Capacidades técnicas, legales y de gestión para equipos blue team y red team

Johan Camilo Castillo Acosta

Asesor

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia - UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería ECBTI

Especialización en Seguridad Informática

2025

_____

Jenny Fernanda Restrepo Santacruz

_____ _____

Jurado Jurado

2025

Resumen

Este informe técnico profundiza en aspectos clave de la ciberseguridad, comenzando por el marco legal colombiano. Se analiza la Ley 1273 de 2009 (Delitos Informáticos), la Ley 1581 de 2012 (Protección de Datos Personales), el Decreto 1377 de 2013 y la Ley 1266 de 2008 (Habeas Data financiero), destacando su papel fundamental en la protección de la información. Sin embargo, se enfatiza la necesidad urgente de que esta normativa evolucione para enfrentar las amenazas cibernéticas modernas. Para fortalecer la seguridad del país, se propone un enfoque ágil que combine legislación actualizada, capacitación constante, inversión tecnológica y cooperación internacional. El informe también aborda la metodología de pentesting, describiendo sus fases estándar: reconocimiento, explotación, post-explotación (mantenimiento del acceso) y la elaboración del informe. Se mencionan las herramientas utilizadas, como el sistema operativo Kali Linux, Nmap para identificación de red y Metasploit para explotación de vulnerabilidades, resaltando la importancia de la navegación por el sistema de ficheros para comprometer sistemas operativos obsoletos.

Además, el informe presenta un análisis de caso hipotético sobre las implicaciones éticas y legales en acuerdos laborales, donde un contrato con cláusulas ilegales y condiciones dudosas, como la prohibición de denunciar espionaje o la ocultación de información ilícita, expone al profesional de ciberseguridad a riesgos legales y reputacionales significativos, comprometiendo su integridad y responsabilidad social. Finalmente, se definen las funciones esenciales de los Red Teams, quienes simulan ataques para evaluar la efectividad de los mecanismos de defensa y la capacidad de respuesta operativa. Los Blue Teams se identifican como la primera línea de defensa activa, encargados de proteger la infraestructura tecnológica y mantener los controles de seguridad. Por último, se describe el rol del Equipo de Respuesta a Incidentes (CSIRT), que

interviene tras un incidente de seguridad para minimizar su impacto, restaurar la operatividad y aplicar las lecciones aprendidas para futuras mejoras en la defensa.

Palabras clave**:** Ciberseguridad, legislación colombiana, Pentesting, Implicaciones éticas y legales, Equipos de seguridad

Abstract

This technical report delves into key aspects of cybersecurity, starting with the Colombian legal framework. It analyzes Law 1273 of 2009 (Computer Crimes), Law 1581 of 2012 (Personal Data Protection), Decree 1377 of 2013 and Law 1266 of 2008 (Financial Habeas Data), highlighting their fundamental role in the protection of information. However, it emphasizes the urgent need for these regulations to evolve in order to face modern cyber threats. To strengthen the country's security, it proposes an agile approach that combines updated legislation, constant training, technological investment and international cooperation. The report also discusses the pentesting methodology, describing its standard phases: reconnaissance, exploitation, post-exploitation (maintenance of access) and reporting. The tools used are mentioned, such as the Kali Linux operating system, Nmap for network identification and Metasploit for vulnerability exploitation, highlighting the importance of file system navigation for compromising obsolete operating systems.

In addition, the report presents a hypothetical case analysis on the ethical and legal implications of employment agreements, where a contract with illegal clauses and dubious conditions, such as the prohibition to report espionage or the concealment of illicit information, exposes the cybersecurity professional to significant legal and reputational risks, compromising his or her integrity and social responsibility. Finally, the essential functions of Red Teams, who simulate attacks to evaluate the effectiveness of defense mechanisms and operational response capacity, are defined. Blue Teams are identified as the first line of active defense, in charge of protecting the technological infrastructure and maintaining security controls. Finally, the role of the Incident Response Team (CSIRT) is described, which intervenes after a security incident to

minimize its impact, restore operability and apply lessons learned for future defense improvements.

Keywords**:** Cybersecurity, Colombian legislation, Pentesting, Ethical and legal implications, Security equipment, Colombian law

Contenido

Introducción 12

Objetivos 13

Objetivo General 13

Objetivos Específicos 13

Desarrollo del informe 14

Marco Legal de Ciberseguridad en Colombia 14

Las Fases del Pentesting 16

Análisis ético y legal de un acuerdo laboral en el contexto de la ciberseguridad 17

Laboratorio de Simulación de Ataque Controlado. 19

Repuesta ante un ataque informático. 34

¿Cómo podemos prevenir el ataque identificado y otros futuros ataques? 34

Conclusiones 36

Recomendaciones 37

Referencias Bibliográficas 38

Apéndices 40

Apéndice A. 40

Glosario

Ataques de fuerza bruta

En este tipo de ataque, se prueba metódicamente cada posible combinación de caracteres para una contraseña hasta que se encuentra la correcta, logrando así el acceso no autorizado a un sistema.

Blue Team

También llamado equipo de defensa o de seguridad, tiene la importante tarea de salvaguardar los sistemas y redes informáticas de una empresa frente a los ataques cibernéticos. Son los encargados de proteger activamente la infraestructura digital de una organización.

Delito Informático

Los delitos informáticos, conocidos también como ciberdelitos, son simplemente acciones ilegales realizadas a través de la tecnología y las comunicaciones. En otras palabras, es cuando alguien utiliza computadoras, internet o cualquier otro medio digital para cometer un crimen.

Equipos de respuestas

También conocidos como CSIRT, son grupos de ciberseguridad que gestionan y mitigan incidentes de seguridad desde su detección hasta la recuperación total. Su rol es crucial para proteger los sistemas y datos de una organización.

Exploit

Es un programa o código malicioso creado específicamente para aprovechar una debilidad o fallo de seguridad en un sistema informático, una aplicación o un dispositivo. Su objetivo es conseguir acceso sin permiso, ejecutar comandos o llevar a cabo acciones que no son deseadas por el usuario.

Firewall

Un firewall funciona como un guardián de seguridad que se encarga de proteger una red o un sistema informático, impidiendo que personas o programas no autorizados puedan entrar.

Intrusión

Una intrusión ocurre cuando alguien logra entrar o acceder sin permiso a un sistema informático, una red o un dispositivo.

Red Team

Es un equipo de expertos en ciberseguridad que actúa como si fuera un atacante, ya sea desde fuera o desde dentro de una organización. Su misión es simular ataques reales para encontrar debilidades y evaluar qué tan segura es la empresa.

Seguridad de la Red

La seguridad de la red engloba todas las acciones y reglas establecidas para proteger una red informática de posibles peligros y ataques digitales.

Vulnerabilidad

En la seguridad de la red, una vulnerabilidad es como un punto débil o un defecto en un sistema, una aplicación o en la infraestructura. Los atacantes pueden aprovechar esta falla para poner en riesgo la seguridad, acceder a información privada o causar daños.

Lista de Figuras

Figura 1 Software Virtualbox Con El Banco De Trabajo..... 19

Figura 2 Dirección Ip Máquina Virtual con Windows 19

Figura 3 Dirección Ip Máquina Virtual con Kali Linux y Prueba de Ping Hacia la Maquina con Windows. 20

Figura 4 Escaneo de la Red – Nmap 192.168.1.0/24..... 21

Figura 5 Escaneo de la Maquina Windows – Nmap -Sv -Sc 192.168.1.81. 22

Figura 6 Escaneo de la Maquina Windows – Nmap -Sv --Script Vuln 192.168.1.81. 23

Figura 7 Limpiar y Reiniciar la BD Msfdb Reinit..... 25

Figura 8 Ingreso a Metasploit. 26

Figura 9 Search CVE-2017-0143. 26

Figura 10 Search CVE-2012-1182. 27

Figura 11 Search CVE-2011-3192. 27

Figura 12 Search CVE-2007-6750. 28

Figura 13 Utilización del Exploit..... 29

Figura 14 Configuración de los Parámetros del Exploit, Ip Origen, Ip Destino y Puerto. 29

Figura 15 Ejecución del Exploit. 29

Figura 16 Uso de Comandos Shell y Whoami. 30

Figura 17 Usuarios Actuales de la Maquina Atacada. 30

Figura 18 Estado Actuales de la Maquina Atacada. 31

Figura 19 Evidencia de la Creación del Usuario en la Maquina Atacada. 31

Figura 20 Interacción en la Maquina Atacada. 32

Figura 21 Utilizamos el Comando Search para la Vulnerabilidad Rejetto Hfs. 32

Figura 22 Seleccionamos la Opción Rejetto_Hfs_Exe. 33

Figura 23 Configuración de los Parámetros Exploit. Ip Destino y Ejecución Exploit “Run”. 33

Figura 24 Interacción con la Maquina Windows Mediante la Vulnerabilidad Rejetto Hfs. 33

Introducción

En un mundo donde cada vez dependemos más de la tecnología, la ciberseguridad se vuelve crucial para proteger nuestros datos y mantenernos seguros en línea. Para enfrentar los constantes desafíos digitales, es fundamental contar con profesionales especializados, y aquí entran en juego los Red Teams y Blue Teams.

Estos equipos de élite simulan un verdadero "juego de guerra": el Red Team actúa como atacante, buscando y explotando vulnerabilidades en la red y los sistemas, mientras que el Blue Team se encarga de defender, protegiendo proactivamente la infraestructura y los datos de la organización. Juntos, no solo fortalecen la seguridad actual, sino que también aprenden constantemente sobre las nuevas y futuras tácticas de los ciberdelincuentes, ofreciendo una visión completa para adelantarse al sabotaje de la información.

Objetivos

Objetivo General

Comprender las estrategias de protección y respuesta ante amenazas cibernéticas mediante el análisis de la legislación colombiana en ciberseguridad, las etapas y herramientas del pentesting, y las implicaciones éticas y legales asociadas a acuerdos laborales

Objetivos Específicos

Analizar el marco legal colombiano referente a la protección de datos y delitos informáticos, subrayando su evolución y la necesidad de una adaptación constante ante las amenazas digitales modernas.

Describir las etapas del pentesting y las herramientas clave utilizadas en cada una, identificando su aplicación en la detección y explotación de vulnerabilidades.

Identificar las implicaciones éticas y legales en acuerdos laborales y su impacto en la responsabilidad profesional.

Ejecutar un laboratorio de ataque controlado informático en tiempo real y, basándose en el análisis de las vulnerabilidades identificadas, y proponer medidas de hardenización específicas para fortalecer la postura de seguridad.

Desarrollo del informe

Marco Legal de Ciberseguridad en Colombia

Evolución y Normativa Clave la legislación colombiana en ciberseguridad representa una base importante, pero su continua y rápida evolución es crucial para hacer frente a las amenazas cibernéticas modernas. El vertiginoso avance tecnológico a menudo supera el ritmo de la creación de leyes, lo que demanda un enfoque más ágil, preventivo y transversal. Este enfoque debe integrar la legislación, la capacitación, la inversión pública y la cooperación internacional para garantizar una protección efectiva.

Ley 1273 de 2009

Delitos Informáticos Esta ley surgió como una respuesta directa a los desafíos de la era digital, buscando proteger la información que manejamos diariamente. La Ley 1273 de 2009 actualizó el Código Penal colombiano para sancionar conductas como el acceso no autorizado a sistemas informáticos, la interceptación de datos, el daño informático, el uso de software malicioso y la violación de la privacidad de los datos personales. En esencia, esta normativa reconoce la información y los datos como bienes de alto valor, merecedores de una protección legal clara y contundente frente a las amenazas digitales. (Congreso de Colombia, 2009)

La Ley 1581 de 2012

Se promulgó para salvaguardar la información personal de los ciudadanos colombianos, asegurando su manejo responsable tanto en entidades públicas como privadas. Esta norma garantiza el derecho de cada individuo a conocer, actualizar y corregir sus datos personales, estableciendo principios esenciales como la legalidad, la finalidad del uso, la libertad del titular, la veracidad, el acceso y la circulación restringida de la información. Además, exige a quienes recolectan y utilizan datos personales asumir responsabilidades claras y contar con la

autorización expresa de los titulares. También introduce la figura del Habeas Data, una herramienta legal que permite a cualquier ciudadano defender su privacidad y exigir respeto por su información. (Congreso de Colombia, 2012)

El Decreto 1377 de 2013

Fue creado para facilitar la aplicación práctica de la Ley 1581 de 2012. Este decreto clarifica cómo las organizaciones deben obtener el consentimiento de las personas para usar su información, especialmente en el caso de bases de datos preexistentes a la entrada en vigor de la ley. Asimismo, establece medidas concretas para garantizar la seguridad de los datos y exige que las entidades implementen políticas claras sobre su tratamiento, junto con mecanismos accesibles para que los ciudadanos puedan ejercer sus derechos sobre su información personal. (Presidencia de la República de Colombia, 2013)

Ley 1266 de 2008Habeas Data Financiero

Conocida como la ley de Habeas Data financiero, la Ley 1266 de 2008 tiene como objetivo proteger la información personal relacionada con la vida crediticia, comercial y financiera de los ciudadanos. Esta norma asegura que las personas tengan control sobre el uso de su historial crediticio, permitiéndoles consultarlo, corregirlo y solicitar su actualización. Además, establece que los reportes negativos no pueden permanecer indefinidamente, promoviendo la posibilidad de una segunda oportunidad financiera. También impone a las entidades la responsabilidad de manejar esta información con veracidad y cuidado, evitando su uso indebido o perjudicial para el titular. (Ley 1266 de 2008. Congreso de Colombia. (Congreso de Colombia, 2008)

Las Fases del Pentesting

Reconocimiento

Esta fase inicial se centra en la recopilación de información sobre el objetivo. Se busca conocer el entorno sin interactuar directamente con los sistemas (reconocimiento pasivo) o con interacción controlada (reconocimiento activo). Se recogen datos como nombres de dominio, direcciones IP, registros DNS, correos electrónicos o estructuras de la organización.

Escaneo

Una vez obtenida la información básica, se procede a un escaneo técnico del objetivo. El objetivo es descubrir puertos abiertos, servicios activos y versiones de software. Esta fase es clave para identificar posibles puntos débiles que se podrían explotar más adelante.

Enumeración y Análisis de Vulnerabilidades

En esta etapa se profundiza en la información recopilada para identificar vulnerabilidades conocidas en los servicios detectados. Aquí se establece la conexión entre las versiones de software y los fallos de seguridad ya identificados

Explotación

Esta es la fase crítica del pentesting. Aquí se intenta aprovechar las vulnerabilidades descubiertas para obtener acceso no autorizado al sistema. El atacante podría ejecutar código malicioso, escalar privilegios o extraer datos sensibles

Post-Explotación (Mantenimiento del Acceso)

Una vez que se ha logrado el acceso al sistema, esta fase se enfoca en mantener el control sin ser detectado. Se evalúa el impacto real del acceso y la capacidad de moverse lateralmente dentro de la red.

Informe (Análisis y Reporte)

La fase final consiste en la documentación detallada y profesional de todos los hallazgos. El informe debe incluir las vulnerabilidades detectadas, las pruebas de acceso, el nivel de riesgo asociado y las recomendaciones para mitigar los problemas encontrados.

Análisis ético y legal de un acuerdo laboral en el contexto de la ciberseguridad

Este informe técnico examina con detenimiento un caso que expone serias irregularidades éticas y legales dentro de un proceso de contratación en el sector de ciberseguridad, así como las implicaciones de un caso real de ciberespionaje corporativo. Ambos escenarios ponen en evidencia prácticas que vulneran no solo la legislación colombiana, sino también los principios fundamentales de la ética profesional.

Durante el análisis de un acuerdo laboral se identificaron múltiples deficiencias que comprometen su validez legal y ética. El contrato fue elaborado por un abogado con antecedentes cuestionables, y no contó con una revisión adecuada por parte de la gerencia, lo que genera dudas sobre su legitimidad. A esto se sumó la presión ejercida sobre los aspirantes para firmarlo sin que existieran garantías claras, en un contexto donde además se utilizaban pruebas y condiciones evaluativas poco éticas, como el acceso a información interna de la empresa sin respaldo legal o normativo.

De forma alarmante, uno de los anexos (Anexo 3) contenía cláusulas que violaban directamente disposiciones de la Ley 1273 de 2009, la cual penaliza los delitos informáticos en Colombia. Estas cláusulas incluían la prohibición de reportar actividades sospechosas como espionaje o apropiación indebida de información; la obligación de mantener en secreto datos obtenidos ilegalmente (como interceptaciones o “chuzadas”); y una exoneración total de responsabilidad penal para la empresa contratante.

En términos jurídicos, tales estipulaciones transgreden artículos fundamentales de la ley mencionada, entre ellos:

- Art. 269A: Acceso abusivo a un sistema informático.
- Art. 269C: Interceptación de datos informáticos.
- Art. 269E: Uso de software malicioso.
- Art. 269F: Violación de datos personales.
- Art. 269G: Suplantación de sitios web para capturar información.

Desde una perspectiva ética y profesional, aceptar un cargo bajo estas condiciones representa una amenaza para la integridad del profesional, va en contra de la responsabilidad social que implica la ciberseguridad, y expone al trabajador a riesgos legales y reputacionales considerables.

De acuerdo con el caso de estudio de CyberFort Technologies, una empresa contratada para auditar sistemas de comunicación gubernamentales que incurrió en acceso no autorizado a información sensible, la cual fue luego comercializada en la darknet. Esta acción, además de ilegal, constituye una grave violación ética, al quebrantar la confianza del cliente y traicionar los principios fundamentales de la ciberseguridad. Entre las irregularidades detectadas se incluyen el uso indebido de datos, violación contractual, abuso de capacidades técnicas y un doble discurso frente a los organismos de control.

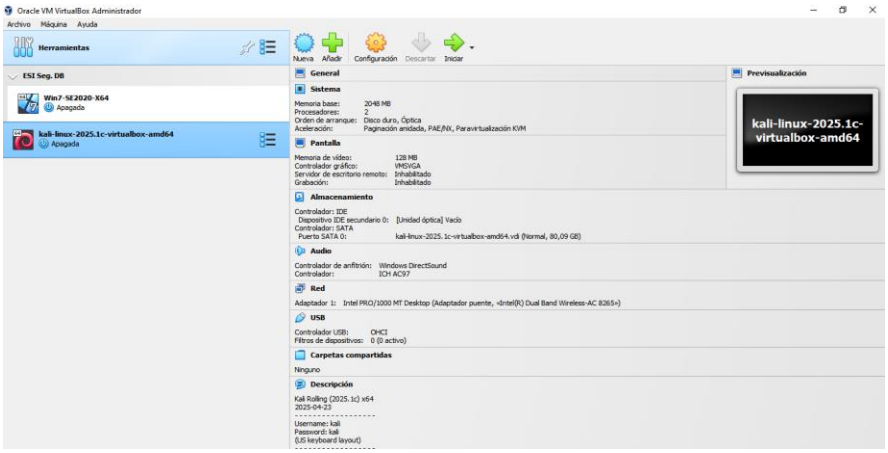
Para prevenir situaciones similares, se recomienda limitar contractualmente el acceso a la información, establecer cláusulas de confidencialidad robustas, reforzar los mecanismos de trazabilidad y control, y exigir compromisos éticos al personal involucrado. Ante casos confirmados, se sugiere rescindir contratos, iniciar acciones legales, implementar auditorías externas y fortalecer la cooperación con entidades de ciberdefensa. Estos incidentes no solo

comprometen la seguridad digital, sino que también generan consecuencias estratégicas y políticas de alto impacto, afectando la confianza institucional y la soberanía tecnológica.

Laboratorio de Simulación de Ataque Controlado.

Figura 1

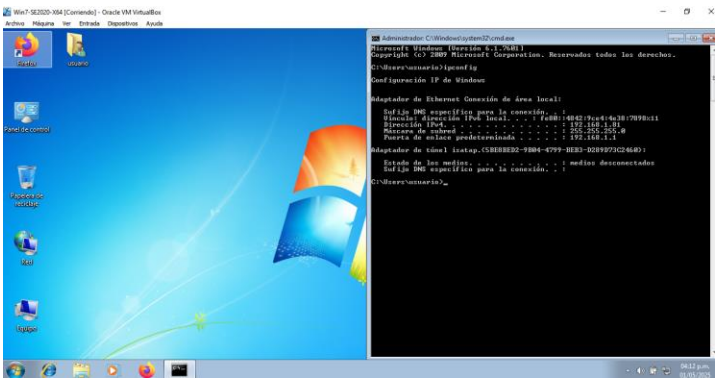
Software Virtualbox con el Banco de Trabajo



Nota. Se crearon dos máquinas virtuales (Windows y Kali Linux) para simular un escenario de ataque y defensa.

Figura 2

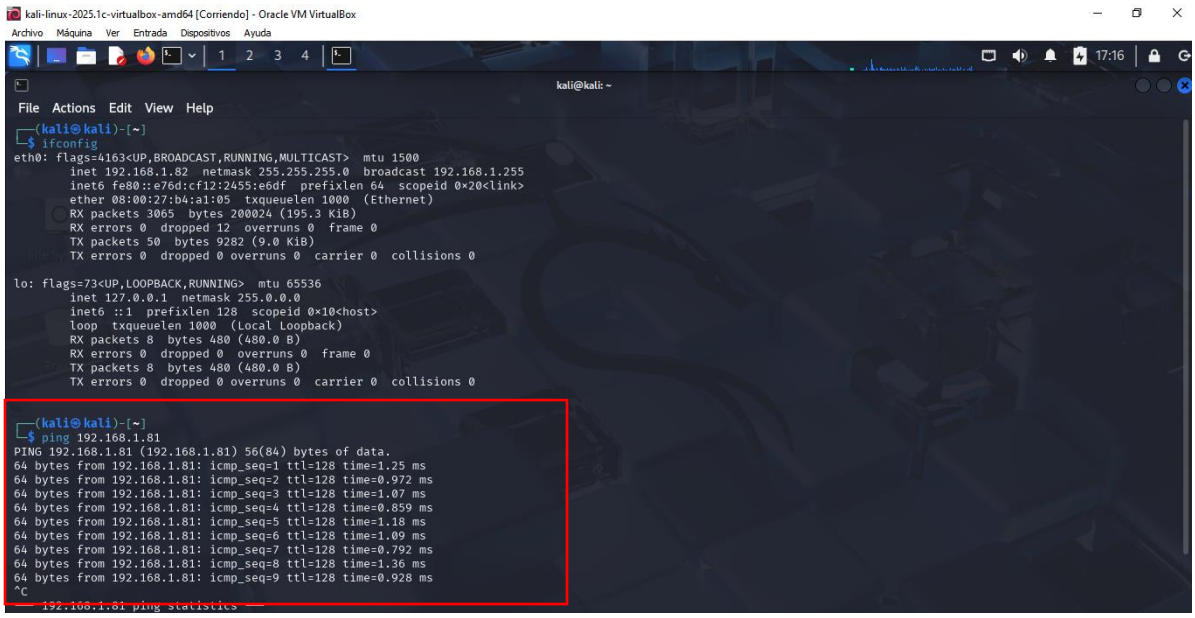
Dirección Ip Máquina Virtual con Windows



Nota. Se observa que la maquina con el OS Windows tiene una ip 192.168.1.81.

Figura 3.

Dirección Ip Máquina Virtual con Kali Linux y Prueba de Ping Hacia la Maquina con Windows.



Nota. Se realiza una prueba de conexión entre las dos máquinas mediante el comando ping.

Nmap (Network Mapper)

Es una herramienta de código abierto fundamental en las pruebas de penetración. En la fase de escaneo, permite detectar equipos y servicios en una red al enviar paquetes específicos y analizar sus respuestas. Su capacidad para localizar puertos disponibles, reconocer sistemas operativos e identificar posibles vulnerabilidades lo convierte en un recurso indispensable para los equipos Red Team. (NMAP Network Scanning, 2024).

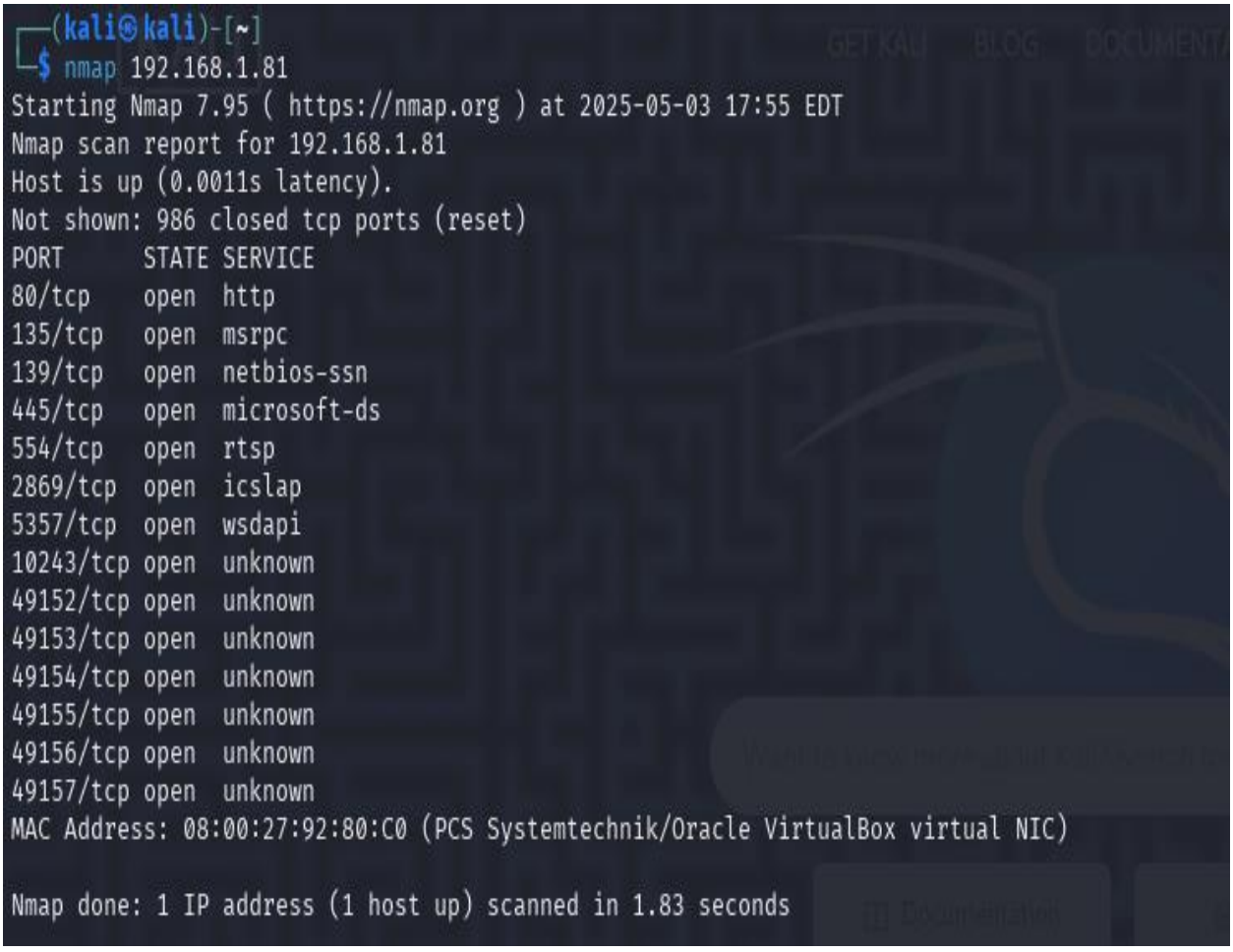
Nmap 192.168.1.0/24

Se realiza para un escaneo del segmento de red, se identificó una máquina con Windows 7 en la dirección IP 192.168.1.81. Este análisis reveló que el equipo tiene varios puertos TCP abiertos, incluyendo el puerto 80 (HTTP para tráfico web), 135 (Microsoft RPC), 139 (NetBIOS Session Service para compartir archivos en redes antiguas), 445 (SMB para compartir recursos

en Windows modernos), 554 (RTSP para streaming), 2869 (UPnP para configuración de dispositivos), 5357 (WSDAPI para descubrimiento de dispositivos), 10243 (Windows Media Player Network Sharing), y el rango dinámico 49152-49157 (RPC y otros servicios de Windows). Además, se encontraron puertos específicos como 2179 (Hyper-V RDP), 3306 (MySQL), 3389 (RDP para control remoto), y 5800/5900 (VNC para acceso remoto).

Figura 4.

Escaneo de la Red – Nmap 192.168.1.0/24



Nota. Se escaneo todo el segmento 192.168.1.0 y se logró observar los puertos de la maquina con Windows.

Para obtener información más detallada acerca de los puertos detectados en la máquina, se procede a la ejecución del siguiente comando.

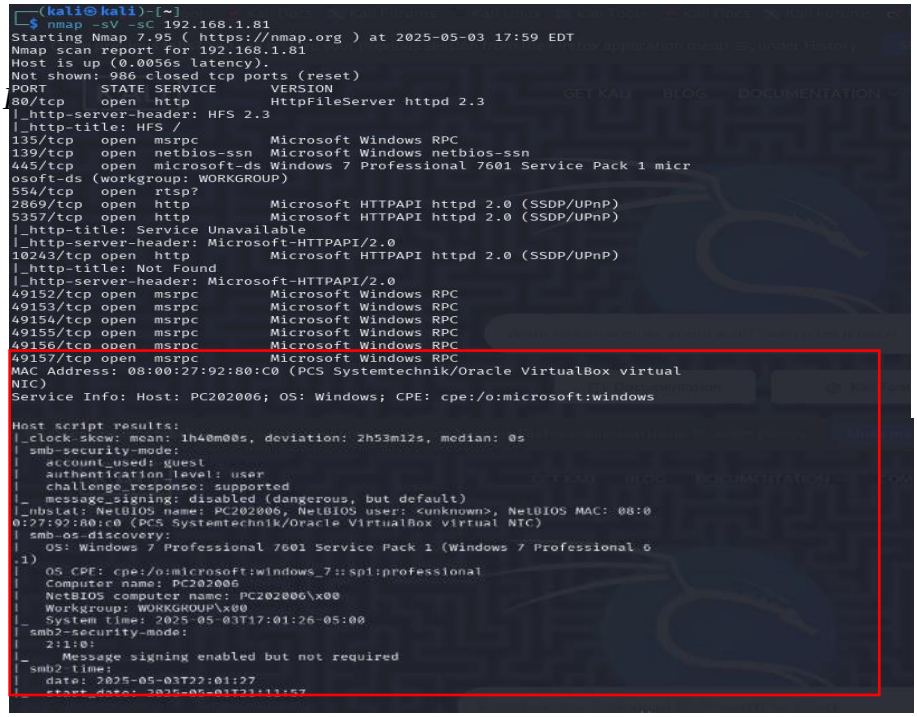
Nmap -sV -sC 192.168.1.81

Este comando se utiliza para escanear la máquina con la dirección IP 192.168.1.81. Su propósito es no solo identificar los puertos que están abiertos, sino también detectar qué servicios se encuentran activos en esos puertos y, si es posible, reconocer vulnerabilidades conocidas asociadas a dichos servicios.

Este comando no solo brinda información detallada sobre el uso de los puertos, sino que también identifica el sistema operativo como Windows 7 Professional Service Pack 1 y confirma que la máquina forma parte del grupo de trabajo WORKGROUP.

Figura 5.

Escaneo de la Maquina Windows – Nmap -sV -sC 192.168.1.81.



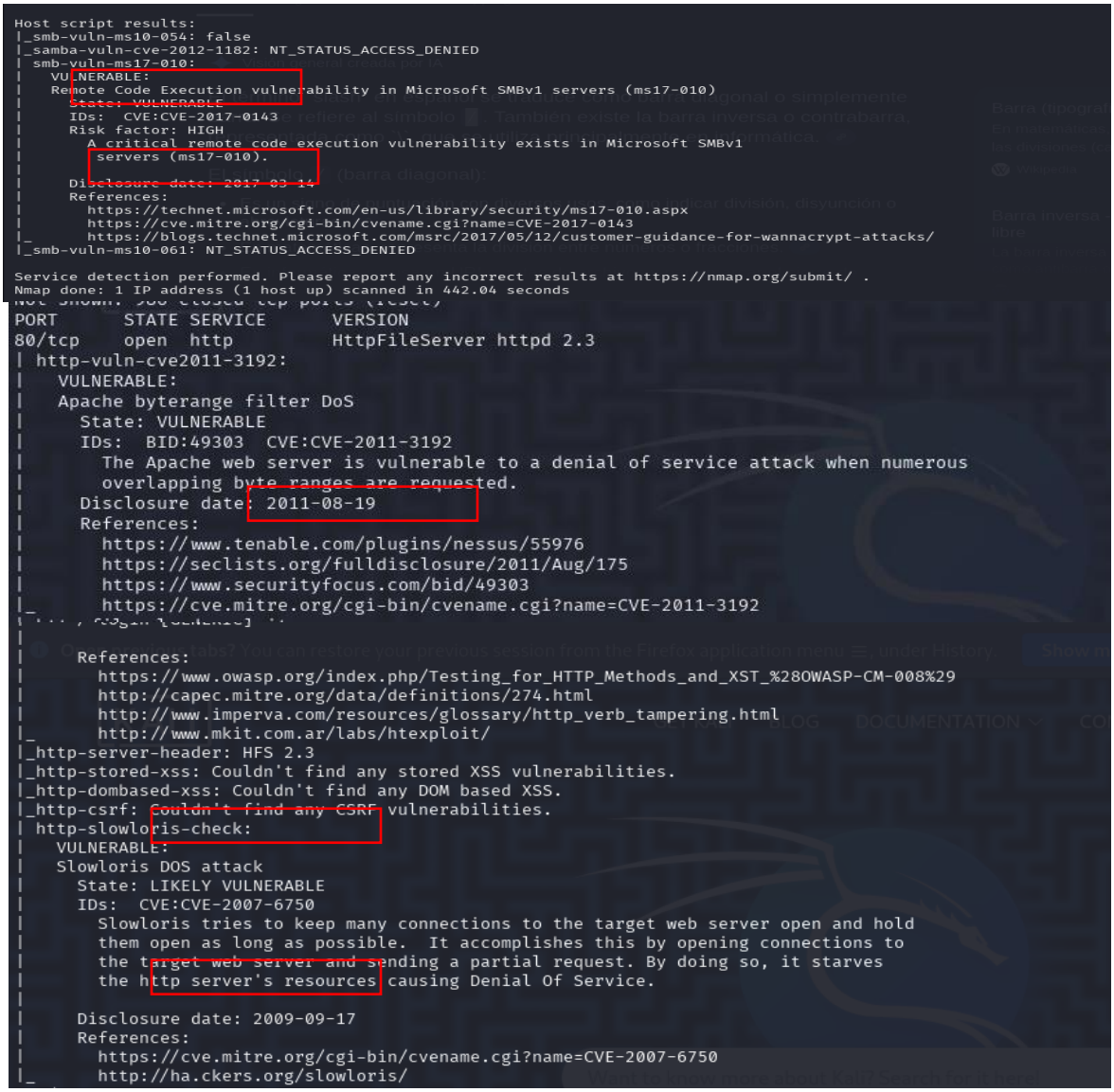
Nota. Identificación de versiones de la máquina.

Nmap -sV --script vuln 192.168.1.81

Se identifican los siguientes ID de vulnerabilidades para su posterior explotación: CVE-2017-0143, CVE-2012-1182, CVE-2011-3192 y CVE-2007-6750

Figura 6.

Escaneo de la Maquina Windows – nmap -sV --script vuln 192.168.1.81.



Nota. Se identifican los siguientes ID de vulnerabilidades para su posterior explotación: CVE-2017-0143, CVE-2012-1182, CVE-2011-3192 y CVE-2007-6750.

CVE-2017-0143 EternalBlue

Es una vulnerabilidad crítica que reside en la forma en que las versiones antiguas de Windows manejan el protocolo SMBv1. Este fallo permite a un atacante enviar paquetes maliciosos para obtener control total del sistema con privilegios de administrador. Su notoriedad se disparó tras la filtración por Shadow Brokers (supuestamente de la NSA), siendo clave en la propagación global de ransomware como WannaCry y malware como NotPetya, que causaron daños significativos en redes empresariales y gubernamentales. (Microsoft, 2017).

CVE-2012-1182 (FFmpeg Buffer Overflow)

Esta vulnerabilidad, identificada como un desbordamiento de búfer, afecta a la función mpeg_decode_frame en la biblioteca FFmpeg. Al procesar archivos de video MPEG maliciosamente manipulados, una aplicación que use una versión vulnerable de FFmpeg puede sufrir corrupción de memoria, ejecución de código arbitrario o denegación de servicio, comprometiendo la estabilidad del sistema. (MITRE, 2012).

CVE-2011-3192 (Apache Range Header DoS)

Conocida como Apache Range Header DoS, esta vulnerabilidad afecta a las versiones 1.3, 2.0 y 2.2 del servidor web Apache HTTP Server. Los atacantes pueden enviar solicitudes HTTP con el encabezado Range modificado para solicitar múltiples fragmentos superpuestos. Esto consume recursos excesivos (CPU y memoria) del servidor, pudiendo llevarlo a fallar o dejar de responder. Al no requerir autenticación previa, representa una amenaza seria para numerosos servidores Apache en todo el mundo. (CVE Details, 2011).

CVE-2007-6750 (Apache HTTP Server Request Header Parsing Flaw)

Finalmente, la vulnerabilidad CVE-2007-6750 también afecta al servidor Apache HTTP Server, originándose en un fallo al procesar ciertos encabezados de solicitudes entrantes. Los

atacantes pueden enviar peticiones maliciosas que causan inestabilidad o saturación del servidor, resultando en una denegación de servicio. Al igual que CVE-2011-3192, no requiere autenticación, lo que la convierte en una amenaza significativa para miles de sitios web y servicios que dependen de Apache (CVE Details, 2007).

Metasploit

Es una herramienta de código abierto clave para profesionales de la ciberseguridad. Su función principal es permitir la creación y ejecución de ataques simulados en sistemas remotos con el fin de descubrir vulnerabilidades. Gracias a su amplia gama de módulos (incluyendo post-explotación e ingeniería social), Metasploit es vital para emular ataques reales, lo que facilita a los equipos de seguridad la identificación y corrección de fallos antes de que sean explotados por atacantes maliciosos. (Metasploit, 2025)

Msfdb Reinit. Este comando se usa para limpiar y restablecer la base de datos de Metasploit a su estado original. Es una operación potente que elimina permanentemente toda la información almacenada, por lo que requiere precaución al ejecutarla.

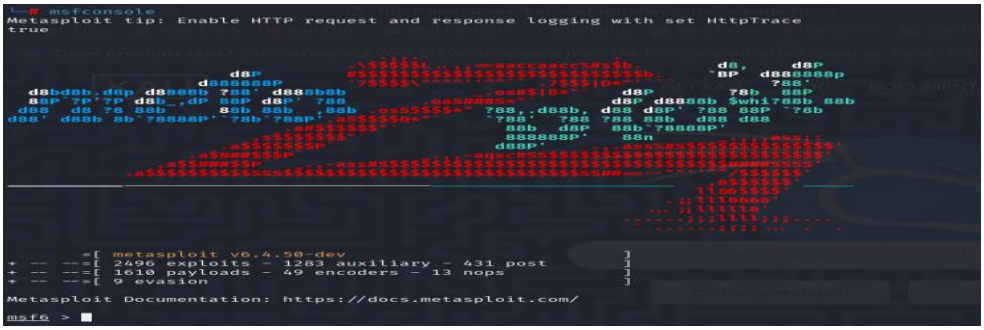
Figura 7.

Limpiar y Reiniciar la BD msfdb reinit

Nota. comando para limpiar y reiniciar los servicios de la BD metasploit.

Figura 8.

Ingreso a Metasploit.

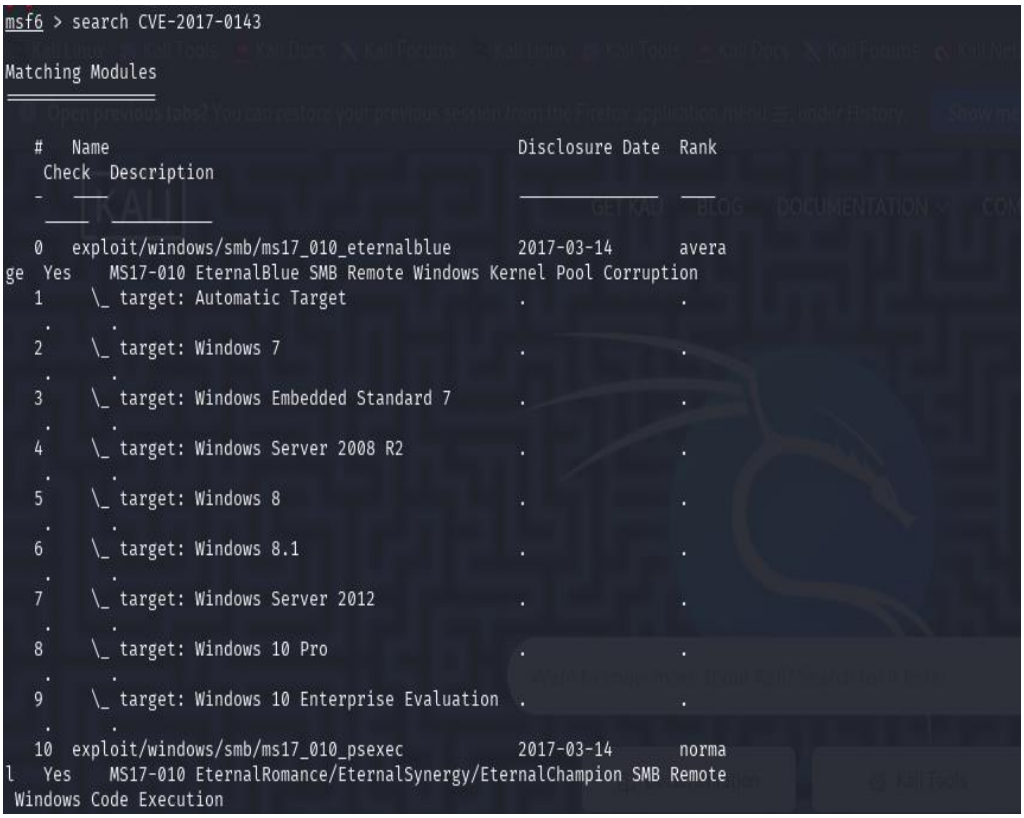


Nota. Ingreso a framework de Metasploit.

Dentro del framework utilizamos el comando de búsqueda de las vulnerabilidades.

Figura 9.

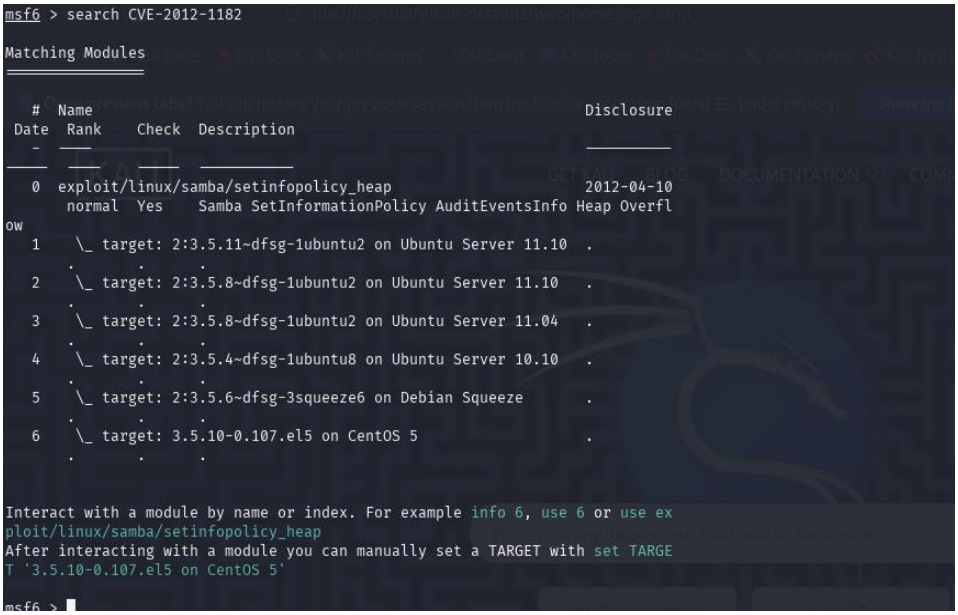
Search CVE-2017-0143.



Nota. Búsqueda y posibles explotaciones de la vulnerabilidad.

Figura 10.

Search CVE-2012-1182.



Nota. Búsqueda y posibles explotaciones de la vulnerabilidad.

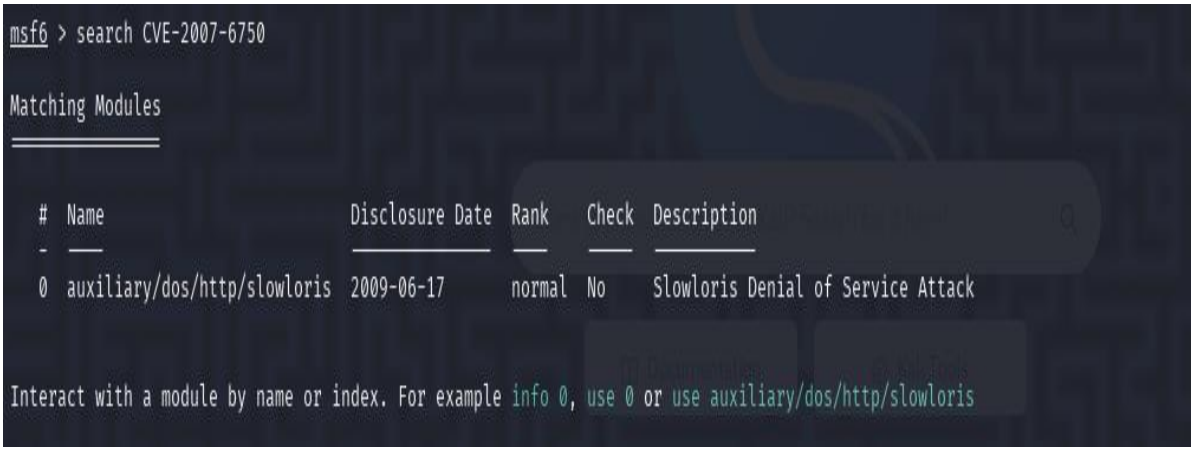
Figura 11.

Search CVE-2011-3192.

Nota. Búsqueda y posibles explotaciones de la vulnerabilidad.

Figura 12.

Search CVE-2007-6750.



Nota. Búsqueda y posibles explotaciones de la vulnerabilidad.

Slowloris. Es una técnica de denegación de servicio (DoS) que satura un servidor web. Lo hace al establecer y mantener una gran cantidad de conexiones HTTP abiertas, enviando un ritmo extremadamente lento. De esta forma, consume todos los recursos del servidor sin necesidad de generar un gran volumen de tráfico.datos a

Para explotar la vulnerabilidad CVE-2017-0143, utilizaremos el siguiente exploit de Metasploit.

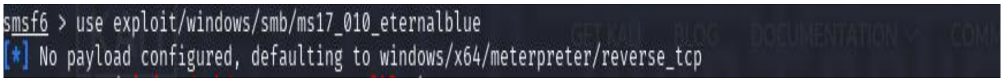
Use exploit/windows/smb/ms17_010_eternalblue

Además, se deben configurar los siguientes parámetros para el ataque con el comando options.

- set RHOSTS [192.168.1.81]
- set LHOST [192.168.1.82]
- set LPORT [445]

Figura 13.

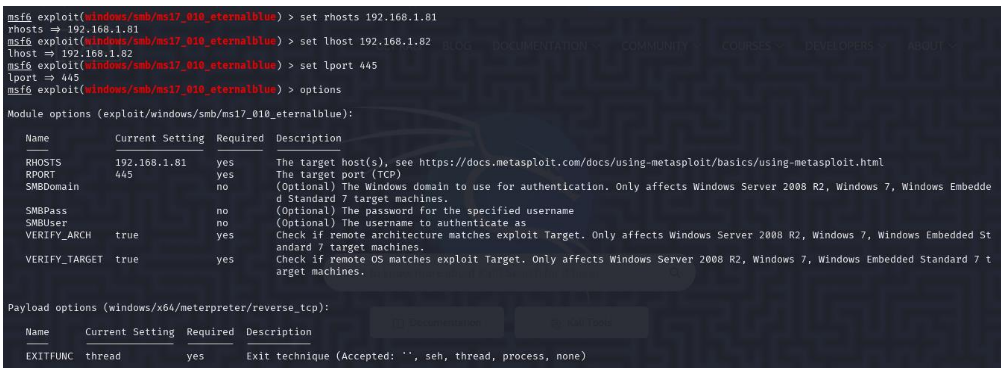
Utilización del Exploit.



Nota. Se selecciono el exploit el cual será utilizado dentro de la vulnerabilidad.

Figura 14.

Configuración de los Parámetros del Exploit, Ip Origen, Ip Destino y Puerto.

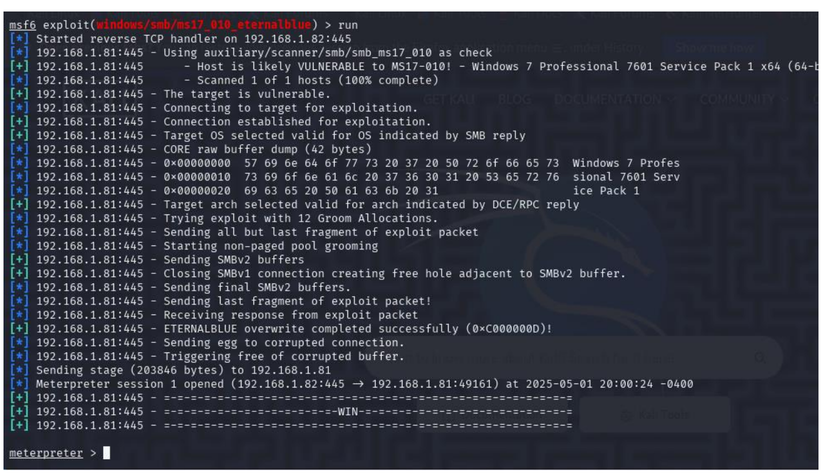


Nota. Se agregaron los parámetros del exploit.

Procedemos a iniciar el ataque mediante el comando run.

Figura 15.

Ejecución del Exploit.



Nota. Se observa que la conexión con la máquina Windows se ha establecido exitosamente.

Utilizamos el comando Shell para interactuar con el sistema operativo del destino y whoami para mostrar la ruta del directorio actual.

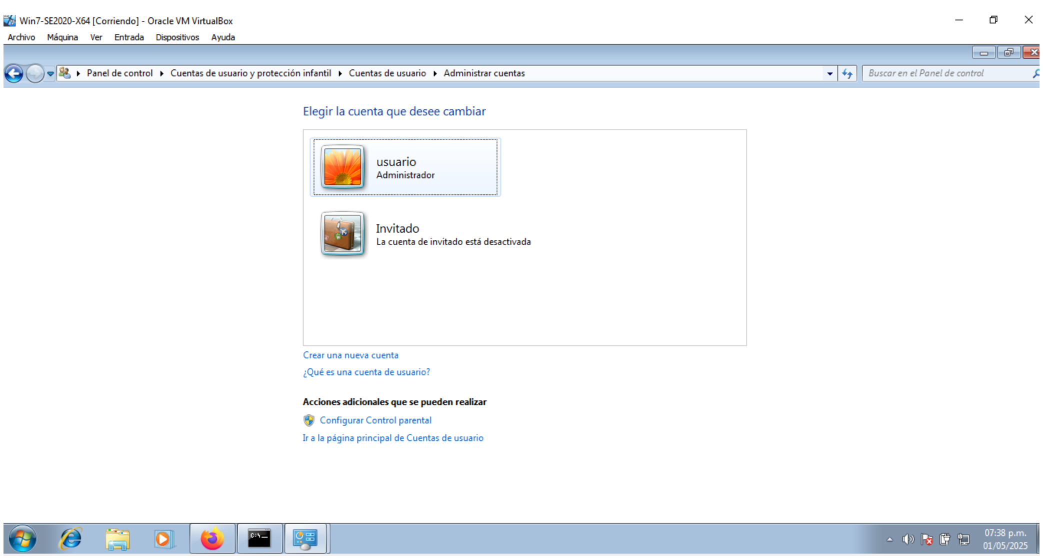
Figura 16.

Uso de Comandos Shell y Whoami.

Nota. Se utiliza el comando Shell para interactuar con la maquina vulnerada.

Figura 17.

Usuarios Actuales de la Maquina Atacada.



Nota. Se reviso los usuarios actuales del sistema.

Se creó el usuario administrador "JohanCastillo" utilizando el comando net user JohanCastillo /add. Posteriormente, se agregó al grupo de administradores con el comando net localgroup Administradores JohanCastillo /add.

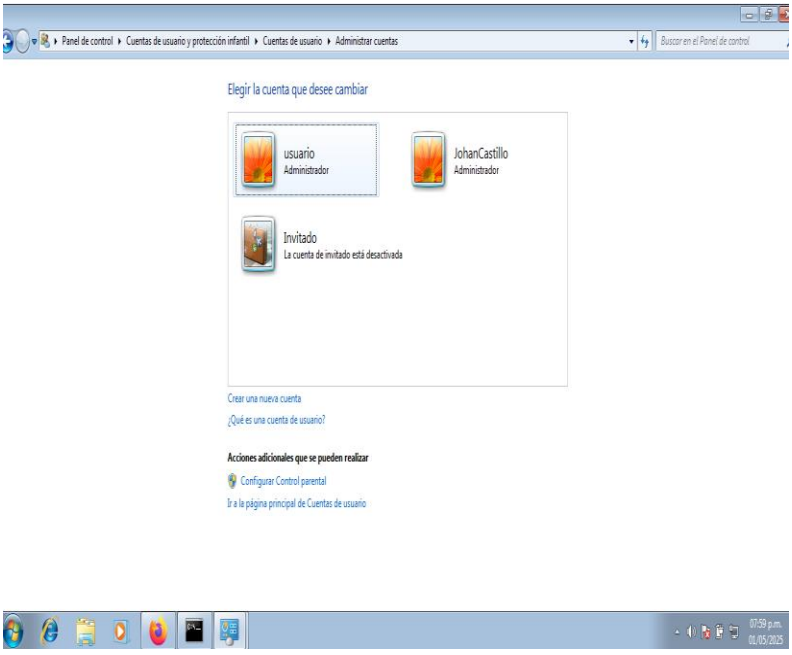
Figura 18.

Datos Actuales de la Maquina Atacada.

Nota. Se puede evidenciar los datos relevantes de la maquina víctima y se crea el usuario administrador.

Figura 19.

Evidencia de la Creación del Usuario en la Maquina Atacada.



Nota. validación de la creación del usuario JohanCastillo.

Figura 20.

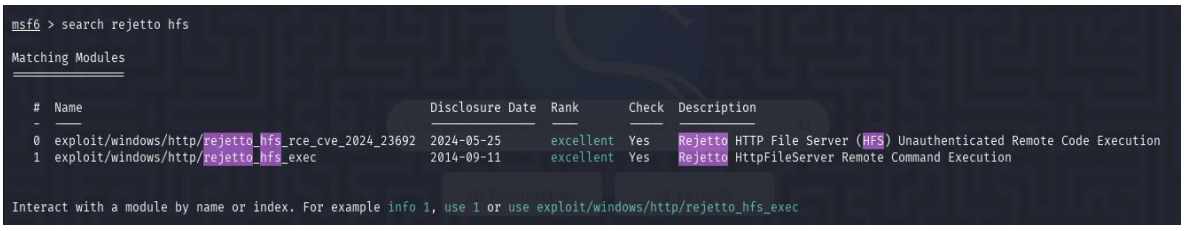
Interacción en la Maquina Atacada.

Nota. Se ejecutó la aplicación .exe ubicada en el directorio del usuario "semi" desde la máquina Kali Linux.

Toma de control de la maquina con la explotación de la vulnerabilidad Rejetto hfs.

Figura 21.

Utilizamos el Comando Search para la Vulnerabilidad Rejetto Hfs.



Nota. Se procede a ocupar el exploit de la vulnerabilidad rejetto.

Figura 22.

Seleccionamos la Opción Rejetto_Hfs_Exe.

Nota. Ocupamos el exploit Rejetto para su posterior configuración.

Figura 23.

Configuración de los Parámetros Exploit. Ip Destino y Ejecución Exploit "Run".

Nota. Proceso de la ejecución del exploit.

Figura 24.

Interacción con la maquina Windows mediante la vulnerabilidad rejetto hfs.

Nota. Interacción con los ficheros y documentos de la maquina atacada.

De acuerdo con la figura 24 se observa que ahora tenemos control de la máquina atacada y podemos visualizar todos los documentos de las diferentes carpetas del sistema operativo.

Repuesta ante un ataque informático.

Cuando se identifica un posible ataque en la red, la respuesta inmediata consiste en verificar la alerta y analizar su origen y gravedad, considerando fuentes como sistemas IDS, IPS, EDR o firewalls. Si la amenaza es confirmada, se procede a su contención, aislando los dispositivos afectados y bloqueando el tráfico malicioso mediante herramientas de seguridad. Al mismo tiempo, se deben recopilar evidencias digitales tanto volátiles como persistentes para su análisis forense, y notificar al equipo especializado en respuesta a incidentes (CSIRT).

¿Cómo podemos prevenir el ataque identificado y otros futuros ataques?

Para prevenir ataques similares a EternalBlue, se recomienda aplicar el parche MS17-010 y desactivar el protocolo SMBv1, promoviendo el uso de versiones más seguras. Además, se deben implementar buenas prácticas como la segmentación de red, auditorías regulares, control de accesos basado en el principio de mínimo privilegio, y monitoreo continuo con soluciones IDS/IPS y SIEM. Es esencial distinguir entre el Blue Team, que se dedica a la defensa proactiva, y el equipo de respuesta a incidentes, que actúa cuando ya se ha producido un evento. Al trabajar con el CIS (Center for Internet Security), el Blue Team puede apoyarse en sus marcos y estándares para fortalecer la seguridad mediante configuraciones seguras y gestión de vulnerabilidades. Herramientas como SIEM facilitan la recolección y análisis de datos en tiempo real, mejorando la detección, respuesta y cumplimiento normativo. En cuanto a la contención de ataques, se destacan tecnologías como firewalls de próxima generación (NGFW), sistemas de aislamiento de endpoints integrados en EDR, y plataformas IDS/IPS como Snort, Suricata, Cisco

Secure IPS o Wazuh, que permiten una detección y mitigación eficaz de amenazas en tiempo real.

Conclusiones

La ciberseguridad no debe entenderse únicamente como un conjunto de herramientas tecnológicas, sino como un campo estratégico y transversal que requiere conocimiento, conciencia y compromiso a todos los niveles de la organización. Desde este enfoque, se concluye que la construcción del conocimiento en ciberseguridad implica desarrollar una comprensión profunda sobre las amenazas actuales, las vulnerabilidades inherentes a los sistemas y el factor humano como vector crítico de riesgo. La integración de buenas prácticas, marcos normativos y cultura de seguridad fomenta entornos digitales resilientes y éticamente responsables. Promover la formación continua, el análisis crítico de incidentes y la adopción de medidas preventivas fortalece no solo la capacidad técnica, sino también la toma de decisiones informadas, contribuyendo a una postura de seguridad madura y sostenible. Solo mediante la educación constante y el aprendizaje organizacional se puede enfrentar con eficacia un entorno digital cada vez más complejo y desafiante.

Recomendaciones

Para fortalecer la seguridad informática en una organización, se recomienda una estrategia integral enfocada en tres frentes clave: ataques cibernéticos, vulnerabilidades técnicas e ingeniería social. En cuanto a los ataques cibernéticos (como malware, ransomware o DDoS), es fundamental implementar una defensa en profundidad que combine múltiples capas de protección (firewalls, EDR, IDS/IPS y WAF), respaldada por soluciones SIEM que permitan la detección temprana de anomalías y la correlación de eventos. Además, debe establecerse un plan de respuesta a incidentes (IRP) probado mediante simulacros, segmentar la red para limitar el impacto de intrusiones y mantener copias de seguridad frecuentes, seguras y con acceso restringido. Respecto a las vulnerabilidades técnicas, se sugiere establecer un programa de gestión de vulnerabilidades con escaneos regulares, automatizar parches y actualizaciones, aplicar el principio de mínimo privilegio, fortalecer las configuraciones siguiendo estándares como los CIS Benchmarks, y realizar pruebas de penetración periódicas. En lo relacionado con la ingeniería social, es crucial implementar programas continuos de formación en ciberseguridad, realizar simulacros de phishing, establecer canales seguros de verificación de identidad, habilitar autenticación multifactor (MFA) para accesos críticos y fomentar una cultura de reporte interno. Todas estas medidas deben integrarse dentro de un marco de gestión de seguridad como ISO/IEC 27001, y actualizarse regularmente con base en el contexto organizacional, la evolución tecnológica y las amenazas emergentes.

Referencias Bibliográficas

CVE Details. (2011). CVE-2011-3192: Apache HTTPD Range Header DoS. CVE Details. https://www.cvedetails.com/cve/CVE-2011-3192/

CVE Details. (2007). CVE-2007-6750: Apache HTTP Server ap_get_basic_auth_pw Authentication Bypass Vulnerability. CVE Details. https://www.cvedetails.com/cve/CVE-2007-6750/

Congreso de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - la información y los datos.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de Colombia. (2008). *Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Metasploit. (2025). Metasploit Framework. https://www.metasploit.com/

Microsoft. (2017). Microsoft Security Bulletin MS17-010-Critical.https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

MITRE. (2012). CVE-2012-1182 Detail. Common Vulnerabilities and Exposures. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1182

NMAP Network Scanning. (2024). *Nmap: The Network Mapper. https://nmap.org/*

Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012, sobre protección de datos personales.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Apéndices

Apéndice A.

Enlace del Video de la Sustentación

https://unadvirtualedu-my.sharepoint.com/:f:/g/personal/jccastillo_unadvirtual_edu_co/Evq3EnXJNitHr0ktk8b9G_wBFehdEuwUFdBDQDAy2kxWDQ?e=M4eJp2