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

Dany Fernando Arevalo Castellanos

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Resumen

El presente informe técnico integra el análisis, desarrollo y resultados de las Etapas 1 a 4 del laboratorio de ciberseguridad, las cuales abarcan las actividades de reconocimiento, análisis de vulnerabilidades, ejecución del ataque por parte del Red Team y las acciones defensivas implementadas por el Blue Team; adicionalmente, con base en el escenario descrito en el Anexo 6 – Etapa 5, se consolidan y articulan las estrategias ofensivas y defensivas aplicadas, correlacionando la cadena de ataque, el movimiento lateral, los indicadores de compromiso y las estrategias de detección, contención y hardenización, para finalmente presentar conclusiones y recomendaciones orientadas al fortalecimiento de la postura de ciberseguridad en entornos corporativos tanto simulados como reales, alineadas con estándares y buenas prácticas como CIS Benchmarks, CCN-STIC, NIST y los lineamientos del CSIRT Académico UNAD.

***Palabras clave*:** Blue Team, hardenización, incidentes, Red Team, vulnerabilidades.

Abstract

This technical report integrates the analysis, development, and results of Stages 1 to 4 of the cybersecurity laboratory, which include reconnaissance activities, vulnerability analysis, Red Team attack execution, and defensive actions carried out by the Blue Team; additionally, based on the scenario described in Annex 6 – Stage 5, the offensive and defensive strategies applied are consolidated and articulated, correlating the attack chain, lateral movement, indicators of compromise, and detection, containment, and hardening strategies, in order to present conclusions and recommendations aimed at strengthening the cybersecurity posture in both simulated and real corporate environments, aligned with standards and best practices such as CIS Benchmarks, CCN-STIC, NIST, and the guidelines of the UNAD Academic CSIRT.

***Keywords*:** Blue Team, hardening, incidents, Red Team, vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Análisis Forense Digital:

Disciplina encargada de identificar, preservar y examinar evidencia digital para reconstruir incidentes de seguridad.

Blue Team:

Equipo defensivo responsable de monitorear, detectar y responder a incidentes de ciberseguridad dentro de una organización.

Cadena de Custodia:

Proceso documentado para preservar la integridad de la evidencia digital desde su recolección hasta su análisis.

Ciberseguridad:

Conjunto de prácticas, tecnologías y procesos orientados a proteger sistemas, redes y datos de accesos o daños no autorizados.

Contención:

Acciones destinadas a frenar la propagación de un incidente de seguridad y limitar su impacto.

Correlación de Eventos:

Proceso mediante el cual un SIEM relaciona múltiples eventos para identificar patrones sospechosos o ataques.

Escalamiento de Privilegios:

Técnica mediante la cual un atacante incrementa sus permisos dentro de un sistema.

Exploit:

Software o técnica que aprovecha una vulnerabilidad para ejecutar acciones no autorizadas en un sistema.

Firewall:

Sistema que filtra el tráfico de red siguiendo reglas predefinidas para proteger equipos y redes.

Hardening:

Conjunto de medidas para fortalecer la seguridad mediante configuración segura, eliminación de servicios innecesarios y políticas de control.

Host Comprometido:

Equipo que ha sido vulnerado o manipulado por un atacante, perdiendo su integridad o control.

IDS (Intrusion Detection System):

Sistema que detecta actividades sospechosas monitoreando tráfico de red o registros del sistema.

IPS (Intrusion Prevention System):

Sistema que, además de detectar, puede bloquear tráfico o actividades consideradas maliciosas.

Indicador de Compromiso (IoC):

Evidencia que sugiere que un sistema ha sido afectado por actividades maliciosas.

Lateral Movement (Movimiento Lateral):

Técnica en la que un atacante se desplaza entre sistemas dentro de una red comprometida.

Log:

Registro generado por aplicaciones, sistemas o dispositivos que documenta eventos relevantes para auditoría o análisis.

Malware:

Software malicioso diseñado para causar daño, robar información o comprometer sistemas.

Pentesting:

Prueba controlada que simula ataques reales para identificar y validar vulnerabilidades en sistemas y redes.

Persistencia:

Mecanismo usado por un atacante para mantener acceso continuo a un sistema comprometido, incluso tras reinicios.

Pivoting:

Técnica de ataque que utiliza un host comprometido como puente hacia otras máquinas dentro de la red.

Política de Contraseñas:

Conjunto de reglas que definen requisitos de complejidad, longitud y mantenimiento seguro de credenciales.

Privilegios Mínimos:

Principio de seguridad que establece que los usuarios deben tener únicamente los permisos estrictamente necesarios para realizar sus funciones.

Red Team:

Equipo ofensivo especializado en simular ataques reales para evaluar la resiliencia de la organización frente a amenazas.

RCE (Remote Code Execution):

Vulnerabilidad que permite ejecutar código remotamente en un sistema objetivo sin autorización.

Respuesta a Incidentes:

Proceso estructurado para gestionar incidentes de seguridad mediante detección, análisis, contención, erradicación y recuperación.

Riesgo Residual:

Riesgo que permanece después de aplicar controles o medidas de mitigación.

Segmentación de Red:

División de una red en zonas aisladas para limitar el movimiento lateral de atacantes.

SIEM (Security Information and Event Management):

Plataforma que recolecta, analiza y correlaciona eventos de seguridad para facilitar la detección y respuesta ante incidentes.

Vulnerabilidad:

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

Introducción

Esta etapa integra los resultados ofensivos y defensivos obtenidos durante las actividades de Red Team y Blue Team. El ataque ejecutado sobre la Máquina 1 mediante un servicio vulnerable expuesto que permitió reconstruir la cadena de compromiso, identificar debilidades críticas y evaluar la capacidad defensiva del entorno mediante acciones de detección, contención, análisis y hardenización. Este informe consolida las estrategias aplicadas durante las Etapas 1 a 4, articulando los aspectos técnicos, éticos y normativos para fortalecer la postura de ciberseguridad del entorno simulado.

Justificación

La construcción de este informe es esencial para comprender de manera integrada cómo interactúan las actividades ofensivas y defensivas dentro de un entorno de ciberseguridad. A partir del ataque ejecutado por el Red Team y la respuesta del Blue Team, se evalúan las debilidades del sistema, la efectividad de los controles técnicos y la necesidad de mejorar estrategias de seguridad para reducir la superficie de ataque, aumentar la capacidad de detección y garantizar la continuidad operativa. Asimismo, se justifica por el componente educativo que permite al estudiante dominar conceptos aplicados de reconocimiento, explotación, respuesta a incidentes y análisis forense.

Objetivos

Objetivo General

Analizar y articular de manera integral las estrategias ofensivas (Red Team) y defensivas (Blue Team) desarrolladas en las etapas anteriores del componente práctico, con el fin de evaluar la seguridad del entorno simulado, identificar brechas críticas, fortalecer los mecanismos de detección y respuesta, y proponer mejoras técnicas, legales y procedimentales que optimicen la postura de ciberseguridad de la organización.

Objetivos Específicos

Describir y correlacionar las técnicas, herramientas y hallazgos del Red Team, destacando el vector de ataque explotado, la cadena de compromiso y las evidencias forenses obtenidas durante las fases de reconocimiento, explotación y movimiento lateral.

Evaluar la efectividad de las acciones defensivas implementadas por el Blue Team, analizando los mecanismos de detección, contención, hardening y monitoreo aplicados, y relacionándolos directamente con los riesgos materializados por el ataque.

Integrar un análisis técnico de las Etapas 1 a 4, identificando patrones, vulnerabilidades recurrentes, indicadores de compromiso (IoC) y oportunidades de mejora a nivel de arquitectura, políticas, segmentación y controles de seguridad.

Incorporar consideraciones éticas y legales, analizando cómo las actividades de Red Team y Blue Team deben alinearse con normativas, buenas prácticas y marcos de actuación como NIST, CIS, CCN-STIC y los lineamientos de gestión de incidentes del CSIRT Académico UNAD.

Desarrollo del Informe

Estrategias Red Team

SecureNova Labs implementó una estrategia de Red Team diseñada para poner a prueba rigurosamente la seguridad interna de una infraestructura empresarial simulada. Este ejercicio se centró en replicar meticulosamente las Tácticas, Técnicas y Procedimientos (TTPs) empleados por atacantes profesionales. Las acciones ofensivas ejecutadas fueron cruciales para descubrir fallos de seguridad críticos, confirmar la viabilidad de su explotación y cuantificar el daño potencial que un adversario real podría infligir a los sistemas de la organización. A continuación, se detalla el despliegue de las estrategias utilizadas en este escenario ofensivo.

Las estrategias aplicadas por el Red Team siguieron un flujo metodológico estructurado acorde con las fases tradicionales de un ejercicio de intrusión (reconocimiento → explotación → post-explotación → movimiento lateral → prueba de control). A continuación, se describen de forma ampliada:

Escenario inicial

Se propone investigar un escenario de compromiso controlado donde se identificó una potencial exfiltración de información. El incidente inicial se rastreó hasta una *workstation* Windows (Host-A). La investigación inicial revela una cadena de eventos maliciosos: una aplicación comprometida fue explotada para establecer una puerta trasera remota, permitiendo la ejecución de comandos y la elevación de permisos, lo que derivó en la creación subrepticia de una cuenta administrativa.

Posteriormente, se observaron trazas de expansión de la brecha hacia el servidor secundario (Host-B) para acceder a los datos críticos. Para verificar el *modus operandi* del adversario y obtener una comprensión profunda del ataque, se recreará el entorno exacto utilizando máquinas virtuales aisladas. Esto permitirá validar cada paso de la intrusión, generar

la documentación técnica pertinente, establecer una cronología forense y articular un programa de remediación robusto

Reconocimiento activo y pasivo

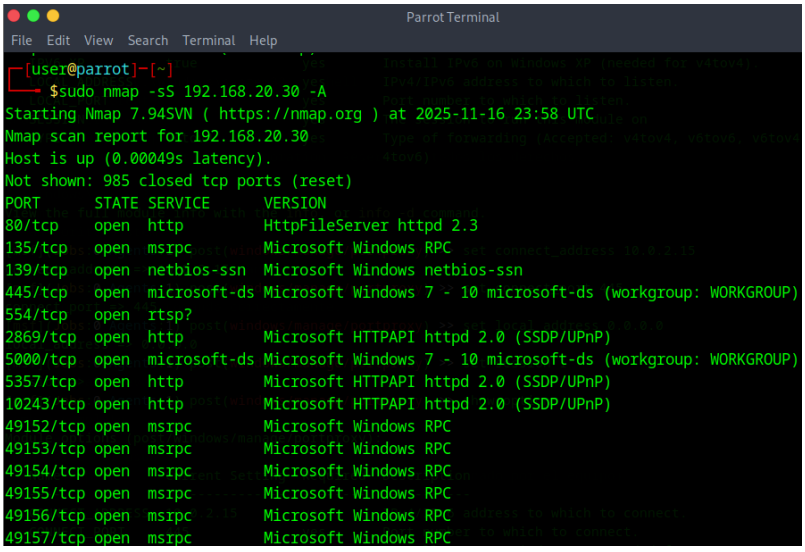
El Red Team inició con la recolección de información de la infraestructura simulada, utilizando técnicas pasivas (observación de ARP, identificación de servicios visibles sin interacción directa) y técnicas activas como:

- *Nmap* para obtención de huellas del sistema operativo (OS fingerprinting) y versiones de servicios.

El objetivo de esta fase fue mapear la superficie de ataque e identificar máquinas potencialmente vulnerables sin generar alertas tempranas.Una vez iniciado el aplicativo se realiza un escaneo con nmap desde parrot hacía el Host_A con el comando sudo nmap -sS 192.168.20.30 -A,

Figura 1

Escaneo con nmap desde Parrot hacia el Host_A



Fuente: Autoría propia

Resultado del Escaneo Nmap

El comando ejecutado (sudo nmap -sS 192.168.20.30 -A) reveló la siguiente información crítica sobre el Host-A (IP $192.168.20.30$):

- Puerto Abierto: TCP/80.
- Servicio Identificado: HttpFileServer (HFS), correspondiente a Rejetto.
- Versión Específica: HFS 2.3.

La Vulnerabilidad Crítica (RCE).

La identificación de HttpFileServer (HFS) versión 2.3 es el hallazgo clave que justifica el vector de ataque del Red Team.

- Naturaleza de HFS: Este software es una aplicación legítima diseñada para compartir archivos mediante protocolo HTTP de manera sencilla.
- La Debilidad (RCE): La versión HFS 2.3 contiene una vulnerabilidad de Ejecución Remota de Código (RCE) bien documentada (a menudo referenciada con el CVE respectivo o conocida por el módulo de Metasploit hfs_exec).

Esta vulnerabilidad RCE permite al atacante inyectar comandos arbitrarios en el sistema operativo del Host-A a través de la interfaz web de HFS, generalmente manipulando la función de búsqueda (o *search*). Esta explotación es el punto de partida que le otorga al atacante el acceso inicial no autorizado y la capacidad de iniciar la cadena de explotación (ejecución de comandos, escalada de privilegios y movimiento lateral), tal como se describió en la fase anterior del análisis.

Explotación del servicio HFS (RCE)

El Red Team utilizó el módulo de Metasploit: exploit/windows/http/rejetto_hfs_exec

Este módulo aprovecha el manejo inseguro de parámetros en la aplicación HFS para ejecutar comandos arbitrarios en el sistema objetivo.

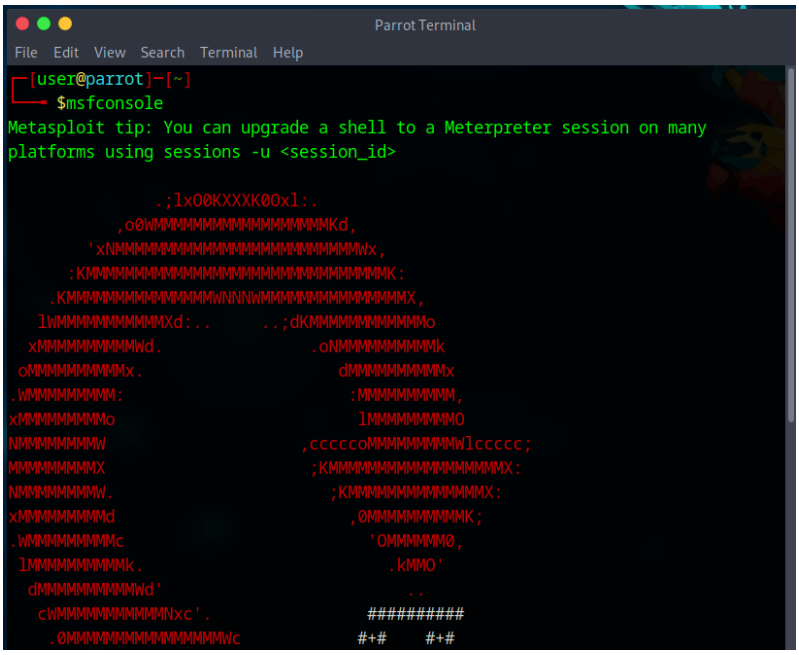
Resultados principales:

- Ejecución de payload remoto (reverse shell).
- Validación de que el servicio HFS no tenía protecciones de sandboxing ni restricciones ACL.

Esta explotación permitió ejecución remota de código (RCE), confirmando el vector inicial de fuga de información identificado en el escenario.

Figura 2

Ejecución de Metasploit en Parrot

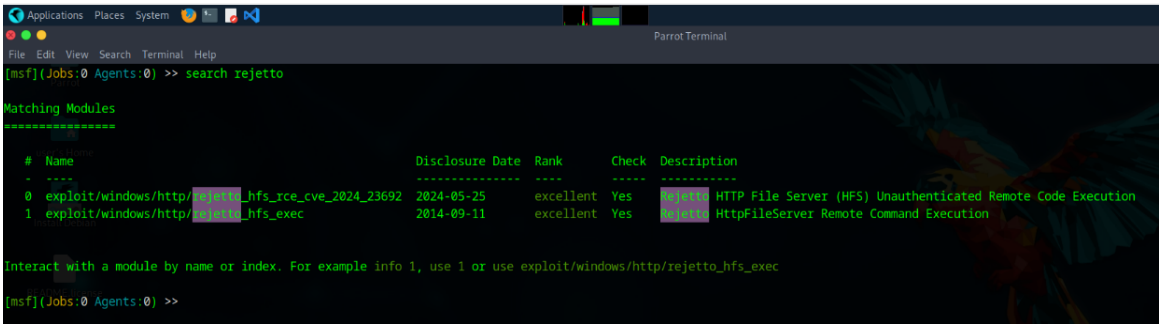


Fuente: Autoría propia

Se evidencian dos vulnerabilidades conocidas para la aplicación Rejetto (Figura 3). Con el comando use 1, se ingresa a la 1 y se da aplica un show options para mirar sus parámetros de configuración (Figura 4).

Figura 3

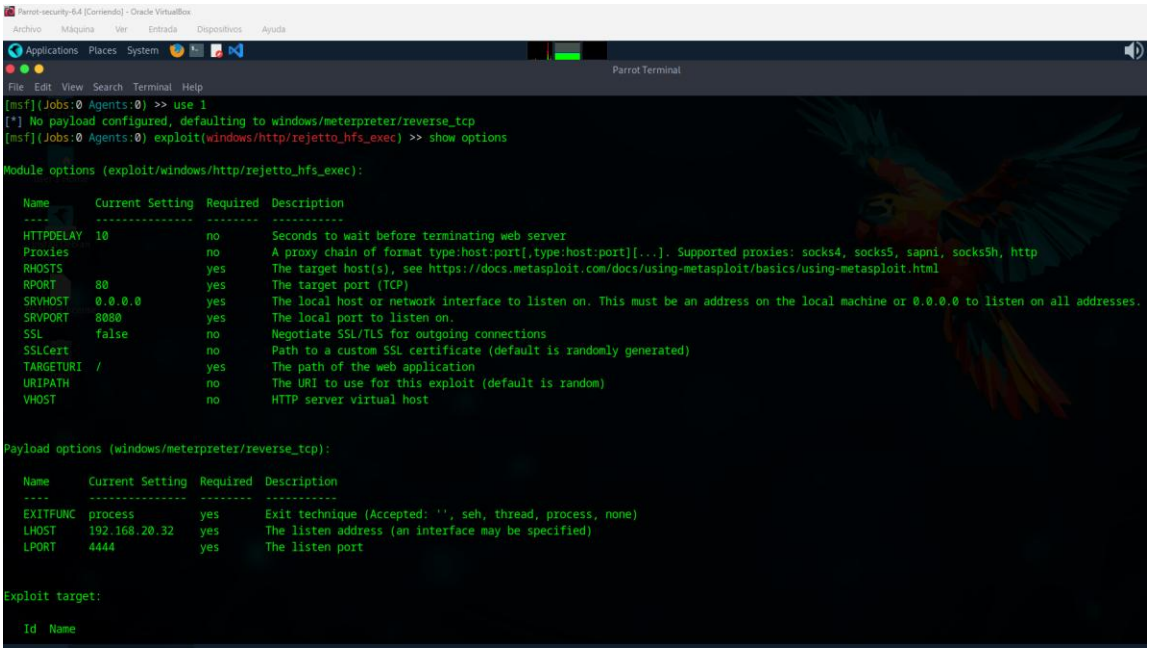
Ejecución comando search rejetto



Fuente: Autoría propia

Figura 4

Ejecución comando show options

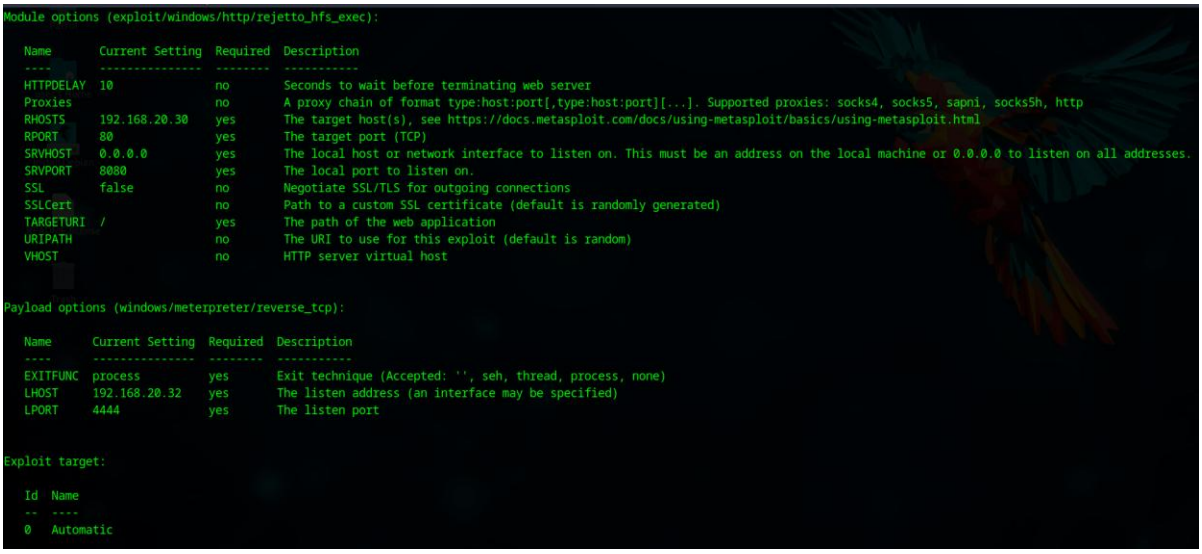


Fuente: Autoría propia

Se configura con set rhosts 192.168.20.30 la IP para realiza el ataque al Host_A por el puerto TCP/80, visualizados con show options (Figura 5).

Figura 5

Visualización de parámetros exploit 1



Fuente: Autoría propia

Establecimiento de sesión Meterpreter

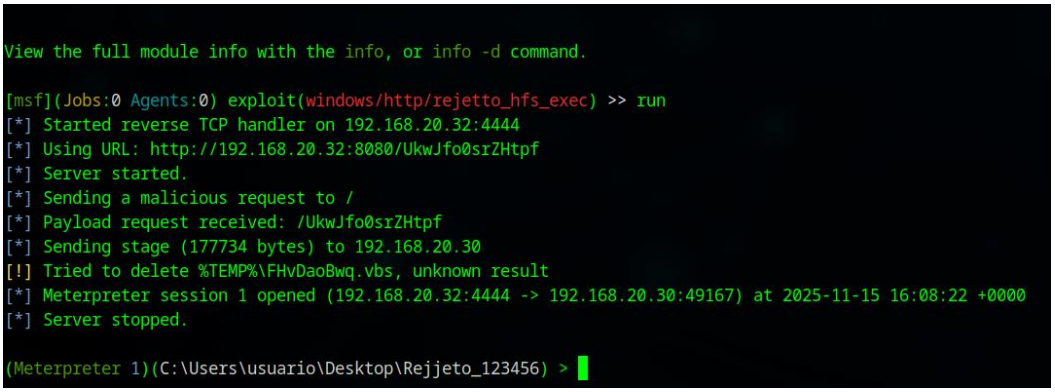
Tras la explotación, se obtuvo una sesión Meterpreter, permitiendo al Red Team:

- Interactuar con el sistema comprometido.
- Obtener privilegios del usuario en ejecución.
- Ejecutar comandos locales y herramientas de post-explotación.
- Cargar módulos adicionales (mimikatz, enum_shares, network_discovery, etc.).

Meterpreter permitió un control total de Host-A con capacidades avanzadas de evasión, carga dinámica y ocultamiento.

Figura 6

Ejecución exploit y acceso al Host_A

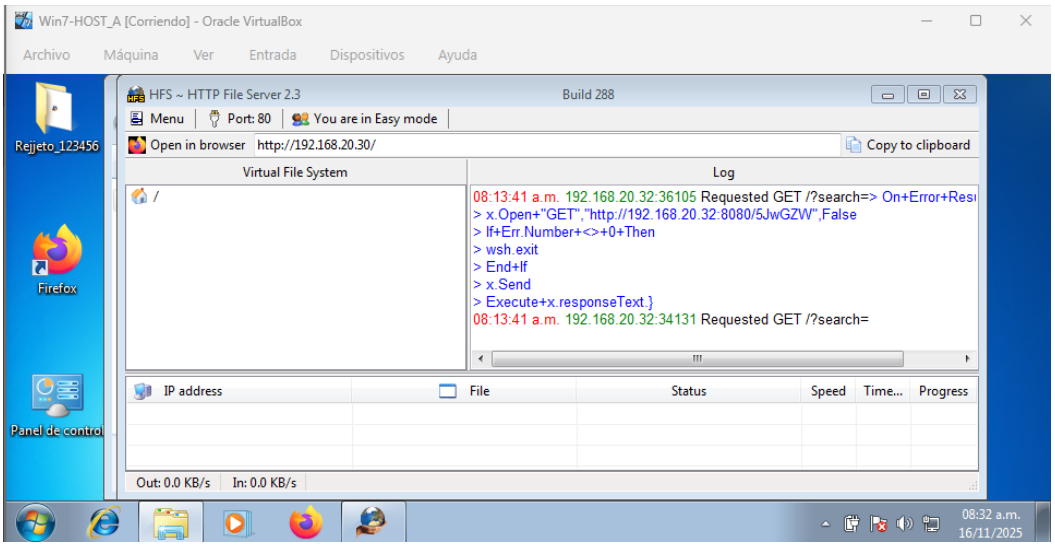


Fuente: Autoría propia

Se evidencia en la aplicación rejetto en el Host_A, registros de la acción realizada, mostrando que se tuvo acceso a la máquina (Figura 15).

Figura 7

Registros del acceso en aplicación rejetto en Host_A



Fuente: Autoría propia

Enumeración interna del sistema y la red

Una vez dentro de Host-A, la enumeración incluyó:

Enumeración del sistema local

- Listado de usuarios y grupos.
- Identificación de procesos en ejecución.
- Revisión de servicios instalados.
- Verificación de permisos.

Enumeración de red

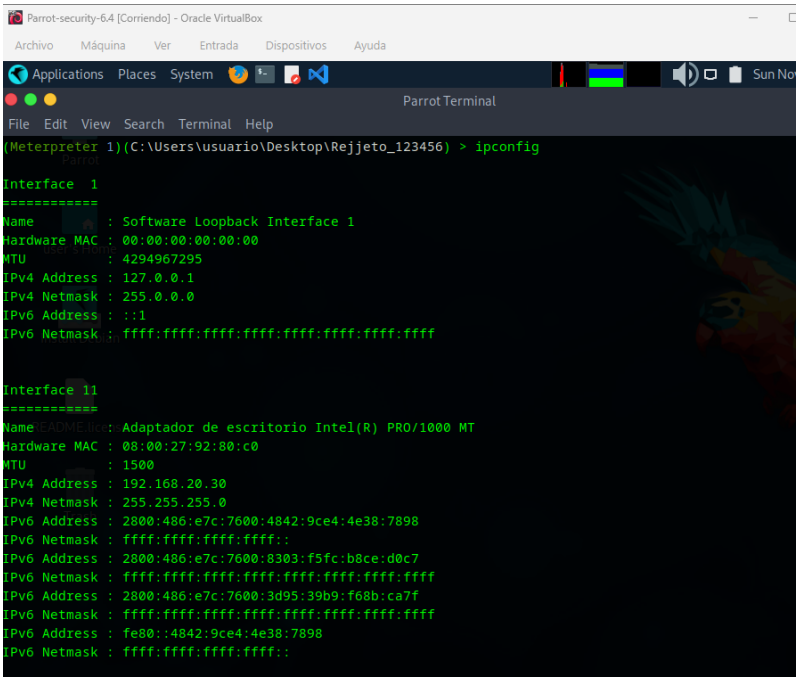
- Identificación de otras máquinas disponibles en la red interna.
- Descubrimiento del **Host-B** mediante rutas internas.
- Validación de puertos y servicios expuestos, principalmente: SMB en puerto 445

y uso de SMBv1, lo cual indicó alto riesgo.

Estos resultados motivaron el uso de pivoting para llegar a Host-B.

Figura 8

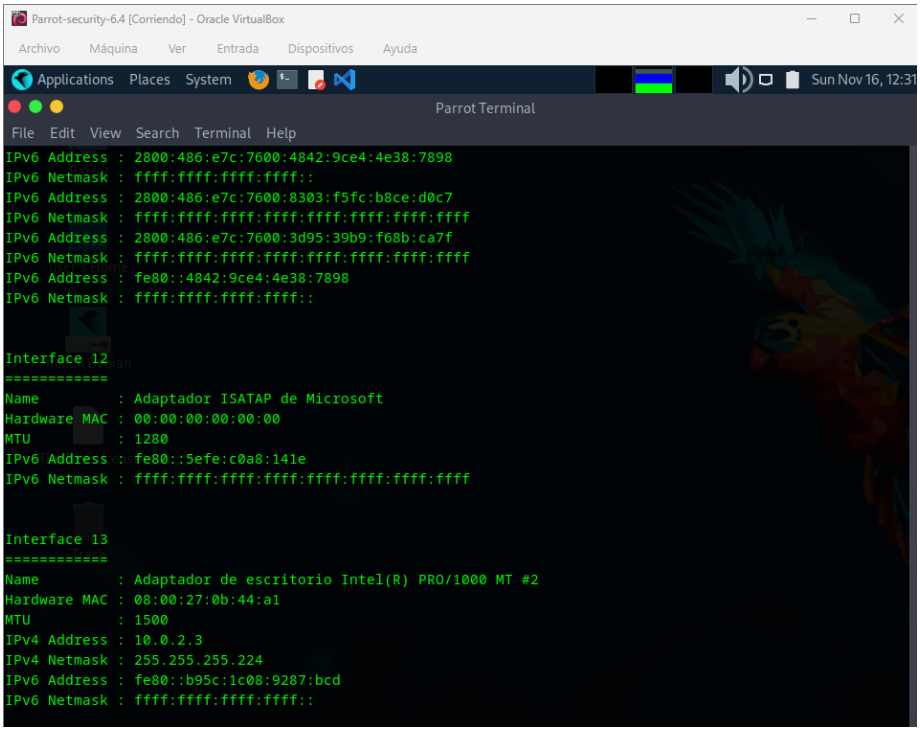
Ipconfig adaptador 1 IP 192.168.20.30



Fuente: Autoría propia

Figura 9

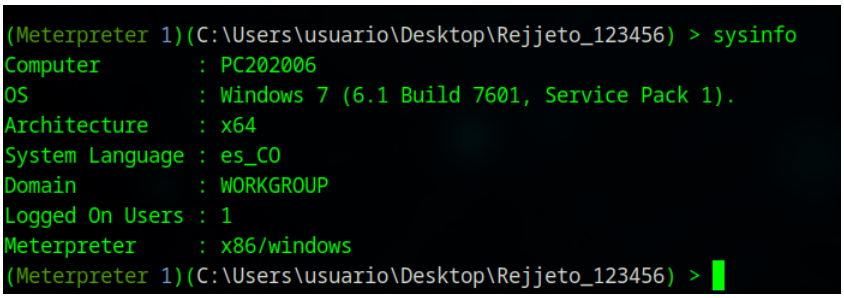
Ipconfig adaptador 2 IP 10.0.2.3



Fuente: Autoría propia

Figura 10

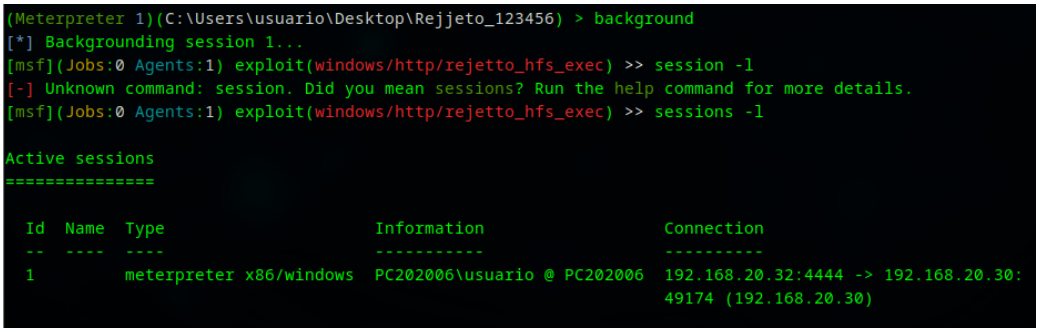
Comando Sysinfo



Fuente: Autoría propia

Figura 11

Comando background y verificación de sesiones activas



Fuente: Autoría propia

Pivoting hacia Host-B

Mediante los comandos de Metasploit:

- autoroute add
- portfwd add

El Red Team estableció rutas persistentes para que el tráfico hacia Host-B se canalizara a través de Host-A, convirtiéndolo en un pivote.

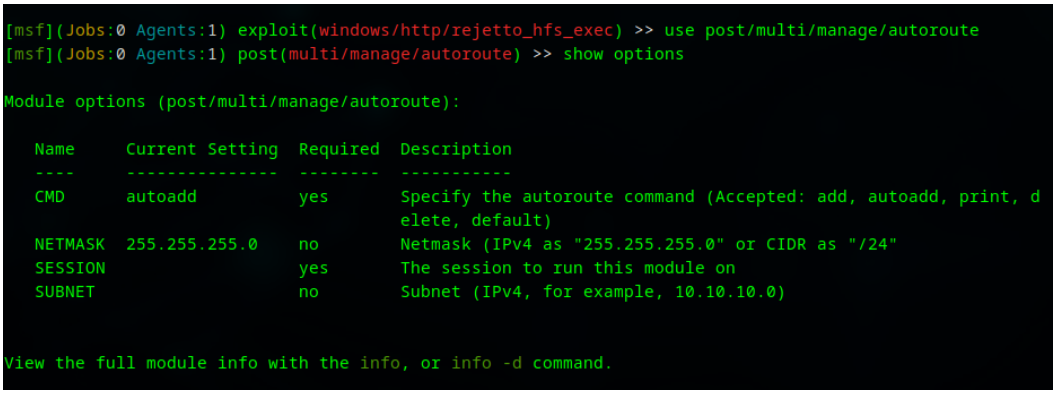
Con esta técnica, el atacante logró:

- Redirigir tráfico SMB hacia la red interna.
- Ejecutar ataques desde una posición dentro de la red.
- Eludir controles perimetrales o filtros externos.

Esta fase demostró la importancia de segmentación de red y firewalls internos, los cuales estaban ausentes.

Figura 12

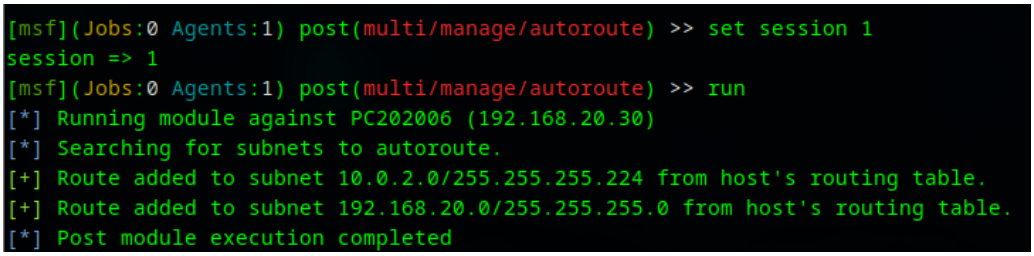
Comando use post/multi/manage/autoroute



Fuente: Autoría propia

Figura 13

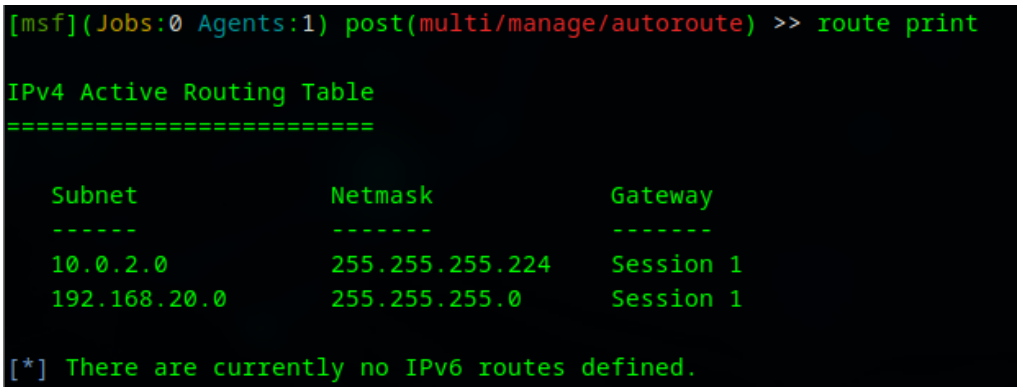
Comando set session 1 y ejecución para agregar las rutas



Fuente: Autoría propia

Figura 14

Comando route print para observar las rutas agregadas sesión 1



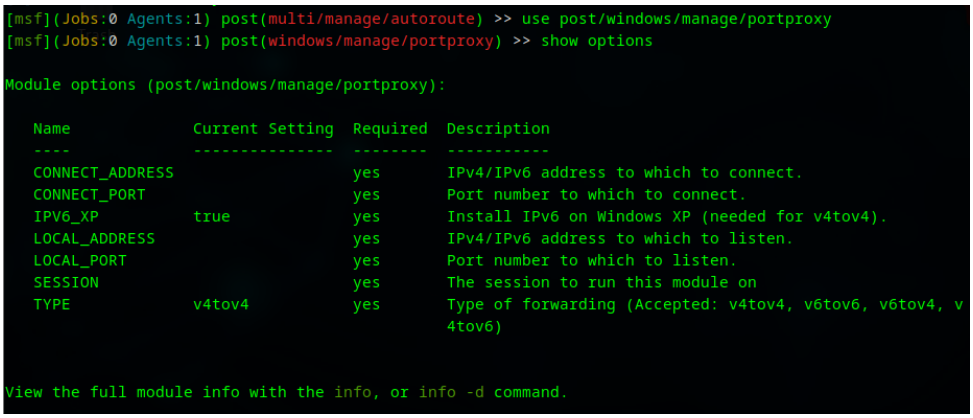
Fuente: Autoría propia

Con el módulo *post/windows/manage/portproxy* que sirve para crear un túnel interno dentro del propio Host-A, de forma que un puerto local del Host-A se enlace con un puerto de Host-B.

Este módulo está configurando una regla de proxy local persistente en la máquina Windows que tienes bajo control (el Pivote). El objetivo es redirigir el tráfico que llega al Pivote (Host_A) hacia una máquina dentro de su red interna (Host_B).

Figura 15

Comando post/windows/manage/portproxy



Fuente: Autoría propia

Se realiza la siguiente configuración al módulo:

Tabla 1

Configuración establecida modulo portproxy

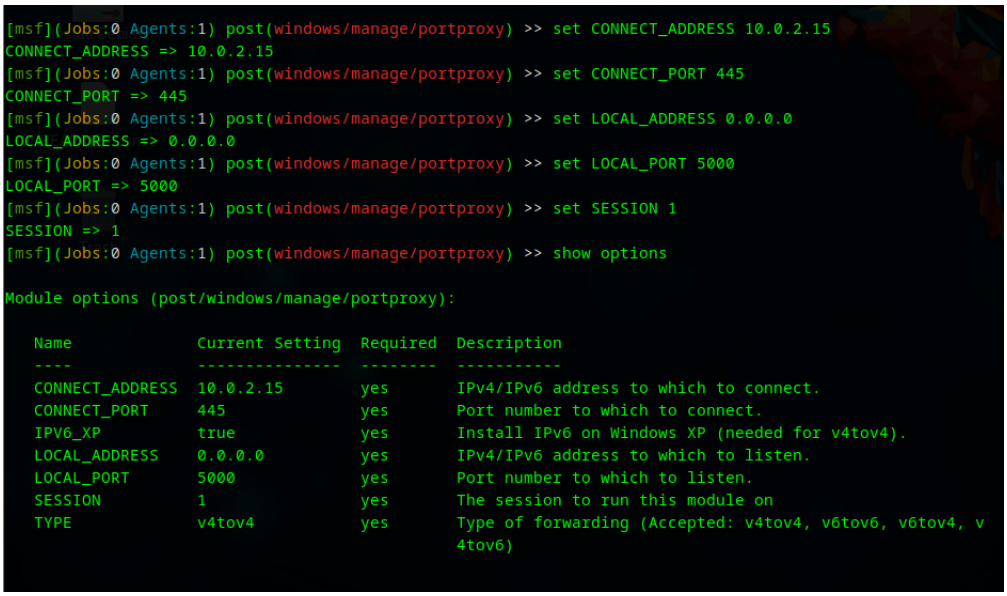
Opción	Valor	Significado
SESSION	1	Se usará la Sesión 1 de Meterpreter para interactuar con la máquina Windows comprometida.
LOCAL_ADDRESS	0.0.0.0	La máquina Pivote escuchará en todas sus interfaces de red.
LOCAL_PORT	5000	El puerto que el Pivote escuchará para recibir el tráfico de reenvío.

CONNECT_ADDRESS	10.0.2.15	La IP de destino interna a la que el Pivote enviará el tráfico.
CONNECT_PORT	445	El puerto de destino interno al que el Pivote enviará el tráfico. (El puerto 445 es típicamente para SMB/compartición de archivos).

Fuente: Autoría propia

Figura 16

Configuración establecida modulo portproxy



Fuente: Autoría propia

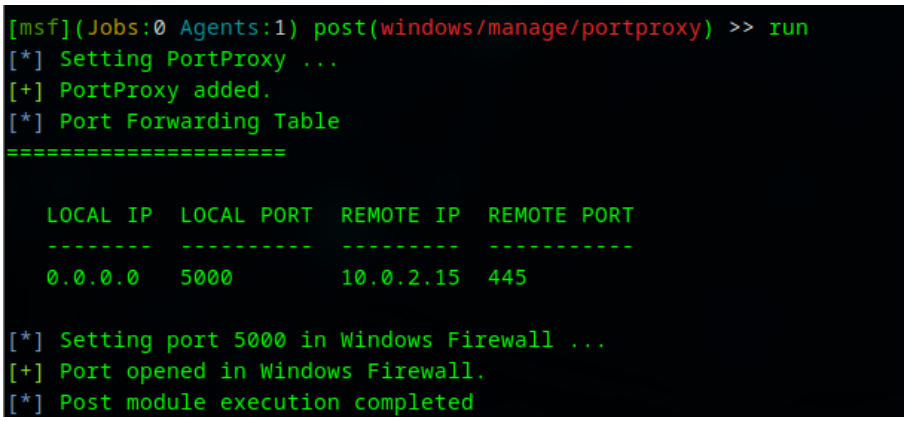
Al ejecutar este módulo (run), se establece la siguiente regla de túnel en la máquina Pivote:

- La máquina Windows Pivote empezará a escuchar en el puerto 5000.
- Cualquier tráfico que desde la máquina atacante se envíe a la IP del Pivote en el puerto 5000 será reenviado automáticamente y de forma persistente a la máquina interna con IP 10.0.2.15 en su puerto 445 (SMB).

En esencia se está abriendo una "puerta" en el Pivote (puerto 5000) para acceder al servicio SMB (:445) de una máquina inaccesible (10.0.2.15).

Figura 17

Ejecución módulo portproxy



Fuente: Autoría propia

Explotación de SMBv1 (EternalBlue – MS17-010)

Sobre Host-B se detectó:

- SMBv1 habilitado.
- Falta del parche MS17-010.

El Red Team utilizó el módulo:

exploit/windows/smb/ms17_010_eternalblue

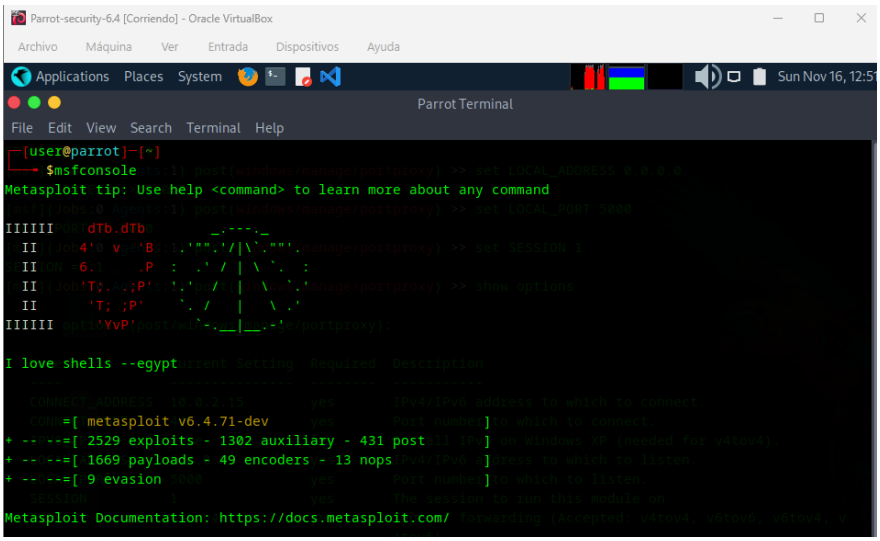
El ataque permitió:

- Ejecución remota de código en el kernel.
- Obtención directa de una sesión con privilegios de sistema.
- Control total sobre Host-B.

Esta vulnerabilidad es una de las más críticas en entornos Windows legacy y permitió un movimiento lateral exitoso.

Figura 18

Ejecución en otra ventana de metasploit



Fuente: Autoría propia

Mediante el comando de búsqueda (search eternalblue), se inicia la exploración de vulnerabilidades explotables en el entorno. EternalBlue es un *exploit* diseñado para capitalizar una vulnerabilidad de Ejecución Remota de Código (RCE) inherente a la implementación del protocolo SMBv1 (Server Message Block versión 1) de Microsoft.

Detalles del Fallo:

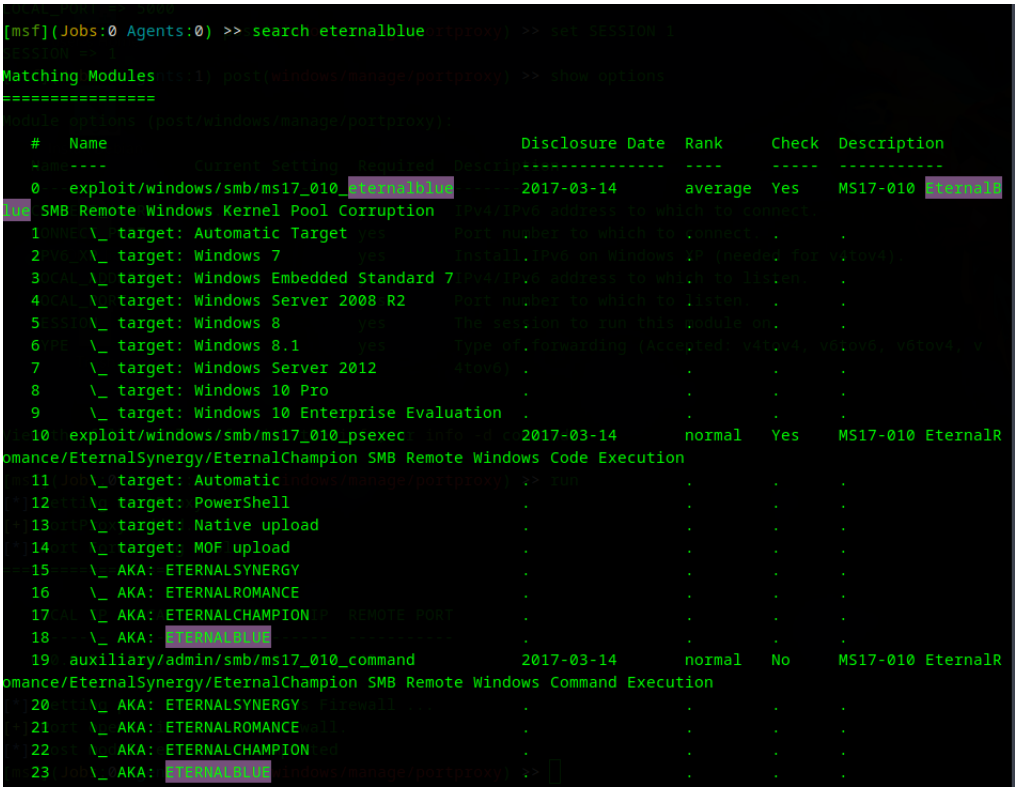
- Protocolo: Afecta a SMBv1, usado para la compartición de recursos en redes Windows.
- Identificador: La vulnerabilidad es la CVE-2017-0144.
- Técnica: El *exploit* opera enviando un paquete de datos malicioso al puerto SMB (TCP 445) del host objetivo. Este paquete está diseñado para desencadenar un desbordamiento de búfer en la memoria del *kernel* debido a un manejo incorrecto de las peticiones de red por parte del sistema.

Consecuencias de la Explotación Exitosa:

- RCE Total: Permite al atacante inyectar y ejecutar código propio (como un *payload* Meterpreter) en el sistema.
- Control Absoluto: El código malicioso se ejecuta con privilegios de nivel SYSTEM, otorgando control total sobre la máquina.
- Capacidad de Gusano: Una característica destacada es que la explotación no requiere autenticación. Esta capacidad de propagación automática sin credenciales lo hizo *wormable*, siendo utilizado por *malware* como WannaCry y NotPetya para moverse lateralmente y propagarse por redes enteras."

Figura 19

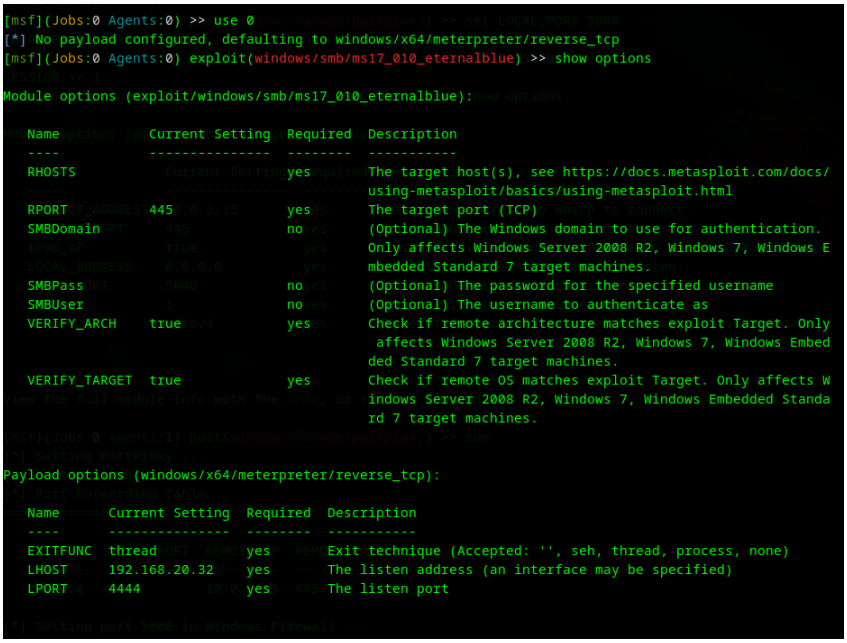
Ejecución search eternalblue



Fuente: Autoría propia

Figura 20

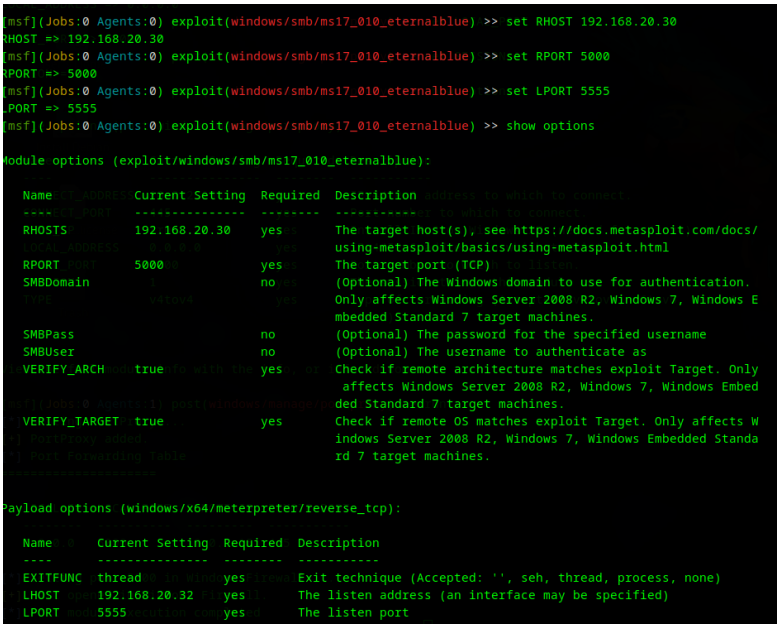
Ejecución en Eternalblue de la opción 0



Fuente: Autoría propia

Figura 21

Configuración parámetros en eternalblue



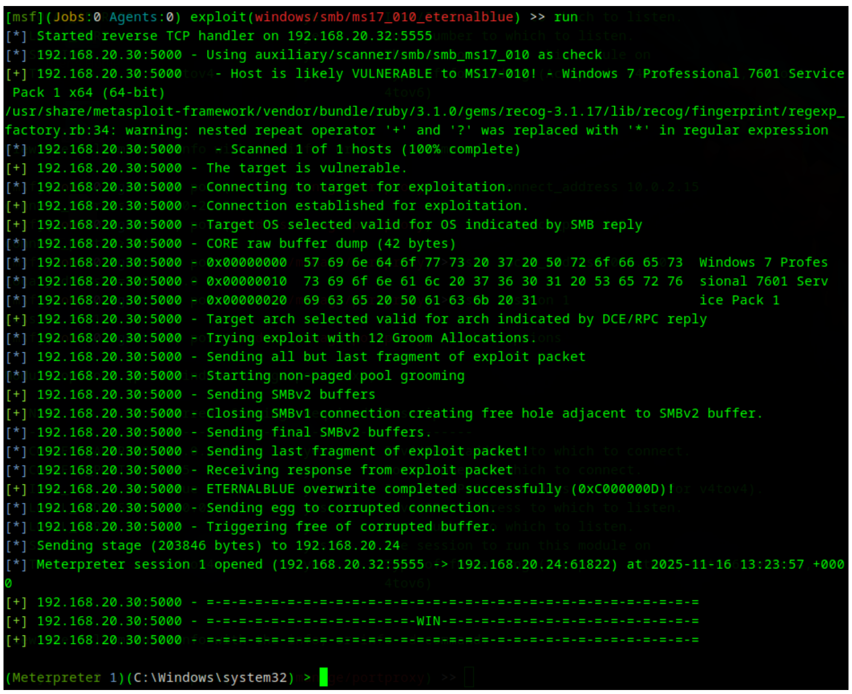
Fuente: Autoría propia

Se procedió a la ejecución del exploit (run) contra un objetivo interno (identificado aquí como 10.0.2.15, el Host-B). La vulnerabilidad MS17-010 (EternalBlue) fue confirmada como explotable, obteniendo un resultado afirmativo ("WIN").

Este paso no fue un ataque directo, sino que requirió una técnica de pivoteo (pivoting) a través del Host-A (el sistema ya comprometido) para alcanzar la red interna donde residía el Host-B.

Figura 22

Ejecución exploit Eternalblue



Fuente: Autoría propia

Creación de cuenta administrativa "DanyArevalo"

Como prueba de concepto (PoC), el Red Team creó una cuenta administrativa en Host-B:

net user DanyArevalo P@ssw0rd! /add

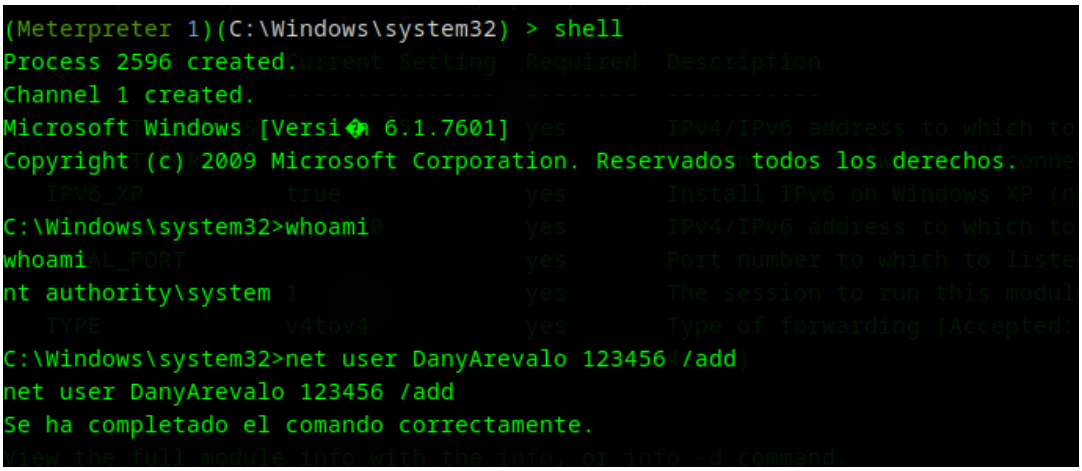
net localgroup administrators DanyArevalo /add

Esto permitió demostrar:

- Escalamiento de privilegios total.
- Persistencia en el sistema.
- Verificación del nivel de compromiso.
- Registro en logs (eventos 4720 y 4728), posteriormente identificados por el Blue Team.

La cuenta fue creada únicamente en la máquina clonada para efectos de laboratorio, documentada y eliminada como parte del cierre del ejercicio.

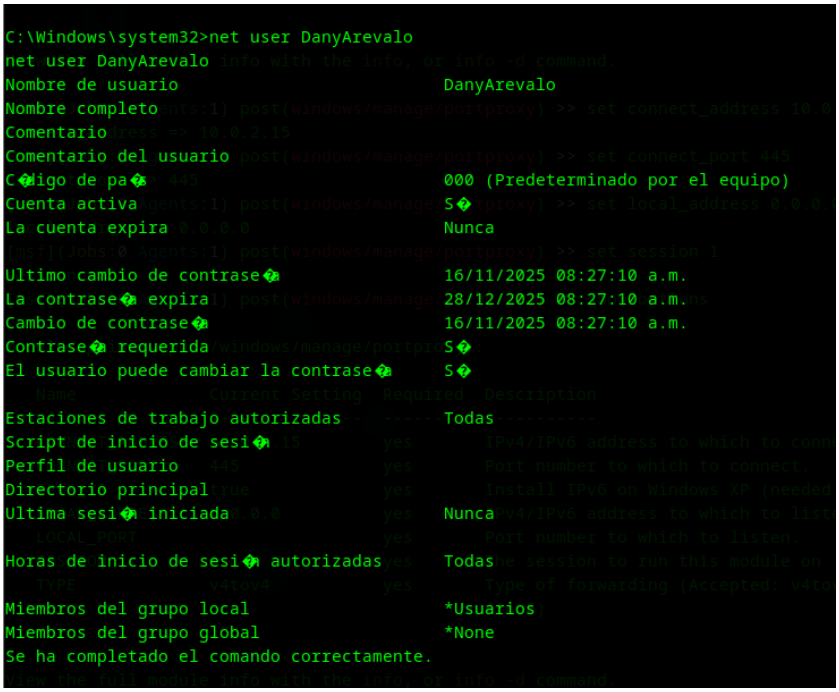
Figura 23 *Ejecución comando Shell y creación de la cuenta usuario.*



Fuente: Autoría propia

Figura 24

Ejecución comando Shell y creación de la cuenta usuario.



Fuente: Autoría propia

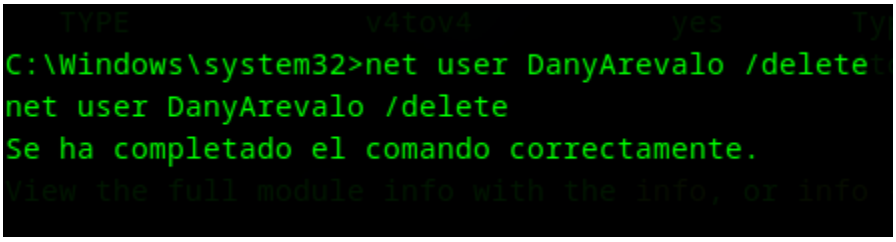
Figura 25

Verificación en el Host_B de la creación de la cuenta usuario.

Fuente: Autoría propia

Figura 26

Eliminación de la cuenta usuario en el Host_B



Fuente: Autoría propia

Tabla 2

Resumen pentesting

Fase	Acción	Resultado
Reconocimiento	Escaneo de red y servicios	Identificación de HFS vulnerable
Explotación inicial	RCE en puerto 80	Shell remoto en Host-A
Post-explotación	Enumeración interna	Mapeo de Host-B y servicios SMB
Pivoting	autoroute/portfwd	Acceso a la red interna
Explotación lateral	EternalBlue	Compromiso total de Host-B
Persistencia	Cuenta “DanyArevalo”	Demostración de control total

Fuente: Autoría propia

Análisis de Vulnerabilidades Explotadas

Durante el desarrollo del ejercicio Red Team se identificaron y explotaron dos vulnerabilidades críticas dentro del entorno Windows configurado para las Etapas 1 a 3. Estas vulnerabilidades permitieron el compromiso inicial del Host-A, el movimiento lateral hacia Host-B y la posterior demostración de control. A continuación, se presenta un análisis técnico detallado de cada una, su impacto, causa raíz y relevancia en el laboratorio.

Vulnerabilidad en Host-A: Rejetto HFS (Remote Code Execution – RCE)

Descripción general

El primer punto de entrada en la red fue una instancia del servidor HTTP Rejetto HFS (HTTP File Server) ejecutándose en Host-A y expuesta a través del puerto 80. La versión detectada presentaba una vulnerabilidad conocida que permite ejecución remota de comandos (RCE) debido al manejo inseguro de parámetros en solicitudes HTTP.

Causa raíz

- La aplicación estaba desactualizada.
- No tenía implementado ningún mecanismo de validación de entrada.
- Se encontraba expuesta sin controles de firewall.
- No se aplicaron políticas de restricción de aplicaciones ni AppLocker.

Impacto en el ejercicio

- Compromiso total del Host-A mediante ejecución remota.
- Obtención de una sesión interactiva controlable (Meterpreter).
- Posibilidad de ejecutar acciones de post-explotación como: Enumeración del sistema, acceso a archivos, descubrimiento de rutas y segmentos internos.
- Inicio del movimiento lateral hacia Host-B.

Conclusión técnica

El servicio vulnerable actuó como vector principal de entrada y demostró la importancia de mantener inventario, control y actualización de software, así como la necesidad de limitar servicios expuestos en estaciones de trabajo.

Vulnerabilidad en Host-B: SMBv1 habilitado – MS17-010 (EternalBlue)

Descripción general

Host-B presentaba el protocolo SMBv1 habilitado y carecía del parche de seguridad correspondiente al boletín MS17-010, asociado a la vulnerabilidad utilizada históricamente en ataques como WannaCry.

Esta falla permite que un atacante ejecute código con privilegios elevados de manera remota mediante el envío de paquetes especialmente manipulados al servicio SMB.

Causa raíz

- Sistema operativo sin parches de seguridad críticos.
- Uso de un protocolo obsoleto (SMBv1) ampliamente desaconsejado.
- Falta de medidas de segmentación o ACL internas.
- Falta de monitoreo de conexiones SMB provenientes de equipos no autorizados.

Impacto en el ejercicio

- Compromiso inmediato con permisos de **SYSTEM**, el nivel más alto del sistema.
- Acceso directo a archivos internos.
- Capacidad de ejecutar código arbitrario.
- Control total sobre el host objetivo.
- Permisión para crear un usuario administrativo temporal ("DanyArevalo") como PoC de persistencia.

Conclusión técnica

La ausencia del parche MS17-010 y el uso de SMBv1 constituyeron una vulnerabilidad de nivel crítico, facilitando que el movimiento lateral fuera exitoso y permitiera comprometer el segundo host sin interacción del usuario.

Relación Entre Ambas Vulnerabilidades

Las vulnerabilidades explotadas formaron una cadena de ataque, demostrando cómo una falla inicial puede escalar progresivamente cuando no existe:

- monitoreo adecuado,
- segmentación de red,
- políticas de hardening,
- control de servicios expuestos,
- gestión de vulnerabilidades continua.

Secuencia lógica del compromiso:

- **RCE en HFS** → acceso remoto a Host-A.
- **Enumeración** → descubrimiento de Host-B y servicios SMB.
- **Pivoting** → reencaminamiento del tráfico hacia interior de la red.
- **EternalBlue** → ejecución remota en Host-B.
- **Escalamiento y persistencia** → creación de cuenta administrativa.

Riesgo Residual Identificado

Incluso tras el compromiso controlado, se concluye que:

- La red es vulnerable a ataques automatizados tipo gusano.
- Un atacante real podría cifrar la infraestructura completa.
- La red interna carece de mecanismos de detección temprana.
- La ausencia de SIEM o IDS genera ceguera operacional.

Estrategias Blue Team

La respuesta del Blue Team conforma la segunda y crítica fase del análisis integrado de SecureNova Labs; tras la simulación ofensiva completa en el laboratorio (incluyendo explotación remota, establecimiento de sesiones de control, pivoteo y movimiento lateral), el equipo defensivo debe concentrar sus esfuerzos no solo en la detección oportuna de las actividades del adversario, sino también en la contención inmediata sin comprometer la evidencia forense, la realización de un análisis exhaustivo del alcance del incidente, el subsiguiente fortalecimiento (*hardening*) de los sistemas para eliminar vulnerabilidades y, crucialmente, la definición de un plan estratégico para la prevención de futuras reincidencias.

Lo primero que realizaría como Blue Team es aplicar un proceso de identificación y contención rápida, siguiendo buenas prácticas de gestión de incidentes.

Detección y análisis inicial del incidente

Mediante la revisión de eventos del sistema y monitoreo de procesos sospechosos, el Blue Team identificó:

- Conexiones no autorizadas en el puerto 80
- Ejecución de procesos asociados a HFS
- Inicio de sesiones remotas
- Actividad anómala en servicios SMB

Estos indicadores permitieron confirmar la presencia de un ataque activo.

Aislamiento de la máquina comprometida (contención inicial)

Las acciones prioritarias incluyeron:

- Aislar Host-A de la red para evitar exfiltración
- Detener el proceso hfs.exe
- Bloquear puertos que coincidían con actividades de explotación (80 y 445)

- Restringir conexiones sospechosas detectadas

El propósito fue impedir la propagación del ataque y preservar la evidencia volátil.

Captura de evidencias volátiles

Usaría herramientas GPL como:

- Sysinternals (Process Explorer, TCPView)
- WinPmem o MemProcFS para memoria RAM
- LogonTracer para identificar accesos indebidos

La guía CCN-STIC 495 recalca la importancia de capturar evidencia antes de reiniciar el sistema (CCN-CERT, 2018).

Escaneo interno de integridad del sistema

Revisaría:

- Usuarios creados (buscando cuentas anómalas)
- Tareas programadas y servicios persistentes
- Llaves de registro sospechosas
- Modificación de archivos del sistema

Iniciar proceso formal de respuesta a incidentes

Según la guía UNAD-CSIRT (2024), se deben:

- Clasificar el tipo de incidente
- Evaluar impacto
- Activar plan de respuesta
- Escalar según criticidad

Medidas de hardenización para que el ataque no se repita.

Eliminación y bloqueo del servicio vulnerable (Rejetto HFS)

- Prohibición de servidores no autorizados en estaciones Windows.

- Restricción de ejecución mediante AppLocker o SRP.

Aplicación estricta de CIS Benchmarks para Windows 7/10, según CIS Security (2020), se debe:

- Deshabilitar servicios innecesarios.
- Configurar firewall local por defecto en modo restrictivo.
- Asegurar políticas de contraseñas y privilegios.
- Activar auditoría avanzada.

Segmentación de red

Evitar que Host-A pueda comunicarse directamente con Host-B:

- VLANs separadas
- Reglas ACL que controlen tráfico lateral
- Bloqueo de SMB (445) donde no sea necesario

Aplicación de parches de seguridad (especialmente SMBv1)

Host-B fue comprometido vía EternalBlue/MS17-010.

Debe:

- Deshabilitar SMBv1
- Instalar parches acumulativos
- Habilitar SMB Signing

Control de privilegios mínimos

- Deshabilitar usuario administrador local
- Uso de LAPS para contraseñas
- Auditoría de creación de cuentas

Implementar un SIEM y alertas en tiempo real

Un SIEM cumple tres funciones esenciales:

- Visibilidad total de lo que ocurre en la red
- Correlación inteligente para detectar amenazas reales
- Soporte al análisis y respuesta ante incidentes

Para alertar en este caso puntual:

- Conexiones elevadas en puertos 80, 4444, 3389
- Creación de usuarios admin
- Accesos remotos no autorizados

Sin un SIEM, un ataque como el realizado en Host-A → Host-B podría tardar horas o días en detectarse.

En el ataque Red Team realizado durante la Etapa 3 (Red team), el compromiso comenzó con la explotación del servicio vulnerable Rejetto HFS 2.3 expuesto en el puerto TCP/80, seguido por el establecimiento de una sesión remota, la extracción de información del sistema y finalmente un pivoting hacia Host-B a través de redes internas no segmentadas.

En función de ese vector de ataque, cada acción defensiva propuesta se encuentra alineada de forma directa con los riesgos identificados:

Tabla 3

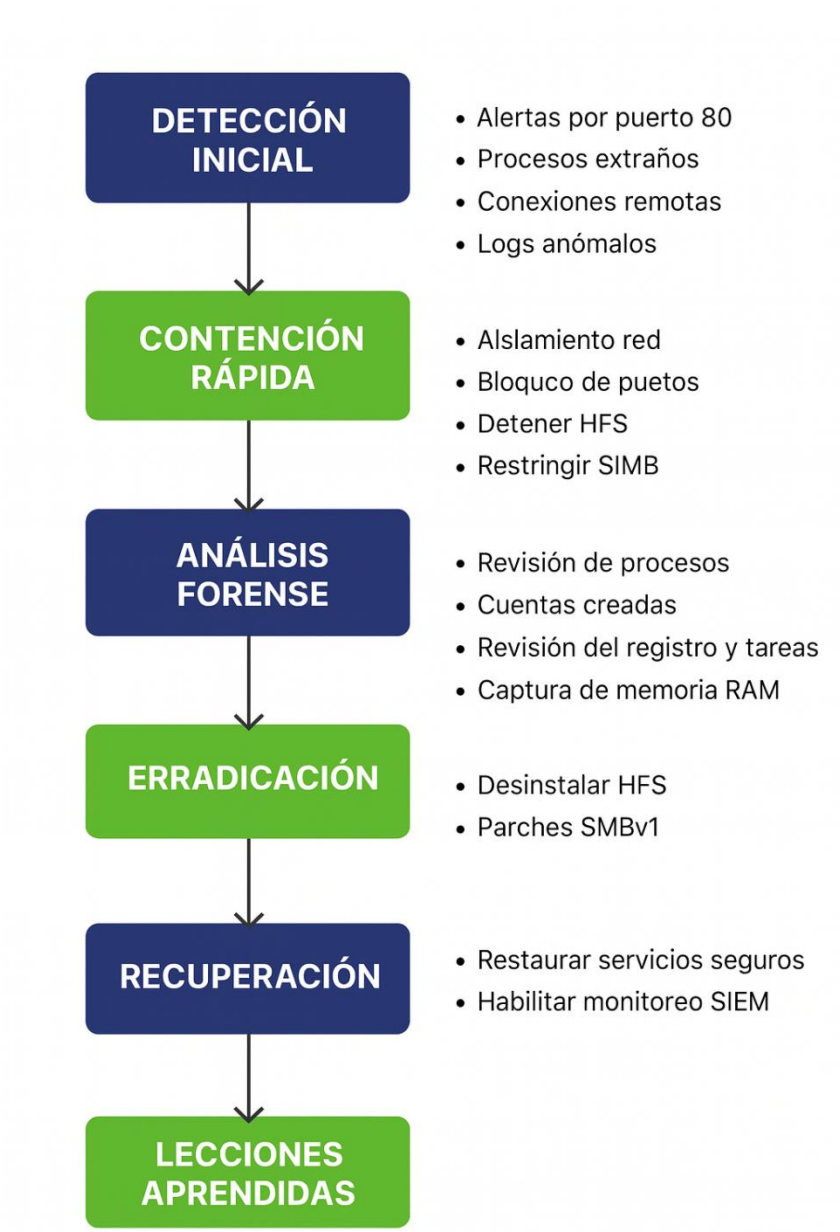
Vector de ataque Red Team

Vector de ataque Red Team	**Acción defensiva Blue Team (Hardenización)**	**Justificación**
Exposición del puerto 80 con aplicación no autorizada	Restricción de software con AppLocker / SRP	Evita ejecución de servidores no permitidos (GUIAR CIS)
Uso de RCE contra HFS	Firewall local restringido + IDS/IPS	Bloquea tráfico anómalo y reduce superficie de ataque
Movimiento lateral desde Host-A a Host-B	Segmentación de red y ACL entre VLANs	Host-A no debería tener rutas directas a redes críticas
Explotación de SMBv1 en Host-B	Parches MS17-010, deshabilitar SMBv1	Elimina vulnerabilidad EternalBlue utilizada en la intrusión
Creación de usuario admin malicioso	Auditorías avanzadas + LAPS	Evita persistencia, detecta cambios y protege privilegios
Falta de monitoreo y correlación	Implementación de SIEM	Permite alertar conexiones, usos de privilegios y anomalías

Nota: Esta tabla muestra el vector de ataque usado por el red team junto con la acción preventiva del blue team. *Fuente*. Autoría propia

Figura 27

Diagrama de flujo.



Fuente: Autoría propia

Evaluación del Riesgo Residual

Incluso después del hardening propuesto, pueden persistir riesgos residuales, tales como:

Reaparición de software no autorizado

Un usuario interno podría reinstalar aplicaciones como HFS u otros servicios inseguros.

Mitigación:

- Implementar **AppLocker** con reglas de ejecución por ruta y hash.
- Auditorías automáticas en SIEM para detectar binarios no aprobados.

Intentos de movimiento lateral con nuevas técnicas

Aunque bloquees SMBv1, un atacante podría usar:

- Pass-the-Hash
- RDP brute force
- WMI lateral movement

Mitigación:

Alertas SIEM sobre:

- Múltiples fallos de autenticación
- Accesos desde cuentas privilegiadas
- Eventos de creación de servicios remotos

Persistencia no detectada

El atacante pudo dejar:

- Tareas programadas
- Entradas en RunOnce

- Puertas traseras ofuscadas

Mitigación:

- Escaneo regular con Sysinternals Autoruns
- Comparación de integridad (hashing)
- Monitoreo de cambios en el registro

Exposición de puertos olvidados

Un pequeño cambio en la configuración puede reabrir un puerto sensible.

Mitigación:

- Implementar Nmap programado (inventario de puertos)
- Reglas de firewall centralizado (GPO)

Aprendizajes clave para la defensa

El ejercicio permitió concluir que:

- La visibilidad de logs es fundamental para detectar compromisos tempranos.
- La ausencia de parches críticos representa un riesgo severo.
- La segmentación interna habría limitado la capacidad de pivoting.
- Los entornos Windows requieren políticas de ejecución controlada obligatorias.
- La correlación de eventos mejora drásticamente la eficiencia del equipo Blue Team.

El Blue Team logró identificar el ataque, validar el compromiso, contener la amenaza y aplicar medidas de remediación que fortalecieron la seguridad del entorno. El análisis forense

permitió reconstruir la cadena completa del ataque, demostrando la importancia de integrar procesos de hardening, monitoreo continuo y plataformas SIEM para prevenir incidentes similares en entornos reales.

Analisis técnico Etapas 1 a la 4

Etapa 1. Fundamentos de Operaciones Red Team y Blue Team

La interacción coordinada entre Red Team y Blue Team permite simular escenarios realistas de ataque y defensa, fortaleciendo tanto la detección temprana como la capacidad de respuesta organizacional, tal como se evidencia en estudios recientes de ejercicios competitivos y colaborativos en ciberseguridad (Chindrus & Caruntu, 2023).

Este enfoque metodológico se alinea con modelos de pruebas de penetración orientados a riesgos, los cuales priorizan activos críticos, probabilidad de explotación e impacto potencial, permitiendo una evaluación más realista de la postura de seguridad de la organización (Álvarez, 2018).

Esta etapa presenta un análisis integral que combina el marco legal colombiano con la metodología y herramientas técnicas esenciales para la ciberseguridad ofensiva (Pentesting/Red Team) y el montaje de un laboratorio controlado.

Marco Legal Colombiano y su Aplicación

El análisis comienza estableciendo la base jurídica, lo cual es fundamental para cualquier prueba de seguridad ética.

Ley 1273 de 2009 (Delitos Informáticos): Modifica el Código Penal para tipificar conductas que afectan la confidencialidad, integridad y disponibilidad (CIA) de sistemas e información. Es la base penal para sancionar intrusiones y *malware* (Congreso de la República de Colombia, 2009).

Ley 1581 de 2012 (Protección de Datos Personales): Establece el régimen general para el tratamiento de datos personales en Colombia, definiendo derechos de los titulares y obligaciones de las empresas. La autoridad de control y vigilancia es la Superintendencia de Industria y Comercio (SIC) (Congreso de la República de Colombia, 2012).

Ley 1266 de 2008 (Habéas Data): Regula específicamente la información financiera y crediticia.

Aplicación Práctica: Todo *pentest* debe realizarse bajo autorización escrita y un Acuerdo de Reglas de Compromiso (ROE) para evitar incurrir en los delitos tipificados por la Ley 1273. La Fiscalía General de la Nación es la entidad que investiga y persigue penalmente estos delitos.

Metodología de Pentesting (8 Etapas)

El pentesting constituye una práctica fundamental para identificar debilidades técnicas antes de que sean explotadas por actores maliciosos, permitiendo a las organizaciones evaluar de forma controlada la seguridad de sus sistemas y mejorar su resiliencia frente a ataques reales (Incibe, 2019).

Desde una perspectiva empresarial, el pentesting no solo permite identificar fallos técnicos, sino que constituye una herramienta estratégica para reducir riesgos, cumplir normativas y fortalecer la confianza en los sistemas de información (PandaSecurity, 2018).

Diversos estudios recientes destacan la evolución de técnicas, herramientas y metodologías de pruebas de seguridad como un factor clave para la identificación temprana y mitigación de vulnerabilidades en entornos cada vez más complejos (Sanne, 2024).

En esta etapa se describe el ciclo de *pentesting* estructurado en ocho etapas, cada una con su propósito, actividades y una herramienta representativa (Palomo Luna et al, 2024):

Tabla 4

Etapas pentesting

Etapa	Objetivo Principal	Herramienta Clave
Pre-engagement	Definir alcance, objetivos y reglas de compromiso (ROE).	Contrato / Alcance firmado.
Reconocimiento	Recopilar información del objetivo (OSINT).	Shodan o theHarvester.
Mapeo y Escaneo	Identificar *hosts* activos, puertos y servicios.	Nmap (escaneo de puertos y detección de servicios).
Análisis de Vulnerabilidades	Buscar vulnerabilidades conocidas (*CVEs*).	OpenVAS o Nessus (escáneres automáticos).
Explotación	Obtener acceso al sistema aprovechando una vulnerabilidad.	Metasploit Framework (para *exploits* y *payloads*).
Post-explotación	Escalar privilegios y realizar movimiento lateral.	Mimikatz (credenciales) o BloodHound (mapeo AD).
Persistencia y Limpieza	Documentar vectores de persistencia y borrar rastros de la prueba.	Módulos controlados de Metasploit.
Reporte y Presentación	Documentar hallazgos, riesgos y recomendaciones.	Plantillas profesionales (ej. OWASP) o Dradis/Faraday.
Retesting	Verificar que las correcciones aplicadas mitigaron los hallazgos críticos.	Mismas herramientas de las etapas previas.

Nota: Etapas del pentesting con su herramienta clave.

La aplicación de metodologías abiertas de testeo de seguridad, como OSSTMM, ha demostrado ser efectiva en contextos institucionales colombianos para la evaluación estructurada de riesgos y controles de seguridad (Zuluaga, 2017).

Herramientas Clave y su Sinergia

El documento detalla las herramientas esenciales y cómo se relacionan entre sí en un flujo de trabajo:

Metasploit Framework: Es la plataforma modular por excelencia para la explotación controlada, la generación de *payloads* y la automatización de ataques reproducibles. Su comando use exploit/windows/smb/ms17_010_eternalblue ejemplifica su uso en la etapa de explotación. El uso de entornos deliberadamente vulnerables, como Metasploitable 2, permite a los equipos de seguridad practicar técnicas de explotación y defensa en escenarios controlados, facilitando el aprendizaje práctico y la validación de herramientas (Rapid7, 2012).

Nmap: Escáner de redes fundamental para las fases de Reconocimiento y Mapeo. Permite el descubrimiento de *hosts*, puertos y la detección de versiones de sistemas operativos y servicios mediante su *Scripting Engine (NSE)*.

OpenVAS (GVM): Escáner de código abierto enfocado en la evaluación de vulnerabilidades. Utiliza bases de datos actualizables (*NVTs*) para clasificar riesgos y generar informes de remediación.

ExploitDB: Repositorio *online* de Pruebas de Concepto (PoC) y *exploits* públicos. Se usa para buscar código basado en software o CVEs, como en el ejemplo de buscar el PoC para EternalBlue (CVE-2017-0144).

CVE (Common Vulnerabilities and Exposures): Un catálogo estandarizado que proporciona identificadores únicos para vulnerabilidades conocidas (ej. CVE-2021-34527). Es crucial para la correlación entre los resultados del escaneo (Nmap/OpenVAS) y la búsqueda de

exploits (ExploitDB/Metasploit). El uso del catálogo CVE (Common Vulnerabilities and Exposures) permite estandarizar la identificación y clasificación de vulnerabilidades, facilitando la correlación entre herramientas de escaneo, explotación y gestión de riesgos (MITRE Corporation, s. f.).

Banco de trabajo. Anexo 1 – Escenario 1

Montaje del Laboratorio (Banco de Trabajo)

La parte práctica asegura un entorno seguro para ejecutar las pruebas técnicas.

Entorno: Se utiliza VirtualBox para montar el laboratorio con dos imágenes OVA:

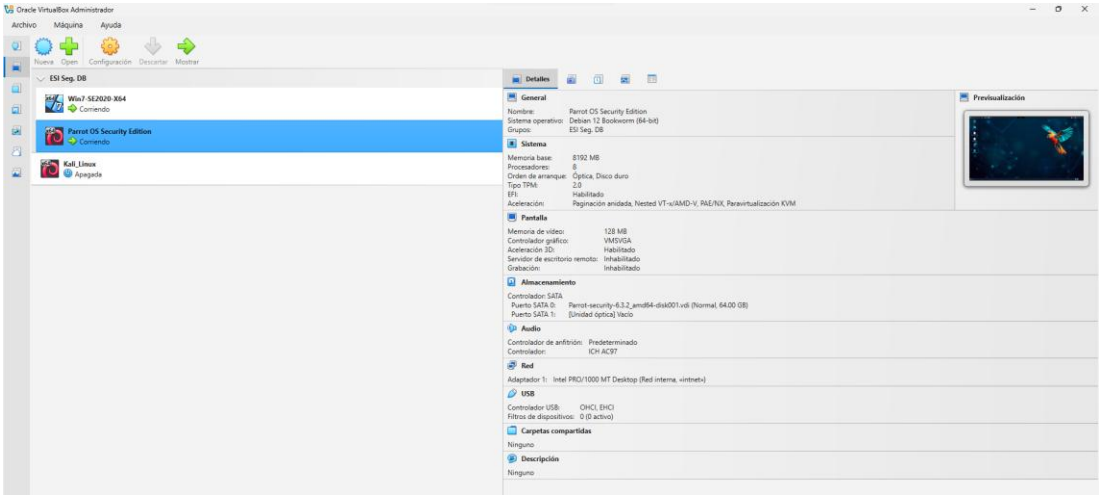
Parrot Security 6.3 (Debian): La máquina atacante, preconfigurada con una amplia colección de herramientas de seguridad. Su IP es $10.0.2.15$.

Windows x64: La máquina víctima. Su IP es $10.0.2.3$.

Conectividad: Se estableció una red NAT llamada Red_Lab_BTBR con segmento $10.0.2.0/24$ para garantizar la comunicación bidireccional entre las máquinas virtuales, verificada mediante la prueba de ping

Figura 28

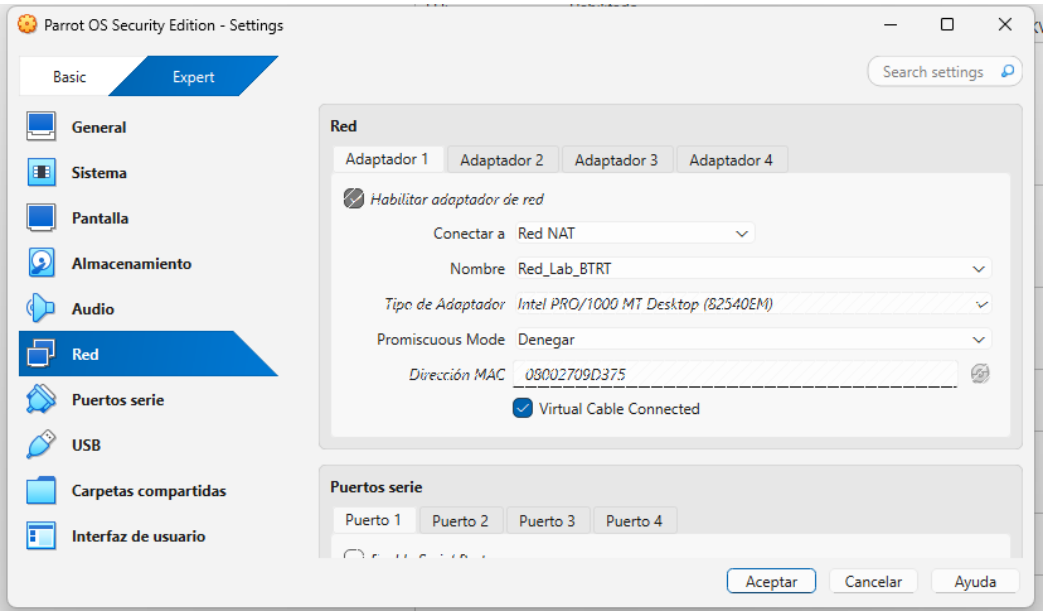
Virtualbox con las OVA cargadas



Fuente: Autoría propia

Figura 29

Configuración red Parrot Security

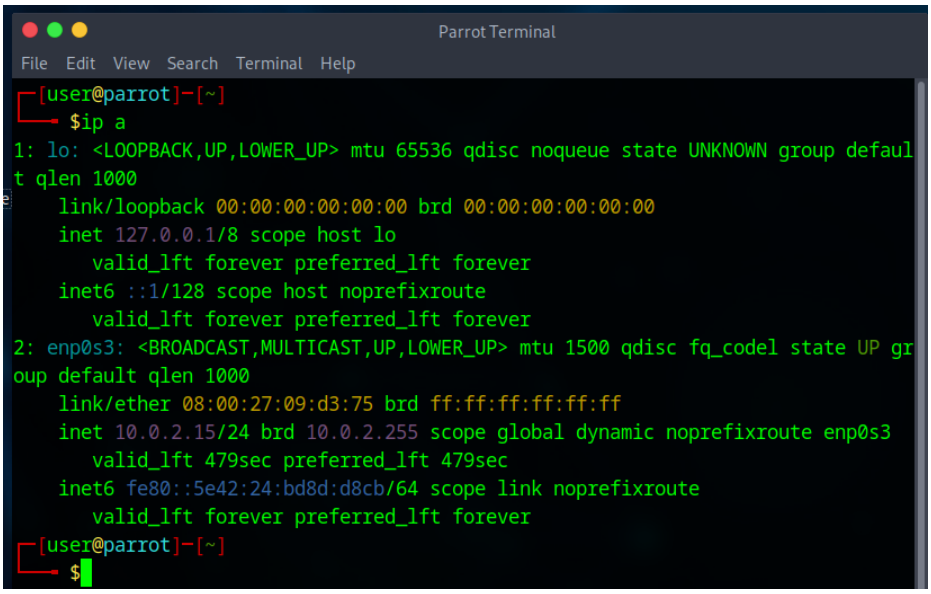


Fuente: Autoría propia

Con el comando *ip a*, se valida la IP que tomó la VM con OS Parrot Security: 10.0.2.15

Figura 30

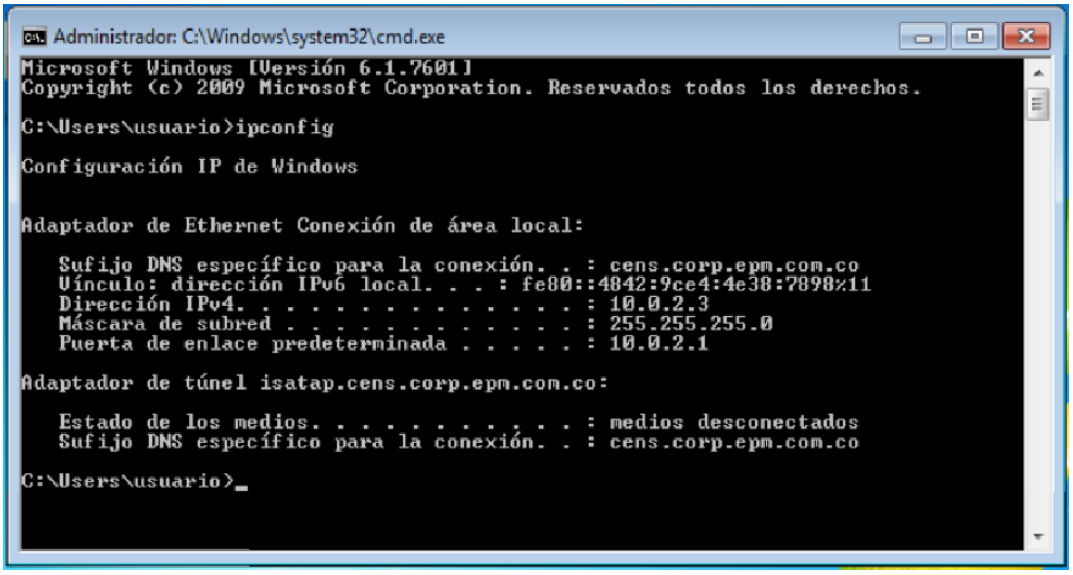
IP maquina atacante: 10.0.2.15



Fuente: Autoría propia

Figura 31

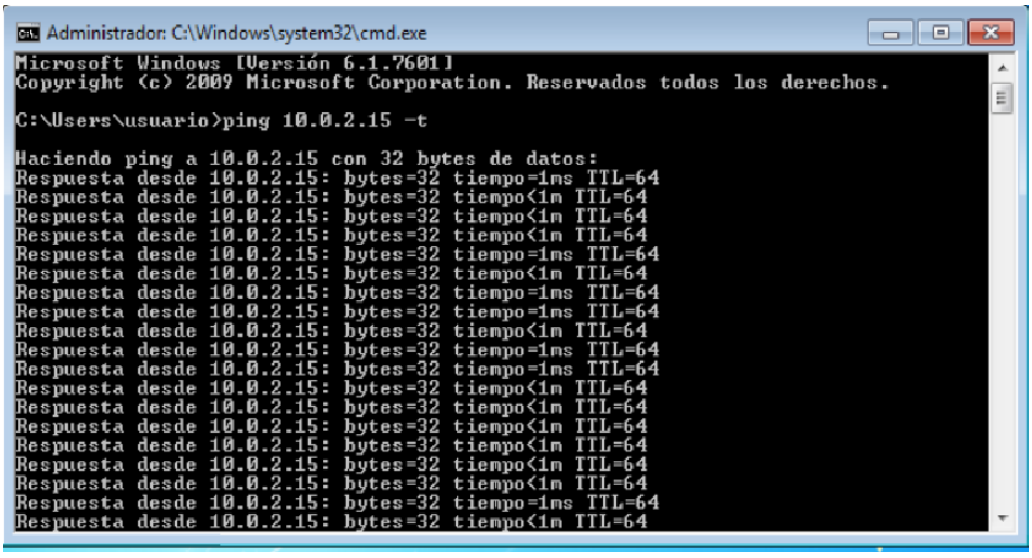
IP Host_A: 10.0.2.3



Fuente: Autoría propia

Figura 32

Prueba de conectividad entre las dos VM



Fuente: Autoría propia

Etapa 2. Ética Profesional y Marco Normativo en Operaciones de Seguridad

El análisis técnico de la Etapa 2: Ética Profesional y Marco Normativo en Operaciones de Seguridad se centra en la evaluación de un acuerdo de confidencialidad (Anexo 3) de la empresa SecureNova Labs, determinando sus implicaciones éticas y legales bajo el marco normativo colombiano.

Conflicto Ético y Legal Central

El documento concluye que el acuerdo de confidencialidad de SecureNova Labs presenta un claro conflicto entre los intereses empresariales y el cumplimiento ético-legal. El acuerdo busca normalizar y encubrir actividades que, fuera de un marco legal autorizado, son constitutivas de delito.

Cláusulas Ilegales y No Éticas Identificadas

Se identifican cláusulas específicas en el Anexo 3 que promueven el ocultamiento de actividades ilícitas:

Ocultamiento de Delitos: El acuerdo obliga a la parte receptora a no divulgar información sobre "procesos ilegales dentro de SecureNova Labs" y prohíbe denunciar ante autoridades "actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros".

Normalización del Delito: La definición de "información confidencial" incluye explícitamente "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos" , lo cual sugiere la realización o uso de interceptaciones no autorizadas.

Eximición de Responsabilidad: Una cláusula obliga al receptor a eximir a SecureNova Labs de "cualquier responsabilidad legal y penal" en caso de que la información ilegal sea descubierta.

Vulneración a la Ley 1273 de 2009

Las conductas normalizadas en el acuerdo vulneran directamente el Título VII-BIS del Código Penal colombiano (Ley 1273/2009):

Tabla 5

Vulneración a la Ley 1273 de 2009

Conducta Normalizada	Artículo Vulnerado (Ley 1273/2009)
Accesos Abusivos	Art. 269A - Acceso abusivo a un sistema informático (acceso sin autorización o fuera de lo acordado).
Interceptación de Información ("Chuzadas")	Art. 269C - Interceptación de datos informáticos (intercepción de comunicaciones o datos sin orden legal).

Nota: Se muestran las conductas normalizadas en el acuerdo vulneran directamente el Título VII-BIS del Código Penal colombiano (Ley 1273/2009)

Además, el diseño del acuerdo, al obligar al ocultamiento y buscar eximir a la empresa, podría configurar figuras penales conexas como encubrimiento u obstrucción a la justicia.

Conflicto con el Código de Ética (COPNIA)

El acuerdo es incompatible con el Código de Ética del COPNIA (Consejo Profesional Nacional de Ingeniería), el cual exige al ingeniero actuar con:

- Integridad y Legalidad.

- Deber de Denuncia: Obligación de denunciar conductas ilícitas.

Responsabilidad Profesional: Aceptar dicho contrato contraviene los deberes éticos, exponiendo al profesional a sanciones disciplinarias y a la posible pérdida de la licencia. (Consejo Profesional Nacional de Ingeniería, 2015)

Mecanismos de Control y Prevención

El análisis propone una serie de controles técnicos y organizacionales para evitar el uso indebido de herramientas forenses y el abuso de acceso durante las auditorías, basado en el principio de minimización:

Tabla 6

Mecanismos de Control y Prevención

Tipo de Control	Mecanismo Propuesto
Técnico	Uso del principio de mínimo privilegio (*Least Privilege*), credenciales temporales (*Just-in-Time access*), registro de sesiones y *logging* inmutable para trazabilidad.
Organizacional	Segregación de funciones, doble aprobación para acciones de alto riesgo (ej. extracción masiva) , canales de denuncia protegidos (*whistleblower*) , y auditorías externas periódicas.
Contractual	Eliminar cláusulas que obliguen a no denunciar o eximan a la empresa de responsabilidad; incluir la obligación de cumplimiento legal y cooperación con autoridades.

Nota: Se observan Mecanismos de Control y Prevención

Etapa 3. Componente Práctico

El análisis técnico de la Etapa 3: Componente Práctico detalla la ejecución de una simulación de ataque ofensivo (*Red Team operation*) en un entorno de laboratorio controlado. El objetivo principal fue demostrar la cadena de ataque completa, desde el acceso inicial a una máquina expuesta hasta el movimiento lateral (pivoteo) hacia un sistema interno.

Entorno de Laboratorio y Objetivo Inicial

El ejercicio se llevó a cabo en VirtualBox, con la siguiente configuración:

Máquina Atacante (Host-A): Parrot Security 6.3 (distribución Linux enfocada en seguridad).

Máquina Víctima Inicial (Máquina 1): Un sistema Windows vulnerable que representa el punto de entrada a la red.

Máquina Objetivo Interno (Máquina 2 o Host-B): Un sistema interno (vulnerable a EternalBlue) que representa un recurso de alto valor, accesible solo a través de la Máquina 1.

Acceso Inicial: Explotación del Servidor HTTP

El vector de acceso inicial se centró en la explotación remota de un servicio de intercambio de archivos:

Vulnerabilidad Explotada: Ejecución Remota de Código (RCE) en el software HttpFileServer (HFS) 2.3.

Herramienta y Módulo: Se utilizó Metasploit Framework con el módulo exploit/windows/http/hfs_exec.

Resultado Técnico: La explotación fue exitosa, permitiendo al atacante obtener una sesión de Meterpreter sobre la Máquina 1, confirmando el compromiso inicial del sistema.

Post-Explotación y Preparación para el Movimiento Lateral

Una vez dentro de la Máquina 1, el atacante ejecutó tareas de post-explotación para asegurar el control y obtener credenciales:

Escalada de Privilegios: Se creó un nuevo usuario administrador (Dany) con privilegios elevados.

Pivoteo y Movimiento Lateral (Host-A a Host-B)

Esta fase demostró una técnica crítica de *Red Team* para alcanzar la Máquina 2 (Host-B), que se asume estaba protegida o segmentada de la red externa:

Configuración de Pivoteo: Utilizando la sesión de Meterpreter en la Máquina 1, se configuró una ruta de red temporal (route add) para que el tráfico del atacante pudiera pasar a través de la Máquina 1 y alcanzar la red interna de la Máquina 2.

Ataque a la Máquina Interna: Se seleccionó un nuevo objetivo interno (la Máquina 2), que fue identificada como vulnerable a MS17-010 (EternalBlue) en el puerto SMB (TCP 445).

Exploitation a Través del Túnel: El atacante lanzó el *exploit* EternalBlue, forzando el tráfico a utilizar la ruta pivotada a través de la Máquina 1.

Resultado Final: Se obtuvo una segunda sesión de Meterpreter en el Host-B, confirmando el éxito del movimiento lateral y el compromiso profundo de la red simulada.

Conclusión Técnica

La Etapa 3 demuestra rigurosamente la integración de múltiples TTPs (Tácticas, Técnicas y Procedimientos) de intrusión en una cadena de ataque:

Vector Inicial: Explotación de RCE en una aplicación web (HFS 2.3).

Persistencia y Escalada: Creación de un usuario administrador y *dumping* de credenciales.

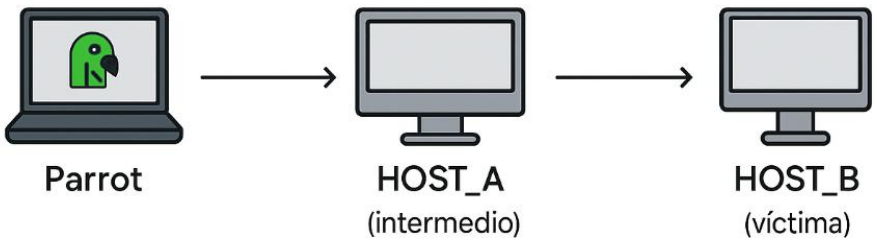
Movimiento Lateral: Uso de pivoteo (routing) a través de la máquina inicial para acceder a la red interna.

Explotación Secundaria: Uso del *exploit* EternalBlue (MS17-010) en el sistema interno (Host-B).

El resultado subraya la necesidad de implementar una defensa en profundidad, no solo parchando aplicaciones perimetrales (HFS), sino también eliminando vulnerabilidades internas (MS17-010) y aplicando políticas de mínimo privilegio para prevenir la escalada y el movimiento lateral.

Figura 33

Diagrama de conexión



Fuente: Autoría propia

Etapa 4. Respuesta y Contención ante Incidentes de Seguridad

El análisis técnico de la Etapa 4**,** Respuesta y Contención ante Incidentes de Seguridad se aborda desde la perspectiva del Blue Team (Equipo de Defensa), centrándose en la gestión de incidentes y la mitigación de las vulnerabilidades explotadas por el Red Team en la fase anterior.

Rol y Contexto Operacional del Blue Team

La comparación entre enfoques ofensivos y defensivos evidencia que el éxito de una estrategia de ciberseguridad depende de la retroalimentación continua entre ambos equipos, fortaleciendo la capacidad de detección, contención y aprendizaje organizacional (Kotwani et al., 2023). El enfoque Red Team–Blue Team ha sido aplicado incluso en evaluaciones de confianza a

nivel de hardware, demostrando su efectividad como modelo integral de validación de seguridad en múltiples capas tecnológicas (Rajendran et al., 2011). La Etapa 4 se enfoca en la respuesta a un escenario de compromiso validado. El Blue Team tiene la tarea de responder al ataque donde la Máquina 1 (Windows) fue comprometida a través de la explotación de una aplicación vulnerable en el puerto TCP/80, lo que permitió el acceso remoto y el movimiento lateral a un host interno.

El objetivo principal del Blue Team es:

Identificar los Indicadores de Compromiso (IOCs) generados por el ataque.

Contener la amenaza y aplicar mecanismos de hardening para prevenir la repetición del incidente.

Diferenciar su rol frente a un equipo de Respuesta a Incidentes (IR Team).

Fundamentos Metodológicos y Marco de Control

El Blue Team emplea marcos de seguridad reconocidos para estructurar su respuesta y fortificar la infraestructura:

Gestión de Incidentes: Se utilizan los lineamientos de gestión de incidentes del CSIRT Académico UNAD y guías CCN-STIC.

Hardenización de Sistemas: Se aplican controles de seguridad recomendados por los CIS Benchmarks para fortalecer la configuración del sistema operativo. El objetivo es reducir la superficie de ataque y mejorar el monitoreo.

Valor de la Plataforma SIEM

Los sistemas SIEM permiten centralizar, correlacionar y analizar eventos de seguridad, mejorando significativamente la detección de comportamientos anómalos y ataques avanzados en entornos empresariales complejos (Moreno, 2015). El ejercicio resalta la importancia de la función de un SIEM (Security Information and Event Management) en la defensa corporativa. Un SIEM es crucial para:

Centralizar y normaliza los *logs* de seguridad.

Correlacionar eventos de la Máquina 1 (ej. ejecución de *shell* remota en el puerto 80) con la Máquina 2 (ej. tráfico SMBv1/445 anómalo o uso del pivote) para detectar el movimiento lateral en tiempo real.

Generar alertas tempranas que permitan la detección y contención rápida del incidente, limitando el alcance del compromiso.

Acciones Técnicas Clave para la Contención y Remediación

Basándose en el ataque simulado de la Etapa 3, el análisis técnico del Blue Team debe enfocarse en los siguientes puntos para lograr el hardening:

Contención de la Máquina 1 (Vector Inicial):

Aislar la Máquina 1 de la red (segmentación o desconexión) para detener la sesión de Meterpreter y el pivoteo.

Forzar la rotación de credenciales comprometidas (el usuario Dany y el *hash* crackeado usuario).

Remediación de la Vulnerabilidad RCE (Máquina 1):

Desinstalar o actualizar urgentemente la aplicación HttpFileServer 2.3 que permitió la Ejecución Remota de Código (RCE) en el puerto 80.

Remediación de la Vulnerabilidad EternalBlue (Máquina 2):

Aplicar el parche de seguridad MS17-010 para la CVE-2017-0144.

Deshabilitar el protocolo SMBv1 en todos los *hosts* internos para eliminar el vector de ataque usado en el movimiento lateral.

Hardenización del Sistema Operativo (Ambos Hosts):

Implementar configuraciones de mínimo privilegio (*Least Privilege*) para restringir la capacidad de escalada de privilegios y creación de usuarios administrativos ilícitos.

Mejorar la configuración de *logging* de eventos de seguridad (ej. creación de usuarios, *logon/logoff* fallidos, actividad de puertos inusual) para optimizar la capacidad de detección del SIEM.

Relación con Aspectos Legales y Éticos

El ejercicio desarrollado en las Etapas 1 a 4 permitió simular un escenario controlado de ataque y defensa cibernética. Sin embargo, incluso dentro de un laboratorio académico, es fundamental relacionar estas actividades con las obligaciones legales, éticas y profesionales aplicables a los procesos de ciberseguridad. La siguiente sección integra estos elementos desde la perspectiva Red Team y Blue Team.

Legalidad de las actividades de prueba

La efectividad del marco legal colombiano frente a la ciberdelincuencia ha sido objeto de análisis académico, evidenciando avances normativos, pero también desafíos en su aplicación y persecución judicial (Rincón Arteaga et al., 2022).

Las acciones de intrusión, explotación y movimiento lateral realizadas por el Red Team solo son válidas dentro de un entorno aislado, controlado y autorizado, como el propuesto en este ejercicio académico. Fuera de este contexto, estas actividades podrían constituir delitos tipificados en múltiples normativas, tales como:

- Acceso no autorizado a sistemas informáticos
- Alteración o destrucción de datos
- Interceptación indebida de comunicaciones
- Creación de cuentas o usuarios sin permiso

En Colombia, estos comportamientos están regulados principalmente por:

- Ley 1273 de 2009: Delitos informáticos y protección de datos.
- Ley 1581 de 2012: Protección de datos personales.
- Constitución Política Art. 15: Derecho a la intimidad y habeas data.

El ejercicio evitó vulnerar estas normas al desarrollarse exclusivamente sobre máquinas privadas, sin información real y con consentimiento explícito como parte del programa

académico. Estas actividades se desarrollaron conforme a los acuerdos académicos y lineamientos institucionales establecidos por la UNAD para la realización de prácticas controladas en entornos de laboratorio.

Ética profesional en las prácticas Red Team

El Red Team tiene la responsabilidad ética de: No exceder el alcance autorizado

Solo se explotan vulnerabilidades en host definidos y con objetivos previamente acordados.

Documentar cada acción

Esto garantiza transparencia, reproducibilidad y trazabilidad.

No generar daño permanente ni destruir información

El propósito es demostrar vulnerabilidades, no comprometer la integridad del sistema.

Respetar la privacidad de datos

Aunque las máquinas del laboratorio no contienen información real, el principio ético exige manejar todo contenido encontrado de manera responsable.

Minimizar el impacto

Toda acción de prueba debe buscar el menor impacto posible en sistemas o servicios.

Con estas prácticas, el Red Team actúa bajo el principio de **ética ofensiva**, donde la agresión técnica está justificada solo como mecanismo para mejorar la seguridad.

Ética y deberes del Blue Team

El Blue Team debe actuar con los principios de buena práctica defensiva, entre ellos:

Integridad

No modificar evidencia sin la debida cadena de custodia.

Objetividad

Basar conclusiones en logs, artefactos y evidencia técnica, no en suposiciones.

Confidencialidad

Todo hallazgo forense, credencial descubierta o dato técnico debe manejarse con reserva.

Responsabilidad

Actuar rápida y diligentemente ante un incidente real para evitar mayores daños.

Proporcionalidad

Las acciones de contención deben ser las mínimas necesarias para detener la amenaza sin afectar indebidamente la operación.

Relación con marcos legales de ciberseguridad y protección de datos

Las prácticas desarrolladas en el ejercicio se alinean con normas y marcos ampliamente usados en el sector, como:

- NIST Cybersecurity Framework (funciones Detect–Respond–Recover).
- ISO/IEC 27001 – Seguridad de la información.
- Regulaciones CIIP (Infraestructuras Críticas) aplicables en sectores como energía, banca y salud.
- Buenas prácticas del CCN-STIC en entornos gubernamentales.

Estos marcos exigen:

- Gestión documentada de incidentes
- Preservación de evidencia
- Monitoreo continuo
- Políticas de acceso y privilegios mínimos
- Pruebas de seguridad autorizadas

El ejercicio replicó estos principios dentro de un entorno académico controlado.

Responsabilidad del profesional en ciberseguridad

El rol de los especialistas Red Team y Blue Team debe ejercerse bajo estándares éticos elevados, reconociendo que:

La ciberseguridad no consiste solo en capacidad técnica, sino también en responsabilidad social.

El objetivo prioritario es proteger sistemas, datos y usuarios.

Toda acción debe justificarse bajo un propósito legítimo.

Actuar fuera de los marcos éticos y legales podría causar daños significativos a organizaciones, usuarios o incluso infraestructuras críticas.

Conclusión general de los aspectos legales y éticos

El ejercicio reafirma que tanto las pruebas ofensivas como defensivas deben realizarse siempre dentro de un marco:

- Autorizado
- Controlado
- Limitado en alcance
- Documentado
- Respetuoso de la ley y la ética profesional

La comprensión de estas obligaciones permite que futuros profesionales de la ciberseguridad realicen pruebas de pentesting, análisis forense y respuesta a incidentes de forma segura, ética y conforme a la normativa vigente.

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/admluABcoeQ

Conclusiones

El desarrollo integral de las Etapas 1 a 4 permitió evidenciar cómo la interacción entre actividades ofensivas (Red Team) y defensivas (Blue Team) constituye un proceso esencial para evaluar y fortalecer la postura de seguridad de una organización. El ejercicio demostró que una vulnerabilidad aparentemente simple —como la ejecución de un servicio desactualizado o la presencia de SMBv1— puede desencadenar un compromiso mayor, comprometiendo varios equipos dentro de la misma red y permitiendo movimiento lateral, escalamiento de privilegios y persistencia del atacante.

Desde la perspectiva del Red Team, se comprobó que la cadena de ataque es posible gracias a fallos acumulativos: falta de gestión de vulnerabilidades, ausencia de segmentación interna y configuraciones inseguras en servicios críticos. Las técnicas empleadas, como el reconocimiento activo, la explotación RCE, el pivoting y la explotación de SMB, evidencian la necesidad de un ciclo continuo de evaluación de riesgos. Estas actividades permitieron validar la efectividad de técnicas comunes que serían explotadas por actores maliciosos en un entorno real.

Por su parte, el Blue Team demostró la importancia de la monitorización, la correlación de eventos y la respuesta oportuna. La reconstrucción del timeline, la identificación de IoC y la aplicación de medidas de contención reflejan buenas prácticas alineadas con estándares como NIST, CIS Benchmarks y guías CCN-STIC. El análisis forense permitió comprender el alcance real del ataque y elaborar acciones correctivas que fortalecen la defensa del entorno.

El ejercicio evidenció, además, que la seguridad no depende únicamente de herramientas, sino de procesos: políticas claras, monitoreo continuo, gestión de parches, segregación de red y controles de acceso adecuados. Asimismo, resalta la responsabilidad ética y legal de quienes realizan pruebas de seguridad, pues estas deben ejecutarse únicamente en entornos autorizados y documentarse de forma íntegra y transparente.

Finalmente, se concluye que la interacción entre Red Team y Blue Team genera un aprendizaje profundo y práctico, y es clave para construir organizaciones más resilientes. La combinación de análisis ofensivo y defensivo permite identificar debilidades reales, mejorar capacidades de detección y respuesta, y elevar el nivel de madurez en ciberseguridad. Este ejercicio académico fortalece competencias esenciales para enfrentar amenazas actuales y futuras, demostrando que la seguridad es un proceso continuo y en constante evolución.

Recomendaciones

Se recomienda implementar un programa formal de gestión de vulnerabilidades basado en un ciclo continuo de identificación, análisis, priorización y remediación. Este proceso debe apoyarse tanto en herramientas automáticas de escaneo como en revisiones manuales periódicas, con el fin de reducir la exposición a riesgos críticos. La ausencia de este enfoque estructurado puede permitir que vulnerabilidades de alto impacto, como la ejecución remota de código (RCE) en HFS o la vulnerabilidad MS17-010, permanezcan sin ser detectadas o corregidas oportunamente.

Asimismo, es fundamental eliminar servicios innecesarios y aplicar un endurecimiento (hardening) estricto en los sistemas. El uso de aplicaciones no autorizadas, obsoletas o sin soporte, como HFS, debe prohibirse de manera explícita. Los hosts deben configurarse conforme a buenas prácticas reconocidas, tales como CIS Benchmarks o las guías CCN-STIC, deshabilitando protocolos inseguros como SMBv1 y restringiendo la ejecución de aplicaciones mediante mecanismos de control como AppLocker o Software Restriction Policies (SRP).

La implementación de una adecuada segmentación de red constituye otro control clave. La infraestructura debe dividirse en zonas claramente definidas, tales como DMZ, red de usuarios y red de servidores, con el objetivo de minimizar el impacto de un posible compromiso. Esta separación reduce significativamente el riesgo de movimiento lateral por parte de un atacante. Adicionalmente, los firewalls internos deben configurarse bajo el principio de mínimo privilegio, permitiendo únicamente el tráfico estrictamente necesario entre los diferentes segmentos.

Para fortalecer la capacidad de detección, se recomienda desplegar una plataforma SIEM que permita el monitoreo centralizado y la correlación de eventos de seguridad. La falta de visibilidad suele facilitar que un atacante avance sin ser detectado durante periodos prolongados.

Un SIEM permitiría identificar patrones anómalos, generar alertas ante eventos críticos como la creación indebida de cuentas o la explotación de vulnerabilidades y facilitar procesos de investigación forense y cumplimiento normativo.

De igual manera, es necesario establecer políticas estrictas basadas en el principio de privilegio mínimo. Los accesos administrativos deben limitarse a cuentas dedicadas, debidamente monitoreadas y auditadas. Se recomienda implementar soluciones como LAPS para la gestión segura de contraseñas de administradores locales, realizar auditorías periódicas de privilegios y eliminar cuentas innecesarias, obsoletas o sin uso.

La aplicación oportuna de parches de seguridad es un aspecto crítico para reducir la superficie de ataque. Los sistemas operativos, servicios y aplicaciones deben mantenerse actualizados, especialmente frente a vulnerabilidades de alto impacto conocidas, como MS17-010. El proceso de actualización debe ser periódico, documentado y validado previamente en entornos de prueba para minimizar el riesgo de afectaciones operativas.

En paralelo, se debe fortalecer la capacidad de respuesta a incidentes mediante la formalización de procedimientos claros para el Blue Team. Estos procedimientos deben contemplar la detección temprana, la contención inicial del incidente, la recolección y preservación de evidencias, la erradicación de la amenaza, la recuperación de los sistemas y la elaboración de un informe post-mortem. La realización de simulacros periódicos contribuirá a mejorar la preparación y eficacia del equipo ante incidentes reales.

Adicionalmente, la implementación de controles de monitoreo de red, como sistemas IDS/IPS, permitiría detectar de manera temprana patrones de explotación o conexiones inusuales similares a las observadas durante el ataque. Estos controles actúan como una línea de defensa preventiva y complementan las capacidades de detección del SIEM.

La capacitación continua del personal técnico es otro pilar fundamental. Tanto los equipos de Red Team como de Blue Team deben recibir formación constante en nuevas técnicas de ataque, controles de seguridad actuales, herramientas de detección y respuesta, así como en buenas prácticas de análisis forense digital. Este enfoque reduce la brecha entre el conocimiento teórico y la aplicación práctica en escenarios reales.

Finalmente, se recomienda adoptar progresivamente un modelo de seguridad Zero Trust, el cual parte del principio de que ningún usuario, dispositivo o aplicación es confiable por defecto. Este enfoque promueve la verificación constante de identidad y contexto, reduce el movimiento lateral dentro de la red y mejora la protección frente a accesos no autorizados. Zero Trust puede implementarse de forma gradual y adaptarse a las particularidades y madurez de cada entorno organizacional.

Referencias Bibliográficas

Álvarez, V. (2018). *Propuesta de una metodología de pruebas de penetración orientada a riesgos*. Repositorio Institucional UEES, 1–26. https://repositorio.uees.edu.ec:8443/server/api/core/bitstreams/f3c021ac-13c7-4506-8d52-ed6b36d8130b/content

CCN Cert. (2018). *Guía de seguridad de las TIC (CCN-STIC-495): Seguridad en IPv6* (pp. 10–29). https://www.ccncert.cni.es/pdf/guias/series-ccn-stic/guias-deacceso-publico-ccnstic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

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* (Versión 1.0, pp. 5–31). https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_valoración_y_evaluación_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 Benchmarks*. https://www.cisecurity.org/cis-benchmarks/

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: Protección de la información y los datos*. Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012: Protección de datos personales*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Consejo Profesional Nacional de Ingeniería. (2015). *Código de Ética para el ejercicio de la Ingeniería y profesiones afines* (pp. 3–26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

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, 7*(12), 1–11. https://doi.org/10.55041/IJSREM27675

Mitre Corporation. (s. f.). *What is a CVE?* https://www.redhat.com/en/topics/security/what-is-cve

Moreno, P. (2015). *Técnicas de detección de ataques en un sistema SIEM*. USFQ (pp. 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). *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

PandaSecurity. (2018). *Pentesting: Una herramienta muy valiosa para tu empresa*. 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*. In *2011 IEEE 29th International Conference on Computer Design (ICCD)* (pp. 285–288). https://doi.org/10.1109/ICCD.2011.6081410

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

Rincón Arteaga, J. A., Castiblanco Hernández, S. A., Quijano Díaz, A., Urquijo Vanegas, J. D., & Pregonero León, Y. K. (2022). *Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos? Criminalidad.* https://pesquisa.bvsalud.org/portal/resource/esLa/biblio-1417091

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

Zuluaga, A. D. (2017). *Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la Rama Judicial, seccional Armenia.*. [Proyecto aplicado, Universidad Nacional Abierta y a Distancia UNAD]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/17410

Apéndices

Apéndice A

Resultado de revisión en Turnitin

turnitin

Recibo digital

Este recibo confirma que Turnitin ha recibido tu trabajo. A continuación, encontrarás la información del recibo perteneciente a tu entrega.

Autor del envío	DANY FERNANDO AREVALO CASTELLANOS
Identificador del trabajo de Turnitin (Identificador de referencia)	2840203639
Título del Envío	Informe ETAPA5_Seminario
Título de Tarea	ECBTI - Draftbank 2
Fecha del envío	08/12/25, 14:06

Imprimir

Nota. Se observa el recibo digital del cargue del documento en Turnitin.