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

Jeyson Javier Calderon Rosas

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Dedicatoria

Dedico inicialmente este trabajo a Dios y la virgen María, por brindarme la vida, la sabiduría y la fortaleza necesaria con el fin de superar los retos que se presentaron en esta etapa de formación académica.

A mi familia, por sus demostraciones de amor, apoyo y motivación permanente, logrando ser mi inspiración en mi crecimiento personal y profesional.

Finalmente, a aquellas personas que no dudaron de mis capacidades y fueron esa voz de empuje a seguir adelante en mi proceso académico, tanto en el pregrado como en el posgrado.

Agradecimientos

En primer lugar, agradezco a Dios por proveerme la fortaleza, la sabiduría y la perseverancia necesarias para culminar satisfactoriamente este proceso académico.

Así mismo, agradezco a mi familia por la motivación, el acompañamiento y el apoyo incondicional brindados durante el desarrollo de esta etapa de formación profesional, siendo un pilar fundamental y sostén para la llegada a la solución de cada uno de mis objetivos.

Agradezco también a mis compañeros de estudio por el intercambio de conocimientos y el apoyo brindado durante la ejecución de las diferentes actividades académicas.

Resumen

El presente trabajo analiza los aspectos técnicos, legales, éticos y defensivos relacionados con la ciberseguridad en entornos red team y blue team. Su propósito es comprender las metodologías empleadas para la identificación, evaluación y mitigación de vulnerabilidades, así como la importancia del cumplimiento normativo y ético en el ejercicio profesional de la seguridad informática. Para ello, se realizó una revisión de la legislación colombiana aplicable, especialmente la Ley 1273 de 2009 y la Ley 1581 de 2012, junto con el estudio de las fases del pentesting, incluyendo reconocimiento, escaneo, explotación y post-explotación. Como parte de la metodología, se analizaron herramientas especializadas como Nmap, Metasploit, OpenVAS, CVE y ExploitDB, utilizadas en procesos de evaluación de seguridad. Asimismo, se desarrolló un laboratorio virtual mediante VirtualBox con máquinas Windows y Kali Linux, en el cual se ejecutaron actividades de reconocimiento, explotación de vulnerabilidades, pivoting y escalamiento de privilegios. Adicionalmente, se examinó el caso "SecureNova Labs" con el fin de identificar riesgos asociados al ciberespionaje y evaluar sus implicaciones legales y éticas conforme a los lineamientos del COPNIA. Los resultados obtenidos evidencian la importancia de integrar estrategias ofensivas y defensivas para fortalecer la protección de los activos de información. Finalmente, se concluye que la implementación de controles como hardening, SIEM, CIS Controls, EDR, NAC y firewalls contribuye significativamente a la prevención, detección y respuesta ante incidentes de seguridad, fortaleciendo la postura de ciberseguridad de las organizaciones.

***Palabras clave*:** Blue team, ciberseguridad, hardening, pentesting, red team.

Abstract

This paper analyzes the technical, legal, ethical, and defensive aspects related to cybersecurity in red team and blue team environments. Its purpose is to understand the methodologies used for the identification, assessment, and mitigation of vulnerabilities, as well as the importance of regulatory and ethical compliance in the professional practice of information security. To this end, a review of applicable Colombian legislation was conducted, especially Law 1273 of 2009 and Law 1581 of 2012, along with a study of the penetration testing phases, including reconnaissance, scanning, exploitation, and post-exploitation. As part of the methodology, specialized tools such as Nmap, Metasploit, OpenVAS, CVE, and ExploitDB, used in security assessment processes, were analyzed. Additionally, a virtual laboratory was developed using VirtualBox with Windows and Kali Linux machines, in which reconnaissance, vulnerability exploitation, pivoting, and privilege escalation activities were performed. Additionally, the "SecureNova Labs" case was examined to identify risks associated with cyber espionage and evaluate its legal and ethical implications in accordance with COPNIA guidelines. The results obtained demonstrate the importance of integrating offensive and defensive strategies to strengthen the protection of information assets. Finally, it is concluded that the implementation of controls such as hardening, SIEM, CIS Controls, EDR, NAC, and firewalls significantly contributes to the prevention, detection, and response to security incidents, strengthening the cybersecurity posture of organizations.

***Keywords*:** Blue team, cybersecurity, hardening, pentesting, red team.

Tabla de Contenido

Lista de Figuras 12

Lista de Tablas 15

Lista de Apéndices 16

Glosario 17

Introducción 19

Justificación 21

Objetivos 23

- Objetivo General 23
- Objetivos Específicos 23

Desarrollo del informe 24

Fundamentos de operaciones red team y blue team 24

- Análisis de la legislación relacionada con delitos informáticos 24
- Análisis sobre el ejercicio de Pentesting 25
  - Reconocimiento 26
  - Escaneo y Enumeración 26
  - Explotación 27
  - Post-Explotación 27
  - Reporte 28
- Análisis de herramientas de ciberseguridad 29
  - Herramientas de ciberseguridad 29
    - Metasploit 29
    - Nmap 29
    - OpenVAS 30

Servicios en línea de ciberseguridad 30
ExploitDB 30
CVE 30
Evidencia de la implementación del montaje del banco de trabajo 31
Despliegue del montaje 38
Características técnicas de Windows 39
Características técnicas de Kali Linux 39
Ética profesional y marco normativo en ciberseguridad 39
Identificación de procesos ilegales y no éticos en el acuerdo 40
Vulneración de la Ley 1273 de 2009 41
Artículo 269A – Acceso abusivo a un sistema informático 41
Artículo 269C – Interceptación de datos informáticos 42
Artículo 269F – Violación de datos personales 42
Decisión profesional frente a la oferta laboral (enfoque ético y COPNIA) 42
Análisis del caso “Ciberespionaje y Ética en SecureNova Labs” 43
Acceso a información sensible en auditorías 44
Mecanismos de supervisión y control en empresas de ciberseguridad 46
Respuesta ante actos de ciberespionaje y restauración de la confianza 47
Componente práctico – practicas simuladas 49
Resumen de la actividad realizada 49
Reconocimiento 50
Herramientas implementadas 50
Acciones realizadas 51
Escaneo y enumeración 60

Herramientas implementadas 60
Explotación inicial 62
Escalada y movimiento lateral 67
Herramientas implementadas 68
Utilización del portproxy para la ampliación del pivot 74
Explotación del host interno 76
Post-Explotación 80
Aspectos fundamentales que situaron la exploración hacia el fallo de seguridad informática el cual afectó directamente al Host-A, con Windows 7. 84
"SecureNova Labs detectó fugas de información desde una estación de trabajo Windows (Host-A)." 84
"La imagen forense indica que la máquina ejecutaba una aplicación vulnerable probablemente explotada para obtener shell." 85
"Evidencias de la creación no autorizada de un usuario con permisos administrativos." 85
"Los registros sugieren movimientos laterales desde Host-A hacia un servidor secundario (Host-B)." 85
"Misión del red team: determinar el vector de fuga en Host-A, validar si la vulnerabilidad fue explotada y si existió escalamiento de privilegios." 86
"Reproducir en un laboratorio aislado el pivoting Host-A → Host-B." 86
"Se habría obtenido información sensible desde el servidor secundario." 86
Herramientas utilizadas en la etapa de reconocimiento y análisis 86
Nmap 86
Resultados destacados 86
Metasploit Framework 87

Módulo utilizado 87
Afectación del ataque a las máquinas con Windows 7 en la red. 87
Validación de vulnerabilidades en las máquinas con Windows tras el paso a paso 88
Timeline 89
Plan de remediación integral 91
Respuesta y contención ante incidentes de ciberseguridad 93
Aspectos para tener en cuenta en caso de un ataque en tiempo real 93
Aislamiento del host comprometido 94
Deshabilitación de accesos comprometidos 94
Segmentación y bloqueo de tráfico 95
Eliminación de rutas de pivoting 95
Preservación de evidencia 95
Propuesta de medidas de hardenización para que no se repita el ataque 96
Control de vulnerabilidades y parcheo 96
Reducción de superficie de ataque 96
Segmentación y microsegmentación de red 97
Endurecimiento de SMB y protocolos administrativos 97
Principio de mínimo privilegio 98
Protección avanzada de endpoints (EDR) 98
SIEM y monitoreo centralizado 98
Control del tráfico de salida 98
Copias de seguridad y continuidad operativa 99
Capacitación y cultura de seguridad 99
Diferencias entre un equipo blue team y un equipo de respuesta a incidentes informáticos 99

Blue team 100
Equipo de respuesta de incidentes informáticos 100
Utilización de CIS (Center for Internet Security) en equipo blue team 102
Hardenización de sistemas 102
Creación de baselines de seguridad 103
Aplicación de CIS Controls 103
Reducción de superficie de ataque 104
Auditoría y cumplimiento 104
Funciones y características principales de un SIEM 105
Recolección centralizada de logs 105
Correlación de eventos 106
Alertas en tiempo real 106
Detección de anomalías 107
Gestión de incidentes y análisis forense 107
Dashboards y monitoreo centralizado 108
Cumplimiento normativo 108
Herramientas de contención de ataques informáticos 109
Firewall 109
EDR (Endpoint Detection and Response) 110
NAC (Network Access Control) 111
Relación entre hallazgos identificados y controles de mitigación 112
Evidencias de Sustentación 114
Conclusiones 115
Recomendaciones 117

Acciones inmediatas (prioridad urgente) 117

Acciones de mediano plazo (prioridad media) 117

Acciones permanentes (prioridad continua) 118

Referencias Bibliográficas 120

Apéndices 123

Lista de Figuras

Figura 1 *Descarga de la herramienta VirtualBox* 31

Figura 2 *Instalación de la herramienta VirtualBox* 32

Figura 3 *Ingreso al repositorio para descargar de recursos objeto de estudio* 32

Figura 4 *Descarga de Kali Linux última versión Hacker Machine* 33

Figura 5 *Máquinas debidamente montadas en el entorno de virtualización* 33

Figura 6 *Máquina con Windows 7 instalada y características de esta.* 34

Figura 7 *Máquina con Linux instalada y características de esta* 34

Figura 8 *Configuración del adaptador de red como adaptador puente Windows* 35

Figura 9 *Configuración del adaptador de red como adaptador puente Linux* 35

Figura 10 *Con el comando IPCONFIG se obtiene la dirección IP en Windows* 36

Figura 11 *Con el comando IFCONFIG se obtiene la dirección IP en Linux* 36

Figura 12 *Ping a la dirección IP de la máquina con Linux desde Windows* 37

Figura 13 *Ping a la dirección IP de la máquina con Windows desde Linux* 37

Figura 14 *Montaje del banco de trabajo* 38

Figura 15 *Red a implementar* 52

Figura 16 *Alistamiento de máquinas* 53

Figura 17 *Configuración de adaptador puente en Hacker Machine* 53

Figura 18 *Creación de la red NAT* 54

Figura 19 *Actualización de sistema operativo Kali* 55

Figura 20 *Validación dirección IP del Hacker Machine* 55

Figura 21 *Escanear la red para identificar las máquinas conectadas* 56

Figura 22 *Validación de la IP en la Victim Machine* 57

Figura 23 *Ping de conexión entre Hacker Machine y Victim Machine* 57

Figura 24 *Descarga de Rejetto a Victim Machine* 58

Figura 25 *Se ejecuta el HFS en Victim Machine* 59

Figura 26 *Creación de carpeta Hacker Machine en el repositorio* 59

Figura 27 *Escaneo de los puertos* 61

Figura 28 *Visualización del reporte de escaneo, servicios abiertos y puerto 80* 61

Figura 29 *Inicialización de Metasploit* 62

Figura 30 *Búsqueda de vulnerabilidades de Rejetto con el Metasploit* 63

Figura 31 *Selección de la vulnerabilidad* 63

Figura 32 *Se visualizaron las opciones* 64

Figura 33 *Configuración del target host con la dirección IP de la Victim Machine* 65

Figura 34 *Se explotó la vulnerabilidad con el comando run* 65

Figura 35 *Se ejecutó el comando ipconfig para validar la conexión* 66

Figura 36 *Ejecución de comando sysinfo para verificar información de la Victim Machine* 66

Figura 37 *Visualización del exploit en el HFS desde la ip de la Hacker Machine* 67

Figura 38 *Ejecución de autoroute y sesión de Meterpreter activa* 69

Figura 39 *Visual de la información de la sesión entre las máquinas* 69

Figura 40 *Enrutamiento del tráfico de las interfaces* 70

Figura 41 *Configuración del segmento de red de la Internal Machine en el RHOSTS* 71

Figura 42 *Visualización de las máquinas activas en el segmento de red* 71

Figura 43 *Escaneo de puertos abiertos en la Internal Machine* 72

Figura 44 *Se creó el túnel* 73

Figura 45 *Verificar funcionamiento del túnel* 74

Figura 46 *Configuración de la conexión portproxy* 75

Figura 47 *Ejecución del portproxy* 76

Figura 48 *Ejecución de Metasploit para encontrar el EternalBlue* 76

Figura 49 *Búsqueda del exploit EternalBlue* 77

Figura 50 *Visualización de las opciones del EternalBlue* 78

Figura 51 *Configuración del exploit EternalBlue* 79

Figura 52 *Ejecución del EternalBlue pivot a la Internal Machine* 80

Figura 53 *Visualización de información del equipo y usuario logueado* 81

Figura 54 *Confirmación de usuario logueado y dirección IP la Internal Machine* 81

Figura 55 *Confirmación de la dirección IP de la Internal Machine* 82

Figura 56 *Ejecución del comando getsystem* 82

Figura 57 *Ejecución de Shell, creación del usuario y elevación de privilegios* 83

Figura 58 *Validación de Internal Machine con la cuenta Jeyson_Calderon configurada* 84

Lista de Tablas

Tabla 1 *Línea de tiempo de la actividad realizada* 89

Tabla 2 *Comparación entre equipos* 101

Tabla 3 *Hallazgo, riesgo y control* 112

Lista de Apéndices

Apéndice A *Resultado de revisión en Turnitin* 123

Glosario

Blue team:

Grupo responsable de la protección, seguimiento y seguridad de las infraestructuras tecnológicas.

Ciberseguridad:

Conjunto de costumbres y buenas prácticas orientadas a proteger los sistemas, las redes y los datos digitales.

CIS Controls:

Controles de seguridad utilizados con el fin de proteger y asegurar las infraestructuras tecnológicas.

EDR:

Herramienta de ciberseguridad que permite detectar y responder a las amenazas ya presentes en los dispositivos finales.

Exploit:

Código o técnica utilizada para aprovechar la existencia de una vulnerabilidad informática.

Firewall:

Sistema seguido para el control y filtrado del tráfico de red, tanto del tráfico entrante como del tráfico saliente.

Hardening:

Proceso de fortalecer la seguridad de sistemas, redes y aplicaciones mediante la eliminación de vulnerabilidades y configuraciones inseguras, reduciendo así la superficie de ataque.

NAC:

Tecnología que permite controlar y restringir el acceso de los dispositivos a la red.

Nmap:

Herramienta utilizada para escaneo de puertos y reconocimiento de redes.

Pentesting:

Evaluación de seguridad que permite realizar ataques controlados para llegar a identificar las vulnerabilidades.

Pivoting:

Técnica utilizada para acceder a otras redes desde un determinado sistema ya comprometido.

Red team:

Grupo especializado que ejecuta simulaciones de ataques para evaluar la postura de seguridad de una organización.

SIEM:

Plataforma que permite consolidar, correlacionar y controlar seguridad informática.

Vulnerabilidad:

Debilidad en el sistema que puede ser la utilizada por un atacante.

Introducción

Hoy en día, la ciberseguridad se ha vuelto un aspecto esencial para la protección de la información, las infraestructuras tecnológicas y la continuidad operativa de las organizaciones. La continua evolución de las amenazas informáticas, los ataques dirigidos y las vulnerabilidades de los sistemas, entre otros factores, han traído consigo la necesidad de implantar estrategias de defensa y de ataque que se ocupen de poder prevenir, detectar y responder a un incidente de seguridad en el marco de las organizaciones. En este sentido, los enfoques red team y blue team contribuyen dentro de los procesos de aseguramiento de la información para lograr conocer las técnicas utilizadas por los atacantes, así como los mecanismos de defensa puesto en marcha para proteger los activos digitales.

El desarrollo de estas actividades permitió abordar integralmente los componentes fundamentales de la seguridad informática. Por un lado, se llevó a cabo el estudio de los fundamentos de las operaciones red team y blue team, en paralelo al análisis de la legislación colombiana en lo referente a delitos informáticos y protección de datos personales; por otro lado, se llevó a cabo el análisis del componente ético y profesional de la ciberseguridad, mediante un estudio del caso “SecureNova Labs”, el análisis de los riesgos legales y las vulneraciones a la privacidad, así como la importancia del cumplimiento del Código de Ética del COPNIA. A la par, se desarrolló un laboratorio práctico con máquinas virtuales Windows y Kali Linux y se llevaron a cabo actividades de reconocimiento, escaneo, explotación de vulnerabilidades, pivoting, movimiento lateral, y post-explotación con uso de herramientas especializadas como Nmap y Metasploit.

Finalmente, se han analizado estrategias defensivas mediante la respuesta y contención de incidentes de ciberseguridad desde la perspectiva blue team, en la cual se dieron a conocer mecanismos de hardening, el monitoreo de los eventos mediante sistemas del tipo SIEM, la

aplicación de controles CIS, así como herramientas de seguridad como firewalls, EDR y NAC, haciendo hincapié en la importancia que tienen para reducir los riesgos y mejorar la postura de seguridad de las organizaciones. De esta forma, el trabajo ha permitido la fusión de los conocimientos teóricos y de los conocimientos prácticos en la materia de la prevención, detección y mitigación de los incidentes informáticos en entornos controlados, fomentando una concepción más amplia e integral de la ciberseguridad actual.

Justificación

La presente actividad es de gran relevancia puesto que la ciberseguridad se ha vuelto fundamental en el día a día de las organizaciones y personas que dependen de las tecnologías de la información. Al igual que el aumento de los ataques informáticos, la existencia de vulnerabilidades y amenazas hace imprescindible que las personas del sector conozcan tanto las metodologías que utilizan los atacantes con fines ofensivos como las que usan para defender la información y asegurar la continuidad operativa de las organizaciones. Así pues, el desarrollo de las cuatro fases permitió consolidar conocimientos relacionados con la identificación de riesgos, el análisis de la vulnerabilidad y, por último, la práctica de controles de seguridad sobre los sistemas tecnológicos.

A la vez, la investigación posibilitó entrelazar las facetas técnica, legal y ética que son esenciales dentro del desempeño profesional de la seguridad informática. El estudio de la legislación colombiana sobre cibercriminalidad y protección de los datos de carácter personal propició entender la transcendencia de la normatividad para la salvaguarda de la información. De igual forma, el análisis del caso “SecureNova Labs” propició la reflexión sobre el compromiso ético del profesional ante el uso de información sensible, el ciberespionaje y las posibles repercusiones legales como resultado de malas prácticas en la ciberseguridad. La actividad de trabajo colaborativo permitió establecer que la seguridad informática no depende solamente de herramientas tecnológicas sino también posee principios éticos y del correcto actuar profesional.

Por otro lado, la implementación del laboratorio práctico y el análisis de estrategias del blue team permitieron desarrollar habilidades en reconocimiento, explotación y contención de amenazas dentro de un ambiente controlado, mediante el uso de herramientas como Nmap, Metasploit, SIEM, EDR y controles CIS. Este enfoque facilitó la comprensión de la ejecución de ataques y la identificación de mecanismos adecuados para la prevención, detección y respuesta

ante incidentes de seguridad. De este modo, ha permitido mayor capacitación y desarrollo de las competencias técnicas y analíticas necesarias ante los nuevos retos de la ciberseguridad y una visión generalista orientada a la protección de la infraestructura tecnológica y de activos críticos de información.

Objetivos

Objetivo General

Analizar los fundamentos técnicos, legales, éticos y de defensa de la ciberseguridad a partir del estudio de las operaciones red team y blue team, la realización de laboratorios prácticos, y la aplicación de estrategias de prevención, detección y respuesta ante incidentes informáticos en ambientes controlados.

Objetivos Específicos

Identificar y analizar las principales normas colombianas referentes a la seguridad cibernética, enfocadas en la prevención de delitos informáticos y la protección de datos personales en entornos digitales, incluyendo su aplicación en casos reales.

Entender y poder aplicar las fases del pentesting mediante actividades de reconocimiento, escaneo, explotación y post-explotación en las máquinas virtuales.

Aplicar herramientas de la ciberseguridad como lo son Nmap, Metasploit, OpenVAS, servicios CVE para el análisis, la validación y la evaluación de vulnerabilidades en los sistemas de la información.

Evaluar la importancia de la ética profesional y las estrategias de respuesta a incidentes, considerando el cumplimiento del Código de Ética del COPNIA, así como el uso de mecanismos de hardening, controles CIS, SIEM, firewalls, EDR y NAC.

Desarrollo del informe

Fundamentos de operaciones red team y blue team

A continuación, se exponen los fundamentos de la ciberseguridad y las operaciones red team y blue team, así como a estudiar la legislación colombiana relacionada con delitos informáticos y protección de datos, junto con los conceptos básicos de pentesting, vulnerabilidades y herramientas utilizadas para la identificación de riesgos en entornos tecnológicos. También se da la posibilidad para estudiar a fondo conceptos detallados de cada uno de los temas expuestos, haciendo hincapié en la importancia de la ciberseguridad.

Análisis de la legislación relacionada con delitos informáticos

En Colombia, y en base a las diferentes normativas existentes en materia de delitos informáticos y en materia de protección de datos personales, se han evidenciado avances muy notables como respuesta a los peligros provenientes de la utilización de las tecnologías de la información.

Una de las leyes que más relevancia ha tenido es la Ley 1273 de 2009, la cual viene a introducir la protección de la información y la de los datos en calidad de "bien jurídico" protegido dentro del Código Penal colombiano, expuesto por el Congreso de la República de Colombia (2009).

Esta norma hace el tipo de conductas como el acceso abusivo a sistemas informáticos, la interceptación de datos informáticos, tanto de aquellos que se refieran a daños informáticos como de aquellos referidos al uso de software malicioso que permite sancionar todo tipo de acciones que menoscaban la confidencialidad, integralidad y disponibilidad de la información. Según el Congreso de la República de Colombia esta norma es un avance muy importante ya que adapta la normatividad penal existente a los entornos digitales.

Por otro lado, la Ley 1581 de 2012 establece el régimen general de protección de datos personales en Colombia, comprendiendo para tal efecto el derecho que tienen todas las personas a conocer, actualizar y rectificar la información completa o parcial que repose en bases de datos, según el Congreso de la República de Colombia (2012). Esta política se fundamenta en la existencia de suficientes principios, como la legalidad, finalidad, libertad, veracidad, transparencia y seguridad, los cuales deberán ser aplicables por las organizaciones en la utilización de datos personales.

Por otra parte, el Decreto 1377 de 2013 regula aspectos concretos de la Ley 1581, tales como la autorización del titular, las políticas del tratamiento de datos y los procedimientos para consultas y reclamo, Ministerio de Comercio, Industria y Turismo (2013). Este decreto permite operacionalizar la ley y poder llevarla a la práctica en la práctica organizacional.

En resumen, estas normas constituyen un marco jurídico fuerte que no solo sanciona los delitos informáticos, sino que también se hace eco de la adecuada gestión de la información, además de permitir un mínimo cumplimiento de la aplicación de las normas para la seguridad de la información, con lo cual se tiende a contrastar con los esfuerzos en la aplicación internacional de la seguridad de la información.

Análisis sobre el ejercicio de Pentesting

El pentesting, también conocido como prueba de penetración, constituye una de las prácticas más relevantes en la ciberseguridad ofensiva. Esta metodología permite a las organizaciones evaluar su postura de seguridad de manera controlada mediante la simulación de ataques cibernéticos reales. El propósito de este procedimiento no es solo identificar las vulnerabilidades, sino también evaluar su efecto y la habilidad de reacción de los sistemas y equipos de seguridad del cliente. Sin duda, el pentesting está organizado con un método que

asegura la legalidad, la trazabilidad y la eficacia de las pruebas, según lo establece el NIST (2018). A continuación, se describe las etapas principales.

Reconocimiento

El objetivo de esta fase inicial es obtener la mayor cantidad de datos sobre el objetivo. Se dividirá en:

- Reconocimiento pasivo: Sin interacción directa con el sistema, por ejemplo, búsqueda en redes sociales, DNS o WHOIS.
- Reconocimiento activo: Interacción directa con el objetivo, esto ocurre al escanear una red.

En este paso se encuentran activos digitales, como direcciones IP, dominios, subdominios, infraestructura de IT, puntos de acceso, etc.

Lyon (2009) dice que herramientas como Nmap permiten encontrar hosts, servicios y ayuda a formar el primer esbozo de la superficie de ataque.

Desde un punto de vista estratégico, esta fase es importante, pues un reconocimiento bien realizado disminuye la incertidumbre y potencia las probabilidades de éxito en el siguiente paso.

Escaneo y Enumeración

En esta etapa se realiza un análisis detallado de los objetivos con el propósito de identificar vulnerabilidades específicas en los sistemas evaluados, mediante la ejecución de las actividades descritas a continuación: escaneo de puertos (TCP/UDP); identificación de versiones de servicios; detección de sistemas operativos y enumeración de usuarios, recursos compartidos y configuraciones.

La enumeración ayuda a recopilar información sensible que normalmente no se revela, tal es el caso de cuentas de usuario o políticas internas de sistema.

Para Scarfone y Mell (2007), esta tarea es extremadamente importante para identificar debilidades explotables en el sistema, ya que le permite correlacionar los servicios activos encontrados con las vulnerabilidades disponibles en la documentación pública de dicha vulnerabilidad, y herramientas de análisis automatizado como NMAP o OpenVAS pueden integrarse con bases de datos como es el caso de CVE para mejorar la precisión de la evaluación.

Explotación

En este punto se procura hacer uso de las vulnerabilidades detectadas previamente en orden de hacer que el sistema caiga en revisión. Cuando para ejecutar pruebas de penetración, se pone en práctica el trabajo de sistemas que simulan ataques reales mediante la ejecución de técnicas como:

- Inyecciones SQL.
- Ejecución remota de código, RCE.
- Ataques de fuerza bruta.
- Explotaciones de desbordamientos de buffer

Usar sistemas de tipo framework como Metasploit, le permite a quien se encarga de la ejecución de explotación automatizar la ejecución de exploits, así como verificar si alguna vulnerabilidad es realmente explotable Center for Internet Security (s.f.).

Esta fase, en términos de ética, debe ser efectuada con el estricto marco de controles y autorizaciones en donde se interactúa contra sistemas productivos.

Post-Explotación

Una vez que se ha conseguido comprometer el sistema de un cliente, el siguiente paso es realizar un análisis de la extensión del acceso conseguido. En esta fase se llevan a cabo acciones como:

- Escalamiento de privilegios: Obtención de permisos con el nivel de Administrador del sistema.
- Movimiento lateral: Ingreso en otros sistemas existentes dentro de la red.
- Persistencia: Mantener el acceso al sistema expuesto.
- Exfiltración de datos: Arrancar alguna porción de información sensible

Esta etapa permite calcular el impacto real de un ataque. Se colocará como ejemplo que una vulnerabilidad que de una indicación de apertura capaz de dar acceso completo a la infraestructura crítica que rodea a una organización ejemplo con Metasploit.

Según NIST (2018), esta fase es muy importante para entender el impacto que desarrolla una brecha y permite justificar la creación de controles adicionales para prevenir una amenaza futura.

Reporte

El informe es el producto final del pentesting y también uno de los elementos más importante de todo el proceso, el cual debe incluir:

- Descripción pormenorizada de vulnerabilidades.
- Evidencias (capturas, logs, pruebas)
- De nivel de criticidad (alto, medio, bajo)
- Impacto en el negocio
- Recomendaciones de mitigación

Un buen informe no sólo habla sobre el problema técnico, sino que traduce los hallazgos en un lenguaje entendible para poder tomar decisiones estratégicas.

Según el NIST (2018), un informe de buena calidad influye de forma directa en el nivel de mejora de la organización en su postura de seguridad.

Análisis de herramientas de ciberseguridad

En torno a los temas asociados a la ciberseguridad, el uso de herramientas especializadas y servicios en línea es muy importante para poder identificar, explotar y gestionar vulnerabilidades. Estas herramientas permiten a los expertos simular ataques, realizar análisis de infraestructuras y, por último, mejorar controles de seguridad en las organizaciones.

Herramientas de ciberseguridad

Metasploit: Se trata de un framework de código abierto muy famoso para ejecutar procesos de pruebas de penetración. Esta herramienta permite desarrollar, probar y ejecutar exploits contra sistemas con vulnerabilidades.

Metasploit dispone de una base de datos de vulnerabilidades y módulos que proveen automatizar ataques, lo cual significa que se puede verificar fallos de seguridad en entornos controlados, e incluso funciones de post-explotación, como escalada de privilegios, persistencia y recolección de datos.

"Metasploit es la herramienta fundamental para realizar procesos de evaluación de seguridad, ya que es capaz de reproducir escenarios reales de ataque y medir el impacto de vulnerabilidades identificadas" Center for Internet Security (s.f.).

Nmap: Network Mapper es una aplicación de código abierto diseñada para el descubrimiento de redes y la auditoría de seguridad. Permite el descubrimiento de dispositivos conectados, de puertos abiertos, de servicios en ejecución y de sistemas operativos según lo indicado por Nmap Project (2024).

Es una herramienta muy versátil, ya que permite realizar escaneos avanzados (detección de versiones, evasión de firewalls, ejecución de scripts mediante el NSE (Nmap Scripting Engine)).

Según Lyon (2009), Nmap es una herramienta clave de las fases iniciales del pentesting, pues permite recopilar información útil para pasar a la identificación de la superficie de ataque.

OpenVAS: Open Vulnerability Assessment System es un escáner de vulnerabilidades que permite detectar las fallas en sistemas, redes y aplicaciones. Funciona mediante la utilización de pruebas de seguridad conocidas (NVTs) y que son constantemente actualizadas, para poder detectar nuevas vulnerabilidades, según OpenVAS (s.f.).

Esta aplicación genera informes detallados, que clasifican las vulnerabilidades según su criticidad, lo que permite realizar una priorización de las medidas correctivas.

OpenVAS es una buena solución para la gestión continua de la vulnerabilidad Greenbone Networks (s.f.), sobre todo en entornos organizacionales que requieren monitorización continua.

Servicios en línea de ciberseguridad

ExploitDB: Exploit Database es un repositorio público que permite consultar información sobre vulnerabilidades, exploits o Proof of Concept (PoC). Nos permitirá que los profesionales de la seguridad estudien el funcionamiento de los exploits y cómo están hechas tales vulnerabilidades.

Se adopta en el ámbito académico como parte del desarrollo de investigaciones para el aprendizaje.

La información crítica sobre las vulnerabilidades que pueden ser encontradas mediante este servicio, ayudará con el desarrollo de estrategias defensivas (en el uso de ExploitDB) Center for Internet Security (s.f.).

CVE: Common Vulnerabilities and Exposures es un estándar internacional que asigna identificadores únicos a las vulnerabilidades en la seguridad, haciendo posible una mejor manera de organizar, hacer seguimiento y correlacionar la información en diferentes herramientas y plataformas de seguridad.

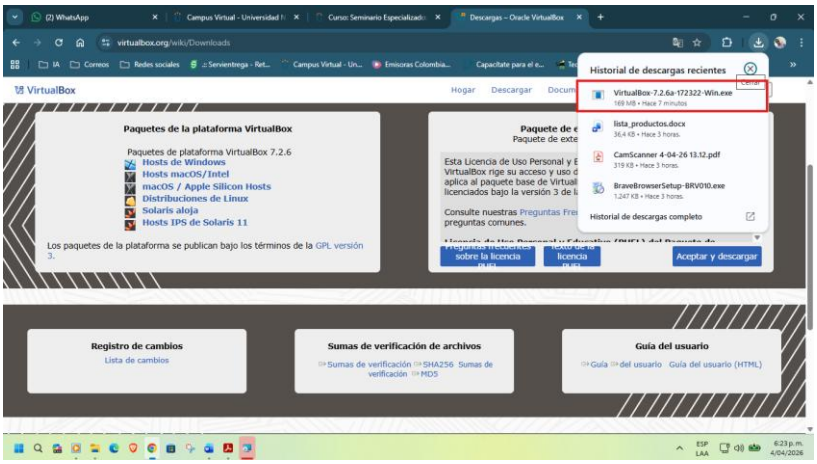
Cada vulnerabilidad publicada en CVE ofrece una descripción, referencias y su identificador único, el cual ayuda a la propia correspondencia y descripción de la vulnerabilidad.

De acuerdo con MITRE Corporation (s.f.), el CVE es de particular importancia para estandarizar la forma de describir información sobre vulnerabilidades, y puede ayudar enormemente a la comunicación entre los profesionales.

Evidencia de la implementación del montaje del banco de trabajo

Figura 1

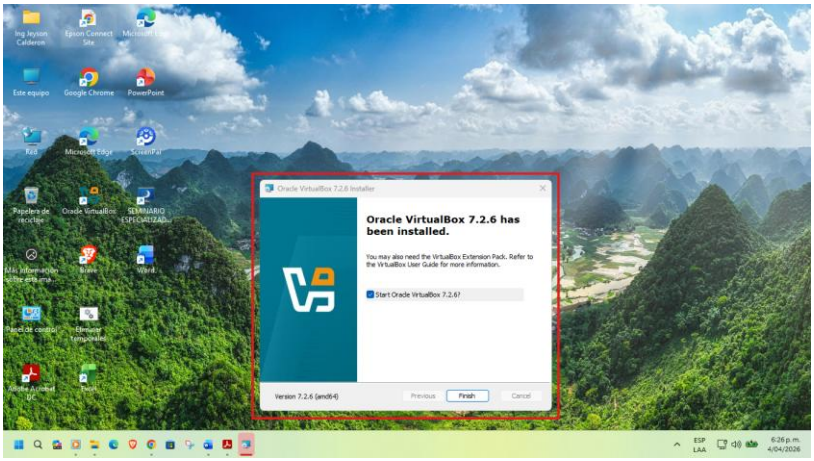
Descarga de la herramienta VirtualBox



Nota. Proceso de descarga de Oracle VirtualBox desde su sitio oficial, herramienta base para el despliegue de las máquinas virtuales que conformarán el laboratorio de pentesting en un entorno aislado y controlado.

Figura 2

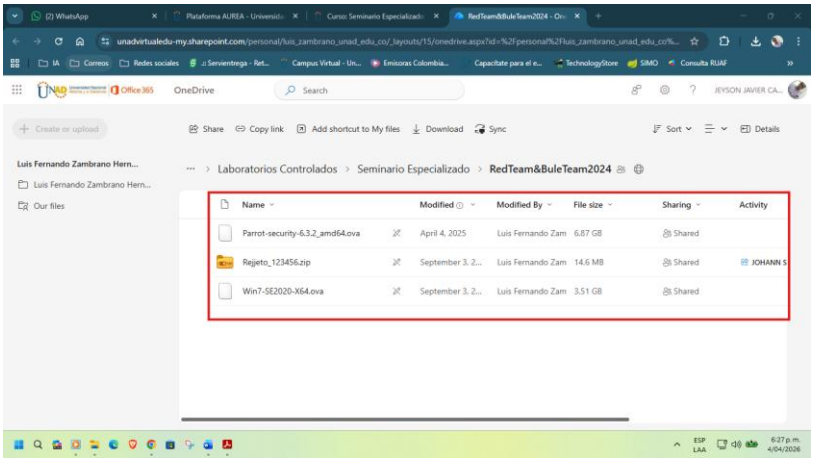
Instalación de la herramienta VirtualBox



Nota: Asistente de instalación de VirtualBox, el cual culmina el proceso de instalación de la aplicación para su uso, para garantizar el funcionamiento óptimo de las máquinas virtuales durante las fases de escaneo y explotación.

Figura 3

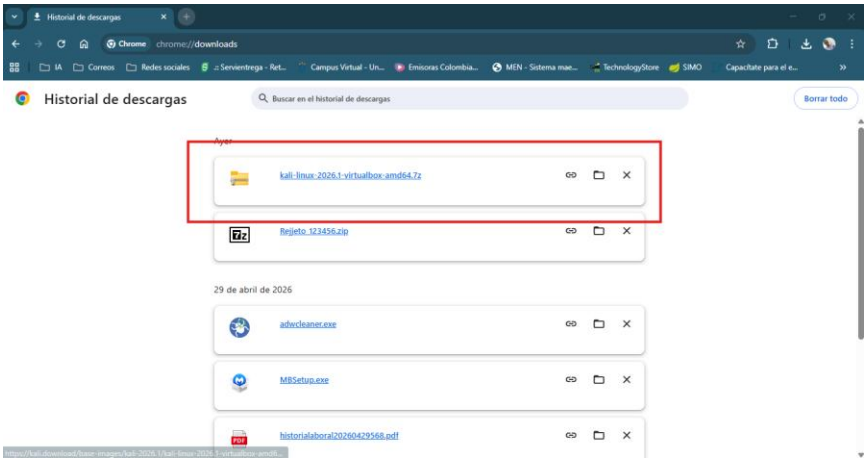
Ingreso al repositorio para descargar de recursos objeto de estudio



Nota: Obtención de Rejetto HFS (aplicación vulnerable) y la imagen de Windows 7 desde el repositorio. Estos recursos serán desplegados en la Victim Machine e Internal Machine para simular servicios susceptibles de explotación durante el laboratorio.

Figura 4

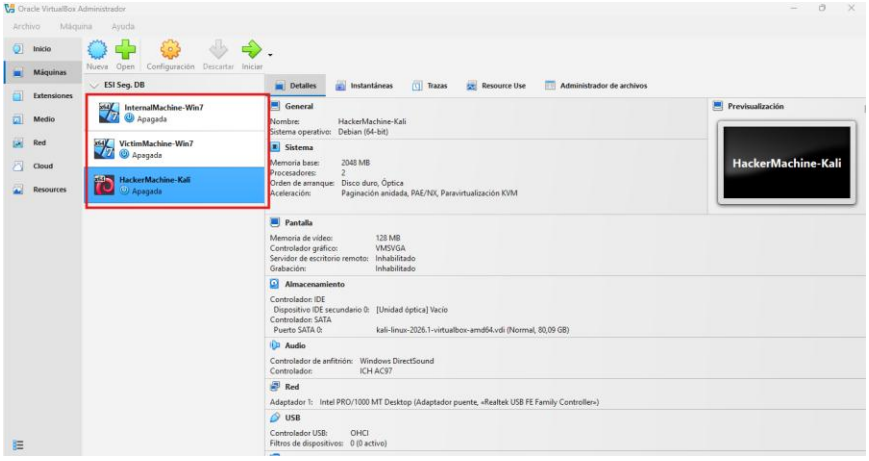
Descarga de Kali Linux última versión Hacker Machine



Nota: Descarga de Kali Linux desde el repositorio oficial, distribución especializada en pentesting que actuará como Hacker Machine, proporcionando herramientas nativas como Nmap, Metasploit Framework y Meterpreter para las fases de reconocimiento, explotación y post-explotación.

Figura 5

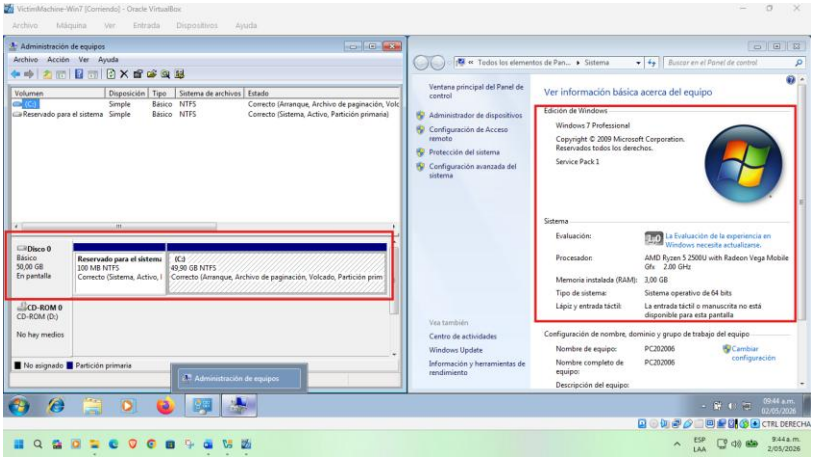
Máquinas debidamente montadas en el entorno de virtualización



Nota: Vista general de las tres máquinas virtuales configuradas: Hacker Machine (Kali Linux), Victim Machine (Windows 7) e Internal Machine (Windows 7). Esta arquitectura permite reproducir un escenario de ataque realista con pivoting y movimiento lateral.

Figura 6

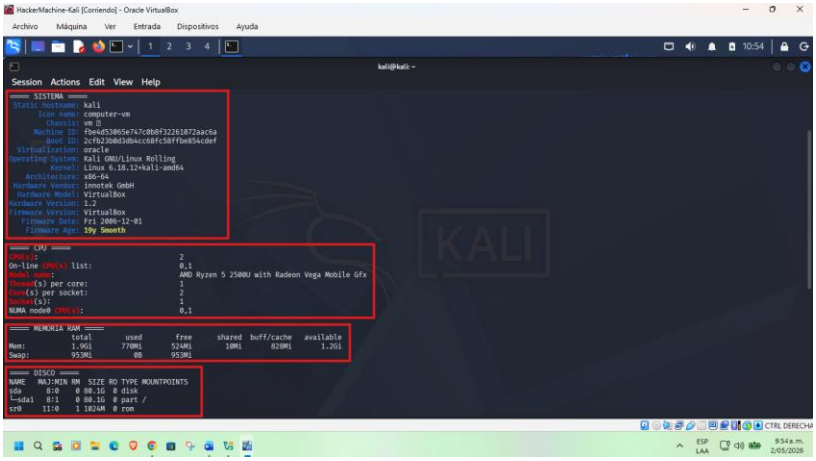
Máquina con Windows 7 instalada y características de esta.



Nota: Panel de sistema de Windows 7 Professional mostrando las especificaciones asignadas (procesador, 3 GB RAM, 50 GB disco). Este sistema fue seleccionado por contener vulnerabilidades conocidas (SMBv1, EternalBlue) que serán explotadas durante el laboratorio.

Figura 7

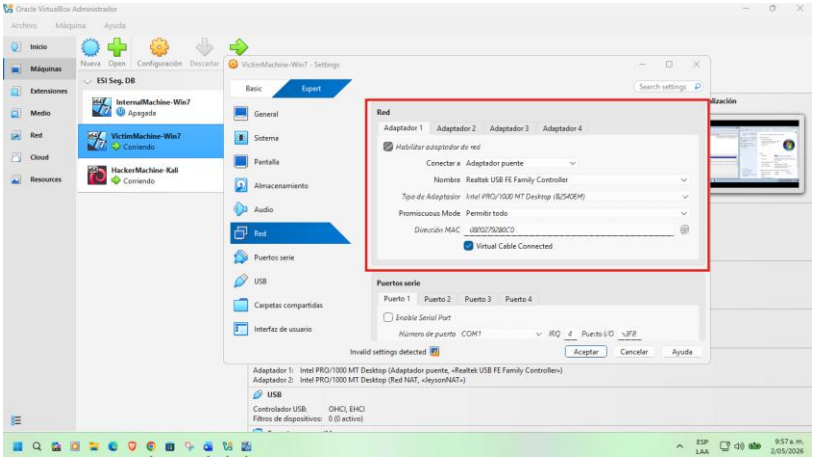
Máquina con Linux instalada y características de esta



Nota: Terminal de Kali Linux mostrando la versión del kernel y los recursos asignados (2 GB RAM, 80 GB disco). Esta máquina concentra las herramientas ofensivas necesarias para ejecutar las fases completas del pentesting.

Figura 8

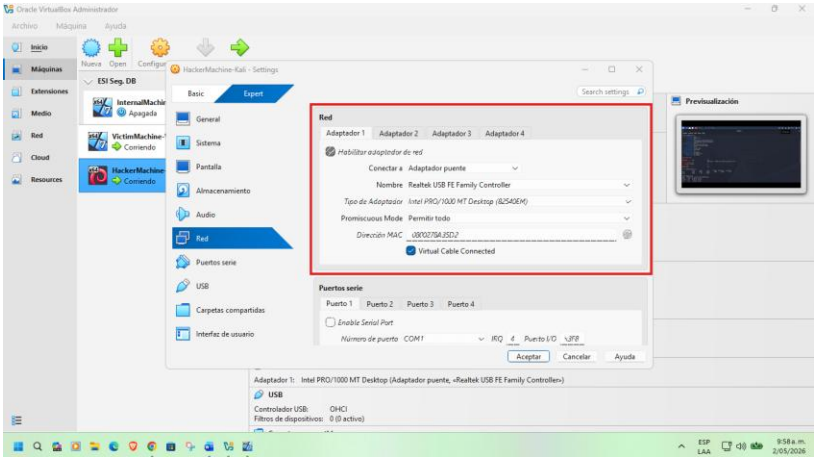
Configuración del adaptador de red como adaptador puente Windows



Nota: Configuración de red de la Victim Machine en modo "Adaptador Puente", permitiendo obtener una IP dentro de la subred física del host y facilitando la comunicación directa con la Hacker Machine para las fases de reconocimiento y explotación.

Figura 9

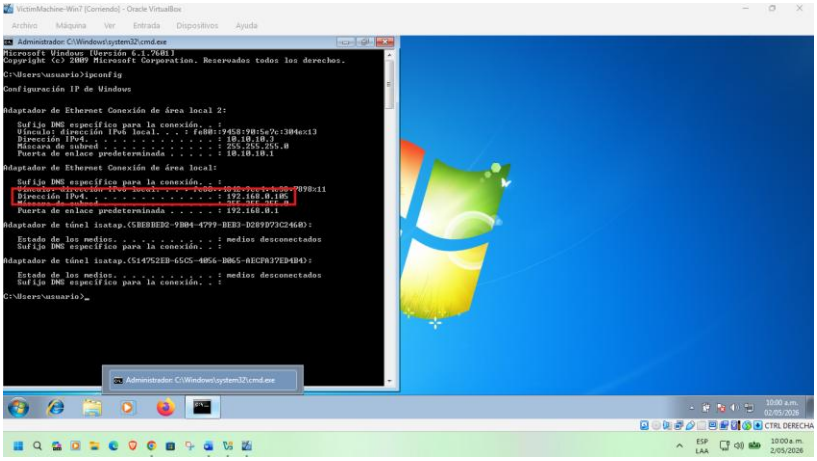
Configuración del adaptador de red como adaptador puente Linux



Nota: Configuración de red de Kali Linux en modo "Adaptador Puente", posibilitando el descubrimiento de hosts mediante arp-scan y la ejecución de escaneos de puertos con Nmap sin restricciones de enrutamiento.

Figura 10

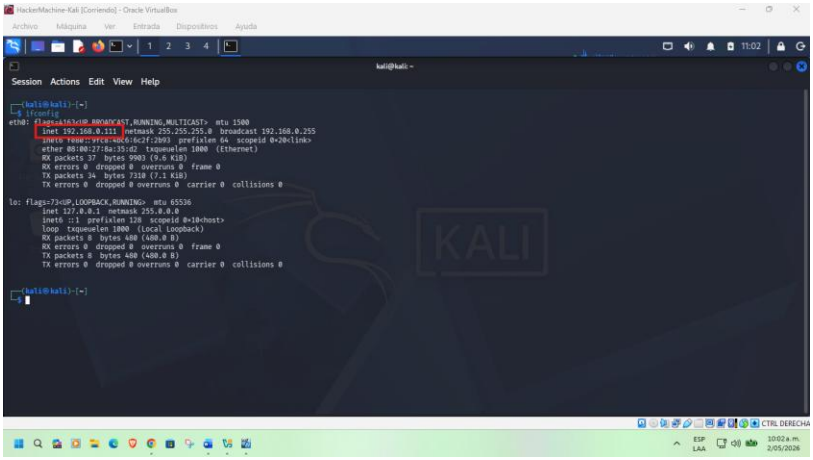
Con el comando IPCONFIG se obtiene la dirección IP en Windows



Nota: Ejecución del comando ipconfig en Windows mostrando la IPv4 asignada (192.168.56.105). Esta información es crítica para configurar correctamente las herramientas de escaneo y explotación apuntando al objetivo específico.

Figura 11

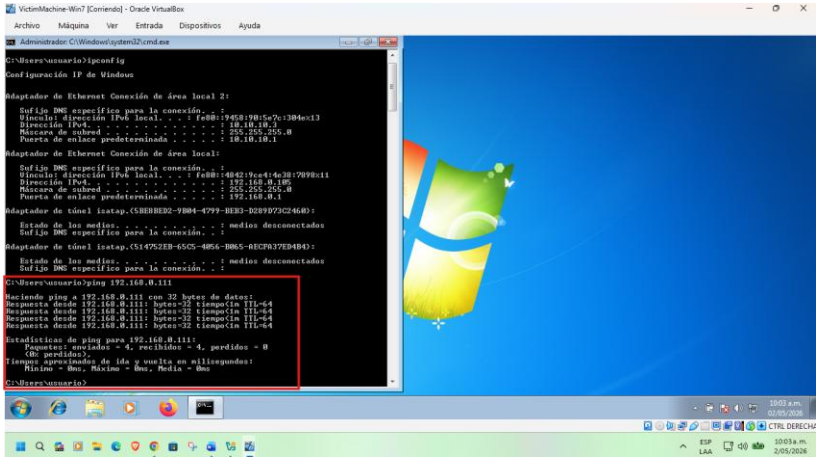
Con el comando IFCONFIG se obtiene la dirección IP en Linux



Nota: Comando ifconfig en Kali Linux revelando la IP 192.168.56.111 en el mismo segmento de red que la Victim Machine, validando la conectividad necesaria antes de iniciar el reconocimiento activo.

Figura 12

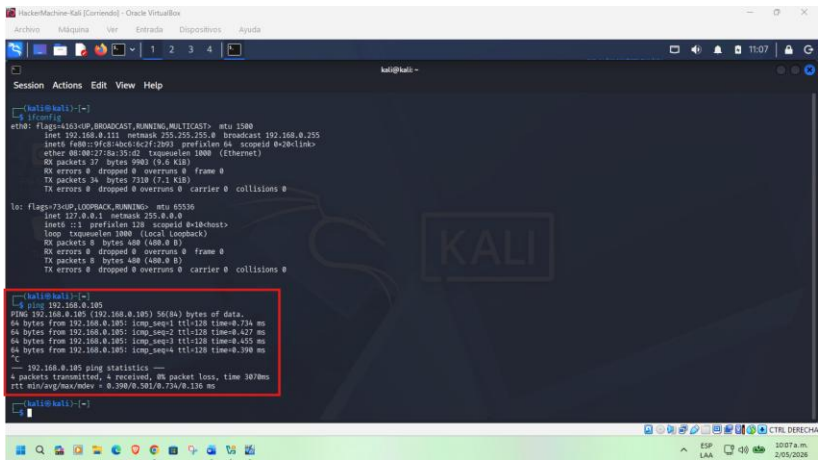
Ping a la dirección IP de la máquina con Linux desde Windows



Nota: Comando ping desde la Victim Machine hacia Kali Linux con respuesta exitosa, confirmando comunicación bidireccional y ausencia de bloqueo ICMP, requisito previo para el escaneo de puertos.

Figura 13

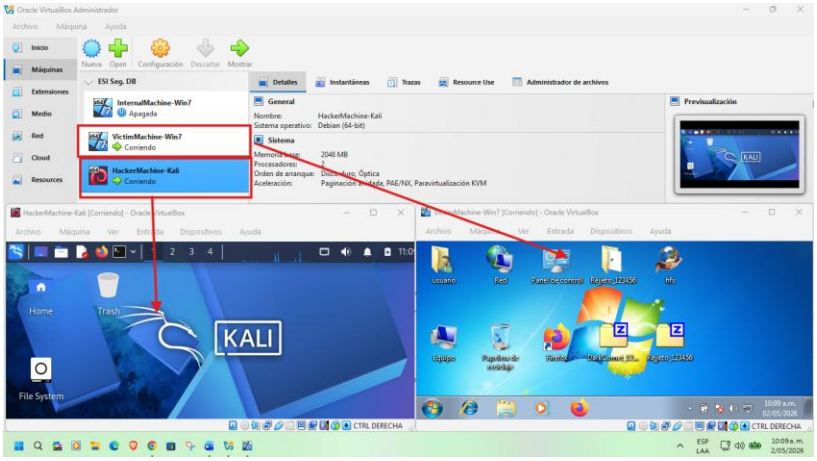
Ping a la dirección IP de la máquina con Windows desde Linux



Nota: Comando ping desde Kali Linux hacia la Victim Machine con respuesta exitosa, validando que el objetivo está activo y accesible para las herramientas de reconocimiento y explotación.

Figura 14

Montaje del banco de trabajo



Nota: Vista simultánea de las tres máquinas virtuales en ejecución, confirmando que el entorno de laboratorio está completamente funcional y listo para iniciar las actividades de pentesting: reconocimiento, explotación, pivoting y post-explotación.

Despliegue del montaje

El banco de trabajo fue puesto en funcionamiento mediante la utilización de la herramienta de virtualización Oracle VM VirtualBox, mediante la cual se desplegaron las dos máquinas virtuales: una máquina con el sistema operativo Windows 7 y otra máquina con Kali Linux bien habilitada. Las dos máquinas de trabajo se configuraron utilizando un adaptador de red en modo adaptador puente, de forma que tuviesen acceso a Internet a través de este medio, para que pudiesen comunicarse entre sí, simulando así un entorno controlado de pruebas.

Por lo que respecta a las características técnicas, a cada infraestructura de máquina virtual se le establecieron unas cualidades de trabajo adecuadas para conseguir un rendimiento adecuado en la ejecución de las herramientas de seguridad informática.

Para validar la conectividad, se llevó a cabo una prueba por medio del comando ping, que determinó comunicación satisfactoria entre ambas máquinas, confirmando el correcto funcionamiento del tipo de entorno de trabajo en banco de trabajo para conseguir el laboratorio de pruebas y trabajo estable para las herramientas de seguridad informática

Características técnicas de Windows

- Memoria RAM: 3 GB
- Procesador: AMD Ryzen 5 2500U with Radeon Vega Mobile Gfx (2.00 GHz)
- Disco Duro: 50 GB
- Sistema Operativo: Windows 7 Professional
- Dirección IP: 192.168.56.105

Características técnicas de Kali Linux

- Memoria RAM: 2 GB
- Procesador: AMD Ryzen 5 2500U with Radeon Vega Mobile Gfx (2.00 GHz)
- Disco Duro: 80 GB
- Sistema Operativo: Kali GNU/Linux Rolling
- Dirección IP: 192.168.56.111

La máquina marcada como Internal Machine está clonada de la Victim Machine por lo cual las características son idénticas entre ellas, cambia simplemente la dirección IP

Ética profesional y marco normativo en ciberseguridad

Se analiza las actividades de los equipos red team y blue team en el contexto organizacional, considerando los aspectos éticos y legales aplicables.

Identificación de procesos ilegales y no éticos en el acuerdo

Al realizar un análisis crítico del Anexo 3 – Acuerdo, se detecta la existencia de muchas cláusulas que no solo carecen de validez ética, sino que también podrían ser constitutivas de una vulneración del ordenamiento jurídico colombiano. Desde la óptica de un experto en seguridad informática, este tipo de documentos deben evaluarse tal como lo establece la legislación, pero también de acuerdo con los principios de confidencialidad, integridad y disponibilidad de la información (la información no se pierde, no es de ningún modo manipulable, etc.) y del respeto por los derechos fundamentales, tanto humanos como de la civilización.

"la información confidencial o sobre procesos ilegales dentro de SecureNova Labs no podrán ser divulgados" (UNAD, s.f.).

Esta cláusula me parece de una gran criticidad, ya que extiende la obligación de confidencialidad a prácticas ilegales. Desde el punto de vista jurídico esto resulta ineficaz, pues ningún contrato puede obligar a una persona a encubrir comportamientos delictivos. Desde la perspectiva de la seguridad de la información, esto sería una derivación crítica del principio de legalidad y del deber de reporte de incidentes.

Adicionalmente, se establece:

"No denunciar ante las autoridades actividades sospechosas de espionaje..." UNAD (s.f.)

Este punto resulta ser una clara vulneración del deber ciudadano y profesional de reporte de delitos. En el ámbito de la ciberseguridad, el deber de no notificar puede dar lugar a la continuidad de amenazas o vulneraciones, que afectan en primer lugar a toda organización y asimismo a terceros.

Un tercer elemento para tener en cuenta y también relevante es que se reitera o se establece que las actividades delictivas quedan inclusas en la definición de lo que se considera información confidencial:

“datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos” UNAD (s.f.).

Esta parte refleja una normalización de actos asociados al ciberespionaje y/o a acceder sin consentimiento a sistemas, lo cual va en la línea de los principios éticos propios de la profesión.

Con todos estos elementos en cuenta, el documento finalmente establece:

- Un uso fraudulento de la confidencialidad.
- Una intención encubridora de la actividad delictiva.
- Una falta de alineación con las normas internacionales de ciberseguridad.

Por lo tanto, desde un análisis técnico de la cuestión, unido a la cuestión ética de la misma, se puede concluir sin dudar en que el documento no es ni de fiar ni aceptable en un contexto profesional medianamente serio.

Vulneración de la Ley 1273 de 2009

Las prácticas contenidas en el acuerdo pueden encuadrarse en una variedad de conductas tipificadas por la Ley 1273 de 2009, que establece la protección de la información y los sistemas informáticos como bien jurídico, de acuerdo con el Congreso de la República de Colombia (2009).

En primer lugar, el punto se refiere a accesos no permitidos, lo que se vincula con:

Artículo 269A – Acceso abusivo a un sistema informático

Este delito castiga el acceso sin autorización a los sistemas informáticos. La forma de referirse a este tipo de prácticas dentro del acuerdo refleja una posible implicación en actividades delictivas.

Artículo 269C – Interceptación de datos informáticos

La mención de interceptación de información va directamente relacionada con este delito, que castiga la interceptación no autorizada de información.

Artículo 269F – Violación de datos personales

El tratamiento de información sensible puede llegar a tener como consecuencia la vulneración de este código, así como de derechos fundamentales tales como la privacidad.

Desde una perspectiva técnica aludida, estas conductas van en detrimento de la confidencialidad de la información, uno de los ejes de la seguridad informática. Desde una perspectiva delictiva estas prácticas pueden implicar responsabilidades penales tanto para el ejecutor como para quien encubre.

La prohibición de denunciar este tipo de prácticas pone a las partes en riesgo jurídico agravado, es decir, impide que se produzcan acciones para evitar dichas conductas, dificultando la acción e impidiendo que se frene el proceso delictivo.

Decisión profesional frente a la oferta laboral (enfoque ético y COPNIA)

Desde una óptica profesional, ética y técnica, nunca la decisión de aceptar una oferta laboral puede sustentarse solamente en criterios económicos. En este caso, aunque la retribución que se indica es muy elevada, la naturaleza del compromiso que se recoge y las prácticas que se describen ineludiblemente suponen incluso un choque directo con los mismos principios fundamentales del ejercicio profesional.

El Código Ético del COPNIA expresa que el ingeniero debe actuar con responsabilidad, con integridad, con transparencia y respeto por la ley; debe no participar en actividades que pudieran afectar a la sociedad. COPNIA (s.f.). En este caso, aceptar la oferta significa:

- Ser cómplice de una posible actividad ilegal.
- Comprometer la integridad profesional.

- Asumir riesgos legales y reputacionales.

Desde el enfoque de la ciberseguridad el profesional debe ser garante de la protección de la información y no cómplice de su vulneración.

Además, este tipo de situaciones pone de manifiesto la relevancia del juicio ético profesional, el cual debe primar incluso ante incentivos económicos elevados.

En consecuencia, la decisión más correcta es la negativa a la oferta, priorizando la legalidad, la ética y la sostenibilidad de la carrera profesional.

Análisis del caso "Ciberespionaje y Ética en SecureNova Labs"

La situación expuesta describe el hecho de que una organización de carácter internacional presenta disociaciones internas que pueden derivar en ciberespionaje, lo cual de una forma más técnica es debido a una mala praxis en el gobierno de la seguridad de la información. Este comportamiento también puede ser suscrito en el ámbito de la legalidad, en el que puede ser configurado como un delito informático, perjudicar el derecho a la privacidad y atentar contra la información sensible.

Esta forma de ilustrar la práctica ciberespionaje también puede ser retribuida a nivel organizacional y en estos términos no puede dejar de reconocer que el mismo ilustra las deficiencias en materia de:

- Gestión del riesgo.
- Control interno.
- Supervisión de procesos legales.

A nivel ético, el caso evidencia la contradicción interna entre la imagen corporativa y la forma de práctica de la organización en tejidos internos, lo cual merma la confianza de los clientes y otros interesados.

Esta forma de práctica ciberespionaje es otra de las formas de indicar que la ciberseguridad no depende únicamente de la tecnología, sino también de la cultura organizacional que le provee viabilidad a la misma en cuanto a la ética y la legalidad.

Acceso a información sensible en auditorías

La obtención de información sensible en el marco de una auditoría de seguridad es un elemento de carácter indefectible y necesario dentro de los procesos de evaluación de carácter técnico, pero supone, al mismo tiempo, uno de los máximos riesgos desde el enfoque ético, legal y operativo. Como experto en seguridad informática, hay que tener claro que dicha obtención de información puede hacerse bajo la condición de llevarla a cabo bajo un enfoque de control estricto, de trazabilidad y de responsabilidad profesional.

Las auditorías de seguridad demandan visibilidad sobre los activos críticos, las configuraciones, las credenciales, los logs de eventos y hasta la información confidencial para detectar las vulnerabilidades efectivas y así determinar la postura de seguridad de la organización. Sin embargo, esto puede suponer un vector de riesgo si el acceso no es gestionado como es debido. Por este motivo, el acceso tiene que estar limitado según el principio de menor privilegio, en donde cada auditor debe poder acceder a la información exclusivamente necesaria para el cumplimiento de la función. NIST (2018).

Desde la perspectiva técnica, ya implica implementar controles como:

- Gestión de identidades y accesos (IAM), que permita dotar de permisos temporales y controlados.
- Autenticación multifactor (MFA), que reduzca el riesgo de accesos no controlados.
- Registro y monitoreo de actividades (logging), que garantice la trazabilidad de las acciones realizadas por los auditores.

A la vez que, debe ser evidente que dicho acceso esté legitimado mediante acuerdos de confidencialidad (NDA) bien firmados, cuyo contenido debe ser legalmente válido (por contra debe ser tachado, como se ha evidenciado en el caso SecureNova Labs) y no incluir cláusulas abusivas o contrarias a la ley. Estos acuerdos deben especificar explícitamente:

- El alcance del acceso.
- El uso de la información.
- Las obligaciones del auditor/contratista.
- Las sanciones en caso de incumplimiento.

Desde la perspectiva ética, el profesional en ciberseguridad debe actuar sobre principios de integridad, confidencialidad y responsabilidad, garantizando que la información a la que accede no sea utilizada para fines no consentidos. Este aspecto también está en línea con los estándares internacionales como el ISO/IEC 27001 que subrayan la protección como el aspecto básico de la seguridad.

Otro aspecto fundamental sería la utilización de ambientes controlados de auditoría como laboratorios aislados o bien máquinas virtuales, que permitan la ejecución de pruebas a partir de las auditorías informáticas sin afectar directamente a los sistemas productivos. Esto minimizará el riesgo de impacto operacional y, a su vez, limitaría la exposición de información sensible.

Las organizaciones igualmente deberían establecer mecanismos de supervisión continua, de forma tal, que las diferentes actividades de los auditores fuesen revisadas por equipos tanto internos como externos, puesto que esto ayudaría a la detección de comportamientos atípicos y, de hecho, a prevenir abusos.

En último lugar, desde el punto de vista legal, el acceso a información sensible deberá ajustarse a normativas como la protección de datos personales o la legislación referente a delitos instruccionales; un uso indebido de dicha información podría tener consecuencias penales tal

como lo establece la Ley 1273 de 2009 en Colombia como lo indica el Congreso de la República de Colombia (2009).

En conclusión, el acceso a información sensible dentro de un proceso de auditoría informática es necesario; sin embargo, este debe estar bien regulado por medio de controles técnicos, legales o de tipo ético. La idea es que cada una de las partes se encuentre en equilibrio, es decir, en que la auditoría permita hacer un examen lo suficientemente profundo de la información sensible, sin importar si se corren nuevos riesgos que en particular podría causar la auditoría. La auditoría informática debe servir para asegurar que la organización se encuentra a salvo en su entropía y en el presente control; por lo tanto, debe enriquecer sus controles y, ante todo, su seguridad informática.

Mecanismos de supervisión y control en empresas de ciberseguridad

En la situación actual en la que las herramientas de ciberseguridad cuentan con capacidades muy avanzadas (análisis forense, explotación vulnerabilidades, acceso a sistemas), la necesidad de establecer mecanismos de supervisión y control es fundamental porque el insider threat es uno de los riesgos más críticos.

Desde un punto de vista profesional, es necesario contar con medidas además de desear que el analista tenga ética individual; hay que diseñar un entorno controlado en el que las acciones sean trazables, auditables y justificables.

Uno de los mecanismos más destacados es la segregación de funciones, que permite que nunca haya un único profesional que controle un proceso crítico. Si realizara el análisis la misma persona que aprueba o valida los resultados, el riesgo de abuso de privilegios sería mayor.

De forma adyacente, el uso de sistemas de monitoreo continuo como los sistemas SIEM (Security Information and Event Management) facilita registrar y analizar todas las actividades de los usuarios generando alertas ante comportamientos anómalos. Este tipo de control es

fundamental para detectar accesos no autorizados o un uso no autorizado de herramientas, según Singer y Friedman (2019).

Otro de los aspectos de suma importancia lo constituyen los controles de acceso basados en roles (RBAC), también el principio de mínimo privilegio, para asegurar que cada usuario pueda acceder únicamente a la información que realmente necesita para sus tareas NIST (2018), limitando así las acciones en caso de que un usuario pretenda llevar a cabo acciones no autorizadas.

Se debe definir políticamente el uso de herramientas de ciberseguridad, en el cual que se incluyan aspectos tales como los límites de acción, los procedimientos permitidos y las consecuencias ante infracciones, alineando estas políticas con estándares internacionales como ISO/IEC 27001.

Las auditorías internas y externas son otro de los aspectos que tienen un peso relevante a la hora de evaluar periódicamente el cumplimiento de la política y de las desviaciones. Si se entiende desde el plano de la mejora continua, sirven para consolidar aún más la postura de seguridad organizacional.

Por lo tanto, los mecanismos de control han de ir acompañados de tecnología, procesos y cultura organizacional de forma que el uso de herramientas avanzadas pueda adaptarse a un uso ético, legal y controlado.

Respuesta ante actos de ciberespionaje y restauración de la confianza

Cuando una entidad se percata de que una empresa de ciberseguridad comprometida con la organización lleva a cabo prácticas de espionaje, la reacción ha de ser inmediata, formal, estructurada y debe responder a aspectos éticos y legales. Este tipo de incidentes tienen implicaciones desde un punto de vista técnico, como así también de carácter reputacional y legal, de alto impacto.

En primer lugar, es necesario hacer una comunicación formal a la autoridad competente ya que este tipo de conductas podrían haber constituido delitos informáticos conforme a normas de derecho positivo. El Congreso de la República de Colombia (2009) en la Ley 1273 de 2009 por medio de la cual se modifica el Código Penal y se crea el bien jurídico de la protección de la información y de los datos. De no abrir esta fase, la organización podría llegar a tener responsabilidad de lo sucedido.

Simultáneamente, se ha de llevar a cabo una investigación forense digital, por medio de la cual se determinará el alcance del incidente, los sistemas afectados, datos sensibles, organización, presuntos responsables, etc. Este tipo de investigaciones deben ser realizadas por un equipo independiente que permita dar certeza a la organización de que se están obteniendo los resultados en forma objetiva.

La interrupción en la vinculación, la terminación de contratos, la revocación de accesos a sistemas, redes o bases de datos, son algunas de las acciones que también tienen cabida, pues permiten dar contención a la incidencia, evitando con ello que continúe la fuga o manipulación de información.

Desde el punto de vista de la estrategia, es necesario implementar un plan de gestión de crisis que contemple que exista comunicación con las partes afectadas (clientes, partners, entidades reguladoras) y donde la transparencia es clave para mantener la credibilidad institucional.

De manera a restaurar la confianza, la organización tendrá que aplicar medidas correctivas como:

- Reforzar los controles de acceso.
- Aplicar auditorías externas independientes.
- Revisar políticas de contratación y de selección de proveedores.

- Alinear los estándares de seguridad con los estándares internacionales.

Para el NIST (2018), la adecuada gestión de incidentes permite incrementar la resiliencia de la organización y evitar la recurrencia.

Por último, desde la óptica de la ética, este tipo de situaciones refuerza la necesidad de las empresas de ciberseguridad de tener que basar su actuación en principios de responsabilidad, legalidad y transparencia. La confianza es un activo esencial en este sector y perderla puede resultar irreversible.

En consecuencia, la reacción a un ciberespionaje debe ser completa, es decir, una combinación de acciones legales, técnicas y estratégicas cuyo objetivo sea mitigar el impacto teniendo como objetivo la sanción del ataque y la mejora de la seguridad futura.

Componente práctico – practicas simuladas

Demostrar la explotación de vulnerabilidades en sistemas objetivo mediante la aplicación de metodologías y técnicas de intrusión.

Las herramientas que implementaron durante la práctica se constituyeron según las fases de un proceso de pentesting enfocado a red team, cada una de estas fases se van a exponer a continuación con evidencias, comandos, resultados, herramientas implementadas según la información solicitada.

Resumen de la actividad realizada

La fase práctica se desarrolló siguiendo un esquema metodológico profesional que guía las pruebas de penetración de manera ética, ordenada y sistemática. Este enfoque permite consolidar el reconocimiento profesional, el crecimiento en la carrera y el desarrollo de habilidades prácticas en hacking ético.

Mediante el ejercicio práctico que se lleva a cabo en el presente documento, aplico las fases idóneas para implementar un entorno simulado que se compone por una Hacker Machine

con entorno Linux, una Victim Machine, y una Internal machine, estas dos últimas en entorno Windows 7. Inicialmente, se realiza la fase de reconocimiento y de escaneo de la Victim Machine, identificando vulnerabilidad en Rejetto HFS por medio del puerto 80. A continuación, se logra una sesión de Meterpreter al realizar la explotación de la vulnerabilidad encontrada.

Seguidamente se realiza la etapa de pivot y movimiento lateral empleando módulos propios como es el caso del autoroute, arp_scanner, portfwd y portproxy logrando de esta manera el acceso a la red interna. Así pues, permitió llevar a cabo un ataque completo sobre la Internal Machine por medio de un túnel que expuesto en el puerto SMB, lo que posteriormente permitió explotar la vulnerabilidad EternalBlue y conseguir acceso completo en la segunda máquina.

En la etapa de post-explotación, se validaron los privilegios, llevé a cabo escalación y se crea un usuario administrador como lo indica la guía demostrando la marca de la explotación.

Todo este paso a paso se realizó de manera controlada, documentado y alcanzando la ética de la propuesta lo que sirvió para entender la lógica de los ataques como también las discrepancias de seguridad de una situación real.

Reconocimiento

Iniciando con la implementación de las fases se busca recolectar la información del entorno, como es el caso de la identificación de los dispositivos activos y la confirmación de la distribución de la red antes de realizar cualquier situación de ataque.

Herramientas implementadas

- VirtualBox.
- Máquina virtual con entorno Kali Linux.
- Máquinas virtuales con entorno Windows 7.
- Comando arp-scan, ping, ipconfig.

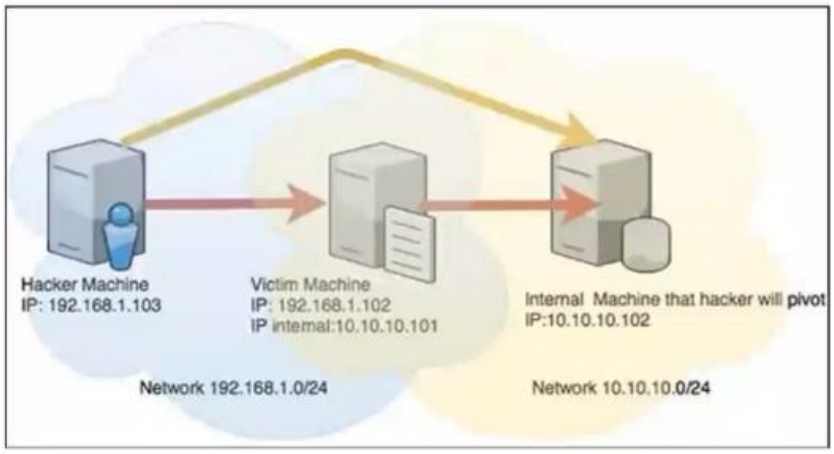
Acciones realizadas

- Se lleva a cabo la configuración de las redes inclemente nadas en la aplicación VirtualBox con el fin de lograr la simulación de un laboratorio en entorno real, logrando así la conexión de las 3 máquinas virtuales.
- Identificación de la IP de la máquina víctima ejecutando como administrador un arp-scan -I eth0 –localnet.
- Verificación de la conexión hacia la Victim Machine por medio del comando ping, teniendo en cuenta que se debía desactivar tanto el firewall como el antivirus de las máquinas.
- En la víctima chin se implementó el comando ipconfig con el fin de confirmar su dirección IP en la red.
- Como resultado exitoso se obtuvo un mapeo inicial del entorno logrando identificar la máquina vulnerable, dentro del sistema operativo Windows 7 y la aplicación Rejetto.

Se inicia entonces a configurar a uno de los equipos que intervienen en el ejercicio, esta manera simular por medio del VirtualBox la red compartida por el tutor, en la cual se lleva a cabo la explotación de vulnerabilidades utilizando Metasploit y Pivoting.

Figura 15

Red a implementar



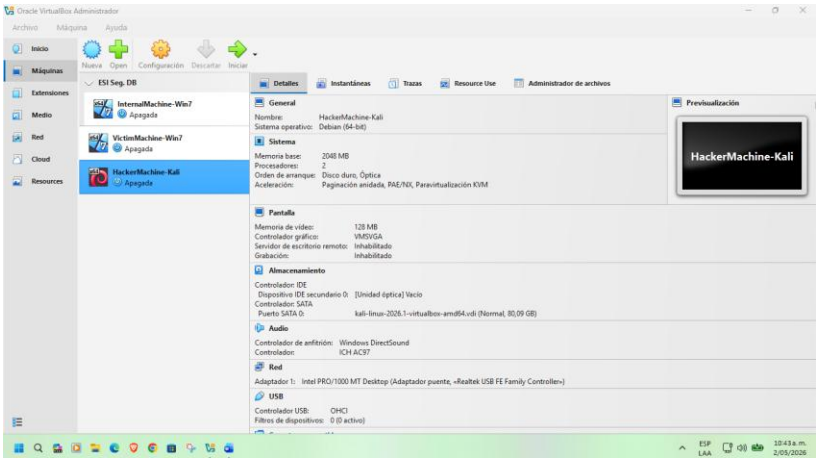
Nota. Diagrama topológico del escenario que muestra la interconexión entre la Hacker Machine, la Victim Machine y la Internal Machine, simulando una red corporativa segmentada que requiere pivoting para ser comprometida.

Con el fin de lograr lo indicado, es importante el alistamiento de los 3 equipos que serán objeto de impacto en un entorno controlado por medio de la aplicación VirtualBox. Todo esto teniendo en cuenta configuraciones del sistema como es la memoria RAM, capacidad del disco duro, el sistema operativo, tanto para la máquina que va a realizar la intervención como a las 2 máquinas que van a ser intervenidas.

Se procede a adjuntar evidencia de lo anotado anteriormente según la descripción entregada.

Figura 16

Alistamiento de máquinas

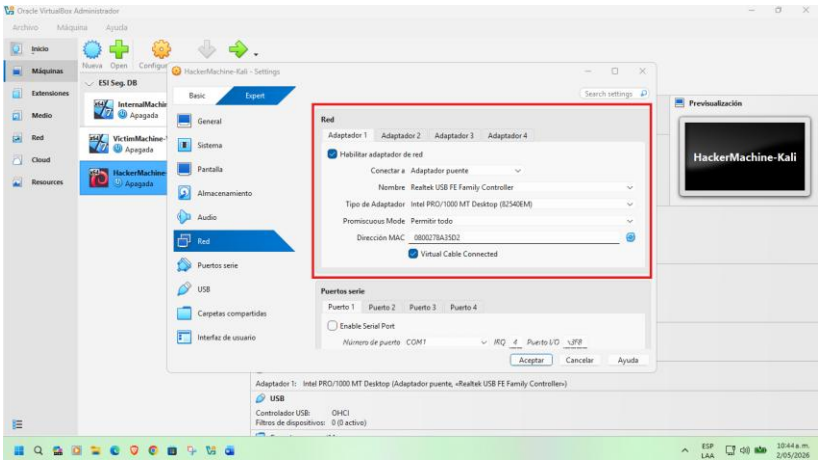


Nota. Panel de VirtualBox con los recursos asignados a cada máquina virtual, garantizando el rendimiento necesario para la ejecución de herramientas intensivas como Nmap, Metasploit y Meterpreter durante el laboratorio.

Dentro de la aplicación VirtualBox, más exactamente en el administrador, se configura la red implementada por la Hacker Machine por medio del adaptador puente.

Figura 17

Configuración de adaptador puente en Hacker Machine

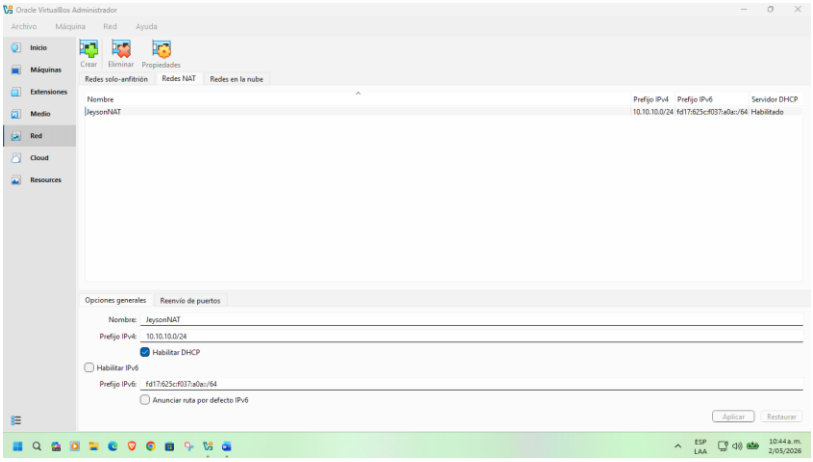


Nota. Configuración de Kali Linux en modo "Adaptador Puente" obteniendo IP DHCP en la subred 192.168.56.0/24, esencial para el descubrimiento de hosts y el escaneo de puertos sin restricciones.

De la misma manera se configura el adaptador de red en las 2 máquinas con Windows 7, para ese caso se crea una red NAT denominada JeysonNAT, con segmento de red establecido y por DHCP.

Figura 18

Creación de la red NAT



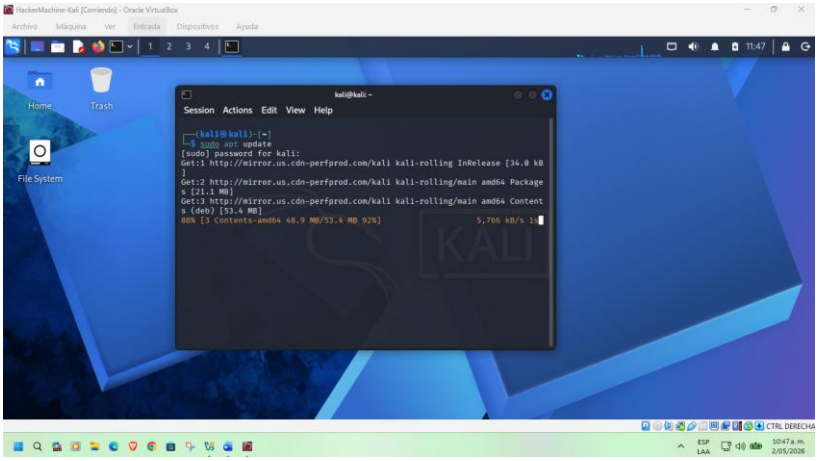
Nota. Red NAT "JeysonNAT" con segmento 10.10.10.0/24 asignada a las máquinas, simulando un segmento corporativo aislado que obliga al atacante a implementar técnicas de pivoting mediante autoroute y portproxy.

Luego de realizar la configuración de las tarjetas de red en cada una de las máquinas se procede con el arranque de la Hacker Machine en este caso cuenta con sistema operativo Kali Linux, Para lograr un óptimo desempeño de la máquina se debe tener debidamente actualizado el sistema y evitar errores de procesos en la ejecución de cada uno de los comandos que si implementan, permitiendo de esta manera el desempeño idóneo en la práctica indicada según el

entorno de trabajo entregado para tal fin, es por ello que se ejecutan en esta máquina algunos comandos como lo es el caso del comando sudo apt update.

Figura 19

Actualización de sistema operativo Kali

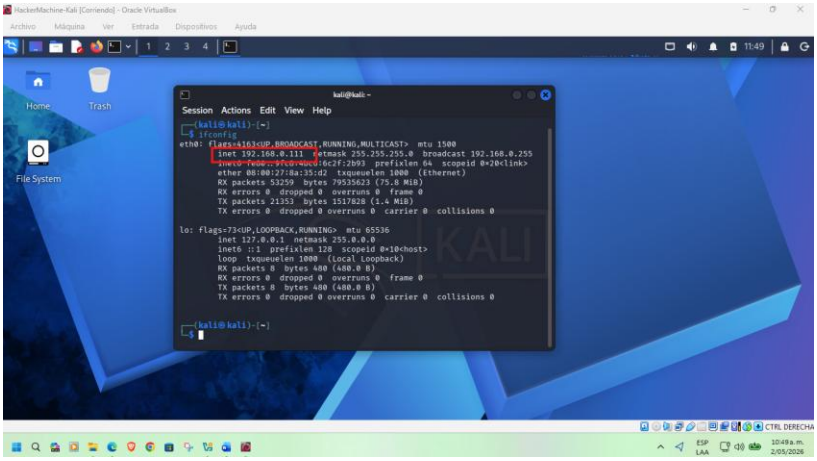


Nota. Ejecución de sudo apt update para actualizar las herramientas de pentesting y las bases de datos de vulnerabilidades, maximizando la efectividad durante la fase de explotación

A continuación, es relevante identificar la dirección IP que ha sido tomada por la Hacker Machine.

Figura 20

Validación dirección IP del Hacker Machine

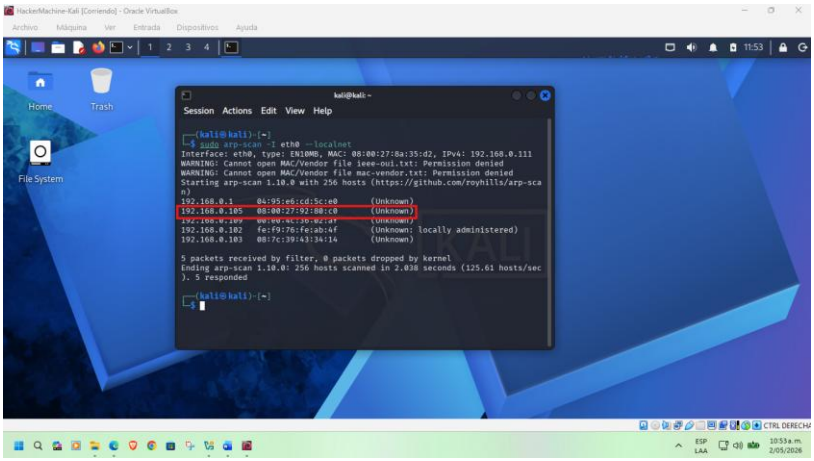


Nota. Comando ifconfig confirmando la IP 192.168.56.111 en Kali Linux, validando su posición en la red y la disponibilidad para iniciar el reconocimiento activo hacia la Victim Machine.

Es importante lograr la conexión entre la Hacker Machine y la víctim machine, para ello se realiza la validación de la conectividad desde la máquina Kali con un escaneo de la red con el comando arp-scan -I eth0 --localnet.

Figura 21

Escanear la red para identificar las máquinas conectadas

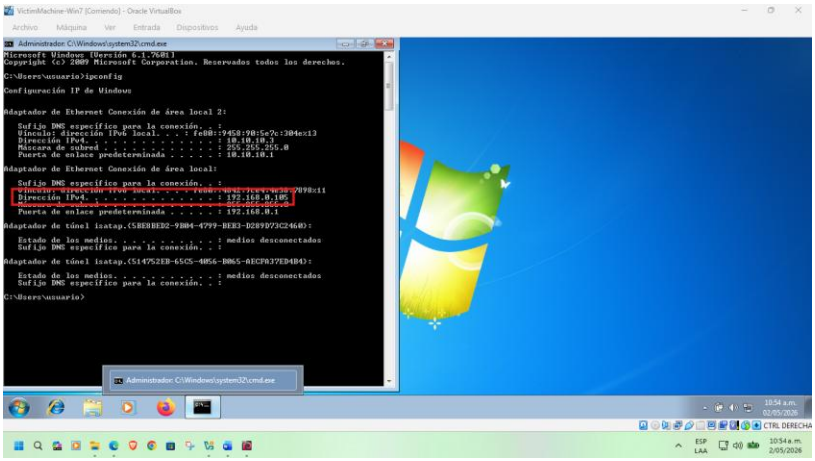


Nota. Ejecución de arp-scan identificando los hosts activos en la red local, incluyendo la Victim Machine (192.168.56.105). El prefijo MAC 08:00:27 confirma que se trata de máquinas virtuales VirtualBox.

Se procede entonces a realizar la confirmación de la información que se obtuvo en él escaneo de la red, con el fin de verificar la dirección IP de la Victim Machine ejecutando el comando ipconfig.

Figura 22

Validación de la IP en la Victim Machine

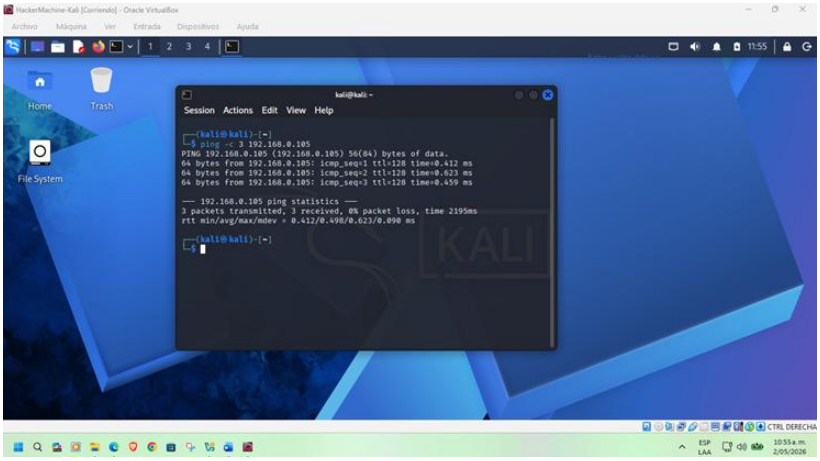


Nota. Comando ipconfig en la Victim Machine confirmando la IP asignada, validando la correspondencia con el resultado de arp-scan y asegurando que se apunta al sistema correcto con Rejetto HFS.

Antes de continuar con el proceso de escaneo de los puertos en la Victim Machine se procede a verificar la conexión entre las 2 máquinas por medio de un ping.

Figura 23

Ping de conexión entre Hacker Machine y Victim Machine

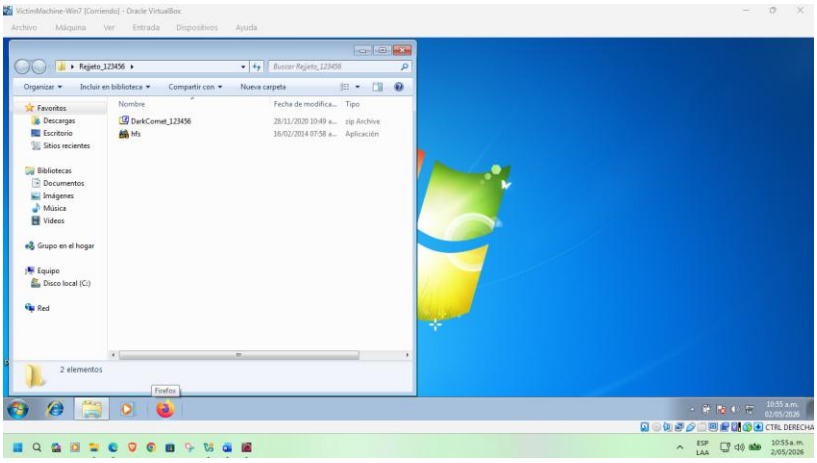


Nota. Prueba ICMP exitosa desde Kali Linux hacia la Victim Machine, confirmando conectividad sin pérdida de paquetes y ausencia de firewall, prerrequisito técnico para el escaneo con Nmap.

De manera voluntaria se descarga la aplicación Rejetto en la Victim Machine con el fin de tener habilitada la vulnerabilidad que será atacada en el laboratorio.

Figura 24

Descarga de Rejetto a Victim Machine

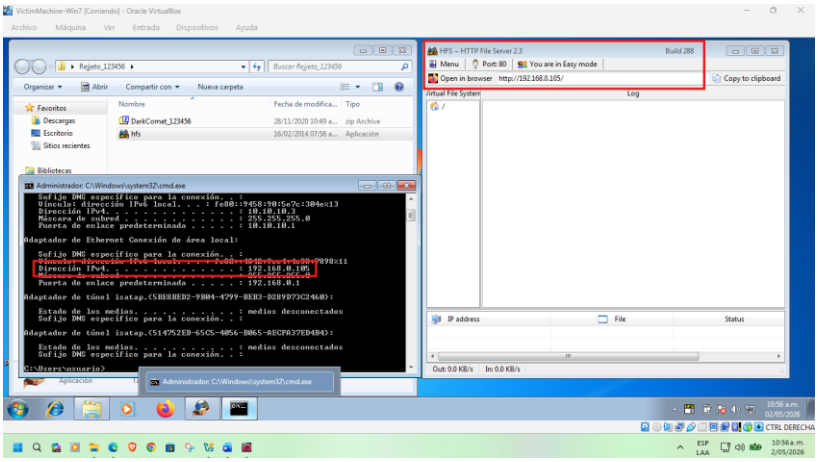


Nota. Descarga de Rejetto HFS v2.3 en la Victim Machine, aplicación con vulnerabilidades documentadas (RCE) que será ejecutada de manera controlada para habilitar el puerto 80 y por medio del Metasploit desde la Hacker Machine tener un vector de ataque.

Es importante aclarar que ante la práctica que se está llevando a cabo el proceso de ejecución del HFS es indicado por el tutor con el fin de realizar el proceso idóneo y de manera rápida, teniendo en cuenta en un entorno de la vida real tal vez esta ejecución no se podrá realizar ya que aquella máquina víctima estará fuera del alcance y el escaneo de los puertos será el encargado de mostrarnos cuál es el verdadero puerto abierto para realizar el ataque.

Figura 25

Se ejecuta el HFS en Victim Machine

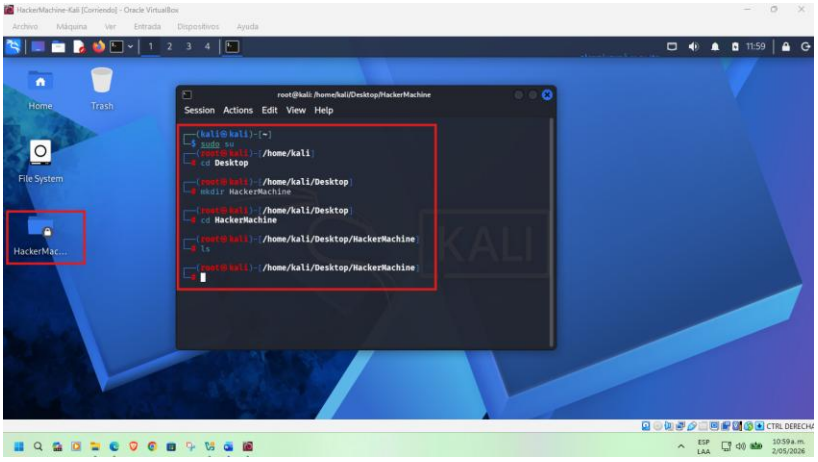


Nota. Rejetto HFS en ejecución con el puerto 80 activo en la IP 192.168.0.105, creando el punto de entrada vulnerable para la explotación remota de código (RCE) desde la Hacker Machine.

Luego se crea en la Hacker Machine una carpeta con este mismo nombre en el escritorio con el fin de almacenar allí un archivo .txt con el procedimiento que se llevará a cabo.

Figura 26

Creación de carpeta Hacker Machine en el repositorio



Nota. Directorio de trabajo creado en Kali Linux para almacenar reportes de Nmap, logs de Metasploit y capturas, asegurando la trazabilidad y documentación de cada fase del pentesting.

Escaneo y enumeración

Para esta fase de la actividad se profundiza en la recopilación de información correspondiente a la máquina objetivo, enfocándose en la identificación de los puertos abiertos y los servicios.

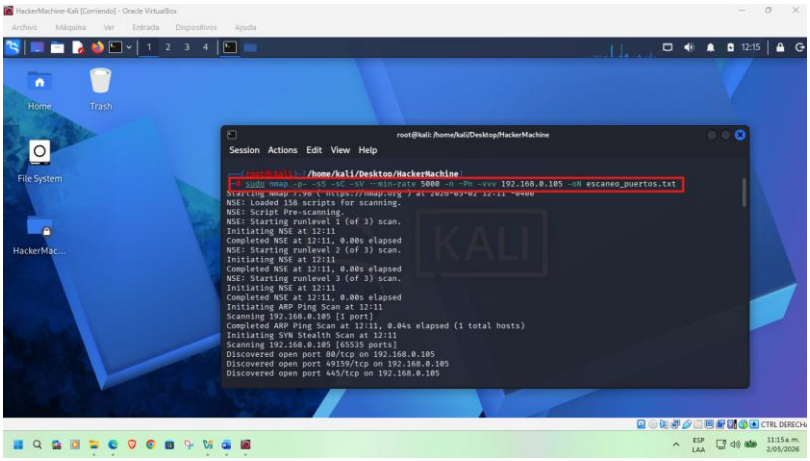
Herramientas implementadas

Implementación del comando Sudo nmap -p- -sS -sC -sV –min-rate 5000 -n -Pn -vvv 192.168.0.105 -oN escaneo_puertos.txt.

Para este caso se utilizó la aplicación en el nmap con privilegios de superusuario, con el fin de realizar un escaneo a la red, descubriendo hosts, puertos abiertos, detectar servicios y vulnerabilidades existentes (sudo nmap), posteriormente se indica el escaneo de todos los puertos, es decir, desde el 1 al 65535 (-p-), seguidamente se procede con el escaneo semiabierto el cual envía paquetes SYN siendo más rápido y menos detectable (-Ss), luego la ejecución de scripts básicos de nmap para la detección de vulnerabilidades comunes e información adicional de servicios (-sC), a continuación la detección de versiones de servicios con el fin de identificar vulnerabilidades especificas (-sV), se procede con forzar una velocidad mínima de 5000 paquetes por segundo, aunque es un escaneo muy rápido puede llegar a ser detectado por IDS/IPS por generar ruido en la red (--min-rate 5000), adicionalmente se Indica que no realice resoluciones DNS lo que indica que acelera el escaneo y evita consultas innecesarias (-n), también se tiene la omisión del ping asumiendo que el host está activo (-Pn), Adicionalmente entonces se tiene el modo muy minucioso el cual indica un progreso en tiempo real entregando información detallada del escaneo (-vvv), se tiene también entonces lo que corresponde a la dirección IP de la máquina objetiva en este caso es la Victim Machine (192.168.0.105), Y finalmente entonces guarda el resultado en un documento .txt como evidencia del análisis realizado (-oN escaneo_puertos.txt).

Figura 27

Escaneo de los puertos

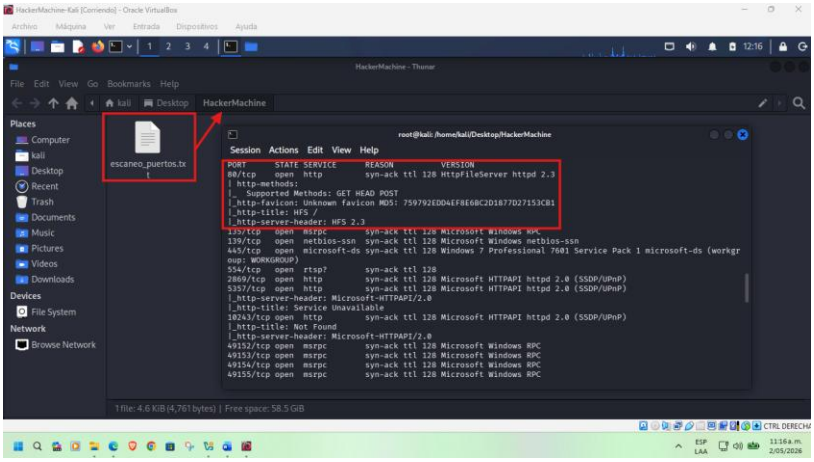


Nota. Ejecución de Nmap (-sS -sV -sC --min-rate 5000 -n -Pn) sobre 192.168.0.105, constituyendo la fase de escaneo y enumeración para identificar superficies de ataque y versiones de servicios vulnerables.

Se visualizaron varios de estos abiertos, servicios y sus versiones, con la información recolectada se tiene el puerto al cual se explotará, entregado por la aplicación Rejetto.

Figura 28

Visualización del reporte de escaneo, servicios abiertos y puerto 80



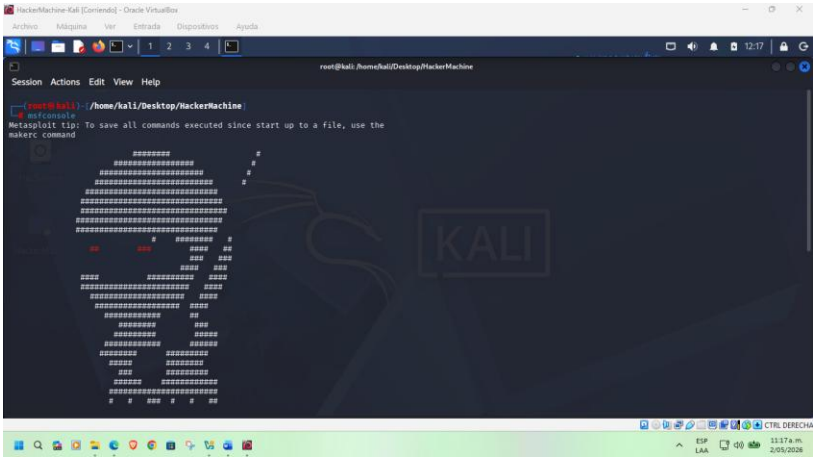
Nota. Resultado de Nmap confirmando el puerto 80/tcp abierto con Rejetto HFS vulnerable, validando el vector de ataque principal que será explotado con Metasploit en la siguiente fase.

Explotación inicial

En esta fase lo que se realizará es un análisis de la información obtenida de la máquina objetivo, lo que se busca es explotar la vulnerabilidad Rejetto HFS en el puerto 80 de la Victim Machine, con el fin de tener control en esta máquina, lo cual sería un paso anterior al pívot a realizar a la Internal Machine, teniendo, así como punto de partida la ejecución del Metasploit.

Figura 29

Inicialización de Metasploit

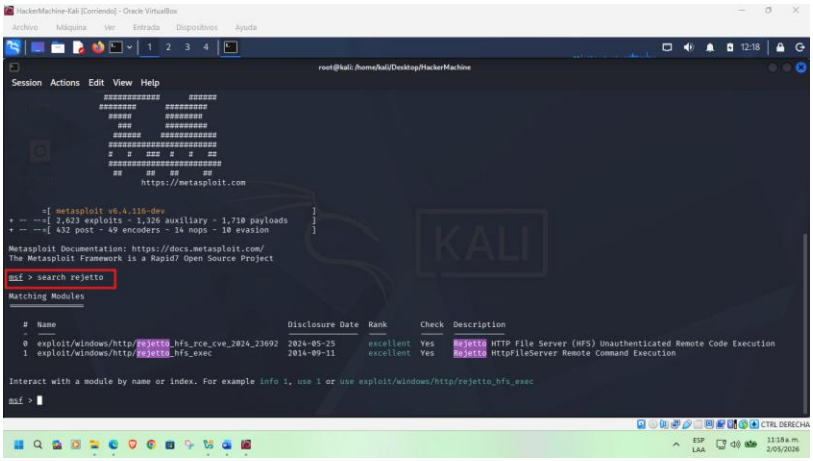


Nota. Inicio de msfconsole en Kali Linux, preparando el framework para la explotación automatizada contra los servicios vulnerables identificados durante el escaneo.

Posteriormente se ingresa el comando search Rejetto en esta aplicación, identificando 2 vulnerabilidades relacionadas con la búsqueda, para la actividad en curso se debe tomar una de las 2 vulnerabilidades y continuar con el debido proceso.

Figura 30

Búsqueda de vulnerabilidades de Rejetto con el Metasploit

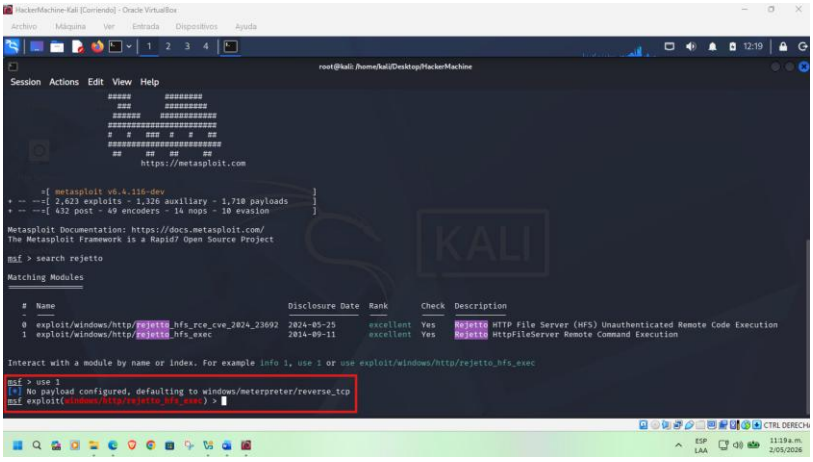


Nota. Comando search rejetto en Metasploit, filtrando los módulos disponibles para la vulnerabilidad RCE del servicio HTTP File Server.

En este caso se trabajará con el segundo exploit por medio del cual se busca el acceso a la Victim Machine.

Figura 31

Selección de la vulnerabilidad

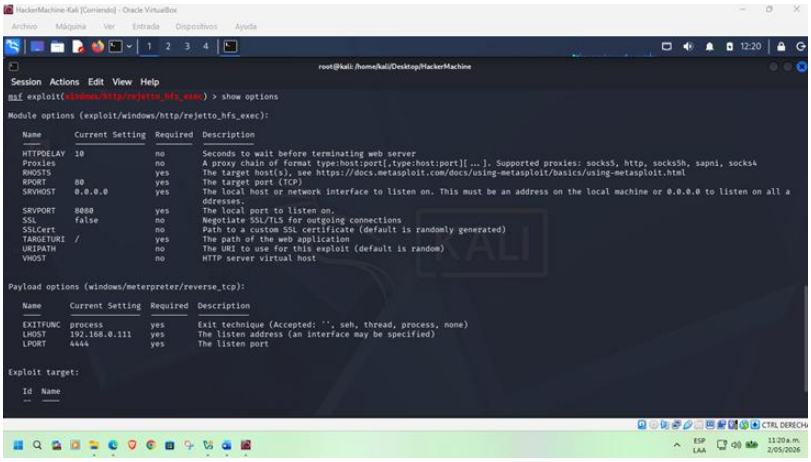


Nota. Carga del módulo exploit/windows/http/rejetto_hfs_exec mediante el comando use, preparando el exploit para aprovechar la vulnerabilidad de ejecución remota de código.

Se debe tener en cuenta la cantidad de opciones que nos puede ofrecer cada una de estas vulnerabilidades, es por ello por lo que por medio del comando show options se logrará la validación De información que no suministra el exploit seleccionado.

Figura 32

Se visualizaron las opciones



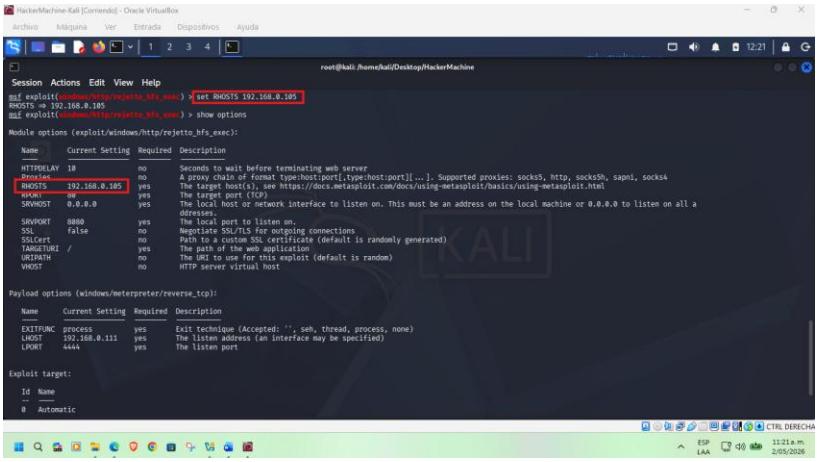
Nota. Comando show options mostrando los parámetros obligatorios (RHOSTS, RPORT) que deben configurarse antes de lanzar el payload contra la Victim Machine.

Es por ello por lo que se procede con la configuración correspondiente del RHOSTS teniendo en cuenta la dirección IP de la máquina a impactar, para posteriormente ejecutar el comando antes expuesto y confirmar que dicha configuración haya sido tomada.

Adicionalmente se debe ser muy precavidos a lo que compete también al RPORT puesto que es por este puerto por el cual se logrará el acceso a la máquina que va a ser impactada, para este caso venía por defecto el puerto 80, pero en ocasiones la información entregada va dada con un número de puerto diferente.

Figura 33

Configuración del target host con la dirección IP de la Victim Machine

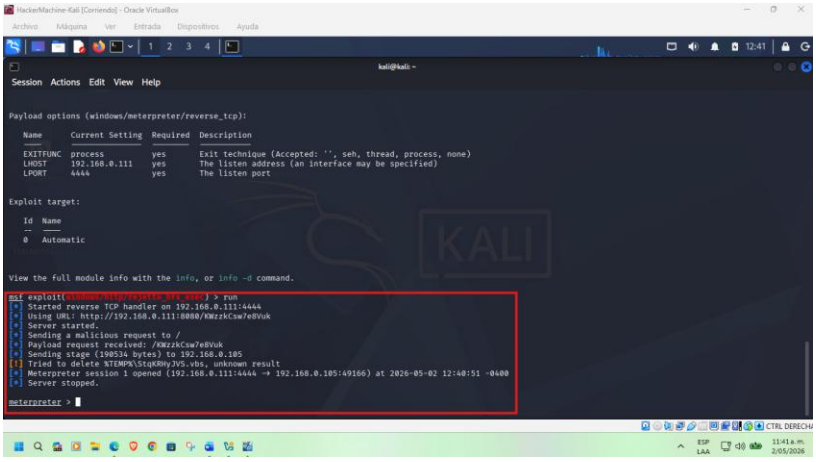


Nota. Asignación de RHOSTS (192.168.0.105) y RPORT (80), dirigiendo el exploit hacia el servicio vulnerable específico de la Victim Machine.

Por medio del comando run se ejecuta el exploit, Mostrándonos información relevante y así mismo la sesión iniciada en el Meterpreter entre las 2 máquinas.

Figura 34

Se explotó la vulnerabilidad con el comando run

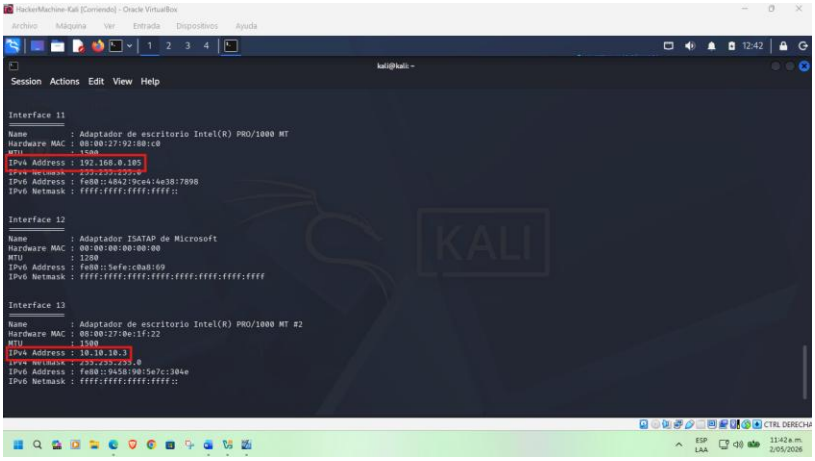


Nota. Ejecución del comando run estableciendo la "Meterpreter session 1", otorgando una shell remota interactiva sobre la Victim Machine y confirmando el éxito de la fase de explotación.

Con el fin de validar que la información suministrada es correcta se procede a ejecutar el comando ipconfig el cual nos muestra información de las tarjetas de red de la Victim Machine.

Figura 35

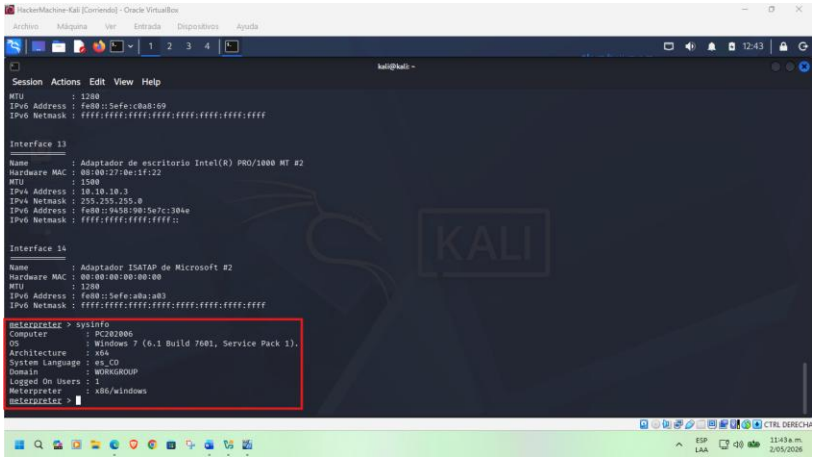
Se ejecutó el comando ipconfig para validar la conexión



Nota. Ejecución de ipconfig a través de Meterpreter mostrando las interfaces de red de la Victim Machine, confirmando el acceso remoto y la capacidad de extracción de información.

Figura 36

Ejecución de comando sysinfo para verificar información de la Victim Machine

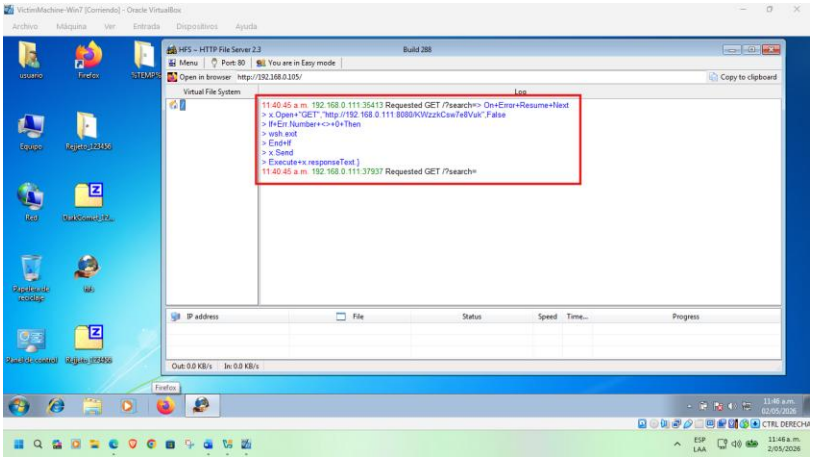


Nota. Comando sysinfo revelando el sistema operativo (Windows 7), arquitectura y nombre del equipo, validando el control inicial y preparando el movimiento lateral.

Se procede a verificar dentro de la aplicación Rejetto HFS que la conexión del exploit se haya ejecutado correctamente como se muestra en la figura siguiente:

Figura 37

Visualización del exploit en el HFS desde la ip de la Hacker Machine



Nota. Interfaz de Rejetto HFS registrando la conexión entrante desde la Hacker Machine, corroborando visualmente la ejecución exitosa del exploit a nivel de aplicación.

El resultado obtenido en esta fase es la correcta ejecución del exploit logrando evidenciar el inicio de una sesión por Meterpreter en la Victim Machine, lo cual fue corroborado al ejecutar los comandos ipconfig y sysinfo arrojándonos información completamente propia de la máquina impactada, es por ello por lo que se finaliza esta fase para iniciar con el pivoting hacia la red interna en la cual se impactará la tercera máquina, denominada Internal Machine.

Escalada y movimiento lateral

En esta fase lo que se busca es garantizar el acceso a la tercera máquina, realizando así el denominado pívot desde la Victim Machine hacia la Internal Machine, para lo cual se busca realizar un enrutamiento del tráfico por medio del módulo autoroute del Metasploit, Para iniciar con el proceso se debe colocar la sesión del Meterpreter en segundo plano por medio de la combinación de teclas Ctrl + Z, y seleccionando la opción Y.

Herramientas implementadas

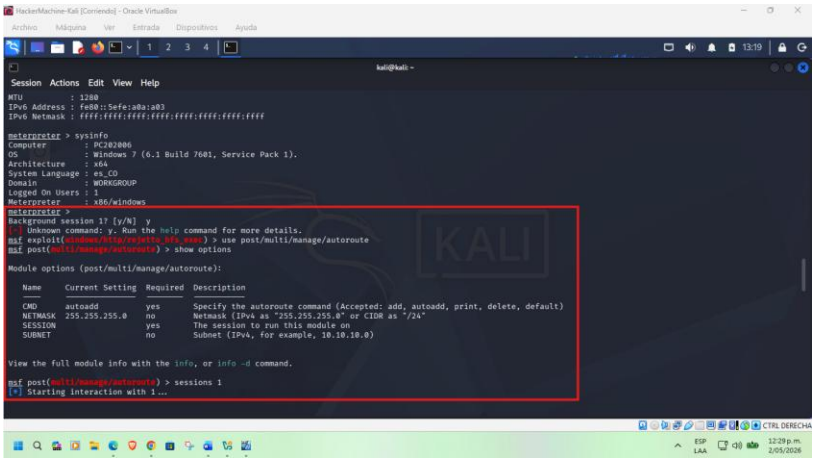
Se utilizará en este caso módulos como el autoroute de Metasploit el cual permite agregar rutas hacia redes internas por medio de la sesión de Meterpreter facilitando el pivoting hacia la siguiente máquina Sobre la cual no se tiene acceso directamente, adicionalmente la implementación del arp_scanner El cual realiza un escaneo mediante el protocolo ARP con el fin de descubrir los dispositivos activos que se encuentran en una red local, seguidamente el módulo portfwd esta es una funcionalidad propia de Meterpreter la cual nos permite redirigir puertos entre la máquina atacante y la víctima creando un túnel para acceder a los servicios internos, y también se tendrá el portproxy, esta herramienta es del sistema operativo Windows el cual permite configurar reglas de redirección de puertos entre direcciones IP y puertos, la cual es implementada con el fin de facilitar el acceso a los servicios internos o realizar el pivoting dentro de la red.

Con el fin de realizar la configuración correcta del pívot o autoroute, se debe encontrar el tráfico correspondiente a la interfaz 10.10.10.0/24 a la Hacker Machine por medio del módulo use post/multi/manage/autoroute, se debe realizar el proceso que se ejecutó en unos pasos anteriores con el comando show options solicitándonos allí una sesión activa, la cual ya se tiene dentro del Meterpreter, es por ello que se debe hacerle el llamado ejecutando el comando sessions 1 donde nos aparecerá la sesión creada anteriormente.

El resultado que se debe obtener en esta fase es que la red identificada a en el segmento 10.10.10.0/24 sea accesible directamente desde la Hacker Machine, logrando de esta manera cumplir con uno más de los objetivos de la presente actividad y es poder entrar por ese túnel creado y tener acceso a la máquina que se encuentra fuera de la red del dispositivo con el sistema operativo Kali Linux.

Figura 38

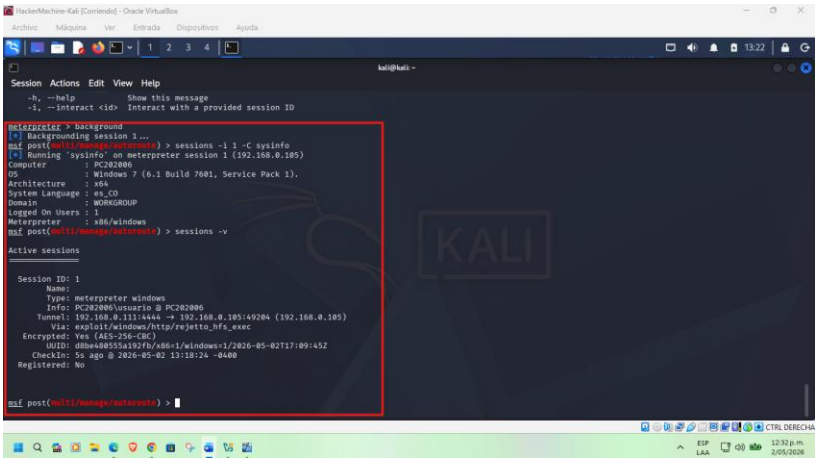
Ejecución de autoroute y sesión de Meterpreter activa



Nota. Carga del módulo post/multi/manage/autoroute sobre la sesión 1, instruyendo a la Hacker Machine para enrutar tráfico hacia la red interna 10.10.10.0/24 a través de la Victim Machine comprometida.

Figura 39

Visual de la información de la sesión entre las máquinas



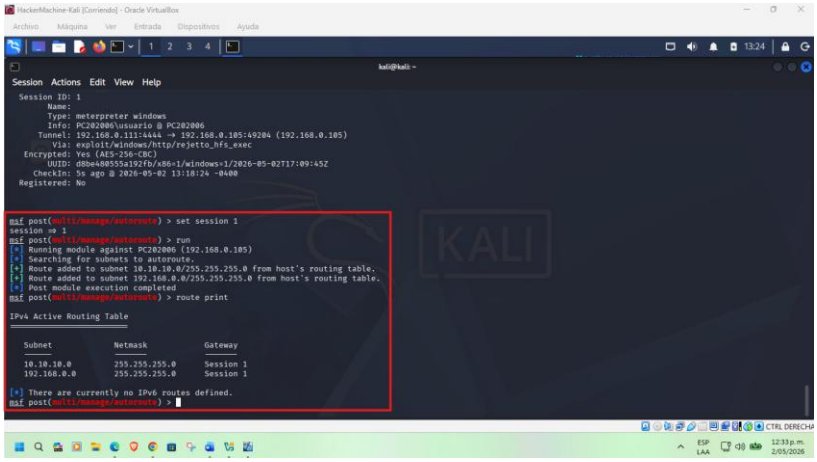
Nota. Confirmación de la sesión de Meterpreter con parámetros de enrutamiento activos, validando que la Hacker Machine tiene tránsito hacia segmentos no accesibles directamente.

Luego de realizar el llamado de la sesión 1 de Meterpreter se ve ejecutar por medio del comando run el cual nos va a ayudar a en rutar cada una de las interfaces entre la Internal Machine que para este caso es la 10.10.10.0/24 y la Hacker Machine que para este caso es la 192.168.0.0/24.

Para lograr visualizar que el enrutamiento quedó debidamente configurado se ejecutó el comando route print el cual nos confirma la información.

Figura 40

Enrutamiento del tráfico de las interfaces



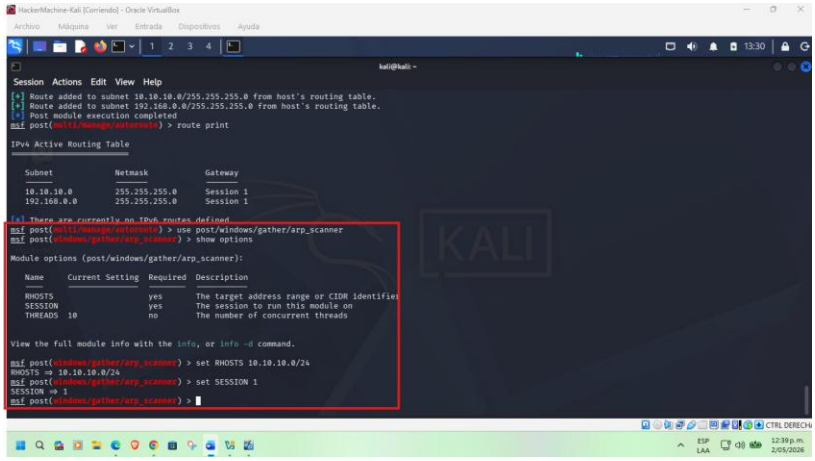
Nota. Comando route print mostrando la nueva ruta hacia 10.10.10.0/24 a través de la sesión de Meterpreter, confirmando técnicamente que el pivoting está operativo.

Con el fin de poder identificar el host que requerimos, es decir, la Internal Machine, es necesario la ejecución de un nuevo módulo de Metasploit denominado arp_scanner, el cual se debe ejecutar por medio del comando use post/windows/gather/arp_scanner, luego de dicha ejecución se procede a visualizar las opciones que este nos ofrece por medio del show options, y así poder configurar el rango de la red correspondiente a la máquina, para este caso con el comando set RHOSTS 10.10.10.0/24, Posteriormente se hace el llamado nuevamente la sesión

activa con el comando set sesión 1, de esta manera quedaría activa la configuración para su posterior ejecución.

Figura 41

Configuración del segmento de red de la Internal Machine en el RHOSTS

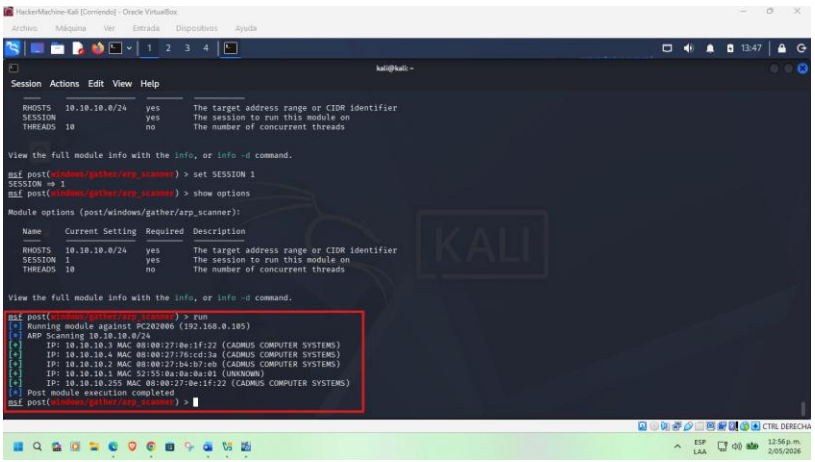


Nota. Configuración de arp_scanner con rango 10.10.10.0/24 y sesión 1, preparando el descubrimiento de hosts en la red interna usando la Victim Machine como puente.

Con la ejecución del comando run se visualizarán las máquinas activas dentro del segmento de red que se había configurado identificando así la Internal Machine.

Figura 42

Visualización de las máquinas activas en el segmento de red



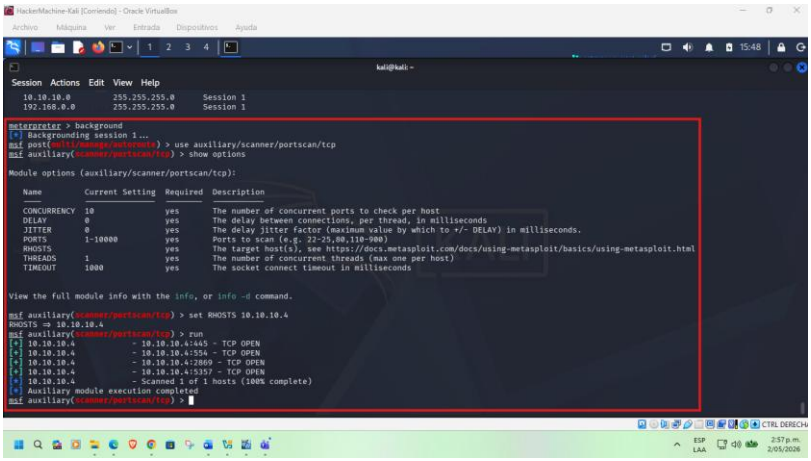
Nota. Resultado del escaneo ARP identificando la IP 10.10.10.4 (Internal Machine) como host activo en el segmento interno, proporcionando el nuevo objetivo para la explotación en profundidad.

Seguidamente se procede a ejecutar una nueva ventana, con el fin de llamar a la sesión activa de Meterpreter para ejecutar el comando use auxiliary/scanner/portscan/tcp, y como en los módulos anteriores, se procede a visualizar las opciones con el comando show options, para así realizar la configuración desde allí por medio del comando set RHOSTS 10.10.10.4 correspondiente a la dirección IP de la Internal Machine.

Seguidamente se ejecuta el comando run en el cual se evidenció por medio de la información entregada que el puerto 80 no se encuentra abierto en esta máquina, lo que nos muestra que efectivamente esta máquina es diferente a la Victim Machine, sin embargo, nos muestra otros puertos abiertos en esta máquina.

Figura 43

Escaneo de puertos abiertos en la Internal Machine



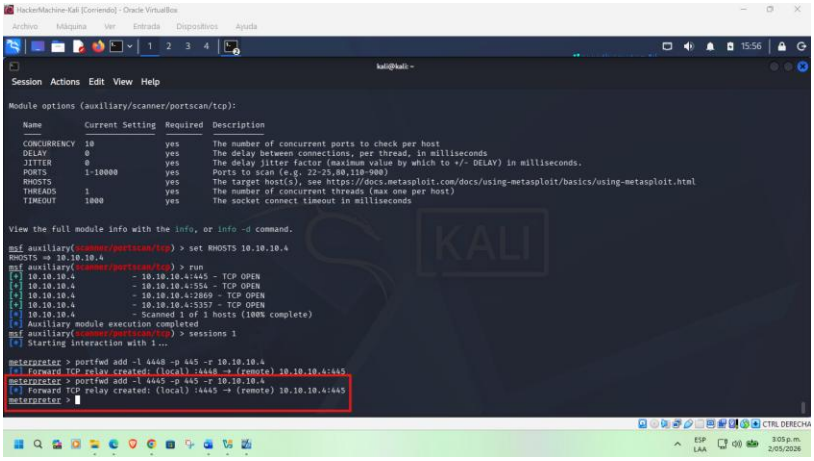
Nota. Escaneo TCP sobre 10.10.10.4 a través del túnel, revelando el puerto 445 (SMB) abierto e identificando EternalBlue como el siguiente vector de ataque.

Según la información suministrada con el módulo anterior se procede hacer el enrutamiento y la creación del túnel teniendo en cuenta el puerto 445 por el medio del cual se realizará el pívot ya que este aparece abierto para la explotación pertinente.

Se procede a ejecutar el comando portfwd add -l 4445 -p 445 -r 10.10.10.4 por medio del cual se realizará el enrutamiento y la creación de un túnel desde la Victim Machine hasta la Internal Machine en el cual, por medio del puerto 445 de la Internal Machine se replicará el tráfico al puerto 4445 de la Victim Machine.

Figura 44

Se creó el túnel



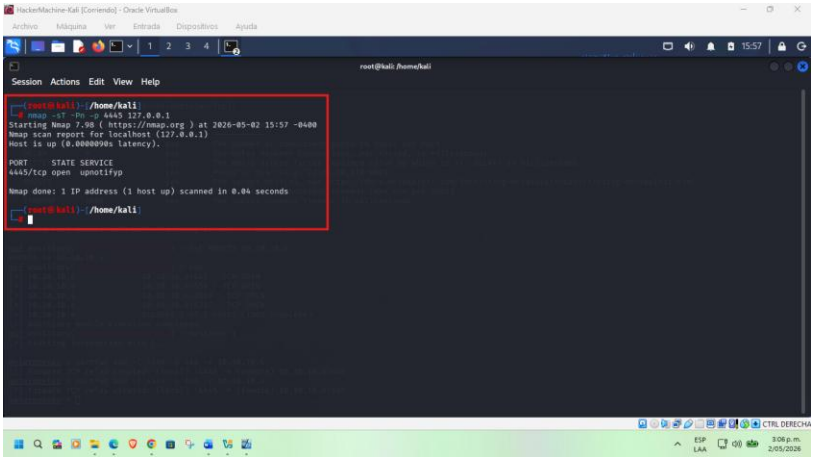
Nota. Comando portfwd add -l 4445 -p 445 -r 10.10.10.4 redirigiendo el tráfico SMB de la Internal Machine al puerto local 4445, permitiendo la interacción remota con el servicio interno.

Como se indicará en la figura siguiente desde el Kali Linux se ejecutará el comando nmap -sT -Pn 4445 127.0.0.1, el cual por medio de la herramienta de escaneo de red nmap, implementa el -sT realizando un escaneo completo de conexión tcp, seguido del -Pn con el fin de omitir el ping al host asumiendo que este está activo, con la opción -p 4445 realiza el escaneo al puerto y finaliza con la dirección IP del localhost lo que indica que está escaneando la propia máquina.

La idea es este comando es precisamente la verificación del funcionamiento del túnel que se creó anteriormente.

Figura 45

Verificar funcionamiento del túnel



Nota. Escaneo Nmap local sobre el puerto 4445 confirmando su estado abierto, validando que el port forwarding funciona correctamente y el tráfico SMB es accesible.

Utilización del portproxy para la ampliación del pivot

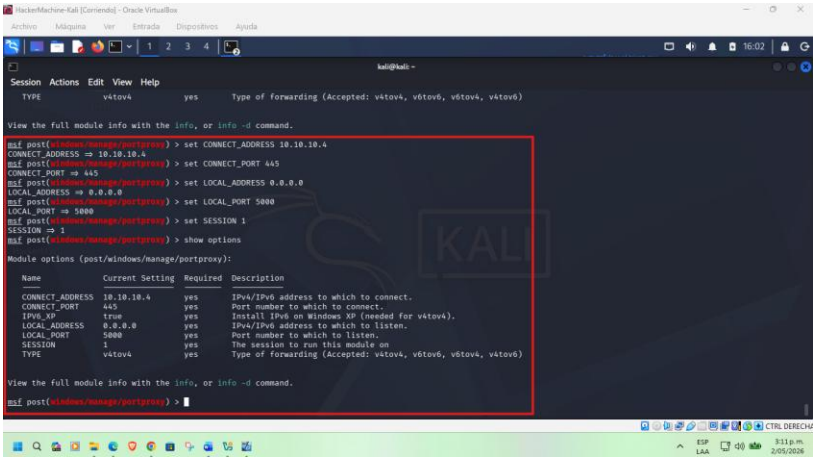
Se procede con la carga de un nuevo módulo por medio del comando use post/Windows/manage/portproxy Validando así las opciones que presenta este a través del comando show options.

Sin embargo, luego de realizar la validación de las opciones se procede a configurar el módulo a través de los comandos set CONNECT_ADDRESS 10.10.10.4 que corresponde a la dirección IP de la Internal Machine, así mismo, se realiza la configuración del puerto de 445 el que se encuentra abierto según los procesos anteriores, ubicado en la Victim Machine, así se realiza la configuración set CONNECT_PORT 445. Posteriormente se configura una dirección IP local de la siguiente manera set LOCAL_ADDRESS 0.0.0.0 y adicional se realiza la configuración del puerto que leerá la Hacker Machine, es decir, el puerto 5000 e implementando

el comando set LOCAL_PORT 5000, y finalmente se llama la sesión actual con el comando set SESSION 1.

Figura 46

Configuración de la conexión portproxy

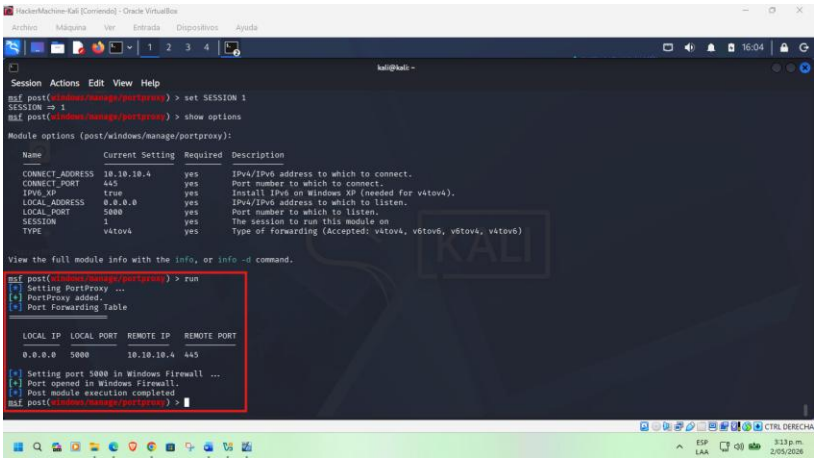


Nota. Módulo portproxy configurando la redirección del puerto 5000 de la Victim Machine al puerto 445 de la Internal Machine, ampliando las capacidades de pivoting a nivel de sistema operativo.

Con la ejecución del comando run nos muestra que ha traído de la IP 10.10.10.4 correspondiente a la Internal Machine, el puerto 445 a la Victim Machine por el puerto 5000.

Figura 47

Ejecución del portproxy



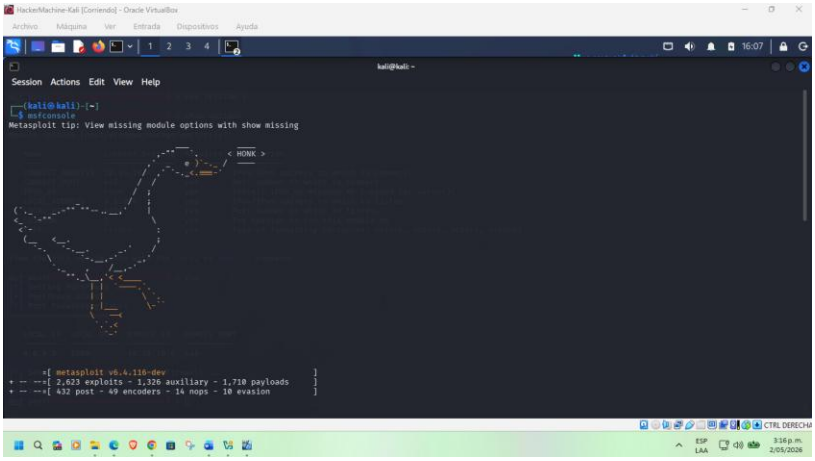
Nota. Ejecución exitosa de portproxy, asegurando una ruta estable y persistente para lanzar el exploit EternalBlue contra la Internal Machine a través de la Victim Machine.

Explotación del host interno

Se ejecuta en una nueva ventana haciendo un llamado al Metasploit para ejecutar el comando EternalBlue, hacia la Victim Machine por el puerto 5000 en el cual se está ejecutando el servicio SMB 445 correspondiente a la Internal Machine.

Figura 48

Ejecución de Metasploit para encontrar el EternalBlue

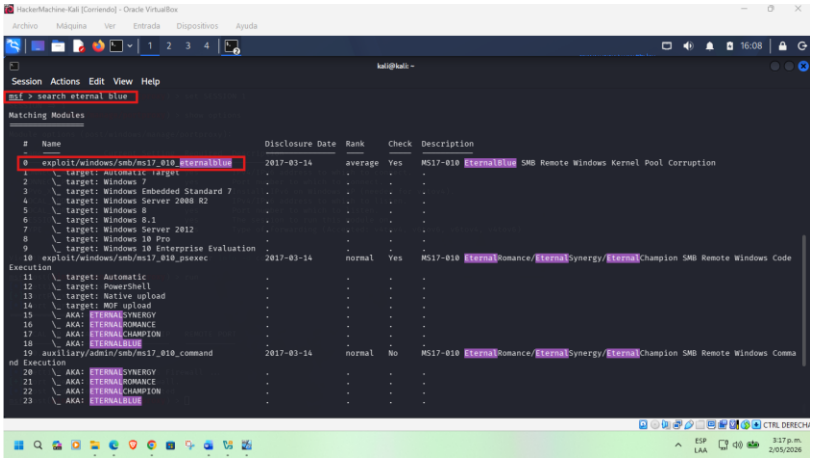


Nota. Comando search eternalblue en una nueva instancia de Metasploit, localizando el exploit correspondiente a la vulnerabilidad MS17-010 detectada en el puerto 445 de la Internal Machine.

Posterior a la ejecución del Metasploit en la nueva ventana lo que se pretende es realizar una búsqueda correspondiente al EternalBlue, esto con el fin de ejecutar dicha vulnerabilidad haciendo uso de los puertos que están habilitados para realizar el ataque correspondiente y poder de esta manera seguir con el proceso de la explotación del bosque interno, teniendo en cuenta que esta es una de las indicaciones dadas para la ejecución de la práctica que se viene desarrollando en este momento.

Figura 49

Búsqueda del exploit EternalBlue

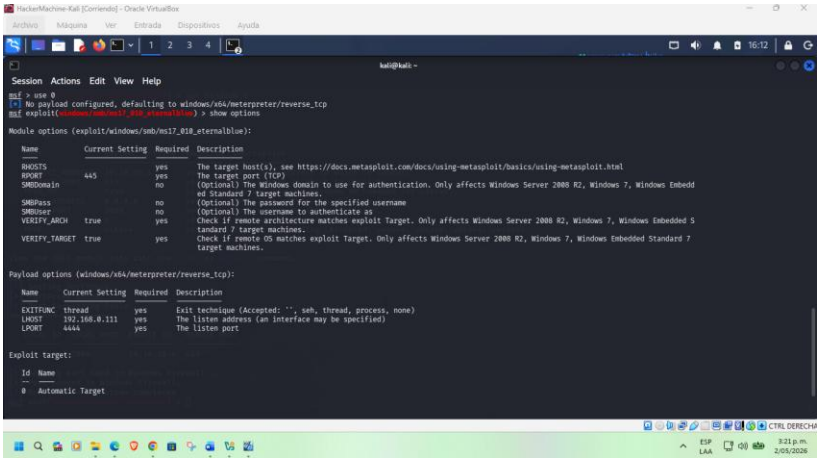


Nota. Listado de módulos para EternalBlue, seleccionando el exploit que aprovecha el fallo de manejo de paquetes SMB para obtener ejecución remota de código en la máquina interna.

Como en los módulos anteriores se procede a ejecutar el comando show options con el fin de validar las opciones y realiza la configuración del exploit EternalBlue 0.

Figura 50

Visualización de las opciones del EternalBlue

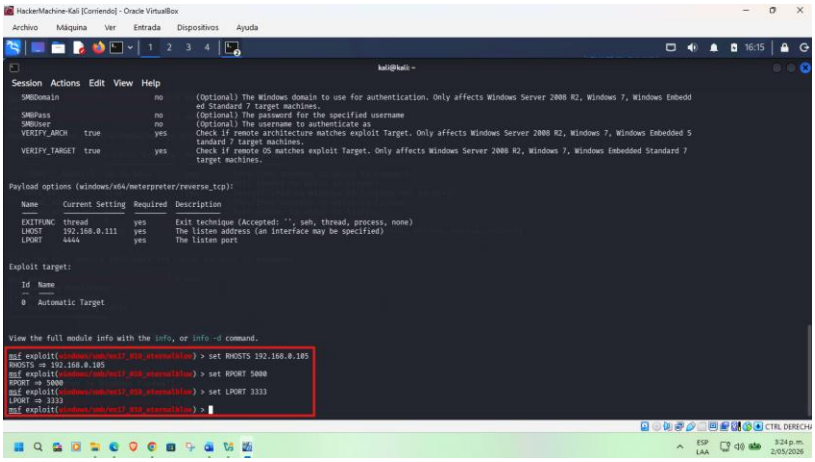


Nota. Comando show options mostrando los parámetros requeridos (RHOSTS, RPORT, payload) que deben adaptarse al entorno de pivoting configurado previamente.

Se procede con la configuración de la dirección IP de la Victim Machine por medio del comando set RHOST 192.168.0.105, posteriormente se configura el puerto 5000 teniendo en cuenta que es allí donde se está ejecutando el servicio SMB 445 de la Internal Machine ayudado del comando set RPORT 5000 y como puerto de escucha se utilizará un puerto distinto a los implementados, para ello se tomará el 3333 con el comando set LPORT 3333.

Figura 51

Configuración del exploit EternalBlue



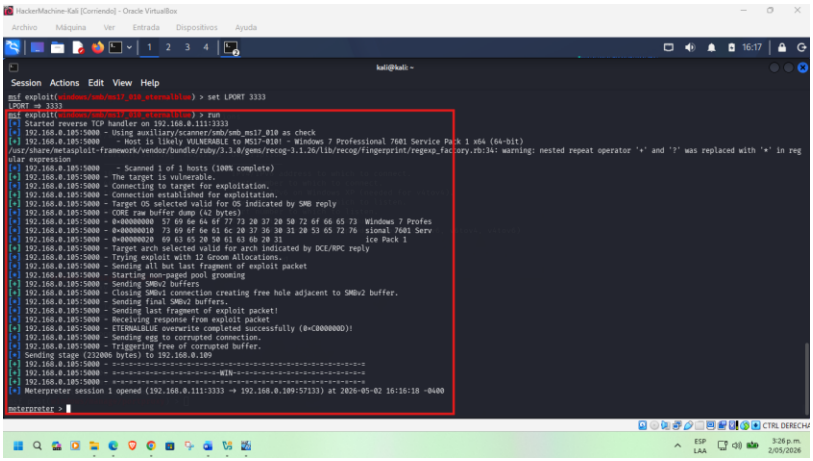
Nota. Asignación de RHOSTS (IP Victim Machine), RPORT (5000, puerto del portproxy) y LPORT (3333), adaptando el exploit para que el tráfico atraviese los túneles creados.

Se reconoce que con la ejecución del exploit EternalBlue por medio del comando run el cual nos va a mostrar una sesión abierta en el Meterpreter, indicándonos que la configuración que se realizó en el módulo anterior se ejecutó de la manera idónea para la elaboración del laboratorio simulado como lo muestra la figura siguiente.

Dando culminación a esta fase con feliz término, teniendo como resultado el correcto funcionamiento de cada uno de los módulos y la explotación correcta de cada una de las vulnerabilidades impactadas.

Figura 52

Ejecución del EternalBlue pivot a la Internal Machine



Nota. Ejecución del exploit EternalBlue abriendo la "Meterpreter session 2", confirmando el éxito del movimiento lateral y el compromiso total de la Internal Machine.

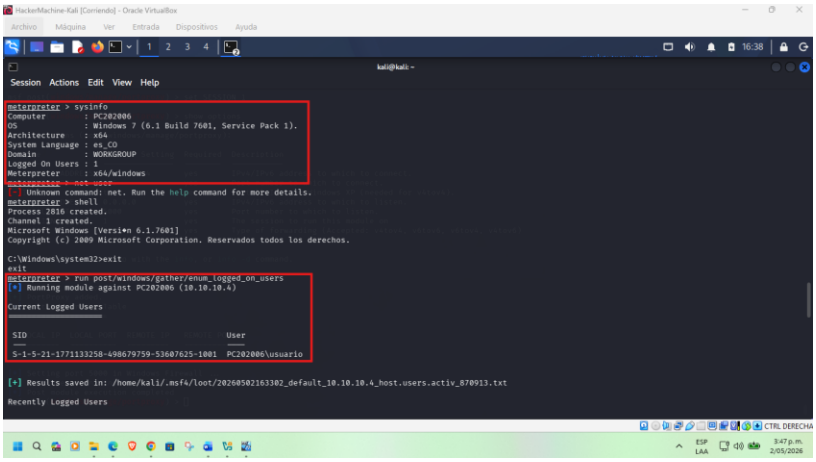
Post-Explotación

Por medio de la sesión obtenida de Meterpreter, se procede a realizar la validación de la información tanto del equipo como el usuario que se logueo en la Internal Machine, con la ejecución de comandos como sysinfo, run post/windows/gather/enum_logged_on_users, getuid, ipconfig, Con estos comandos se corrobora una vez más que el pivot y el túnel que se creó para la conexión entre estas 2 máquinas se ejecutó de la manera más correcta evidenciando así que el proceso, y el paso a paso que se llevó a cabo cumplió las expectativas hasta este punto.

Vale la pena aclarar que se realizaron diferentes pruebas tanto del sistema como de comandos para lograr el término de esta actividad, hasta tal punto que se implementaron algunos comandos adicionales más complementarios como es el caso del run post/windows/gather/enum_logged_on_users, El cual nos muestra una información más detallada como el SID correspondiente al usuario y así mismo el nombre de usuario y se encuentra en la máquina.

Figura 53

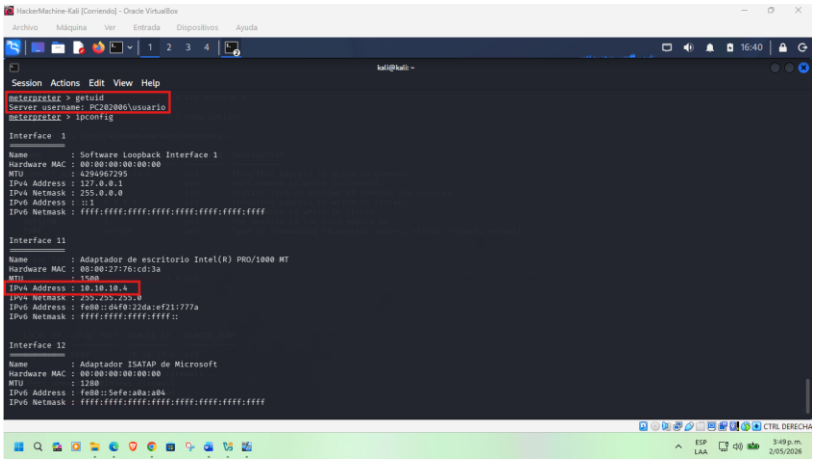
Visualización de información del equipo y usuario logueado



Nota. Comandos sysinfo y getuid en la sesión 2, mostrando el control sobre la Internal Machine y el contexto del usuario actual, iniciando la fase de post-explotación.

Figura 54

Confirmación de usuario logueado y dirección IP la Internal Machine

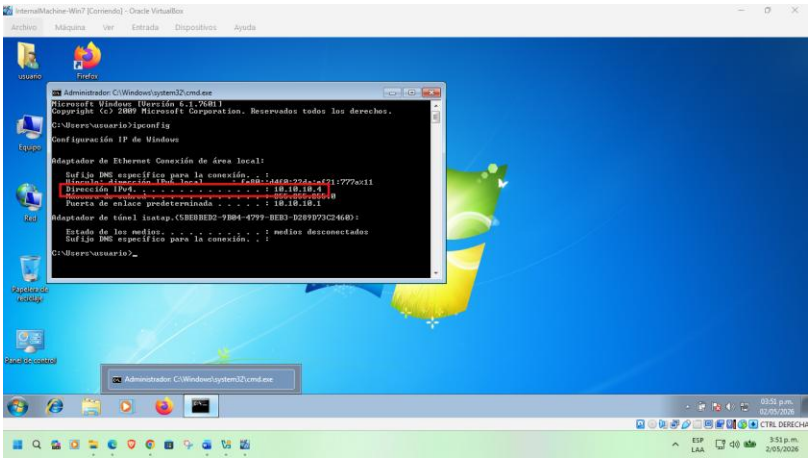


Nota. Enumeración de la identidad y red de la Internal Machine, confirmando la posición del atacante en el segmento interno antes de la escalada de privilegios.

Como una prueba más de la información que se suministra anteriormente se procede a consultar la dirección IP del Internal Machine por medio del comando ipconfig.

Figura 55

Confirmación de la dirección IP de la Internal Machine

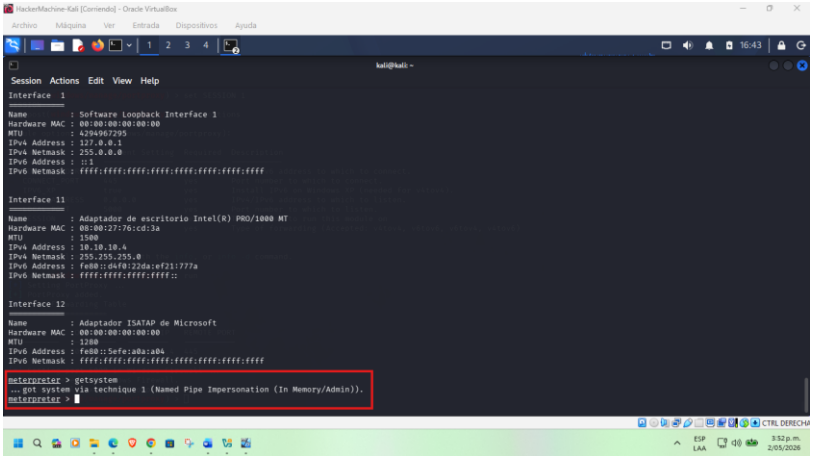


Nota. Configuración IP de la Internal Machine (10.10.10.4) obtenida a través de la sesión comprometida, corroborando la penetración exitosa del segmento de red aislado.

Posterior a ello se realizará la ejecución de un nuevo comando denominado getssystem, el cual nos ayudará a escalar privilegios en la máquina de Windows en la cuenta logueada

Figura 56

Ejecución del comando getsystem



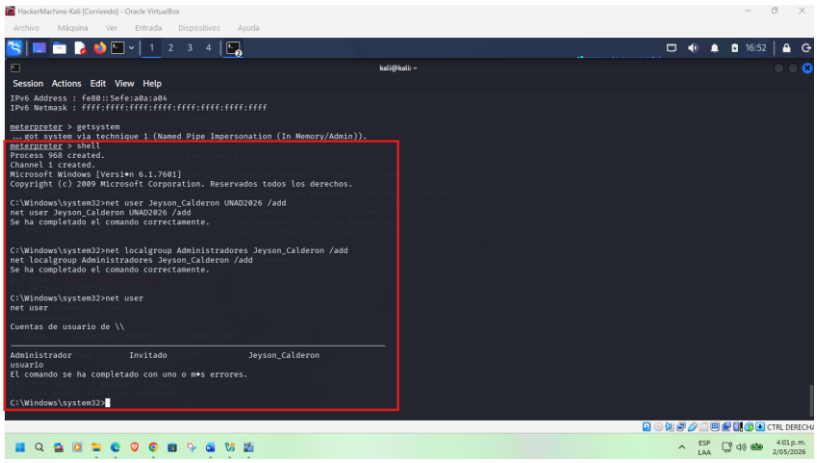
Nota. Ejecución de getsystem logrando la escalada a NT AUTHORITY\SYSTEM, otorgando control total e irrestricto sobre el sistema operativo Windows de la Internal Machine.

Luego la ejecución del comando anterior y la cuenta lo vea con privilegios de administrador, se procede a ejecutar el comando Shell, el cual se utiliza dentro de la sesión de Meterpreter con el fin de abrir una consola del sistema operativo en la Internal Machine.

Para dar continuidad con la actividad indicada por el tutor se procede a ejecutar el comando net user Jeyson_Calderon UNAD2026 /add, Con el fin de crear un usuario de red a nombre del estudiante Jeyson Calderon con una contraseña UNAD2026, posteriormente se procede a agregar dicha cuenta al grupo de Administradores de la máquina impactada por medio del comando net localgroup Administradores Jeyson_Calderon /add, Para finalmente por medio del comando net user listar los usuarios que se crearon en la Internal Machine.

Figura 57

Ejecución de Shell, creación del usuario y elevación de privilegios



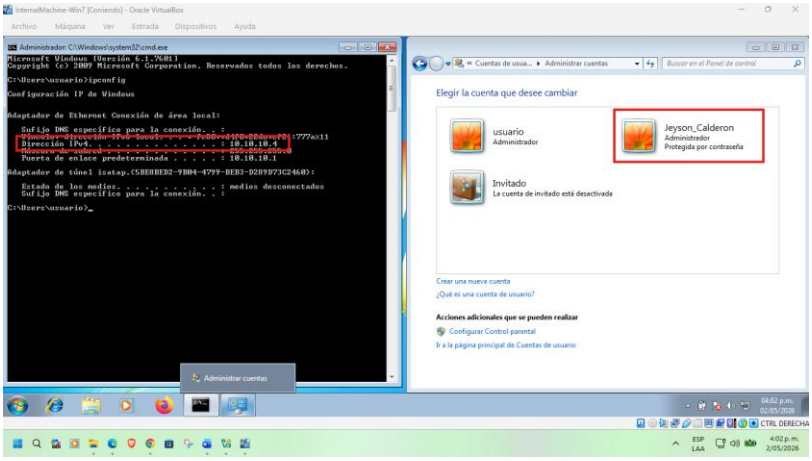
Nota. Ejecución de shell seguida de net user y net localgroup para crear el usuario "Jeyson_Calderon" con privilegios de Administrador, estableciendo persistencia en el sistema comprometido.

Y como evidencia final se ingresa directamente a la máquina impactada y desde el entorno de panel de control se ingresa a la opción cuentas de usuario, administrar cuentas, logrando ver que la cuenta de usuario con privilegios elevados de administrador se encuentra

igualmente configura y activa para su funcionamiento, dando así por terminada la práctica simulada.

Figura 58

Validación de Internal Machine con la cuenta Jeyson_Calderon configurada



Nota. Panel de Control de Windows mostrando la cuenta "Jeyson_Calderon" como Administrador, evidencia final que valida el éxito completo de la post-explotación y el control persistente del activo.

Aspectos fundamentales que situaron la exploración hacia el fallo de seguridad informática el cual afectó directamente al Host-A, con Windows 7.

"SecureNova Labs detectó fugas de información desde una estación de trabajo Windows (Host-A)."

Este resultado indica que el origen del incidente se verifica o detecta en la Máquina-1, lo que permite encaminar las indagaciones iniciales hacia dicha máquina. Y, dado que se trata de ser una estación con sistema Windows, se añade a las vulnerabilidades comunes que se suelen tener en cuenta y que pueden ser aprovechadas mediante aplicaciones web o servicios inseguros.

"La imagen forense indica que la máquina ejecutaba una aplicación vulnerable probablemente explotada para obtener shell."

Este pequeño pasaje es reiteradamente interesante, pues refleja: la existencia de una aplicación vulnerable, la posibilidad de explotación de forma remota con posibilidad de obtener una shell y evidencias de una posible explotación anterior, de hecho, estos resultados coinciden con el patrón de comportamiento del servicio Rejetto HFS, el cual es conocido de antemano por permitir la ejecución remota de órdenes, razón por la cual, en el laboratorio, se ha atacado al puerto 80 con dicho exploit.

"Evidencias de la creación no autorizada de un usuario con permisos administrativos."

De esta forma, se demostraba que el atacante había conseguido conseguir elevar privilegios en la Máquina-1 y haber alcanzado el nivel de control suficiente para poder ejecutar los comandos con permisos de administración. Este aspecto fue el que fue crítico, pues la explotación de Rejetto HFS y la escalación a SYSTEM eran acordes al escenario en el que se crean usuarios con privilegios de administración a través de herramientas como Meterpreter.

"Los registros sugieren movimientos laterales desde Host-A hacia un servidor secundario (Host-B)."

Esta información parece indicar que se realizaron técnicas desde la Máquina-1 de tipo pivoting, tunneling o proxisización del tráfico. Esta evidencia es coherente con las actividades que se desarrollaron en el laboratorio, como la ejecución de autoroute, el escaneo ARP y las herramientas de portfw y portproxy, que se refiere a la exposición del puerto SMB en un túnel. Lo que claramente corrobora que Host-A actuó como el host para el segundo host (Host-B).

"Misión del red team: determinar el vector de fuga en Host-A, validar si la vulnerabilidad fue explotada y si existió escalamiento de privilegios."

Este punto puntualiza de manera contundente los puntos a investigar: un ataque que ataca un servicio vulnerable (la aplicación web), una explotación válida que permita obtener una shell y un proceso de escalado que termine siendo la creación de un usuario administrador. En otras palabras, confirma que la vulnerabilidad tenía que reproducirse en la Máquina-1 y que de esta vulnerabilidad debía permitirse la ejecución remota de comandos. Todos estos hechos concuerdan perfectamente con el exploit de Rejetto HFS usado en la práctica.

"Reproducir en un laboratorio aislado el pivoting Host-A → Host-B."

Esto da evidencia de que Host-A tenía el acceso a otra subred, actuó como un intermediario y disponía de rutas internas activas, confirmando así que la máquina 1 era vulnerable y esto permitió al atacante acceder y comprometer a la infraestructura interna**.**

"Se habría obtenido información sensible desde el servidor secundario."

Este punto establece que la Máquina-1 actuó como el punto de entrada inicial; que el Host-A tuvo la función de enlace hacia el Host-B y que la explotación alcanzó un nivel de criticidad suficiente como para poder realizar la extracción de información.

Herramientas utilizadas en la etapa de reconocimiento y análisis

Nmap: Fue la herramienta inicial que se empleó para escanear los puertos que se encuentren abiertos en el Host-A, para identificar los servicios y las versiones de tales y ubicar también el puerto vulnerable correspondiente a la aplicación Rejetto HFS. El comando que se ejecutó fue: sudo nmap -p- -sS -sC -sV --min-rate 5000 -n -Pn -vvv 192.168.11.10 -oN escaneo_puertos.txt

Resultados destacados

- Se obtuvo como resultado que el puerto 80/tcp se encontraba abierto.
- Se identificó que el servicio HFS (Http File Server) se encontraba presente.

- Se verificó que la Máquina-1 ejecutaba una aplicación vulnerable la cual era accesible mediante HTTP.

Este resultado coincide con aquellos que se recogen en el Anexo 4 donde se da cuenta de que una estación Windows ejecutaba una aplicación vulnerable que se utilizaba como vector de compromiso.

Metasploit Framework: Se utilizó para validar la vulnerabilidad que se había identificado con anterioridad, haciendo uso de módulos que estaban disponibles para Rejetto HFS, según Rapid7 (2024).

Módulo utilizado: exploit/windows/http/Rejetto_hfs_exec

Con esta herramienta se ejecutó con éxito un exploit real sobre la Máquina-1, confirmando el hecho de que el servicio que se ejecutaba en el puerto 80 era vulnerable y la posibilidad de realizar un acceso tipo shell a través de Meterpreter.

Por lo tanto, la aplicación que se ha mencionado de manera indirecta en el Anexo 4 – Escenario 3 es, en efecto, aquella que resultó preparada para la explotación de su vulnerabilidad a través de Host-A, la aplicación que habilitó el acceso no autorizado. Y, en el laboratorio del capítulo 2, aquella aplicación sería Rejetto HFS siempre y cuando se ejecutara sobre 80/tcp.

Afectación del ataque a las máquinas con Windows 7 en la red.

El ataque planteado en el escenario descrito tiene un impacto negativo sobre las máquinas que utilizan el sistema operativo Windows (Host-A y Host-B), puesto que queda comprometida la confidencialidad, la integridad y la disponibilidad.

En primer lugar, el ataque afecta a la máquina denominada Host-A (Victim Machine) aprovechando una vulnerabilidad existente en la aplicación web Rejetto HFS, que se encontraba escuchando en el puerto 80. Tras explotar dicha vulnerabilidad, el agresor puede ejecutar código

de forma remota mediante el marco de trabajo Metasploit y tiene acceso tipo shell gracias a la sesión de Meterpreter.

Dicho acceso inicial permite el control parcial del sistema y afecta de forma directa la confidencialidad, ya que permite consultar la información interna, los procesos y la configuración del equipo. A continuación, por técnicas de escalado de privilegios (parecido al uso del comando getsystem), se logra obtener el control total del sistema (a nivel de SYSTEM), comprometiéndose así la integridad, dado que se puede mantener la configuración, se pueden ejecutar comandos administrativos, y se puede alterar el estado del sistema.

Adicionalmente, se observa la creación de un usuario administrador no autorizado, el cual se puede considerar un mecanismo de persistencia y que permite al atacante mantener el acceso incluso después de reinicios o comprobaciones básicas de seguridad.

Comprometida ya la máquina Host-A, esta es reconvertida como punto de pivoting en la red interna, pudiendo llegar a acceder a la máquina Host-B (Internal Machine). Efectuando un aprovechamiento de las técnicas de enrutamiento (autoroute), escaneo interno (arp_scanner) y redirección de puertos (portfwd y portproxy), el atacante logra oponerse a las restricciones de red en las que se encontraba y acceder a servicios internos que en principio no eran alcanzables.

En Host-B, el ataque se continúa utilizando la vulnerabilidad EternalBlue sobre el servicio SMB (puerto 445), y logra acceso remoto y control sobre esta máquina. La extensión del ataque permite la posible exfiltración de información sensible, puesto que esto afecta gravemente la confidencialidad de los datos almacenados en este servidor.

Validación de vulnerabilidades en las máquinas con Windows tras el paso a paso

El registro exhaustivo de cada una de las distintas operaciones llevadas a cabo para validar la vulnerabilidad en la máquina Windows (Host-A), además de las evidencias adjuntas, estaba ya registrado en el primer apartado del presente documento. En el apartado 1 anterior se

disponen las órdenes utilizadas, el resultado de la ejecución de estas y las capturas que atestiguan el paso dado en el proceso de reconocimiento, escaneo, explotación y validación del acceso al sistema.

Asimismo, en el mismo apartado se encontraba integrada también la descripción del proceso de pivoteo realizado hacia la segunda máquina (Host-B), donde se puede ver cómo, desde el acceso a la máquina comprometida, se han creado rutas de comunicación a la red interna. La comunicación generada permitió conocer nuevos hosts, hacer escaneos internos, redirigir puertos y finalmente explotar servicios vulnerables de la segunda máquina validando así el movimiento lateral por la infraestructura.

Por consiguiente, el conjunto de evidencias evidenciado en el apartado anterior corroboraba de forma exhaustiva la ejecución del ataque, la validación de la vulnerabilidad en la máquina Windows y la correcta ejecución de técnicas de pivoteo hacia la segunda máquina.

Timeline

Tabla 1

Línea de tiempo de la actividad realizada

Fecha/Hora	Evento	Evidencia	Interpretación
10:00	Reconocimiento de red	arp-scan -I eth0 --localnet	Identificación de Host-A en la red
10:02	Validación de conectividad	ping 192.168.0.105	Confirmación de comunicación con la víctima
10:05	Escaneo de puertos	Nmap	Identificación de puertos abiertos
10:06	Detección puerto 80	Resultado Nmap	Servicio HTTP vulnerable activo
10:07	Identificación de servicio	Rejetto HFS	Aplicación vulnerable detectada

Fecha/Hora	Evento	Evidencia	Interpretación
10:09	Inicio explotación	Metasploit	Uso de exploit Rejetto_hfs_exec
10:10	Acceso inicial	Sesión Meterpreter	Compromiso de Host-A
10:12	Validación del sistema	sysinfo, ipconfig	Confirmación de acceso a Windows
10:15	Configuración pivoting	autoroute	Enrutamiento hacia red interna
10:17	Descubrimiento red interna	arp_scanner	Identificación de Host-B
10:20	Escaneo interno	portscan/tcp	Identificación puerto 445 abierto
10:22	Creación de túnel	portfwd add -l 4445 -p 445	Redirección de tráfico SMB
10:24	Validación del túnel	nmap -p 4445 127.0.0.1	Confirmación del pivoting
10:26	Configuración avanzada	portproxy	Exposición del servicio SMB
10:28	Explotación Host-B	EternalBlue	Acceso remoto a segunda máquina
10:30	Sesión activa	Meterpreter session 2	Compromiso de Host-B
10:32	Escalamiento privilegios	getsystem	Acceso nivel SYSTEM
10:34	Acceso shell	shell	Ejecución de comandos Windows
10:36	Creación usuario	net user	Persistencia en el sistema
10:38	Asignación privilegios	net localgroup administrators	Control total del sistema
10:40	Validación final	Panel de control Windows	Evidencia de usuario creado

Nota: Se expone el timeline de la ejecución de las actividades desarrolladas en el componente practico de la actividad actual, aclarando que las horas son tentativas, ya que la actividad demoro varios días.

Plan de remediación integral

La totalidad del análisis del incidente (descrito en el escenario) más la reproducción del ataque en el laboratorio, dice que la infraestructura con la que se ha trabajado presenta debilidades considerables de configuración y gestión de vulnerabilidades, y, por tanto, se ofrece un plan de remediación que permita mitigar el nivel de seguridad de los sistemas de Windows comprometidos, y prevenir acontecimientos similares en el futuro.

En primer lugar, es necesario corregir la vulnerabilidad del software Rejetto HFS, que fue utilizada como vector de entrada en la máquina pollutants: Host-A, es recomendable su desinstalación o actualización a una versión segura, pero no permitir la exposición de servicios innecesarios en el puerto 80. Probablemente será necesaria la aplicación oportuna de parches de seguridad en el sistema operativo Windows, especialmente por los servicios críticos de este (SMB), para evitar una situación similar a estas, las vulnerabilidades conocidas y explotación a través de EternalBlue.

Asimismo, se hace necesario llevar a cabo una correcta segmentación de red que evite la comunicación directa con otras subredes. En la práctica de enseñanza se observó como la máquina comprometida (Host-A) era utilizada como trampolín para llegar a la red interna y esto significa la ausencia de controles para el aislamiento de esta red. La segmentación de red, junto a la implementación de firewalls adecuadamente configurados, permite restringir este tipo de movimientos laterales y la reducción de la superficie de ataque.

Con respecto a la gestión de accesos, hay que aplicar el principio de "mínimo privilegio", aunque en dicho principio también se incluye el hecho de que los usuarios deben avocarse únicamente a los permisos estrictos que necesitan para realizar su trabajo. La creación de cuentas administrativas no autorizadas, como la que se ha evidenciado en el ejercicio realizado, supone un riesgo crítico. Por este motivo es imprescindible establecer controles de auditoría y monitoreo

en lo que se refiere al proceso de creación y modificación de usuarios, así como también el establecimiento de políticas de contraseñas robustas.

Un segundo punto relevante es el correspondiente al monitoreo y la detección de eventos de seguridad, para ello considera que la organización debe desplegar mecanismos para reconocer actividades anómalas como escaneos de red, intentos de explotación, escalada de privilegios o movimientos laterales, entre otros. Para lograrlo, una recomendación es la implementación de soluciones de monitoreo centralizado y correlación de eventos (SIEM), así como también de herramientas de detección y respuesta para endpoints (EDR), las que permitirán tener una visibilidad constante del estado de los sistemas.

Por otra parte, es importante fortalecer la gestión de logs garantizando que los eventos relevantes del sistema, de la red y de las aplicaciones sean procesados y analizados periódicamente, lo que permitirá ayudar en la detección temprana de incidentes y también en la construcción de líneas de tiempo (timelines) forenses más precisas en caso de incidentes de seguridad.

Conectado con el aspecto anterior, desde la operativa la organización debe tener un plan de respuesta de seguridad formal, el cual contemple procedimientos claros para la contención, erradicación y recuperación de ataques. En el caso analizado, una respuesta adecuada e inmediata podría haber permitido naturalmente el aislar la máquina comprometida, evitando así la propagación a otras máquinas de la red.

Por último, se propone fomentar una cultura de seguridad en dicha organización por medio de procesos de capacitación y concientización, así como llevando a cabo pruebas de penetración y ejercicios del tipo red team/blue team de forma recurrente. Este tipo de prácticas como la de esta actividad, que se ha llevado a cabo en este escenario, permiten descubrir

debilidades reales en los distintos sistemas y mejorar la postura de seguridad vinculado a la organización de manera continua.

Por lo tanto, la aplicación de este plan de remediación no solo permitirá corregir las vulnerabilidades explotadas en el escenario, sino que significará fortalecer la seguridad de la infraestructura tecnológica en su conjunto, ya que permitirá disminuir el nivel de riesgo de la organización y mejorar la capacidad de detección y respuesta ante incidentes de seguridad de las tecnologías de la información.

Respuesta y contención ante incidentes de ciberseguridad

Diseñar estrategias de contención a partir del análisis de riesgos y vulnerabilidades presentes en una infraestructura tecnológica TI.

Aspectos para tener en cuenta en caso de un ataque en tiempo real

Desde la mirada de un experto en seguridad TI, la primera acción que hay que realizar ante un posible incidente es verificar, desde el punto de vista técnico, si efectivamente existe un ataque activo o simplemente una anomalía operacional. Para ello, es importante ejecutar un primer proceso de identificar y analizar coincidencias de Indicadores de Compromiso (IoC).

Para Patagonia (2025), la primera fase frente a un incidente de seguridad consiste en la identificación y confirmación del incidente, para lo cual se requiere revisar los logs, las alertas y los eventos de seguridad. En esta fase se examinan logs del sistema operativo, eventos del firewall, alertas generadas por el EDR, tráfico de red, autenticaciones sospechosas y conexiones no autorizadas.

Por cuestiones meramente técnicas se revisaría:

Autenticaciones fallidas o accesos fuera de horas, procesos sospechosos funcionando en memoria, conexiones salientes a direcciones IP no conocidas, elevaciones de privilegios no

esperadas, creación de túneles o caminos internos, actividad relacionada con PowerShell, CMD o Meterpreter, escaneos internos ARP o tráfico lateral de red.

En un escenario tal como el planteado durante el laboratorio, en el que el atacante utiliza Metasploit y técnicas de pivoting, una señal clara indicativa de un compromiso sería detectar conexiones entre subredes normalmente no interrelacionadas y tráfico SMB o RDP no habitual.

Ya con el incidente confirmado, la primera medida indispensable es la contención. Conforme a Illumio (s.f.), una de las primeras recomendaciones sería la de aislar inmediatamente el equipo comprometido de la red para evitar una posible propagación e impedir que el atacante pudiera comunicarse.

La contención inicial abarcaría las siguientes acciones:

Aislamiento del host comprometido

La acción para realizar sería la desconexión del equipo infectado, tanto con la red del cliente o la de internet; al menos físicamente con los medios y la infraestructura que tuviera a disposición o a través de la utilización de herramientas con EDR/NAC. Esto impediría que continuara la ejecución de acciones de movimiento lateral o la exfiltración de información por parte del atacante.

Deshabilitación de accesos comprometidos

Sosmatic (2025) considera que ante un compromiso de seguridad hay que bloquear credenciales comprometidas y deshabilitar accesos remotos que pudieran ser comprometidos tal como VPN, RDP o cuentas administrativas.

Por lo tanto, deben hacerse: Reset de contraseñas sensibles, revocación de sesiones, desactivación de cuentas sospechosas, bloqueo de tokens y credenciales comprometidas, aplicación de MFA de emergencia.

Segmentación y bloqueo de tráfico

Después, se realizarían cambios temporales de reglas en firewall interno y se realizaría segmentación con tal de limitar el tráfico no deseado. Fortinet (s.f.) afirma que las ACL permiten restringir las conexiones entre segmentos de red y reducir la superficie de ataque.

En el caso de detección de explotación sobre SMB, RDP o RPC, se procederá a la prohibición inmediata de la comunicación entre los puertos o pathway para evitar la propagación.

Eliminación de rutas de pivoting

En ataques en los que se usaría Metasploit, sería frecuente que el atacante genere rutas internas (puede usar autoroute o tunneling). Offensive Security (s.f.) arroja luz sobre el concepto de pivoting, que permite usar un equipo comprometido como un puente hacia otras redes internas.

Por lo tanto, se revisaría: Tabla de rutas, túneles activos, reglas NAT sospechosas, servicios de port forwarding, conexiones persistentes.

Si detectara rutas maliciosas, deben ser eliminadas inmediatamente

Preservación de evidencia

La importancia radica en controlar el incidente, pero la adecuada conservación de la prueba digital para análisis forenses posteriores también es necesaria. Esto engloba: Capturas de memoria, exportar logs, hashes de archivos considerados sospechosos, evidencia del tráfico de red, registro cronológico sobre la actuación realizada.

Finalmente se tiene que clasificar el incidente según la criticidad y el impacto sobre la misma organización para la llegada del plan de respuesta a incidentes.

Y para concluir, las acciones iniciales deben ser: Comprobar técnicamente el incidente, contener el ataque, aislar sistemas, bloquear accesos con compromisos, eliminar movimiento lateral, conservar la prueba, conservar continuidad operativa.

Las acciones para llevar a cabo a partir de estas son las que permitirán contener el impacto mientras se lleva a cabo el proceso de erradicación y la recuperación del entorno.

Propuesta de medidas de hardenización para que no se repita el ataque

Tras analizar el ataque evidenciado durante la fase del red team era evidente la existencia de múltiples debilidades en cuanto a la exposición de servicios, mala segmentación, controles de acceso débiles, así como un control de los logs muy limitado para esta fase.

Desde la ciberseguridad defensiva se ubica el hardening o hardenización en diferentes capas: en aplicaciones, sistema operativo, endpoint, red, en el control de logs y controles de identidad.

Control de vulnerabilidades y parcheo

La primera medida consiste en la eliminación o actualización de aplicaciones vulnerables con conexión a Internet, sobre todo para servicios concretos como HFS/Rejetto (HTTP File Server), que fue utilizado como parte del ejercicio de explotación.

Aragon (2008) documenta numerosas vulnerabilidades de ejecución remota de código sobre versiones vulnerables de Rejetto HFS. Por estos motivos, toda organización debería seguir un programa formal de gestión de vulnerabilidades y un parcheo de forma continua.

Como especialista en seguridad se propone: Inventario activo actualizado, escaneo de forma periódica de vulnerabilidades, priorización de vulnerabilidades críticas, gestión de parches automatizada, eliminación del software obsoleto.

Reducción de superficie de ataque

De acuerdo con el NIST (2008), al reducir los servicios expuestos se disminuyen las posibilidades de explotación.

De la misma forma, sería necesario deshabilitar servicios innecesarios: Limitar puertos abiertos, implementar host-based firewalls, aplicar listas de control de acceso, restringir servicios administrativos.

También debe considerarse ubicar servicios públicos en una DMZ y no directamente sobre redes internas.

Segmentación y microsegmentación de red

Una de las principales vulnerabilidades observadas en el laboratorio fue la posibilidad de realizar movimiento lateral mediante pivoting.

De acuerdo con Check Point (s.f.), la segmentación de la red es una de las defensas más eficaces contra ataques laterales.

Propondría, en consecuencia: Separa las redes críticas con VLAN, implementa firewalls internos, restringe la comunicación entre segmentos, implementa microsegmentación, limita el tráfico este-oeste, configura filtrado de salida (egress filtering).

Esto hace que un atacante no pueda utilizar un host comprometido para pivoteo hacia otros activos internos.

Endurecimiento de SMB y protocolos administrativos

Muchos ataques avanzados tienen lugar por aprovechamiento de protocolos inseguros o mal configurados.

Devore (2023) menciona que SMBv1 es una vulnerabilidad crítica en entornos Windows.

Por lo tanto, sería fundamental: Deshabilitar SMBv1, activar SMB signing, restringir SMB/RDP/RPC, endurecer permisos NTFS, auditar recursos compartidos, implementar políticas de acceso restringido.

Principio de mínimo privilegio

Una de las técnicas de hardening más importantes es la restricción de privilegios administrativos.

Se propone: Emplear cuentas administrativas separadas, implementar MFA, utilizar modelos JIT/JEA, restringir privilegios locales, auditar cuentas privilegiadas.

Esto reduce significativamente el impacto de credenciales comprometidas.

Protección avanzada de endpoints (EDR)

Aarness (2025) expresa que las soluciones EDR pueden detectar comportamientos maliciosos avanzados en tiempo real.

La organización debiera implementar la detección de: Shells reversos, monitoreo de PowerShell, bloqueo de binarios sospechosos, control de la aplicación, detección basada en comportamiento, aislamiento automático de endpoints.

Para un endurecimiento de PowerShell, Balkin (2025) sugiere las firmas digitales y políticas de ejecución restringida.

SIEM y monitoreo centralizado

El monitoreo centralizado es fundamental para detectar actividades anómalas. Jurado Moreano (2015) comenta que los SIEM permiten correlacionar eventos provenientes de un conjunto múltiple de fuentes, y detectar patrones de ataque.

Como contra medida defensiva propondría: Correlación de logs, alertas en tiempo real, detección de ARP scanning, monitoreo de tráfico lateral, identificación de tunneling, dashboards de amenazas.

Control del tráfico de salida

El filtrado del tráfico de salida disminuye la capacidad del atacante para comunicarse con servidores C2.

Se podría establecer: Filtrado DNS, whitelisting de destinos, proxy de inspección TLS, restricción de conexiones externas.

Copias de seguridad y continuidad operativa

Ante una situación de estas, es recomendable para toda organización que se deba contar con elementos importantes como el caso de: Backups offline, respaldos versionados, procedimientos de recuperación, simulacros periódicos, planes de continuidad.

Todo esto con el objetivo de reducir tiempos de recuperación ante incidentes críticos.

Capacitación y cultura de seguridad

IBM (s.f.) afirma que la respuesta a los incidentes no depende únicamente de la tecnología, sino también de los procesos y de las personas.

Por eso, es importante: Capacitar al SOC, mantener los playbooks, actualizar los IoCs y los TTPs, realizar ejercicios de red team/blue team, fortalecer la cultura organizacional.

Por lo tanto, la hardenización debe ser integral sobre la infraestructura, sobre las identidades, sobre el control y sobre la operación, para reducir la posibilidad de explotación y el impacto de los futuros incidentes.

Diferencias entre un equipo blue team y un equipo de respuesta a incidentes informáticos

En el contexto de una organización existen tanto el blue team como el equipo de respuesta a incidentes informáticos, que desempeñan funciones muy importantes en la protección de esa infraestructura tecnológica a través de sus propias funciones. Si bien es cierto que estos desempeñan funciones muy importantes en el área defensiva de la ciberseguridad, también es cierto que existen notables diferencias relacionadas con sus objetivos, funciones, herramientas y el momento en que funcionan al detectar una amenaza.

Blue team

Tiene un enfoque principalmente preventivo y defensivo y que su función es proteger de forma continua (mediante el monitoreo permanente, la hardenización, el análisis de vulnerabilidades y la aplicación de controles de seguridad).

Para la UNAD (2025), el blue team debe hacer un análisis de lo que ocurre continuamente a nivel técnico con el fin de contener todo tipo de amenazas y mantener protegida la infraestructura tecnológica.

Desde la perspectiva operativa, el blue team trabaja de forma diaria llevando a cabo actividades como el monitoreo SIEM, la configuración de cortafuegos, la segmentación de redes, el control de logs, la implementación de controles EDR y el hardening de servidores y endpoints, además de detectar comportamientos sospechosos incluso antes de que se conviertan en incidentes críticos, su objetivo es reducir la probabilidad de éxito de un ataque y mejorar la postura de seguridad de la organización.

Equipo de respuesta de incidentes informáticos

Tiene como denominación Incident Response Team (IR Team), ése que se activa cuando el incidente ya se ha producido o se está produciendo. La acción primordial del equipo IRT es contener el ataque, erradicar el ataque, recuperar los servicios comprometidos y preservar la información digital para la analítica forense.

Las tareas del proceso de respuesta a incidentes definidos en el NIST SP 800-61 indicada por Mitratech (2021) se recogen en fases de preparación, identificación, contención, erradicación, recuperación y la fase de lecciones aprendidas. En este sentido, el IR Team es un equipo técnico especializado en la gestión de crisis de ciberseguridad centrado en la minimizar el impacto operativo y en la restauración a la normalidad tan pronto como sea posible.

Las tareas principales del equipo IR Team son, entre otras, la validación técnica del ataque, el aislamiento de sistemas comprometidos, la analítica forense, la recuperación de servicios, la eliminación del malware y la documentación técnica del incidente. También se encargan de coordinar comunicaciones internas y de manejar crisis en eventos de alta criticidad.

A continuación, se presenta una comparación entre ambos equipos:

Tabla 2

Comparación entre equipos

Blue team	Equipo de respuesta a incidentes
Tiene un enfoque preventivo y defensivo.	Tiene un enfoque reactivo y correctivo.
Trabaja de manera continua monitoreando la infraestructura.	Actúa cuando el incidente ya ocurrió o está en proceso.
Realiza hardenización y fortalecimiento de sistemas.	Ejecuta contención, erradicación y recuperación.
Gestiona vulnerabilidades y controles de seguridad.	Analiza el impacto y la causa raíz del incidente.
Utiliza herramientas SIEM, EDR, firewalls y monitoreo.	Utiliza herramientas forenses y de análisis de incidentes.
Busca evitar que ocurra un ataque.	Busca minimizar el daño del incidente.

Nota. Análisis de los comportamientos de cada uno de los equipos motivo de estudio

A pesar de que sus funciones son diferentes, ambos equipos se ayudan dentro de una estrategia global de ciberseguridad. El blue team constantemente reforzará la postura defensiva de la organización, y el equipo de respuesta a incidentes entrará en escena cuando las medidas

preventivas se vean superadas. Trabajar conjuntamente es lo que permite mejorar la capacidad de detección, contención y recuperación ante amenazas avanzadas.

Utilización de CIS (Center for Internet Security) en equipo blue team

Formando parte de un equipo blue team, el CIS representa una de las referencias más relevantes para asegurar la postura de seguridad de una organización. Center for Internet Security (s.f.) es la organización que establece lineamientos, benchmarks y controles en su propuesta orientada a mejorar la configuración segura de sistemas, aplicaciones y dispositivos tecnológicos. Desde la perspectiva de un profesional especializado en la seguridad informática, el CIS permite poner en producción las buenas prácticas internacionales para reducir las vulnerabilidades, mitigar los riesgos y mejorar la capacidad defensiva de la infraestructura tecnológica. Por otro lado, el escenario de referencia que propone la UNAD (2025), habla por sí mismo, al conseguir que se hagan vigentes estrategias de aseguramiento y de fortalecimiento de la infraestructura tecnológica en el marco de controles de seguridad orientados a prevenir y a contener las amenazas.

Hardenización de sistemas

Los CIS Benchmarks son configuraciones técnicas recomendadas para las diferentes plataformas tecnológicas: sistemas operativos, servidores, bases de datos, navegadores, cortafuegos, dispositivos de red y cloud; con estos se logra endurecer la seguridad de los sistemas mediante procesos de endurecimiento para reducir la superficie de ataque.

En el seno de un equipo blue team, los benchmarks son usados para deshabilitar servicios inseguros, realizar una reducción de puertos abiertos innecesarios, limitar privilegios administrativos y endurecer protocolos de autenticación y comunicación. Igualmente permiten endurecer los endpoints y servidores críticos con configuraciones seguras validadas previamente por personal experto en ciberseguridad. Según Center for Internet Security (s.f.), la

implementación de esta configuración permite prevenir explotaciones como consecuencia de errores en la configuración y servicios vulnerables expuestos a la red.

Creación de baselines de seguridad

Un uso significativo de CIS en el blue team está asociado a la generación de líneas base o baselines de seguridad. Estas líneas base permiten fijar configuraciones estándar que deben ser cumplidas por todos los equipos de la organización y que deben ser cumplidas en la preparación para la producción.

Desde una perspectiva defensiva, estas baselines permiten conseguir la homogeneidad a lo largo de la infraestructura tecnológica y poder localizar los cambios no trazados o no autorizados. Igualmente permiten comprobar que los sistemas mantendrán configuraciones acordadas a la par de políticas internas, así como las exigencias de normativas internacionales. Esto reduce considerablemente los errores de configuración y favorece el control respecto a activos tecnológicos a nivel de la organización, a lo que también se refiere en las estrategias defensivas del escenario académico de la UNAD (2025).

Aplicación de CIS Controls

Los CIS Controls se comprenden como un conjunto de controles priorizados encaminados a prevenir ataques y mejorar la posibilidad de defensa de las organizaciones. Así lo indica Center for Internet Security (s.f.) afirmando que estos controles hacen que se fortalezcan procesos relacionados al inventario de activos, gestión de vulnerabilidades, control de accesos y monitorización continua.

En el contexto de lo planteado por un equipo blue team, como en el caso de los CIS Controls, esto sería para identificar los activos críticos, llevar a cabo la gestión de vulnerabilidades de forma periódica e identificar y proteger endpoints. De este modo, los CIS Controls vendrían a ser útiles para moldear las formas de hacer el monitoreo de los eventos de

seguridad y controlar los privilegios administrativos, pero también facilitarían el detectar de forma más eficiente las actividades sospechosas u otros ataques a los sistemas. Esto mismo se considera para dar forma a lo que es una estrategia defensiva, de una forma totalmente estructurada como lo establecen las amenazas avanzadas, que se intenta igualmente dentro de los procesos de "Contención"/"Post-Compromised" y el"Hardening" que propone la UNAD (2025).

Reducción de superficie de ataque

El ejercicio realizado durante la fase red team demostró la existencia de configuraciones inseguras y de servicios expuestos en la infraestructura de la infraestructura tecnológica. En este sentido, CIS permite reducir significativamente la superficie de ataque mediante configuraciones seguras y controles preventivos.

Un especialista en seguridad informática utilizaría CIS para deshabilitar servicios innecesarios, minimizar el acceso administrativo, reforzar protocolos inseguros o, además, reducir la exposición de los sistemas a las redes no confiables; de este modo, se hace más complicado que un atacante pueda ejecutar explotación remota, movimiento lateral o escalamiento de privilegios dentro de la organización. Ayuda también a la segmentación y refuerzo de configuraciones, de modo que se minimizan los vectores de ataque de pivoting y propagación internos, similares a los analizados en el ejercicio práctico que se hizo la UNAD (2025).

Auditoría y cumplimiento

El CIS también es una guía importante para los procesos de auditoría y cumplimiento que se llevan a cabo en la organización. Los benchmarks y controles creados por el CIS permiten la verificación de configuraciones seguras y la evaluación del nivel de madurez defensiva que tiene la infraestructura tecnológica.

Desde la perspectiva del blue team, estas herramientas permiten la generación de reportes técnicos, la validación del cumplimiento interno o la evaluación continua de riesgos, y también ayudan a mejorar la trazabilidad de configuraciones y detectar vulnerabilidades o disconformidades respecto a políticas de seguridad predefinidas. Esto facilita el fortalecimiento de los procesos de gestión de riesgos y mejora continua de la organización a partir de una actividad académica de aseguramiento y contención promovida por la UNAD (2025).

Por último, se puede decir que el CIS actúa como una guía técnica y estratégica que va a permitir al blue team reforzar la infraestructura tecnológica y reducir riesgos, consolidando las capacidades defensivas frente a amenazas cibernéticas.

Funciones y características principales de un SIEM

Un SIEM (Security Information and Event Management) es una plataforma que se encarga de recoger, correlacionar, analizar y monitorizar eventos de seguridad de diversas fuentes de dispositivos y sistemas de la propia organización. Estas herramientas permiten una centralización de la información de seguridad mejorando la detección y respuesta ante eventos impropios. La visión de Microsoft (s.f.): "Mediante SIEM se puede detectar, investigar y responder libros importantes incidentes de ciberseguridad. Un SIEM utiliza la analítica de eventos y logs para hacerlo en forma centralizada para eventos y logs generados en la infraestructura tecnológica". En el contexto expuesto por la UNAD (2025), las soluciones SIEM son fundamentales para mejorar las capacidades defensivas y los procesos de monitorización que pueden llevar a cabo un equipo blue team.

Recolección centralizada de logs

Una de las funciones más destacadas de un SIEM es la de recopilar y centralizar logs de diferentes fuentes de información. Las fuentes que se pueden incluir son los firewalls, servidores,

sistemas operativos Windows y Linux, IDS/IPS, antivirus, soluciones EDR, aplicaciones corporativas y routers y switches, por poner solo algunos de estos.

La centralización de los logs permite al equipo de seguridad tener una visibilidad completa del entorno tecnológico desde una sola plataforma, lo cual simplifica el análisis de los eventos sin que los administradores tengan que examinar cada dispositivo en particular. Además, la centralización de los logs permite llevar trazabilidad de las actividades realizadas en la infraestructura, facilitando así procesos de auditoría y análisis forense. Jurado Moreano (2015) argumenta en este sentido que esta forma de centralización mejora de forma notable la gestión de eventos de seguridad y mejora notablemente el tiempo de respuesta ante incidentes de seguridad.

Correlación de eventos

Se entiende por correlación de eventos la capacidad de relacionar múltiples registros que, salvo por el hecho de coincidir en el tiempo o en la estación, parecen ser independentes, con el fin de detectar patrones de comportamiento comunicados a potenciales ataques a la red o a la información. Así, por ejemplo, el SIEM puede correlacionar los eventos de intentos fallidos de autenticación junto con el de un acceso exitoso inmediato y el de un escaneo interno de red y el de una elevación de privilegios, todos ellos realizados desde un único ordenador o usuario.

Cuando estos eventos se correlacionan entre sí, el SIEM podrá generar alertas indicando la posible existencia de una amenaza activa. Jurado Moreano (2015) indica que las correlaciones de eventos son una de las funciones más importantes de un SIEM, ya que permitirán descubrir ataques complejos que resultarían invisibles a partir del análisis aislado de logs.

Alertas en tiempo real

Además, los SIEM tienen la capacidad de generar alertas automáticas en tiempo real basadas en la detección de comportamientos anómalos dentro de la red corporativa. Estas alertas

pueden generarse frente a eventos basados en accesos no autorizados, ataques de fuerza bruta, escaneos internos, tráfico no habitual, creación de túneles sospechosos o movimiento lateral.

La capacidad de generar alertas de forma continua, o en tiempo real, da la oportunidad del equipo blue team de reaccionar con rapidez ante posibles incidentes, aplicar medidas de contención antes de que el ataque bese aquellos servicios críticos de la organización. En los escenarios de ciberseguridad modernos esta capacidad es fundamental dado que puede reducir el tiempo de detección y el impacto operativo de una amenaza.

Detección de anomalías

Los SIEM modernos añaden otras funcionalidades avanzadas de detección de anomalías basadas en reglas de correlacionado, comportamiento de usuarios y análisis estadístico. Esta funcionalidad permite conocer actividades que son diferentes del comportamiento normal de la organización.

Por ejemplo, el sistema puede responder a conexiones fuera de horario laboral, transferencias anómalas de información, ejecución de procesos inesperados o acceso desde ubicaciones no habituales. Microsoft (s.f.) considera que muchos de los SIEM actuales están utilizando inteligencia artificial y análisis de comportamiento para mejorar la detección de amenazas avanzadas y ataques persistentes.

Gestión de incidentes y análisis forense

Otra de las funciones relevantes que se consideran de un SIEM es el apoyo en los procesos de gestión de incidentes y análisis forense. Este tipo de plataformas nos permiten almacenamiento de registros históricos, se generan líneas de tiempo y almacenan elementos de prueba digital asociados con actividades sospechosas de la infraestructura tecnológica.

Desde la perspectiva de esta nueva capacidad, los analistas de la seguridad pueden reconstruir un incidente de seguridad, conocer la forma de ataque y saber qué ha hecho el

atacante en el entorno afectado. Igualmente, la información acumulada da pie a la redacción de informes técnicos, de mejora de los procesos de respuesta y recuperación de incidentes de ciberseguridad.

Dashboards y monitoreo centralizado

Los SIEM también proporcionan dashboards o paneles con la información que nos permiten tener un estado general de la seguridad de la organización en tiempo real. Los datos que generan estos dashboards afectan a elementos que tienen que ver con amenazas activas, eventos críticos, tendencias de ataque, tráfico sospechoso y comportamiento de los usuarios.

De tal forma, esta centralización facilita la operativa diaria del SOC y del equipo blue team ya que permite clasificar incidentes y actuar rápidamente frente a posibles amenazas. Además, los dashboards ayudan a mejorar el análisis estratégico de riesgos y en la mejora de los procesos de monitoring y supervisión continua de la infraestructura tecnológica.

Cumplimiento normativo

Por último, los SIEM son importantes en procesos de cumplimiento normativo y de auditoría. Estas plataformas permiten almacenar logs históricos, generar reportes automáticos y mantener trazabilidad de eventos de seguridad, favoreciendo el cumplimiento de estándares y marcos regulatorios (ISO 27001, NIST, PCI-DSS, GDPR).

Desde el punto de vista organizacional, esta capacidad favorece también la demostración del cumplimiento de la empresa respecto de controles de monitoreo y gestión de eventos en buena práctica internacional y de los procesos de auditoría interna y de evaluación continua de riesgos en la propia organización.

En conclusión, un SIEM es una herramienta básica en cualquier estrategia defensiva de ciberseguridad porque permite centralizar eventos, detectar amenazas, correlacionar actividades sospechosas y mejorar la capacidad de respuesta ante incidentes de seguridad informática

Herramientas de contención de ataques informáticos

Las herramientas de contención de ciberataques tienen como objetivo principal impedir, limitar o aislar una amenaza activa en una infraestructura tecnológica. Estas herramientas ayudan a reducir el impacto de un incidente de seguridad, detener un ataque en progreso y proteger los activos críticos de la organización mientras se llevan a cabo los mecanismos de análisis y recuperación. Desde la perspectiva de un experto en la especialidad de la seguridad informática, la contención es uno de los pasos más relevantes en la respuesta a incidentes, dado que una reacción rápida puede conseguir evitar amplias afectaciones sobre servicios, usuarios y datos corporativos. En términos del escenario considerado por la UNAD (2025), los controles de seguridad y los medios de contención son un medio indispensable para agrandar las capacidades defensivas contra amenazas avanzadas.

Firewall

El firewall constituye una de las herramientas más sublimes que nos permiten contener ataques por parte de sistemas maliciosos. Su objetivo fundamental consiste en la monitorización y mediante el filtrado o control del tráfico que entre o que salga de la infraestructura tecnológica.

Según se desprende de la definición que da Sophos (s.f.), un firewall es un mecanismo de seguridad que permite bloquear conexiones no autorizadas y los sistemas de seguridad de los sistemas frente a tales accesos maliciosos.

En un escenario de ataque, el firewall para el bloqueo de direcciones IP cuya razón de ser levantan sospechas, el blindaje de puertos vulnerables o la contención de conexiones activas que guardan relación con la actividad maliciosa. Permiten también la posibilidad de aplicar segmentación de red o restringir la comunicación entre las distintas subredes, dificultar el movimiento lateral del atacante dentro de la organización. Si se empleasen ataques parecidos al que se vió desarrollado durante la fase red team podría darse la circunstancia de que un firewall

bien configurado pudiese impedir las conexiones relativas a pivoting, tunneling o acceso remoto no autorizado.

Adicionalmente, los firewalls modernos incorporan capacidades avanzadas como la de realizar inspección profunda de paquetes, filtrado de aplicaciones o detección de amenazas, lo que permite una capacidad de contener ataques mucho más complejos.

EDR (Endpoint Detection and Response)

Las soluciones EDR son herramientas para proteger y monitorizar endpoints como estaciones de trabajo, servidores y equipos corporativos, según Aarness (2025), que argumenta que los EDR permiten detectar, analizar y permitir respuestas a amenazas avanzadas ejecutando una monitorización continua del comportamiento de los dispositivos.

Desde el punto de vista de un equipo blue team, los EDR son esenciales para contener ataques activos al estar en una fase en que no es necesario apagar el sistema directamente afectado, se pueden ejecutar diferentes tareas hasta el punto de poder contener ataques. De esta forma, los EDR permiten aislar equipos comprometidos de la red corporativa, finalizar procesos maliciosos, bloquear malware y detectar actividad sospechosa constituida por shells inversos, ejecución de PowerShell o escalamiento de privilegios.

Finalmente, los EDR permiten conservar evidencia digital útil para procesos de análisis forense y reconstrucción del incidente. El ciclo de vida de un ataque queda definido y se puede así localizar el origen del ataque y las acciones ejecutadas por el atacante en el entorno comprometido. Debido a estas características, las soluciones EDR son uno de los mecanismos más efectivos para reducir los tiempos de respuesta y el impacto operativo de un incidente de seguridad.

NAC (Network Access Control)

Es un potente recurso orientado a controlar y gestionar los dispositivos que intentan conectarse a la red corporativa. El objetivo principal de una solución de NAC es verificar qué dispositivos pueden acceder a la infraestructura tecnológica y qué condiciones de seguridad se les permite dicha conexión. Desde el punto de vista de un especialista en seguridad, esta solución de NAC representa un mecanismo básico para aumentar los controles de acceso y reducir los riesgos de tener dispositivos comprometidos o no autorizados. Fortinet (s.f.) comenta que NAC permite implementar políticas de autenticación, validación y cumplimiento de la seguridad antes de dar acceso a los recursos de la red.

En la dirección de un proceso de contención de incidentes, una solución de NAC permite determinar dispositivos sospechosos y recortar automáticamente su conectividad, evitando las potenciales propagaciones de amenazas de seguridad por parte de los dispositivos no autorizados y/o los dispositivos comprometidos. De hecho, estas herramientas pueden mover equipos comprometidos hacia VLAN de cuarentena, limitar el acceso del recurso crítico y bloquear protocolos inseguros mientras se produce el análisis correspondiente. Esta capacidad tiene una importancia significativa si se consideran ataques que requieran movimiento lateral, propagación de malware o accesos no autorizados entre distintas partes de la red.

Desde una óptica defensiva, el NAC también puede potenciar las políticas de seguridad organizacionales puesto que comparte el estado de los dispositivos y como condición de conexión a la red habilita la verificación del estado de la máquina en aspectos como antivirus actualizado, parches de seguridad, configuraciones de protección, etc. Del mismo modo, también puede enriquecer la visibilidad y el control de los activos conectadas a la infraestructura tecnológica favoreciendo de esta manera al equipo blue team respecto a accesos no autorizados,

detección de comportamientos inusuales y limitaciones de la propagación de las amenazas ya dentro de la red corporativa.

Relación entre hallazgos identificados y controles de mitigación

A fin de mejorar la postura de seguridad de la organización, los controles del blue team propuestos se corresponden con las vulnerabilidades y técnicas descritas en el desarrollo del laboratorio de pentesting. La siguiente tabla muestra la relación entre los hallazgos obtenidos y las medidas de mitigación propuestas.

Tabla 3

Hallazgo, riesgo y control

Hallazgo identificado durante el laboratorio	**Riesgo asociado**	**Control blue team recomendado**
Servicio Rejetto HFS vulnerable expuesto en el puerto 80	Acceso remoto no autorizado	Hardening, actualización de software y gestión de vulnerabilidades
Escaneo y enumeración de servicios	Exposición innecesaria de servicios	Firewall, ACL y reducción de superficie de ataque
Obtención de acceso inicial mediante Metasploit	Compromiso del sistema objetivo	EDR y monitoreo de comportamiento
Pivoting entre segmentos de red	Movimiento lateral del atacante	Segmentación de red
Explotación de EternalBlue (SMBv1)	Compromiso de equipos internos	Gestión de parches y deshabilitación de SMBv1

Hallazgo identificado durante el laboratorio	**Riesgo asociado**	**Control blue team recomendado**
Escalamiento de privilegios	Control total del sistema comprometido	Principio de mínimo privilegio y monitoreo de cuentas
Actividades maliciosas sobre los endpoints	Persistencia y ejecución de código malicioso	EDR
Eventos anómalos generados durante el ataque	Falta de detección temprana	SIEM y correlación de eventos

Nota: La relación entre los hallazgos identificados y los controles implementados pone de manifiesto la necesidad de relacionar las actividades ofensivas de un red team con mecanismos de prevención, detección y respuesta que corresponden a un blue team. Con ello se pretende reducir la superficie de ataque, limitar el movimiento lateral, detectar actividades sospechosas y, de este modo, mejorar la resiliencia de la infraestructura frente a incidentes de ciberseguridad.

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/g52dr-HO5x0

Conclusiones

El estudio comparativo de la Ley 1273 de 2009, de la Ley 1581 de 2012 y el análisis del caso SecureNova Labs, así como de la responsabilidad moral, llevaron a concluir que el ejercicio de la ciberseguridad debe llevar dispuesto un cumplimiento legal muy riguroso. La decisión del COPNIA de rechazar las prácticas de ciberespionaje, es demostrativa de cómo la integridad profesional y la protección de la información deben estar por encima de cualquier tipo de incentivo económico, logrando así la sostenibilidad de la carrera y el respeto por los derechos fundamentales.

El laboratorio práctico sirvió para comprobar el funcionamiento de las metodologías ofensivas en un entorno controlado. Con Nmap se detalla que el puerto 80 es vulnerable, que se puede explotar en el servicio de Rejetto HFS que ofrece Metasploit. Con la obtención oportuna de la sesión de Meterpreter, se expresa como el funcionamiento de una aplicación vulnerable puede suponer un vector de entrada para realizar el compromiso inicial del sistema.

Con respecto al movimiento lateral, a través de la técnica de pivoting se utilizó autoroute y portproxy con el objetivo de exponer el puerto SMB de la Internal Machine que permitió la explotación de la vulnerabilidad EternalBlue, en la post-explotación se realizó el comando getsystem para la escalada de privilegios a nivel system; además, la creación del usuario administrativo Jeyson_Calderon validó la persistencia y el control total sobre la Internal Machine, lo que demostró que no segmentar la red puede ser muy perjudicial.

Las estrategias defensivas responden directamente a las vulnerabilidades explotadas en el laboratorio. El hardening y los CIS Controls mitigan las configuraciones inseguras (como Rejetto HFS y SMBv1) reduciendo la superficie de ataque. El SIEM detecta eventos anómalos como el escaneo ARP y el tunneling, mientras que el EDR bloquea actividad maliciosa en endpoints (escalada de privilegios y creación de usuarios). Finalmente, el firewall y el NAC restringen el

tráfico y el pivoting lateral, demostrando que la defensa efectiva requiere la articulación de tecnología y procesos.

El informe integró las perspectivas red team y blue team, demostrando que la ciberseguridad organizacional no depende solo de herramientas tecnológicas. La reproducción de ataques en entornos aislados, sumada a la propuesta de un plan de remediación basado en segmentación, mínimo privilegio y monitoreo continuo, consolidó una visión integral para garantizar la confidencialidad, integridad y disponibilidad de la información.

Recomendaciones

Acciones inmediatas (prioridad urgente)

Aplicar urgentemente los parches correspondientes a las vulnerabilidades explotadas en el laboratorio: Rejetto HFS (puerto 80) y EternalBlue sobre SMBv1 (puerto 445), además de desinstalar software obsoleto. Para comprobar su efectividad, se deben ejecutar nuevos escaneos con Nmap y OpenVAS que confirmen el cierre de puertos vulnerables y la correcta aplicación de los parches.

Aplicar configuraciones seguras basadas en los CIS Benchmarks, deshabilitando protocolos inseguros como SMBv1 y eliminando cuentas no autorizadas como la creada durante la post-explotación (Jeyson_Calderon). Su efectividad se valida mediante auditorías de configuración comparadas contra los baselines CIS definidos, identificando cualquier desviación persistente.

Restringir permisos de usuarios y servicios, eliminando cuentas administrativas no autorizadas e implementando autenticación multifactor (MFA) en accesos críticos. Para validar su cumplimiento, se recomienda realizar auditorías de cuentas usando herramientas como PowerView o BloodHound, junto con la revisión exhaustiva de políticas de grupo (GPO).

Acciones de mediano plazo (prioridad media)

Implementar VLANs y firewalls internos para impedir el pivoting y movimiento lateral, tal como se evidenció al enrutar tráfico desde la Victim Machine hacia la Internal Machine con autoroute y portproxy. Su efectividad se confirma revisando las reglas de firewall y ejecutando pruebas controladas de conectividad entre segmentos para garantizar el aislamiento adecuado.

Desplegar una solución SIEM que centralice logs y correlacione eventos anómalos como escaneos ARP, tunneling y movimientos laterales ejecutados en la práctica. Para validar su

implementación, se deben revisar las alertas generadas ante simulaciones de ataques y confirmar la correcta correlación de eventos.

Implementar soluciones EDR para detectar y contener actividad maliciosa como shells reversos, escalada de privilegios con getsystem y creación de usuarios no autorizados. Su efectividad se comprueba ejecutando pruebas controladas de explotación con el EDR activo y confirmando la generación de alertas y la contención automática.

Implementar una solución NAC que valide el cumplimiento de políticas de seguridad (antivirus, parches, configuración segura) antes de permitir el acceso a la red corporativa. Para garantizar su efectividad, se deben conectar dispositivos no conformes y validar su redirección automática a una VLAN de cuarentena.

Acciones permanentes (prioridad continua)

Realizar ejercicios continuos de pentesting y defensa para validar la efectividad de los controles implementados y detectar nuevas debilidades. Su efectividad se mide documentando los resultados de cada simulación y evaluando la mejora en los tiempos de detección y respuesta (MTTD/MTTR) a lo largo del tiempo.

Diseñar y probar periódicamente planes de respuesta que incluyan procedimientos de contención, erradicación y recuperación alineados con los hallazgos del laboratorio (aislamiento de hosts, eliminación de rutas de pivoting, preservación de evidencia). Para confirmar su efectividad, se deben ejecutar simulacros al menos dos veces al año y evaluar los resultados mediante lecciones aprendidas.

Implementar programas continuos de capacitación en ingeniería social, phishing y buenas prácticas digitales, dado que el factor humano sigue siendo un vector de riesgo principal. Su impacto se mide aplicando campañas de phishing controlado y evaluando la tasa de reportes y clics maliciosos, lo cual permite identificar las áreas que requieren mayor refuerzo formativo.

Garantizar que todas las actividades de pentesting se realicen bajo el cumplimiento de la Ley 1273 de 2009, la Ley 1581 de 2012 y el Código de Ética del COPNIA, únicamente en entornos autorizados. Para validar su cumplimiento, se debe contar con autorizaciones formales (NDA y scope documentado) antes de cualquier prueba de seguridad, asegurando así la trazabilidad y legalidad de las acciones realizadas.

Referencias Bibliográficas

Aarness, A. (2025). *What is endpoint detection and response (EDR)?* https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

Aragon, F. M. (2008). *Rejetto HTTP file server (HFS) 1.5/2.x - Multiple vulnerabilities.* https://www.exploit-db.com/exploits/31056

Balkin, B. (2025). *Defiéndase contra los ataques de Powershell.* https://calcomsoftware.com/defiendase-contra-los-ataques-de-powershell/

Center for Internet Security. (s.f.). *CIS benchmarks list.* https://www.cisecurity.org/cis-benchmarks

Check Point. (s.f.). *Network segmentation security best practices.* https://www.checkpoint.com/cyber-hub/network-security/what-is-network-segmentation/network-segmentation-security-best-practices/

Colombia. (2009). *Ley 1273 de 2009. Función Pública*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Colombia. (2012). *Ley 1581 de 2012. Función Pública.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

COPNIA. (s.f.). *Código de ética profesional del ingeniero en Colombia.* https://www.copnia.gov.co/

Devore, J. (2023). *Active directory hardening series - Part 2 – Removing SMBv1. Microsoft Tech Community.* https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/active-directory-hardening-series---part-2-%E2%80%93-removing-smbv1/3988317

Fortinet. (s.f.). *¿Qué es una lista de control de acceso de red (ACL)?* https://www.fortinet.com/lat/resources/cyberglossary/network-access-control-list

Fortinet. (s.f.). *What is network access control (NAC)?* https://www.fortinet.com/resources/cyberglossary/what-is-network-access-control

IBM. (s.f.). *What is incident response?* https://www.ibm.com/think/topics/incident-response

Illumio. (s.f.). *¿Qué es la respuesta a incidentes? Una guía detallada para organizaciones.* https://www.illumio.com/es-mx/cybersecurity-101/incident-response

Jurado Moreano, P. J. (2015). *Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management) [Tesis de maestría, Universidad San Francisco de Quito]. Repositorio USFQ.* https://repositorio.usfq.edu.ec/handle/23000/4911

Lyon, G. F. (2009). *Nmap network scanning.* https://nmap.org/book/toc.html

Microsoft. (s.f.). *¿Qué es SIEM?* https://www.microsoft.com/es-co/security/business/security-101/what-is-siem

Ministerio de Comercio, Industria y Turismo. (2013). *Decreto 1377 de 2013. Función Pública*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Mitratech. (2021). *Uso de NIST SP 800-61 para prepararse ante el próximo incidente se seguridad de terceros.* https://mitratech.com/es-la/centro-de-recursos/blog/nist-sp-800-61/

MITRE Corporation. (s.f.). *Common vulnerabilities and exposures (CVE).* https://cve.mitre.org/

MITRE Corporation. (2024). *Mitre att&ck framework.* https://attack.mitre.org/

NIST. (2018). T*echnical guide to information security testing and assessment (NIST Special Publication 800-115). National Institute of Standards and Technology.* https://nvlpubs.nist.gov/

NIST. (2008). *Guide to general server security (NIST Special Publication 800-123). National Institute of Standards and Technology.* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf

Nmap Project. (2024). *Nmap reference guide.* https://nmap.org/book/man.html

Offensive Security. (s.f.). *Pivoting (Metasploit unleashed).* https://www.offsec.com/metasploit-unleashed/pivoting/

OpenVAS. (s.f.). *OpenVAS documentation. Greenbone Networks*. https://www.greenbone.net/

Patagonia, I. (2025). *Incident response: Cómo prepararse para responder con eficacia ante incidentes de ciberseguridad. IT Patagonia.* https://itpatagonia.com/incident-response-que-es/

Rapid7. (2024). *Metasploit framework documentation.* https://docs.rapid7.com/metasploit/

Scarfone, K., & Mell, P. (2007). *Guide to intrusion detection and prevention systems (IDPS) (NIST Special Publication 800-94). National Institute of Standards and Technology.* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf

Singer, P., & Friedman, A. (2019). *Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.* https://global.oup.com/academic/content/series/w/what-everyone-needs-to-know-wentk/?lang=en&cc=co

Sophos. (s.f.). *¿Qué es un firewall?* https://www.sophos.com/es-es/cybersecurity-explained/firewall

Sosmatic. (2025). *Qué hacer si te han hackeado: Pasos urgentes para proteger tus datos.* https://www.sosmatic.com/que-hacer-si-te-han-hackeado-pasos-urgentes-para-proteger-tus-datos/

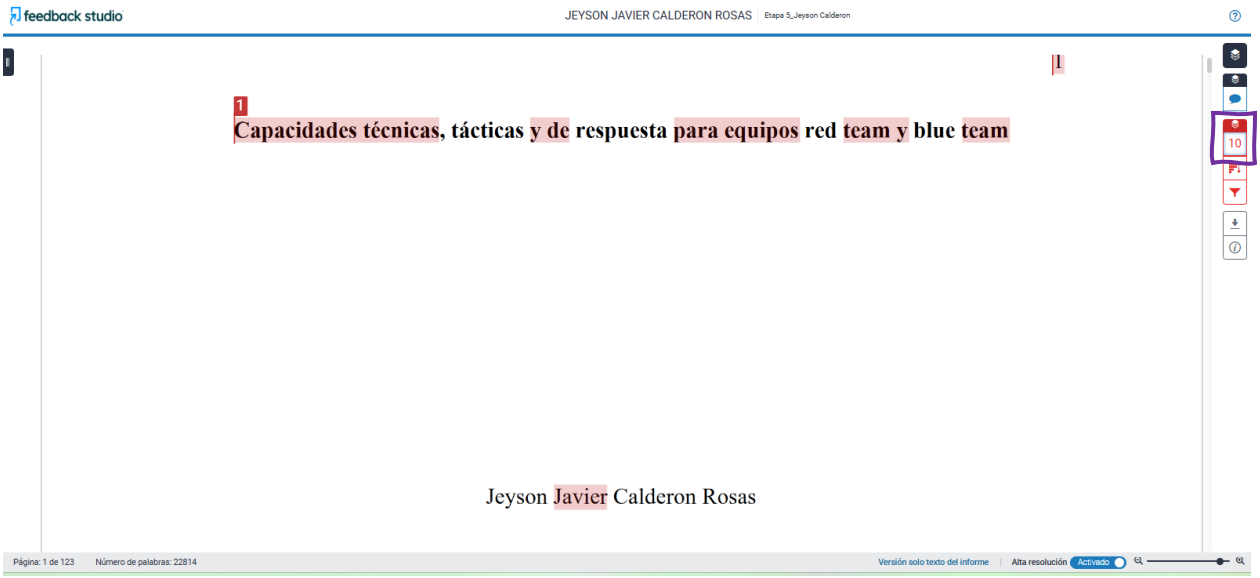
UNAD. (2025). *Anexo 2: Escenario 2 y Anexo 3: Acuerdo.* Material de curso.

UNAD. (2025). *Anexo 5: Escenario 4.* Material de curso.

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. Reporte de similitud generado por la herramienta Turnitin (Feedback Studio) correspondiente al informe final titulado "Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team", el documento obtuvo un índice de similitud del 10%, este resultado evidencia la originalidad del contenido, el adecuado uso de parafraseo técnico y el correcto manejo de fuentes bibliográficas a lo largo del informe.