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

Oscar David Perilla Molina

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

A mis padres y familiares, por su apoyo constante y por enseñarme el valor del esfuerzo y la perseverancia.

A mis docentes, quienes con su guía y conocimientos hicieron posible este proceso de formación.

Y a todas las personas que, de una u otra forma, aportaron a la culminación de este trabajo final.

Agradecimientos

Agradezco a Dios por la oportunidad de crecer y ser mejor persona y profesional, a la Universidad y a cada uno de los docentes que acompañaron este proceso formativo. Su dedicación, profesionalismo y guía fueron fundamentales para el desarrollo de este trabajo. Extiendo mi gratitud a mi familia, por su apoyo incondicional, y a quienes, con sus aportes, comentarios y conocimientos, contribuyeron a enriquecer este proyecto.

A todos, gracias por ser parte de este logro.

Resumen

El objetivo del presente informe es analizar y documentar un ejercicio avanzado de ciberseguridad mediante un enfoque metodológico dual que integra actividades ofensivas de Red Team y acciones defensivas de Blue Team en un entorno controlado. Desde la perspectiva ofensiva, se ejecutó una metodología de pruebas de penetración que incluyó reconocimiento, escaneo de servicios, explotación de vulnerabilidades y movimiento lateral, aplicada sobre una infraestructura compuesta por dos sistemas Windows vulnerables (Host-A y Host-B) y una máquina atacante Parrot. El análisis permitió identificar la exposición del protocolo SMB y la vulnerabilidad MS17-010 (EternalBlue), cuya explotación facilitó el acceso inicial, el escalamiento de privilegios y la implementación de técnicas de pivoting mediante un proxy SOCKS para comprometer un segundo host. Desde la perspectiva defensiva, se desarrolló un proceso de respuesta a incidentes alineado con la guía NIST 800-61, mediante la identificación de indicadores de compromiso, el análisis de conexiones, procesos y eventos del sistema, el aislamiento del host afectado y la preservación de evidencia volátil para análisis forense. Como resultado, se confirmaron las técnicas de intrusión empleadas, se contuvo el incidente y se definió un plan de hardening orientado a mitigar riesgos futuros, incluyendo gestión de parches, deshabilitación de SMBv1, segmentación de red, fortalecimiento de credenciales y monitoreo continuo mediante SIEM y SOAR.

Palabras clave**:** EternalBlue, hardening, NIST, pivoting, SIEM

Abstract

This report examines an advanced cybersecurity exercise conducted under a dual methodological approach that combines offensive Red Team operations and defensive Blue Team incident response activities within a controlled laboratory environment. The offensive assessment followed a structured penetration testing workflow, including service discovery, vulnerability exploitation, privilege escalation, and lateral movement across two intentionally vulnerable Windows hosts. The analysis confirmed the exploitation of the MS17-010 vulnerability affecting the SMB protocol, enabling initial compromise and network pivoting through a SOCKS-based tunneling mechanism. From a defensive standpoint, the incident was investigated using an incident response framework aligned with NIST SP 800-61, focusing on the identification of indicators of compromise, analysis of system processes and network connections, host isolation, and preservation of volatile memory for forensic examination. The results demonstrate the effectiveness of coordinated Red Team and Blue Team activities in validating attack paths, detecting intrusions, and defining targeted containment and hardening measures, including patch management, protocol deprecation, network segmentation, credential reinforcement, and continuous monitoring through SIEM and SOAR platforms.

Keywords: EternalBlue, hardening, NIST, pivoting, SIEM

Tabla de contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team: Equipo responsable de la defensa de la infraestructura tecnológica de una organización. Su labor se centra en la detección, análisis, contención y mitigación de incidentes de seguridad, así como en la implementación de medidas preventivas como monitoreo continuo, hardening y gestión de vulnerabilidades (S2GRUPO, 2024).

CIS (Center for Internet Security): Organización internacional dedicada al desarrollo de estándares y controles de seguridad reconocidos globalmente. Los CIS Benchmarks proporcionan guías técnicas para el fortalecimiento de sistemas operativos, aplicaciones, dispositivos de red y servicios tecnológicos (Center for Internet Security, n.d.).

EDR (Endpoint Detection and Response): Solución de seguridad enfocada en la protección de endpoints que permite detectar comportamientos maliciosos, analizar procesos en tiempo real, responder ante amenazas y recopilar evidencia para análisis forense (Trend Micro, 2025).

EternalBlue: Exploit que aprovecha la vulnerabilidad MS17-010 en el protocolo SMBv1 de sistemas Windows, permitiendo la ejecución remota de código. Ha sido utilizado en ataques de alto impacto como WannaCry y facilita accesos no autorizados y movimientos laterales dentro de redes comprometidas Avast. (2020).

Hardening: Proceso de fortalecimiento de sistemas mediante la eliminación de configuraciones inseguras, aplicación de parches, restricción de servicios innecesarios, refuerzo de políticas de autenticación y reducción de la superficie de ataque, con el fin de prevenir intrusiones (Hardening Informático, n.d.).

Metasploit: Framework de pruebas de penetración utilizado para identificar vulnerabilidades, desarrollar y ejecutar exploits y payloads controlados. Es ampliamente empleado en auditorías de seguridad y entornos de práctica autorizados para actividades de post-explotación y movimiento lateral (Imperva, n.d.).

Movimiento lateral (Lateral Movement): Conjunto de técnicas empleadas por un atacante tras comprometer un sistema inicial, con el objetivo de desplazarse dentro de la red interna y acceder a equipos con mayores privilegios mediante credenciales robadas, exploits o comunicaciones internas legítimas (Cloudflare, n.d.).

Pivoting: Técnica utilizada durante ataques o pruebas de penetración que permite a un atacante moverse desde un sistema comprometido hacia otros equipos de la red interna, mediante la creación de túneles o proxys que habilitan el acceso a segmentos originalmente inaccesibles (Deep Hacking, 2021).

Red Team: Equipo encargado de simular ataques reales contra una organización con el propósito de evaluar su nivel de seguridad. Emplea técnicas ofensivas como explotación de vulnerabilidades, movimiento lateral, ingeniería social y evasión de controles defensivos para identificar fallos críticos antes de que sean explotados por actores maliciosos (IBM, 2025).

SIEM (Security Information and Event Management): Plataforma que centraliza, correlaciona y analiza eventos de seguridad provenientes de múltiples fuentes, permitiendo la detección de anomalías, generación de alertas, análisis forense y monitoreo en tiempo real (Microsoft, n.d.).

SMB (Server Message Block): Protocolo de red utilizado principalmente en sistemas Windows para el intercambio de archivos, impresoras y otros recursos. Versiones antiguas como SMBv1 presentan vulnerabilidades críticas que pueden permitir ejecución remota de código o divulgación de información (IBM, 2025).

SOAR (Security Orchestration, Automation and Response): Tecnología que permite automatizar y orquestar respuestas ante incidentes de seguridad, ejecutando acciones como aislamiento de equipos, bloqueo de direcciones IP, generación de reportes y deshabilitación de cuentas comprometidas (Palo Alto Networks, n.d.).

Sockets / SOCKS Proxy: Protocolo que permite enrutar tráfico de red a través de un servidor intermedio. En contextos de pruebas ofensivas, se utiliza para redirigir conexiones desde la máquina atacante hacia redes internas mediante un host previamente comprometido, facilitando técnicas de pivoting (Proxy SOCKS, n.d.).

Introducción

Hoy en día donde la tecnología se ha convertido en la base de casi todas las actividades humanas, entender cómo ocurren los ataques informáticos y cómo responder a ellos ya no es un tema exclusivo, es una necesidad. Durante el desarrollo de este trabajo, se tiene la oportunidad de ver ambos lados de la ciberseguridad, el del atacante que busca explotar una vulnerabilidad y el del defensor que debe reaccionar, analizar y proteger su infraestructura bajo presión.

La primera parte del ejercicio se centró en entender cómo un sistema vulnerable puede convertirse en la puerta de entrada para un atacante. A través de herramientas de reconocimiento, escaneo y explotación, se reprodujo un ataque real usando la vulnerabilidad EternalBlue, lo que permitió observar de primera mano cómo una acción que se posterga (actualización) puede abrir el camino a un movimiento lateral y comprometer otros equipos dentro de la red. Esta experiencia dejó claro lo rápido que puede escalar una intrusión cuando no existen medidas preventivas adecuadas.

La segunda parte se abordó desde el rol del Blue Team, donde el objetivo ya no era atacar, sino contener y recuperar. Aquí se evidencia la necesidad de analizar logs, procesos, conexiones y evidencia en memoria, siguiendo buenas prácticas como las que plantea el NIST 800-61. También fue fundamental aplicar medidas de hardening, comprender la utilidad de herramientas como los SIEM y revisar controles de seguridad como los del CIS, que ayudan a fortalecer cualquier infraestructura.

Este trabajo reúne esas dos miradas: la ofensiva y la defensiva. Ambas se complementan y permiten entender mejor cómo se producen los ataques y qué acciones concretas pueden evitar que un incidente aislado se convierta en una crisis mayor.

Justificación

La ciberseguridad se ha convertido en uno de los pilares fundamentales para el funcionamiento de cualquier organización, sin importar su tamaño o sector. Los ataques informáticos ya no son eventos aislados, sino situaciones reales y constantes que pueden afectar servicios vitales, esto debido a que pueden comprometer información crítica y detener por completo la operación de una empresa. Por esta razón, entender cómo se origina un ataque, cómo avanza y cómo debe ser contenido es un conocimiento que trasciende lo técnico y se convierte en una competencia esencial para cualquier profesional del área.

Este trabajo tiene una gran relevancia porque integra dos perspectivas que, aunque diferentes, se complementan profundamente: la visión del Red Team, encargado de simular ataques reales, y la del Blue Team, responsable de detectar, responder y fortalecer la infraestructura ante esas mismas amenazas. Al realizar ambas fases dentro de un mismo escenario controlado, fue posible observar de manera práctica la importancia de mantener sistemas actualizados, aplicar buenas prácticas de hardening, monitorear la red y reaccionar con rapidez ante señales tempranas de intrusión.

Asimismo, la simulación del ataque mediante EternalBlue y el análisis defensivo posterior permiten comprender de primera mano los riesgos que enfrenta cualquier entorno que descuide la gestión de vulnerabilidades o carezca de controles de seguridad sólidos. Se realizo la aplicación de metodologías reconocidas, como el marco NIST 800-61 para la respuesta a incidentes, y estándares como los controles CIS, que orientan buenas prácticas para reducir la superficie de ataque.

Objetivos

Objetivo General

Analizar de forma detallada un escenario de ciberseguridad que combina técnicas ofensivas y defensivas, identificando el paso a paso de como se produce una intrusión mediante la explotación de vulnerabilidades, y aplicando procedimientos de respuesta, contención y hardening que permitan fortalecer la infraestructura afectada.

Objetivos Específicos

Identificar y documentar el vector de ataque, las vulnerabilidades explotadas, las técnicas de movimiento lateral empleadas y las evidencias generadas durante el proceso ofensivo, comprendiendo el alcance real del compromiso en el entorno simulado.

Aplicar un proceso estructurado de respuesta a incidentes basado en el marco NIST 800-61, analizando conexiones, procesos, eventos del sistema y evidencia volátil para contener la intrusión, preservar información clave y evaluar el impacto del ataque.

Diseñar y proponer medidas de hardening y mejora continua, incorporando buenas prácticas, controles CIS, segmentación, parches de seguridad y herramientas como SIEM/SOAR, con el fin de reducir la superficie de ataque y prevenir incidentes similares en el futuro.

Estrategias de red team

Las estrategias de Red Team implementadas se fundamentan en los marcos Cyber Kill Chain y MITRE ATT&CK, seleccionados por su capacidad para modelar amenazas reales y permitir una evaluación objetiva de la postura defensiva de una organización. El propósito del Red Team no es únicamente vulnerar sistemas, sino poner a prueba controles, procesos y capacidades humanas, simulando escenarios realistas de ataque.(*Tactics - Enterprise | MITRE ATT&CK®*, n.d.). A continuación, se listan las fases que se utilizan usualmente en esta área:

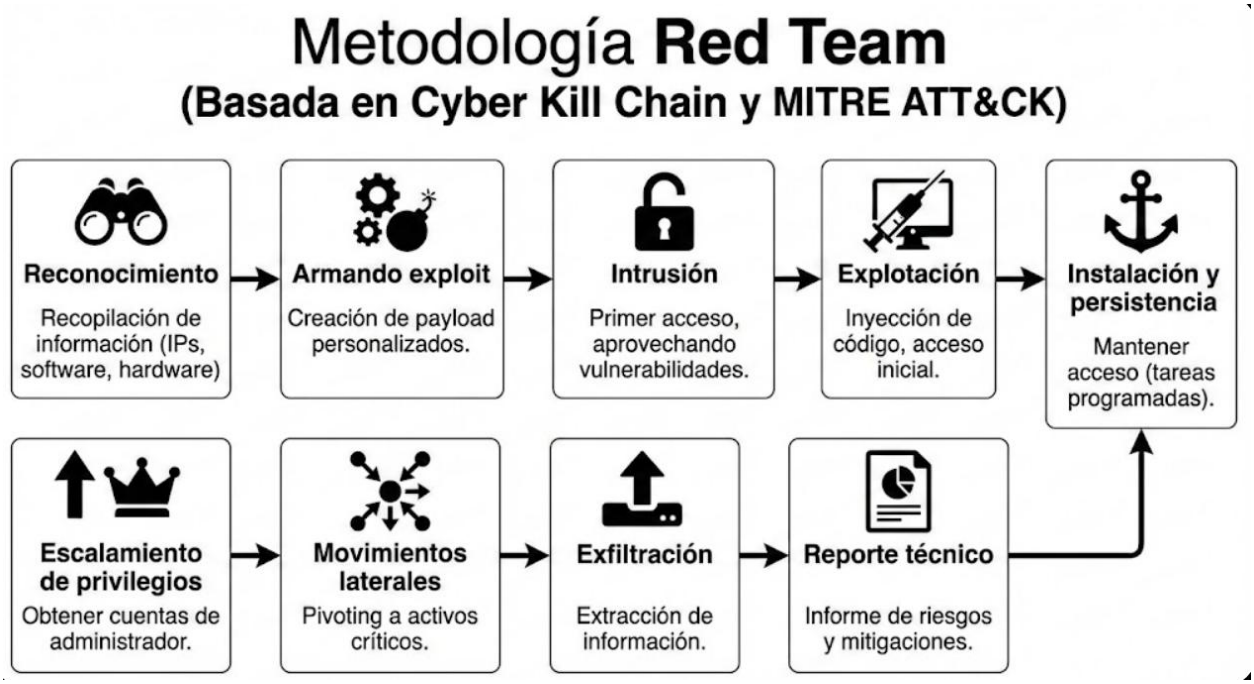
- **Reconocimiento:** Son técnicas utilizadas para recopilar la mayor cantidad de información de la víctima, es decir, se realiza un escaneo de activos (páginas web, bases de datos, canales de atención, hardware utilizado, software utilizado, versiones, IPs, entre otros). El reconocimiento puede ser activo o pasivo, cuando este es pasivo, se recopila información sin interactuar directamente con los sistemas, y activo, cuando se realizan interacciones controladas para identificar servicios, tecnologías y configuraciones. esta fase evidencia la importancia de la gestión de activos y de la exposición controlada de la información, ya que cualquier dato accesible puede ser utilizado para planificar ataques más precisos. (*Reconocimiento, Táctica TA0043 - Enterprise | MITRE ATT&CK®*, n.d.)
- **Armando exploit:** En esta fase se realiza la creación de los payload personalizados de acuerdo con las vulnerabilidades que se encontraron en la fase anterior. Esta fase destaca la diferencia entre ataques genéricos y ataques dirigidos, ya que un exploit correctamente contextualizado incrementa la probabilidad de éxito y reduce la detección, el armamento evidencia la necesidad de controles defensivos basados en comportamiento y no únicamente en firmas.

- **Intrusión:** La intrusión representa el punto de transición entre la planificación y la ejecución del ataque. Teóricamente, esta fase se enfoca en lograr el acceso inicial al sistema objetivo, aprovechando vulnerabilidades técnicas o errores de configuración e implementación.
- **Explotación:** El principal objetivo de esta fase es que el atacante logra ejecutar código o comandos en el sistema comprometido. Valida el impacto real de la vulnerabilidad explotada y habilita las fases posteriores del ataque.
- **Instalación y persistencia:** En esta fase se tiene como objetivo mantener el acceso incluso si el sistema se reinicia o se activa una mitigación sencilla. Para esto se crean tareas programadas y se manipulan los recursos.
- **Escalamiento de privilegios:** En esta fase se hace una revisión interna de vulnerabilidades y se explotan, esto se realiza para tener acceso a crear cuentas de administrador en los diferentes equipos e ir escalando con ayuda de la fase siguiente a los activos más críticos.
- **Movimientos laterales:** En esta fase el atacante tiene la capacidad para desplazarse dentro del entorno, comprometiendo múltiples sistemas. Acá se evidencia la importancia de la segmentación de red y del principio de mínimo privilegio.
- **Exfiltración:** Esta fase representa la materialización del impacto del ataque, mediante la extracción de información sensible. Teóricamente, esta fase pone de relieve la importancia de los controles de monitoreo de tráfico saliente y de la protección de datos.
- **Reporte técnico:** Creación de informe que permita mitigar los riesgos de seguridad encontrados y mostrar la gravedad de la vulnerabilidad.

A continuación, se muestra en una ilustración lo mencionado anteriormente.

Figura 1.

Fases de ataque



Fuente: Imagen tomada de (*Your 101 Guide to MITRE ATT&CK Enterprise Matrix*, n.d.)

Estrategias de blue team

En esta sección se presentan las estrategias, metodologías y paso a paso que se recomienda que un equipo de blue team utilice.

Las estrategias utilizadas para este equipo se basan en anticipar, detectar, contener y recuperar ante ataques de seguridad, por esta razón la estrategia que se sugirió es la del marco NIST 800-61. (Nelson et al., 2025)

- **Preparación:** Esta es la fase más importante de toda la estrategia utilizada, debido a que fortalece la infraestructura ante cualquier incidente. Acá se implementa la hardenización de los sistemas, se realiza la gestión de parches y actualizaciones, se aplican los controles CIS y se implementan equipos detectivos y reactivos como SIEM, SOAR, EDR, NGFW, NAC, entre otros.
- **Detección y análisis:** En esta fase se identifican las señales tempranas de un ataque, esto hace referencia a conexiones poco usuales (geográficamente sospechosas), escaneo de puertos, entre otras. Las herramientas que permiten tener este control son los SIEM y SOAR.
- **Contención:** El objetivo de esta fase es que luego de detectar el ataque, este mismo sea mitigado sin destruir la evidencia. Las herramientas utilizadas en este caso son los firewalls, switch, NAC,
- **Erradicación:** Esta fase es vital en un equipo de blue team, esto debido a que en esta fase se realiza la eliminación de todo el ataque y de esto depende que el atacante no tenga ninguna ayuda para seguir dentro del sistema. En esta fase se realizan las actualizaciones, instalación de parches de seguridad, aplicación de mejores practicas CIS.

- **Recuperación:** En esta fase el equipo infectado se reintegra a la infraestructura de forma gradual, es decir, con agentes, monitoreo intensivo tanto de trafico como de acciones, es decir, SNMP y SIEM.
- **Lecciones aprendidas:** Esta es la fase mas critica e importante del proceso, esto debido a que es donde se documenta lo ocurrido, lo que significa que es donde va a quedar el plan de acción e impacto del incidente.

A continuación se muestra en una figura el proceso mencionado.

Figura 2.

Estrategia de blue team

Fuente: Autoría propia

Red Team y Blue Team no son enfoques opuestos, sino complementarios, diseñados para evaluar y fortalecer la postura de ciberseguridad de una organización. La diferencia fundamental radica en el objetivo, la temporalidad de las acciones, el uso de herramientas y la relación con el marco legal y ético.

El Red Team adopta una postura ofensiva controlada, simulando el comportamiento real de un atacante con el propósito de identificar debilidades o vulnerabilidades sobre personas, procesos y tecnología. Por otro lado, el Blue Team opera desde una perspectiva defensiva y reactiva, enfocada en prevenir, detectar, contener, erradicar y recuperar frente a incidentes de seguridad reales o simulados. A continuación se presenta la siguiente tabla comparativa.

Tabla 1

Diferencias entre blue y red team

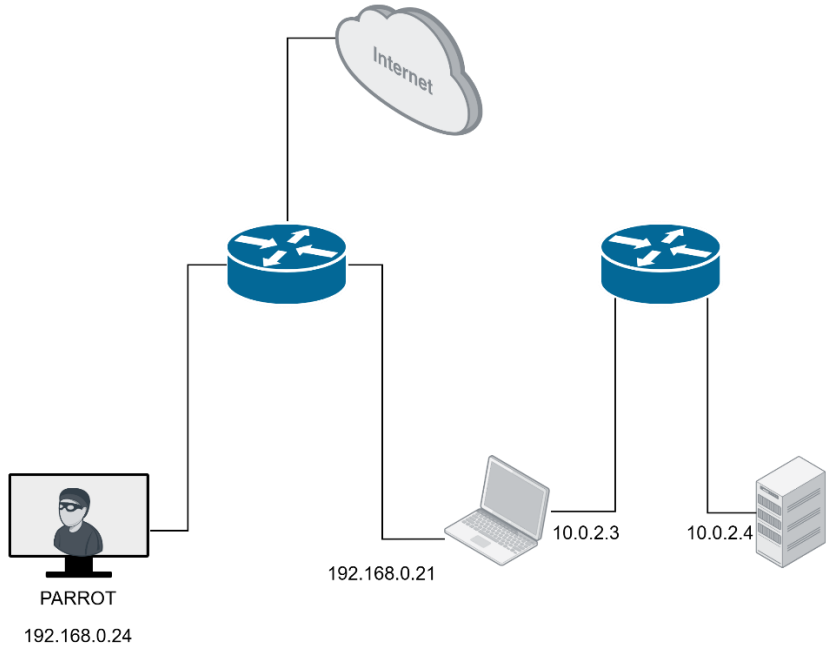
Aspecto	Red Team	Blue Team
Enfoque	Ofensivo	Defensivo
Objetivo	Explotar debilidades	Prevenir y responder
Temporalidad	Puntual y controlada	Continua
Herramientas	Metasploit, exploits, OSINT	SIEM, SOAR, EDR, NGFW
Relación legal	Bajo alcance autorizado	Cumplimiento normativo
Resultado final	Evidencia de fallas	Mejora de la postura de seguridad

Análisis desarrollo

En esta sección se explica el trabajo realizado durante el desarrollo del curso, se simulo el siguiente escenario, está compuesto de dos enrutadores (físico y virtual) y tres maquinas (Atacante – Host A y Host B). De acuerdo con lo anterior y lo mencionado en el anexo 4, el atacante debe intervenir el Host A y escalar privilegios para alcanzar y vulnerar el Host B.

Figura 3.

Topología propuesta



Fuente: Autoría propia.

Con lo anterior, se empieza a explicar el paso a paso realizado desde la maquina atacante. En la maquina Parrot se realizó un update lo cual permite actualizar la lista de paquetes disponibles (*Apt-Get Update En Linux Para Actualizar Repositorios*, n.d.)

Figura 4.

Apt-update

Fuente: Autoría propia

Con lo anterior se aplica ahora el comando upgrade el cual nos permite instalar las actualizaciones de sistema que estén disponibles. (*Diferencia Entre Apt-Get Update y Apt-Get Upgrade*, n.d.)

Figura 5.

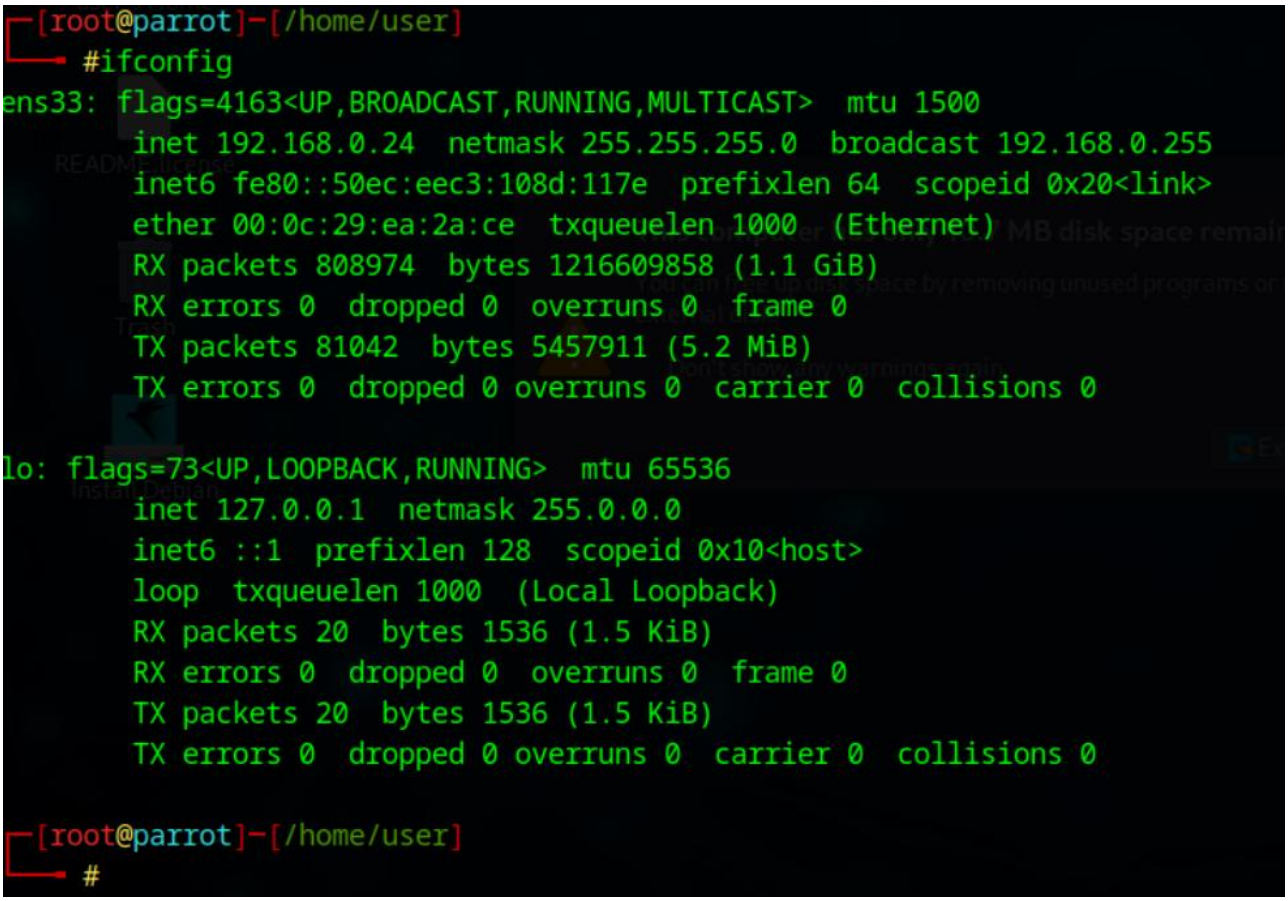
Apt upgrade

Fuente: Autoría propia

Luego de tener el sistema operativo actualizado se procede a validar el direccionamiento que tiene la máquina, en la interfaz **ens33** se tiene configurada la IP de forma dinámica.

Figura 6.

Ifconfig

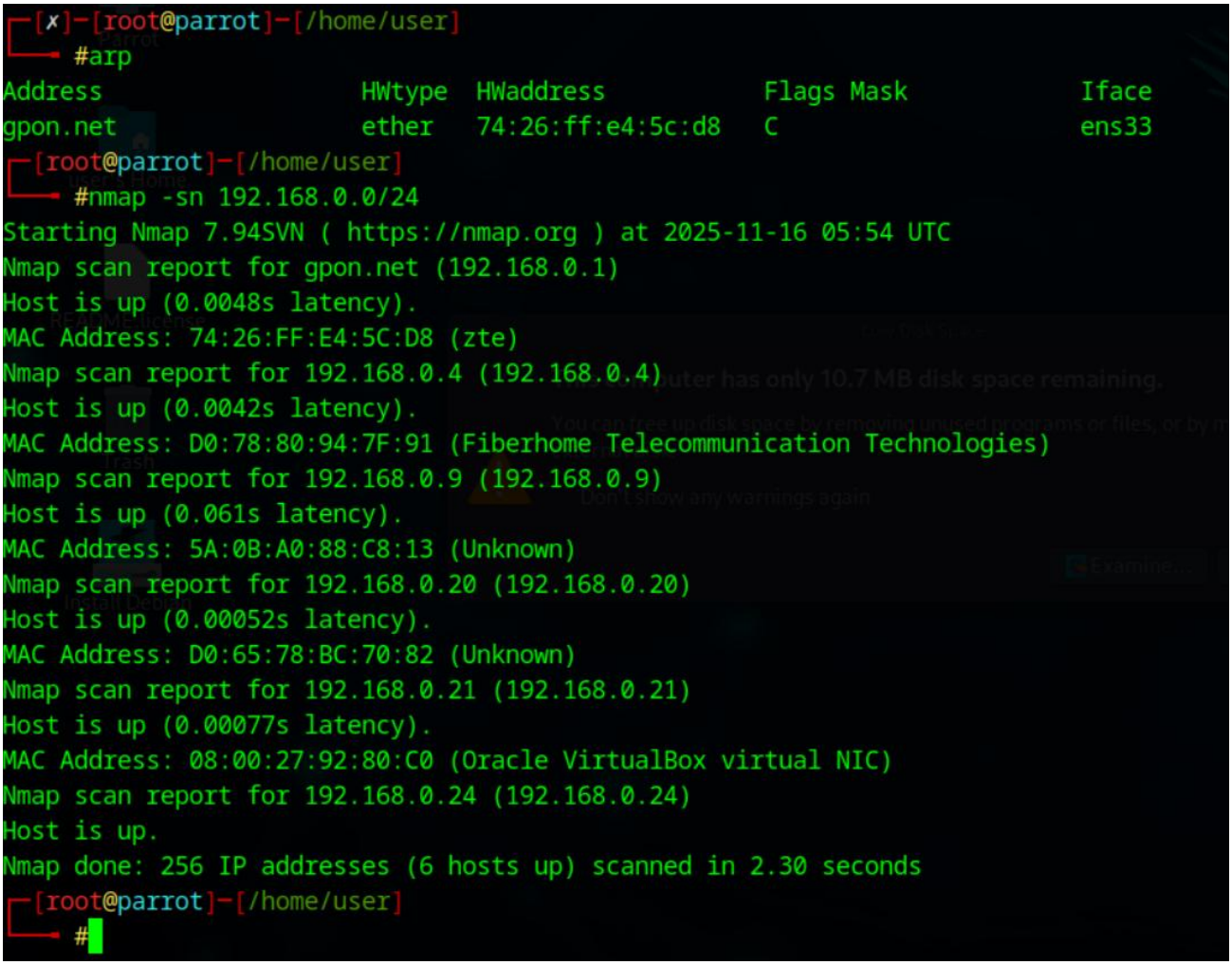


Fuente: Autoría propia

Luego de esto se realiza la revisión de la tabla ARP de la máquina, como no se encuentra ningún host sobre la tabla, se realiza un escaneo sencillo sobre toda la red en NMAP.

Figura 7.

Revisión ARP



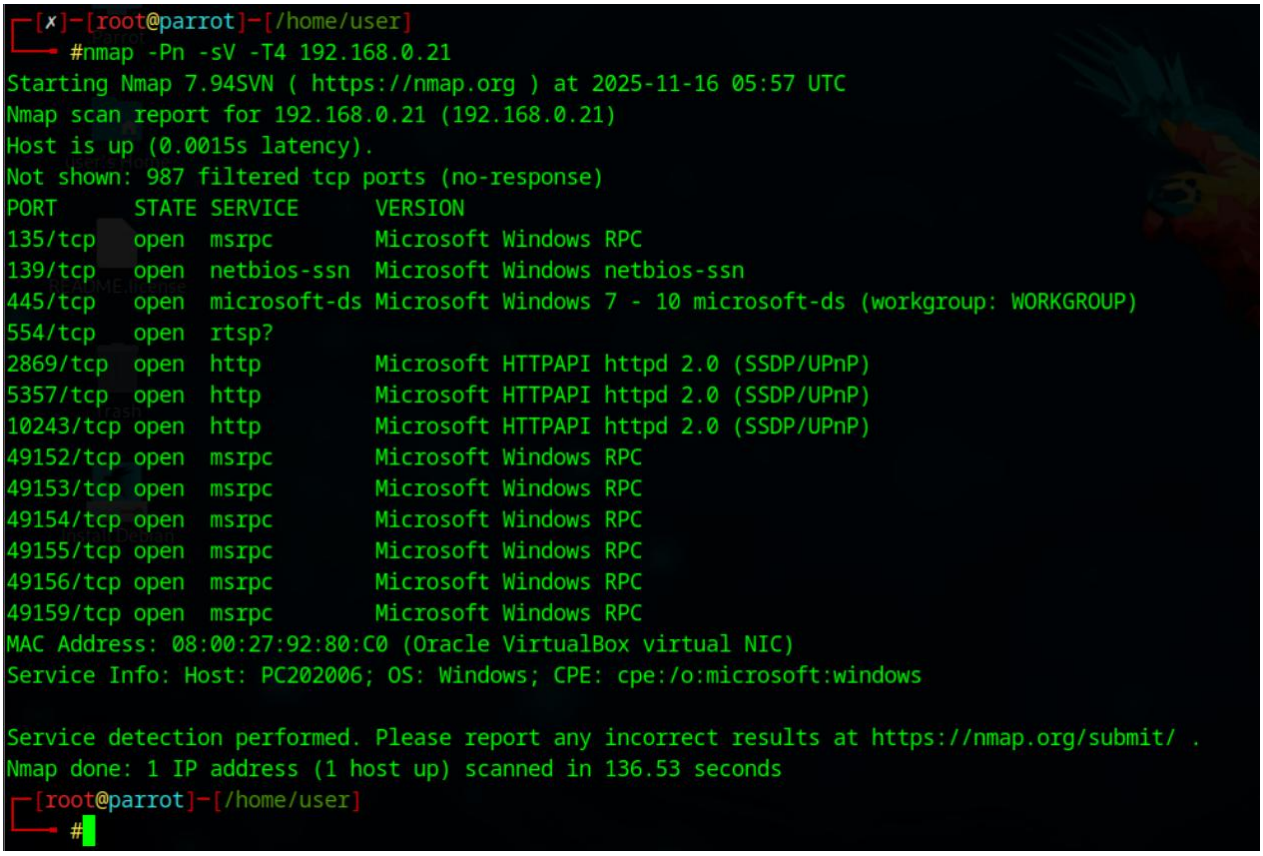
Nota: Autoría propia

De acuerdo con la figura 7, se evidencia que se está corriendo una máquina virtual sobre VirtualBox con la IP 192.168.0.21.

Con lo anterior se empieza a realizar un escaneo más detallado sobre el host mencionado anteriormente, se aplica el comando **-Pn** lo cual permite que el host destino no responda a ping y continue realizando el escaneo. El comando **-sV** permite la detección de servicios y versiones y el comando **T4** permite un escaneo pasivo de forma equilibrada. Figura 8.

Figura 8.

Nmap inicial

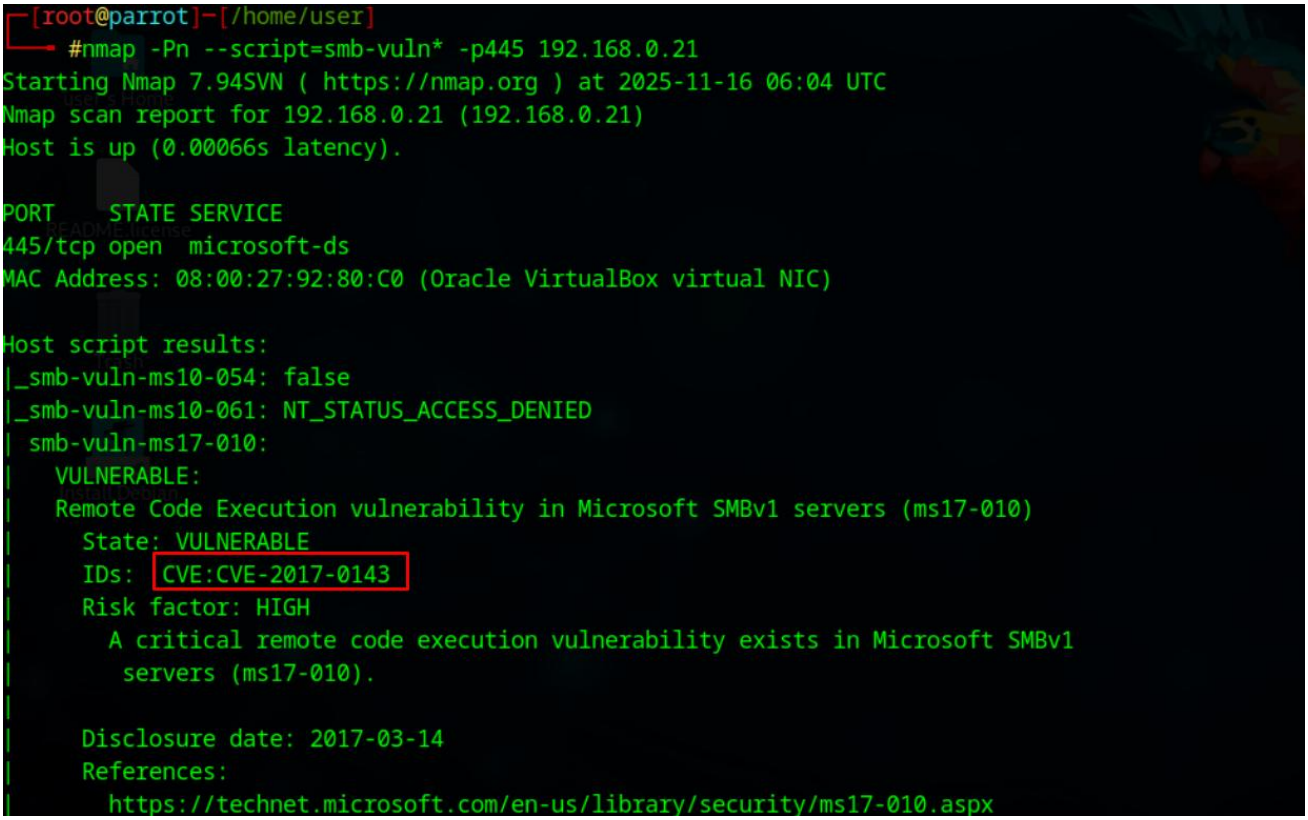


Fuente: Autoría propia

Después de realizar el escaneo se evidencia que los puertos 135, 139 y 445 se encuentran abiertos. Usualmente Windows presenta los puertos 135 y 139, por lo tanto, se realiza un escaneo de vulnerabilidades con nmap para el puerto 445.

Figura 9.

Nmap para vulnerabilidades SMB



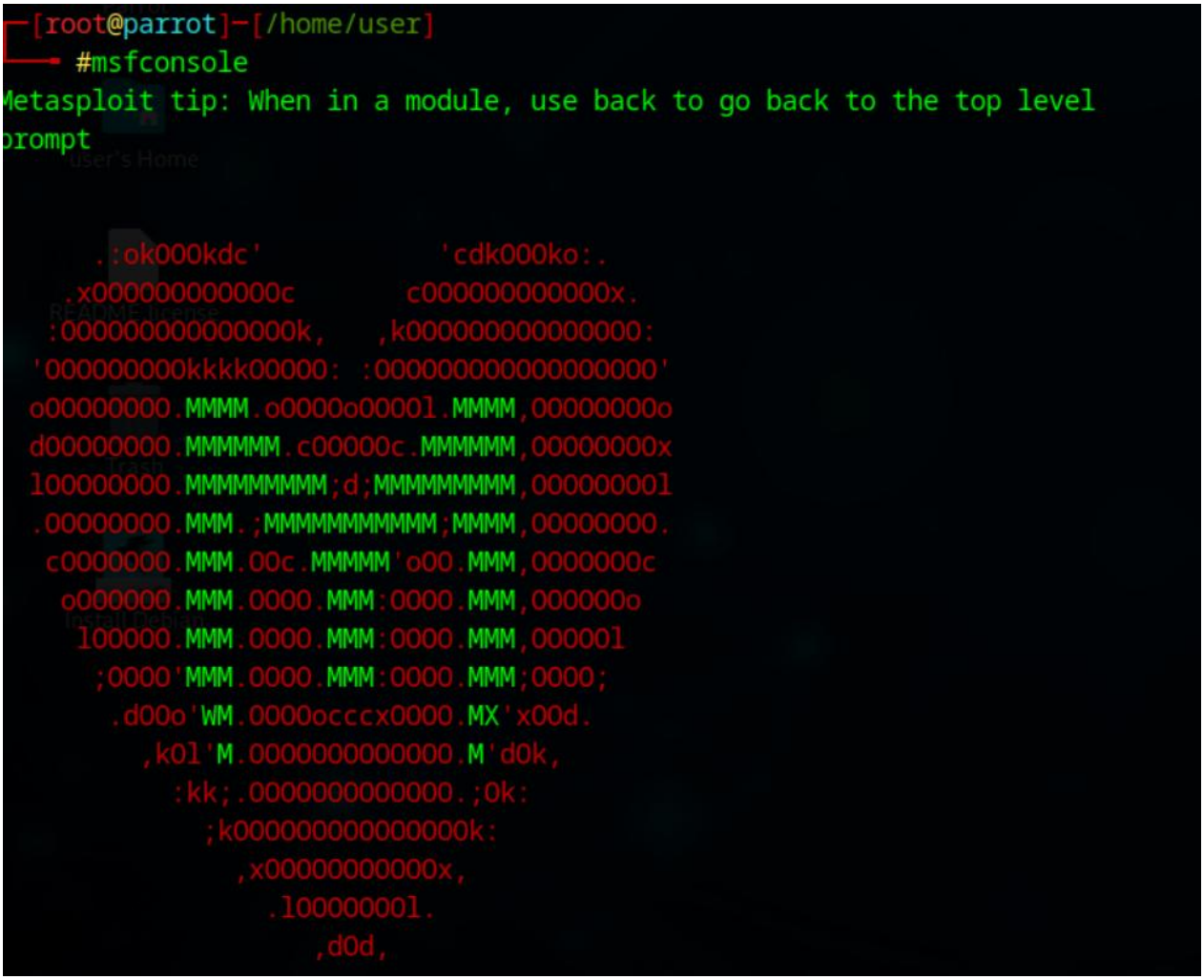
Fuente: Autoría propia

De acuerdo con el escaneo realizado se encuentra que la versión SMB encontrada presenta la vulnerabilidad con ID CVE-2017-0143 la cual hace referencia a ejecutar código sobre el protocolo SMB y tener acceso al sistema. (*NVD - Cve-2017-0143*, n.d.)

Con lo anterior se abre la consola de metasploit, framework utilizado para hacer pruebas de penetración de acuerdo a una base de datos de vulnerabilidades conocidas y sus respectivos payloads. (*What Is Metasploit | Tools & Components Explained | Imperva*, n.d.)

Figura 10.

Metasploit

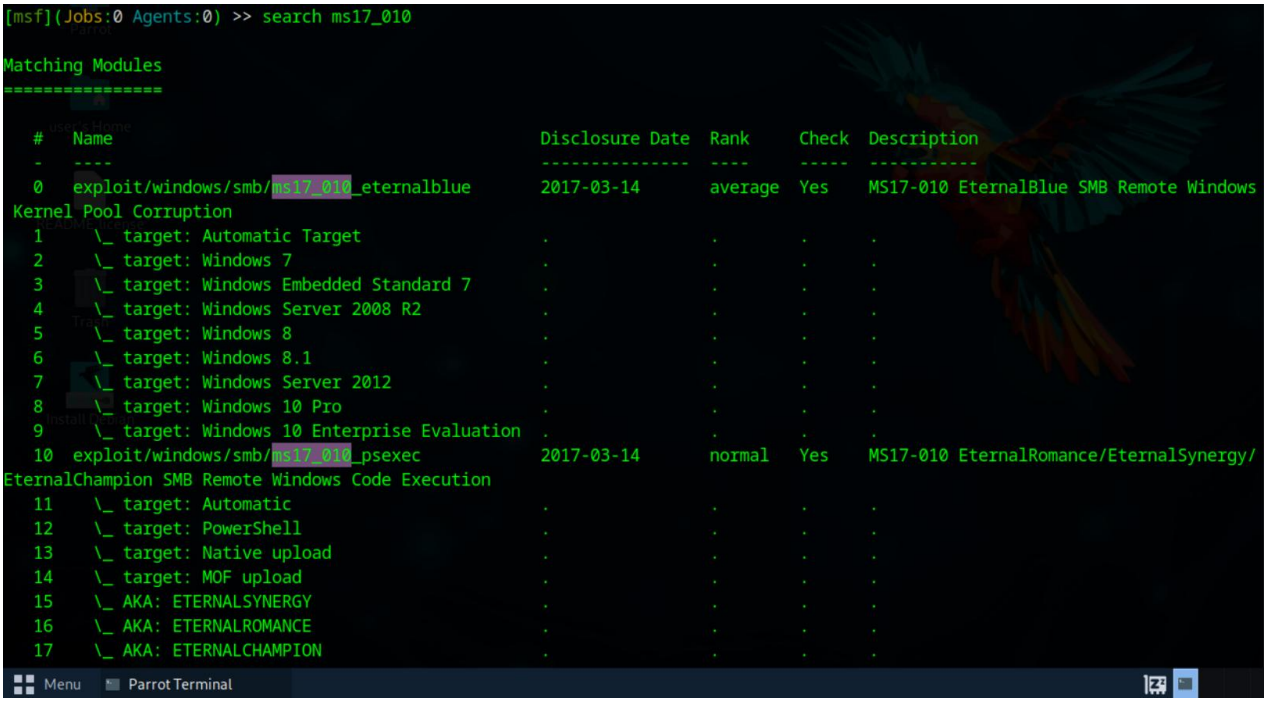


Fuente: Autoría propia

Luego de ingresar en la consola, se realiza la búsqueda de los ataques conocidos sobre SMB, y se encuentra en la base de datos el modulo de eternalblue, vulnerabilidad y exploit sobre Microsoft. (*El Exploit EternalBlue | MS17-010 Explicado*, n.d.)

Figura 11.

Eternalblue

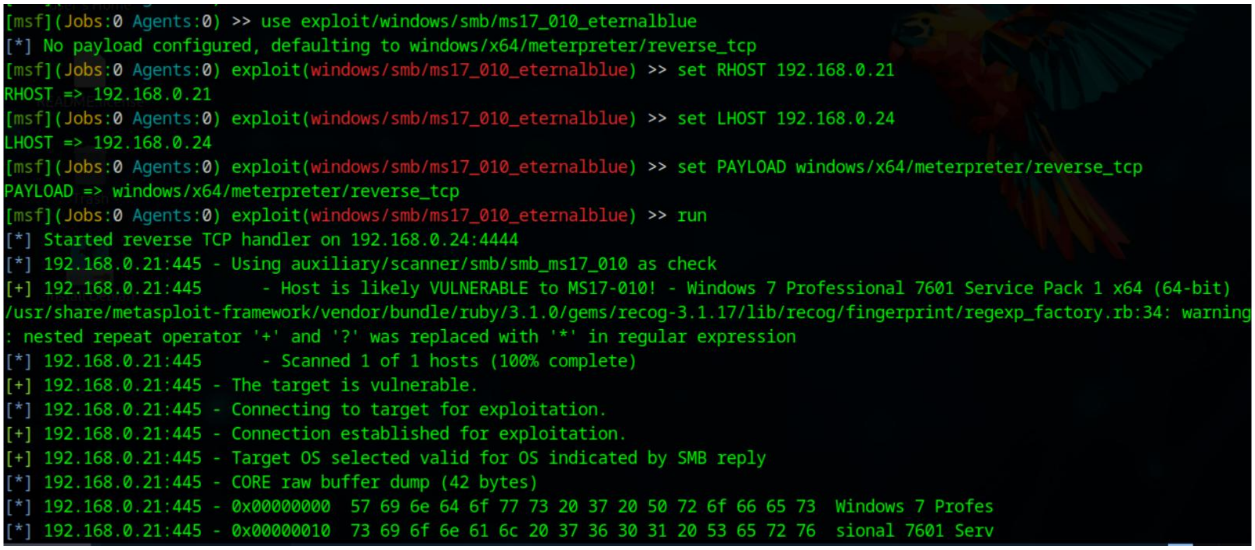


Fuente: Autoría propia

Para aplicar este modulo se configura el host destino, origen y payload a cargar.

Figura 12.

Configuración payload

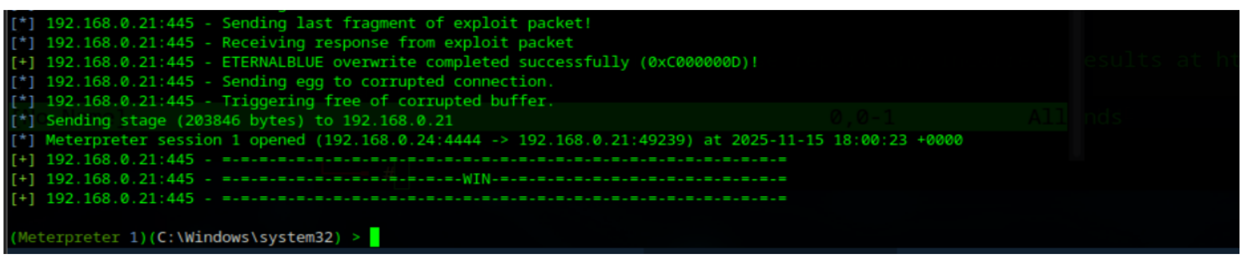


Fuente: Autoría propia

Con la acción realizada anteriormente se evidencia acceso a la maquina pivote (Host-A)

Figura 13.

Intrusión host-A

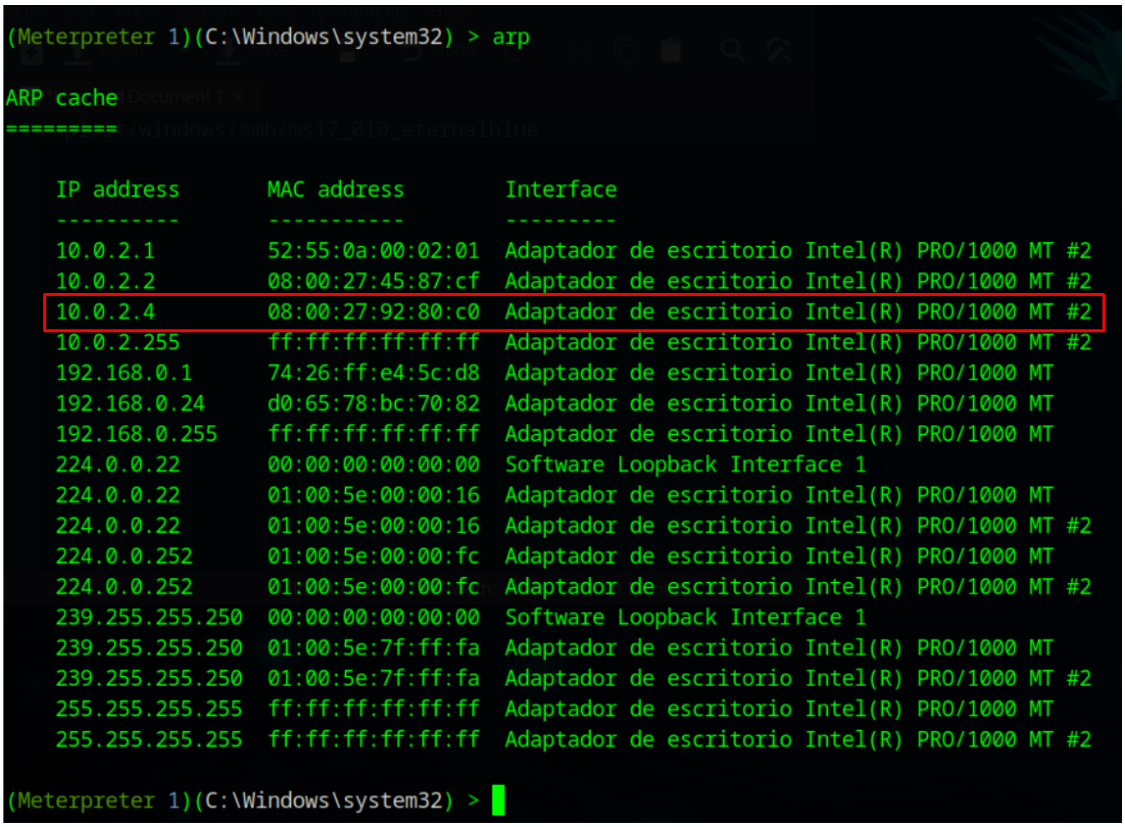


Fuente: Autoría propia

De acuerdo con los permisos anteriores, se realiza una búsqueda en la tabla arp de la máquina para verificar en que entorno se encuentra y los posibles movimientos laterales a realizar.

Figura 14.

ARP para movimiento lateral



Fuente: Autoría propia

Luego de esto se deja la sesión de meterpreter abierta pero gestionada desde metasploit, esto se realiza con el comando background.

Dentro de la consola de metasploit se ejecuta el módulo para aplicar rutas que dirijan el tráfico hacia el pivote.

Figura 15.

Agregar rutas a la sesión

```
[msf](Jobs:0 Agents:1) exploit(windows/smb/ms17_010_eternalblue) >> use post/multi/manage/autoroute
[msf](Jobs:0 Agents:1) post(multi/manage/autoroute) >> set session 1
session => 1
[msf](Jobs:0 Agents:1) post(multi/manage/autoroute) >> run
[*] Running module against PC202006 (192.168.0.21)
[*] Searching for subnets to autoroute.
[+] Route added to subnet 192.168.0.0/255.255.255.0 from host's routing table.
[*] Post module execution completed
[msf](Jobs:0 Agents:1) post(multi/manage/autoroute) >> route

IPv4 Active Routing Table
=========================

   Subnet             Netmask            Gateway
   ------             -------            -------
   10.0.2.0           255.255.255.0      Session 1
   192.168.0.0        255.255.255.0      Session 1

[*] There are currently no IPv6 routes defined.
[msf](Jobs:0 Agents:1) post(multi/manage/autoroute) >>
```

Fuente: Autoría propia

Luego de este proceso se realiza la configuración de los socks proxy, esto permite realizar el salto desde el Host-A (Comprometido) al servidor destino. (Host-B). Esto se realiza por medio del puerto 1081. Este proceso es más conocido como pivoting y hace referencia a navegar en redes aisladas sin estar realmente adentro.

Figura 16.

Configuración socks proxy

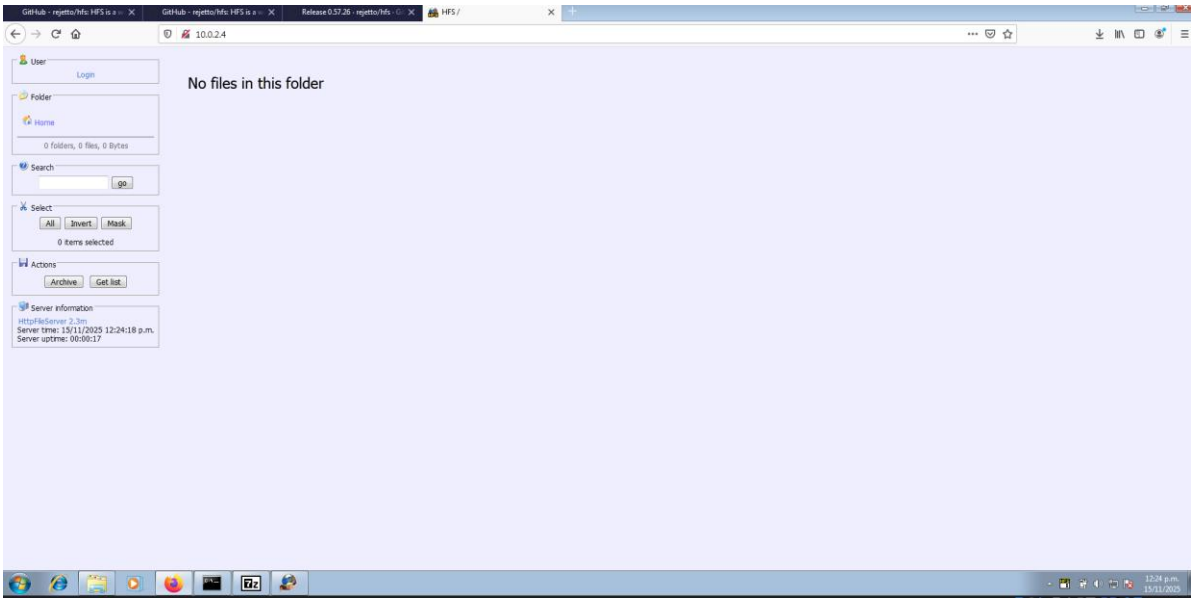
```
[msf](Jobs:1 Agents:1) auxiliary(server/socks_proxy) >> use auxiliary/server/socks_proxy
[msf](Jobs:1 Agents:1) auxiliary(server/socks_proxy) >> set SRVHOST 127.0.0.1
SRVHOST => 127.0.0.1
[msf](Jobs:1 Agents:1) auxiliary(server/socks_proxy) >> set SRVPORT 1081
SRVPORT => 1081
[msf](Jobs:1 Agents:1) auxiliary(server/socks_proxy) >> set VERSION 5
VERSION => 5
[msf](Jobs:1 Agents:1) auxiliary(server/socks_proxy) >> run
```

Nota: Autoría propia

Con el proceso anterior realizado, se abre otro terminal y se realiza un curl (Figura 18) hacia el servidor destino (Host-B), en este se monta una pagina web como sobre HFS (Sistema de archivos jerargico) figura 17.

Figura 17.

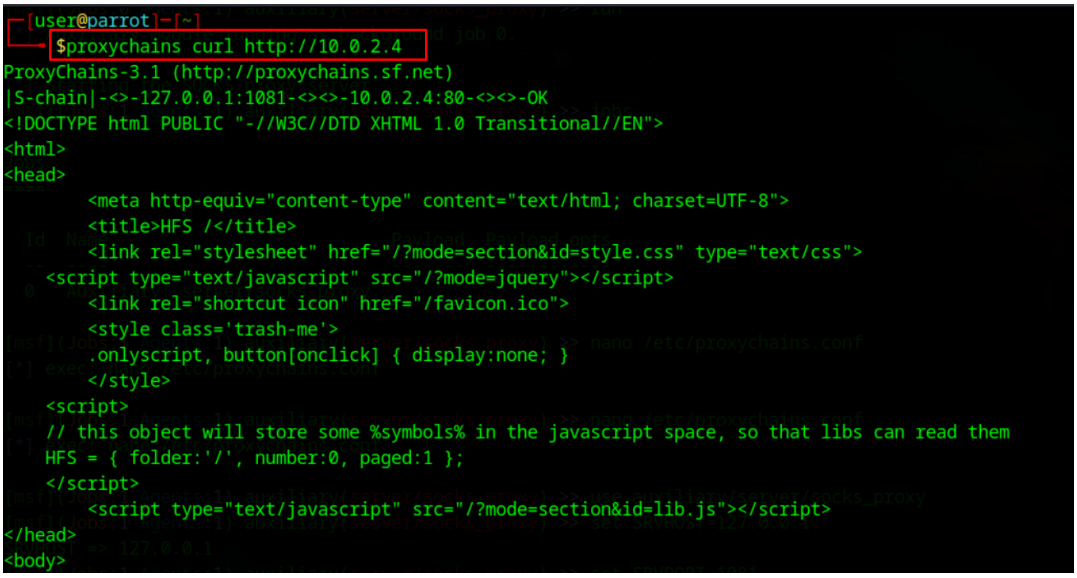
Evidencias de servidor HFS



Fuente: Autoría propia

Figura 18.

Curl http movimiento lateral



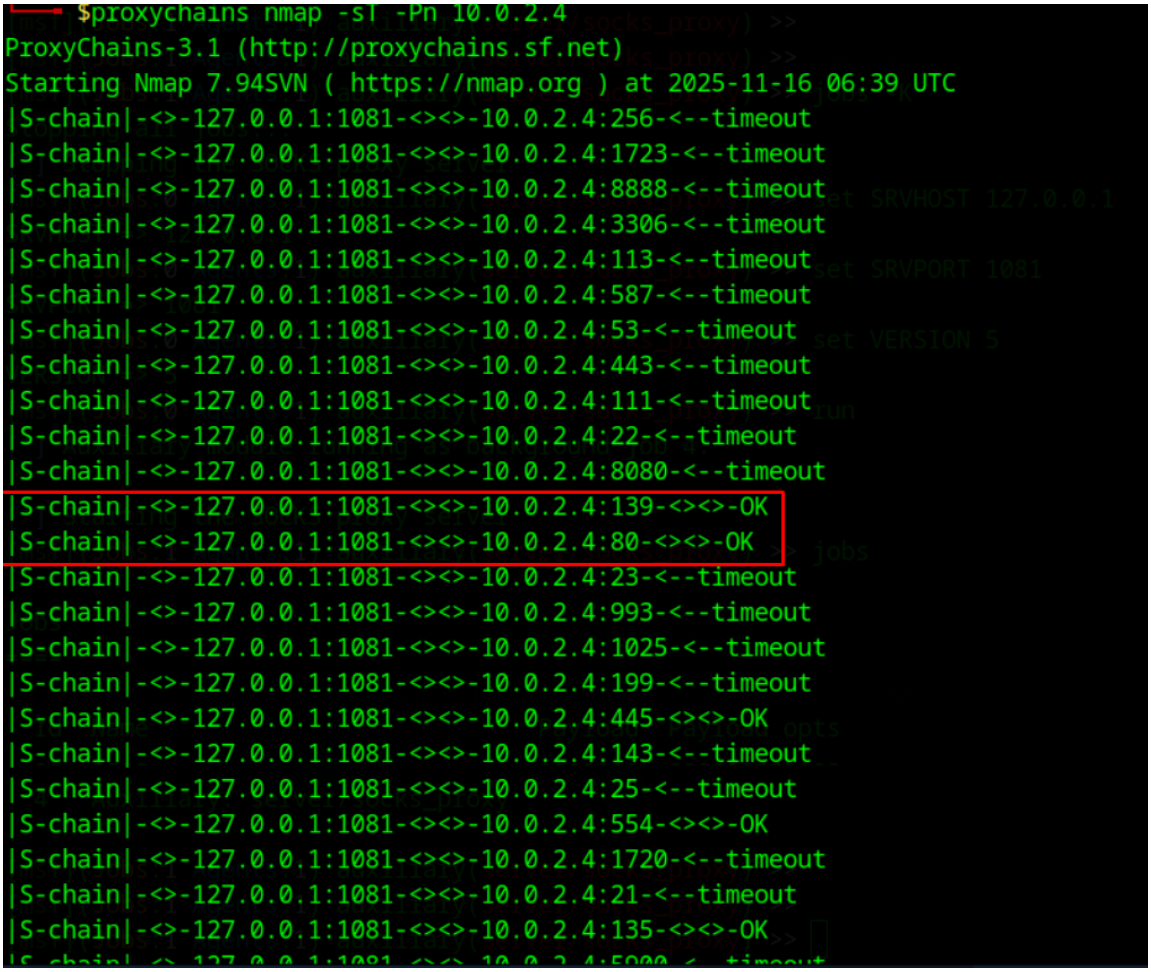
Fuente: Autoría propia

Como se evidencia en la figura 16 y como se realiza en la figura 17 se utiliza el comando proxychain, el cual hace referencia a una herramienta que permite enrutar el tráfico TCP hacia determinadas aplicaciones sobre un proxy (Configurado en figura 14). (*Cómo Usar Proxychains y Tor En Linux Para Ser Anónimo En Internet*, n.d.)

Con esta técnica se realiza un nmap desde el host-A hacia el host-B. En donde se encuentran los puertos 139,80,445 y 554 abiertos, razón por la cual el curl sobre http respondió correctamente en las pruebas anteriores (Figura 19).

Figura 19.

Nmap hacia Host-B

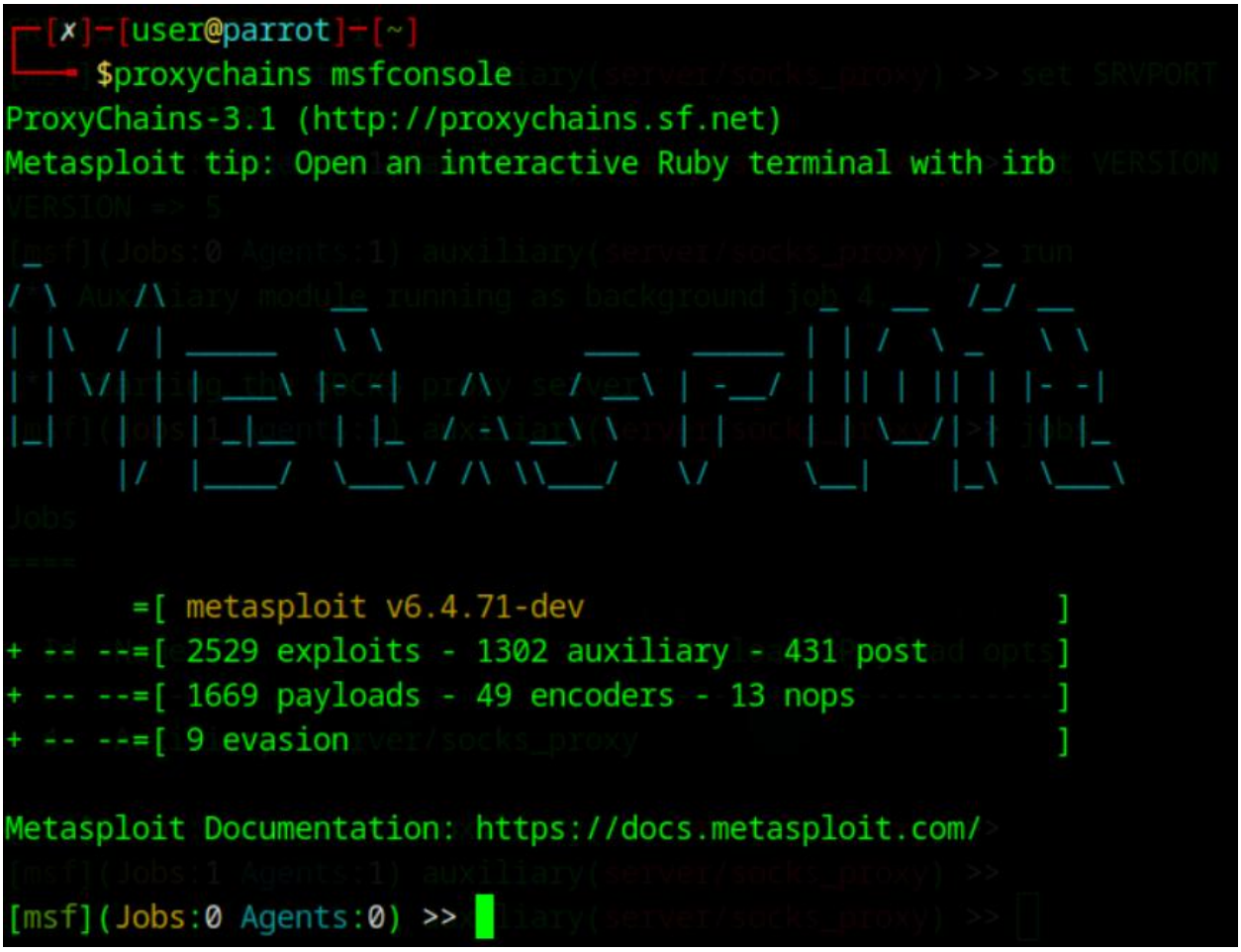


Fuente: Autoría propia

Con esta misma técnica se abre la consola de metasploit (Figura 18) para aprovechar la vulnerabilidad del protocolo SMB para tener acceso no autorizado a la maquina y asi crear el usuario solicitado por la guía. (Figura 19)

Figura 20.

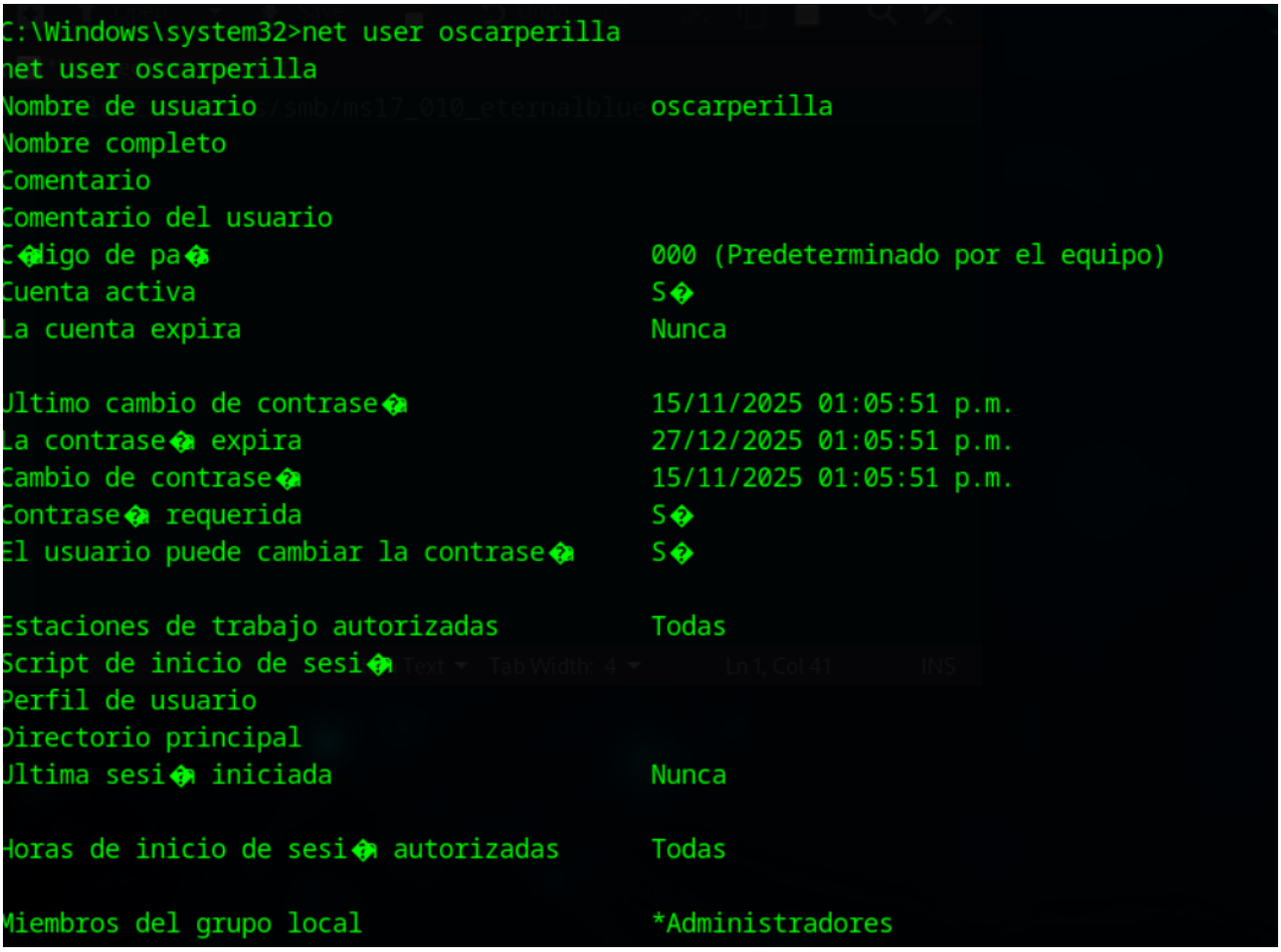
Sesión metasploit para Host-B



Fuente: Autoría propia

Figura 21.

Creación de usuarios



Fuente: Autoría propia

Con el proceso anterior se logra realizar un movimiento lateral en la red e intervenir en un servidor de archivos critico para la compañía. A continuación, se realiza una tabla en donde se presenta cada proceso realizado y la herramienta empleada (Fases de pentesting).

Tabla 2.

Fases del pentesting

Fase	Objetivo	Acciones realizadas
1. Reconocimiento	Identificar hosts, puertos y servicios expuestos.	Nmap hacia Host-A
		Pivoting desde host-A a Host-B realizando escaneo de puertos con nmap
2. Enumeración	Recolectar información detallada del cada host	Puertos 135, 139, 445, 554 abiertos en Host-A
		Puertos 135, 139, 445, 554 abiertos en Host-B
		Realizar fingerprinting manual con proxychains y curl
3. Análisis de vulnerabilidades	Determinar pisobles servicios vulnerables	Revisión de vulnerabilidades SMB en metasploit y nmap
4. Explotación	Ejecución de código o acceso no autorizado.	Aplicar sploit y payload para intrusión a los sistemas windows con eternalblue
		Aplicación de payload en Metasploit para montar el proxy y realizar movimientos laterales con SOCKS proxy.
5. Post-explotación	Mantener acceso y extraer información.	Enumerar sistema comprometido.
		Pivoting desde Host-A hacia Host-B
		Creación de usuario con permisos de administración
6. Reporte	Documentar hallazgos.	Evidencias de acceso.
		Vulnerabilidades detectadas.

Fuente: Autoría propia

Acciones iniciales en un ataque en tiempo real

Para esta ocasión se hace uso del marco normativo NIST 800-61 enfocado a un equipo de blue team el cual presenta las fases de Preparación, detección, análisis, contención, erradicación y recuperación de acuerdo con (*Reconocimiento, Táctica TA0043 - Enterprise | MITRE ATT&CK®*, n.d.)

1. Detección y análisis: En esta fase o primer paso, se debe confirmar de forma técnica que exista un ataque, esto quiere decir que se debe buscar su naturaleza y ver que equipos de la infraestructura están infectados.
   Este paso se realiza verificando que conexiones están activas en el momento del ataque (Revisando en orden ascendente en el modelo osi). Para el caso del ataque simulado se realizo con el comando *netstat -a | find "445"* y *tasklist /v.*
   Luego de lo anterior empezar a revisar los logs de inicio de sesión y sesiones activas sobre el equipo, esto permite revisar alguna intrusión en tiempo real.
   La siguiente tarea de esta fase luego de tener la evidencia clara de la existencia de un ataque es tomar la captura de evidencia voltail (Memoria ram y uso de drivers). De acuerdo a la solicitud del anexo 5 de la guía entregada por el docente se recomienda la herramienta WinPmem. (*WinPmem Memory Imager*, n.d.)
2. Contención: Esta fase se basa en gran cantidad en la anterior debido a tiene como objetivo detectar el avance del ataque sin destruir la evidencia ya que esta servirá para un análisis posterior (fase 3). Para lo anterior se realizan las siguientes acciones.
   a. Aislamiento de equipos comprometidos: Realizar el aislamiento de los hosts comprometidos a nivel de switch en la red, esto permite detener el ataque sin modificar las evidencias obtenidas sobre el equipo.

   b. Bloquear vectores de ataque: Como en el escenario simulado no se contaba con un firewall perimetral, el bloqueo se debe realizar por medio del firewall local del equipo o deshabilitando los servicios comprometidos, en este caso SMB (Sin embargo la cadena de custodia quedaría afectada en este ultimo paso).
   c. Mantener equipo encendido
3. Análisis profundo: Esta fase se realiza luego de que se confirma que el ataque no continuo, y corresponde a analizar la memoria con herramientas como Volatility la cual nos permite ver procesos maliciosos, inyecciones de código sobre la máquina, escalamiento de privilegios y conexiones del atacante, esto nos permite tener un panorama 360 del ataque y ver el alcance del mismo. (*Home of The Volatility Foundation | Volatility Memory Forensics - The Volatility Foundation - Promoting Accessible Memory Analysis Tools Within the Memory Forensics Community*, n.d.)
4. Fase de erradicación: Esta fase es corta, consiste en eliminar todos los accesos, artefactos instalados por el cliente, aplicar parches sobre la vulnerabilidad explotada y aplicando permisos de accesos sobre el equipo.
5. Fase de recuperación: En esta fase se verifica el estado e integridad del sistema y se realiza la incorporación del host a la red de forma controlada y se coloca en monitoreo el equipo revisando posibles tareas e intensos nuevos de intrusión.
6. Lecciones aprendidas: Esta fase consiste en documentar los hallazgos encontrados, bloquear los indicadores de compromiso y fortalecer las reglas sobre los equipos o herramientas de seguridad.

Hardening sobre la infraestructura

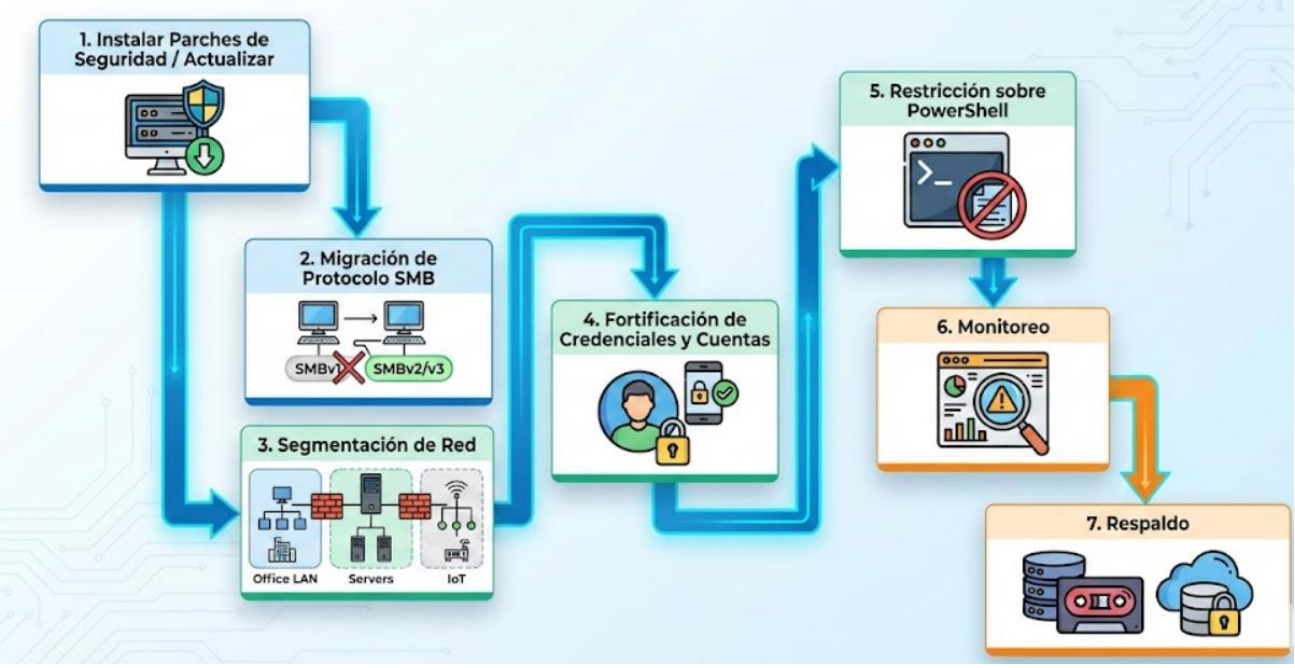
Teniendo en cuenta que el ataque se basó en la explotación de la vulnerabilidad de eternalblue (MS17-010) y luego un movimiento lateral con escalamiento de privilegios, la hardenización debe realizarse en diferentes niveles de la infraestructura. A continuación, se explica a detalle cada paso a realizar.

1. Instalar parche de seguridad sobre el equipo o actualizar: En este proceso se debe aplicar el parche de seguridad para mitigar eternalblue y aprovechar el evento sucedido para implementar una política de patch management continuo lo que permite acutalizar el sistema de forma automática o programada, según como el administrador vea la necesidad. Otra acción que se debe tomar sin embargo requiere de validaciones extensas y planificación sobre la migración es subir las maquinas a un sistema operativo que cuente con soporte.
2. Migración de protocolo SMB: En este paso se debe deshabilitar el protocolo SMB en su versión 1 y migrar los servicios sobre una versión segura y que incorpore cifrado (SMB2/SMB3).
3. Segmentación de red: En este paso se recomienda aplicar microsegmentación de red, impidiendo que un host comprometido afecte la red con movimientos laterales. Adicionalmente configurando el firewall de Windows de forma correcta permitiendo conexiones al puerto 445 únicamente desde segmentos autorizados.
4. Fortificacion de credenciales y cuentas: Quitar cuentas administrativas de nombre genérico, es decir, cuentas con el usuario admin, administrador, entre otros. Adicionalmente implementar políticas de contraseñas evitando la sobreutilización y rotación obligatoria.

5. Restriccion sobre powershell: Este paso consiste en habilitar el Constrined language mode en la powershell y bloquear la ejecución no autorizada.
6. Monitoereo: Este paso consiste en aplicar herramientas de monitoreo activo y pasivo, es decir, monitorear recursos con plataformas que soporten SNMP y hacer uso de SIEM o SOAR para tener un monitoreo activo con detección de amenazas, intrusión y creación de usuarios en los equipos.
7. Respaldo: Tener respaldo de los servidores de la infraestructura y aplicar prácticas como los templates línea base en seguridad de Microsoft o el benchmarks CIS.

Figura 22

Hardenización en infraestructura.



Fuente: Autoría propia

Diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos

Estos dos equipos son de vital importancia en un grupo SOC o CSOC por tal motivo, se crea la siguiente tabla comparativa.

Tabla 3

Comparación blueteam y IR team

Criterio	Blue Team	Equipo de Respuesta a Incidentes (IR Team)
Enfoque	Proactivo y preventivo	Reactivo se actúa cuando el incidente ya está ocurriendo.
Objetivo general	Mantener la infraestructura segura y reducir la superficie de ataque.	Contener, erradicar y recuperar los sistemas comprometidos.
Actividades principales	Monitoreo continuo, hardening, gestión de vulnerabilidades, auditorías, configuración segura.	Detección, análisis forense, contención, erradicación de malware, recuperación y lecciones aprendidas.
Tiempo de intervención	Operación continua 24/7; seguridad diaria.	Intervención esporádica solo ante incidentes confirmados o sospechosos.
Competencias requeridas	Administración de seguridad, redes, SIEM, firewalls, EDR, políticas de seguridad.	Forense digital, análisis de malware, contención avanzada, investigación técnica.
Herramientas típicas	SIEM, IDS/IPS, firewalls, WAF, EDR/XDR, sistemas de monitoreo.	Volatility, Autopsy, FTK Imager, Wireshark, Sysinternals, TheHive/MISP.
Orientación del trabajo	Operacional, mantenimiento y mejora continua.	Manejo de crisis, respuesta inmediata y recuperación del incidente.
Entregables	Reportes de vulnerabilidades, políticas, configuraciones endurecidas, monitoreo.	Informe forense, línea de tiempo del ataque, evidencias, acciones de mitigación.

Nota. Comparación red and blue team (*Red vs Blue Team: Simulaciones de Ciberataques Para Mayor Seguridad*, n.d.)

Center For Internet Security

Es una organización internacional sin ánimo de lucro dedicada a mejorar la ciberseguridad a nivel global mediante la creación de estándares, guías y controles de seguridad ampliamente aceptados. Su principal objetivo es crear prácticas que permitan a las organizaciones proteger sus sistemas, reducir vulnerabilidades y fortalecer su postura defensiva frente a ataques informáticos.

Con lo anterior, al estar en un equipo de blue team se utilizarían los benchmark del CIS para realizar hardenización de sistemas (servidores o firewalls), ajustar configuraciones inseguras.

Esto se realiza aplicando los 18 controles que ayudan a proteger la infraestructura, con esto, algunos controles gestionan el inventario de activos, vulnerabilidades, accesos y monitoreo continuo. (*CIS Critical Security Controls*, n.d.)

SIEM

En los equipos de blue team, tener un monitoreo y predicción mas detallada, ahorra bastante tiempo y esfuerzo por las amenazas sofisticadas que existen que existen hoy en día. Por esta razón, en la tabla 2 se explica que es un SIEM, cómo funciona y cuáles son sus características principales. (*¿Qué Es SIEM? | Seguridad de Microsoft*, n.d.)

Tabla 4

Explicación SIEM

Aspecto	Descripción
Concepto de SIEM	Es una plataforma centralizada que recopila, correlaciona, analiza y visualiza eventos de seguridad provenientes de múltiples sistemas, permitiendo la detección, monitoreo y respuesta ante incidentes en tiempo real.
Recolección y centralización de logs	Agrupa y almacena eventos de firewalls, sistemas operativos, servidores, EDR, bases de datos y aplicaciones para mantener trazabilidad completa.
Correlación de eventos	Utiliza reglas y algoritmos para detectar patrones anómalos combinando información de distintas fuentes, permitiendo identificar ataques complejos.
Detección en tiempo real	Genera alertas automáticas cuando detecta actividades sospechosas, como explotación de vulnerabilidades, movimientos laterales o creación no autorizada de usuarios.

Análisis forense	Facilita la reconstrucción de la línea de tiempo de un ataque mediante consultas avanzadas y análisis de logs históricos.
Gestión de alertas y automatización (SOAR)	Clasifica eventos según su criticidad y permite acciones automáticas de respuesta, como bloquear direcciones IP, aislar hosts o deshabilitar cuentas comprometidas.
Cumplimiento normativo	Ayuda a cumplir regulaciones como ISO 27001, PCI-DSS, GDPR o NIST gracias a la trazabilidad y almacenamiento seguro de logs.
Visualización y dashboards	Ofrece paneles gráficos para monitorear amenazas, tendencias y el estado general de la seguridad organizacional.

Herramientas de contención

Las herramientas de contención hacen referencia a equipos como firewalls, waf, edr, entre otros. Por tal motivo, a continuación, se listan las siguientes herramientas.

1. PfSense: Este es un firewall open source basado en FreeBSD que permite bloquear tráfico malicioso, cortar conexiones activas del atacante y aplicar reglas estrictas para contener un ataque. (*PfSense® - World's Most Trusted Open Source Firewall*, n.d.)
2. Crowdsec: Sistema colaborativo que analiza comportamientos sospechosos y permite bloquear actores maliciosos mediante "bouncers" en firewalls, servidores web y sistemas. (*CrowdSec WAF: The Collaborative Future of Web App Security*, n.d.)
3. OpenWAF: Herramienta diseñado para proteger aplicaciones web contra ataques comunes como inyecciones SQL, cross-site scripting (XSS), file inclusion, ejecución remota de código (RCE) y explotación de vulnerabilidades conocidas. Está basado en el motor de inspección profunda ModSecurity, pero ofrece una arquitectura más moderna, flexible y extensible.(*GitHub - Titansec/OpenWAF: Web Security Protection System Based on Openresty*, n.d.)

Con lo anterior se crea la siguiente tabla comparativa

Tabla 5.

Comparación herramientas de contención

Comparación herramientas

Herramienta	**Tipo de solución**	**Funciones principales**	**Ventajas**	**Limitaciones**
PfSense	Firewall perimetral y de red (Open Source)	- Filtrado y bloqueo de tráfico malicioso- Cortar conexiones activas del atacante- Reglas avanzadas de firewall- IDS/IPS opcional con Snort o Suricata- VPN, NAT y segmentación	- Totalmente open source- Altamente configurable- Comunidad amplia- Ideal para contención de tráfico a nivel de red	- Requiere conocimientos técnicos- No incluye protección específica para aplicaciones web

CrowdSec	Sistema colaborativo de detección y respuesta (Open Source)	- Analiza comportamiento sospechoso- Bloqueo automático mediante *bouncers*- Inteligencia colectiva en tiempo real- Integración con firewalls, servidores web y bases de datos	- Respuesta automatizada y compartida- Ligero y fácil de integrar- Reduce falsos positivos gracias al modelo colaborativo	- Depende de agentes y bouncers externos- Requiere red para compartir indicadores
OpenWAF	Web Application Firewall (Open Source)	- Protección contra ataques web: SQLi, XSS, RCE, LFI/RFI- Basado en ModSecurity + OpenResty- Reglas de inspección profunda- Mitigación de exploits conocidos	- Muy eficaz para proteger aplicaciones web- Arquitectura moderna y flexible- Fácil de extender con nuevas reglas	- No protege nivel de red- Requiere ajuste de reglas y pruebas para evitar bloqueos falsos

Análisis legal del proceso

El ejercicio desarrollado incluye actividades de explotación, intrusión, análisis y respuesta ante incidentes, sin embargo, estas actividades son reguladas por algunos lineamientos legales, los cuales garantizan la protección de datos. A continuación, se presentan las leyes que regulan y tratan el desarrollo del proceso.

1. Protección de datos personales y confidencialidad (Ley 1581 de 2012): Toda operación que involucre sistemas informáticos está sujeta a la normativa sobre protección de datos personales. Los equipos de Red Team y el Blue Team, deben garantizar:

- Confidencialidad de la información tratada durante el análisis.
- No divulgación de datos sensibles o privados obtenidos durante la intrusión controlada.
- Custodia adecuada de la evidencia digital recolectada.

Las prácticas realizadas en este laboratorio deben replicarse con protocolos formales en entornos reales para garantizar el cumplimiento de esta ley.

2. Responsabilidad penal en el manejo de sistemas informáticos (Ley 1273 de 2009 – Delitos Informáticos)

Esta ley protege la información y los datos como bien jurídico, incorporando delitos como:

- Acceso no autorizado a sistemas
- Obstaculización o interrupción ilegítima de sistemas
- Abuso de dispositivo
- Violación de datos personales

Las actividades de explotación, movimiento lateral, extracción de datos o uso de herramientas como Metasploit solo pueden ser realizadas:

- Con autorización documentada
- Dentro de un alcance definido
- Con acuerdos de confidencialidad
- Con la cadena de custodia formalizada

3. Gestión de incidentes y marco legal aplicable (Ley 1266 de 2008 y Decreto 1377 de 2013): La respuesta a incidentes, como la desarrollada por el Blue Team, está estrechamente relacionada con el tratamiento adecuado de datos y la transparencia organizacional. La organización debe:
    - Notificar incidentes relevantes a los titulares de datos cuando exista riesgo de afectación.
    - Implementar controles que garanticen integridad, disponibilidad y confidencialidad.
    - Registrar y documentar incidentes en cumplimiento de las normas de Habeas Data.

4. Obligaciones de seguridad para organizaciones (Ley 1581 de 2012 y Circular SIC 02 de 2023)

La Superintendencia de Industria y Comercio menciona que las organizaciones deben implementar medidas técnicas, administrativas y humanas para proteger los datos personales. El uso de herramientas como EDR, SIEM, firewalls y segmentación, descritas en este proyecto, son parte de las medidas exigidas por la normativa. Esto significa que la falta de controles como parches actualizados, hardening o monitoreo podría interpretarse como negligencia o incumplimiento legal.

5. Cadena de custodia y preservación de evidencia digital (Manual de Cadena de Custodia – Fiscalía General de la Nación)

El análisis forense realizado en las etapas del proyecto implica la manipulación de evidencia digital. Legalmente, la correcta cadena de custodia requiere:

- Identificación del equipo comprometido
- Adquisición forense confiable (herramientas certificadas)
- Documentación del procedimiento
- Integridad garantizada mediante hash
- Almacenamiento seguro de imágenes y registros

6. Buenas prácticas alineadas a estándares internacionales

Además del marco legal colombiano, el proceso realizado se ajusta a estándares como:

- NIST 800-61 (respuesta a incidentes)
- ISO 27001 / 27037 / 27041 (gestión de seguridad y evidencia digital)
- CIS Controls (endurecimiento y protección)

7. Responsabilidad organizacional y contractual

En una operación real de Red Team o respuesta a incidentes:

- Debe existir un contrato o autorización formal (Rules of Engagement).
- Las pruebas deben realizarse sin afectar la operación ni los datos.
- La organización es responsable por garantizar que las acciones del personal no infrinjan normas penales o administrativas.

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/v9dgb1IRBfs

Conclusiones

Este ejercicio permitió ver, de manera muy cercana y práctica, cómo una vulnerabilidad olvidada puede convertirse en la puerta principal para un atacante. Explorar EternalBlue y lograr acceso al Host-A mostró que incluso un detalle técnico aparentemente menor puede desencadenar un compromiso serio si no se aplican actualizaciones a tiempo.

El movimiento lateral y el pivoting demostraron que cuando una red no está segmentada ni bien protegida, un atacante puede moverse con facilidad entre equipos internos. Esta experiencia ayudó a comprender que la seguridad no depende solo de un firewall o un antivirus, sino de una estructura completa de controles bien diseñada.

Desde el rol del Blue Team, quedó claro que una buena respuesta a incidentes requiere orden, método y análisis cuidadoso. Herramientas como Volatility, los registros del sistema y el uso del marco NIST 800-61 fueron clave para entender qué ocurrió, cómo ocurrió y cómo detenerlo sin afectar la evidencia.

Las herramientas de contención estudiadas, demostraron que no existe una única solución que proteja todo. La defensa efectiva es el resultado de varias capas que trabajan juntas: detección, bloqueo, monitoreo y protección a nivel de red y aplicación.

Finalmente, este proyecto permitió unir lo ofensivo y lo defensivo, entendiendo que ambas miradas se necesitan mutuamente para fortalecer la seguridad. Más allá de lo técnico, dejó una enseñanza valiosa: la ciberseguridad es un equilibrio entre anticiparse a las amenazas y reaccionar correctamente cuando algo falla, siempre dentro de un marco legal y ético.

Referencias Bibliográficas

Avast. (2020). El exploit EternalBlue (MS17-010) explicado.

https://www.avast.com/es-es/c-eternalblue

Center for Internet Security. (n.d.). CIS Critical Security Controls.

https://www.cisecurity.org/controls

Cloudflare. (n.d.). ¿Qué es el movimiento lateral en ciberseguridad?

https://www.cloudflare.com/es-es/learning/security/glossary/what-is-lateral-movement/

CrowdSec. (2025). CrowdSec WAF: The collaborative future of web application security.

https://www.crowdsec.net/blog/crowdsec-waf-the-collaborative-future-of-web-application-security

Cyberbit. (2025). Your 101 guide to the MITRE ATT&CK Enterprise Matrix.

https://www.cyberbit.com/cybersecurity-training/mitre-attck-framework-enterprise-matrix/

Deep Hacking. (2021). ¿Qué es el pivoting?

https://deephacking.tech/que-es-el-pivoting/

IBM. (2025). Protocolo SMB.

https://www.ibm.com/docs/es/aix/7.3.0?topic=management-smb-protocol

IBM. (2025). ¿Qué es el Red Teaming?

https://www.ibm.com/es-es/think/topics/red-teaming

Imperva. (n.d.). What is Metasploit? Tools and components explained.

https://www.imperva.com/learn/application-security/metasploit/

KeepCoding. (n.d.). Apt-get update en Linux para actualizar repositorios.

https://keepcoding.io/blog/apt-get-update-en-linux/

Linux Hispano. (2013). Diferencia entre apt-get update y apt-get upgrade.

https://www.linuxhispano.net/2013/05/03/diferencia-entre-apt-get-update-y-apt-get-upgrade/

Microsoft. (n.d.). ¿Qué es SIEM?

https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

MITRE ATT&CK. (2020). Reconnaissance (TA0043).

https://attack.mitre.org/tactics/TA0043/

MITRE ATT&CK. (n.d.). Enterprise tactics.

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

National Institute of Standards and Technology. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61r3).

https://doi.org/10.6028/NIST.SP.800-61R3

National Vulnerability Database. (2017). CVE-2017-0143.

https://nvd.nist.gov/vuln/detail/CVE-2017-0143

Palo Alto Networks. (n.d.). What is SOAR?

https://www.paloaltonetworks.lat/cyberpedia/what-is-soar

pfSense. (n.d.). World's most trusted open source firewall.

https://www.pfsense.org/

RedesZone. (n.d.). Cómo usar Proxychains y Tor en Linux para ser anónimo en Internet.

https://www.redeszone.net/tutoriales/seguridad/proxychains-tor-linux-ocultar-identidad-internet/

S2GRUPO. (2024). Blue team en ciberseguridad: definición, funciones y herramientas.

https://s2grupo.es/blue-team-en-ciberseguridad-definicion-funciones-y-herramientas/

SOAX. (n.d.). What is a SOCKS proxy? Definition and key features.

https://soax.com/glossary/socks-proxy

Trend Micro. (2025). What is endpoint detection and response (EDR)?

https://www.trendmicro.com/es_mx/what-is/xdr/edr.html

Velocidex. (n.d.). WinPmem memory imager.

https://winpmem.velocidex.com/

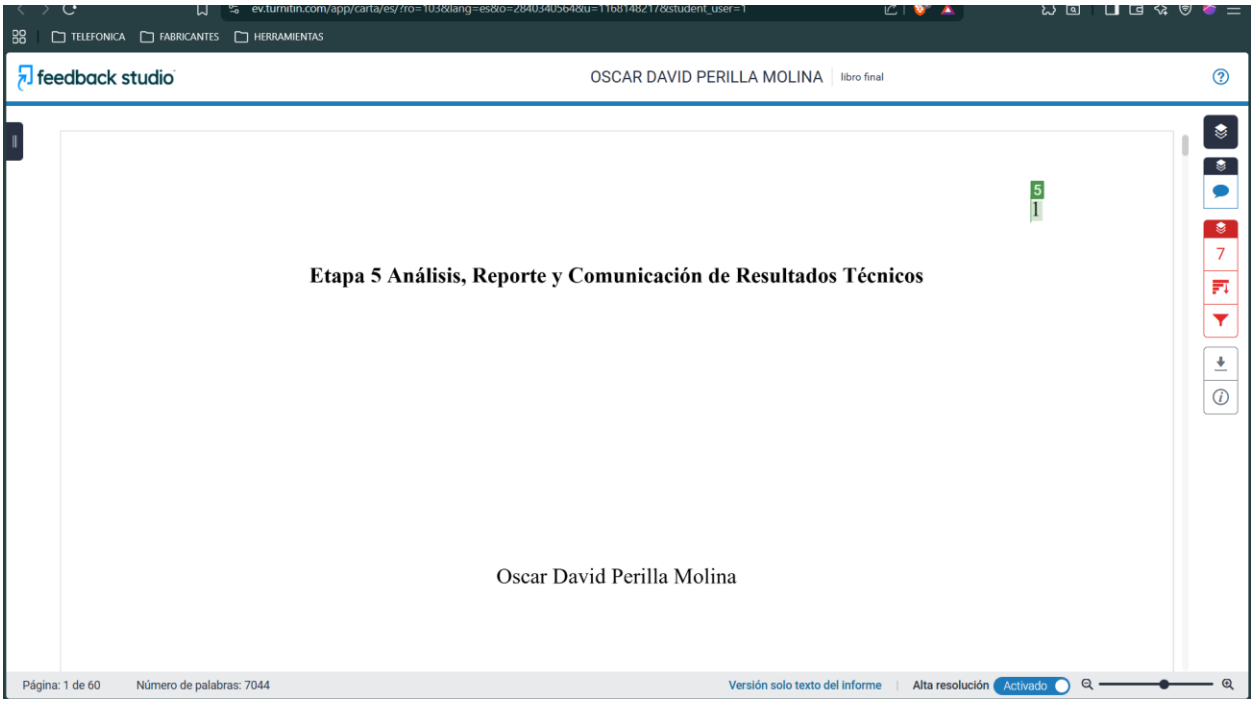
Volatility Foundation. (n.d.). Volatility memory forensics.

https://volatilityfoundation.org/

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Se hace una descripción del contenido de la tabla en cuestión de lo que se esté exponiendo dentro de esta, para referenciar la tabla se puede tomar el ejemplo de la figura en este documento.