Capacidades técnicas, tácticas y de respuesta para equipos Red Team y Blue Team

José Mauricio Ovalle Vargas

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en seguridad informática

2025

Resumen

El proyecto desarrolló un ejercicio integral de ciberseguridad ofensiva y defensiva basado en cuatro etapas que permitieron analizar de manera articulada los aspectos legales, técnicos y éticos de los enfoques Red Team y Blue Team. En primer lugar, se estudió el marco legal colombiano en materia de delitos informáticos y protección de datos, junto con las fases del hacking ético y el uso de herramientas de análisis de vulnerabilidades en un entorno de laboratorio virtual. Posteriormente, se realizó un análisis ético y jurídico del acuerdo de confidencialidad de SecureNova Labs, identificando cláusulas contrarias a la normativa vigente y al Código de Ética del COPNIA. En la fase ofensiva se explotó una vulnerabilidad en Rejetto HFS y se ejecutó movimiento lateral entre sistemas mediante EternalBlue dentro de una infraestructura controlada. Finalmente, desde la perspectiva del Blue Team, se abordó la respuesta al incidente mediante el análisis en tiempo real, la aplicación de medidas de hardening y la evaluación de herramientas de monitoreo y contención, con el fin de fortalecer la seguridad y la mejora continua de infraestructuras de tecnologías de la información.

***Palabras clave*:** Blue Team, Ciberseguridad, Eternalblue, Pentesting, Red Team

Abstract

The project developed a comprehensive offensive and defensive cybersecurity exercise based on four stages that allowed an articulated analysis of the legal, technical and ethical aspects of the Red Team and Blue Team approaches. First, the Colombian legal framework on computer crimes and data protection was studied, together with the phases of ethical hacking and the use of vulnerability analysis tools in a virtual laboratory environment. Subsequently, an ethical and legal analysis of SecureNova Labs' confidentiality agreement was carried out, identifying clauses contrary to the current regulations and the COPNIA Code of Ethics. In the offensive phase, a vulnerability in Rejetto HFS was exploited and lateral movement between systems was executed using EternalBlue within a controlled infrastructure. Finally, from the perspective of the Blue Team, the incident response was addressed through real-time analysis, hardening measures and evaluation of monitoring and containment tools, in order to strengthen the security and continuous improvement of information technology infrastructures.

***Keywords*:** Blue Team, cybersecurity, eternalBlue, pentesting, Red Team

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Glosario

Active Response:

Acción automática ejecutada por soluciones de seguridad como Wazuh ante la detección de eventos críticos, con el fin de contener o mitigar una amenaza de manera inmediata.

ARP Scan:

Técnica de escaneo de red que permite identificar dispositivos activos dentro de una subred mediante el uso del protocolo ARP.

Blue Team:

Equipo responsable de la defensa, monitoreo, endurecimiento (hardening) y contención de incidentes de seguridad en una infraestructura tecnológica.

CIS Benchmarks:

Conjunto de estándares y guías de configuración segura desarrollados por el Center for Internet Security para fortalecer sistemas, aplicaciones y dispositivos de red.

EternalBlue:

Exploit que aprovecha la vulnerabilidad MS17-010 del protocolo SMBv1 para lograr ejecución remota de código en sistemas Windows vulnerables.

Hardening:

Conjunto de medidas técnicas orientadas a reducir la superficie de ataque de un sistema mediante la eliminación o restricción de servicios, configuraciones y accesos innecesarios.

Hashdump:

Técnica utilizada para extraer los hashes de contraseñas almacenados en un sistema comprometido con el fin de analizarlos o reutilizarlos en ataques posteriores.

Kiwi:

Extensión de Meterpreter basada en Mimikatz que permite la extracción de credenciales en texto plano y hashes directamente desde la memoria del sistema.

Metasploit:

Framework de código abierto utilizado en pruebas de penetración que integra módulos de explotación, escaneo y postexplotación para evaluar la seguridad de sistemas.

Pivoting:

Técnica de movimiento lateral que permite utilizar una máquina previamente comprometida como punto de acceso para alcanzar otros sistemas dentro de una red privada.

Proof of Concept:

Demostración práctica que valida la posibilidad de explotación de una vulnerabilidad o la efectividad de una técnica específica en un entorno controlado.

Red Team:

Equipo ofensivo encargado de simular ataques reales con el objetivo de identificar vulnerabilidades y brechas de seguridad en una organización.

Rejetto HFS:

Servidor web ligero que presenta vulnerabilidades conocidas de ejecución remota de código, comúnmente utilizado en laboratorios de pruebas de seguridad.

SIEM:

Sistema de gestión de eventos e información de seguridad que permite la recolección, correlación y análisis de registros en tiempo real.

SMB:

Protocolo de compartición de archivos utilizado en sistemas Windows, cuya versión SMBv1 es considerada vulnerable y obsoleta.

Introducción

El presente informe documenta el ciclo completo de un ejercicio Red Team & Blue Team realizado en SecureNova Labs con el objetivo de comprender, aplicar y analizar técnicas ofensivas y defensivas dentro de un entorno controlado. La actividad simuló un escenario real en el que un atacante compromete un servidor Windows mediante un servicio vulnerable y posteriormente ejecuta movimiento lateral dentro de la red. A partir de esta situación, el Blue Team tuvo la responsabilidad de detectar, analizar y contener el ataque utilizando exclusivamente herramientas de código abierto. Este documento articula los aspectos técnicos, éticos y normativos involucrados, y propone recomendaciones orientadas a fortalecer la postura de seguridad y la capacidad de respuesta ante incidentes.

Justificación

La creciente sofisticación de los ciberataques y la dependencia crítica de los sistemas informáticos en las organizaciones hacen indispensable la formación de profesionales capaces de comprender tanto las tácticas ofensivas como las estrategias defensivas en entornos reales.

Este proyecto se justifica en la necesidad de integrar la teoría jurídica, ética y técnica con la práctica operativa mediante un laboratorio completo que simula un ataque real y su correspondiente respuesta. El estudio del marco legal (incluyendo la Ley 1273 de 2009 y la Ley 1581 de 2012) permite al estudiante ejecutar pruebas de seguridad dentro de los límites de la legalidad, mientras que la evaluación de acuerdos organizacionales expone los riesgos éticos asociados al manejo de información sensible.

La práctica ofensiva mediante la explotación de vulnerabilidades demuestra cómo fallos menores pueden comprometer sistemas enteros, y la fase defensiva permite adquirir competencias esenciales para la detección temprana, la contención, el análisis y la mitigación del daño. Este enfoque transversal contribuye al fortalecimiento de habilidades críticas para el ejercicio profesional en ciberseguridad, promoviendo una cultura de responsabilidad, resiliencia y mejora continua en infraestructuras tecnológicas.

Objetivos

Objetivo General

Analizar, ejecutar y documentar el ciclo completo de un ejercicio Red Team & Blue Team en un entorno controlado, integrando los componentes legales, técnicos y éticos que permitan comprender las vulnerabilidades explotadas, las estrategias de defensa aplicadas y las acciones necesarias para fortalecer la seguridad de la infraestructura TI.

Objetivos Específicos

Examinar el marco legal y ético colombiano aplicable a los delitos informáticos y al manejo de datos personales, con el fin de establecer los lineamientos que deben guiar la ejecución responsable de pruebas de seguridad.

Describir y aplicar las fases metodológicas del pentesting, incluyendo reconocimiento, escaneo, explotación y post-explotación, utilizando herramientas de análisis de vulnerabilidades y servicios de información como Nmap, Metasploit, CVE y ExploitDB.

Evaluar los riesgos éticos y jurídicos asociados al acuerdo de confidencialidad propuesto por SecureNova Labs, identificando cláusulas contrarias a la legislación colombiana y al Código de Ética del COPNIA.

Ejecutar un ataque ofensivo controlado mediante la explotación de los servicios vulnerables y lograr movimiento lateral, analizando el impacto técnico del compromiso y la evidencia generada en el proceso.

Aplicar estrategias defensivas propias del Blue Team, incluyendo análisis de eventos, medidas de hardening, uso de marcos CIS, implementación de herramientas de contención y diferenciación entre roles defensivos e incident response.

Desarrollo

Legislación Colombiana Relevante

En Colombia, el marco legal en materia de delitos informáticos y protección de datos personales se ha desarrollado progresivamente para responder a los riesgos asociados al uso indebido de la información. Este conjunto normativo establece obligaciones para las personas naturales y jurídicas, así como sanciones ante conductas que vulneren la confidencialidad, integridad o disponibilidad de la información.

La Ley 1273 de 2009 modificó el Código Penal colombiano para incluir los denominados delitos informáticos, tipificando conductas como el acceso abusivo a un sistema informático, la interceptación de datos, el daño informático y la suplantación de identidad digital (Congreso de la República de Colombia, 2009). Esta norma constituye el pilar penal de la ciberseguridad en el país, dado que busca proteger los datos y la infraestructura tecnológica frente a ataques o manipulaciones no autorizadas.

La Ley 1581 de 2012 estableció el régimen general de protección de datos personales, desarrollando el derecho constitucional al habeas data, imponiendo obligaciones a las organizaciones en cuanto al tratamiento, almacenamiento y circulación de información personal (Congreso de la República de Colombia, 2012). Esta ley es complementada por el Decreto 1377 de 2013, el cual reglamenta parcialmente su aplicación y define los procedimientos para la obtención del consentimiento informado por parte de los titulares de los datos (Presidencia de la República de Colombia, 2013).

De igual forma, la Ley 1266 de 2008 regula el manejo de datos financieros, crediticios y comerciales, estableciendo principios de veracidad, integridad y finalidad en la administración de la información económica (Congreso de la República de Colombia, 2008). Finalmente, la Ley

1621 de 2013 aborda las actividades de inteligencia y contrainteligencia, delimitando el uso legítimo de la información por parte del Estado en el marco del respeto a los derechos fundamentales (Congreso de la República de Colombia, 2013).

Pentesting y sus Etapas

Las pruebas de penetración (pentesting) constituyen un proceso sistemático que permite evaluar la seguridad de los sistemas informáticos mediante la simulación controlada de ataques. Este tipo de auditoría técnica busca identificar vulnerabilidades y verificar la efectividad de los controles implementados (Kaur et al., 2023).

Las etapas del pentesting siguen un flujo metodológico ordenado, cuya aplicación práctica se detalla a continuación:

- Planeación y alcance: En esta etapa se define el objetivo, el alcance, los recursos y las limitaciones de la prueba. Incluye la obtención del consentimiento del cliente y la firma del documento Rules of Engagement. La gestión de esta fase puede apoyarse con plataformas como Dradis Framework, que facilitan la documentación y organización del proyecto.
- Reconocimiento (OSINT): Consiste en la recopilación pasiva de información pública sobre la organización, sus dominios y direcciones IP. Herramientas como theHarvester o Recon-ng permiten automatizar esta búsqueda sin interactuar directamente con los sistemas objetivo (Simões et al., 2022).
- Escaneo y enumeración: En esta fase se identifican los puertos abiertos, servicios activos y sistemas operativos presentes mediante escaneos activos. Una herramienta ampliamente utilizada es Nmap, que permite realizar detección de versiones y análisis de red (Nmap Project, s.f.).

- Análisis de vulnerabilidades: Una vez detectados los servicios, se procede a correlacionarlos con vulnerabilidades conocidas. Para esta etapa se recomienda OpenVAS, que realiza un escaneo automatizado y genera reportes de riesgo basados en el sistema CVSS (Greenbone Networks, s.f.).
- Explotación: Se busca comprobar si las vulnerabilidades detectadas pueden ser aprovechadas. Metasploit Framework es el entorno más empleado para pruebas controladas, dado que integra exploits y payloads con mecanismos de registro y reversión seguros (Rapid7, s.f.).
- Post-explotación y escalada de privilegios: Se centra en analizar el alcance real del acceso obtenido tras comprometer un sistema, evaluando tanto los privilegios disponibles como las acciones que un atacante podría ejecutar con ellos. En este punto se validan rutas de escalada de privilegios, persistencia, movimiento lateral y extracción de información sensible. Herramientas como Meterpreter permiten operar de forma flexible sobre el sistema comprometido, mientras que utilidades de auditoría local como LinPEAS y WinPEAS ayudan a identificar configuraciones débiles, permisos inseguros y caminos potenciales de elevación de privilegios (Alabdan, 2020).
- Reporte y remediación: Finalmente, se documentan los hallazgos, evidencias y recomendaciones. El informe técnico debe ser claro, reproducible y debe contener un análisis de impacto y priorización de mitigaciones.

El pentesting debe entenderse como un proceso científico, se formula una hipótesis de vulnerabilidad, se ejecutan pruebas controladas, se registran resultados y se presentan conclusiones éticas y verificables. El cumplimiento de las normas legales y los principios de responsabilidad profesional son esenciales en todo el ciclo de la prueba.

Herramientas de Ciberseguridad

El uso de herramientas y bases de datos especializadas constituye una parte fundamental de la práctica profesional en ciberseguridad. Estas permiten automatizar tareas, correlacionar vulnerabilidades y validar controles técnicos en redes y sistemas.

Metasploit Framework: es un entorno de código abierto que facilita la creación, prueba y ejecución de exploits de manera controlada (Rapid7, s.f.). Su estructura modular permite realizar tareas de explotación, post-explotación y validación de defensas, convirtiéndose en una herramienta clave para equipos Red Team.

Nmap (Network Mapper): es una herramienta de descubrimiento de red y escaneo de puertos utilizada para la fase de reconocimiento y enumeración. Permite identificar hosts activos, servicios y sistemas operativos, lo que la convierte en un componente esencial para el diagnóstico de seguridad (Nmap Project, s.f.).

OpenVAS: es un sistema de evaluación de vulnerabilidades que realiza análisis automatizados basados en una base de datos actualizada de fallas de seguridad. Proporciona informes con niveles de riesgo y recomendaciones, lo que la hace ideal para tareas de Blue Team (Greenbone Networks, s.f.).

En cuanto a servicios en línea, Exploit Database (ExploitDB) es un repositorio público mantenido por Offensive Security que recopila exploits y pruebas de concepto documentadas, utilizadas para el aprendizaje y validación de vulnerabilidades (Exploit Database, s.f.).

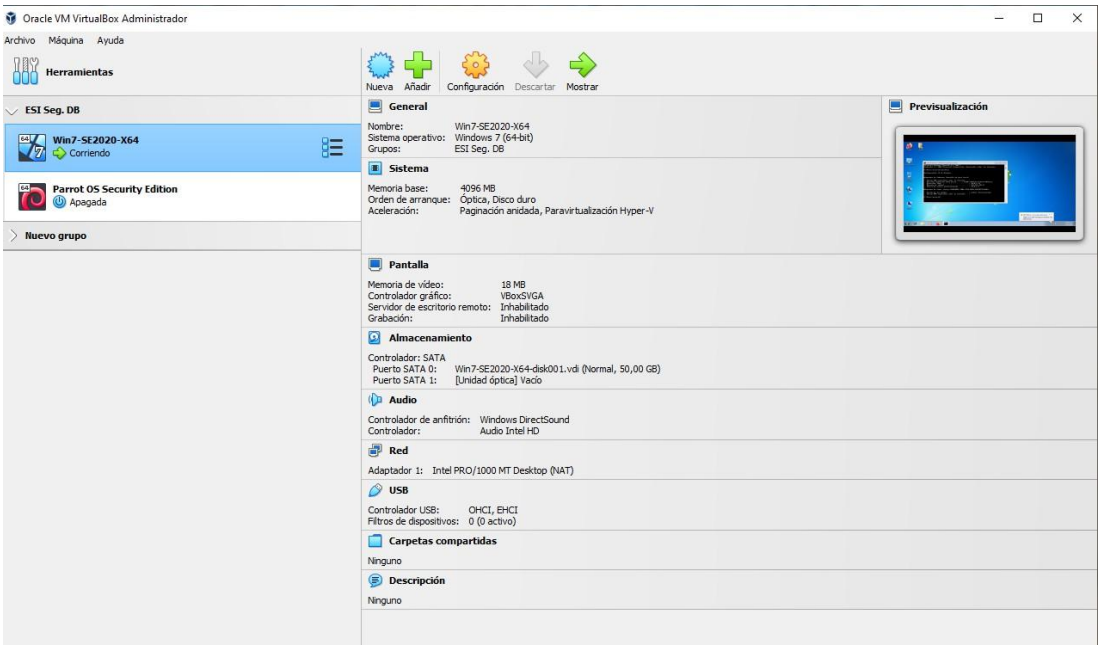
El sistema CVE (Common Vulnerabilities and Exposures): administrado por MITRE Corporation, proporciona identificadores estandarizados para vulnerabilidades conocidas, facilitando la comunicación y priorización de parches de seguridad (MITRE, s.f.).

Montaje máquinas virtuales en VirtualBox

Configuración de la máquina virtual “W7” en VirtualBox. La Ilustración 1a muestra los parámetros principales asignados a la VM: sistema operativo Windows 7, memoria RAM asignada (4 GB), CPU (1 vCPU), disco virtual (VDI) con tamaño reservado dinámicamente, controlador de disco SATA y adaptador de red 1 configurado en modo Host-Only/Red interna con NAT desactivado para pruebas de laboratorio. Estos ajustes facilitan la interconexión entre máquinas en un entorno controlado y minimizan el impacto sobre la red host.

Figura 1

Maquina W7 configuración



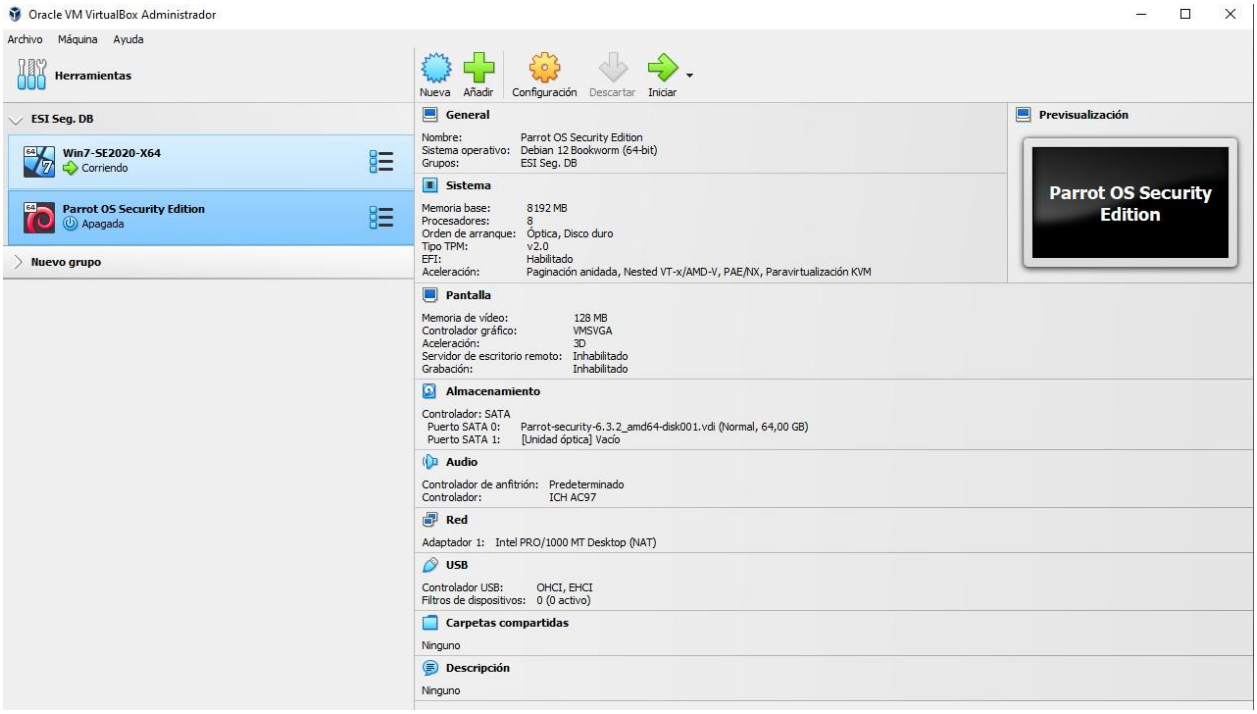
Nota. Montaje de máquinas virtuales.

Configuración de la máquina virtual “Parrot” (Parrot OS) en VirtualBox. La Ilustración 2 presenta los parámetros básicos: sistema operativo Linux (Parrot Security OS), memoria RAM asignada (8 GB), CPU, disco virtual y adaptador de red 1 configurado en la misma red privada

que la VM W7 (NAT), permitiendo comunicación directa entre equipos de laboratorio para pruebas de pentesting y defensa.

Figura 2

Maquina Parrot Configuración



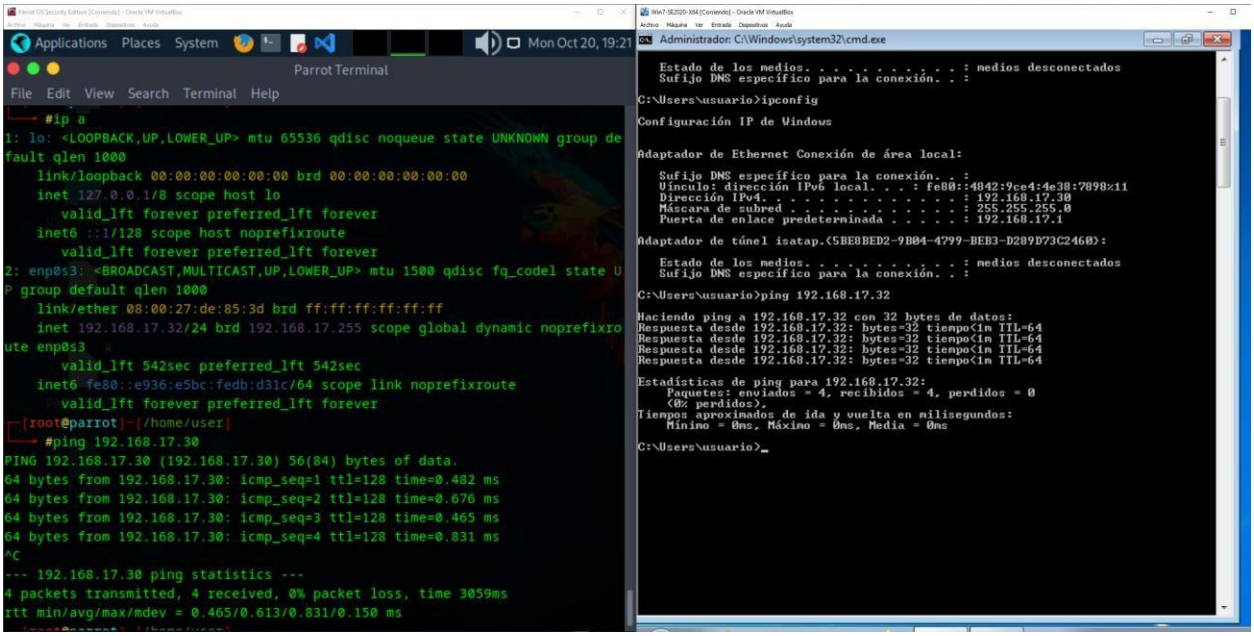
Nota. Configuración de parrot en VirtualBox.

Verificación de conectividad entre máquinas virtuales mediante comando ping. La captura muestra la salida del ping desde la VM Parrot hacia la VM W7: Parrot: 192.168.17.32;

W7: 192.168.17.30. La respuesta positiva confirma conectividad ICMP en la red privada 192.168.17.0/24 y valida la configuración de interfaces en las VMs para pruebas de laboratorio.

Figura 3

Comunicación Exitosa Entre Maquinas



Nota. Verificación de conectividad entre máquinas virtuales.

La fase ofensiva inició con la identificación del servicio vulnerable Rejetto HFS en Host A, cuya versión era susceptible a ejecución remota de código (RCE). El atacante explotó esta brecha para obtener acceso inicial y desplegar una sesión remota. Posteriormente se ejecutó reconocimiento interno desde A hacia la red 2.0, donde se detectó la presencia de Host B. Una vez identificado el acceso SMB sobre el puerto 445, se utilizó el exploit EternalBlue (MS17-010) para realizar movimiento lateral.

El pivoting permitió al Red Team ejecutar comandos y crear una cuenta administrativa efímera en Host B, completando el compromiso del segmento interno. Estas acciones reflejan

técnicas comunes de adversarios reales, como se describe en INCIBE (2019) y en la literatura de pentesting.

Ética Profesional y Marco Normativo en Operaciones de Seguridad

Dentro del acuerdo de confidencialidad presentado por SecureNova Labs este contiene procesos ilegales y éticamente cuestionables, los cuales vulneran principios fundamentales del derecho y de la ciberseguridad profesional. En particular, el documento establece obligaciones para la parte receptora que pueden considerarse ilegales y moralmente cuestionables.

Por ejemplo, la cláusula cuarta, numerales tres y cuatro, señala que el firmante debe "no denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros" y "abstenerse de denunciar y publicar la información confidencial e ilegal que conozca" (SecureNova Labs, 2025, p. 4). Estas disposiciones suponen un claro conflicto con el deber ciudadano de denunciar los delitos, contemplado en el artículo 67 del Código Penal Colombiano (Ley 599 de 2000).

Dichas cláusulas vulneran los principios de legalidad, transparencia e integridad profesional. Desde una perspectiva ética, el Código de Ética del Consejo Profesional Nacional de Ingeniería, establece que los profesionales de la ingeniería y la tecnología deben actuar de conformidad con la ley y con los valores de honestidad, responsabilidad y respeto por el bien común (COPNIA, 2005, arts. 1, 4 y 8).

Por tanto, al obligar al aspirante a guardar silencio frente a actividades ilícitas, el acuerdo promueve el encubrimiento y desnaturaliza el verdadero propósito de la confidencialidad, que debe proteger la información legítima, no ocultar delitos.

Dentro de los artículos de la Ley 1273 de 2009, el acuerdo podría vulnerar diversos artículos de la Ley 1273 de 2009, la cual modifica el Código Penal para tipificar los delitos

informáticos y la protección de los datos. En primer lugar, el artículo 269A establece como delito el acceso abusivo a un sistema informático sin autorización; si la información que se pretende mantener en reserva proviene de actividades de intrusión o espionaje digital, el silencio impuesto al firmante implicaría tolerar o encubrir ese delito. En segundo lugar, el artículo 269B sanciona la obstaculización ilegítima de sistemas informáticos o redes de telecomunicaciones; al impedir que se denuncien actividades sospechosas, se podría facilitar indirectamente este tipo de acciones ilícitas.

De igual modo, el artículo 269F, referente a la violación de datos personales, podría ser vulnerado, dado que el acuerdo no garantiza que la información sensible sea tratada conforme a los principios de finalidad y legalidad establecidos por la Ley 1581 de 2012 sobre protección de datos personales. El artículo 269H, que penaliza la utilización ilícita de software malicioso, también podría verse comprometido si la empresa utiliza herramientas ofensivas sin autorización durante sus pruebas de Red Team y la parte receptora omite reportarlo. Este acuerdo representa un riesgo jurídico, pues expone al firmante a responsabilidades penales derivadas de la complicidad o encubrimiento de conductas delictivas.

Decisión Profesional Ante la Oferta Laboral

Aunque la empresa ofrece un salario mensual de quince millones de pesos colombianos y un contrato vitalicio, desde una perspectiva ética y profesional, no sería apropiado aceptar un empleo en tales condiciones. El Código de Ética del COPNIA (2005) es claro al indicar que los profesionales deben rechazar cualquier actividad que sea contraria a la ley, a la moral o al interés público (arts. 10 y 11). Además, el ejercicio de la ingeniería y la tecnología implica una responsabilidad social que trasciende los beneficios económicos personales. La integridad, la transparencia y la honestidad son pilares que no pueden negociarse frente a incentivos

financieros, especialmente en el ámbito de la ciberseguridad, donde la confianza y la ética son esenciales para la protección de los sistemas y los datos de terceros.

Aceptar un acuerdo que exige omitir denuncias sobre actividades ilegales implicaría una falta grave a la ética profesional y una violación directa de la responsabilidad social del ingeniero o tecnólogo. La decisión correcta sería rechazar la oferta y reportar las irregularidades observadas a las autoridades competentes, contribuyendo así a la defensa de la legalidad y a la consolidación de una práctica profesional responsable y transparente.

Ciber espionaje y Ética en SecureNova Labs

En el escenario descrito sobre el caso “Ciber espionaje y Ética en SecureNova Labs”, se plantean implicaciones éticas y legales significativas respecto al acceso, uso y manipulación de información sensible. Las empresas de ciberseguridad deben contar con acceso limitado, controlado y temporal a la información de sus clientes, estrictamente para fines de auditoría o pruebas de penetración autorizadas. Este acceso debe enmarcarse en los principios de necesidad, proporcionalidad y consentimiento informado, conforme a los lineamientos de la ISO/IEC 27001:2022 y la Ley 1581 de 2012. De esta manera se garantiza que el tratamiento de la información cumpla con las obligaciones de confidencialidad y transparencia, evitando cualquier uso indebido o explotación comercial no autorizada.

Para prevenir la utilización inadecuada de herramientas de análisis forense o de hacking ético, las organizaciones deben implementar mecanismos robustos de control y supervisión. Entre estos se destacan las políticas de acceso basado en privilegios mínimos, la auditoría continua de registros (logging), la segregación de funciones entre los equipos Red y Blue Team, así como la realización de capacitaciones periódicas en ética profesional y cumplimiento

normativo. Estas medidas permiten mitigar riesgos y reforzar la confianza institucional, elemento esencial en el ecosistema digital.

En caso de que la empresa de ciberseguridad incurra en actos de espionaje, los gobiernos y organizaciones contratantes deben actuar con firmeza. Las acciones adecuadas incluyen la terminación inmediata del contrato, la notificación a las autoridades judiciales y administrativas, la imposición de sanciones legales y la adopción de medidas correctivas para proteger a las víctimas y restaurar la confianza pública. Tales procedimientos reflejan el principio de responsabilidad social corporativa y el compromiso con la seguridad y soberanía digital del Estado. En este sentido, la ética profesional debe prevalecer siempre como pilar del ejercicio de la ciberseguridad, garantizando que la tecnología sirva al bien común y no a intereses contrarios a la ley.

Practica Simulada

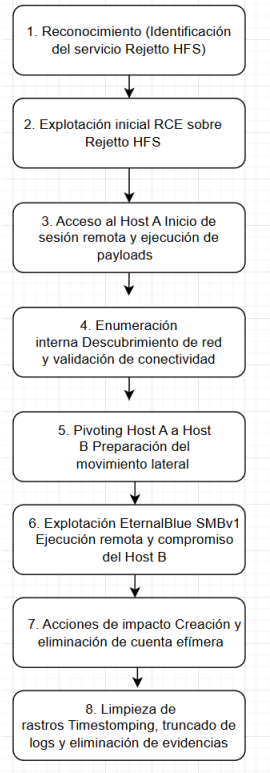
La fase ofensiva inició con la identificación del servicio vulnerable Rejetto HFS en Host A, cuya versión era susceptible a ejecución remota de código (RCE). El atacante explotó esta brecha para obtener acceso inicial y desplegar una sesión remota. Posteriormente se ejecutó reconocimiento interno desde A hacia la red 2.0, donde se detectó la presencia de Host B. Una vez identificado el acceso SMB sobre el puerto 445, se utilizó el exploit EternalBlue (MS17-010) para realizar movimiento lateral.

Para facilitar la comprensión del incidente y ofrecer una visión estratégica del flujo de acciones realizadas por el atacante, se incorpora un resumen gráfico de la cadena de ataque, alineado con el estilo de análisis utilizado en metodologías como MITRE ATT&CK y los modelos de Kill Chain. Esta representación permite observar de manera secuencial los vectores

de entrada, las técnicas empleadas, los momentos de persistencia, los mecanismos de escalamiento y, finalmente, el impacto en los sistemas comprometidos.

Figura 4

Cadena de Ataque



Nota. El diagrama resume de forma secuencial las fases del ataque identificadas durante el análisis forense, desde el reconocimiento inicial del servicio vulnerable hasta la explotación, el movimiento lateral hacia el Host B y las acciones de impacto y ocultamiento ejecutadas por el atacante. La representación permite visualizar la progresión lógica del compromiso y su relación con las evidencias técnicas recopiladas en cada etapa.

El pivoting permitió al Red Team ejecutar comandos y crear una cuenta administrativa efímera en Host B, completando el compromiso del segmento interno. Estas acciones reflejan

técnicas comunes de adversarios reales, como se describe en INCIBE (2019) y en la literatura de pentesting.

Para esta fase se utilizaron diversas herramientas del framework Metasploit y utilidades complementarias en Parrot OS, organizadas conforme a las fases formales de un proceso de pentesting. En la fase de reconocimiento y enumeración, se empleó Nmap para identificar servicios expuestos y verificar la presencia del servidor HFS en la Máquina-1 Windows. Posteriormente, dentro de Metasploit, se utilizaron módulos como auxiliary/scanner/smb/smb_version y auxiliary/scanner/portscan/tcp para obtener información adicional sobre los servicios SMB, su versión y los puertos abiertos.

Durante la fase de explotación, se usó el módulo exploit/windows/http/rejetto_hfs_exec, diseñado para ejecutar código remoto a través de la vulnerabilidad presente en HFS 2.3, lo que permitió obtener una sesión Meterpreter con privilegios de SYSTEM. En la fase de post-explotación, se ejecutaron módulos como post/windows/gather/arp_scanner para identificar otros equipos dentro de la red interna, y post/windows/manage/portproxy junto con autoroute para establecer pivoting hacia la Máquina-B mediante reenvío de puertos.

Finalmente, herramientas de credencial dumping como mimikatz (extensión kiwi) permitieron extraer credenciales y hashes que apoyaron el proceso de movimiento lateral. Cada una de estas herramientas fue documentada mediante capturas, registros de comandos y resultados directos obtenidos durante la práctica.

La información proporcionada en el anexo 4 permitió identificar con precisión el fallo de seguridad de la Máquina-1 Windows. En primer lugar, la máquina se encontraba ejecutando Rejetto HTTP File Server (HFS) versión 2.3, un software conocido por contener vulnerabilidades críticas de ejecución remota de comandos (RCE), específicamente la CVE-2014-6287.

Adicionalmente, la topología de red señalaba que este equipo se encontraba directamente expuesto al atacante, lo que facilitaba el acceso al puerto 80 donde HFS se encontraba publicado.

La descripción funcional del servidor empleado para compartir archivos y el hecho de que se ejecutaba con privilegios elevados en el sistema permitieron deducir que, de ser comprometido, otorgaría control total sobre el sistema operativo. Toda esta información, combinada con los resultados del escaneo inicial, fue determinante para reconocer que la vulnerabilidad explotable correspondía a la implementación insegura del parser de comandos del servidor HFS 2.3.

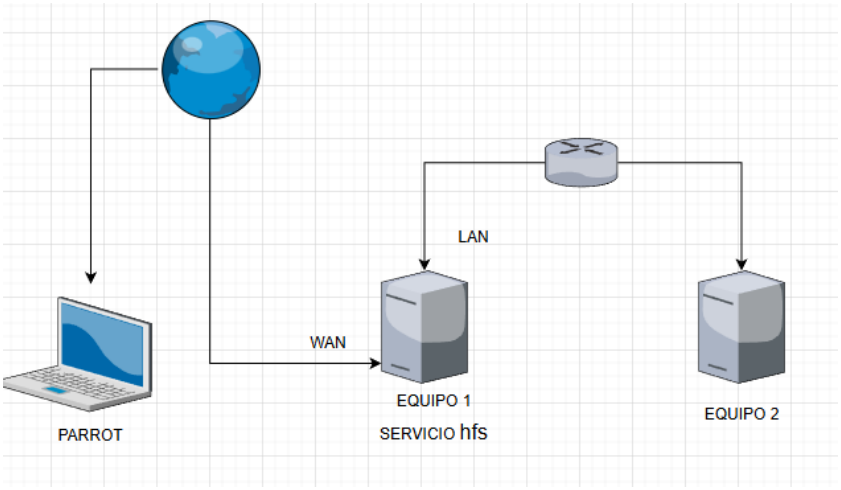
La vulnerabilidad de la Máquina-1 Windows fue identificada mediante el uso combinado de Nmap y Metasploit. Nmap permitió detectar que la aplicación vulnerable, Rejetto HFS 2.3, se encontraba publicada en el puerto 80/TCP, lo cual fue confirmado a través de scripts NSE y banner grabbing. Posteriormente, dentro del entorno Metasploit, el módulo exploit/windows/http/rejetto_hfs_exec permitió verificar automáticamente la presencia de la vulnerabilidad al reconocer la versión específica del servicio y confirmar que era susceptible a explotación. Por tanto, la herramienta clave para identificar el fallo fue la enumeración activa de servicios realizada por Nmap, complementada por la validación del exploit correspondiente dentro de Metasploit.

El ataque realizado afectó directamente a las máquinas Windows dentro de la red al comprometer inicialmente la Máquina-1 (HFS) y utilizarla como punto de salto para alcanzar la Máquina-B mediante técnicas de pivoting. Al explotar la vulnerabilidad RCE en HFS, se obtuvo una sesión Meterpreter con privilegios de NT AUTHORITY\SYSTEM, lo que permitió ejecutar acciones de post-explotación, enumerar la red interna, crear reglas de port-proxy y reenviar puertos hacia otros equipos de la red.

Este tipo de ataque demuestra cómo una vulnerabilidad expuesta al exterior puede comprometer no solo el sistema afectado, sino también toda la infraestructura que depende de él. Gráficamente, el ataque puede representarse como un flujo en el cual el atacante entra por el puerto 80 hacia la Máquina-A, obtiene una shell privilegiada, configura rutas internas y utiliza dicha máquina como puente para interactuar con servicios SMB en la Máquina-B, incluso sin credenciales válidas. Este vector de ataque ilustra el riesgo de una cadena de compromisos en entornos donde un solo servicio vulnerable permite acceso lateral hacia máquinas internas aparentemente protegidas.

Figura 5

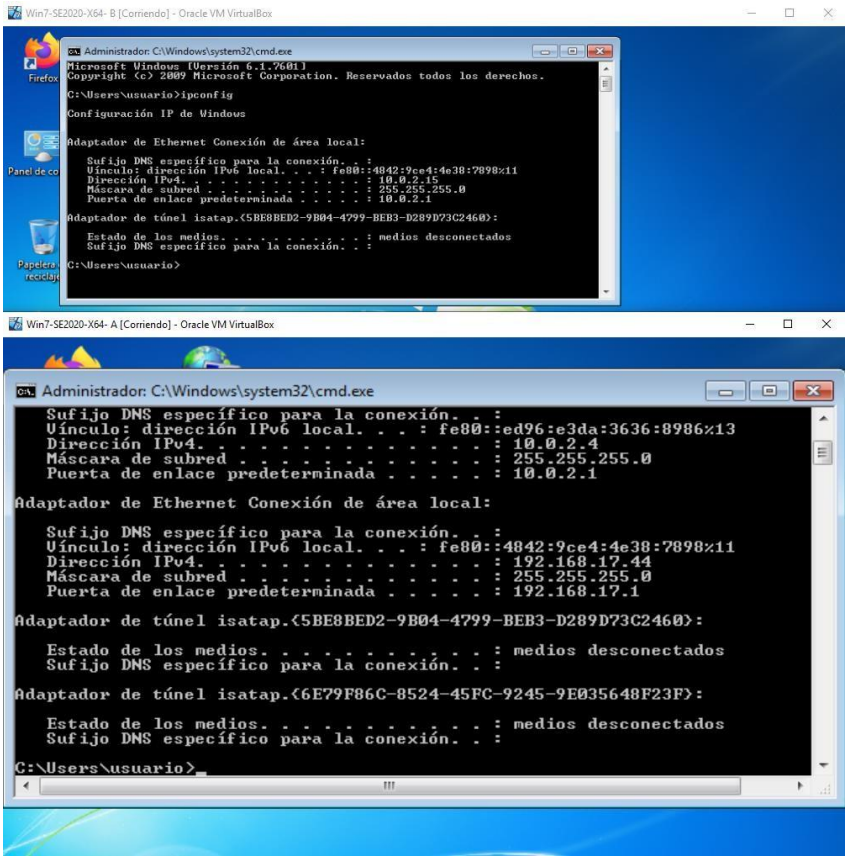
Topología del Escenario de Ataque Utilizada en el Laboratorio



Nota. La figura representa la estructura de red empleada en el escenario de laboratorio, donde el equipo Parrot se conecta por la interfaz WAN al Equipo 1 que expone el servicio HFS vulnerable. Este equipo, a su vez, mantiene comunicación por la red LAN con el Equipo 2, permitiendo ilustrar el vector de acceso inicial y el movimiento lateral observado durante el ataque.

Figura 6

Confirmación de Ip de los Host A y B



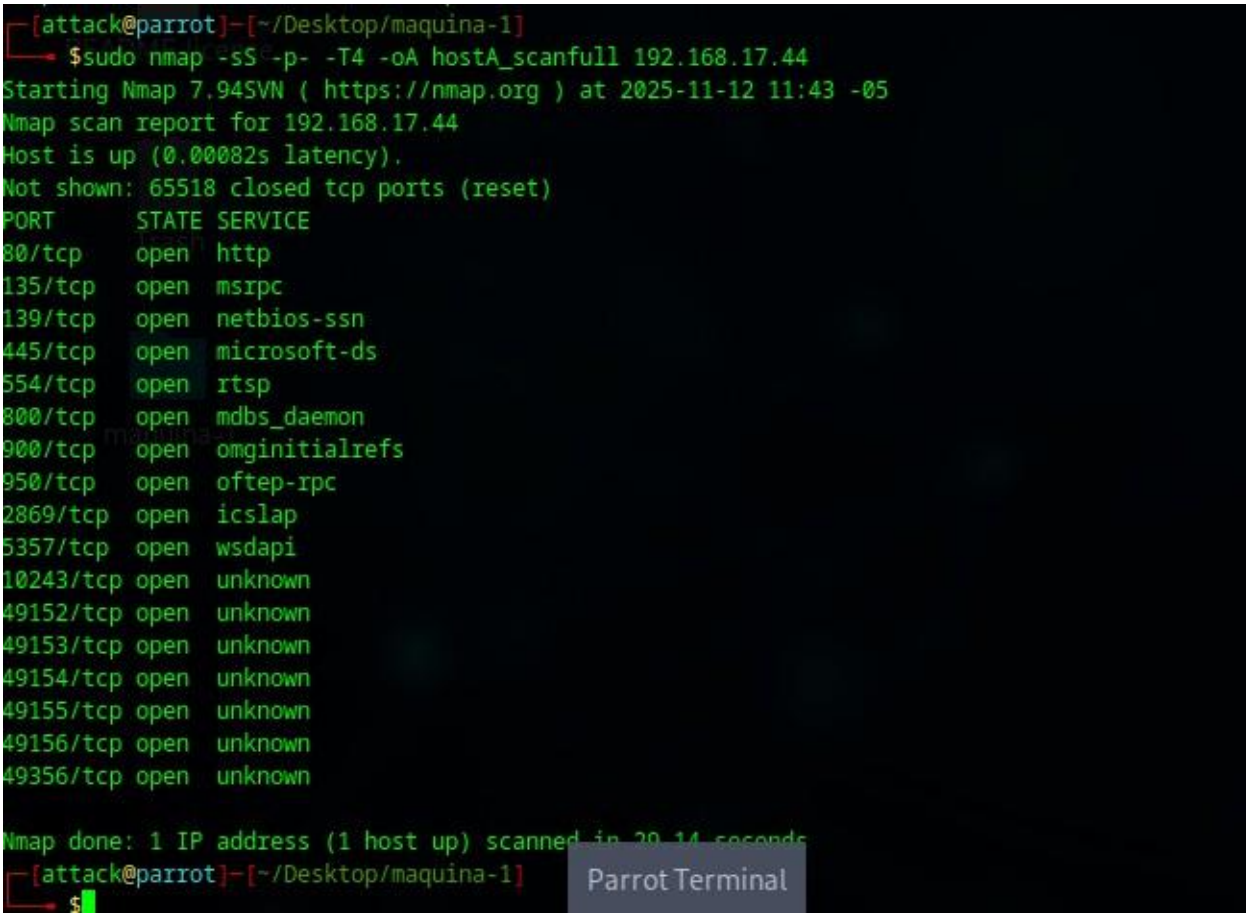
Nota. Dirección ip correspondiente de cada máquina.

Fase de Reconocimiento Activo

Se realiza escaneo de puertos y detección de servicios, con el comando: nmap -sS -p- -T4 -oA hostA_fullscan 192.168.17.44

Figura 7

Resultado Reconocimiento Activo



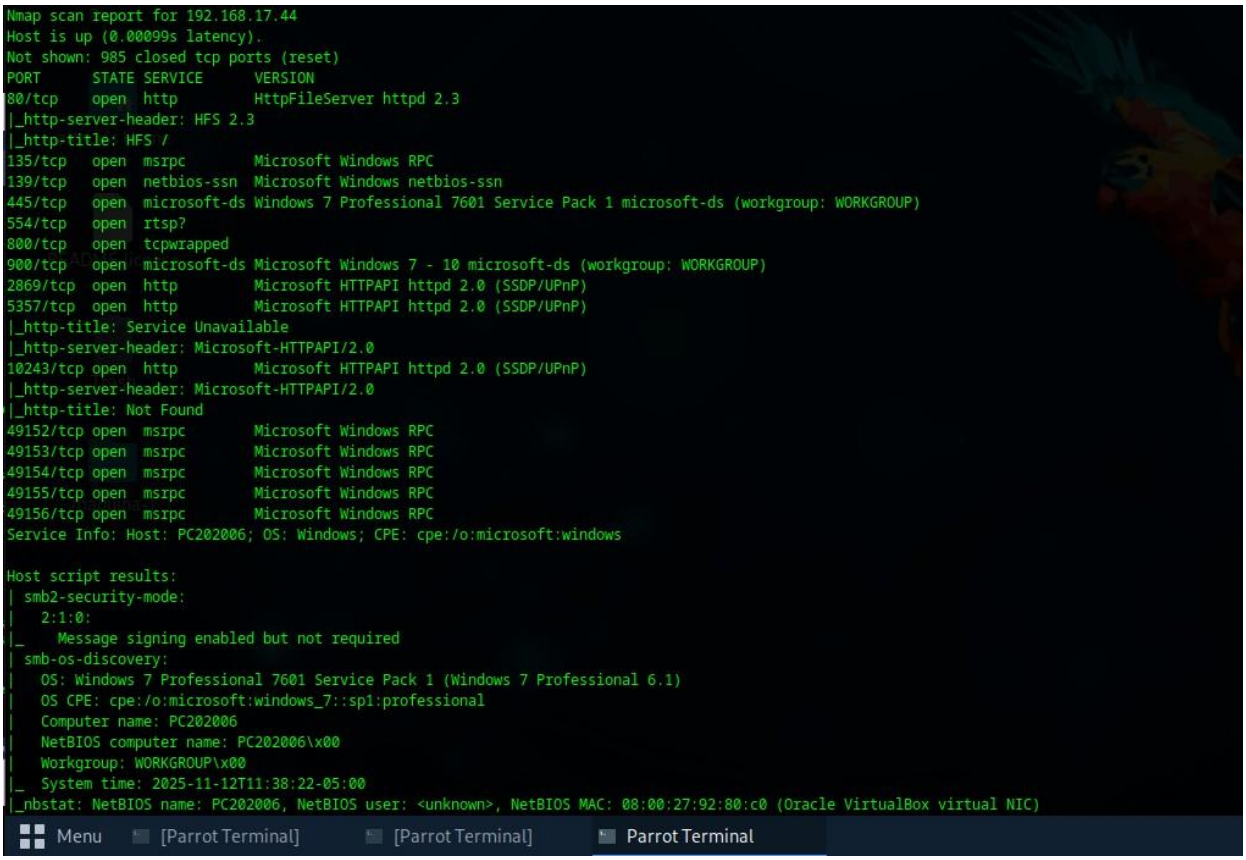
Nota. Puertos analizados con la herramienta Nmap.

Se realiza la detección versión y scripts de vulnerabilidades por medio del comando:

nmap -sV -sC -p 22,80,139,445,3389 -oN hostA_services.txt 192.168.17.44

Figura 8

Respuesta de Verificación de Vulnerabilidad de Host A



Nota. Verificación de tipo de vulnerabilidades.

Host: 192.168.17.44 (PC202006, Windows 7 Professional SP1).

Puertos detectados

- 139/tcp — open — netbios-ssn (SMB sobre NetBIOS).
- 445/tcp — open — microsoft-ds (SMB).

Resultados relevantes del script smb-os-discovery:

- SMB2: message signing enabled but not required: Indica una configuración débil de firma de mensajes (no se exige firma obligatoria), lo que facilita ataques de manipulación o suplantación sobre SMB.

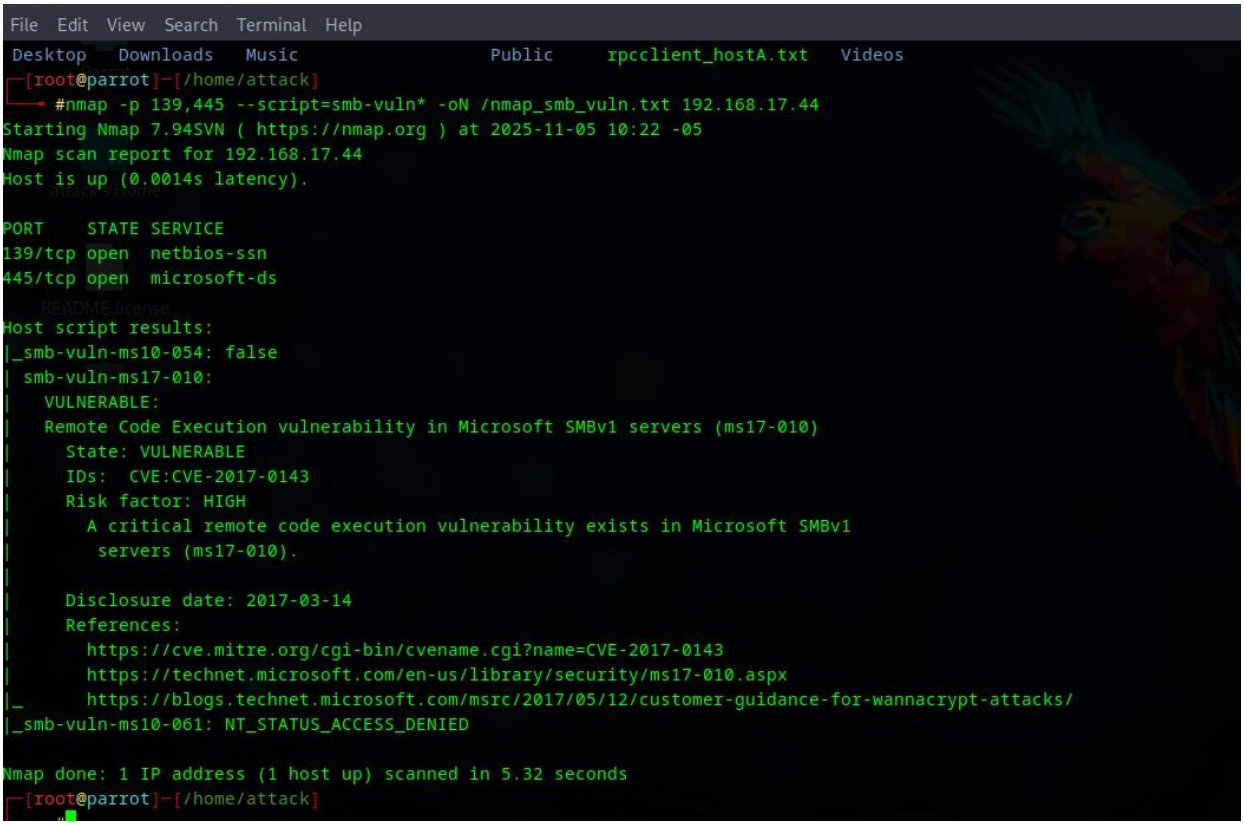
- Account_used: guest / authentication_level: user sugiere que existen recursos accesibles con privilegios mínimos (guest) o con una autenticación de usuario poco estricta.
- Las secciones smb2-security-mode y smb-security-mode reflejan parámetros de seguridad que, en combinación con un sistema Windows 7 sin parches, pueden ser aprovechables por exploits públicos conocidos.

El vector de ataque más evidente en la máquina escaneada es SMB (puertos 139/445). Un sistema con Windows 7 y SMB expuesto es un candidato típico para vulnerabilidades como MS17-010 (EternalBlue) si no se encuentra parcheado. Además, la presencia de shares accesibles con acceso guest o configuraciones permisivas incrementa el riesgo de movimiento lateral y exfiltración de información.

Se ejecuta el comando de ilustracion4 para comprobar MS17-010 y otras vulnerabilidades SMB:

Figura 9

Verificar Vulnerabilidades SMB (nmap NSE)



Nota. Confirmación de vulnerabilidades de forma detallada.

El escaneo arrojó que los puertos 139/tcp (netbios-ssn) y 445/tcp (microsoft-ds) están abiertos en el host 192.168.17.44 (PC202006, Windows 7 Professional SP1). El script de comprobación de vulnerabilidades SMB informó la presencia de la vulnerabilidad MS17-010 (EternalBlue), con el siguiente detalle:

- Vulnerabilidad: Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010).
- Estado detectado por el script: VULNERABLE.
- ID asociado: CVE-2017-0143 (reportado como parte de MS17-010).

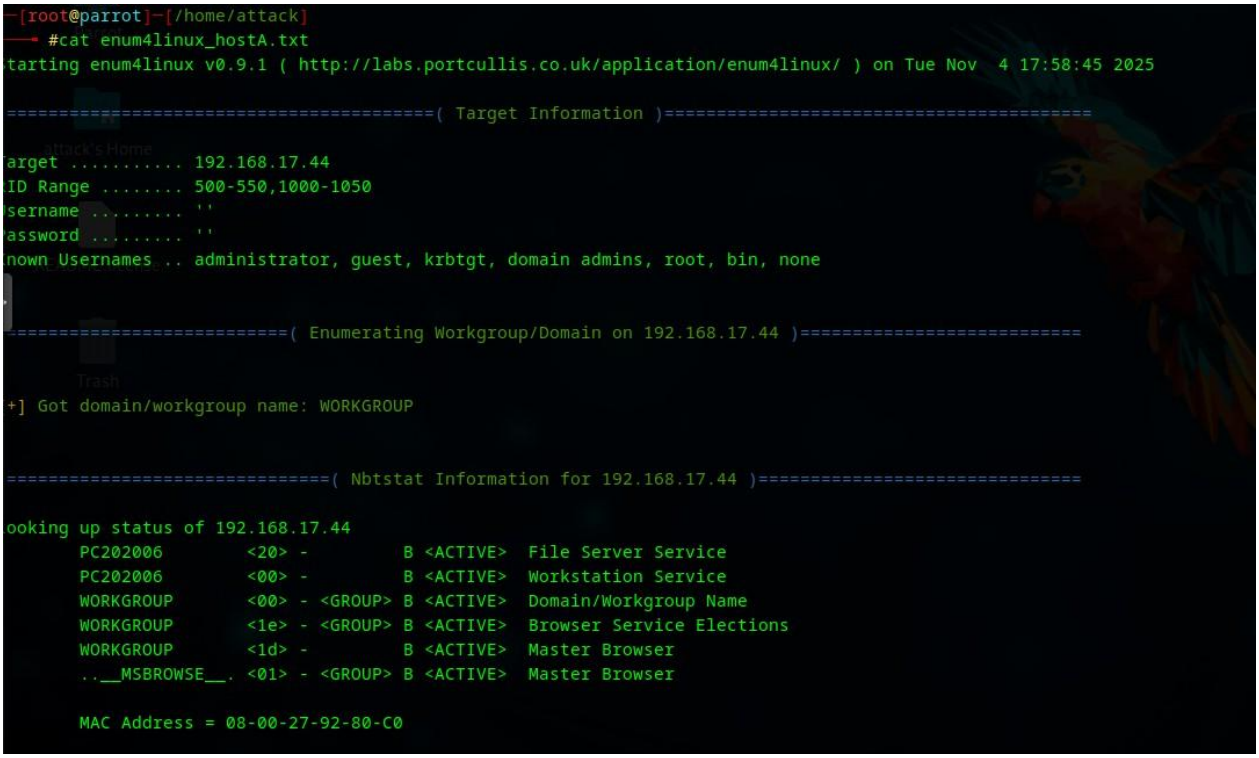
- Factor de riesgo: ALTO.
- Fecha de divulgación: 2017-03-14.
- Referencias técnicas: páginas oficiales de Microsoft y CVE para MS17-010.

La combinación de un sistema Windows 7 con los puertos SMB (139/445) expuestos y la detección positiva del script smb-vuln-ms17-010 indica que la máquina es un candidato probable para explotación remota mediante el exploit conocido como EternalBlue (MS17-010). Dada la criticidad de esta vulnerabilidad (ejecución remota de código), su explotación permitiría, en condiciones favorables, la ejecución de payloads remotos y potencialmente un escalamiento de acceso y movimiento lateral dentro de la red.

Se ejecutó enum4linux -a 192.168.17.44 contra el host objetivo y se registró la salida completa en evidence/enum4linux_hostA.txt. Del resultado extraído se obtienen datos relevantes para la identificación del activo y su rol en la red: el equipo reporta el nombre PC202006, pertenece al workgroup: WORKGROUP y presenta servicios NetBIOS activos que indican funciones de File Server y Workstation Service. Además, se obtiene la dirección MAC: 08:00:27:92:80:C0, útil para correlación con inventario y segmentación. Estos artefactos confirman la presencia de servicios SMB/NetBIOS accesibles y aportan contexto para el riesgo de movimiento lateral y exfiltración descrito en el análisis de vulnerabilidades.

Figura *10*

Salida de enum4linux para 192.168.17.44



Nota. Muestra de resultados de escaneo almacenado en archivo de texto.

El proceso inicial, indica que el escaneo fue anónimo (null session) (Username: '', Password: ''). El RID Range 500-550,1000-1050 son los identificadores por defecto donde enum4linux intentará enumerar usuarios del dominio local. esto confirma que el objetivo (Host-A) acepta conexiones SMB anónimas, al menos hasta cierto punto.

El host pertenece al grupo de trabajo WORKGROUP, típico de estaciones Windows que no están unidas a un dominio Active Directory. Esto dice que es una máquina Windows autónoma, no miembro de dominio.

Información de Nbtstat:

Esta parte proviene del protocolo NetBIOS Name Service (NBNS) y muestra los servicios anunciados por la máquina, que se presentan en la tabla 1.

Tabla 1

Información Nbtstat

Línea	Código NetBIOS	Significado
<20>	File Server Service	La máquina comparte archivos SMB, servicio activo en el puerto 445 o 139.
<00>	Workstation Service	Nombre del host en la red local (PC202006).
<1e>	Browser Service Elections	Indica que participa en elecciones de "browser service" (red de Windows).
<1d>	Master Browser	Este host es el "Master Browser" del grupo de trabajo: recopila listas de equipos SMB visibles.
<01> __MSBROWSE__	Master Browser Group	Señal de que coordina el descubrimiento en la red.
MAC Address	Dirección física virtual (08-00-27 → VirtualBox).	Esto confirma que es una VM Windows corriendo en VirtualBox.

Nota. Información desglosada de la información de nbtsat.

Figura 11

Final de recolección de Información

Nota. Recolección de información final.

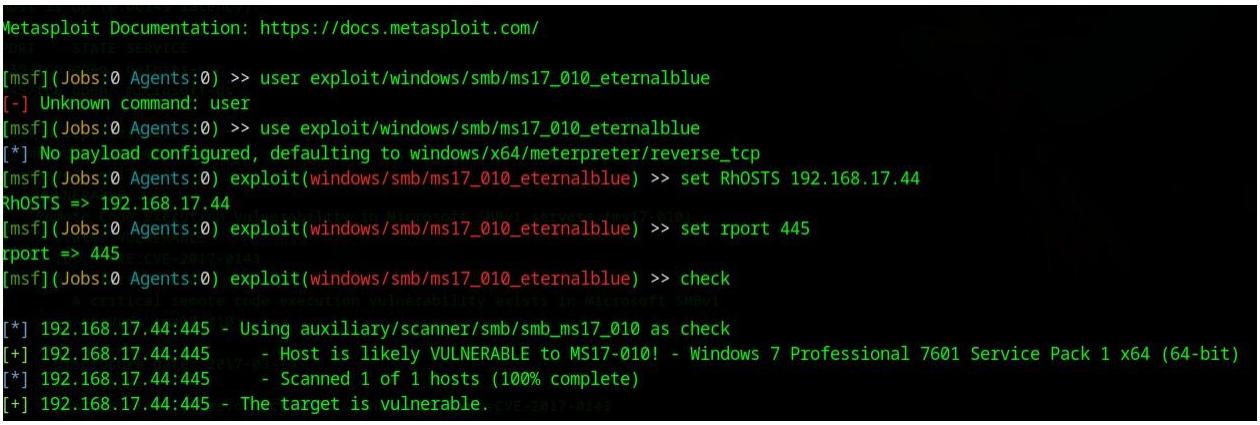
El Host-A tiene SMB activo, pertenece a WORKGROUP y actúa como Master Browser, lo que explica por qué enum4linux logra recolectar esta información sin credenciales. Ya que enum4linux sólo te arrojó información básica (nombre NetBIOS y grupo de trabajo), para continuar con la enumeración se usan otras herramientas como se ve a continuación:

Fase de análisis de vulnerabilidades y revisión de EternalBlue

Del análisis se identificó una vulnerabilidad crítica en el subsistema SMB del host 192.168.17.44. Las evidencias de nmap y la verificación con Metasploit (check) corroboran que el equipo es vulnerable a MS17-010 (CVE-2017-0143), lo cual permite la ejecución remota de código en condiciones favorables. El comando check en Metasploit verifica si el módulo considera el objetivo vulnerable sin lanzar el exploit, es una comprobación válida para la fase de verificación antes de explotar.

Figura 12

Verificación de Vulnerabilidad



Nota. Uso de Metasploit para validar vulnerabilidad.

Se ejecutó en Metasploit el módulo asociado a la vulnerabilidad MS17-010 (EternalBlue) con la instrucción check para verificar la susceptibilidad del host 192.168.17.44 sin realizar explotación activa. La salida registrada y capturada en pantalla indica: Host is likely VULNERABLE to MS17-010!, la comprobación informa que el objetivo es vulnerable y

muestra la identificación del sistema objetivo en este caso Windows 7 Professional 7601 Service Pack 1 (x64 en el entorno de verificación).

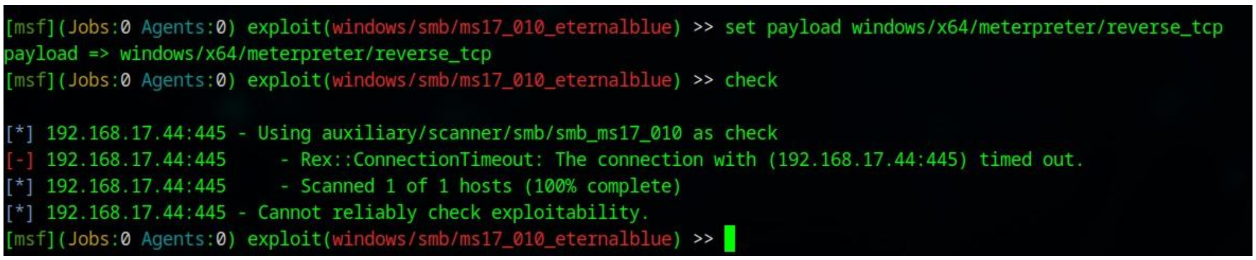
El resultado del check corrobora la detección previa realizada en la fase de escaneo (nmap --script=smb-vuln*) y confirma que el servicio SMB expuesto (puerto TCP 445) es susceptible a la vulnerabilidad MS17-010. Dado que check no planta payloads ni ejecuta el

exploit, este registro constituye evidencia de verificación segura sin afectar la integridad del sistema objetivo.

Fase de Explotación

Figura 13

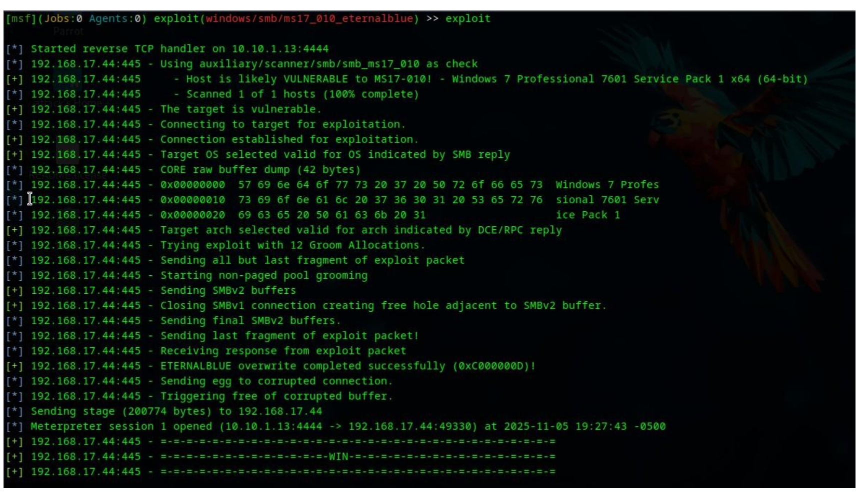
Fase de Explotación Configuración



Nota. Carga en configuración de exploit.

Figura 14

Fase de Explotación



Nota. Ejecución con éxito de exploit.

Se ejecutó con éxito el exploit exploit/windows/smb/ms17_010_eternalblue contra el host 192.168.17.44 (Windows 7 Professional SP1). Metasploit reportó la correcta preparación y envío de los paquetes de explotación, completando la sobrescritura (ETERNALBLUE overwrite

completed successfully) y la transferencia de la stager. Finalmente se abrió la Meterpreter session 1 entre 10.10.1.13:4444 → 192.168.17.44:49330 (timestamp: 2025-11-05T19:27:43 -0500). Esta evidencia confirma la posibilidad de ejecución remota de código (RCE) en el sistema objetivo en el entorno controlado de laboratorio.

Figura 15

Prueba de Alto Privilegio

Nota. Verificación de especificaciones de sistema comprometido.

Tras la explotación controlada, se consiguió una sesión Meterpreter con privilegios NT AUTHORITY\SYSTEM en el host PC202006 (192.168.17.44). La sesión confirma ejecución remota de código con privilegios de sistema en la VM clonada, lo que permite realizar la recolección forense controlada y las acciones de pivoting definidas en la PoC.

Para el esenario del analisis del puerto 80 en el sigiente banner informa que es HFS 2.3 un servidor web muy especifico, el título HTML de la página web es simplemente: HFS /, lo que indica que está corriendo la interfaz por defecto.

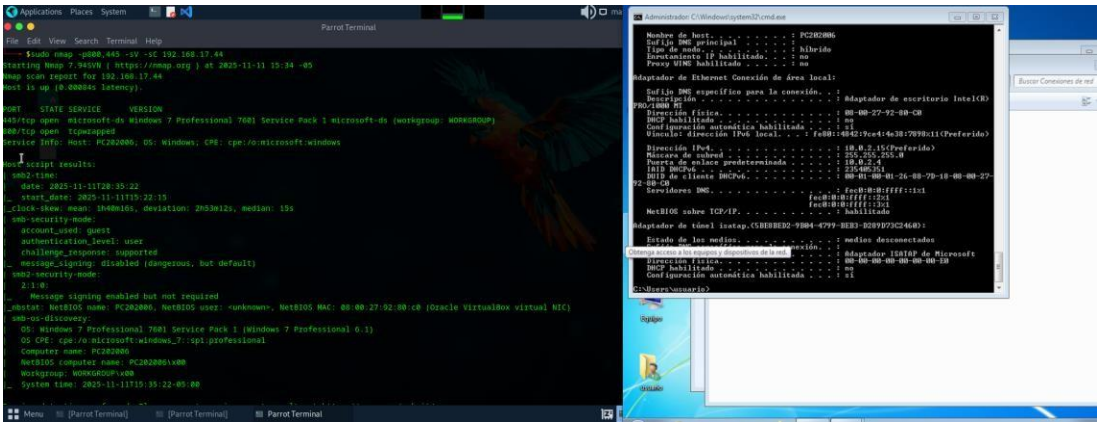
En la fase inicial del reconocimiento, se empleó el escáner de red Nmap con los parámetros -Pn -sV -sC para omitir la detección de host y ejecutar scripts de detección de servicios y versiones en el host 192.168.17.44. Los resultados mostraron que el puerto 80/tcp se

encuentra abierto, ejecutando HttpFileServer 2.3 (HFS), una versión conocida por tener vulnerabilidades de ejecución remota de código (RCE), asociada a CVE-2014-6287.

Posteriormente, se detectó también el puerto 445/tcp abierto, correspondiente al servicio Microsoft-DS (SMB). El script de detección SMB reveló que el sistema remoto es Windows 7 Professional SP1 x64, sin requerir autenticación previa (autenticación guest habilitada), y con SMB signing deshabilitado, lo cual lo hace vulnerable a ataques como SMB relay o ejecución remota vía psexec.

Figura 16

Análisis con Nmap



Nota. Escaneo con la herramienta nmap.

En el lateral derecho de la imagen se muestra la interfaz del sistema objetivo, confirmando visualmente que se trata de un sistema Windows 7 con configuración de red activa y dirección IP 10.0.2.15, lo cual coincide con la información descubierta a través de Nmap. Esta validación visual permite corroborar que el reconocimiento inicial fue exitoso y que el host presenta vulnerabilidades potencialmente explotables.

En el puerto 80/tcp del host objetivo 192.168.17.44, se detectó el servicio HttpFileServer (HFS) v2.3, una herramienta de compartición de archivos vía web. Esta versión específica es

vulnerable a una condición de ejecución remota de comandos (RCE) no autenticada debido a un fallo en el análisis de peticiones HTTP, que permite al atacante inyectar comandos arbitrarios en la URL del servidor .

Figura 17

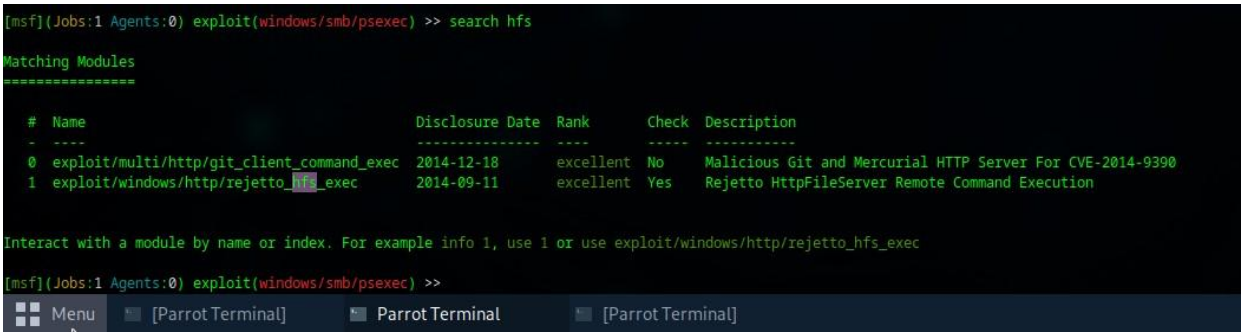
Revisión de Versión de Servicio

Nota. Escaneo especifico con la herramienta nmap.

En esta imagen se muestra el uso del comando search hfs dentro del framework de Metasploit para identificar módulos relacionados con vulnerabilidades en el servicio HTTP File Server (HFS). Como resultado, se encontró el módulo exploit/windows/http/rejetto_hfs_exec, el cual explota una vulnerabilidad de ejecución remota de comandos (RCE) en versiones vulnerables de HFS (HTTP File Server), clasificada con un nivel de fiabilidad *Excellent*. Esta vulnerabilidad permite ejecutar comandos arbitrarios en el sistema objetivo a través de peticiones HTTP especialmente diseñadas.

Figura 18

Búsqueda de Exploit

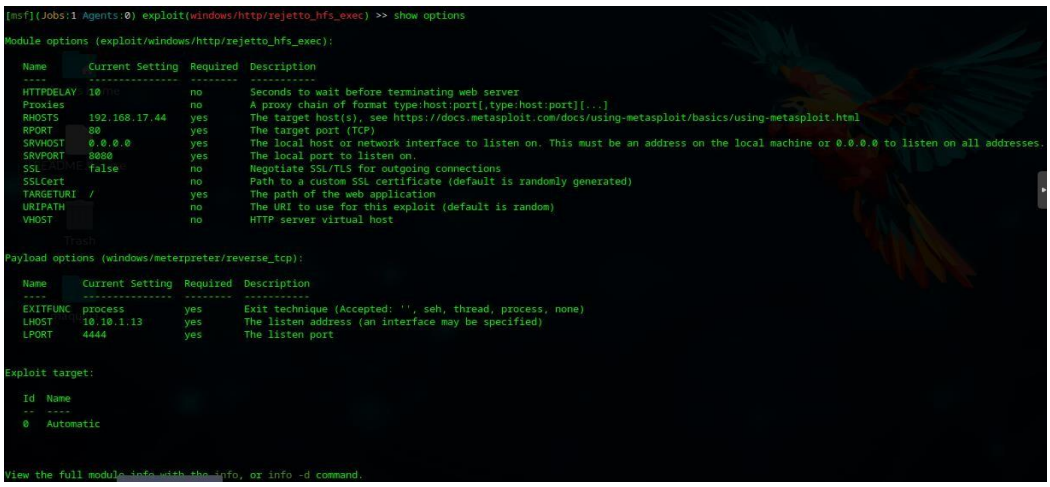


Nota. Búsqueda de exploit de sistema HFS.

La explotación exitosa de esta vulnerabilidad permite la ejecución de comandos directamente en el sistema operativo, en el contexto del usuario con el que se está ejecutando el servidor. En este laboratorio, se utilizó esta falla para obtener una sesión Meterpreter como puerta de entrada inicial al sistema.

Figura 19

Configuración de Exploit

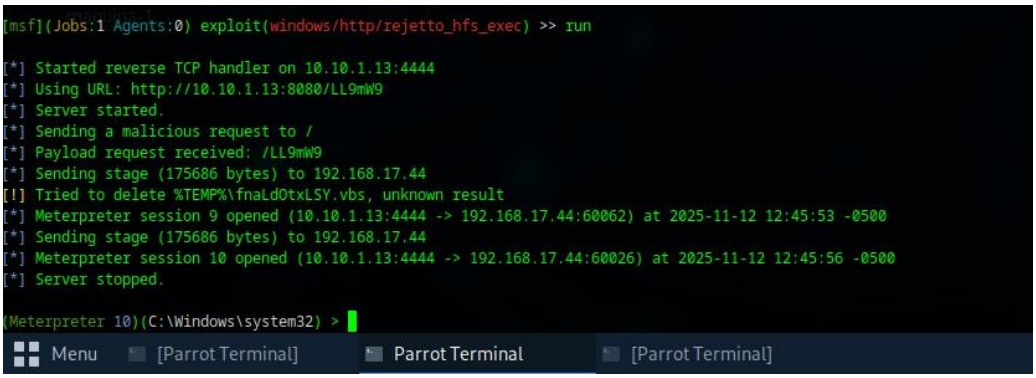


Nota. Configuración establecida para el exploit HFS.

Se utilizó el módulo público de Metasploit exploit/windows/http/rejetto_hfs_exec, el cual automatiza la explotación de esta vulnerabilidad.

Figura 20

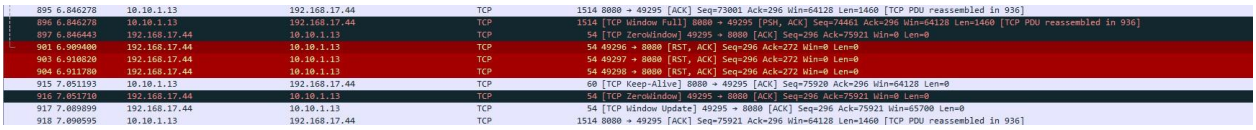
Ejecución de Exploit



Nota. Ejecución de exploit y resultado.

Figura 21

Lectura Wireshark



Nota. Captura de tráfico del proceso del exploit.

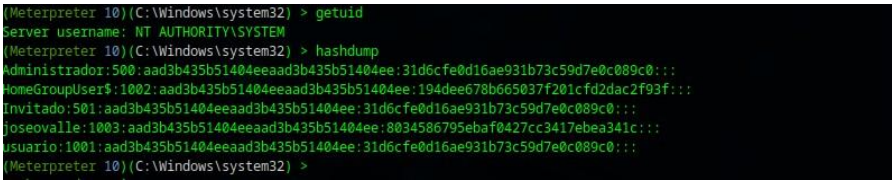
La captura de tráfico evidencia múltiples intentos de conexión TCP entre el equipo atacante (10.10.1.13) y el servicio HTTP de la Máquina-1 en el puerto 8080 (192.168.17.44). En todos los casos, el servidor responde con paquetes *RST, ACK*, lo que indica que la aplicación remota cierra las conexiones de manera abrupta. Este patrón es característico cuando un servicio se encuentra caído, inestable o ha sido interrumpido por la explotación de una vulnerabilidad. En este contexto, los resets sugieren que el servicio Rejetto HFS dejó de responder como

consecuencia del ataque, impidiendo la creación de una sesión estable y confirmando el impacto directo del exploit sobre el proceso objetivo.

Se establece una sesión Meterpreter en el host A, demostrando el compromiso exitoso del host sin requerir autenticación previa.

Figura 22

Hashes de Contraseñas



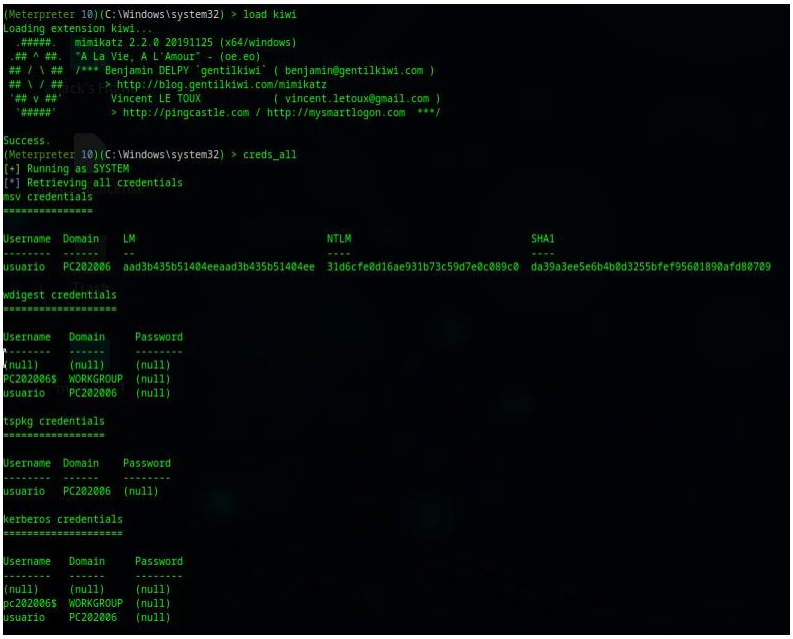
Nota. En esta imagen se observa que, tras la explotación exitosa del servicio vulnerable en Host-A, se obtuvo una sesión Meterpreter con privilegios de NT AUTHORITY\SYSTEM, el nivel más alto en sistemas Windows (getuid).

Posteriormente, se ejecutó el comando hashdump, el cual extrae los hashes de las contraseñas almacenadas localmente en el sistema comprometido. En el resultado se muestran los hashes NTLM de varias cuentas de usuario, incluyendo Administrador, usuario1, Invitado, HomeGroupUsers$, y joseovalle, los cuales podrían ser crackeados posteriormente para suplantación de identidad o movimiento lateral dentro de la red.

En esta captura se muestra el uso de la extensión kiwi en una sesión Meterpreter sobre Host-A, que permite ejecutar funcionalidades del conocido toolset Mimikatz desde Metasploit. Se ejecutó el comando creds_all, el cual recupera todas las credenciales almacenadas en memoria. Entre los datos extraídos se encuentra el hash NTLM del usuario usuario, junto con sus representaciones en LM y SHA1.

Figura 23

Verificación de Credenciales con Kiwi



Nota. En esta captura se muestra el uso de la extensión kiwi en una sesión Meterpreter sobre Host-A, que permite ejecutar funcionalidades del conocido toolset Mimikatz desde Metasploit.

Se ejecutó el comando creds_all, el cual recupera todas las credenciales almacenadas en memoria. Entre los datos extraídos se encuentra el hash NTLM del usuario usuario, junto con sus representaciones en LM y SHA1.

Fase de Post Explotación

Durante la fase de post-explotación, se utilizó el comando sysinfo para recolectar información del sistema operativo, confirmando que se trata de un sistema Windows 7 Service Pack 1 de 64 bits, perteneciente al grupo de trabajo WORKGROUP, y con un usuario actualmente conectado. Posteriormente, mediante el comando shell, se accedió a una línea de comandos tradicional de Windows desde donde se ejecutó el comando net user. Esta herramienta nativa de Windows permite listar todas las cuentas de usuario locales registradas en el sistema.

El resultado evidenció la existencia de las siguientes cuentas: Administrador, Invitado, usuario, joseovalle.

Figura 24

Shell con Meterpreter

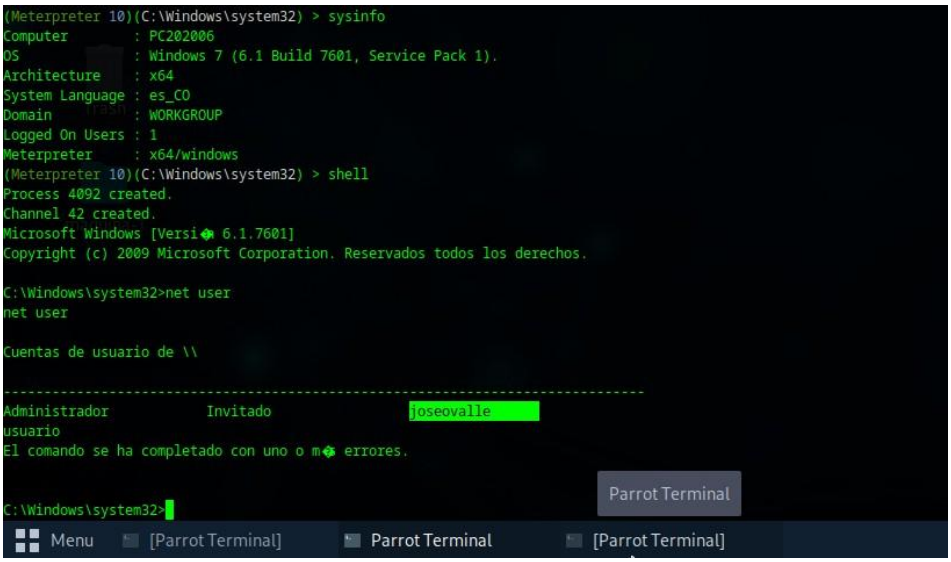
Nota. Proceso de persistencia.

La cuenta joseovalle fue creada previamente durante una etapa de persistencia, como parte del proceso de explotación y movimiento lateral dentro del entorno de red. Su aparición en la lista confirma que la operación fue exitosa y que la cuenta fue añadida correctamente al sistema objetivo.

Esta verificación respalda el éxito de la creación de usuarios y demuestra el control completo del atacante sobre el sistema comprometido.

Figura 25

Verificación de Usuarios

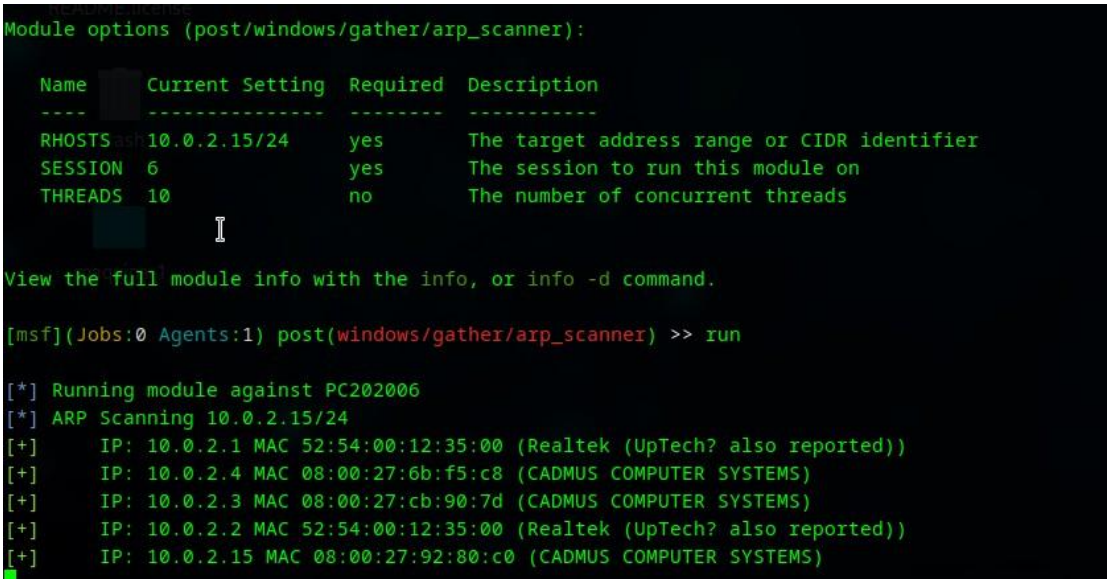


Nota. Escaneo de equipos de red local.

Posteriormente, se ejecutó el módulo post/windows/gather/arp_scanner desde Metasploit con el fin de identificar otros dispositivos conectados dentro de la misma subred local. Este módulo permite aprovechar la visibilidad de red del sistema comprometido para realizar un escaneo ARP y detectar direcciones IP activas junto con sus respectivas direcciones MAC.

Figura 26

Scaner arp



Nota. Resultante de escaneo de red local.

El escaneo arrojó múltiples resultados, identificando varios dispositivos activos en la red con sus direcciones como se muestra a continuación:

- 10.0.2.4 – MAC: 08:00:27:6B:F5:C8 (CADMUS COMPUTER SYSTEMS)
- 10.0.2.3 – MAC: 08:00:27:CB:90:7D (CADMUS COMPUTER SYSTEMS)
- 10.0.2.2 – MAC: 52:54:00:12:35:00 (Realtek – UpTech)
- 10.0.2.15 – MAC: 08:00:27:92:80:C0 (CADMUS COMPUTER SYSTEMS)

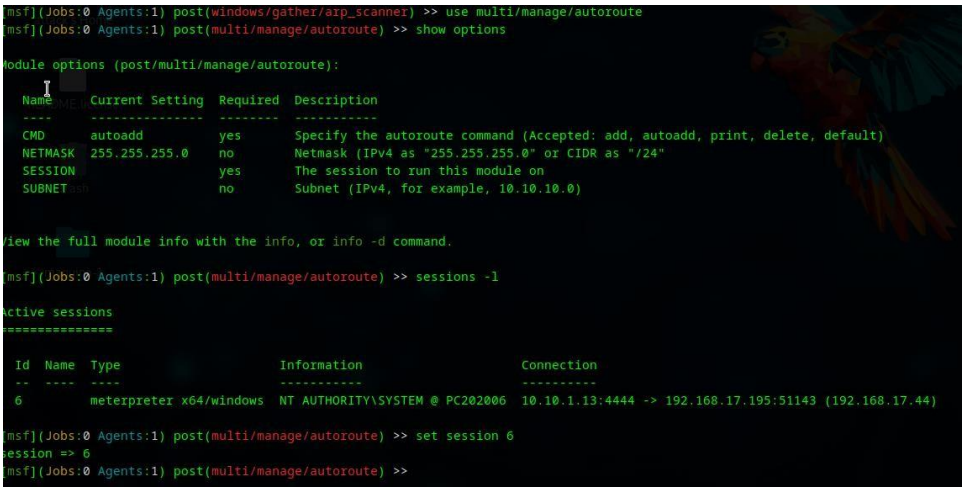
Esta información es fundamental para realizar técnicas de movimiento lateral, ya que permite identificar posibles objetivos accesibles desde el host comprometido, así como reconocer fabricantes o sistemas operativos a partir de las direcciones MAC. El escaneo demuestra que el atacante tiene visibilidad dentro de la red y puede interactuar con otros dispositivos conectados.

Se utilizó el módulo post/multi/manage/autoroute de Metasploit para establecer rutas que permitan pivotar hacia otros objetivos de la red interna a través del host comprometido.

El módulo autoroute configura reglas de enrutamiento internas dentro del framework de Metasploit, permitiendo redirigir tráfico desde la máquina atacante (Parrot) hacia subredes alcanzables únicamente por el host comprometido (Host-A).

Figura 27

Creación de Rutas Automáticas

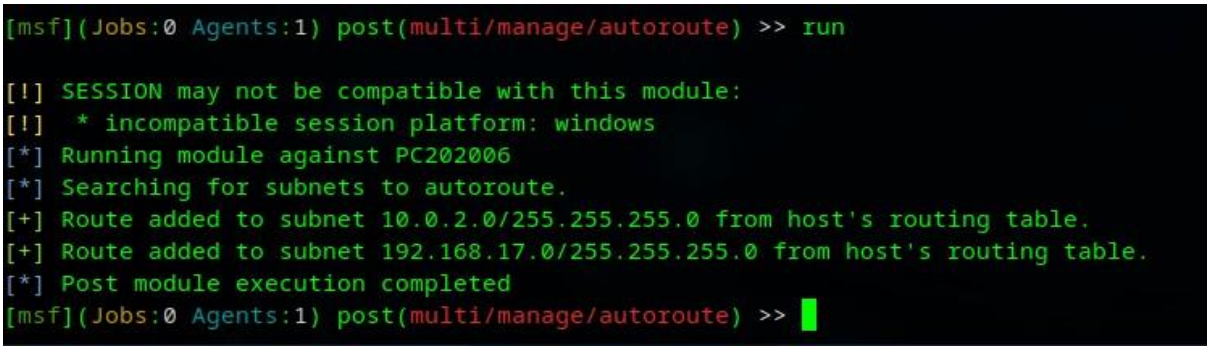


Nota. configuración de módulo de autoroute.

Esta técnica es fundamental en escenarios donde la red objetivo está segmentada y no es accesible directamente desde la máquina atacante.

Figura 28

Ejecución Rutas

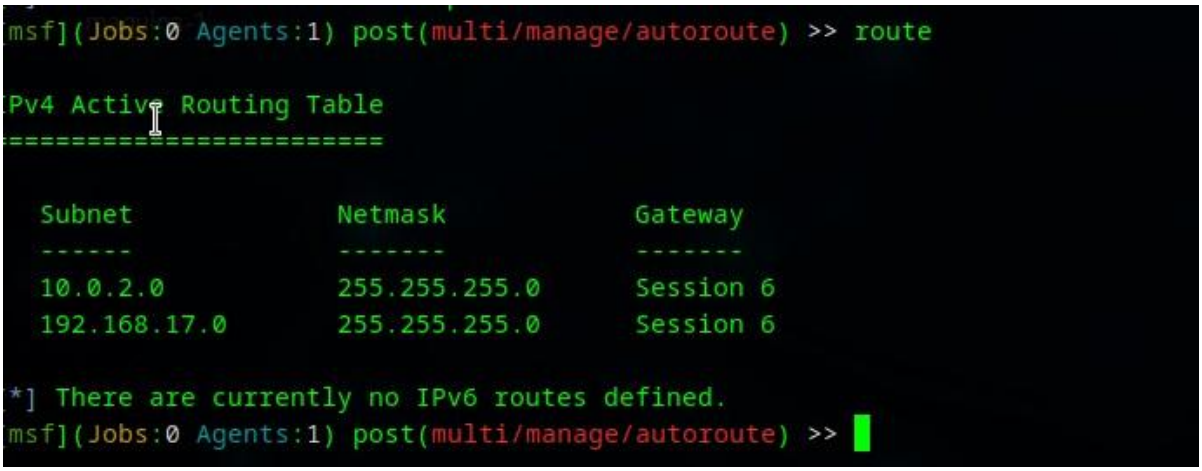


Nota. Confirmación y estado de aplicación de modulo autoroute.

Aunque la plataforma del sistema remoto (Windows) no es totalmente compatible con este módulo (como lo indica el mensaje de advertencia incompatible session platform: windows).

Figura 29

Verificación Rutas



Nota. Confirmación de tabla de rutas activa.

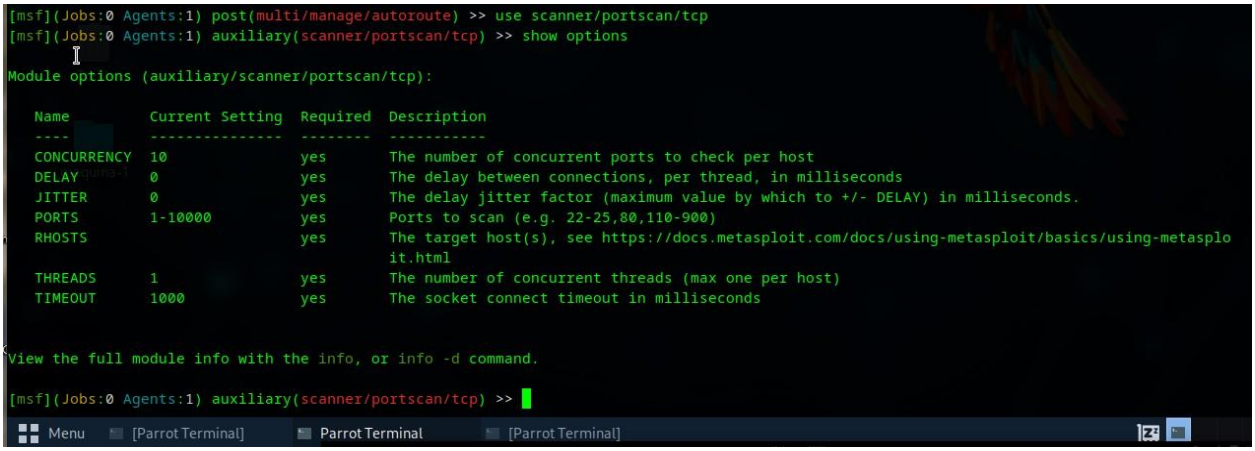
La ejecución fue exitosa y se añadieron dos rutas de red a la tabla de rutas del entorno de Metasploit:

- 10.0.2.0/24: red interna donde se encuentra el Host-B.
- 192.168.17.0/24: red externa por donde se conecta el atacante (Parrot OS).

Aquí se utilizó el módulo auxiliar auxiliary/scanner/portscan/tcp de Metasploit para realizar un escaneo de puertos TCP sobre el Host-B a través de la red interna previamente descubierta.

Figura 30

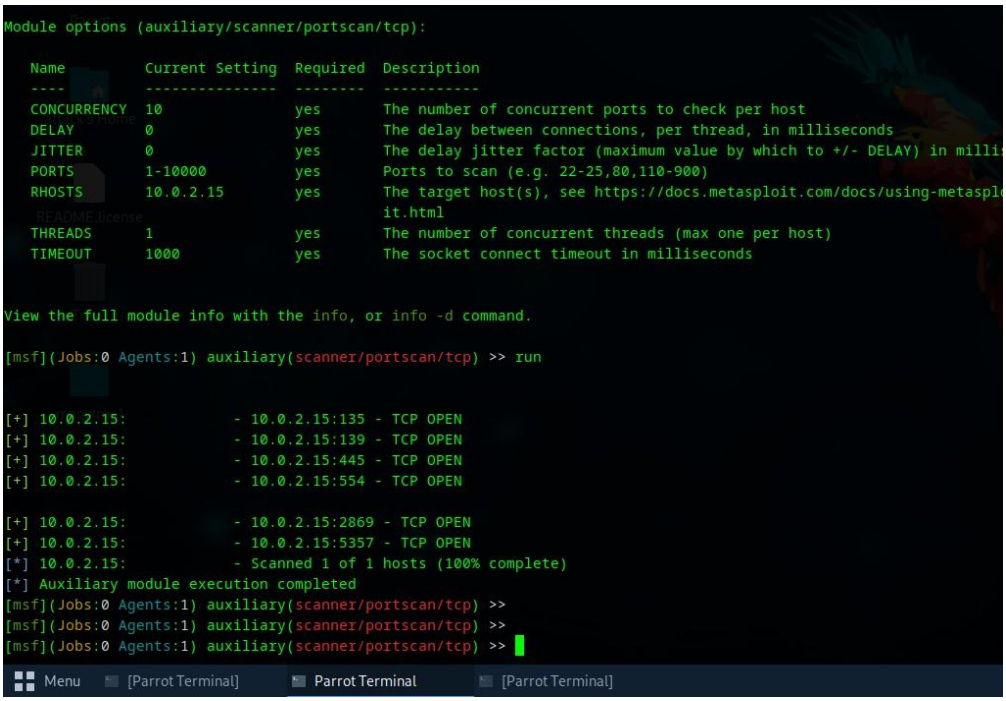
Scanner de Puertos



Nota: Configuración scanner de puertos, se muestra la configuración previa del escáner. Este módulo permite identificar los puertos TCP abiertos en el sistema destino.

Figura 31

Resultado de Portscan



Nota: Resultado de proceso de portscan. Detectando vecinos.

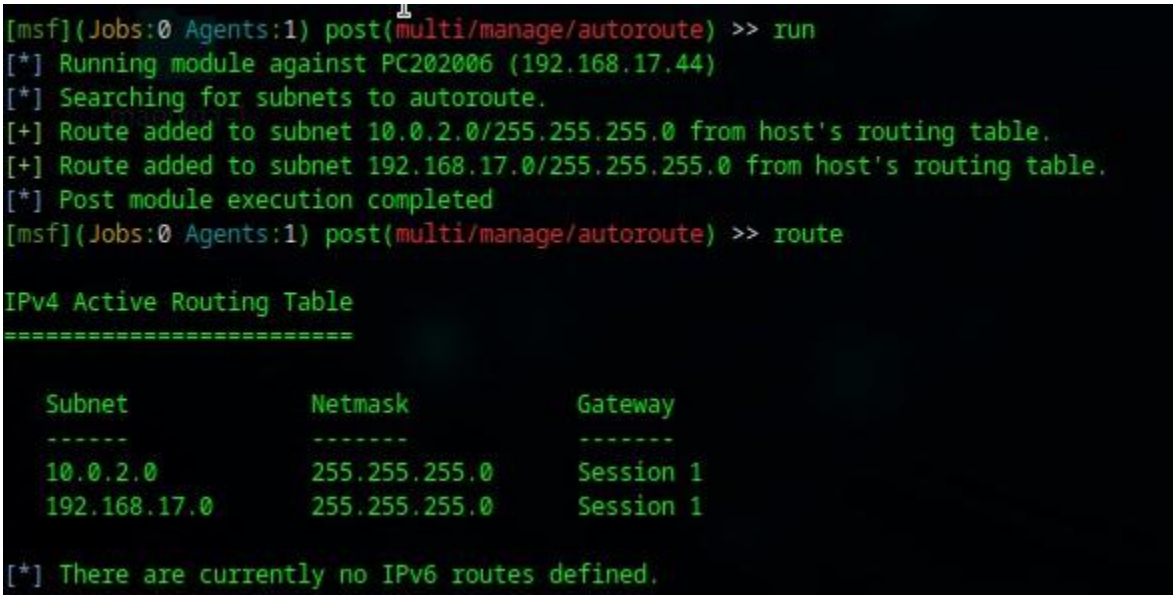
El módulo auxiliary/scanner/portscan/tcp desde Metasploit Framework, apuntando hacia el Host-B (10.0.2.15) tras establecer pivoting mediante el Host-A comprometido. Se utilizó el rango de puertos del 1 al 10000, y se identificaron los siguientes puertos abiertos en el sistema objetivo:

- 135/tcp – Microsoft RPC
- 139/tcp – NetBIOS Session Service
- 445/tcp – Microsoft-DS (SMB, usado para compartir archivos)
- 554/tcp – RTSP (Real Time Streaming Protocol)
- 2869/tcp – Microsoft SSDP (UPnP)
- 5357/tcp – WSDAPI (Web Services on Devices)

Estos servicios abiertos son indicativos de una máquina con sistema operativo Windows, y el puerto 445, en particular, representa una superficie de ataque crítica para módulos de administración remota como psexec o ataques SMB relay. Este escaneo confirma que el pivoting desde Host-A está funcionando correctamente, ya que se logró acceso y enumeración de puertos en una máquina (Host-B) no accesible directamente desde la red del atacante.

Figura 32

Configuración Automática de Rutas Mediante Autoroute en Metasploit



Nota. Confirmación de rutas asociadas a la sesión de meterpreter.

En la figura se observa la ejecución del módulo post/multi/manage/autoroute dentro de una sesión Meterpreter comprometida en el Host-A. Este módulo permite agregar rutas automáticamente a las subredes accesibles desde el equipo comprometido, habilitando el pivoting hacia otras máquinas de la red interna.

El comando run ejecuta el módulo, que identifica dos redes distintas disponibles desde el Host-A:

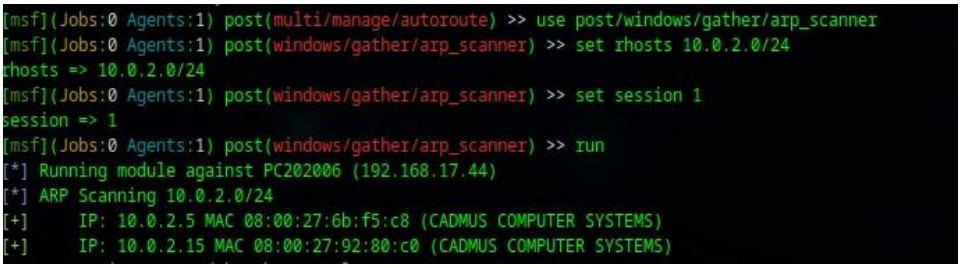
- 10.0.2.0/24, red interna donde se encuentra Host-B.
- 192.168.17.0/24, red donde se encuentra Host-A expuesto hacia Parrot OS.

Ambas rutas se agregan al routing table de Metasploit, utilizando la sesión activa (Session 1) como puerta de enlace. Finalmente, con el comando route, se verifica la tabla de ruteo activa, confirmando que el pivoting está correctamente establecido. Esta configuración es

esencial para permitir que Metasploit envíe tráfico hacia Host-B a través de Host-A, incluso sin acceso directo desde la máquina atacante.

Figura 33

Evidencia – ARP Scan desde Host A hacia la red 10.0.2.0/24



Nota. Se muestra la ejecución del módulo post/windows/gather/arp_scanner a través de la sesión 1 de Meterpreter obtenida en el Host-A.

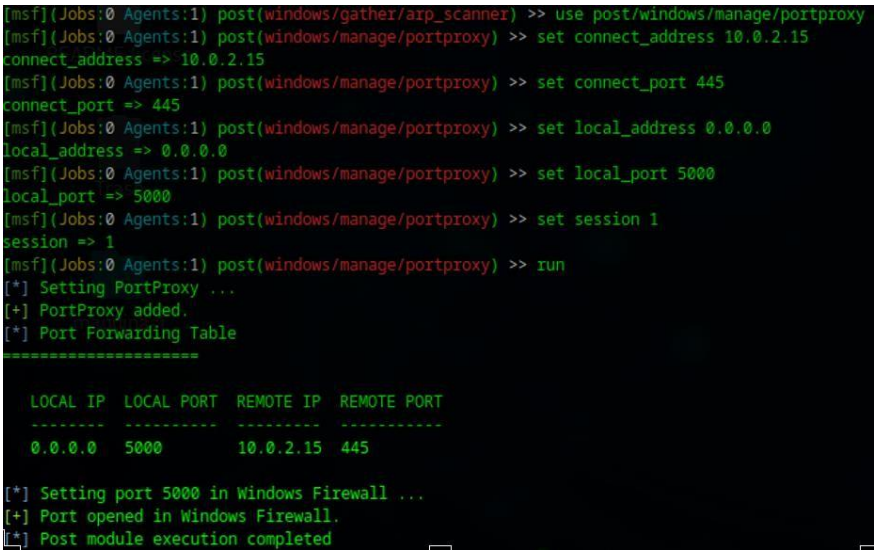
El módulo permite identificar activos dentro de la red 10.0.2.0/24 enviando solicitudes ARP desde la máquina comprometida, lo cual habilita el reconocimiento pasivo dentro del segmento de red interno que no es accesible directamente desde el equipo atacante.

El escaneo detecta dos direcciones IP activas (10.0.2.5 y 10.0.2.15), junto con sus respectivas direcciones MAC, confirmando la presencia del Host-B en la red pivotada y validando que la comunicación lateral a través del Host-A se encuentra correctamente establecida.

El framework Metasploit agrega rutas internas automáticamente y confirma que ahora todo el tráfico hacia las subredes internas será enviado a través de la sesión Meterpreter, permitiendo acceder a equipos que no son visibles directamente desde Parrot OS. Esto habilita el pivoting necesario para interactuar con Host-B (10.0.2.15) a través de Host-A (10.0.2.5)

Figura 34

Autoroute + Tabla de Rutas



Nota. Configuración de pivoting.

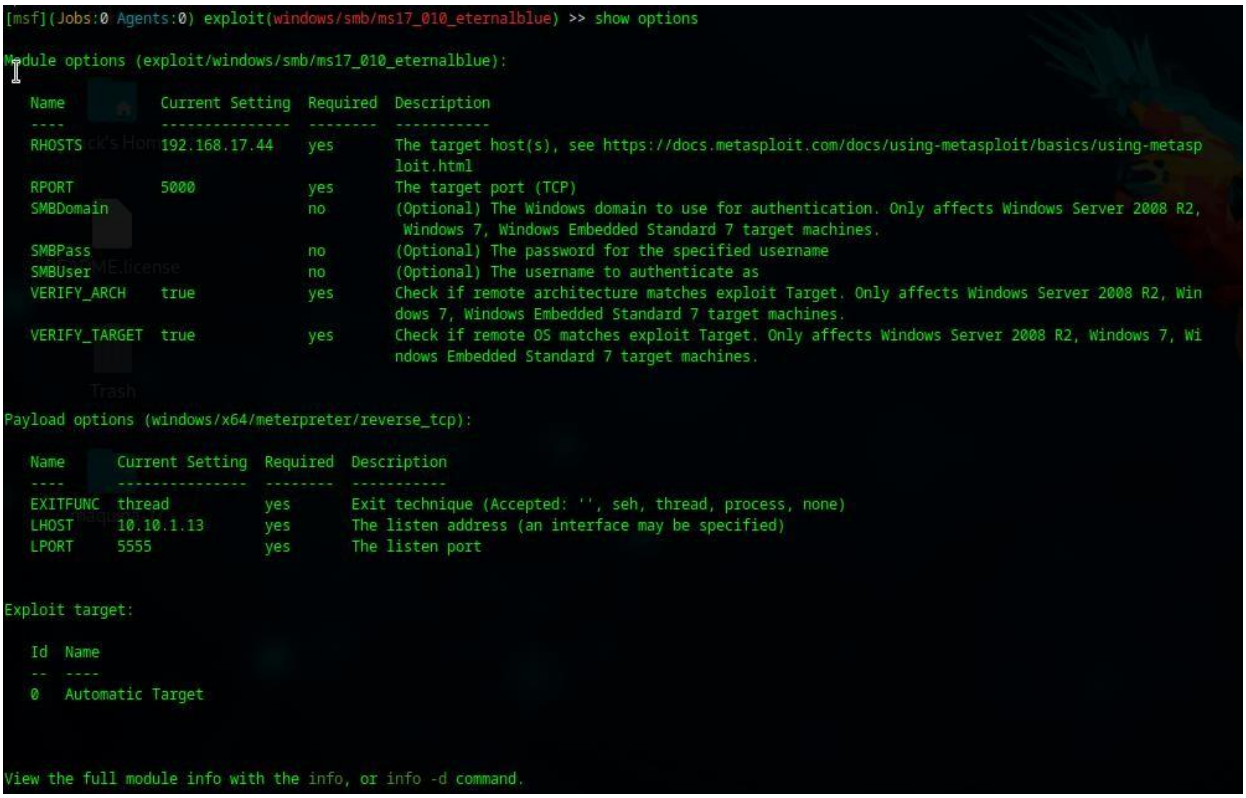
En esta fase se configuró un mecanismo de pivoting desde el equipo comprometido Host-A, permitiendo redirigir tráfico hacia el Host-B a través del puerto SMB (445). Para ello, se utilizó el módulo post/windows/manage/portproxy de Metasploit, el cual habilita reglas de reenvío de puertos en el sistema comprometido utilizando la funcionalidad interna netsh interface portproxy de Windows.

- En la evidencia presentada se observa la configuración del reenvío:
- Dirección remota: 10.0.2.15 (Host-B)
- Puerto remoto: 445 (SMB)
- Puerto local expuesto: 5000
- Dirección local: 0.0.0.0, permitiendo escuchar en todas las interfaces del Host-A
- Sesión utilizada: Sesión 1 (Meterpreter en Host-A)

Tras ejecutar el módulo, se muestra la tabla de Port Forwarding, donde se confirma que el puerto 5000/TCP del Host-A queda vinculado al puerto 445/TCP del Host-B, permitiendo que todo acceso SMB posterior desde Parrot OS hacia 127.0.0.1:5000 sea túnelado automáticamente hacia Host-B. Esta configuración establece el canal necesario para intentar enumeración de usuarios, conexiones SMB, o ejecución remota de comandos utilizando Metasploit, todo a través del túnel pivotado.

Figura 35

Configuración del Exploit MS17-010



Nota. En la imagen se observa la carga del módulo exploit/windows/smb/ms17_010_eternalblue y la revisión de sus parámetros mediante el comando show options.

El módulo MS17-010 EternalBlue dentro del framework Metasploit, utilizando el túnel creado previamente mediante pivoting desde el Host A hacia el Host B. Para dirigir el ataque

hacia el equipo víctima a través del puerto reenviado (5000), se estableció la dirección del objetivo (RHOSTS) como la IP accesible por el pivot, y se configuró RPORT en 5000, correspondiente al puerto local que redirige el tráfico hacia el servicio SMB del Host B (puerto 445). Además, se activaron los parámetros VERIFY_ARCH y VERIFY_TARGET para confirmar automáticamente que el sistema destino coincide con la arquitectura requerida por el exploit.

En cuanto al payload, se seleccionó windows/x64/meterpreter/reverse_tcp, definiendo como LHOST la dirección del atacante (10.10.1.13) y como LPORT el puerto de escucha 5555. Esta configuración permite que, si el exploit es exitoso, la conexión inversa del Host B regrese de manera controlada al atacante a través del canal pivot. Con estos valores establecidos, el entorno queda preparado para ejecutar el ataque EternalBlue utilizando el enrutamiento interno obtenido desde el acceso comprometido al Host A.

Figura 36

Ejecución del Exploit MS17-010

Nota. Ejecución del módulo exploit/windows/smb/ms17_010_eternalblue a través del puerto redirigido 5000 hacia el Host-B.

Fase de Reporte y Remediación

El escaneo inicial confirma que el sistema remoto es potencialmente vulnerable a MS17-010, por lo que Metasploit inicia la fase de explotación enviando la serie de paquetes SMB malformados utilizados por EternalBlue. Durante este proceso, el módulo realiza asignaciones de memoria, envía fragmentos del exploit y ejecuta la técnica de SMB groom para provocar la condición de corrupción de memoria requerida.

Sin embargo, en el punto crítico de la explotación aparece el mensaje “FAIL”, indicando que la creación del race condition o la colocación del groom no logró la sincronización necesaria. Este fallo es común cuando el objetivo tiene parches parciales, configuraciones SMB específicas, diferencias en la memoria, o cuando la comunicación atraviesa redireccionamientos como portproxy/pivoting, los cuales afectan la temporización precisa que EternalBlue requiere para funcionar. A pesar de este fallo puntual, el módulo continúa intentando completar el proceso, aunque normalmente no consigue establecer sesión debido a dicha desincronización.

Respuesta y Contención ante Incidentes de Seguridad

Lo primero que un analista del Blue Team debe indagar ante un ataque en tiempo real es el estado actual de la máquina comprometida y la extensión del movimiento lateral dentro de la red. En un caso como el de SecureNova Labs, donde el atacante ingresó a través de un servicio vulnerable (Rejetto) y utilizó EternalBlue para pivotar desde Host A hacia Host B, la prioridad inicial es aislar el equipo afectado del resto de la red mediante medidas de contención rápida como deshabilitar temporalmente su interfaz de red o aplicar ACLs de emergencia en el firewall sin interrumpir su alimentación eléctrica para no perder evidencia.

A nivel técnico, también se revisan procesos en ejecución, conexiones activas, sesiones remotas y logs del sistema para identificar la puerta de entrada, el payload ejecutado y si existe

persistencia. Este primer paso se fundamenta en las guías del CCN-CERT (2018), que recomiendan una acción inmediata de contención, seguida de la recolección de evidencia para determinar el alcance del incidente antes de ejecutar cualquier acción correctiva definitiva.

Teniendo en cuenta que el ataque del Red Team se basó en un servicio vulnerable (Rejjetto HFS) y en la explotación del SMBv1 mediante EternalBlue, las medidas de hardening deben orientarse a cerrar completamente esas brechas. En primer lugar, la organización debe desinstalar cualquier software no autorizado o que no reciba actualizaciones, así como aplicar parches acumulativos de seguridad del sistema operativo.

También es necesario desactivar SMBv1, reforzar la configuración de firewall en Windows, implementar reglas restrictivas para puertos como 445/139 y habilitar el filtrado del tráfico en el firewall perimetral. Adicionalmente, se deben endurecer los permisos del sistema, activar LSA Protección, aplicar CIS Benchmarks para Windows y establecer monitoreo continuo con un SIEM para detectar anomalías en la actividad de red, tal como recomiendan CIS (2020) y Zambrano Hernández et al. (2024) en sus lineamientos de gestión de incidentes.

Un equipo Blue Team y un equipo de Respuesta a Incidentes (CSIRT Académico UNAD, 2024) comparten objetivos, pero cumplen funciones diferentes dentro del ciclo de defensa. El Blue Team mantiene la seguridad de forma preventiva y permanente: endurece sistemas, configura controles, monitorea eventos, revisa logs, detecta patrones sospechosos y disminuye la superficie de ataque de la infraestructura.

En contraste, un equipo de Respuesta a Incidentes actúa cuando el ataque ya está ocurriendo o se ha confirmado, siguiendo un procedimiento estructurado de contención, erradicación, análisis de causa raíz y recuperación. En conclusión, el Blue Team construye seguridad continua; el IR Team interviene cuando todo ha salido mal.

Si dentro de las funciones del Blue Team se indica trabajar con CIS, el uso principal sería la aplicación de CIS Benchmarks y CIS Controls para fortalecer la configuración de los sistemas y reducir el riesgo de ataques futuros.

Los Benchmarks permiten endurecer sistemas operativos, servidores, navegadores, bases de datos y servicios siguiendo parámetros reconocidos internacionalmente, mientras que los CIS Controls ayudan a priorizar la implementación de controles críticos como inventario de activos, gestión de vulnerabilidades, configuración segura y monitoreo constante. En un escenario como el del laboratorio, el uso de CIS habría evitado que existiera un servicio sin parches vulnerables y habría reducido la probabilidad de explotación del SMBv1.

Un SIEM (Security Information and Event Management) es una plataforma que centraliza, correlaciona y analiza eventos provenientes de múltiples sistemas con el fin de detectar actividades maliciosas en tiempo real. Sus funciones principales incluyen la ingestión de logs, correlación automática, detección de patrones, almacenamiento seguro de evidencia, dashboards de monitoreo y la generación de alertas basadas en reglas de comportamiento. Según Moreno (2015), un SIEM permite identificar ataques complejos que no serían visibles revisando un solo log, y es esencial para evidenciar movimientos laterales como el que ocurrió en el laboratorio: comunicaciones inusuales entre A y B, escaneos de puertos, explotación SMB y creación de cuentas sospechosas.

Entre las herramientas de contención (distintas a las de detección) se pueden considerar varias opciones tanto hardware como software, todas compatibles con entornos sin presupuesto adicional. Una herramienta clave es pfSense, que permite aplicar reglas de firewall estrictas, bloquear rangos de IP, aislar segmentos de red y aplicar listas de control de acceso como contención inmediata.

Otra herramienta útil es OSSEC/Wazuh, que incluye capacidades de respuesta activa (active response) para bloquear direcciones maliciosas, detener procesos y modificar reglas del sistema cuando detecta comportamientos críticos. Como tercera, a nivel de sistema operativo, Windows ofrece Applocker y Políticas de Restricción de Software, que permiten evitar la ejecución de binarios no autorizados, bloquear scripts no firmados y reducir la superficie de ataque. Estas herramientas se enfocan en evitar que el atacante continúe avanzando después del compromiso inicial.

El análisis realizado permitió comprender de forma integral cómo un ataque real puede evolucionar desde la explotación inicial de una vulnerabilidad hasta el movimiento lateral y la escalada de impacto dentro de la infraestructura, como ocurrió en el laboratorio con Rejetto y EternalBlue. La revisión técnica evidenció la importancia de contar con controles preventivos sólidos (hardening, gestión de vulnerabilidades, segmentación y monitoreo) que reduzcan significativamente la superficie de ataque antes de que un actor malicioso logre comprometer el sistema.

Asimismo, el ejercicio confirmó que la contención temprana mediante herramientas abiertas, la correlación de eventos y la aplicación de marcos de referencia como los CIS Benchmarks y las guías del CCN-CERT resultan esenciales para detener la progresión del atacante y preservar la integridad operativa de la organización. En conjunto, este estudio refuerza que el rol del Blue Team no solo se limita a reaccionar ante incidentes, sino a construir una postura defensiva continua que garantice resiliencia, visibilidad y capacidad de respuesta ante amenazas avanzadas.

Evidencia 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 de informe final: https://youtu.be/9VX6Dmj1jf0

Conclusiones

El proceso desarrollado a lo largo de las cuatro etapas permitió comprender la ciberseguridad desde una perspectiva integral que abarca los componentes jurídicos, éticos, ofensivos y defensivos que intervienen en un ejercicio profesional bien estructurado. La fase inicial reforzó que cualquier actividad de pentesting requiere un entendimiento preciso del marco normativo colombiano, ya que la correcta interpretación de la Ley 1273 de 2009 y la Ley 1581 de 2012 define los límites dentro de los cuales un profesional puede operar sin transgredir derechos o incurrir en conductas punibles. Esta base jurídica se convierte en un eje orientador que legitima la práctica técnica y establece parámetros claros de responsabilidad.

El análisis de los acuerdos de confidencialidad de SecureNova Labs evidenció cómo la dimensión ética complementa la dimensión legal. La revisión de las cláusulas permitió identificar riesgos que podrían comprometer la integridad profesional, lo que resalta la necesidad de examinar de forma crítica cualquier documento que condicione el manejo de información sensible. El estudio permitió reconocer que la labor del especialista en seguridad no se limita al dominio técnico: también implica decisiones éticas fundamentadas en principios de transparencia, legalidad y responsabilidad social.

La práctica ofensiva desarrollada en la tercera etapa ofreció una comprensión detallada de cómo un atacante real podría avanzar dentro de una infraestructura vulnerable. La explotación del servicio Rejetto HFS, la escalada de privilegios y las técnicas de movimiento lateral mostraron que una configuración débil o desactualizada puede abrir la puerta a compromisos significativos dentro de una red corporativa. El ejercicio validó la importancia del reconocimiento, la enumeración y el análisis de servicios como etapas críticas para anticipar y modelar posibles rutas de ataque.

El trabajo defensivo permitió abordar la otra cara del proceso: la visibilidad, la respuesta y el fortalecimiento de la infraestructura frente a amenazas activas. El estudio de eventos del sistema, la identificación de anomalías, la implementación de medidas de hardening y la aplicación de marcos de referencia como CIS Benchmarks demostraron que la defensa efectiva depende tanto de controles preventivos como de mecanismos de detección y contención oportunos. El análisis también dejó en evidencia que la madurez defensiva de una organización está directamente relacionada con su capacidad para monitorear de forma continua, gestionar incidentes y reducir la superficie de ataque antes de que un adversario la explote.

Las cuatro etapas permitieron integrar conocimientos jurídicos, técnicos y operativos bajo una visión coherente del ciclo de seguridad. El proyecto amplió la comprensión de cómo interactúan los procesos ofensivos y defensivos, cómo se construye una postura de seguridad robusta y por qué la gestión ética y normativa es esencial para cualquier ejercicio de ciberseguridad. Más que una serie de prácticas aisladas, el proyecto mostró que la seguridad es un proceso dinámico, basado en el aprendizaje constante, la mejora continua y la capacidad de anticiparse y responder a escenarios complejos con criterios técnicos sólidos y responsabilidad profesional.

Recomendaciones

A partir del análisis técnico y del ciclo completo del ejercicio Red Team & Blue Team, se recomienda implementar un proceso de endurecimiento integral que contemple la eliminación de servicios innecesarios o vulnerables, la desactivación de protocolos obsoletos como SMBv1 y la aplicación sistemática de los CIS Benchmarks para asegurar configuraciones basadas en estándares reconocidos internacionalmente.

Asimismo, es indispensable fortalecer la segmentación de la red mediante VLANs y controles perimetrales que limiten el alcance de un atacante en caso de compromiso inicial. Para el Red Team, se sugiere mantener una trazabilidad completa de cada actividad ofensiva, utilizar metodologías estructuradas como PTES u OSSTMM y garantizar que las pruebas se realicen únicamente en entornos autorizados, respetando las implicaciones éticas y legales.

En cuanto al Blue Team, se recomienda consolidar un esquema de monitoreo continúo soportado por SIEM o herramientas abiertas como Wazuh, reforzar políticas de menor privilegio y control de ejecución mediante AppLocker o SRP, y realizar simulacros periódicos de respuesta a incidentes que permitan evaluar la madurez operativa y mejorar los tiempos de detección y contención.

Estas recomendaciones promueven una postura de seguridad orientada a la resiliencia, la prevención y la mejora continua, alineada con los marcos normativos y las mejores prácticas internacionales en ciberseguridad.

Referencias Bibliográficas

Alabdan, R. (2020). Cybersecurity penetration testing: A systematic review of post-exploitation and privilege escalation techniques. *IEEE Access, 8*, 121257–121272. https://doi.org/10.1109/ACCESS.2020.3007014

Centro Criptológico Nacional (CCN-CERT). (2018). *Guía CCN-STIC-495: Seguridad en IPv6*. https://www.ccncert.cni.es

Centro de Respuesta a Incidentes de Seguridad Informática Académico UNAD. (2024). *Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información UNADISTAS*. Universidad Nacional Abierta y a Distancia.

Common Vulnerabilities and Exposures. (2014). *CVE-2014-6287*. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

Congreso de la República de Colombia. (2000). *Ley 599 de 2000: Código Penal colombiano*. Diario Oficial No. 44.097.

Congreso de la República de Colombia. (2008). *Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales*. Diario Oficial No. 47.219.

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —la protección de la información y de los datos— y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*. Diario Oficial No. 47.223.

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587.

Congreso de la República de Colombia. (2013). *Ley 1621 de 2013: Por la cual se dictan normas en materia de inteligencia y contrainteligencia*. Diario Oficial No. 48.769.

Consejo Profesional Nacional de Ingeniería. (2005). *Código de ética profesional de los ingenieros (Ley 842 de 2003)*. Diario Oficial de la República de Colombia.

Dradis Framework. (s. f.). *Collaborative reporting platform for information security teams*. https://dradisframework.com

Exploit Database. (s. f.). *Exploit-DB*. https://www.exploit-db.com

Greenbone Networks. (s. f.). *Greenbone vulnerability management documentation*. https://docs.greenbone.net

Instituto Nacional de Ciberseguridad de España. (2019). *El pentesting: Auditando la seguridad de tus sistemas*. https://www.incibe.es

Kaur, G., Singh, M., & Kumar, R. (2023). Penetration testing methodologies for securing modern information systems: A comprehensive review. *Journal of Information Security and Applications, 73*, 103512.

MITRE. (2024). *Enterprise matrix*. https://attack.mitre.org

Nmap Project. (s. f.). *Nmap: The network mapper*. https://nmap.org

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

Oracle. (2023). *Oracle VM VirtualBox user manual*. https://www.virtualbox.org/manual

Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012*. Diario Oficial No. 48.834.

Rapid7. (2023). *Metasploit framework documentation*. https://docs.metasploit.com

Rejetto. (2014). *HttpFileServer (HFS) version 2.3*. https://www.rejetto.com/hfs

Scarfone, K., & Mell, P. (2019). *Guide to intrusion detection and prevention systems (IDPS)* (NIST Special Publication 800-94). National Institute of Standards and Technology.

SecureNova Labs. (2025). *Acuerdo de confidencialidad – Anexo 3* [Documento interno del caso de estudio].

Simões, P., Cruz, A., & Sampaio, P. (2022). OSINT techniques and tools for cybersecurity. *International Journal of Cybersecurity Intelligence and Cybercrime, 5*(2), 31–45.

Zambrano Hernández, J., Peña Hidalgo, H. J., & Cárdenas Corral, A. (2024). *Guía para la gestión y clasificación de incidentes de ciberseguridad*. Sello Editorial UNAD.

Apéndices

Apéndice A

Resultado de Herramienta Turnitin