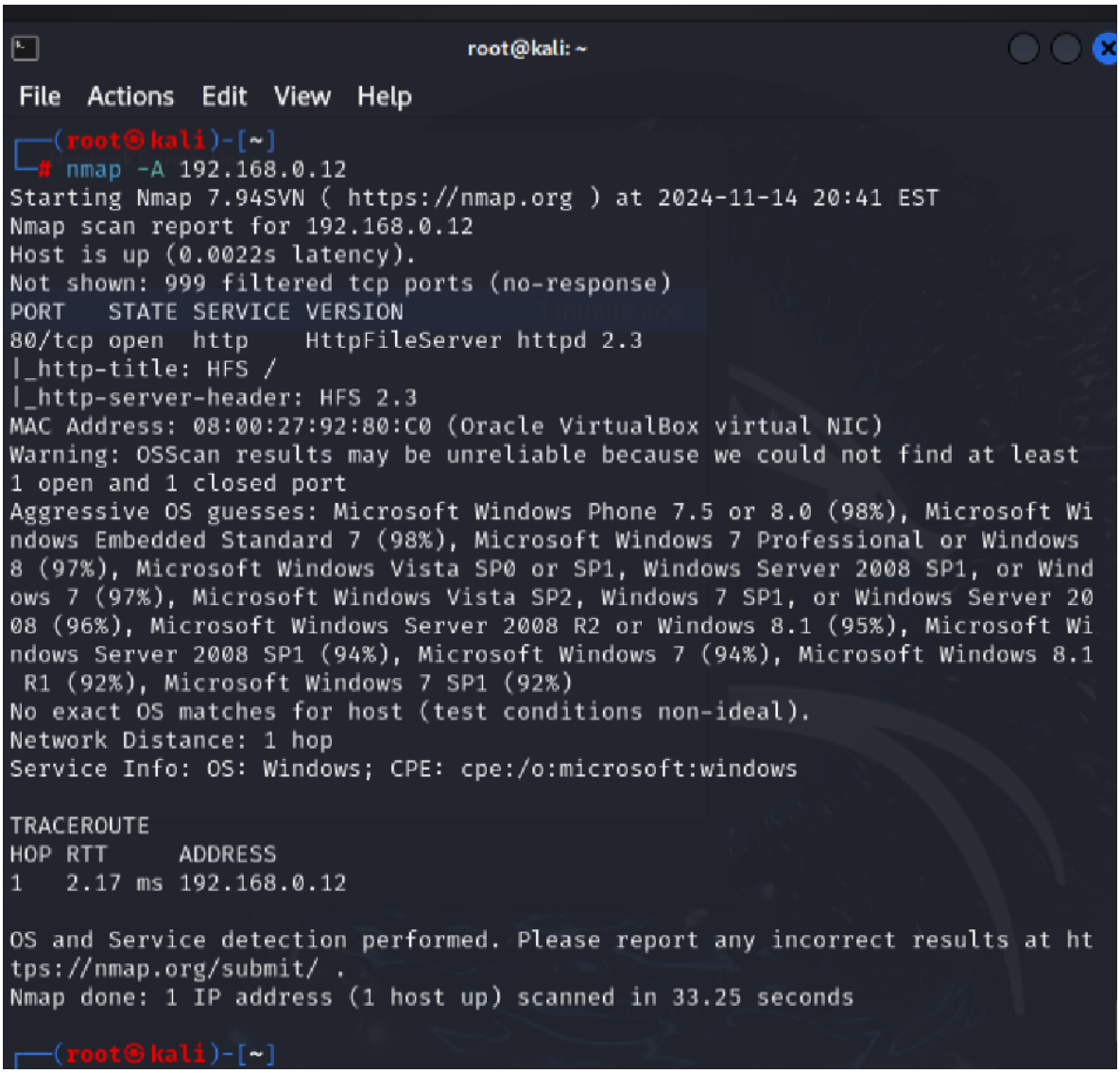
Nota. Fuente: autoría propia

4.2.1.2 Etapa 2: Escaneo

En esta etapa, se exploran los sistemas y redes para identificar puntos de acceso y vulnerabilidades específicas que pueden ser explotadas. El objetivo es detectar puertos abiertos, servicios activos, sistemas operativos y vulnerabilidades en estos sistemas, esto se realiza dentro de la maquina atacante mediante la herramienta **nmap**, la cual ya viene por instalada en el SO.

A continuación para comenzar el escaneo, se escribe el comando: *nmap -A 192.168.0.12*, esto con el fin de solicitar que se ejecute un escaneo hacia el host víctima.

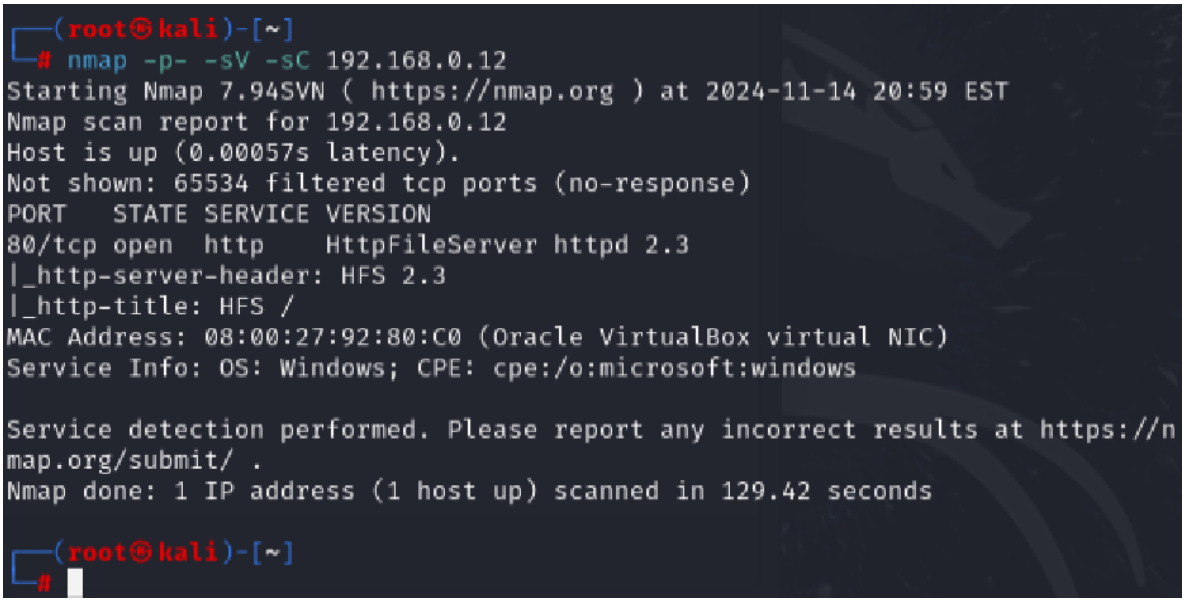
Imagen 11 nmap -A 192.168.0.12



Nota. Fuente: autoría propia

Para solicitar un escaneo más profundo del sistema, donde se detecte servicios detallados, versiones, puertos abiertos y posibles vulnerabilidades, se ejecuta el comando: *nmap -p- -sV -sC 192.168.0.12*

Imagen 12 nmap -p- -sV -sC 192.168.0.12



Nota. Fuente: autoría propia

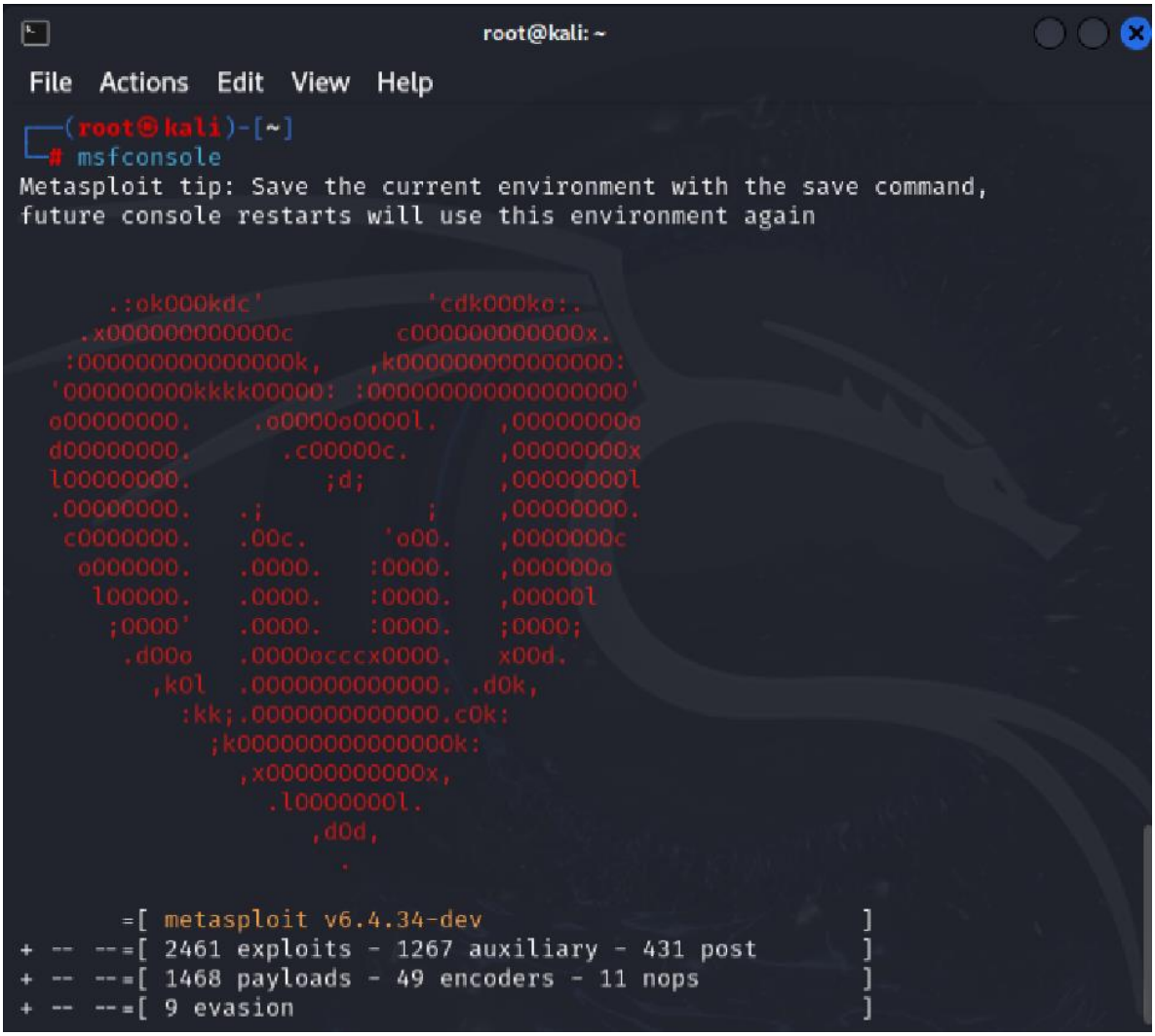
Como resultado de este escaneo se puede evidenciar la información que arroja, como el sistema operativo, la dirección MAC, y los puertos y servicios arriba, como lo es el puerto 80, por donde se está ejecutando el servicio HFS, versión 2.3

4.2.1.3 Etapa 3: Enumeración y explotación

Después del escaneo, se intentará explotar vulnerabilidades encontradas. Esta fase incluye el uso de exploits, técnicas de escalamiento de privilegios, y la explotación de fallos de seguridad en sistemas o aplicaciones. El objetivo es aprovechar la vulnerabilidad en HFS para obtener acceso no autorizado.

Teniendo la información recopilada anteriormente, sobre los puertos y servicios abiertos, se procede a ejecutar la herramienta requerida para esta fase, la cual es Metasploit, mediante el comando: *msfconsole*

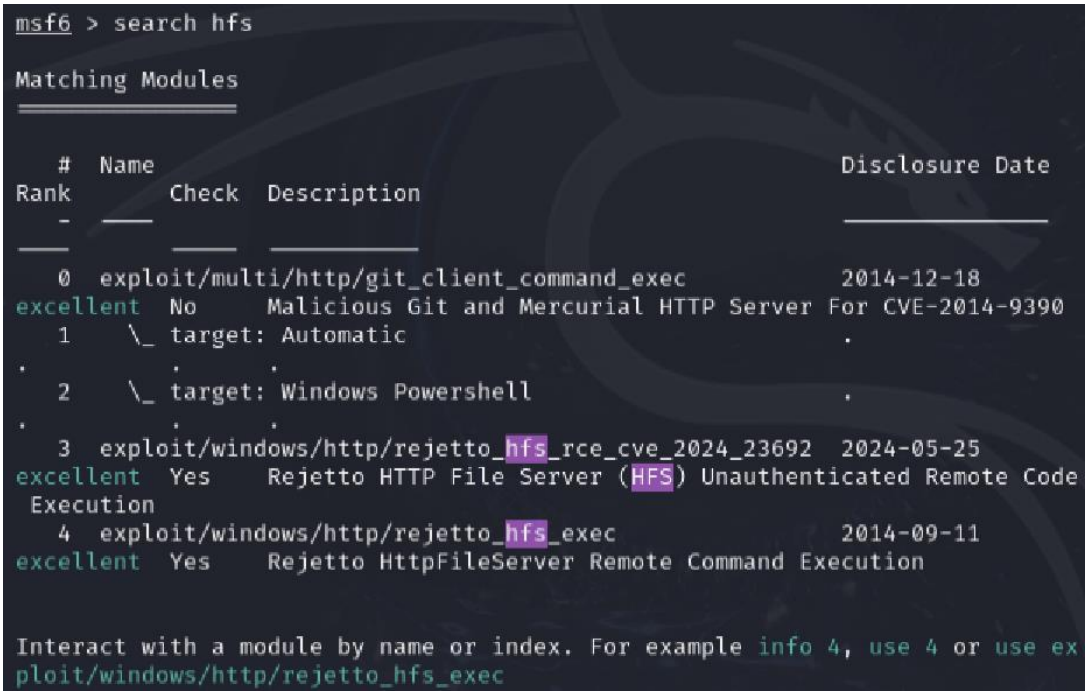
Imagen 13 Metasploit



Nota. Fuente: autoría propia

Para buscar un exploit que aproveche la vulnerabilidad encontrada, se realiza una búsqueda dentro de Metasploit, buscando una palabra relacionada con el servicio. Para este caso se ejecuta el comando: *search hfs*

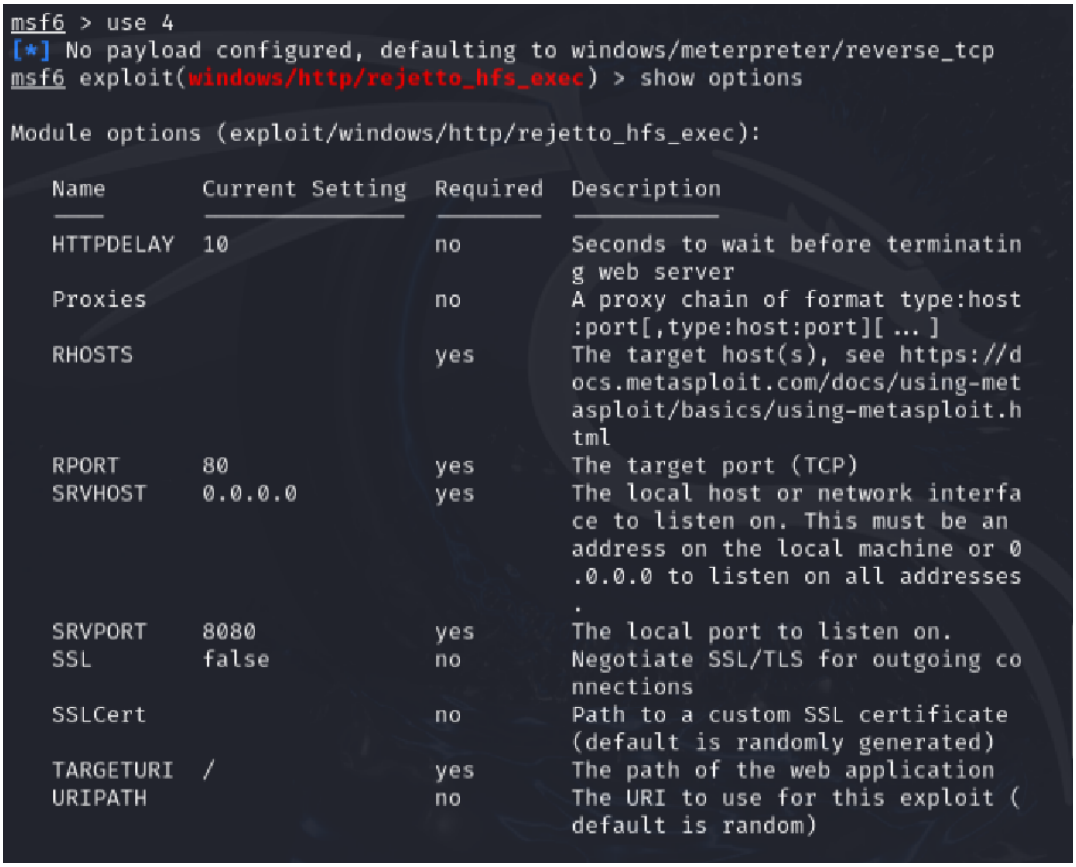
Imagen 14 Search hfs



Nota. Fuente: autoría propia

Se puede validar que se han encontrado varios exploits para HFS, para este caso se utilizará el número 4, por lo que se ingresa el comando: *use 4* que permitirá ingresar en el exploit, para agregar los datos solicitados de la víctima.

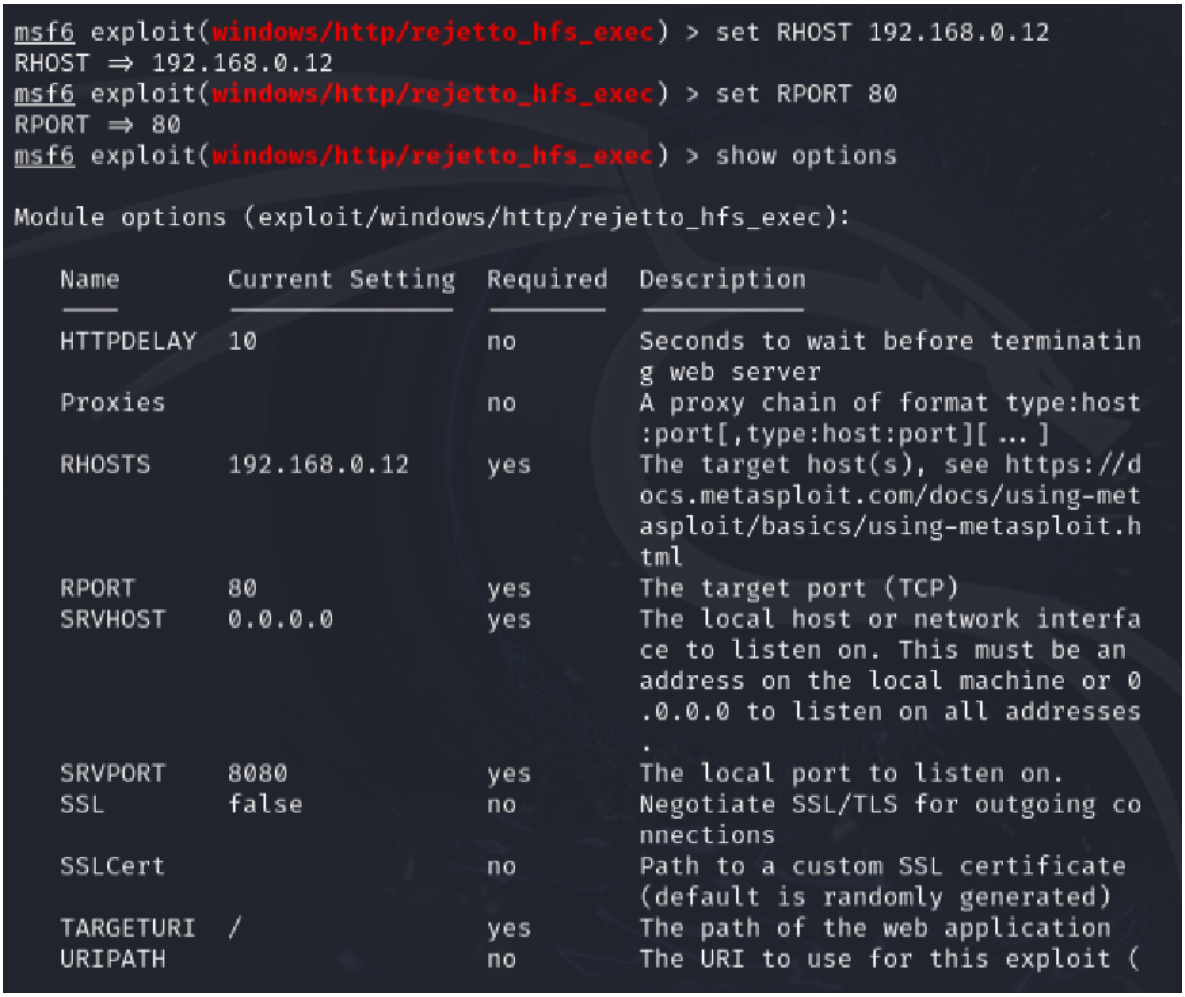
Imagen 15 Ingreso al exploit



Nota. Fuente: autoría propia

Se configura en el exploit, el direccionamiento IP de la maquina victima 192.168.0.12 así como el puerto 80, mediante el comando: *set RHOST 192.168.0.12* y set *RPORT 80*

Imagen 16 Configuración de exploit 1

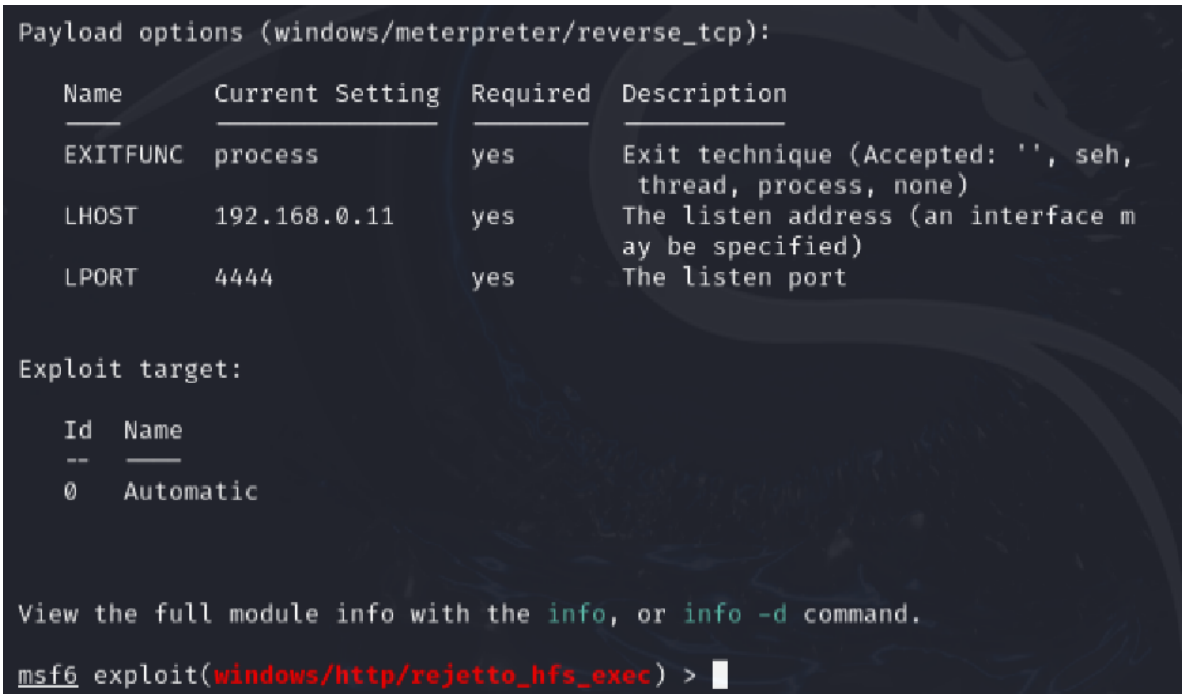


Nota. Fuente: autoría propia

Se valida que la información agregada sea la deseada, mediante el comando: *show options*

Igualmente se valida que este configurada la dirección IP y el puerto desde donde se lanzara el ataque, como lo es el LHOST y el LPORT

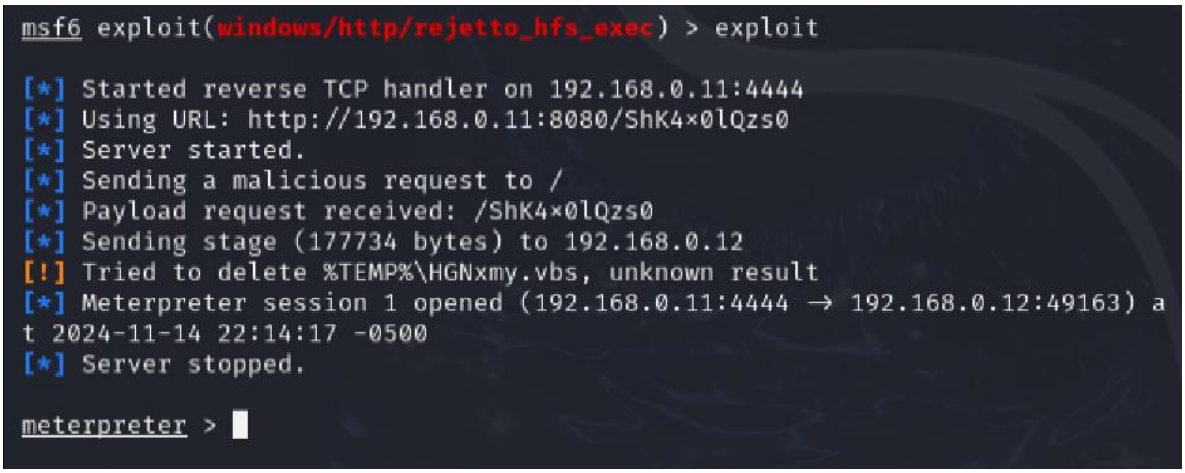
Imagen 17 Configuración de exploit 2



Nota. Fuente: autoría propia

Teniendo todo configurado, se solicita ejecutar el exploit mediante el comando: *exploit*

Imagen 18 Correr exploit



Nota. Fuente: autoría propia

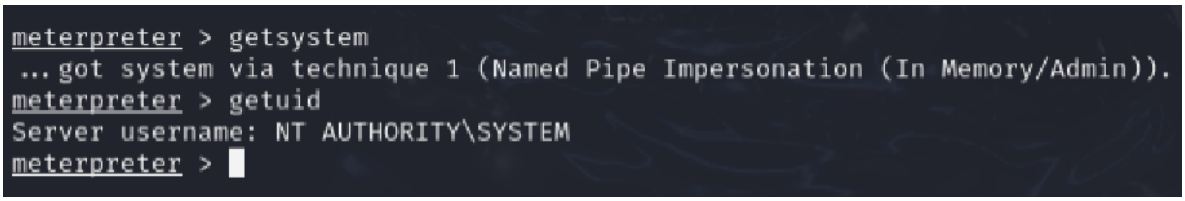
Se puede validar que el exploit es exitoso mediante una sesión establecida “meterpreter”, lo que nos indica que ya estamos dentro de la maquina victima Windows 7.

4.2.1.4 Etapa 4: Post Explotación

Una vez que se logre acceder a la infraestructura (maquina víctima – Windows 7) se valida el acceso obtenido y se evalúa el impacto, tratando de mantener el acceso al sistema durante el mayor tiempo posible sin ser detectado. Esto puede incluir la instalación de puertas traseras (backdoors).

A continuación a manera de ejemplo se asignan permisos de administrador al usuario, para escalar privilegios dentro del sistema, mediante el comando: *getsystem*

Imagen 19 Getsystem



Nota. Fuente: autoría propia

Al adquirir privilegios de administrador o "root", el atacante puede modificar configuraciones críticas, desactivar medidas de seguridad, o instalar malware persistente. Escalar privilegios facilita establecer mecanismos para mantener el acceso a largo plazo, incluso si el sistema es reiniciado o parcialmente reparado.

4.2.2 Detalles del anexo 4 – escenario 3

A continuación, se describe los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows

La información de importancia que arroja el anexo 4 - escenario 3, es la siguiente:

- Equipo terminal de trabajo con sistema operativo Windows 7
- Fuga de información en un equipo Windows 7
- Aplicación vulnerable Rejetto instalada en la maquina Windows 7
- Aplicación que permitiría ejecutar un exploit para realizar un acceso a través de Shell, escalamiento de privilegios u otro tipo de ataque.

4.2.3 Herramientas utilizadas

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la "máquina Windows"? ¿Qué puerto abre la aplicación específica en el anexo?

Para identificar los fallos de seguridad de la máquina Windows, se utilizó **Nmap** como herramienta principal de escaneo. Esta herramienta permitió realizar un análisis detallado de los puertos y servicios activos en la máquina víctima, identificando específicamente el puerto utilizado por la aplicación vulnerable.

La aplicación Rejetto HFS (HTTP File Server) por defecto abre el **puerto 80**, utilizado para servir archivos a través del protocolo HTTP. Durante el análisis con Nmap, se detectó que este puerto estaba abierto y asociado al servicio HTTP, lo que confirmó que la aplicación estaba en ejecución y susceptible a ser explotada debido a sus vulnerabilidades conocidas.

4.2.4 ¿Cómo afecta el ataque a la máquina (Windows)?

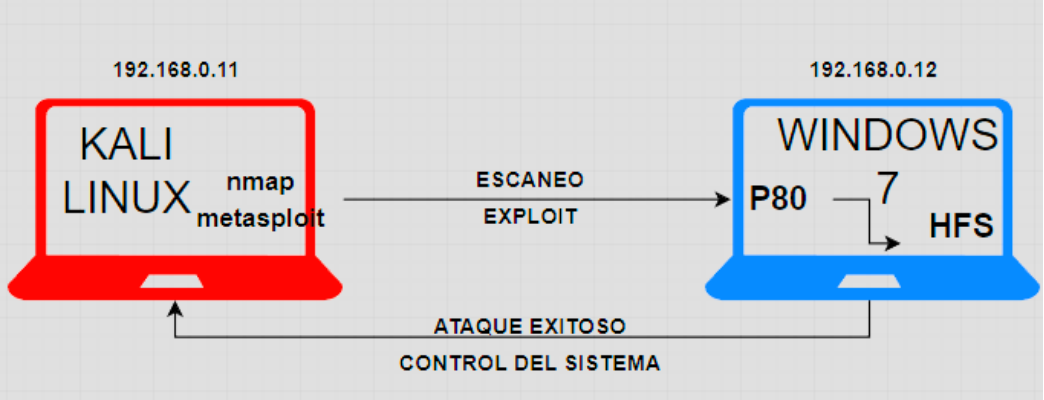
El ataque aprovecha una vulnerabilidad crítica en la aplicación Rejetto HFS (HTTP File Server) en la máquina Windows. Esta vulnerabilidad permite la ejecución remota de código (RCE), lo que significa que un atacante puede ejecutar comandos en el sistema víctima sin autorización.

Una vez identificado el puerto 80 como el servicio activo donde corre HFS, se utilizó una herramienta como lo es Metasploit para explotar la vulnerabilidad. Esto permitió al atacante:

- Ganar acceso remoto a la máquina víctima.
- Obtener privilegios elevados, lo que posibilita controlar totalmente el sistema.
- Robar información sensible almacenada en la máquina, alterar archivos o interrumpir servicios críticos.

Este tipo de ataque compromete la confidencialidad, integridad y disponibilidad de la información y recursos del sistema.

Imagen 20 Ilustración del ataque



Nota. Fuente: autoría propia

4.3 Contención de ataques informáticos

De acuerdo con el problema del anexo 5 – escenario 4 referente a equipo Blueteam y por medio del banco de trabajo configurado en la actividad anterior, dar respuesta a las siguientes preguntas orientadoras:

4.3.1 Pregunta 1

¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Para escoger las acciones a ejecutar en caso de encontrar un ataque en tiempo real, creo que dependería de un factor importante como lo es 1a experiencia y conocimiento que se ha adquirido durante la trayectoria como Especialista en Seguridad Informática, por lo que pensaría en 2 opciones de respuesta inmediata:

- ***Opción 1***: Contención y análisis inicial del sistema comprometido (principiante)

Lo primero sería identificar y contener el ataque en tiempo real para minimizar su impacto. Esto implica desconectar el sistema afectado de la red para evitar que el ataque se propague o que el atacante obtenga más control. Posteriormente, se revisan los logs del sistema y de la red para identificar indicadores de compromiso (IoC), como conexiones sospechosas, procesos no autorizados o archivos modificados.

- Desconectar el sistema interrumpe la actividad sospechosa y protege otros dispositivos y a toda la red.
- Los logs de herramientas como Sysmon y el visor de eventos en Windows permiten rastrear las actividades anómalas (Servicepilot, 2024).
- Este enfoque asegura que el análisis posterior se realice sin riesgos adicionales

- ***Opción 2***: Monitoreo y Recolección de Evidencia en Tiempo Real (experto)

En lugar de desconectar el sistema inmediatamente, se prioriza monitorear el ataque mientras se recopila evidencia forense. Esto incluye capturar el tráfico de red con Wireshark y usar herramientas como Process Explorer para analizar los procesos activos y determinar si el ataque es interno o externo. Una vez recolectada suficiente información, se procede con la contención.

- Monitorear el ataque ayuda a comprender el vector de ataque y los objetivos del atacante
- Herramientas como Wireshark y Process Explorer permiten observar el comportamiento en tiempo real sin interrumpir el sistema inmediatamente (Luz, 2024)
- Esta estrategia es útil si la empresa necesita identificar con precisión al atacante antes de actuar

La opción 1 está orientada a alguien con menos experiencia o que prioriza la protección de la red y sistemas ante un ataque desconocido. Este enfoque es directo, seguro y efectivo para limitar el impacto, pero puede perder valiosa información sobre el ataque en el proceso

La opción 2 requiere mayor experiencia, ya que el profesional debe ser capaz de interpretar rápidamente la actividad sospechosa, utilizar herramientas avanzadas y decidir cuándo actuar. Este enfoque permite un análisis más detallado y puede ayudar a comprender mejor el vector de ataque, pero conlleva el riesgo de que el atacante avance si no se actúa a tiempo.

Ambos enfoques son válidos y aplicables según el contexto, pero la elección correcta dependerá del nivel de confianza y competencia del profesional, así como de los protocolos establecidos en la organización.

4.3.2 Pregunta 2

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Redteam, qué medidas de hardenización propondría para que el ataque no se repita?

Para prevenir futuros ataques como el ejecutado en el ejercicio Redteam, propondría las siguientes medidas de hardenización específicas para la máquina Windows y la red:

- **Actualización y parches**

El ataque aprovechó una vulnerabilidad conocida en Rejetto HFS (CVE-2014-6287) (INCIBE, 2021). Mantener actualizado el sistema operativo y las aplicaciones permite en seguridad informática proteger los sistemas contra exploits conocidos .

Medida: instalar todas las actualizaciones críticas de seguridad para Windows y actualizar o reemplazar HFS con una versión más segura o una solución alternativa

- **Configuración segura del sistema**

Desactivar servicios innecesarios: minimizar la superficie de ataque deshabilitando servicios y puertos no utilizados. Por ejemplo, si HFS no es necesario, se debe desinstalar.

Fortalecer contraseñas: asegurar que todas las cuentas tengan contraseñas fuertes y únicas para evitar ataques de fuerza bruta

- **Firewall y control de acceso**

Reglas estrictas: configurar el firewall para permitir únicamente tráfico legítimo hacia servicios autorizados. Por ejemplo, restringir el acceso al puerto 80 a direcciones IP específicas si HFS debe seguir en uso.

Control de acceso basado en roles (RBAC): implementar políticas que restrinjan el acceso administrativo solo a usuarios específicos y desde dispositivos autorizados (ManageEngine, 2024).

- **Monitoreo y detección**

IDS/IPS: implementar sistemas de detección y prevención de intrusiones para monitorear tráfico sospechoso, como intentos de ejecución remota de código (RCE).

Logs y auditorías: activar el registro de eventos y analizar regularmente los logs del sistema y la red para identificar actividades anómalas

- **Cifrado y protección de datos**

HTTPS: configurar HFS (o cualquier aplicación web) para que utilice HTTPS en lugar de HTTP, protegiendo la comunicación contra ataques de intermediarios

Cifrado de datos sensibles: asegurar que la información almacenada esté cifrada para protegerla en caso de compromiso.

- **Capacitación y concientización**

Entrenamiento de usuarios: enseñar al personal buenas prácticas de seguridad, como reconocer intentos de phishing y proteger credenciales

Simulaciones: realizar ejercicios regulares de Red Team para identificar nuevas vulnerabilidades y probar la respuesta del Blue Team.

4.3.3 Pregunta 3

¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

Equipo Blue Team

Su enfoque principal es la prevención, defensa y monitoreo constante para proteger la infraestructura tecnológica de la organización. Un Blue Team es un equipo proactivo y preventivo enfocado en fortalecer la seguridad de una organización para reducir la probabilidad de ataques exitosos. Sus actividades incluyen la implementación de controles de seguridad, monitoreo continuo de redes y sistemas, detección de amenazas y la aplicación de medidas de hardenización para minimizar vulnerabilidades (Lozano, 2024).

CSIRT (Computer Security Incident Response Team)

Su enfoque principal es responder y gestionar incidentes específicos de ciberseguridad de manera eficiente. El Equipo de Repuesta a Incidentes Informáticos, es un equipo reactivo y táctico que se activa cuando ocurre un incidente de seguridad. Su objetivo principal es contener, investigar y mitigar el impacto del incidente en el menor tiempo posible. Sus actividades incluyen la identificación del vector de ataque, el análisis forense, la recuperación de sistemas afectados y la implementación de soluciones a corto plazo para restaurar la operación (Mendoza, 2015).

Diferencias clave:

- Rol proactivo vs. reactivo: el Blue Team trabaja de manera continua para prevenir ataques, mientras que el CSIRT actúa específicamente en respuesta a un incidente
- Temporalidad: el Blue Team opera de forma constante, mientras que el CSIRT interviene solo en situaciones de emergencia.

Alcance: el Blue Team se enfoca en la seguridad general de la organización, mientras que el CSIRT aborda problemas puntuales y su resolución (Sánchez, 2021).

4.3.4 Pregunta 4

¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS “Center For Internet Security”, usted lo utilizaría para qué fin?

El CIS (Center for Internet Security) es una organización sin fines de lucro que proporciona directrices y herramientas para mejorar la ciberseguridad (Manageengine, 2024).

Dentro del Blue Team, el CIS se convierte en un recurso valioso para establecer estándares de seguridad, implementar controles efectivos, auditar sistemas y mantenerse actualizado frente a nuevas amenazas. Su uso refuerza las capacidades defensivas de una organización de manera práctica y estructurada.

Dentro de un equipo Blue Team, el CIS se utilizaría para los siguientes fines:

- **Hardenización de sistemas y aplicaciones**

Aplicar los CIS Benchmarks, que son configuraciones seguras recomendadas para sistemas operativos, aplicaciones y dispositivos de red. Esto permite reducir la superficie de ataque y fortalecer los entornos críticos (Team, 2022)

- **Gestión de controles de seguridad**

Implementar los CIS Controls, un conjunto de 18 controles prioritarios diseñados para prevenir, detectar y responder a ciberamenazas. Estos controles abarcan desde inventarios de hardware/software hasta respuesta ante incidentes (Team, 2022)

- **Auditorías y evaluaciones**

Utilizar las guías del CIS para realizar evaluaciones periódicas y auditorías de la infraestructura, identificando brechas de seguridad y verificando el cumplimiento de las mejores prácticas (Team, 2022)

- **Monitoreo de amenazas**

Aprovechar los servicios de inteligencia de amenazas del CIS, como el MS-ISAC (Multi-State Information Sharing and Analysis Center), para estar al tanto de las amenazas actuales y preparar estrategias defensivas (CIS, 2024).

4.3.5 Pregunta 5

Explique y redacte las funciones y características principales de lo que es un SIEM

Un SIEM, de sus siglas Security Information and Event Management, es una solución de ciberseguridad que permite recopilar, analizar y correlacionar datos de eventos de múltiples fuentes en una red para detectar amenazas, responder a incidentes y garantizar el cumplimiento normativo (IBM, 2024).

Sus funciones y características principales son:

Funciones

- Recolección de datos: recopila información de múltiples fuentes, como firewalls, servidores, sistemas operativos, bases de datos, aplicaciones y dispositivos de red
- Correlación de eventos: analiza y correlaciona eventos de seguridad en tiempo real para identificar patrones de comportamiento sospechoso o potenciales amenazas
- Alertas en tiempo real: genera alertas automatizadas cuando detecta actividades anómalas o eventos que coinciden con patrones predefinidos de ataques
- Análisis forense: permite investigar incidentes mediante el acceso a registros históricos y la reconstrucción de eventos para comprender cómo ocurrió un ataque (IBM, 2024).

Características principales

- Centralización de logs: integra y organiza los registros de seguridad en un único lugar, facilitando la visibilidad y el análisis
- Automatización de respuestas: puede ejecutar acciones automatizadas, como bloquear una IP o detener un proceso al detectar una amenaza
- Escalabilidad: se adapta al crecimiento de la red empresarial, manejando un volumen creciente de eventos y datos
- Análisis avanzado: incorpora inteligencia artificial y aprendizaje automático para mejorar la precisión de las detecciones y reducir falsos positivos
- Paneles de control intuitivos: proporciona dashboards visuales para monitorear el estado de la seguridad en tiempo real, facilitando la toma de decisiones (IBM, 2024).

4.3.6 Pregunta 6

Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

Las herramientas de contención de ataques informáticos son soluciones diseñadas para bloquear, limitar o mitigar el impacto de un ataque cibernético en tiempo real. A diferencia de las herramientas de detección, que se centran en identificar amenazas, las herramientas de contención toman acciones activas para evitar la propagación del ataque y proteger los activos críticos y los datos de una organización.

Estas herramientas operan en diversas capas de la infraestructura tecnológica, desde el perímetro de la red hasta los dispositivos finales, y tienen como objetivo:

- Aislar sistemas comprometidos: evitar que un ataque afecte otros dispositivos o segmentos de red
- Bloquear el acceso no autorizado: detener intentos de intrusión o exfiltración de datos
- Mitigar la explotación: reducir la capacidad del atacante para aprovechar vulnerabilidades o debilidades en el sistema.

Dentro de las herramientas de hardware más destacadas se tienen:

Firewall Perimetral

Un firewall perimetral es un dispositivo o sistema diseñado para proteger la red interna de una organización al actuar como una barrera entre la red interna y externa. Se ubica en el perímetro de la red, de ahí su nombre, y su función principal es filtrar y controlar el tráfico que entra y sale de la red, siguiendo reglas de seguridad predefinidas, de acuerdo con los requerimientos (Kaspersky, 2024). Dentro de las principales características de un Firewall se tiene:

- Filtrado de tráfico: inspecciona las conexiones entrantes y salientes para permitir o bloquear paquetes según criterios preestablecidos, como IP, puerto, protocolo o contenido.
- Reglas personalizables: permite a los administradores definir políticas específicas según las necesidades de seguridad. Por ejemplo, bloquear puertos específicos o permitir el acceso solo desde ciertas IPs confiables.
- Soporte para NAT (Network Address Translation): ayuda a ocultar las direcciones IP internas de la red, añadiendo una capa de anonimato
- Registro y monitoreo: almacena logs de actividad de red, que son útiles para análisis y auditorías (Kaspersky, 2024)

IPS (Sistema de Prevención de Intrusiones)

Un IPS, de sus siglas Intrusion Prevention System, es una solución diseñada para detectar y bloquear amenazas en tiempo real al analizar el tráfico de red y buscar patrones que coincidan con ataques conocidos o actividades sospechosas. A diferencia de un IDS (que solo detecta), el IPS actúa directamente para detener el ataque. Un IPS es más dinámico y adaptable, respondiendo a patrones nuevos o sospechosos que el firewall tradicional podría no detectar (IBM, IBM, 2024). Dentro de las principales características de un IPS se desatacan:

- Inspección profunda de paquetes (DPI): analiza el contenido de los paquetes de datos para identificar amenazas ocultas, como malware o intentos de explotación.
- Prevención de ataques conocidos: utiliza firmas de ataques predefinidas para bloquear intentos de intrusión basados en patrones reconocidos
- Protección basada en comportamiento: identifica actividades anómalas o sospechosas incluso si no coinciden con firmas específicas (detección heurística)
- Bloqueo automatizado: una vez detectada una amenaza, el IPS toma medidas como cerrar conexiones, bloquear direcciones IP o redirigir tráfico sospechoso
- Integración con SIEM: los IPS suelen integrarse con sistemas SIEM para proporcionar alertas y datos detallados de los incidentes detectados

Un IPS puede bloquear un ataque que intenta explotar la vulnerabilidad CVE-2014-6287 (Rejetto HFS) al detectar el intento de ejecución remota de código basado en patrones conocidos.

Un firewall perimetral y un IPS trabajan juntos para proteger la red. El firewall filtra el tráfico básico según reglas predefinidas, mientras que el IPS realiza una inspección más profunda para bloquear amenazas específicas en tiempo real.

Dentro de las herramientas de software más destacadas se tienen:

Antivirus / Antimalware

Un antivirus es una solución de software diseñada para detectar, bloquear y eliminar software malicioso (malware) de dispositivos informáticos. Es una herramienta básica en cualquier estrategia de seguridad para proteger endpoints (dispositivos finales como PCs, servidores y laptops) de amenazas conocidas y, en algunos casos, de amenazas emergentes (INCIBE, INCIBE, 2019). Dentro de las principales características de un Antivirus se desatacan:

- Detección basada en firmas: el antivirus compara archivos y programas con una base de datos de firmas de malware conocido para identificar amenazas
- Análisis en tiempo real: escanea continuamente el sistema para prevenir la ejecución de archivos maliciosos
- Cuarentena y eliminación: mueve los archivos sospechosos a una zona segura (cuarentena) para evitar que causen daño y los elimina si se confirma que son maliciosos
- Protección de correo electrónico: escanea adjuntos y enlaces en correos electrónicos para detectar phishing y archivos maliciosos

EDR (Detección y Respuesta de Puntos Finales)

Un EDR de sus siglas Endpoint Detection and Response, es una solución avanzada que va más allá del antivirus tradicional. Está diseñada para detectar, responder y contener amenazas avanzadas que afectan a los endpoints, incluso aquellas que pueden eludir los antivirus tradicionales (Tecnozero, 2024). Dentro de las principales características de un EDR se desatacan:

- Monitoreo continuo: analiza en tiempo real los comportamientos y actividades en los endpoints para identificar patrones sospechosos o maliciosos
- Respuestas automatizadas: puede aislar endpoints comprometidos de la red, detener procesos sospechosos o bloquear conexiones maliciosas
- Detección basada en comportamiento: identifica amenazas emergentes y avanzadas como ataques de día cero o malware sin archivos
- Recopilación de datos forenses: proporciona registros detallados del incidente, incluyendo la cadena de eventos, para su análisis y mitigación
- Integración con SIEM: se conecta con sistemas SIEM para proporcionar alertas y correlacionar datos con otros incidentes de seguridad.

Tabla 1 Comparación entre Antivirus y EDR

Aspecto	Antivirus	EDR
Enfoque	Basado en firmas y detección básica	Basado en comportamiento y análisis
Cobertura	Principalmente malware conocido	Amenazas avanzadas y ataques sin archivos
Respuesta	Detecta y elimina malware	Detecta, contiene y responde a incidentes complejos
Capacidades forenses	Limitadas	Detalladas, ideales para análisis de incidentes

Nota. Fuente: autor

Como se puede observar en la tabla; mientras que el antivirus es una solución efectiva para amenazas comunes y conocidas, el EDR ofrece un enfoque más avanzado para proteger endpoints contra ataques sofisticados y persistentes. La combinación de ambas herramientas proporciona una defensa integral para los dispositivos finales.

5 Conclusiones

La ciberseguridad no solo se trata de proteger sistemas, sino de hacerlo dentro de un marco ético y legal que garantice el respeto a las normativas y los derechos de las personas y organizaciones. En este sentido, los equipos Blue Team y Red Team deben operar bajo principios claros que eviten prácticas maliciosas o invasivas fuera de los límites autorizados. Cumplir con leyes como la Ley 1273 de 2009 en Colombia asegura que las actividades de pentesting no vulneren la privacidad ni afecten la operación de terceros. Este enfoque ético no solo fortalece la confianza en los procesos de seguridad, sino que también legitima el trabajo de los equipos de ciberseguridad al alinearse con las mejores prácticas globales y las expectativas legales.

El proceso de pentesting realizado en el laboratorio, desde el escaneo de vulnerabilidades hasta la explotación y escalada de privilegios, demuestra cómo los equipos Red Team pueden identificar fallos críticos en la seguridad de una organización. Estas actividades permiten simular ataques reales para evaluar la resistencia de los sistemas y preparar a los equipos Blue Team para responder eficazmente. La colaboración entre ambos equipos permite cerrar brechas de seguridad y garantizar que las estrategias de defensa sean robustas. Además, la documentación de estas actividades fomenta el aprendizaje continuo, permitiendo que la organización evolucione frente a nuevas amenazas.

La contención de ataques informáticos es una tarea ardua en el ámbito del Blue Team, ya que busca minimizar el impacto de las amenazas detectadas. Implementar herramientas como firewalls, IPS, y estrategias de hardenización asegura que los sistemas comprometidos sean rápidamente aislados y protegidos. Estas medidas, combinadas con un monitoreo continuo y el uso de sistemas como SIEM, permiten una respuesta proactiva y efectiva frente a incidentes. La

colaboración entre Blue Team y Red Team garantiza que las soluciones propuestas no solo sean reactivas, sino que también prevengan futuros ataques, fortaleciendo así la infraestructura de seguridad de la organización.

6 Recomendaciones

En un entorno digital cada vez más amenazado, establecer políticas de seguridad se establece como un pilar fundamental y necesario para proteger los activos tecnológicos, la información sensible y la continuidad operativa de una organización. Las políticas de seguridad no solo ofrecen un marco estructurado para la gestión de riesgos, sino que también definen los lineamientos y responsabilidades necesarias para prevenir, detectar y responder ante ciberamenazas. Su importancia radica en garantizar que todos los actores involucrados, desde los empleados hasta los sistemas tecnológicos, operen bajo estándares que minimicen vulnerabilidades y maximicen la resiliencia frente a ataques.

En este contexto, a continuación, se presentan una serie de políticas estratégicas diseñadas para abordar los desafíos identificados en los ejercicios de Red Team y Blue Team, fortaleciendo así la postura de seguridad de la organización.

Política 1: Fortalecimiento del perímetro

Acciones:

- Adquisición y configuración de firewalls perimetrales: implementar firewalls perimetrales para controlar el tráfico entrante y saliente según reglas predefinidas, asegurando que solo el tráfico legítimo sea permitido. Esto incluye bloquear puertos innecesarios y permitir únicamente los servicios requeridos para las operaciones del negocio
- Firewall de próxima generación (NGFW): usar firewalls avanzados que incluyan inspección profunda de paquetes y funcionalidades como control de aplicaciones y detección de malware

- Implementación de IPS: desplegar sistemas de prevención de intrusiones (IPS) que analicen el tráfico en tiempo real para identificar y bloquear patrones de ataque conocidos, como intentos de explotación de vulnerabilidades o ataques DDoS, etc.
- Integración con SIEM: configurar firewalls e IPS para enviar alertas y logs al sistema SIEM, permitiendo un análisis centralizado de posibles incidentes
- Pruebas regulares: realizar pruebas periódicas para verificar que las reglas y configuraciones del firewall e IPS sean efectivas y estén actualizadas

Logro esperado:

Prevenir accesos no autorizados y proteger la red contra amenazas externas e internas, garantizando una defensa perimetral robusta y adaptable a nuevos vectores de ataque

Política 2: Hardenización de infraestructura

Acciones:

- Configuraciones seguras: asegurar que los sistemas operativos y las aplicaciones estén configurados según las mejores prácticas de seguridad, deshabilitando servicios innecesarios, cambiando configuraciones predeterminadas inseguras y limitando los accesos administrativos
- Gestión de actualizaciones: establecer un cronograma para aplicar actualizaciones y parches de seguridad en sistemas y dispositivos críticos, priorizando las vulnerabilidades con mayor impacto potencial
- Revisión de contraseñas: imponer políticas de contraseñas robustas, incluyendo longitud mínima, complejidad y cambios regulares, para todos los usuarios y cuentas de servicio

- Implementación de herramientas de análisis: utilizar herramientas como Lynis o CIS-CAT para realizar auditorías de hardenización y garantizar el cumplimiento de estándares

Logro esperado:

Reducir significativamente la superficie de ataque de la organización, limitando las oportunidades de explotación por parte de atacantes internos y externos

Política 3: Gestión de vulnerabilidades

Acciones:

- Escaneos regulares: implementar escaneos de vulnerabilidades semanales o mensuales con herramientas como Nessus u OpenVAS para identificar brechas en sistemas, aplicaciones y dispositivos de red
- Priorización de vulnerabilidades: clasificar las vulnerabilidades encontradas según su criticidad y abordar primero las que tienen mayor impacto en la seguridad
- Remediación sistemática: crear un proceso estructurado para corregir vulnerabilidades detectadas, que incluya plazos definidos, responsables y seguimiento
- Evaluación continua: realizar análisis comparativos antes y después de las correcciones para validar que las vulnerabilidades han sido eliminadas o mitigadas correctamente

Logro esperado:

Mitigar riesgos asociados con vulnerabilidades conocidas y fortalecer la postura de seguridad al cerrar brechas antes de que puedan ser explotadas

Política 4: Respuesta a incidentes

Acciones:

- Creación de un plan de respuesta (IRP): diseñar un plan detallado que incluya procedimientos para la identificación, contención, erradicación y recuperación de incidentes de seguridad
- Definición de roles: asignar responsabilidades específicas dentro del equipo de respuesta, incluyendo un líder de incidentes, analistas de seguridad y encargados de comunicación interna y externa
- Pruebas de simulación: realizar simulacros regulares de incidentes para evaluar la efectividad del plan y la capacidad del equipo para actuar bajo presión
- Documentación y lecciones aprendidas: registrar cada incidente para analizar su causa raíz y aplicar mejoras que prevengan su repetición

Logro esperado:

Asegurar una respuesta rápida y efectiva a cualquier incidente, minimizando el impacto en las operaciones y reduciendo tiempos de recuperación

Política 5: Auditoría y monitoreo continuo

Acciones:

- SIEM: implementar una solución SIEM (como Splunk o Wazuh) para recopilar, correlacionar y analizar eventos de seguridad en tiempo real
- Logs centralizados: configurar los sistemas para que envíen sus logs a un servidor central, facilitando el análisis de actividades sospechosas
- Alertas automatizadas: crear reglas en el SIEM para generar alertas automáticas ante eventos inusuales, como intentos fallidos de inicio de sesión o accesos fuera de horario laboral

- Revisión periódica: realizar auditorías trimestrales de los logs y configuraciones para identificar posibles brechas en la seguridad

Logro esperado:

Detectar actividades sospechosas de manera temprana, permitiendo una intervención proactiva antes de que las amenazas escalen

Política 6: Capacitación del personal

Acciones:

- Cursos de ciberseguridad: organizar capacitaciones regulares para todos los empleados, enfocadas en buenas prácticas como evitar enlaces maliciosos y reconocer intentos de phishing
- Simulaciones de ataques: realizar pruebas de simulación, como correos electrónicos de phishing, para medir el nivel de respuesta y concienciar al personal
- Protocolos claros: proporcionar guías claras sobre qué hacer en caso de detectar un incidente de seguridad, como reportarlo inmediatamente al equipo de TI
- Capacitación especializada: entrenar a equipos técnicos en el uso de herramientas avanzadas como SIEM y análisis forense para fortalecer las respuestas a incidentes

Logro esperado:

Reducir el riesgo asociado con el factor humano, promoviendo una cultura de seguridad en toda la organización

7 Bibliografía

CAMPUSCIBERSEGURIDAD. (21 de 05 de 2024). *Metasploit: La herramienta esencial en Ciberseguridad*. Obtenido de https:www.campusciberseguridad.com/blog/item/180-metasploit-herramienta-esencial-ciberseguridad

Cilleruelo, C. (31 de 07 de 2024). *¿Qué es ExploitDB?* Obtenido de https://keepcoding.io/blog/que-es-exploitdb/

CIS. (2024). *Center For internet Security*. Obtenido de Multi-State Information Sharing and Analysis Center: https://www.cisecurity.org/ms-isac

Cusi, H. L. (09 de 10 de 20024). *Open vas: Escáner de vulnerabilidad de código abierto*. Obtenido de https://prezi.com/p/fas7xgq-ghra/open-vas-escaner-de-vulnerabilidad-de-codigo-abierto/

IBM. (2024). *IBM*. Obtenido de ¿Qué es la gestión de eventos e información de seguridad (SIEM)? : https://www.ibm.com/mx-es/topics/siem

IBM. (2024). *IBM*. Obtenido de ¿Qué es un sistema de prevención de intrusiones (IPS)?: https://www.ibm.com/es-es/topics/intrusion-prevention-system

INCIBE. (30 de 05 de 2019). *INCIBE*. Obtenido de https://www.incibe.es/empresas/blog/hace-antivirus-detectar-el-malware

INCIBE. (26 de 02 de 2021). *Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287)*. Obtenido de https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-6287

Jenifa, A. (15 de 05 de 2024). *¿Cómo utilizar Nmap para la exploración de vulnerabilidades?* Obtenido de https://geekflare.com/es/nmap-vulnerability-scan/

Kaspersky. (2024). *Kaspersky* . Obtenido de ¿Qué es un firewall? Definición y explicación: https://latam.kaspersky.com/resource-center/definitions/firewall?srsltid=AfmBOopJmWLQKU9EJLXjD-qVWro10Q064zkaGKgtyjjf26gBGkgKGlU2

Laprovittera, C. (10 de 08 de 2024). *ACHIROU*. Obtenido de El Camino del Hacker – Inicia tu carrera como Hacker: https://achirou.com/el-camino-del-hacker-inicia-tu-carrera-como-hacker/

Lozano, P. A. (30 de 10 de 2024). *OpenWebinars*. Obtenido de Ciberseguridad proactiva: La importancia del Blue Team: https://openwebinars.net/blog/ciberseguridad-proactiva-la-importancia-del-blue-team/

Luz, S. d. (03 de 10 de 2024). *Cómo usar Wireshark para capturar y analizar el tráfico de red*. Obtenido de https://www.redeszone.net/tutoriales/redes-cable/wireshark-capturar-analizar-trafico-red/

ManageEngine. (2024). *Control de acceso basado en roles (RBAC)*. Obtenido de https://www.manageengine.com/latam/device-control/control-de-accesos-basado-en-roles.html#:~:text=%C2%BFQu%C3%A9%20es%20el%20control%20de,a%20los%20niveles%20que%20pertenezcan.

Manageengine. (2024). *Manageengine* . Obtenido de ¿Qué son y cómo implementar los Controles de CIS (CIS Controls / CIS ciberseguridad)?: https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Mendoza, M. A. (18 de 05 de 2015). *Welivesecurity*. Obtenido de ¿Qué es y cómo trabaja un CSIRT para dar respuesta a incidentes?: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

MIRA. (03 de 2024). Obtenido de https://leyes.senado.gov.co/proyectos/images/documentos/textos%20radicados/proyectos%20de%20ley/2023%20-%202024/PL%20254-24%20Seguridad%20Digital%20Ni%C3%B1os.pdf

Pública, D. A. (05 de 01 de 2009). *Funcion Pública* . Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Pública, D. A. (18 de 10 de 2012). *Función Pública*. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Pública, D. A. (27 de 06 de 2013). *Función Pública*. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

REPÚBLICA, C. D. (24 de 07 de 2018). *Función Pública* . Obtenido de https://www1.funcionpublica.gov.co/documents/34645357/34703567/Ley_1928_de_2018.pdf/f6402a0c-bf61-d150-0544-3f44753b5555?t=1560461998293

Sánchez, J. (29 de 07 de 2021). *CodeSpaceAcademy*. Obtenido de El CSIRT y el trabajo de un BlueTeam: https://codespaceacademy.com/csirt-trabajo-blueteam/

Servicepilot. (2024). *Monitoring de la seguridad windows sysmon*. Obtenido de https://www.servicepilot.com/es/integration/monitoreo-windows-sysmon/

TARLOGIC. (2024). *¿Qué es CVE?* Obtenido de https://www.tarlogic.com/es/glosario-ciberseguridad/cve/

Team, C. 4. (20 de 01 de 2022). *Tarlogic*. Obtenido de Controles CIS: las mejores prácticas en ciberseguridad: https://www.tarlogic.com/es/blog/controles-cis-ciberseguridad/

TECNEK. (2024). *TECNEK CIBERSECURITY*. Obtenido de https://www.tecnek.com/noticias-ciberseguridad/179-metodologias-y-fases-del-hacking-etico.html

Tecnozero. (2024). *Tecnozero*. Obtenido de ¿Qué es un EDR? ¿Por qué es diferente de un antivirus?: https://www.tecnozero.com/antivirus-y-anti-ransomware/que-es-un-edr/

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. (2024), Curso Seminario Especializado. Guía para el desarrollo de la actividad – Etapa 5