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

Fredy Augusto Martinez Ríos

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

El presente trabajo académico está dedicado, en primer lugar, a Dios, por brindarme la fortaleza, la sabiduría y la perseverancia necesarias para culminar este proceso de formación profesional de igual manera, se dedica a mi madre, por su apoyo incondicional, sus enseñanzas y su constante motivación, las cuales han sido fundamentales a lo largo de mi vida personal y académica.

Agradecimientos

En un primer momento, agradecer a Dios por sus bendiciones para llegar hasta este momento de mi vida, ya que ha hecho realidad un sueño anhelado desde mi pregrado; al tutor del seminario especializado, Ingeniero EDUVIN TRIGOS SÁNCHEZ por su trabajo y consagración, quien, con sus conocimientos, preparación y paciencia ha permitido el logro de este proyecto académico con éxito y por último a los docentes de la Especialización en Seguridad Informática de la UNAD, quienes siempre me han exigido y motivado en este proceso de formación..

Resumen

El presente informe analiza las capacidades técnicas, tácticas y operativas de los equipos Red Team y Blue Team dentro de los procesos de seguridad informática, integrando un estudio práctico basado en el escenario de laboratorio, inicialmente, se examina el marco legal colombiano relacionado con la protección de datos personales y los delitos informáticos, destacando las implicaciones jurídicas de la normas como la Ley 1273 de 2009, la Ley 1581 de 2012 y la Ley 1712 de 2014, posteriormente, se describen de manera detallada las etapas del pentesting, incorporando herramientas especializadas empleadas en cada fase, tales como Nmap, Metasploit, OpenVAS y diversos recursos de análisis OSINT, este documento también evalúa la validez ética y legal del acuerdo presentado, identificando cláusulas que podrían constituir encubrimiento de actividades ilícitas, vulneración de deberes ciudadanos y transgresión directa de la Ley 1273, con base en ello, se discute la responsabilidad profesional según el código ético del COPNIA, desde el enfoque técnico, se desarrollan actividades de reconocimiento, explotación, post-explotación y pivoting contra el Host-A y Host-B, demostrando el impacto de vulnerabilidades críticas, particularmente la afectación del servicio Rejetto HFS 2.3, además, se analizan fallos que permitieron ejecución remota, creación de cuentas administrativas y movimientos laterales dentro de la red, también se abordan lineamientos éticos, recomendaciones de protección de la información sensible por parte de empresas de ciberseguridad, mecanismos de supervisión, respuesta institucional frente al ciberespionaje y medidas de hardening necesarias para evitar la repetición del ataque evidenciado en el laboratorio.

***Palabras clave*:** ciberespionaje, hardening, pentesting, pivoting, vulnerabilidades.

Abstract

This report analyzes the technical, tactical, and operational capabilities of the Red Team and Blue Team within cybersecurity processes, integrating a practical study based on a laboratory scenario. Initially, the Colombian legal framework related to the protection of personal data and cybercrimes is examined, highlighting the legal implications of regulations such as Law 1273 of 2009, Law 1581 of 2012, and Law 1712 of 2014. Subsequently, the stages of penetration testing are described in detail, incorporating specialized tools used in each phase, such as Nmap, Metasploit, OpenVAS, and various OSINT analysis resources. This document also evaluates the ethical and legal validity of the presented agreement, identifying clauses that could constitute concealment of illicit activities, violation of civic duties, and direct transgression of Law 1273. Based on this, professional responsibility according to the COPNIA code of ethics is discussed. From a technical perspective, reconnaissance and exploitation activities are developed. Post-exploitation and pivoting against Host-A and Host-B, demonstrating the impact of critical vulnerabilities, particularly the impact on the Rejetto HFS 2.3 service. In addition, flaws that allowed remote execution, creation of administrative accounts, and lateral movement within the network are analyzed. Ethical guidelines, recommendations for the protection of sensitive information by cybersecurity companies, monitoring mechanisms, institutional response to cyber espionage, and hardening measures necessary to prevent the repetition of the attack evidenced in the laboratory are also addressed.

Keywords**:** cyber espionage, hardening, pentesting, pivoting, vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Análisis forense digital:

Disciplina de la ciberseguridad orientada a la recolección, preservación y análisis de evidencia digital para investigar incidentes de seguridad o actividades delictivas en sistemas informáticos.

Blue Team:

Equipo responsable de la defensa de los sistemas de información de una organización, encargado de la detección, monitoreo, respuesta y mitigación de amenazas, así como de la implementación de controles de seguridad.

Ciberseguridad:

Conjunto de prácticas, procesos y tecnologías destinadas a proteger los sistemas de información frente a amenazas, vulnerabilidades y ataques que puedan comprometer la confidencialidad, integridad o disponibilidad de los datos.

Confidencialidad:

Principio de seguridad de la información que garantiza que los datos solo puedan ser accedidos por personas, procesos o sistemas autorizados.

Delitos informáticos:

Actividades tipificadas en la legislación penal que involucran el uso indebido de sistemas, redes o información digital, incluyendo acceso no autorizado, interceptación de datos, uso de software malicioso y fraude electrónico.

Explotación:

Fase del pentesting en la que se aprovecha una vulnerabilidad previamente identificada para obtener acceso, ejecutar código o manipular un sistema de manera controlada.

Hardening:

Conjunto de técnicas y configuraciones destinadas a reforzar la seguridad de sistemas, redes o aplicaciones mediante la reducción de su superficie de ataque.

Movimiento lateral (Lateral Movement):

Técnica empleada por atacantes para desplazarse dentro de una red, utilizando un sistema comprometido como punto intermedio para acceder a otros equipos.

Nmap (Network Mapper):

Herramienta de análisis de red que permite identificar hosts, puertos abiertos, servicios y posibles vulnerabilidades en un sistema.

Pentesting (Pruebas de penetración):

Proceso controlado y autorizado que evalúa la seguridad de un sistema mediante técnicas similares a las utilizadas por atacantes, con el fin de identificar y corregir vulnerabilidades.

Pivoting:

Técnica mediante la cual un atacante utiliza un equipo previamente comprometido como puente para acceder a otros sistemas que inicialmente no eran alcanzables desde el exterior.

Post-explotación:

Fase del pentesting que comprende las acciones realizadas después de obtener acceso a un sistema, como la elevación de privilegios, recolección de información y mantenimiento del control.

Red Team:

Equipo de ciberseguridad ofensiva encargado de simular ataques reales con el fin de evaluar la eficacia de las defensas de la organización y medir su resiliencia.

SIEM (Security Information and Event Management):

Solución tecnológica que centraliza, analiza y correlaciona eventos de seguridad provenientes de múltiples fuentes para detectar amenazas y facilitar la respuesta a incidentes.

Vulnerabilidad:

Debilidad presente en un sistema, aplicación o dispositivo que puede ser explotada por un atacante para comprometer sus funciones o la información que gestiona.

Introducción

El crecimiento de las tecnologías de la información y la comunicación ha transformado profundamente la forma en que las organizaciones gestionan, procesan y protegen sus activos digitales, en este contexto, la ciberseguridad se ha consolidado como un componente esencial para garantizar la continuidad operativa, la integridad de la información y la resiliencia frente a amenazas cada vez más sofisticadas, en particular, las operaciones realizadas por equipos Red Team y Blue Team constituyen un eje fundamental en la evaluación y fortalecimiento de la postura de seguridad de las instituciones, al permitir identificar vulnerabilidades, validar controles defensivos y mejorar los procesos de respuesta ante incidentes.

El presente informe tiene como propósito analizar las capacidades técnicas, tácticas y de respuesta de estos equipos, integrando elementos teóricos, normativos y prácticos, para ello, se aborda inicialmente el marco legal colombiano aplicable a los delitos informáticos y la protección de datos personales, con el fin de establecer las obligaciones, limitaciones y responsabilidades que rigen la actuación profesional en el campo de la seguridad informática, así mismo, se desarrolla un estudio detallado de las etapas del pentesting, destacando las herramientas utilizadas en cada fase y su aplicabilidad en entornos controlados.

De manera complementaria, se examina un caso práctico, donde se ejecutan pruebas ofensivas que incluyen reconocimiento, explotación de vulnerabilidades, escalamiento de privilegios y pivoting dentro de una infraestructura simulada, este análisis permite comprender el impacto real de las fallas de seguridad y la importancia del diseño de mecanismos de hardening y monitoreo continuo.

Justificación

La creciente dependencia de las organizaciones hacia infraestructuras digitales ha incrementado significativamente los riesgos asociados a amenazas informáticas, lo que exige la implementación de estrategias avanzadas de protección, detección y respuesta, en este contexto, el estudio de las operaciones Red Team y Blue Team se convierte en una necesidad académica y profesional, dado que estos enfoques permiten evaluar de manera integral la seguridad de los sistemas, identificar vulnerabilidades críticas y fortalecer los mecanismos defensivos de forma proactiva, analizar las dinámicas entre ambos equipos no solo posibilita comprender cómo actúan los adversarios en un entorno real, sino también cómo deben prepararse las organizaciones para anticipar, contener y mitigar ataques.

La elaboración de este informe responde a la importancia de integrar conocimientos teóricos, normativos y prácticos en el campo de la ciberseguridad, la normativa colombiana en materia de delitos informáticos y protección de datos personales establece obligaciones estrictas tanto para ciudadanos como para profesionales del sector, por lo que resulta indispensable comprender el alcance jurídico de las actividades relacionadas con pruebas de penetración y auditorías de seguridad. (Alvarez Intriago, 2025)

El desarrollo práctico basado en la ejecución de pruebas de reconocimiento, explotación, post-explotación y pivoting en un entorno controlado, proporciona evidencia del impacto real que pueden generar las vulnerabilidades no mitigadas dentro de una red corporativa, este tipo de ejercicios fortalecen el aprendizaje aplicado y contribuyen a la formación de especialistas capaces de responder eficazmente ante incidentes de seguridad, así como de diseñar estrategias de hardening que disminuyan la superficie de ataque.

Objetivos

Objetivo General

Examinar las capacidades técnicas, tácticas y operativas de los equipos Red Team y Blue Team, mediante la integración de fundamentos teóricos, normativos y prácticos, con el fin de evaluar la postura de seguridad de una infraestructura tecnológica.

Objetivos Específicos

Revisar marcos conceptuales, normativos y metodológicos aplicables a la ciberseguridad en el contexto colombiano.

Identificar y evaluar las vulnerabilidades presentes en una infraestructura tecnológica simulada, a través de la ejecución controlada de pruebas de penetración, con el fin de evidenciar el impacto de dichas fallas en la seguridad de la información.

Proponer medidas de hardening y estrategias de mejora orientadas al fortalecimiento de los mecanismos de prevención, detección y respuesta ante incidentes, fundamentadas en los resultados del análisis técnico y en las buenas prácticas de seguridad informática.

Desarrollo del Informe

Fundamentos de Operaciones Red Team y Blue Team

Legislación que existe actualmente dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales con sus características principales.

Existen varias leyes y regulaciones que abordan temas relacionados con delitos informáticos y protección de datos personales en Colombia, como la Ley 1581 de 2012 que habla sobre protección de datos personales.

Características principales:

- ✓ Crea un nuevo título en el Código Penal dedicado a los delitos informáticos que tipifica conductas como: acceso abusivo a un sistema informático, interceptación de datos informáticos, daño o alteración de datos o sistemas informáticos, uso de software malicioso (malware), violación de datos personales y hurto por medios informáticos o electrónicos.
- ✓ Establece penas privativas de la libertad y multas para quienes cometan estos delitos.
- ✓ Protege la integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos.
- ✓ Busca fortalecer la seguridad digital y la confianza en el uso de las TIC en Colombia.

Ley 1712 de 2014 trata sobre transparencia en el acceso a la información pública.

Características principales:

- ✓ Reconocimiento del derecho fundamental al acceso a la información pública, toda persona puede solicitar y recibir información de entidades públicas sin necesidad de justificar su solicitud.
- ✓ Clasificación de la información: información pública, Información reservada e Información clasificada.
- ✓ Protección de datos personales estableciendo que la información pública debe manejarse respetando la Ley 1581 de 2012, garantizando la confidencialidad de los datos personales.
- ✓ Promueve el uso de plataformas digitales y tecnologías de la información para facilitar el acceso ciudadano a los datos del Estado.
- ✓ Encargada de promover la transparencia y apoyar a las entidades en el cumplimiento de la ley.

Ley 1273 de 2009 obligó a las entidades estatales a adoptar medidas para proteger la información y sistemas críticos, lo que llevó a que organismos como el MinTIC a desarrollar una política nacional de seguridad digital.

Características principales:

- ✓ Crea un nuevo bien jurídico protegido la ley reconoce como bien jurídico la protección de la información y de los datos, lo que significa que el Estado protege tanto los sistemas informáticos como la información que contienen.
- ✓ También se imponen multas económicas y agravantes si el delito se comete contra entidades públicas, financieras o en perjuicio de menores.
- ✓ Protege la confidencialidad, integridad y disponibilidad de los datos la ley busca asegurar que la información digital sea confiable, accesible solo a personas autorizadas y no pueda ser alterada sin permiso.

- ✓ Incluye el delito de violación de datos personales, que castiga a quien sin autorización obtenga, modifique o difunda información personal contenida en bases de datos.
- ✓ Su objetivo es fortalecer la seguridad en el uso de las tecnologías de la información y fomentar la confianza en las transacciones electrónicas.

Se articula con la Ley 1581 de 2012 (protección de datos personales) y el Decreto 2364 de 2012 (firma digital y autenticación), fortaleciendo la seguridad jurídica en el entorno digital. (Guarnizo Portela, 2024)

Tabla 1

Síntesis de la legislación colombiana

Norma	Año	Objeto de la ley	Características principales
Ley 1273	2009	Protege la información y los datos como bien jurídico autónomo y tipifica los delitos informáticos en Colombia.	Incorpora al Código Penal los delitos de acceso abusivo a sistemas informáticos, interceptación de datos, daño informático, uso de software malicioso y violación de datos personales. Establece sanciones penales y agravantes cuando se afectan entidades públicas o sistemas críticos.
Ley 1581	2012	Establece el régimen general de protección de datos personales.	Define principios para el tratamiento de datos personales como legalidad, finalidad, libertad y seguridad. Reconoce derechos de los titulares y obligaciones de los responsables y encargados del tratamiento de la información.
Decreto 1377	2013	Reglamenta parcialmente la Ley 1581 de 2012.	Establece mecanismos para la autorización del tratamiento de datos personales, políticas de privacidad y deberes de los responsables del manejo de la información.
Ley 1712	2014	Garantiza el derecho fundamental de acceso a la información pública.	Define la clasificación de la información en pública, reservada y clasificada. Promueve la transparencia estatal y exige el manejo responsable de los datos personales conforme a la Ley 1581.
Ley 906	2004	Regula el procedimiento penal colombiano.	Establece el deber legal de denunciar delitos (artículo 67), aplicable a casos de delitos informáticos y actividades ilícitas conocidas en el ejercicio profesional.
Ley 842	2003	Regula el ejercicio de la ingeniería y el código de ética profesional (COPNIA).	Define principios éticos y prohibiciones para los ingenieros, incluyendo la obligación de actuar conforme a la ley y proteger el interés público, aplicable a profesionales de ciberseguridad. (Lleras, 2025)

Nota. Resumen de las características principales con mis propias palabras de la legislación colombiana en el marco de delitos informáticos y protección de datos.

Etapas del proceso de pruebas de penetración (Pentesting) con ejemplos de cada las herramientas.

- ✓ Primer paso es planificación y alcance

Acordar con el cliente los objetivos y reglas de enfrentamiento Rules of Engagement (ROE), alcance como IP, aplicaciones, ventanas de prueba, permisos legales, restricciones y criterios de éxito que incluye firma de contrato y definición de entregables, acuerdos de confidencialidad y cronograma.

Ejemplo de una herramienta:

Jira y/o Trello es utilizada para gestionar tareas, hitos, autorizaciones y el seguimiento del trabajo durante la prueba; también se usan plantillas o frameworks como PTES u OSSTMM para guiar el proceso.

- ✓ Segundo paso reconocimiento pasivo y activo

Recopilar información sobre el objetivo sin (pasivo) o con (activo) interacción directa, el objetivo es mapear superficie de ataque como dominios, correos, subdominios, empleados, tecnología expuesta, mediante actividades de OSINT, búsquedas en DNS/WHOIS, redes sociales, certificados, motores de búsqueda.

Ejemplo de herramienta:

TheHarvester es utilizada para automatizar la recolección de correos, subdominios y hosts desde fuentes públicas como Google, Shodan, LinkedIn entre otros.

- ✓ Tercer paso escaneo y enumeración

Identificar puertos abiertos, servicios y versiones ejecutándose en los sistemas detectados; enumerar recursos shares, usuarios, endpoints y aquí se transforma la información en

blancos concretos, mediante actividades de escaneo de puertos, fingerprinting de servicios, enumeración de directorios, listados de usuarios.

Ejemplo de herramienta:

Nmap es utilizada para el escaneo de puertos y detección de servicios OS; es la herramienta base para saber qué atacar o analizar más a fondo.

- ✓ Cuarto paso análisis de vulnerabilidades

Cruzar resultados de escaneo con firmas y bases de datos para priorizar vulnerabilidades reales frente a falsos positivos, evaluando impacto y probabilidad mediante actividades de escaneo con scanners, correlación de hallazgos, priorización según riesgo.

Ejemplo de herramienta:

Nessus o OpenVAS es utilizado como scanners que identifican vulnerabilidades conocidas y generan informes que sirven para priorizar pruebas manuales.

- ✓ Quinto paso pruebas manuales y explotación controlada

Intentar de forma controlada explotar vulnerabilidades priorizadas para demostrar impacto real como por ejemplo acceso a una cuenta, ejecución remota, filtrado de datos siempre dentro del alcance autorizado mediante actividades como pruebas manuales, uso de exploits comprobados en entornos autorizados, verificación de impacto.

Ejemplo de herramienta:

Metasploit Framework permite probar exploits de forma controlada y lanzar payloads en entornos de prueba; útil para validar que una vulnerabilidad es explotable.

- ✓ Sexto paso post-explotación o exfiltración simulada

Una vez que se logra acceso, se evalúa la extensión del compromiso, qué datos y/o privilegios se pueden alcanzar, posibilidad de moverse lateralmente o mantener el acceso,

verificando impacto y rutas de ataque mediante actividades de recopilación de credenciales, escaneo interno desde la máquina comprometida, pruebas de persistencia simulada.

Ejemplo de herramienta:

Meterpreter es un componente de Metasploit es utilizado como un shell avanzado para interactuar con una máquina comprometida y realizar tareas de post-explotación en pruebas autorizadas.

- ✓ Séptimo paso escalamiento de privilegios

Emplea técnicas para elevar privilegios desde una cuenta limitada hasta administrador/root para demostrar el alcance del compromiso, se documentan los vectores que permiten la elevación mediante actividades de búsqueda de configuraciones débiles, servicios mal configurados, credenciales en claro, exploits locales.

Ejemplo de herramienta:

LinPEAS y/o WinPEAS es utilizado con scripts de enumeración que ayudan a identificar vectores comunes de escalamiento en Linux/Windows; usados para encontrar rutas posibles sin automatizar explotación peligrosa.

- ✓ Octavo paso movimiento lateral y/o pivoting

Desde una máquina comprometida, intentar acceder a otros sistemas de la red para demostrar cómo un atacante podría expandir su control, mediante actividades de uso de credenciales obtenidas, creación de túneles, proxies para alcanzar segmentación interna.

Ejemplo de herramienta:

ProxyChains, SSHuttle o configuración de un proxy SOCKS vía Meterpreter es utilizado para permitir redirigir tráfico y evaluar conectividad interna.

- ✓ Noveno paso remediation temporal y restauración

Antes de terminar de eliminar cualquier artefacto creado por el equipo de pentest como backdoors de prueba, cuentas de prueba, ficheros subidos, dejar el entorno en su estado original mediante actividades de revocar accesos provisionales, eliminar payloads, cerrar sesiones sin dejar evidencia para el cliente. (PandaSecurity, 2018)

Ejemplo de herramienta:

Con procedimientos internos, checklists y scripts de limpieza; no es tanto una herramienta única sino un proceso con control de cambios.

- ✓ Decimo paso reporte técnico y ejecutivo

Documentar todo lo encontrado, evidencia, impacto, pasos reproducibles, evaluando el riesgo y recomendaciones concretas de mitigación y prioridades, mediante la entrega de un reporte ejecutivo para la alta dirección y uno técnico para el área de TI.

Ejemplo de herramienta:

Dradis y/o Serpico son plataformas para recopilar hallazgos, generar plantillas de reporte y exportar informes claros y consistentes.

- ✓ Onceavo paso verificación de mitigaciones

Una vez que el cliente implementa mitigaciones, se revalida que las vulnerabilidades hayan sido corregidas efectivamente, mediante actividades de ejecutar pruebas puntuales sobre los hallazgos corregidos, confirmar cierre y actualizar el reporte final.

Ejemplo de herramienta:

El mismo scanner o pruebas manuales usadas inicialmente, también con herramientas como Nessus, Nmap, Burp, Kali según corresponda.

Definiciones de herramientas de ciberseguridad existentes y/o software especializado.

Metasploit: es un framework que compone un conjunto de herramientas y librerías de código abierto diseñado para desarrollar, probar y ejecutar exploits contra sistemas vulnerables, es ampliamente usado en seguridad informática para pruebas de penetración o pentesting, investigación de vulnerabilidades y formación tanto por profesionales de la ciberseguridad como adversarios. (Palomo Luna, 2024)

Metasploit facilita el proceso de convertir una vulnerabilidad en una prueba práctica que permite seleccionar un exploit es decir un código que aprovecha la vulnerabilidad, combinarlo con un payload es decir el código que se ejecuta en la máquina objetivo y posteriormente realizar sesiones de post-explotación.

Dentro de sus componentes principales está el módulo exploit que aprovecha una vulnerabilidad especifica, el código que una payload que se entrega y ejecuta en el objetivo tras el exploit, los mudulos auxiliares como escáneres, fuzzers, sniffers, bruteforce, los post-modules que recopilan credenciales, escalada de privilegios, persistencia, recolección de información que ayudan a ofuscar payloads para evadir firmas o adaptarse a restricciones.

- ✓ Nmap: conocida en inglés como Network Mapper, es una herramienta open-source para el descubrimiento y el análisis de redes, se usa para identificar hosts activos, servicios puertos abiertos y aplicaciones, en los sistemas operativos, versiones de software y características de seguridad en una red, es una herramienta fundamental para los administradores de red.

De los componentes principales esta nmap que es el binario principal para escaneos desde la línea de comandos, NSE - Nmap Scripting Engine que es un motor de scripts en

programación Lua para tareas automatizadas y permite detección de vulnerabilidades, fuerza bruta y recopilación de información extra.

Así mismo cuenta con ncat que es una utilidad incluida para conexiones de protocolo TCP/UDP, ndiff: que su función es comparar los resultados de escaneos, Zenmap que permite visualizar y guardar resultados.

- ✓ OpenVas en inglés Open Vulnerability Assessment System y es una herramienta de código abierto usada para realizar escaneos de vulnerabilidades en equipos, servidores y redes, su función principal es detectar fallos de seguridad conocidos, clasificarlos según su nivel de riesgo y recomendar cómo solucionarlos.

Esta solución permite analizar sistemas en busca de vulnerabilidades conocidas CVE, detecta configuraciones inseguras, puertos abiertos y servicios vulnerables, genera informes detallados con nivel de riesgo CVSS, ayudando a organizaciones a prevenir ataques antes de que ocurran.

Entre algunas desventajas están que puede generar falsos positivos, requiere buena configuración inicial como ajustes, políticas y actualizaciones, realiza escaneos fuertes que pueden afectar servidores o redes en producción y es más lento que herramientas como Nmap o Masscan porque cuenta con un análisis más profundo.

Servicios en línea:

- ✓ ExploitDB: en ingles Exploit Database, es una base de datos pública y gratuita que recopila exploits, vulnerabilidades, pruebas de concepto PoC y herramientas relacionadas con la seguridad informática, es mantenida por Offensive Security.

ExploitDB se usa para buscar exploits públicos para vulnerabilidades conocidas CVE, analiza cómo funciona un exploit, con fines educativos o para pruebas de seguridad, realiza

pentesting legal en entornos controlados, verifica si un sistema es vulnerable a exploits existentes y esta actualizada en vulnerabilidades reales y técnicas de explotación recientes.

Estas son algunas ventajas es gratuita y de acceso público viene actualizada con miles de vulnerabilidades y PoC reales, es útil para aprendizaje, auditoría, defensa y actualmente es compatible con herramientas como Searchsploit en modo offline

- ✓ CVE: significa Common Vulnerabilities and Exposures lo que traduce Vulnerabilidades y Exposiciones Comunes, es un sistema que asigna un identificador único a cada vulnerabilidad de software o hardware conocida públicamente.

El objetivo del sistema CVE es crear un estándar mundial para identificar vulnerabilidades, así mismo permitir que empresas, investigadores y fabricantes hablen el mismo lenguaje, por ende, facilitar el seguimiento, parcheo y comunicación de fallos de seguridad; sin esta organización de las CVE cada empresa podría nombrar una vulnerabilidad diferente de forma distinta, causando confusiones. (Easttom, 2018)

Proceso resumido para reportar de un CVE, inicialmente el investigador descubre una vulnerabilidad, este la reporta a MITRE o a un CNA que es una autoridad que puede generar CVEs, como Microsoft, Google, entre otros, posteriormente se valida y se asigna un ID CVE oficial y luego se publica para que los fabricantes apliquen parches y los usuarios se protejan.

Fragmentos ilegales en el "acuerdo de confidencialidad", evidenciando procesos ilegales y no éticos.

1) <u>Fragmento del texto del acuerdo de confidencialidad</u>:

"...la parte receptora, se obliga a no divulgar... la información confidencial o sobre procesos ilegales dentro de SecureNova Labs no podrán ser divulgados."

a. Esta cláusula intenta impedir que la parte receptora denuncie actos ilegales, lo cual viola el deber legal ciudadano de denunciar delitos según lo estipulado en el artículo 67 del Código de Procedimiento Penal ley 906 de 2004 en Colombia.

b. También compromete al firmante a encubrir actividades ilícitas, lo cual podría ser considerado como favorecimiento o encubrimiento, delito tipificado en el Código Penal colombiano.

2) Fragmento del texto del acuerdo de confidencialidad:

Se consideran datos confidenciales: "*...datos secretos como 'datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos'.*"

a. Guardar silencio frente a este tipo de información constituye una complicidad pasiva o encubrimiento de un delito tipificado en la legislación colombiana.

b. Así mismo normaliza es decir presenta algo ilegal como si fuera algo común, aceptable o permitido y protege información ilícita que proviene de delitos informáticos tipificados en la Ley 1273 de 2009 en Colombia. (Andrade, 2025)

3) Fragmento del texto del acuerdo de confidencialidad:

"*No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso...*"

a. Esto va directamente en contra del deber legal de denunciar delitos del Art. 67 del Código de Procedimiento Penal.

4) Fragmento del texto del acuerdo de confidencialidad:

"*Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca...*".

a. Esta cláusula no es válida jurídicamente, ya que ningún acuerdo u otro documento privado o público de ser el caso, no puede estar por encima de la ley penal, ni coartar los derechos ciudadanos.

5) Fragmento del texto del acuerdo de confidencialidad:

"...en caso que la información ilegal... sea encontrada en manos del receptor éste deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a SecureNova Labs."

a. Este fragmento intenta trasladar toda responsabilidad penal la parte receptora y proteger a la empresa, lo cual es un acto abusivo, desproporcionado e inválido jurídicamente.

b. En Colombia, la responsabilidad penal es personal e intransferible, por lo que esta cláusula carece de validez.

Artículos de la ley 1273 que vulneran el "acuerdo de confidencialidad".

Artículo 269A acceso abusivo a un sistema informático: este artículo sanciona el ingreso no autorizado a sistemas informáticos y el acuerdo no rechaza esta conducta, sino que la acepta como información protegida y obliga a no denunciarla, lo cual implica encubrimiento del delito.

Artículo 269C interceptación de datos informáticos: la interceptación de información privada sin autorización es un delito informático ya que el acuerdo obliga a la parte receptora a guardar silencio sobre esta práctica, en lugar de denunciarla ante autoridades.

Artículo 269E uso de software malicioso o con fines ilícitos: muchas prácticas de espionaje informático implican software o herramientas para intrusión y obligar a la parte receptora a no denunciar espionaje informático implica permitir una actividad sancionada por esta ley.

Artículo 269F violación de datos personales: si la empresa accede o divulga datos personales sin autorización, está violando este artículo y el acuerdo exige al firmante guardar silencio, promoviendo indirectamente esta conducta ilegal.

Justificación de la propuesta laboral en SecureNova Labs, teniendo en cuenta el código de ética para ingenieros.

Aunque la oferta salarial y contractual es buena, el acuerdo contiene cláusulas que obligan a guardar silencio frente a actos ilegales como interceptación de comunicaciones, accesos abusivos y espionaje informático, aceptar dichas condiciones vulneraría principios establecidos en el código de ética del COPNIA en su artículo Art 32 “prohibiciones generales a los profesionales”; que exigen actuar conforme a la ley, proteger a la sociedad, no participar ni encubrir actos ilícitos y mantener la dignidad e integridad de la profesión; por ello, como profesional en ciberseguridad, solo consideraría vincularme si la empresa se modifica el acuerdo de confidencialidad, eliminando cualquier apartado que contravenga la Constitución Política de Colombia de 1991, la Ley 1273 de 2009 y los principios éticos de la ingeniería enmarcados por COPNIA.

Garantías de acceso a la información sensible de sus clientes durante una auditoría de seguridad.

En el ámbito de la ciberseguridad, las auditorías de seguridad son procesos esenciales para evaluar la fortaleza de las defensas tecnológicas de una organización y detectar posibles vulnerabilidades que puedan ser explotadas por atacantes, sin embargo, durante estas auditorías, las empresas de ciberseguridad acceden a información sensible de sus clientes, lo cual plantea importantes desafíos éticos, legales y técnicos. Por ello, es fundamental establecer límites claros sobre el alcance de dicho acceso y garantizar que el manejo de la información se realice de forma segura y responsable.

El acceso a información sensible debe estar determinado por el principio de necesidad y proporcionalidad, es decir, las empresas auditoras solo deben acceder a los datos estrictamente necesarios para cumplir los objetivos de la auditoría, en ningún caso el proceso debe permitir el acceso indiscriminado o total a los sistemas de información del cliente, ya que esto podría vulnerar su privacidad, la confidencialidad de los datos y la confianza depositada en el auditor, este principio se encuentra alineado con estándares internacionales como la ISO/IEC 27001, que establece directrices para la gestión segura de la información y la protección de los activos digitales dentro de un marco de control. (MINTIC, 2022)

Mecanismos de supervisión y control con herramientas avanzadas de análisis forense.

En el contexto actual de la ciberseguridad, las herramientas avanzadas de análisis forense digital se han convertido en instrumentos fundamentales para la investigación de incidentes, la recolección de evidencias electrónicas y la identificación de vulnerabilidades en los sistemas de información, no obstante, el poder técnico de estas herramientas también implica un alto nivel de riesgo, ya que pueden ser utilizadas con fines no autorizados o éticamente cuestionables, como la intrusión en sistemas ajenos, la manipulación de datos o la violación de la privacidad, por esta razón, resulta indispensable que las empresas de ciberseguridad implementen mecanismos de supervisión y control que aseguren su uso responsable, ético y legal. (Luttgens, 2014)

Se debe establecer una política interna de uso aceptable de herramientas forenses, que defina claramente los límites de su utilización, los escenarios autorizados y las sanciones aplicables en caso de uso indebido, esta política debe estar alineada con la legislación vigente, como la Ley 1273 de 2009, que tipifica los delitos informáticos en Colombia y sanciona el acceso no autorizado, la interceptación de datos o la alteración de información, además, debe incluir los principios éticos contenidos en el Código de Ética del COPNIA Ley 842 de 2003, que

obliga a los ingenieros y profesionales del sector tecnológico a ejercer su labor con responsabilidad, integridad y respeto por los derechos de terceros. (Vargas Lleras, 2025).

Medidas adecuadas para restaurar la confianza, cuando una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje.

Cuando un gobierno u organización descubre que una empresa de ciberseguridad contratada ha participado en actos de ciberespionaje, la respuesta debe ser inmediata, transparente y ajustada al marco legal; en primer lugar, las autoridades competentes deben iniciar investigaciones judiciales y administrativas para determinar la responsabilidad penal y contractual de la empresa implicada.

Paralelamente, se debe suspender o rescindir el contrato con la compañía involucrada, protegiendo los activos de información y evitando cualquier posibilidad de manipulación o destrucción de evidencia, las organizaciones afectadas deben implementar medidas de contención y análisis forense para evaluar el alcance del daño y garantizar la preservación de pruebas que permitan sustentar acciones legales.

Para restaurar la confianza, los gobiernos y empresas deben comunicar los hechos de forma responsable, adoptar políticas de transparencia y fortalecer los mecanismos de supervisión de proveedores de ciberseguridad, así mismo, es esencial establecer procesos de certificación y auditorías independientes que evalúen la idoneidad ética y técnica de los contratistas antes de su vinculación.

Finalmente, se deben reforzar las normas de gobernanza y cumplimiento, promoviendo una cultura basada en la ética, la responsabilidad profesional y la protección de los derechos digitales, la adopción de estándares internacionales como la ISO/IEC 27001 y la exigencia de

códigos de conducta que contribuyan a prevenir la reincidencia y a fortalecer la confianza en el ecosistema de la ciberseguridad.

Herramientas software que se empleó, comandos utilizados y resultados según los pasos de un pentesting.

Las pruebas de penetración, conocidas como pentesting, constituyen una actividad fundamental dentro de la ciberseguridad ofensiva y la auditoría técnica, su propósito es identificar vulnerabilidades en los sistemas, redes o aplicaciones, mediante un entorno controlado, este tipo de evaluación permite a las organizaciones mejorar sus controles de seguridad, reducir superficies de ataque y fortalecer sus capacidades defensivas.

- Reconocimiento: el reconocimiento corresponde a la fase preliminar donde se recopila información del objetivo sin interacción invasiva, el propósito es comprender el contexto tecnológico y operativo del entorno a evaluar, en esta etapa se puede estudiar dominios internos y la topología.

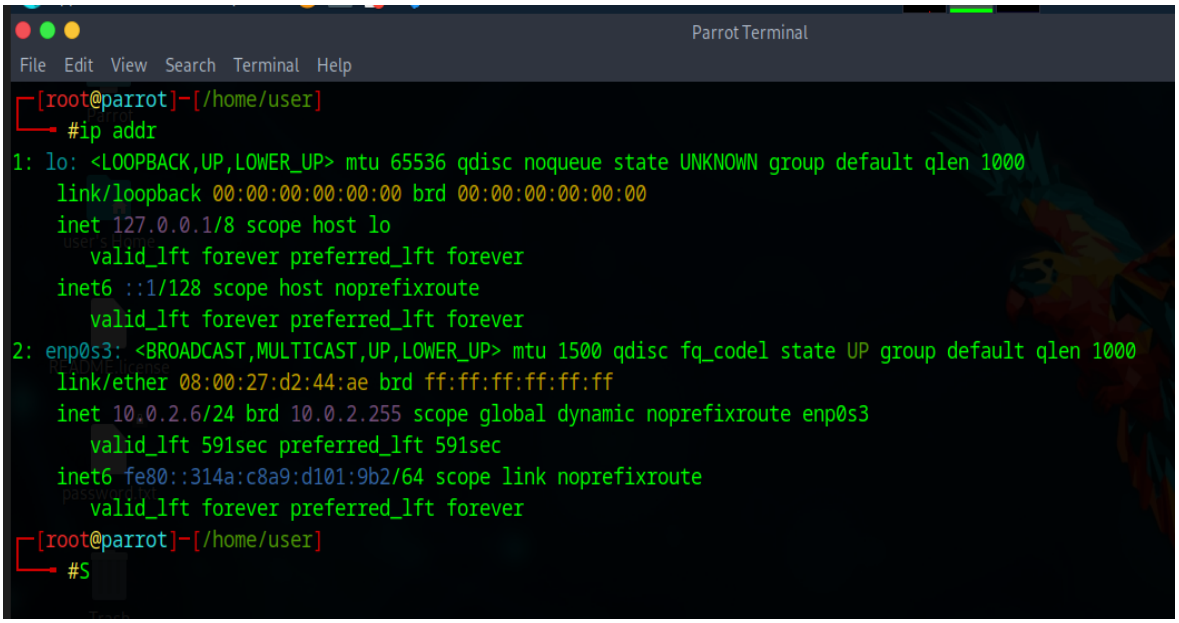
Figura 1

Topología de red

Nota. Captura de pantalla de la topología propuesta en el anexo 4 escenario 3

Figura 2

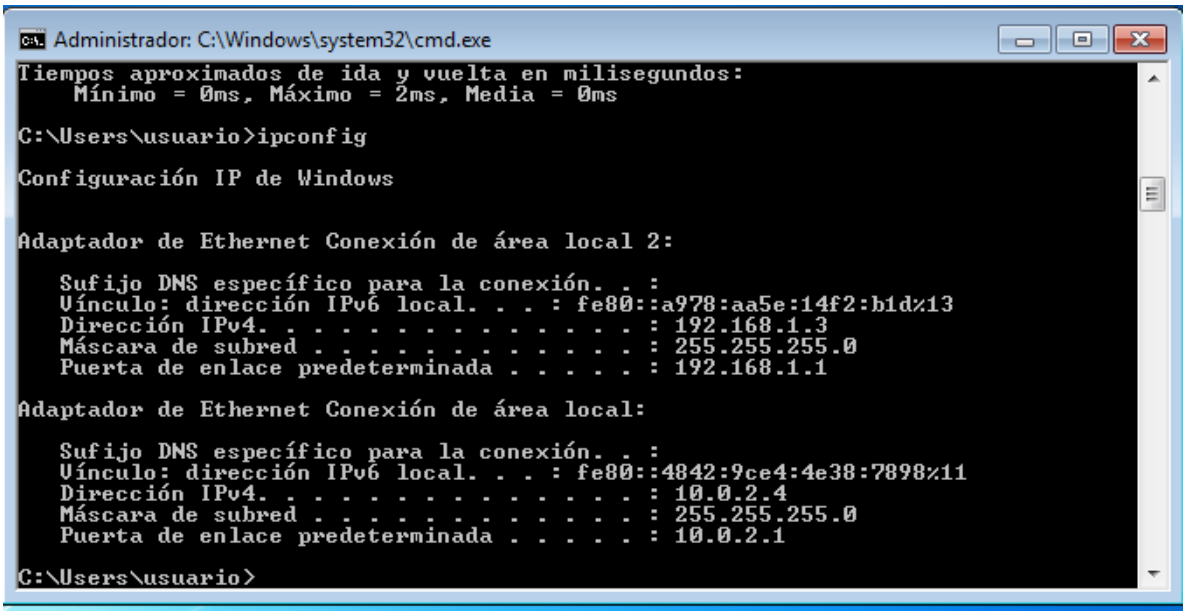
Configuración Ip de Parrot



Nota. Captura de pantalla de la configuración Ip y del segmento de red en Parrot.

Figura 3

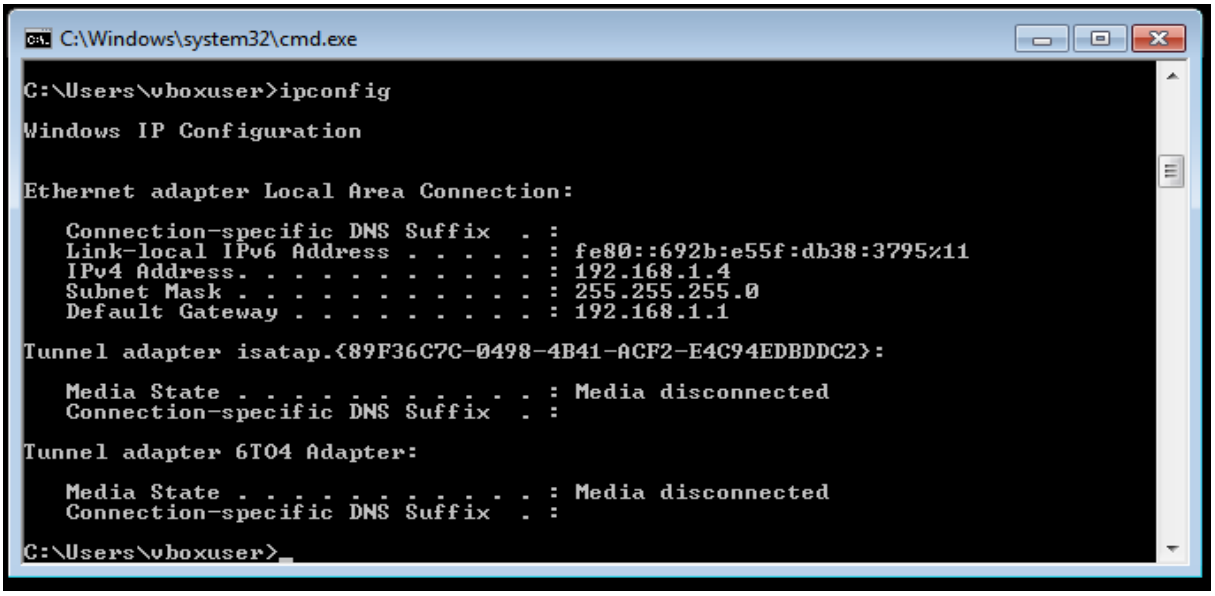
Configuración Ip de Windows 7 Host A



Nota. Captura de pantalla de la configuración Ip del Host A y sus segmentos de red, SO Windows 7.

Figura 4

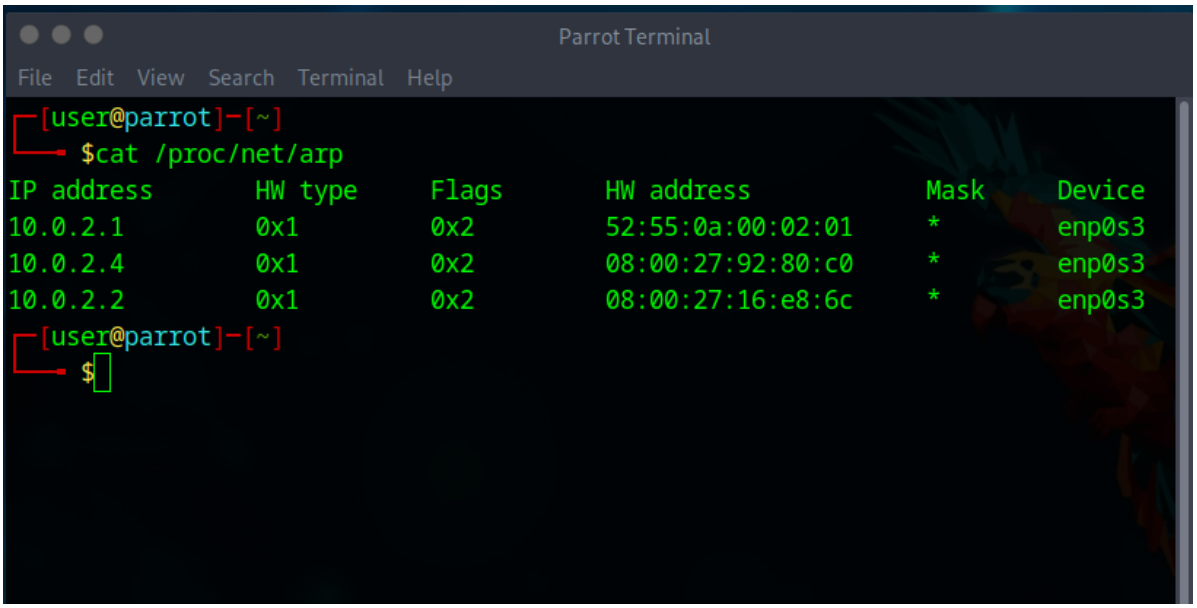
Configuración Ip de Windows 7 Host B



Nota. Captura de pantalla de la configuración Ip del Host A y su segmento de red, SO Windows 7.

Figura 5

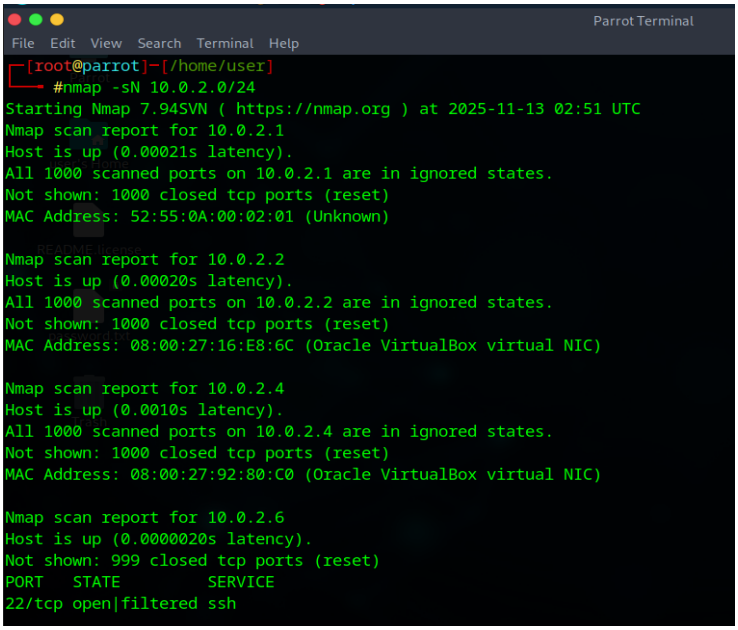
Tabla ARP



Nota. Captura de pantalla de la tabla ARP, con el fin de identificar qué dispositivos están activos en la red local recientemente.

Figura 6

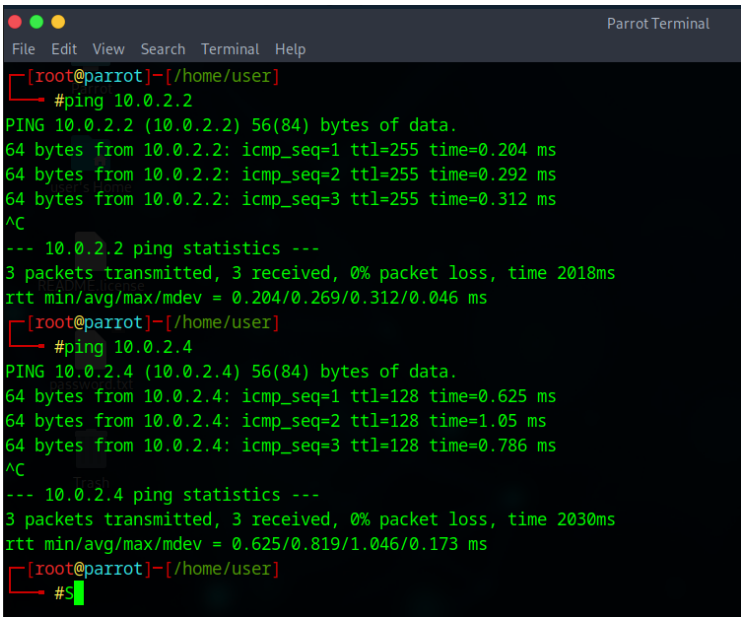
Comando con la herramienta nmap



Nota. Captura de pantalla mediante el comando sudo nmap -sN 10.0.2.0/24 realizando escaneo al segmento de red, se evidencia la IP de dos máquinas virtuales.

Figura 7

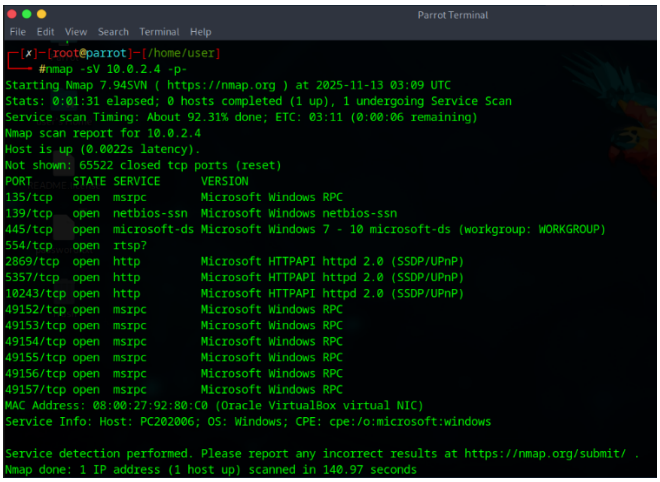
Ping a máquinas virtuales



Nota. Captura de pantalla del ping a las máquinas virtuales estableciendo que de acuerdo con la tabla TTL (Windows=128, CiscoIOS=255).

Figura 8

Pre-escaneo de versiones de los servicios

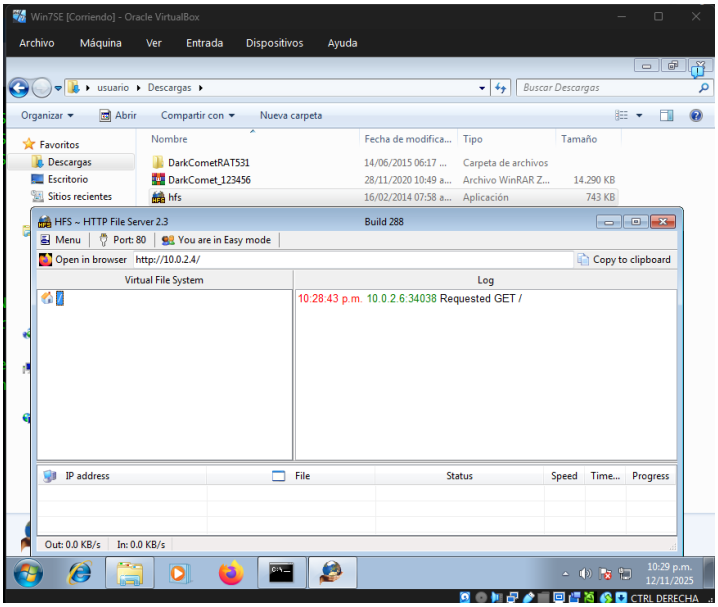


Nota. Captura de pantalla del escaneo de versiones de los servicios que se están ejecutando, puertos en estado abierto del host IP 10.0.2.4.

- Escaneo: esta etapa se orienta a descubrir los puertos y servicios activos en los sistemas objetivo, se realiza una exploración sistemática para identificar la superficie técnica disponible para interacciones posteriores.

Figura 9

Rejetto HFS - HTTP File Server

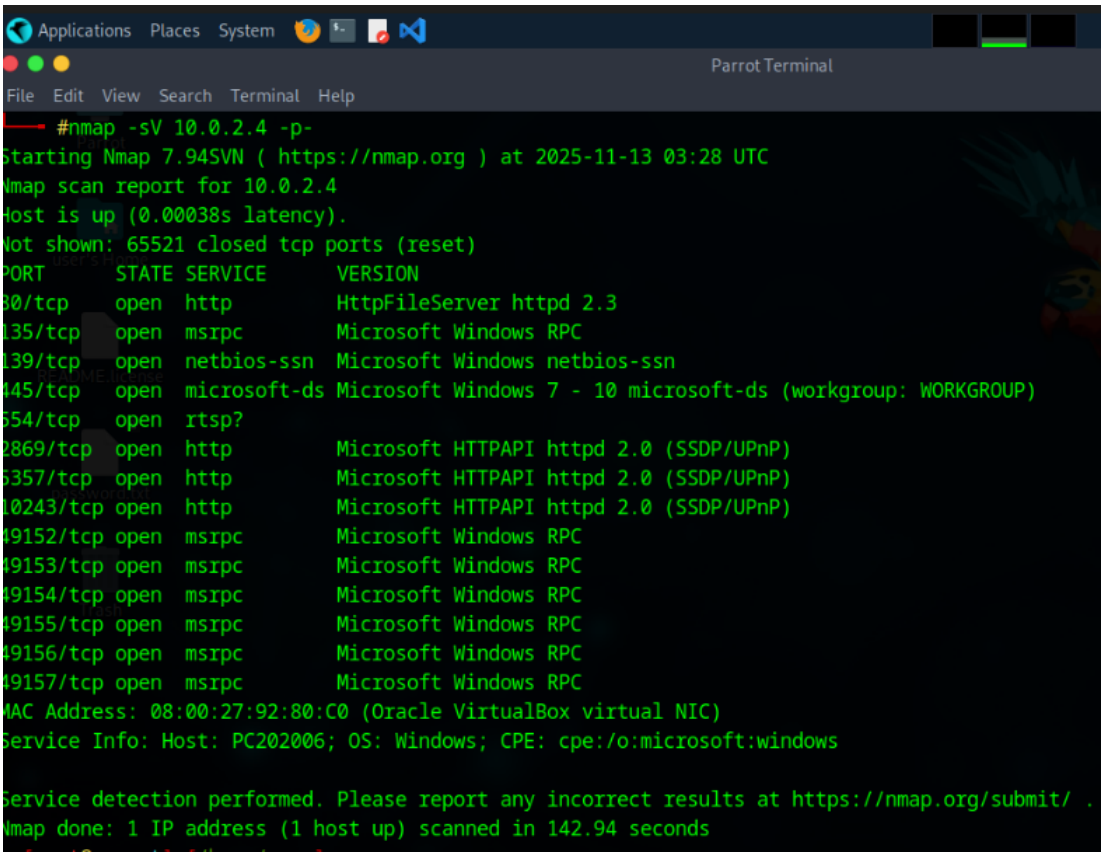


Nota. Captura de pantalla del host A se inician los servicios de la aplicación Rejetto HFS - HTTP File Server.

- Enumeración: consiste en extraer información adicional a partir de los servicios descubiertos, se profundiza en cada uno para descubrir usuarios, directorios, recursos compartidos o configuraciones que puedan facilitar la explotación futura.

Figura 10

Escaneo de versiones de los servicios con NMAP



Nota. Captura de pantalla del host A donde se evidencia en el puerto 80 servicio http versión httpFileServer2.3.

Rejetto HFS - HTTP File Server es una aplicación desarrollada por Rejetto que permite a los usuarios crear un servidor web para compartir archivos a través de un navegador, su objetivo principal es la simplicidad basta con ejecutar la aplicación y arrastrar archivos o carpetas para que queden disponibles a través de una URL. (Wikimedia Foundation, 2025)

Figura 11

Vulnerabilidad en Rejetto HTTP File Server

Nota. Captura de pantalla de la página web incibe-cert donde describe detalladamente sobre la vulnerabilidad CVE-2024-23692 de la aplicación Rejetto. (Incibe, 2025)

Reporte generado con la herramienta de análisis y detección de vulnerabilidades

Mediante el comando sudo nmap -sV -sC --script=vuln -p- 10.0.2.4, el cual realiza un escaneo de red detallado y buscar posibles vulnerabilidades en todos los puertos de un sistema, los resultados de los scripts de vulnerabilidad muestran información detallada sobre vulnerabilidades detectadas, incluyendo el ID de CVE si existe, el nivel de riesgo, y una breve descripción.

```
┌──(root㉿parrot)-[/home/user]
└─# sudo nmap -sV -sC --script=vuln -p- 10.0.2.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-13 03:37 UTC
Nmap scan report for 10.0.2.4
Host is up (0.00093s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         HttpFileServer httpd 2.3
|_http-server-header: HFS 2.3
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
| http-method-tamper:
|   VULNERABLE:
|   Authentication bypass by HTTP verb tampering
|     State: VULNERABLE (Exploitable)
|       This web server contains password protected resources vulnerable to authentication bypass
```

```
|      vulnerabilities via HTTP verb tampering. This is often found in web servers that only limit access to the
|       common HTTP methods and in misconfigured .htaccess files.
|
|    Extra information:
|
|  URIs suspected to be vulnerable to HTTP verb tampering:
|    /~login [GENERIC]
|
|    References:
|      http://www.imperva.com/resources/glossary/http_verb_tampering.html
|      http://capec.mitre.org/data/definitions/274.html
|      https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_%28OWASP-CM-008%29
|_     http://www.mkit.com.ar/labs/htexploit/
| http-vuln-cve2011-3192:
|   VULNERABLE:
|   Apache byterange filter DoS
|     State: VULNERABLE
|     IDs:  BID:49303  CVE:CVE-2011-3192
|       The Apache web server is vulnerable to a denial of service attack when numerous
|       overlapping byte ranges are requested.
|     Disclosure date: 2011-08-19
|     References:
|       https://www.tenable.com/plugins/nessus/55976
|       https://seclists.org/fulldisclosure/2011/Aug/175
|       https://www.securityfocus.com/bid/49303
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:92:80:C0 (Oracle VirtualBox virtual NIC)
Service Info: Host: PC202006; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
```

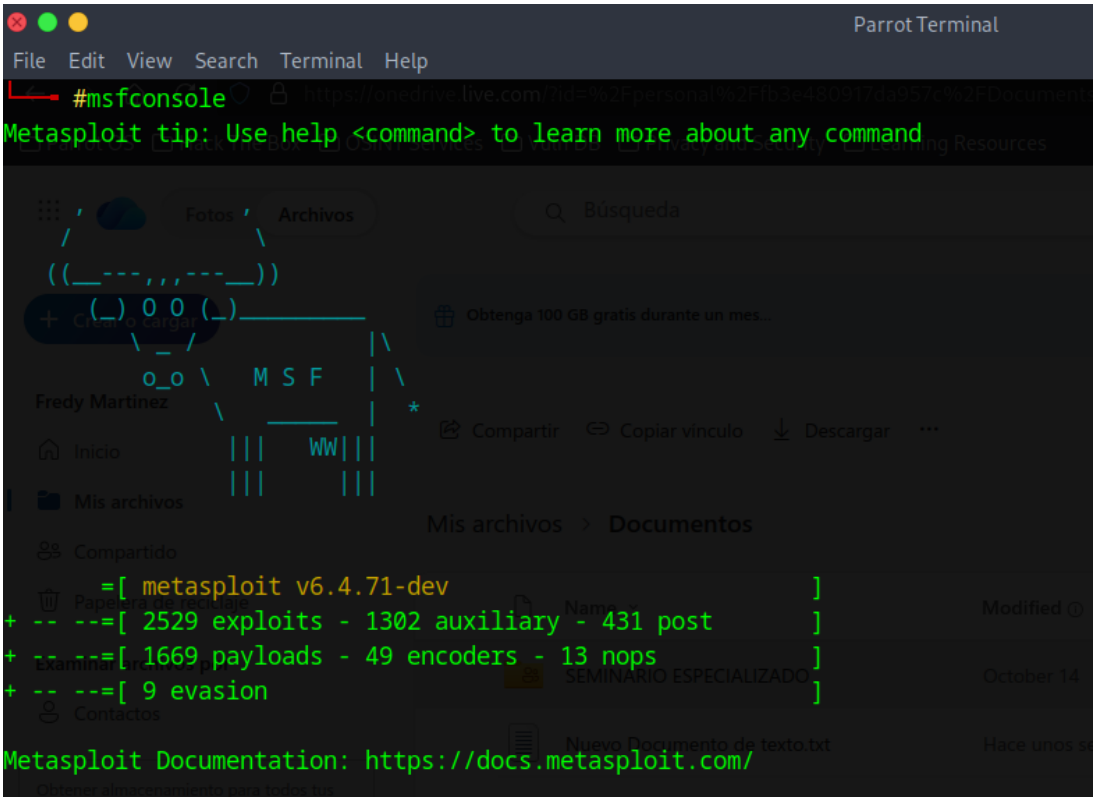
```
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
            Nmap done: 1 IP address (1 host up) scanned in 455.68 seconds
```

- Explotación: el propósito de la explotación es confirmar la existencia y el impacto de las vulnerabilidades detectadas, en el entorno de laboratorio, se seleccionó un servicio vulnerable para validar la posibilidad del acceso no autorizado.

Figura 12

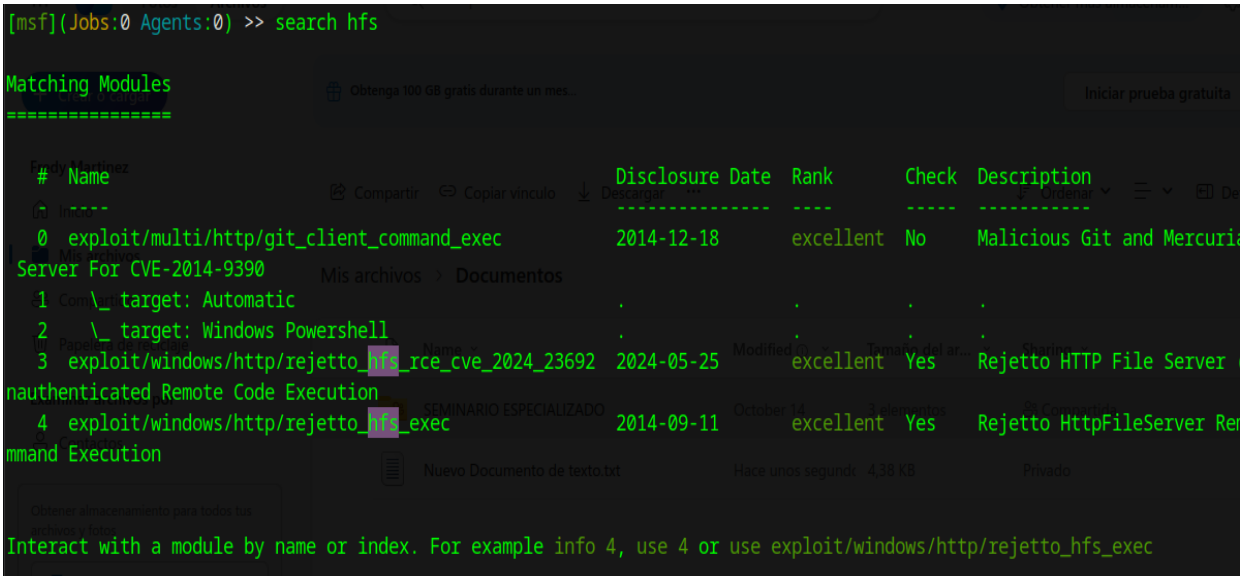
Interfaz de la consola de Metasploit Framework



Nota. Captura de pantalla de Metasploit donde se puede usar comandos para buscar exploits, cargar payloads, realizar escaneos y ejecutar ataques.

Figura 13

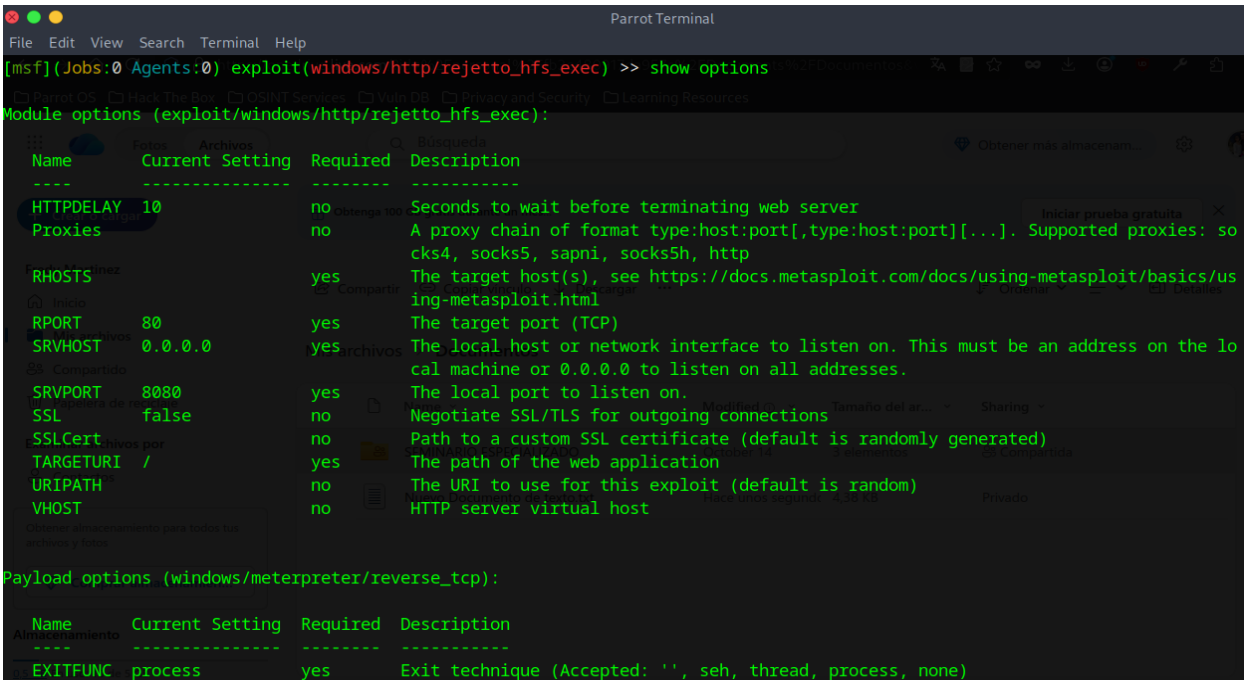
Interfaz de la consola de Metasploit Framework



Nota. Captura de pantalla con el comando buscar “hfs” el cual arroja lo módulos para escoger.

Figura 14

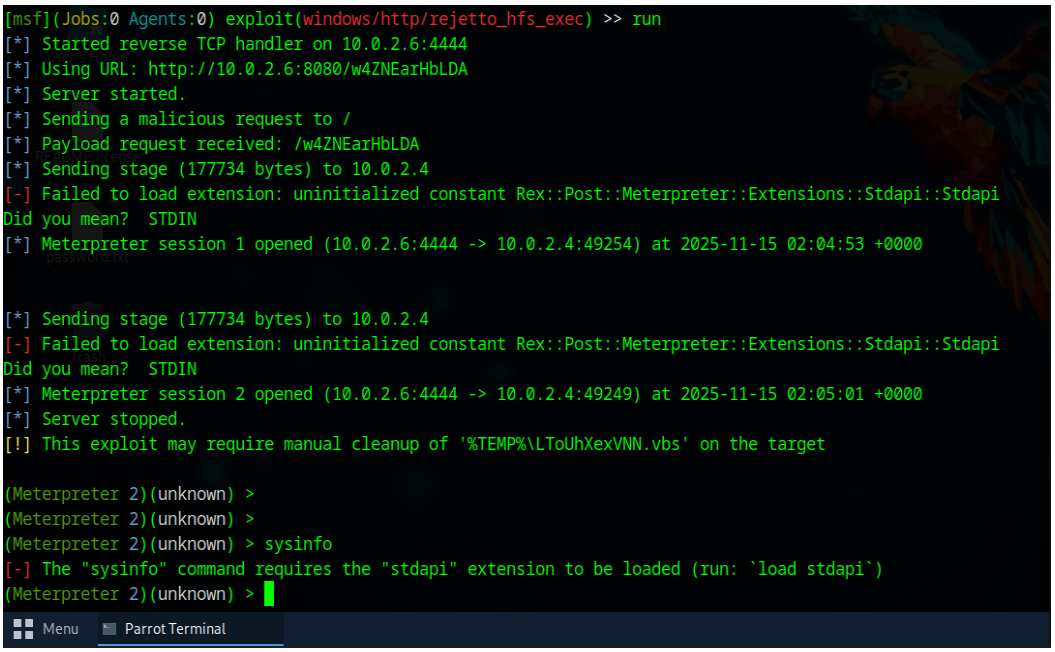
Interfaz de la consola de Metasploit Framework



Nota. Captura de pantalla con el comando show options, con el fin de establecer los parámetros de ataque.

Figura 15

Interfaz de la consola de Metasploit Framework



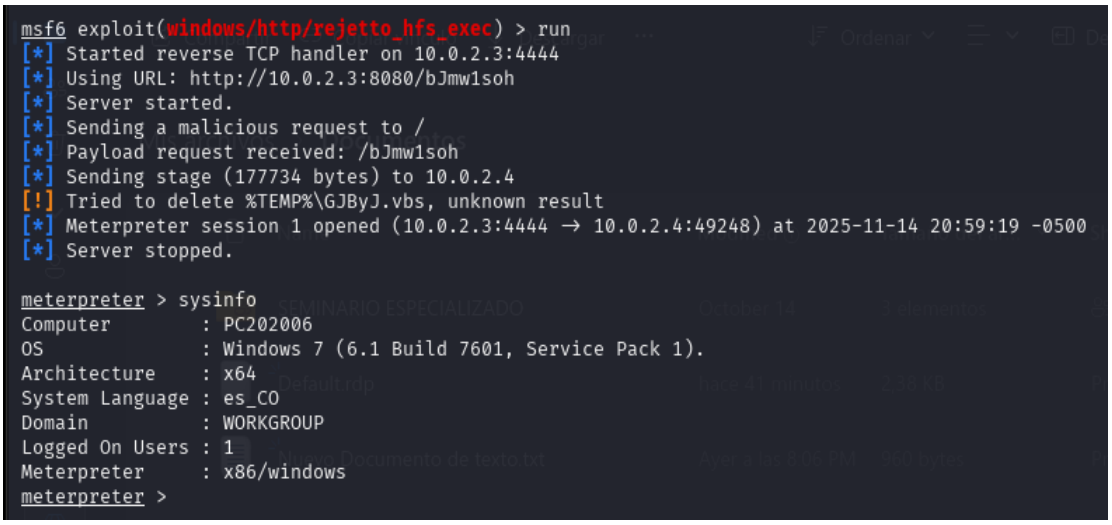
Nota. Captura de pantalla en la que se evidencia que mediante el comando run mestasploit, empieza a realizar el ataque.

En este punto es importante indicar que se emplea el comando “sysinfo” el cual permite obtener información detallada sobre el sistema operativo y sus componentes, pero este arroja un error que el comando requiere que se cargada la extensión “stadapi”; acá se intentaron varias opciones para solucionar el error, entre ellas volver a instalar el metasploit, desactivar defender, firewall del host A, reiniciar los servicios de la aplicación Rejetto HFS, reiniciar maquinas virtuales, sin obtener una solución. (rapid7, 2012)

Por lo anterior se toma la decisión de utilizar Kali Linux con ip 10.0.2.3, el cual si me permite obtener información del SO, así mismo se dejó constancia que se le informo al tutor, sobre el inconveniente y que se hace el cambio de parrot por Kali Linux.

- Post-explotación: esta etapa tiene como objetivo analizar el valor del acceso obtenido, así como el impacto que una intrusión exitosa podría producir. También se evalúan permisos, recursos internos y la posibilidad de moverse lateralmente.

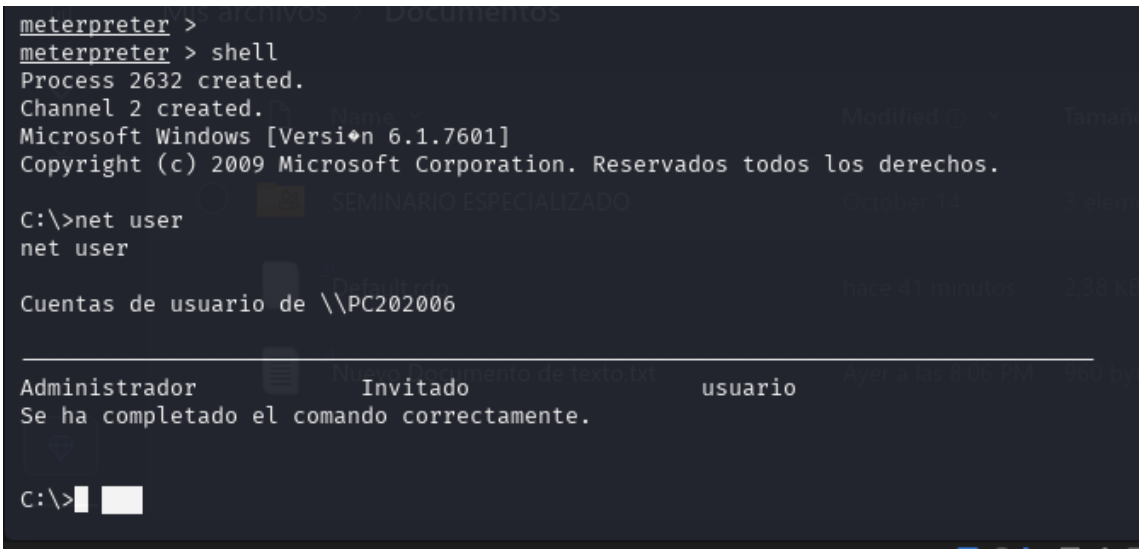
Figura 16 *Interfaz de la consola de Metasploit Framework con Kali Linux*



Nota. Captura de pantalla en la que se evidencia la información del sistema operativo con el comando “sysinfo”.

Figura 17

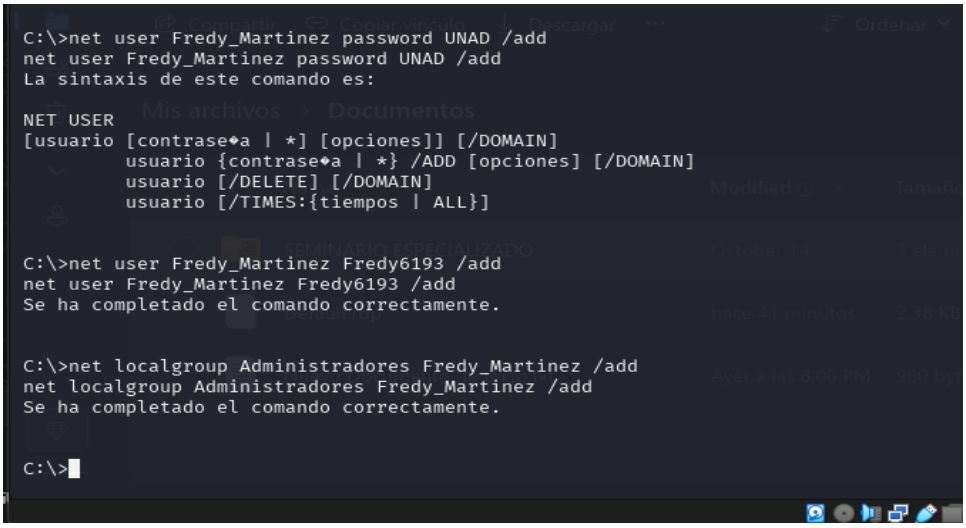
Interfaz de la consola de Metasploit Framework con Kali Linux



Nota. Captura de pantalla en donde se evidencia con el comando “shell” la apertura de la línea de comandos del sistema operativo Windows 7 del Host A.

Figura 18

Interfaz de la consola de Metasploit Framework con Kali Linux

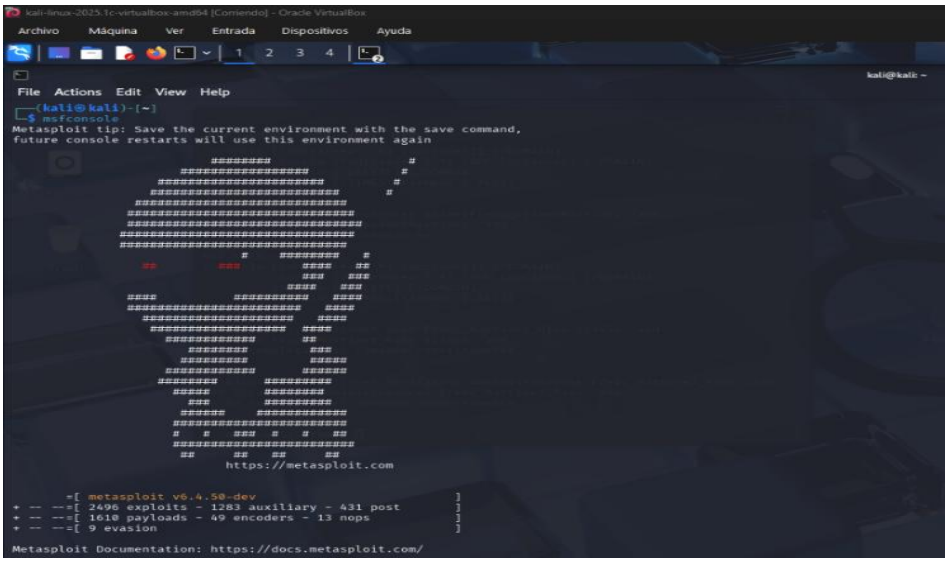


Nota. Captura de pantalla en donde se evidencia la creación del usuario "Fredy_Martinez" y posterior mente se le dan roles al usuario de "Administrador".

- Pivoting: el pivoting consiste en utilizar un sistema comprometido como punto intermedio para acceder a otros sistemas que originalmente no eran alcanzables desde el exterior. Esta técnica permite evaluar el riesgo de propagación dentro de la red interna.

Figura 19

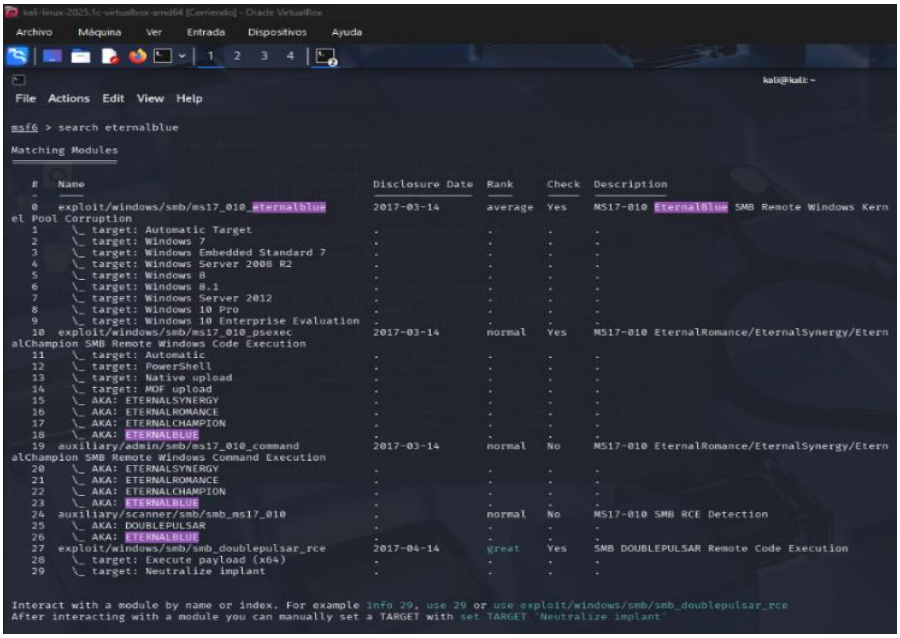
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla de Metasploit donde se puede usar comandos para buscar exploits, cargar payloads, realizar escaneos y ejecutar ataques.

Figura 20

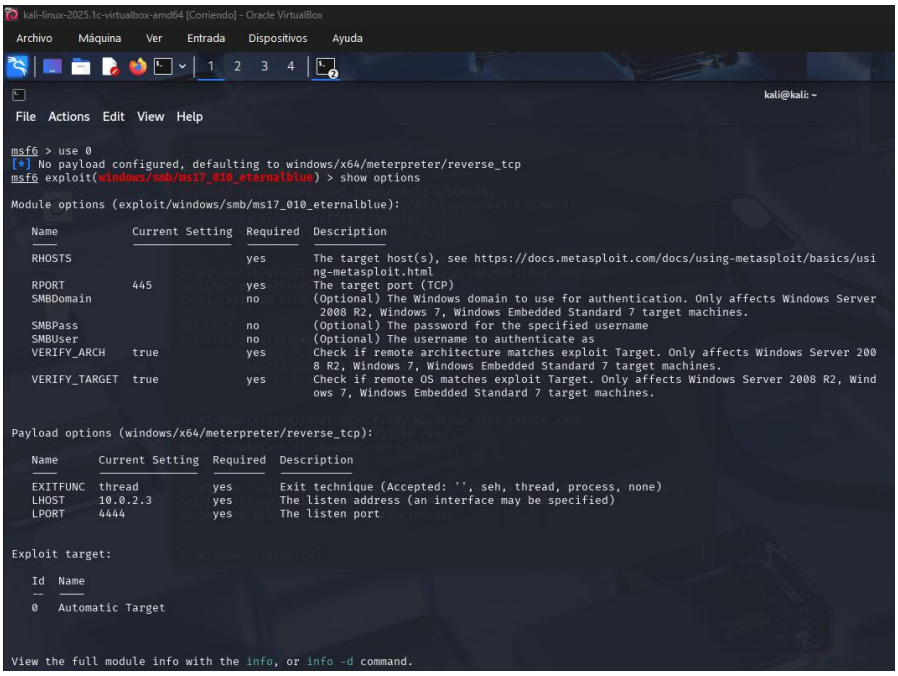
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla donde se consulta un exploit “ethernalblue”, allí también se despliega sus módulos.

Figura 21

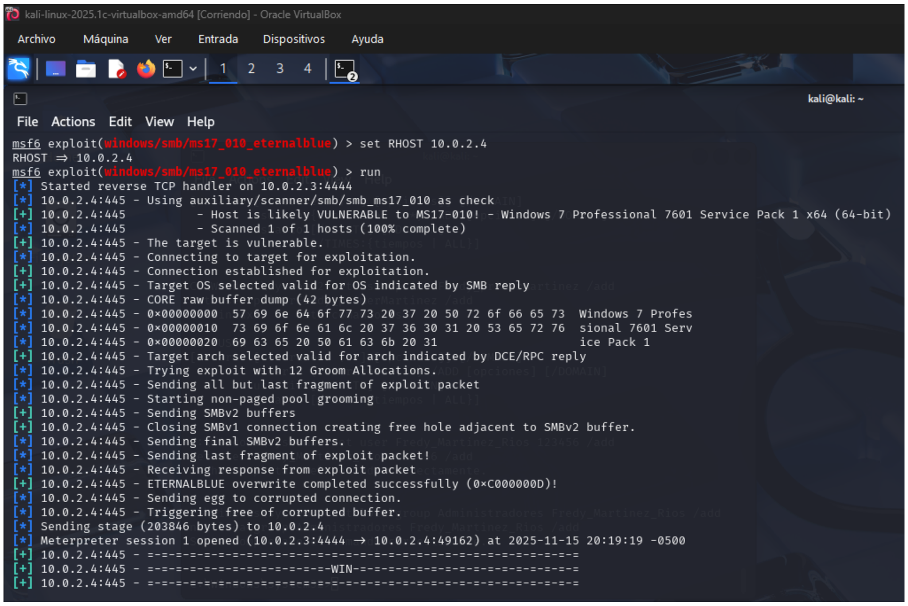
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla en donde se utiliza el módulo “0” y se despliega el comando “show options” para validar sus opciones y del payload.

Figura 22

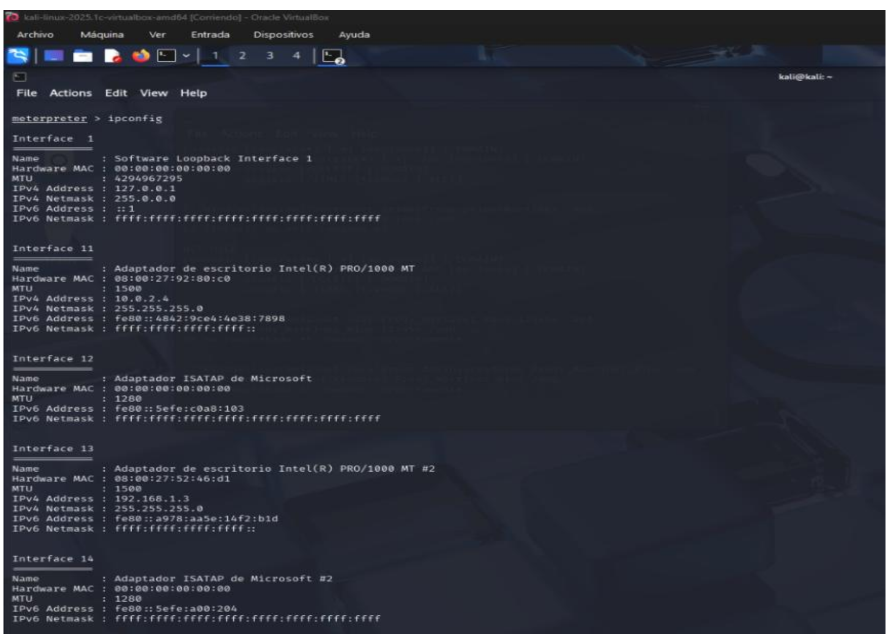
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla en donde se configura mediante el comando set RHOST y se inicia la explotación con el comando "run".

Figura 23

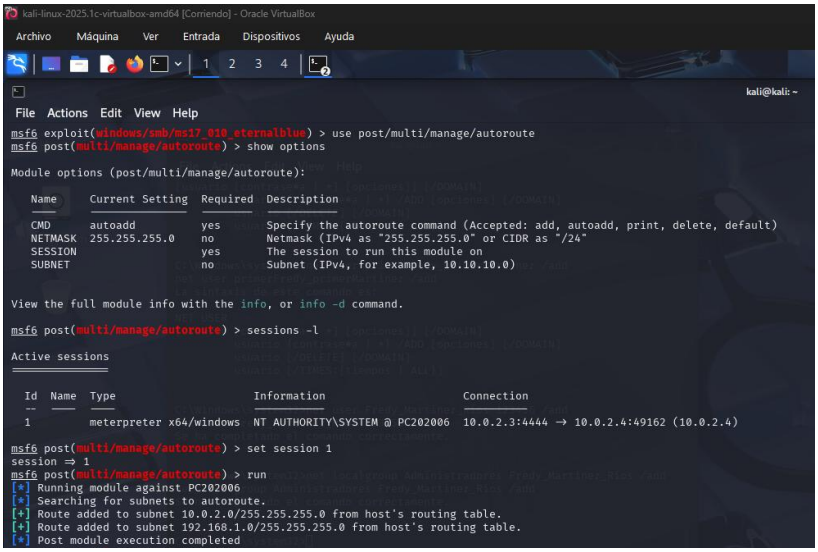
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla en donde se evidencia en la carga útil de ataque meterpreter el comando utilizado "ipconfig", en la interfaz 13 se puede observar la ip del host B, la cual corresponde al segmento 192.168.1.0.

Figura 24

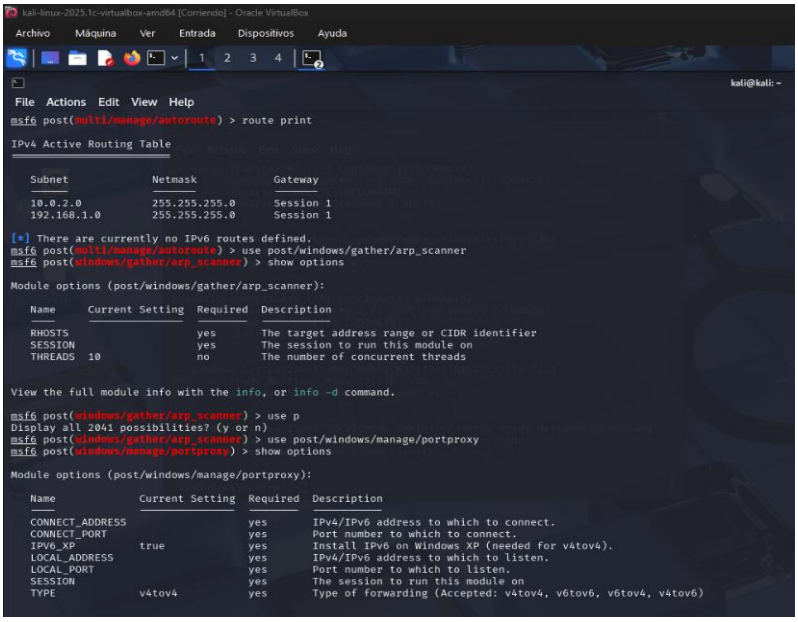
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla en donde se evidencia el empleo módulo post-explotación de Metasploit que se utiliza para agregar rutas de red automáticamente así mismo el comando sesión -l se utiliza para listar todas las sesiones activas que han sido abiertas durante este ejercicio de pentesting.

Figura 25

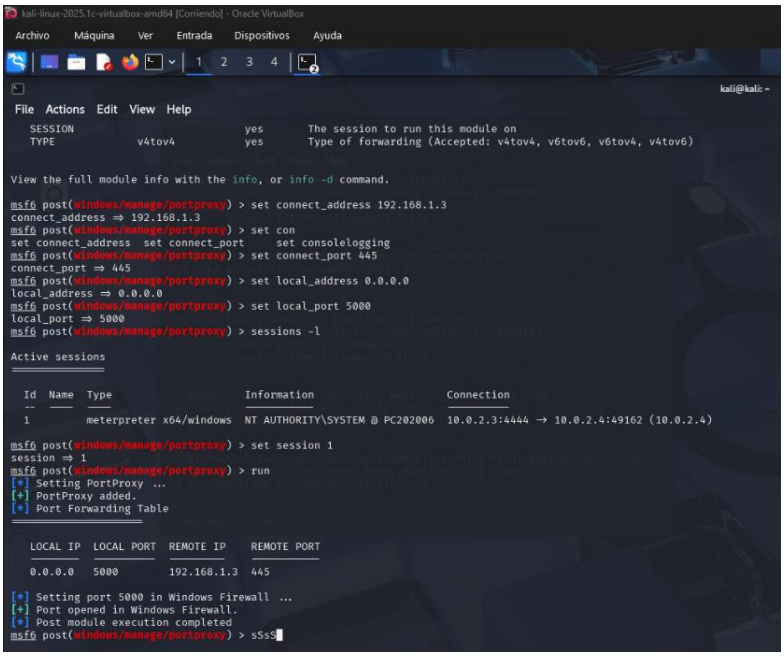
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla en donde se evidencia la tabla de ruteo y módulo de post-explotación de Metasploit que permite realizar un escaneo ARP desde una sesión comprometida en Windows.

Figura 26

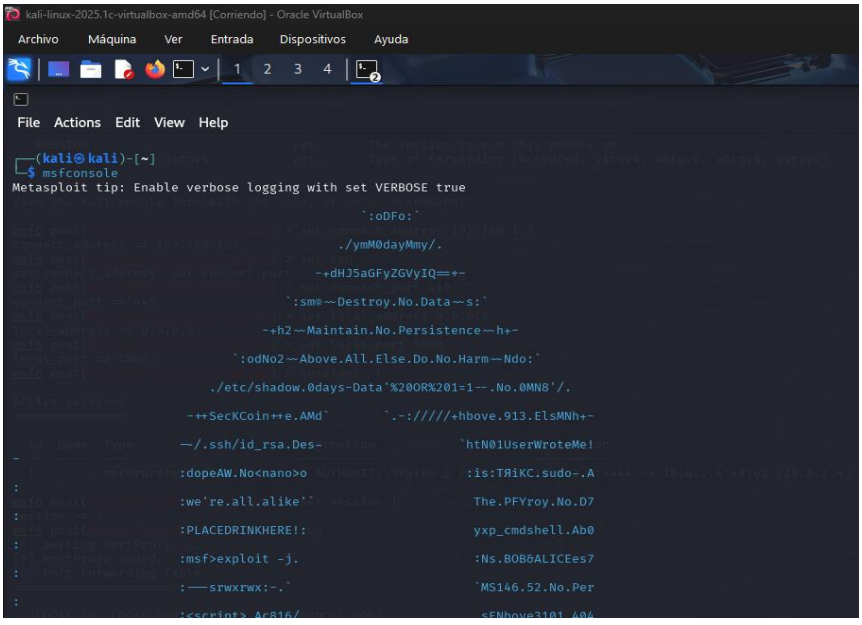
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla en donde se configuran todas las opciones para la explotación del módulo y posterior a ello se finaliza con el comando “run”.

Figura 27

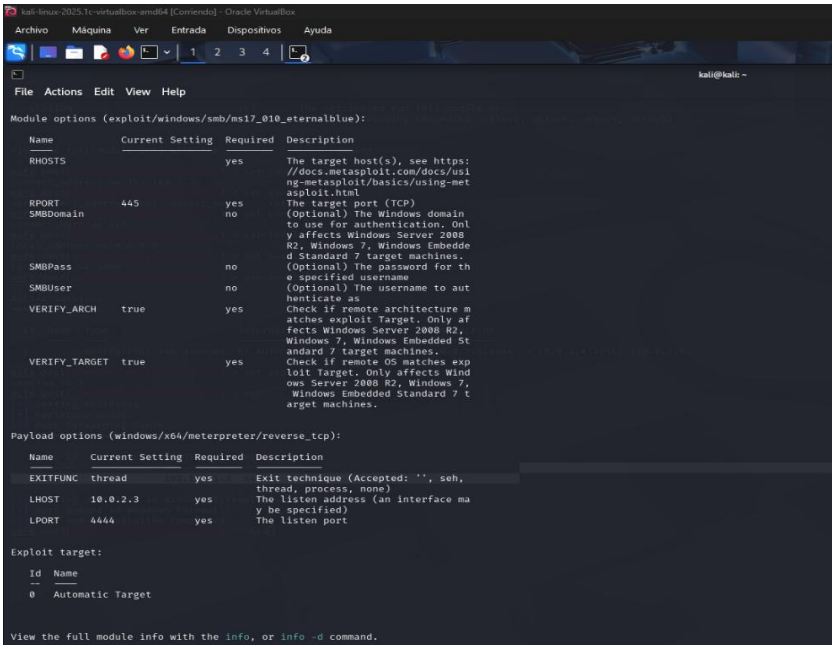
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla de Metasploit en una nueva Shell, donde se puede usar comandos para buscar exploits, cargar payloads, realizar escaneos y ejecutar ataques.

Figura 28

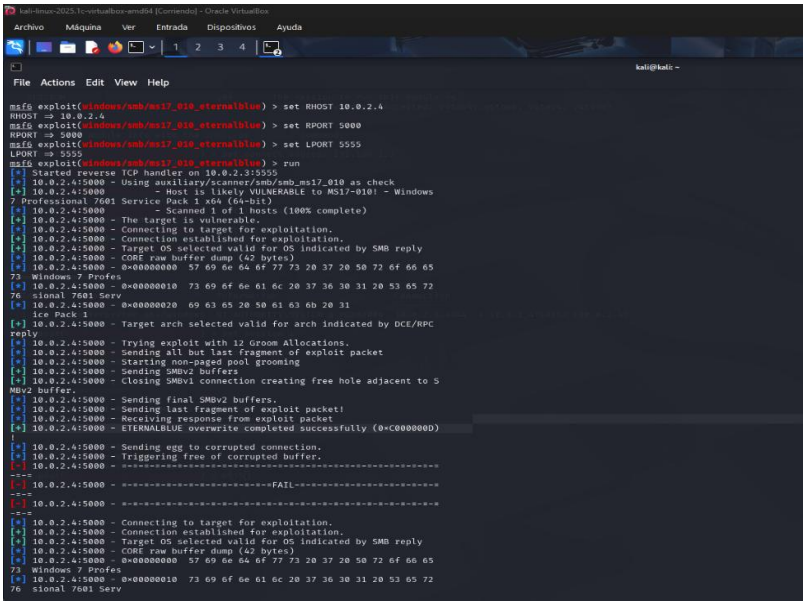
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla donde se consulta nuevamente en una Shell, el exploit “ethernalblue”, allí también se despliega sus módulos.

Figura 29

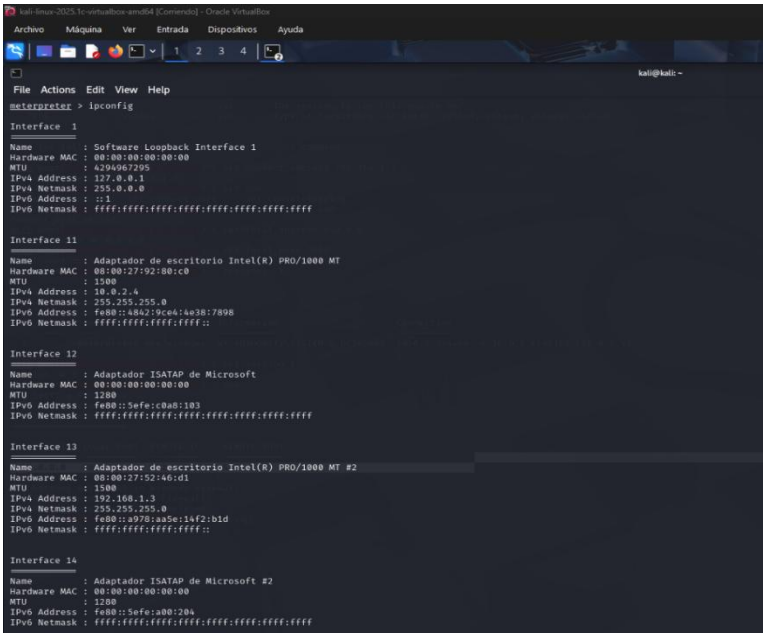
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla en donde se configura el módulo de eternalblue y el puerto a atacar para este caso el 5000, posterior se inicia con el ataque.

Figura 30

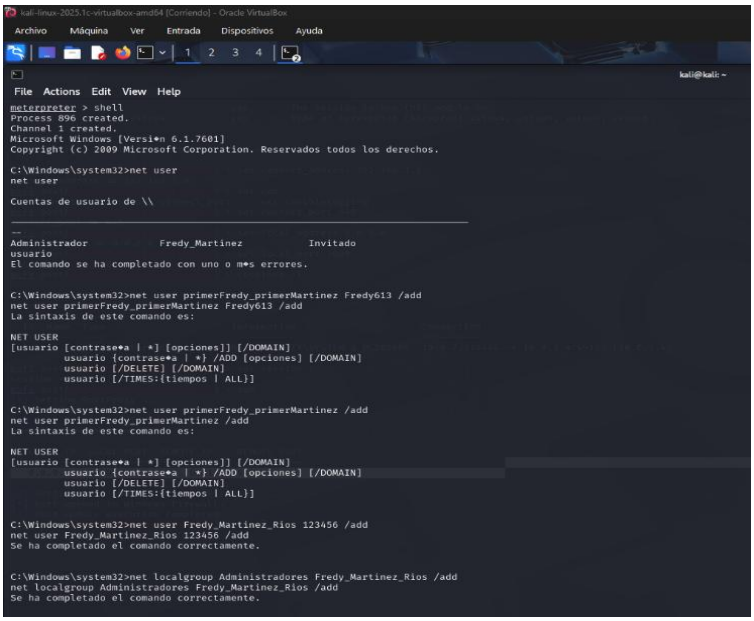
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla en donde se evidencia en la interface Nro 13 la ip 192.168.1.3 del Host B.

Figura 31

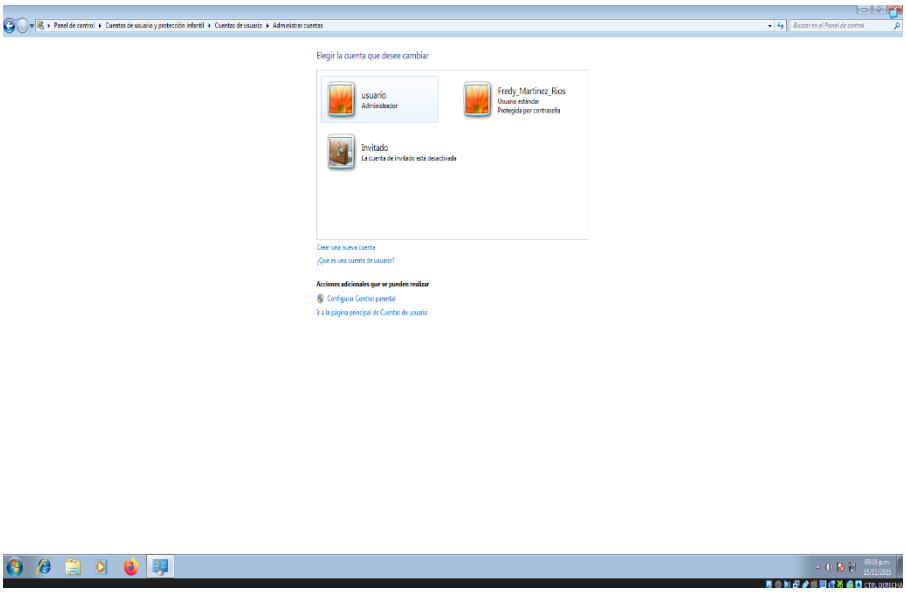
Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla en donde se inicia con una Shell en el Host B y como prueba de la explotación del pivoting se crea un usuario Administrador con el nombre Fredy_martinez_Rios

Figura 32

Interfaz de Metasploit Framework con Kali Linux (pivoting)



Nota. Captura de pantalla en donde se evidencia en el entorno Windows la creación del usuario con roles de Administrador en el Host B.

Nmap: (Network Mapper) es una herramienta de software libre ampliamente utilizada en el ámbito de la ciberseguridad y la administración de redes para la identificación, análisis y diagnóstico de dispositivos conectados a un entorno de red, su función principal consiste en realizar procesos de descubrimiento y auditoría mediante diferentes técnicas de escaneo que permiten obtener información detallada sobre los hosts activos, los puertos abiertos, los servicios en ejecución y posibles configuraciones vulnerables. (Shivanandhan, 2025)

Parrot: es un OS es una distribución del sistema operativo GNU/Linux orientada específicamente a actividades de ciberseguridad, análisis forense digital, auditorías de seguridad y desarrollo de software, desarrollado por la organización Parrot Security, este sistema se caracteriza por integrar un conjunto amplio de herramientas profesionales destinadas a la ejecución de pruebas de penetración, ingeniería inversa, análisis de vulnerabilidades y protección de la privacidad. (Altube, 2025)

Kali Linux: es una distribución del sistema operativo GNU/Linux diseñada específicamente para la realización de auditorías de seguridad, pruebas de penetración y análisis forense digital. Desarrollada y mantenida por la organización Offensive Security, esta distribución se ha consolidado como una de las herramientas más empleadas en el ámbito profesional y académico de la ciberseguridad debido a su robustez, versatilidad y amplio conjunto de utilidades preinstaladas. (School, 2025)

1. A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la Máquina - 1 Windows.

a) El anexo señala que SecureNova Labs detectó fugas de información originadas en una estación de trabajo Windows, este punto constituye el primer indicador crítico, pues sugiere la existencia de un compromiso previo en Host-A y la posible explotación de un vector de ataque que facilitó la exfiltración de datos, la detección de actividad anómala de salida suele asociarse a la ejecución de malware, abuso de procesos legítimos o explotación de aplicaciones vulnerables.

b) El documento indica que la imagen forense revela que la estación Windows tenía en ejecución una aplicación vulnerable, la cual se considera el punto de entrada más probable del atacante, este hallazgo es clave para la identificación del fallo, ya que permite delimitar el análisis al software expuesto y evaluar si dicha aplicación presentaba vulnerabilidades conocidas o configuraciones deficientes que facilitaron su explotación.

c) El anexo menciona que se encontraron rastros que evidencian la obtención de una shell remota, y un posterior escalamiento de privilegios.

Este conjunto de acciones confirma que el atacante no solo logró un acceso inicial, sino que también consolidó un control superior dentro del sistema operativo.

Dichas evidencias permiten inferir que la vulnerabilidad explotada otorgó un nivel de acceso suficiente para ejecutar comandos arbitrarios y elevar permisos, lo cual constituye un fallo de seguridad grave en la Máquina-1.

d) La presencia de un usuario con privilegios administrativos no autorizado constituye otra evidencia determinante, la creación de este tipo de cuentas es una técnica común para mantener persistencia y asegurar el control prolongado sobre un host comprometido.

Este dato es indispensable para determinar la profundidad del compromiso en Host-A y confirma que el atacante alcanzó privilegios de administrador, reforzando la hipótesis de explotación de una vulnerabilidad crítica en el sistema o aplicación afectada.

e) El documento señala actividades asociadas al pivoting desde Host-A hacia Host-B, lo que implica que el Host-A funcionó como punto de apoyo para extender el compromiso a otros sistemas de la red interna, este hallazgo contribuye a la identificación del fallo porque demuestra que el atacante: obtuvo control efectivo del Host-A, explotó la vulnerabilidad de manera exitosa, y utilizó los privilegios adquiridos para desplazarse lateralmente.

El movimiento lateral solo es posible cuando el host inicial presenta un fallo de seguridad explotable que permite el control total del sistema.

f) El anexo solicita que el equipo Red Team reproduzca: el vector de ataque, la explotación de la vulnerabilidad, el escalamiento de privilegios, y el pivoting hacia Host-B.

Esta instrucción confirma que el fallo de seguridad identificado está vinculado directamente a la explotación de la aplicación vulnerable en Host-A y que dicho comportamiento debe ser replicable para validar técnicamente la hipótesis del incidente.

2. ¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “Máquina - 1 Windows”? ¿Qué puerto abre la aplicación específica en el anexo?.

La herramienta que se empleó para poder identificar el fallo de seguridad es NMAP y de acuerdo con el escaneo detallado con el comando sudo nmap -sV -sC --script=vuln -p- a la Ip del host A, donde también se determinó que la aplicación Rejetto HFS - HTTP File Server tiene en estado abierto el puerto 80.

3. Explique con sus palabras y de manera específica cómo afecta el ataque a las máquinas (Windows) encontradas en la red: Haga uso de gráficos para explicar el ataque.

El ataque dirigido a las máquinas Windows identificadas en la red ocasiona un impacto significativo en varios niveles de seguridad: confidencialidad, integridad, disponibilidad y control operativo, el análisis del ataque permite comprender cómo un atacante, mediante la explotación de una aplicación vulnerable Rejetto HFS 2.3, la cual logra comprometer inicialmente el Host-A y posteriormente extenderse hacia el Host-B a través de técnicas de pivoting.

El atacante identifica que el Host-A tiene expuesto un servidor vulnerable Rejetto HFS 2.3 ejecutándose en el puerto 80/TCP, esta aplicación contiene la vulnerabilidad *CVE-2024-23692*, la cual permite ejecución remota no autenticado.

Figura 33

Ataque inicial a Host-A

Nota. Captura de pantalla en donde se evidencia que el atacante obtiene una shell remota con permisos del usuario que ejecuta el servicio.

Una vez controlado el Host-A, el atacante lo utiliza como puente pivoting para acceder al Host-B, el cual se encuentra en otro segmento de red inaccesible desde el equipo atacante, se emplean técnicas con el módulo de autoroute permite redirigir tráfico a través de HostA.

Figura 34

Proceso de Pivoting

Nota. Captura de pantalla en donde se evidencia que el atacante obtiene un punto de acceso adicional dentro de la red y se compromete completamente el segundo equipo sin exposición directa.

Análisis de respuesta al encontrarse un ataque en tiempo real con argumentos técnicos.

La detección de un ataque en tiempo real dentro de un entorno corporativo exige una respuesta inmediata, sistemática y técnicamente fundamentada, teniendo en cuenta el escenario propuesto implica que, uno como miembro del Blue Team debe actuar inicialmente sobre el host comprometido, utilizando herramientas de licencia de software libre libre y/o código abierto; que bajo esta premisa, la prioridad inicial consiste en confirmar la naturaleza del ataque, preservar la integridad de la evidencia y evitar que el incidente escale a otros sistemas de la organización. (Kotwani, 2023)

La primera acción que debe ejecutar el analista Blue Team al encontrarse con un ataque en tiempo real es determinar el estado actual del sistema comprometido, identificando procesos, conexiones de red, artefactos activos y el vector de persistencia, esta verificación inmediata

permite establecer si el atacante mantiene control del sistema y qué alcance tiene el compromiso. A continuación, algunos argumentos técnicos:

- Inspección de los procesos sospechosos en memoria RAM, recurso que mejor refleja la actividad en tiempo real de un sistema comprometido, la primera indagación técnica debe realizarse con herramientas para análisis de memoria como Volatility; el objetivo es identificar procesos sin firma digital, ejecutados desde rutas atípicas como por ejemplo "C:\Users\Public, Temp", esta evaluación responde a la necesidad de detectar actividad maliciosa activa, inyección de código, shells remotos o malware en ejecución.
- Verificación de conexiones de red activas y persistentes, determinando si el atacante mantiene un canal de comunicación activo, algunas de las herramientas empleadas son TCPView y Wireshark; se debe analizar Conexiones establecidas hacia direcciones Ip externas desconocidas, puertos abiertos inusuales o programas asociados a cada conexión, esto permite detectar reverse shells, RATs, túneles o tráfico C2.
- Evaluación del impacto en la red interna teniendo en cuenta que el escenario indica que el ataque podría estar afectando a la infraestructura interna de SecureNova Labs, es prioritario detectar si el equipo está realizando escaneo horizontal con herramientas como Nmap y ARP Sweep; el equipo actúa como pivot para comprometer otros hosts que se han ejecutado scripts automatizados como PowerShell Empire, Metasploit, entre otros; en este punto se revisan tablas ARP, registro de rutas, sniffing con Wireshark para tráfico anómalo interno.
- Validación de mecanismos de persistencia, el analista debe descartar que el atacante haya dejado persistencia mediante tareas programadas "schtasks y/o query", claves Run/RunOnce del registro, servicios creados recientemente y usuarios nuevos de privilegios elevados, es importante mencionar que es crítico eliminar persistencia antes de cualquier neutralización del ataque.

- Aislamiento del equipo siendo una acción inmediata de contención, una vez se verifica que el host está efectivamente comprometido, el primer paso operativo para contener el ataque es aislar el equipo de la red, evitando propagación sin apagarlo, para no destruir evidencia; algunos métodos de aplicación son desconectar el cable de red, deshabilitar el adaptador de red y aplicar reglas de firewall temporal de tipo restrictivas, que permite que el atacante pierda control sin comprometer la integridad del sistema para análisis posterior.

Medidas de hardenización para un ataque, teniendo en cuenta la maniobra ejecutada en el ejercicio de Red Team.

En el ejercicio Red Team se evidenció un conjunto de fallos críticos en la estación de trabajo Windows (Host-A) y en la infraestructura asociada, incluyendo la explotación de una aplicación vulnerable, obtención de una shell remota, escalamiento de privilegios, creación de cuentas administrativas no autorizadas y movimientos laterales hacia un servidor secundario (Host-B) desde donde se extrajo información sensible, dado que el objetivo del Blue Team es evitar que este tipo de ataque se repita, es necesario implementar un conjunto integral de medidas de hardenización a nivel de sistema operativo, aplicaciones, credenciales, red y monitoreo de la siguiente manera: (Chindrus, 2023)

Hardenización del sistema operativo mediante la gestión de parches y actualización de software, el ataque se originó debido a una aplicación vulnerable explotada para obtener Shell, para evitar este vector es posible implementar un proceso estricto de gestión de parches (Patch Management), automatizar actualizaciones mediante WSUS, Intune o scripts GPL, eliminar aplicaciones obsoletas o sin soporte.

Endurecimiento de servicios y deshabilitación de protocolos inseguros como SMBv1, RDP sin NLA, y servicios no utilizados, así mismo aplicar el principio de reducir superficie de

ataque desinstalando roles innecesarios y reforzar credenciales RDP mediante MFA y certificados.

Hardenización de aplicaciones y servicios expuestos mediante análisis de vulnerabilidades continuo con escaneos semanales con herramientas como OpenVAS, Wapiti, Nikto, así mismo aplicar virtualización o sandboxing a aplicaciones riesgosas y aislar aplicaciones inseguras para que un fallo no comprometa el sistema completo.

Endurecimiento de la red y segmentación, separando estaciones de trabajo, servidores, bases de datos y servicios críticos, bloqueando por defecto todo tráfico lateral innecesario, de igual manera aplicar reglas basadas en Zero Trust teniendo presente la siguiente frase “Nada se confía por defecto, todo se valida” e implementar IDS/IPS como Suricata o Snort para detectar pivoting o tráfico.

Diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos.

Los equipos Blue Team tanto como el equipo de respuesta a incidentes informáticos cumplen funciones fundamentales orientadas a la protección, contención y aseguramiento de los activos tecnológicos, sin embargo, aunque ambos comparten el objetivo general de fortalecer la postura de seguridad en las organizaciones, presentan diferencias claras en cuanto a su enfoque, alcance operativo y naturaleza de sus actividades.

El equipo Blue Team se caracteriza por ser un equipo permanente y proactivo, cuyo propósito principal es diseñar, implementar y mejorar continuamente los controles defensivos, dentro de sus funciones incluyen la monitorización de la red, análisis de vulnerabilidades, configuración segura de sistemas, gestión de parches, hardening, detección de anomalías y desarrollo de estrategias defensivas, este equipo trabaja de manera constante, incluso en ausencia

de incidentes activos, y su enfoque se centra en la prevención mediante la gestión del riesgo y el fortalecimiento de la infraestructura tecnológica.

El equipo de respuesta a incidentes informáticos actúa principalmente de forma reactiva, interviniendo cuando ocurre un evento de seguridad que compromete la confidencialidad, integridad o disponibilidad de los sistemas, dentro de su misión se orienta a la identificación, análisis, contención, erradicación y recuperación ante incidentes confirmados, además, documenta lecciones aprendidas y coordina acciones con otras áreas para evitar recurrencias, pero su activación se da esencialmente cuando existe una amenaza materializada o un incidente en curso.

En cuanto al alcance, el equipo Blue Team cubre un espectro más amplio y continuo de actividades defensivas y de mejora, mientras que el CSIRT se concentra en la gestión del ciclo de vida del incidente, desde su detección hasta su cierre formal, por ende el equipo Blue Team opera con una perspectiva táctica y estratégica de largo plazo, mientras que el CSIRT opera bajo presión, en tiempos reducidos y con procedimientos orientados a contener daños de manera inmediata.

Empleabilidad de un CIS "Center For Internet Security" dentro de un equipo Blue Team

Dentro de un equipo Blue Team, el Center for Internet Security - CIS se utiliza como un marco de referencia técnico y metodológico orientado al fortalecimiento de la postura defensiva de la organización, su principal finalidad es proporcionar estándares, guías y controles de seguridad que permitan establecer configuraciones seguras, reducir la superficie de ataque y garantizar una defensa proactiva basada en mejores prácticas internacionalmente aceptadas. (Security, 2021)

En este sentido, el CIS se emplea para implementar los “Critical Security Controls”, un conjunto priorizado de medidas diseñadas para prevenir, detectar y mitigar amenazas informáticas, estas directrices facilitan la identificación de activos, la gestión de vulnerabilidades, la implementación de controles de acceso y la protección de entornos críticos, contribuyendo así a la construcción de una arquitectura defensiva robusta y coherente. (Janwar, 2016)

Asimismo, el equipo Blue Team utiliza los CIS Benchmarks, los cuales consisten en guías detalladas de configuración segura para sistemas operativos, bases de datos, servicios en la nube, componentes de red y aplicaciones, estas guías permiten ejecutar procesos de hardening estandarizados, realizar auditorías de configuración y asegurar que las plataformas tecnológicas operen de acuerdo con parámetros de seguridad validados por la comunidad especializada.

Funciones y características principales de un SIEM.

Un Security Information and Event Management – SIEM, es una solución tecnológica fundamental dentro de la gestión de la ciberseguridad organizacional, su propósito es centralizar, analizar y correlacionar datos provenientes de distintos sistemas, con el fin de detectar amenazas, facilitar la respuesta a incidentes y fortalecer los mecanismos de defensa, estas herramientas se han convertido en un componente esencial dentro de los Centros de Operaciones de Seguridad - SOC, dada su capacidad para generar una visión unificada y en tiempo real del estado de seguridad de la infraestructura tecnológica, unas de las funciones principales del SIEM son:

- La recolección automatizada de registros provenientes de múltiples fuentes, como firewalls, servidores, sistemas operativos, aplicaciones, redes, soluciones antimalware e infraestructura en la nube.

- Incorpora motores de correlación que permiten relacionar eventos independientes para identificar patrones que podrían indicar un comportamiento malicioso.
- Analiza de manera continua los eventos entrantes para identificar actividades sospechosas o fuera de los parámetros normales.
- Identifica un evento o patrón que cumple con los criterios de riesgo, emite alertas priorizadas según criticidad y contexto.
- Análisis posterior a un incidente, permitiendo reconstruir la secuencia de eventos mediante, líneas de tiempo detalladas, búsquedas avanzadas y visualización de patrones de actividad.
- Módulos dedicados a la creación de informes automatizados para evidenciar el cumplimiento de políticas internas y regulaciones externas.

Herramientas de contención de ataques informáticos "hardware o software".

- Los Firewalls de Próxima Generación NGFW, constituyen una de las principales herramientas de contención dentro de la arquitectura de ciberseguridad, su función esencial radica en bloquear o limitar el tráfico malicioso mediante la aplicación de políticas estrictas de control en la capa de red, transporte y aplicación, a diferencia de los firewalls tradicionales, los NGFW integran funcionalidades avanzadas como inspección profunda de paquetes DPI, filtrado basado en aplicaciones, sistemas de prevención de intrusiones IPS y control granular de usuarios.

Desde la perspectiva de la contención, estos dispositivos permiten interrumpir el avance de un ataque mediante el bloqueo de direcciones IP maliciosas, cierre de puertos, restricción del acceso a servicios comprometidos y segmentación de red, reduciendo así la superficie de ataque y evitando la propagación lateral.

- Un Sistema de Prevención de Intrusiones IPS, se configura como una herramienta estrictamente orientada a la contención activa, a diferencia del IDS herramienta de detección, el IPS actúa en línea y es capaz de bloquear automáticamente el tráfico malicioso una vez detectado.

Su operación se basa en la correlación de firmas, análisis heurístico y técnicas de identificación de comportamientos no autorizados, en un escenario de ataque en tiempo real, el IPS puede detener ataques de explotación, mitigar intentos de escalamiento de privilegios, bloquear patrones de reconocimiento hostil y prevenir la ejecución de comandos maliciosos, actuando como una barrera inmediata entre el atacante y los activos críticos de la organización, el carácter reactivo y automático de este sistema lo posiciona como una herramienta esencial para la contención temprana de amenazas. (Grimes, 2022)

- Los sistemas de protección avanzada de endpoints, especialmente aquellos basados en tecnologías EDR (Endpoint Detection and Response) con capacidades de contención, permiten aislar equipos comprometidos del resto de la red, esta acción de aislamiento es considerada una de las medidas de contención más efectivas, ya que detiene la propagación del ataque, impide la comunicación con servidores de comando y control C2 y limita la capacidad del adversario para realizar movimientos laterales.

El aislamiento del endpoint puede realizarse de forma automática o manual, dependiendo de la criticidad del incidente, de igual manera, estas soluciones pueden suspender procesos maliciosos, bloquear cargas útiles payloads, revocar credenciales temporales o cerrar sesiones activas, con el fin de minimizar el daño mientras se realiza la remediación forense.

Evidencias de Sustentación

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

Video de sustentación del informe final: https://youtu.be/7JymotU-4NQ

Conclusiones

En relación con el objetivo general, orientado a analizar las capacidades técnicas, tácticas y operativas de los equipos Red Team y Blue Team, los resultados obtenidos evidencian que la integración de enfoques ofensivos y defensivos permite una evaluación integral de la postura de seguridad de la infraestructura analizada, así mismo el desarrollo del ejercicio práctico demostró cómo la identificación y explotación controlada de vulnerabilidades, junto con el análisis de los mecanismos de respuesta y contención, contribuyen de manera significativa al fortalecimiento de la seguridad informática.

Respecto al primer objetivo específico, centrado en el análisis de los fundamentos teóricos y normativos, se logró establecer una comprensión clara del marco legal colombiano aplicable a los delitos informáticos y la protección de datos personales, este análisis permitió delimitar las responsabilidades éticas y jurídicas del profesional en ciberseguridad, garantizando que las actividades de pentesting y auditoría se desarrollen dentro de un contexto legal y responsable.

En cumplimiento del segundo objetivo específico, relacionado con la identificación y evaluación de vulnerabilidades en un entorno simulado, el ejercicio de laboratorio permitió evidenciar fallos críticos en aplicaciones y configuraciones del sistema operativo, los cuales facilitaron accesos no autorizados, escalamiento de privilegios y movimientos laterales dentro de la red, es por ello que los hallazgos confirmaron la efectividad de las pruebas de penetración como mecanismo para validar el impacto real de las vulnerabilidades sobre la confidencialidad, integridad y disponibilidad de la información.

Finalmente, en correspondencia con el tercer objetivo específico, se formularon medidas de hardening y estrategias de mejora orientadas a la prevención, detección y respuesta ante

incidentes de seguridad, que dichas recomendaciones, fundamentadas en buenas prácticas y estándares reconocidos, permiten reducir la superficie de ataque y fortalecer la resiliencia de la infraestructura tecnológica frente a amenazas futuras.

En síntesis, el desarrollo del informe permitió dar cumplimiento integral de acuerdo a los objetivos planteados, articulando de manera coherente los aspectos teóricos, legales y prácticos, y aportando un análisis técnico riguroso que refuerza la importancia del trabajo coordinado entre los equipos Red Team y Blue Team en la gestión efectiva de la seguridad de la información..

Recomendaciones

Con base en los resultados obtenidos a lo largo del análisis teórico, normativo y práctico desarrollado en el presente informe, se formulan las siguientes recomendaciones orientadas al fortalecimiento de la seguridad de la información y a la mejora de las capacidades operativas de los equipos Red Team y Blue Team:

Fortalecer los procesos de gestión de vulnerabilidades, mediante la implementación de programas formales y continuos de identificación, evaluación y remediación de fallos de seguridad, estos procesos deben incluir escaneos periódicos, análisis manual de vulnerabilidades críticas y la priorización de riesgos de acuerdo con su impacto sobre la confidencialidad, integridad y disponibilidad de la información.

Implementar políticas estrictas de gestión de parches y actualización de software, con el fin de reducir la exposición a vulnerabilidades conocidas, así mismo se recomienda establecer cronogramas de actualización, controles de verificación y mecanismos de seguimiento que aseguren la eliminación oportuna de aplicaciones obsoletas o sin soporte, especialmente aquellas expuestas a redes internas o externas.

Reforzar las medidas de hardening en sistemas operativos, aplicaciones y servicios, aplicando configuraciones seguras basadas en estándares reconocidos como los CIS Benchmarks, incluyendo la deshabilitación de servicios innecesarios, el uso de protocolos seguros, la restricción de privilegios administrativos y la segmentación adecuada de la red para limitar el movimiento lateral de posibles atacantes.

Establecer lineamientos éticos y legales claros para las actividades de ciberseguridad, garantizando que las pruebas de penetración y auditorías se desarrollen bajo acuerdos formales que respeten la legislación vigente y los principios del código de ética profesional, así mismo, se

recomienda fortalecer la capacitación del personal en aspectos jurídicos y de responsabilidad profesional.

Referencias Bibliográficas

Altube, R. (12 de Noviembre de 2025). Obtenido de openwebinars: https://openwebinars.net/blog/parrot-os-que-es-y-caracteristicas-principales/

Alvarez Intriago, V. K. (2025). *semanticscholar*. Obtenido de https://www.semanticscholar.org/paper/PROPUESTA-DE-UNA-METODOLOG%C3%8DA-DE-PRUEBAS-DE-A-Intriago-Karina/f3be44039e5f4c1bfced6ad23455291b2a304c77?p2df

Andrade, S. H. (15 de Diciembre de 2025). Obtenido de secretariasenado: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Chindrus. (2023). *Securing the Network: A Red and Blue Cybersecurity Competition Case Study. Information*. Obtenido de https://doi-org.bibliotecavirtual.unad.edu.co/10.2478/bipie

Easttom, W. C. (2018). Obtenido de Computer security fundamentals: https://www.buscalibre.com.co/libro-computer-security-fundamentals/9780137984787/p/54282025

Grimes, R. A. (2022). Obtenido de Hacking the Hacker: Learn From the Experts Who Take Down Hackers: https://www.wiley.com/en-us/Hacking+the+Hacker%3A+Learn+From+the+Experts+Who+Take+Down+Hackers-p-9781119396215

Guarnizo Portela, M. P. (2024). *La naturaleza jurídica de los delitos informáticos en Colombia*. Obtenido de https://repository.unad.edu.co/handle/10596/41392

Incibe. (2025). Obtenido de Incibe: https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-23692

Janwar, I. (2016). Obtenido de academia: https://www.academia.edu/4903475/Insider_Threat_Protecting_The_Enterprise_From_Sabotage_Spying_And_Theft

Kotwani, B. (2023). Obtenido de Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield: https://www.researchgate.net/publication/376696305_Red_Teaming_vs_Blue_Teaming_A_Comparative_Analysis_of_CyberSecurity_Strategies_in_the_Digital_Battlefield

Lleras, V. (2025). Obtenido de Ley 842 de 2003: https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Luttgens, M. P. (2014). Obtenido de Incident Response & Computer Forensics, Third Edition: https://www.mheducation.com/highered/mhp/product/incident-response-computer-forensics-third-edition.html?viewOption=student

MINTIC, M. d. (2022). Obtenido de mintic: https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas-de-Privacidad-y-Condiciones-de-Uso

Palomo Luna, Z. H. (2024). Obtenido de Una mirada a metodologías para pruebas de penetración en ciberseguridad. Boletín Informativo CSIRT Académico UNAD: https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Boletin/Octubre_2024.pdf

PandaSecurity. (2018). Obtenido de Una herramienta muy valiosa para empresas: https://www.pandasecurity.com/es/mediacenter/retos-pymes-ciberseguridad/

rapid7. (2012). Obtenido de Metasploitable 2: https://docs.rapid7.com/metasploit/metasploitable-2/

School, E. I. (2025). Obtenido de campusciberseguridad: https://www.campusciberseguridad.com/blog/que-es-kali-linux-y-para-que-sirve/

Security, C. f. (2021). Obtenido de CIS Controls v8: Controls and safeguards for cyber defense: https://www.cisecurity.org

Shivanandhan, M. (2025). Obtenido de freecodecamp: https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

Wikimedia Foundation, I. (5 de Septiembre de 2025). Obtenido de wikipedia.org: https://en.wikipedia.org/wiki/HTTP_File_Server

Apéndices

Apéndice A

Resultado de revisión en Turnitin

Nota. En esta imagen se puede observar la revisión del trabajo por la herramienta Tunitin, para este caso arroja un porcentaje del 22% siendo la mayoría perteneciente a la estructura de las preguntas de las guias.