Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

David Esteban Martinez Muñoz

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Resumen

En el presente informe técnico se condesan las actividades desarrolladas a lo largo de las cuatro etapas del seminario “Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team”. Durante este proceso se abordaron aspectos clave como la normativa colombiana en delitos informáticos y protección de datos, principios éticos y legales, pruebas de penetración, hardenización, contención de amenazas y el uso de entornos virtualizados para simular ataques en condiciones controladas. Se fortalecieron habilidades para identificar vulnerabilidades, ejecutar ataques controlados y aplicar medidas de defensa efectivas desde las perspectivas Red Team y Blue Team. Estos conocimientos, además de brindar una comprensión integral de la ciberseguridad ofensiva y defensiva, se convierten en una base sólida para enfrentar desafíos reales en el entorno laboral, donde la capacidad de detectar, responder y contener incidentes en tiempo real es fundamental.

***Palabras clave*:** ciberseguridad, contención, hardenización, pentesting, vulnerabilidades

Abstract

This technical report condenses the activities carried out throughout the four stages of the seminar *"*Strategic Teams in Cybersecurity: Red Team & Blue Team*"* During this process, key topics were addressed, including Colombian regulations on cybercrime and data protection, ethical and legal principles, penetration testing, system hardening, threat containment, and the use of virtualized environments to simulate attacks under controlled conditions. Skills were strengthened to identify vulnerabilities, execute controlled attacks, and implement effective defense measures from both Red Team and Blue Team perspectives. These competencies not only provide a comprehensive understanding of offensive and defensive cybersecurity, but also serve as a solid foundation for addressing real-world challenges in the workplace, where the ability to detect, respond to, and contain incidents in real time is essential.

Keywords**:** cybersecurity, containment, hardening, penetration testing, vulnerabilities

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Glosario

Adversario: Individuo o grupo con intención y capacidad para explotar vulnerabilidades y comprometer sistemas, redes o datos.

Ciberseguridad: Conjunto de prácticas, procesos y tecnologías destinadas a proteger sistemas, redes y datos frente a accesos no autorizados, daños o ataques.

CVE: Estándar internacional para identificar y describir vulnerabilidades de seguridad conocidas en software o hardware, facilitando su gestión.

Equipos Azules (Blue Team): Grupo de defensa encargado de detectar, prevenir y responder a incidentes que amenacen la seguridad de la organización.

Equipos Rojos (Red Team): Grupo que simula ataques cibernéticos para identificar vulnerabilidades y evaluar la eficacia de los controles defensivos.

Firewall: Dispositivo o software que filtra el tráfico de red según reglas de seguridad, permitiendo o bloqueando conexiones.

IDS/IPS: Sistemas diseñados para detectar (IDS) o prevenir (IPS) intrusiones y comportamientos anómalos en la red.

Pruebas de Penetración (Pentesting): Simulación controlada de ataques para identificar vulnerabilidades explotables en sistemas o redes.

Vulnerabilidad: Debilidad en un sistema, aplicación o protocolo que puede ser aprovechada para comprometer la seguridad.

TI (Tecnología de la Información): Conjunto de recursos tecnológicos usados para procesar, almacenar y gestionar información digital.

Introducción

Contar con conocimientos teóricos y prácticos actualizados que fortalezcan las habilidades y la experticia de los profesionales en ciberseguridad es una necesidad clave para enfrentar los retos del panorama actual, en el que los atacantes también se benefician de los avances tecnológicos y del uso de la inteligencia artificial para alcanzar sus objetivos maliciosos. En este contexto, las temáticas abordadas durante el seminario especializado resultan fundamentales para mejorar la preparación técnica y estratégica de los especialistas en Seguridad Informática.

Durante el seminario, se trataron contenidos esenciales que definen las funciones de los equipos Red Team y Blue Team, haciendo énfasis en su rol dentro de una estrategia de seguridad integral. También se analizó el marco legal colombiano, no solo en lo referente a la protección de datos personales, sino también en lo concerniente a la protección de la información y de los sistemas informáticos. Asimismo, se evaluaron conceptos relacionados con la actualización ética y legal que deben mantener los profesionales de ciberseguridad.

Además, se profundizó en los conceptos, fases y procedimientos de las pruebas de penetración como parte de las estrategias ofensivas controladas. En la práctica, se implementó un banco de trabajo virtualizado para ejecutar un laboratorio de pentesting, en el cual se identificó y explotó una vulnerabilidad en un sistema simulado, facilitando la aplicación de los conocimientos adquiridos en un entorno seguro.

Finalmente, se revisaron los elementos fundamentales para la contención de ataques en el marco de la labor de los equipos Blue Team, priorizando la hardenización de sistemas y comprendiendo conceptos claves como Blue Team y CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática).

Objetivos

Objetivo General

Fortalecer las competencias teóricas, prácticas y éticas mediante el análisis y la aplicación de metodologías ofensivas y defensivas, la comprensión del marco legal colombiano y la articulación efectiva de los equipos Red Team y Blue Team, con el propósito de optimizar la postura de seguridad, la toma de decisiones responsables y la capacidad de respuesta ante incidentes en entornos organizacionales.

Objetivos Específicos

Comprender los conceptos, funciones y responsabilidades de los equipos Red Team y Blue Team, así como su papel complementario dentro de una estrategia integral de ciberseguridad en las organizaciones.

Analizar el marco legal colombiano en materia de delitos informáticos y protección de datos personales, promoviendo una actuación profesional ética y conforme a las normativas vigentes.

Aplicar técnicas, herramientas y metodologías de pruebas de penetración (pentesting) en entornos virtualizados controlados, para identificar y explotar vulnerabilidades como parte de las estrategias ofensivas.

Reconocer acciones para la contención de ataques informáticos, incluyendo la hardenización de sistemas, el monitoreo continuo y la gestión coordinada desde los equipos Blue Team y CSIRT.

Etapa 1: Conceptos Equipos de Seguridad

Punto 1

A nivel del marco legal y de normatividad sobre delitos informáticos en Colombia y la protección de datos personales tenemos:

La Ley 1273 de 2009 modificó el código penal colombiano para fortalecer la protección de la información y los datos en los sistemas informáticos. Esta normativa tipifica diversos delitos cibernéticos, incluyendo el acceso abusivo y la obstaculización de sistemas informáticos, así como la interceptación, alteración y destrucción de datos. Además, sanciona el uso de software malicioso, la suplantación de sitios web y la violación de datos personales, entre otros delitos clave para la seguridad digital. Existe un agravante a nivel de las penas por los delitos informáticos cuando son afectados los sistemas del estado y financieros, como también cuando son cometidos por servidores públicos que se encuentren ejerciendo sus funciones (Policía Nacional de Colombia, s. f.).

La Ley 1581 de 2012, la cual establece el marco legal para la protección de los datos personales en Colombia, definiendo las normas que regulan su recolección, almacenamiento, uso, circulación y eliminación. Su propósito es garantizar los derechos de los ciudadanos sobre su información personal, proporcionándoles mecanismos para acceder, actualizar y corregir sus datos, asegurando así su privacidad y control sobre su uso. Además, la Superintendencia de Industria y Comercio (SIC) desempeña un rol clave en la supervisión y protección de los datos personales, previniendo abusos y malas prácticas en su tratamiento por parte de empresas o entidades que no cumplan con los principios de ética y transparencia (Función Pública, 2012).

Decreto 1377 de 2013, el cual reglamenta la Ley 1581 de 2012, estableciendo normas para el tratamiento de datos personales en Colombia. De tal manera que se define la obligatoriedad del consentimiento informado de los titulares para el uso de su información, así como las responsabilidades de quienes la gestionan. Su objetivo es garantizar los derechos de acceso, actualización, rectificación y supresión de los datos mediante la implementación de políticas claras de tratamiento de la información, las cuales deben ser desarrolladas por las entidades responsables y ajustadas a los principios de seguridad, confidencialidad y legalidad (Función Pública, 2013).

El CONPES 3995 de 2020 tiene como propósito reforzar la confianza digital y la ciberseguridad en Colombia, enfrentando los retos y riesgos derivados del avance de las tecnologías de la información y las comunicaciones (TIC). El documento plantea estrategias dirigidas a proteger la infraestructura digital, mejorar las competencias en seguridad digital de individuos, organizaciones y entidades gubernamentales, y fomentar una cultura de prevención y reacción frente a amenazas cibernéticas (Departamento Nacional de Planeación, 2020).

Una institución tan importante como el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia adoptó la Resolución 2239 de 2024, la cual actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación tanto del Ministerio como del Fondo Único de TIC. Esta resolución deroga la Resolución 448 de 2022 y establece lineamientos claros y precisos para el uso y manejo de la información, con el objetivo de gestionar riesgos en seguridad y privacidad, mitigar incidentes y garantizar el cumplimiento de la tríada de seguridad de la información: confidencialidad, integridad y disponibilidad (MinTIC, 2024).

Punto 2

El pentesting también se conoce como pruebas de penetración, donde lo que se busca es encontrar vulnerabilidades en los sistemas informáticos mediante un ataque simulado, de tal manera que las organizaciones puedan descubrir y subsanar las fallas de seguridad antes de que se materialice un incidente real de ciberseguridad. Los encargados de realizar estas pruebas se conocen como pentesters quienes abordan una metodología estructurada en diferentes etapas y utilizan diferentes herramientas especializadas como por ejemplo analizadores de tráfico, escáneres de vulnerabilidades y plataformas de explotación (IBM, s,f).

El pentesting se compone de las siguientes etapas de acuerdo con (Nuñez C, 2021):

Obtención de información inicial y precontrato: En esta fase se establece el alcance de la auditoría de seguridad y se acuerdan los términos contractuales con el cliente. Se define el objetivo del pentesting, las metodologías a utilizar y los límites que deben respetarse para garantizar que la prueba se realice de manera ética y controlada.

Además, se determinan los rangos de direcciones IP que serán analizados y el tipo de prueba a ejecutar:

Caja blanca: Se proporciona acceso total a la información del sistema, permitiendo un análisis exhaustivo.

Caja gris: Se dispone de información parcial, como direcciones IP o credenciales limitadas.

Caja negra: No se ofrece ningún detalle previo, simulando un ataque real desde la perspectiva de un atacante externo.

Para esta etapa se destaca la herramienta Maltego con el fin de recopilar información pública, ya que se basa en OSINT (Open Source Intelligence).

Enumeración: En esta fase se lleva a cabo la identificación y análisis detallado de los sistemas objetivo, recopilando información sobre las direcciones IP accesibles, puertos abiertos, servicios en ejecución y configuraciones del sistema. De tal manera que se obtiene un panorama claro de la infraestructura, con el fin de detectar posibles puntos de entrada que puedan representar vulnerabilidades.

Para lograr un mapeo completo del entorno, se utilizan herramientas especializadas como Nmap (Network Mapper), la cual permite identificar los hosts activos en la red y su sistema operativo, como también permite determinar los puertos abiertos, servicios en ejecución.

Explotación de vulnerabilidades: Una vez identificadas las vulnerabilidades en la fase de enumeración, se procede a ejecutar un plan de explotación con el objetivo de obtener acceso no autorizado a información sensible o comprometer la operatividad del sistema. Esta fase permite evaluar el impacto real de las debilidades detectadas y determinar el nivel de acceso que un atacante potencialmente puede obtener. Herramientas como Metasploit Framework se utilizan para realizar la explotación ya que permite ejecutar exploits dirigidos a vulnerabilidades conocidas, escalar privilegios y obtener acceso remoto a los sistemas que se encuentran comprometidos.

Documentación: Toda la información recopilada durante las fases previas debe ser estructurada y presentada en un informe detallado, el cual será entregado al cliente en dos formatos principales:

Informe Técnico: Dirigido a los equipos de seguridad y tecnología, donde se documentan en detalle las vulnerabilidades detectadas, los métodos de explotación utilizados y los resultados obtenidos en las pruebas de penetración. También incluye recomendaciones específicas para mitigar los riesgos identificados.

Resumen Ejecutivo: Orientado a la alta dirección, emplea un lenguaje claro y comprensible para exponer los principales riesgos de seguridad detectados. Su objetivo es facilitar la toma de decisiones estratégicas para fortalecer la ciberseguridad de la organización.

Para optimizar la documentación de los hallazgos, se emplean herramientas como Dradis, la cual mediante su enfoque colaborativo permite centralizar, organizar y presentar los resultados de manera clara y concisa.

Punto 3

Las herramientas de ciberseguridad son elementos esenciales para alcanzar los objetivos estratégicos relacionados con la protección de las infraestructuras tecnologías y de la información ya que apoyan en el proceso de identificación oportuna de amenazas, la contención eficaz de incidentes de seguridad y la mitigación de riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información. A continuación, se describen algunas herramientas y servicios en línea.

Metasploit: Es una de las herramientas más utilizadas en el ámbito de la ciberseguridad, especialmente en la realización de pruebas de penetración y la ejecución de exploits. Se basa en un framerwork de código abierto que se beneficia de los aportes y desarrollos de una comunidad activa de profesionales en seguridad y desarrolladores, lo que permite su actualización constante y la incorporación de nuevas técnicas, vulnerabilidades y módulos personalizados. La arquitectura flexible de Metasploit facilita la creación, prueba y automatización de exploits en entornos controlados. La herramienta se puede utilizar a través de una interfaz de línea de comandos conocida como MSFConsole, o mediante una interfaz gráfica llamada Armitage, la cual facilita su uso para usuarios menos experimentados (Campus Internacional de Ciberseguridad, 2024).

Nmap: Es una herramienta de código abierto utilizada ampliamente en ciberseguridad para la exploración, mapeo de redes y realización de auditorías de seguridad. Su funcionamiento se basa en el envío de paquetes especialmente diseñados para analizar la infraestructura de red, permitiendo identificar de manera eficiente los dispositivos activos, los servicios que ofrecen, los puertos abiertos y, en muchos casos, el sistema operativo que utilizan, junto con detalles de su versión. De tal manera que a través de esta exploración se puede detectar vulnerabilidades potenciales que pueden ser aprovechadas por los adversarios, lo que permite tomar acciones preventivas y correctivas (Nmap, s. f.).

OpenVAS (Open Vulnerability Assessment System): Es una herramienta de código abierto que permite identificar y evaluar vulnerabilidades, se estructura como un conjunto de servicios y componentes que pueden ser utilizados tanto de forma independiente como integrados en plataformas más amplias de gestión de seguridad, lo que le brinda gran flexibilidad para distintos entornos de análisis. Adicionalmente OpenVas se puede usar por medio de Metasploit, potenciando las pruebas de explotación de vulnerabilidades. Como sucede con Metasploit, OpenVas cuenta con una línea de comandos (OpenVAS CLI) y con una interfaz web llamada Greenbone Security (ESET, s. f.).

ExploitDB: Es un repositorio público en línea que recopila exploits documentados, permitiendo a profesionales de la seguridad e investigadores acceder a ejemplos prácticos de vulnerabilidades descubiertas. Esta plataforma facilita la realización de pruebas de penetración y análisis técnicos orientados a comprender y evaluar las debilidades en materia de seguridad informática (Offensive Security, 2025).

CVE (Common Vulnerabilities and Exposures): Es un catálogo publico donde se han recopilado y clasificado vulnerabilidades de seguridad informática, donde las vulnerabilidades

reciben un código único CVE, a partir del cual se puede realizar el seguimiento y análisis correspondiente. CVE ha contribuido con el fortalecimiento de la capacidad prevenir y mitigar las vulnerabilidades de seguridad. Este sistema lo mantiene la corporación MITRE (IBM, s. f.).

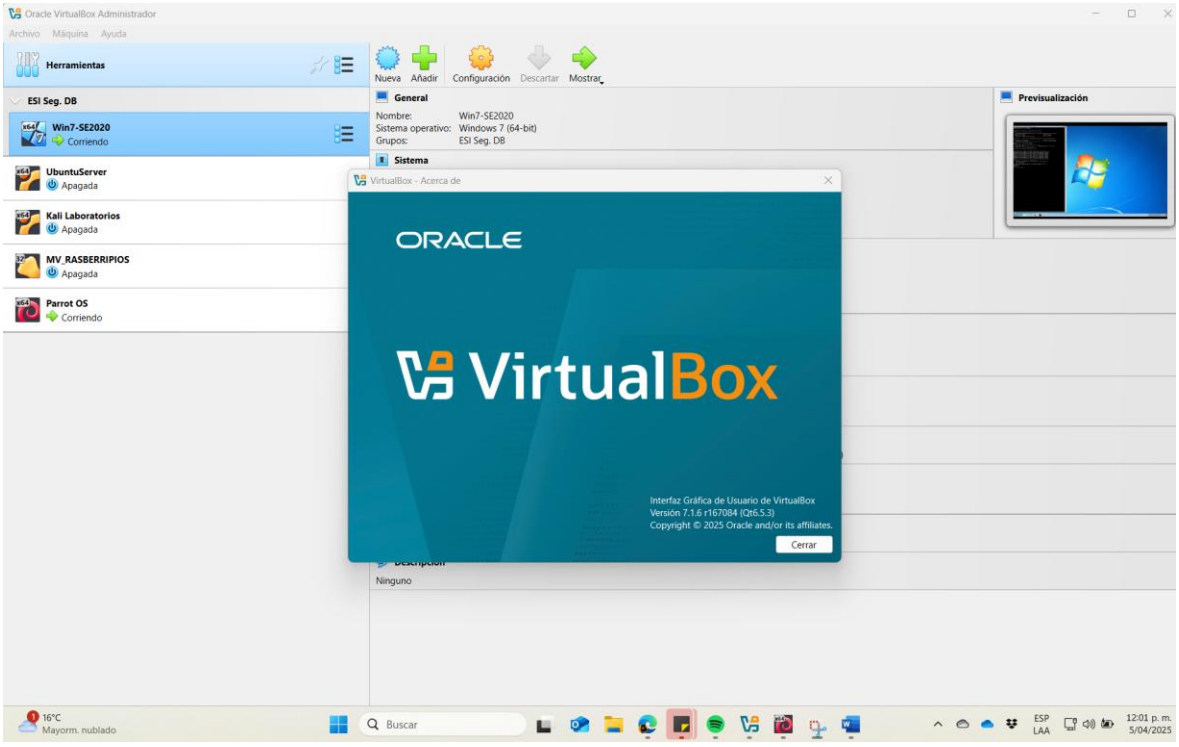
Punto 4

En este punto se llevó a cabo la configuración del 'banco de trabajo', conforme a los requerimientos establecidos por CyberFort Technologies, considerando la importancia de realizar pruebas y análisis de seguridad en entornos controlados, sin afectar los ambientes productivos.

Por lo tanto, en primer lugar, se realizó la instalación de la última versión publicada en el sitio web de Virtual Box (7.1.16) como se muestra a continuación.

Figura 1

Versión instalada de VirtualBox



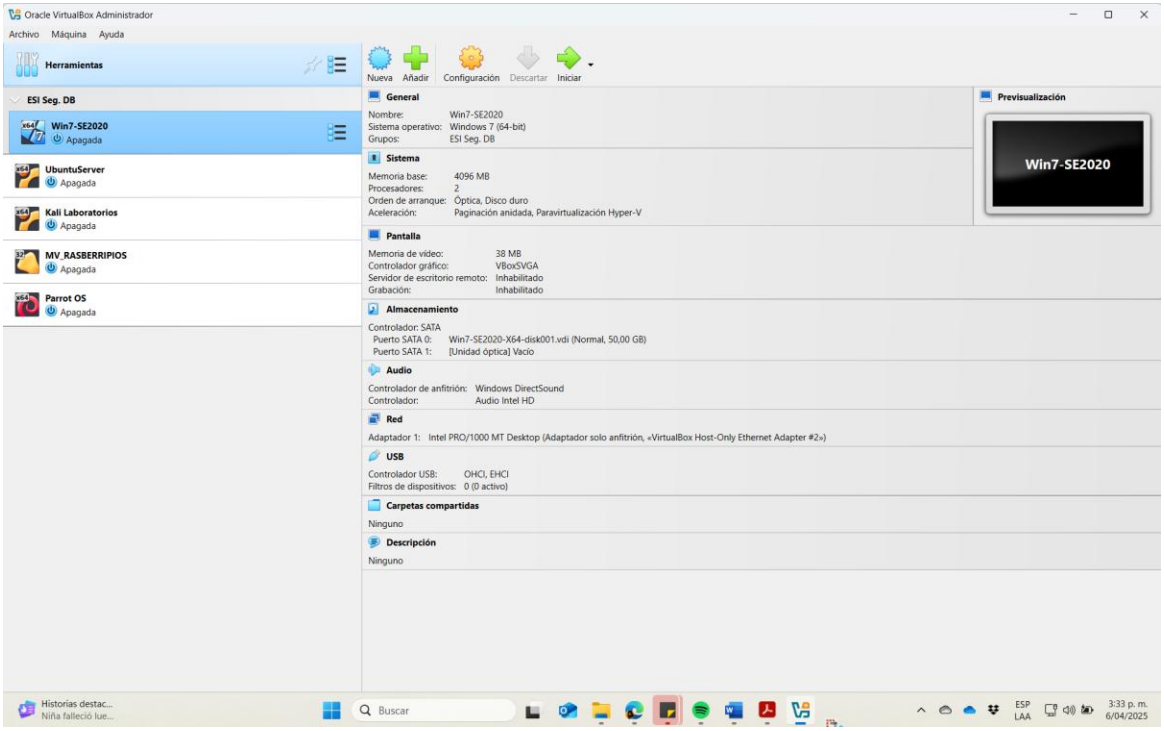
Fuente. Autoría propia.

Una vez se instaló VirtualBox en la última versión, se importaron las imágenes con extensión *.ova de las máquinas con el sistema operativos Windows 7 y Parrot, las cuales se encuentran en la carpeta compartida de OneDrive: RedTeam&BlueTeam2024.

La máquina con el sistema operativo Windows 7 cuenta con cuatro (4) GB de memoria RAM y dos (2) núcleos de CPU, mientras que la máquina Parrot cuenta con ocho (8) GB de memoria RAM y ocho (8) núcleos de CPU.

Figura 2

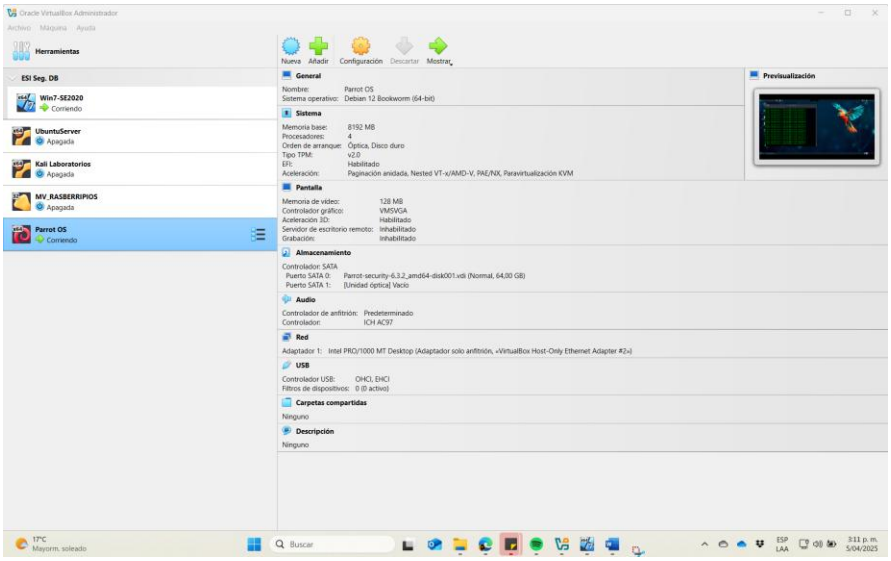
Características de la máquina Windows 7



Fuente. Autoría propia.

Figura 3

Características de la máquina Parrot

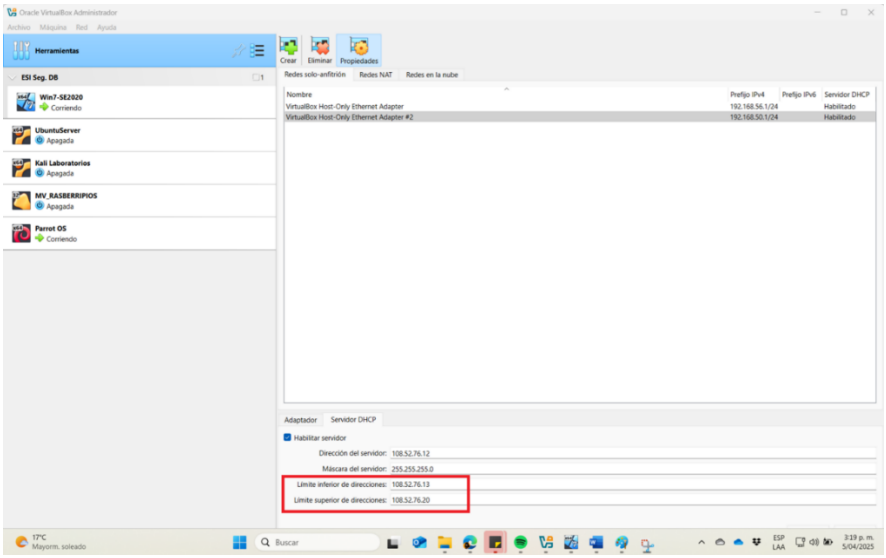


Fuente. Autoría propia.

En VirtualBox se realizó la configuración correspondiente para contar con la asignación de direcciones IP a través de DCHP.

Figura 4

Configuración DCHP desde VirtualBox

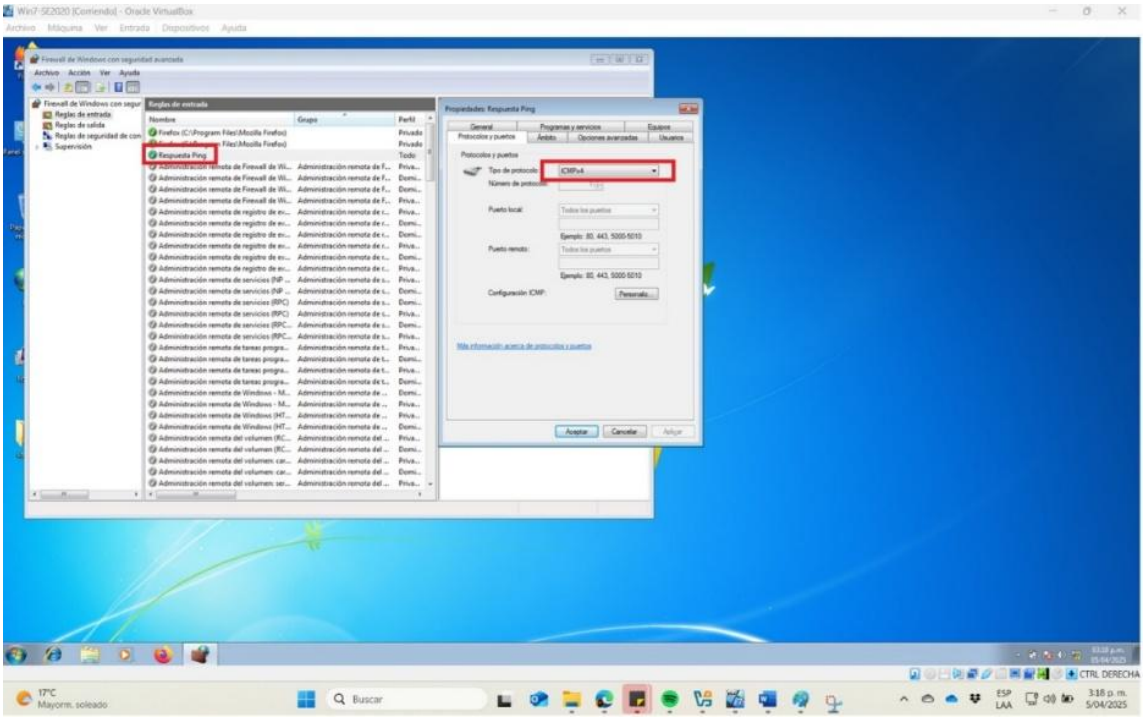


Fuente. Autoría propia.

Por lo tanto, la máquina Windows 7 recibió la IP: 108.52.76.17 y la máquina Parrot la dirección IP: 108.52.76.18. Se verificó la comunicación entre las dos máquinas mediante el comando ping (protocolo ICMP). Es importante tener en cuenta que en la máquina Windows 7 se creó una regla de entrada en el firewall para permitir el ping.

Figura 5

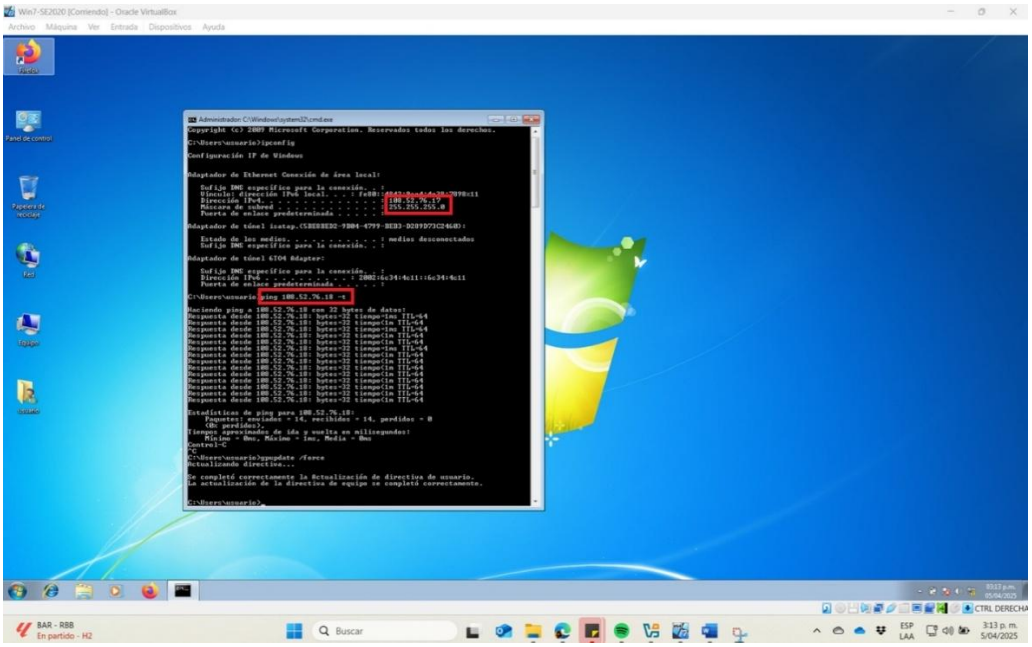
Configuración para permitir ping en la máquina Windows 7



Fuente. Autoría propia.

Figura 6

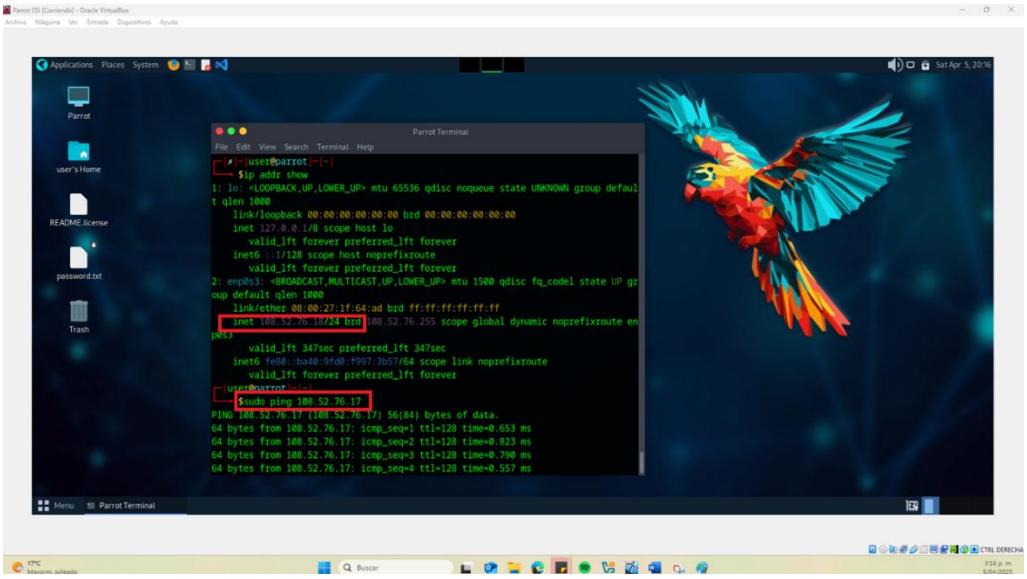
IP asignada y ping a la máquina Parrot desde Windows 7



Fuente. Autoría propia.

Figura 7

IP asignada y ping a la máquina Windows 7 desde Parrot



Fuente. Autoría propia.

Etapa 2: Actualización Ética y Legal

Punto 1

Es fundamental destacar que en el anexo 2 se presenta una primera señal de alerta significativa, relacionada con el despido del abogado que elaboró el contrato de reclutamiento. Según el documento, dicho profesional fue removido de su cargo por haber descubierto procesos ilícitos dentro de la organización, lo cual sugiere un posible acto de retaliación por parte de la empresa. Esta situación pone en evidencia serios cuestionamientos sobre el comportamiento ético y la transparencia institucional de CyberFort Technologies.

Adicionalmente, se evidencia una falta grave en la gestión de la alta dirección, al haber omitido la revisión del contenido contractual y no haber solicitado el acompañamiento del área jurídica para garantizar la validez legal y técnica del documento. De acuerdo con (ARFASA Abogados, 2024), es vital contar con una revisión legal de los contratos para prevenir riesgos de tipo jurídico, operacional y reputacional, adicional a contingencias legales con costos económicos elevados.

Una vez analizado el anexo 2, a continuación, se encuentran los resultados de la revisión del anexo 3 (acuerdo de confidencialidad) a nivel de procesos ilegales y que no van alineados con la ética profesional y empresarial. Se señalaron en negrita las irregularidades detectadas.

Primera clausula: Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, **autoridades legales**, asesores o cualquier persona relacionada con ella, la información confidencial o **sobre procesos ilegales dentro de CyberFort Technologies** no podrán ser divulgados.

Análisis: El hecho de que exista una cláusula que no permita reportar a las autoridades del país sobre procesos ilegales, va en contravía de la legislación del país frente a lo relacionado a delitos informáticos, lo cual puede generar implicaciones legales tanto para la persona que está firmando el acuerdo como para la misma empresa. De cumplir dicha cláusula la persona puede verse involucrada en obstruir la justicia y agravar las penas de acuerdo con la Ley 1273 de 2009. Como profesionales y especialistas en seguridad informática es un deber reportar este tipo de acciones a las autoridades.

Segunda clausula. A nivel de la información confidencial en el punto dos se tiene: Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, **datos secretos como "datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos"**.

Análisis: El hecho de que se incluyan como información confidencial datos obtenidos mediante actividades comúnmente conocidas como "chuzadas", interceptación de información y acceso abusivo a sistemas informáticos, nos da una idea del tipo de empresa con la que se está tratando, la cual reconoce la ejecución de actividades ilegales, sino que además pretende protegerlas contractualmente. Como especialistas en ciberseguridad está situación se debería reportar inmediatamente a las autoridades ya que estas actividades se constituyen como delitos de acuerdo con la Ley 1273 de 2009. Como se mencionó en el análisis anterior el no denunciar estas prácticas delictivas va en contravía de los principios éticos y legales a nivel profesional y derivan en complicidad, la cual es castigada con severidad por la ley.

Cuarta clausula: Se encuentran varios puntos que obligan a la parte receptora a faltar a la ley, la ética y el rigor profesional, inclusive a asumir responsabilidades legales que podrían no corresponderle.

Punto 3: **No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.**

Punto 4: **Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas**.

Punto 7: **Responder por el mal uso que le den sus representantes a la información confidencial.**

Punto 8: **Responder ante las autoridades competentes como responsable en caso de que la información se encuentre en su poder dentro de un proceso de allanamiento**.

Punto 9: **La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte de CyberFort Technologies**.

Análisis: Los puntos mencionados de la cláusula 4, van en contravía de los principios legales y éticos, pasando por las normas jurídicas establecidas en Colombia, ya que la empresa busca evitar la denuncia a las autoridades sobre las actividades delictivas y muy graves como lo es el espionaje y la apropiación de información de terceros, además de que acepta que se realizan procesos ilegales para obtener la información. Adicionalmente, se pretende trasladar la responsabilidad legal de estos hechos a la persona contratada, obligándola a asumir consecuencias que no le corresponden, lo que representa una vulneración de sus derechos fundamentales y una clara falta de ética y de principios por parte de la empresa.

Quinta clausula: Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora: **Mantener la reserva de la información confidencial hasta tanto**.

Análisis: Si bien no se observa algún proceso o práctica ilegal, es muy evidente la falta de revisión del acuerdo, principalmente a nivel de la coherencia y del contenido de la redacción. Esta cláusula es ambigua y no se encuentra detallado el momento cuando vencería.

Octava clausula: En esta cláusula nuevamente se presenta una irregularidad con consecuencias legales y económicas para el receptor, específicamente en este apartado: **En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies**.

Análisis: Como se ha evidenciado en el análisis de cláusulas anteriores, la empresa busca eludir de forma directa su responsabilidad legal, transfiriendo de manera indebida dichas obligaciones a la persona que será contratada (receptor). Además, le impone una carga al receptor frente a la defensa jurídica que se requiriera. El accionar de la empresa es abusivo y por fuera de las normas que rigen el derecho en el país.

Para finalizar hay que dejar muy claro que la empresa CyberFort Technologies, debe ser objeto de investigación por parte de las autoridades, dado que las cláusulas contenidas en el acuerdo evidencian posibles conductas que se pueden configurar delitos como la omisión de denuncia, el encubrimiento de actividades ilícitas y la transferencia indebida de responsabilidades penales.

Punto 2

Teniendo en cuenta a lo descrito en la Ley 1273 de 2009 (Función Pública, 2009) y una vez realizado el respectivo análisis del acuerdo de confidencialidad entre la parte reveladora

(CyberFort Technologies) y la parte receptora (Estudiante UNAD), se están vulnerando los siguientes artículos a partir de las siguientes conductas que se tipifican como delitos.

Acceso abusivo a un sistema informático (Artículo 269A): La empresa presuntamente realiza está practica de acuerdo con la cláusula 2, lo que implica un acceso sin la autorización del titular legitimo. De tal manera que la empresa es objeto de sanciones legales y de penas de prisión para las personas involucradas que pueden ir de los cuarenta y ocho (48) a los noventa y seis meses, como también multas que pueden llegar a los 1000 salarios mínimos.

Interceptación de datos informáticos (Articulo 269C): La empresa presuntamente realiza esta práctica de acuerdo con lo expresando en las cláusulas 2 y 4, lo que se constituye en un delito y que se encuentra por fuera de la ética profesional y laboral. Este delito puede acarrear penas que van de los treinta y seis (36) a los setenta y dos (72) meses de prisión.

Violación de datos personales (Articulo 269F): La empresa presuntamente realiza esta práctica de acuerdo con las cláusulas 2 y 4 como se mencionó anteriormente, este accionar también cuenta con penas que van de los cuarenta y ocho (48) a los noventa y seis (96) meses, adicional a las multas que llegan hasta los 1000 salarios mínimos.

Cabe resaltar que, según lo establecido en la Ley 1273 de 2009, podrían configurarse agravantes penales frente al comportamiento de la empresa, ya que después de haber analizado el acuerdo contractual, presuntamente existe la posibilidad de causar perjuicios a terceros buscando un beneficio económico de manera indebida. El acuerdo de confidencialidad genera una alerta, ya que busca eximir a la empresa de cualquier responsabilidad legal, trasladando todas las implicaciones jurídicas y eventuales consecuencias penales a la persona que suscribe el contrato. Esta acción contraviene principios esenciales del derecho, así como valores éticos y morales propios del ejercicio profesional y con un mayor peso a nivel de la ciberseguridad. Prácticas

como estas comprometen la integridad de quienes se especializaron en el campo de la seguridad informática, debido a que pretenden encubrir posibles actos delictivos y responsabilizar a terceros de las consecuencias. Adicionalmente, en el contexto colombiano, existe un deber legal de reportar cualquier delito del que se tenga conocimiento, de acuerdo con el artículo 67 de la Ley 906 de 2004 (Secretaría del Senado, 2004) y de acuerdo con la Constitución Política de Colombia en el artículo 33 (Secretaría del Senado, 1991) nadie está obligado a declarar contra sí mismo.

Punto 3

Tras revisar detenidamente el acuerdo y evidenciar presuntas prácticas contrarias a la ética profesional y a la legalidad por parte de la empresa CyberFort Technologies, manifiesto de manera categórica mi decisión de rechazar la oferta presentada. Como experto en ciberseguridad, ingeniero de sistemas registrado ante el Consejo Profesional Nacional de Ingeniería (COPNIA), y como persona con principios, considero que dicha propuesta vulnera profundamente mi ética personal y profesional. Ningún salario, por muy elevado o competitivo que sea, justifica comprometer mi integridad, mi tranquilidad y mis valores, ni mucho menos arriesgarme a incurrir en conductas que puedan configurar delitos penalizados por la legislación colombiana.

De acuerdo con el Código de Ética Profesional para el ejercicio de la ingeniería y sus profesiones auxiliares, publicado por (COPNIA, 2003), incurrir en delitos en el marco de una relación contractual podría conllevar sanciones disciplinarias severas, incluyendo la cancelación de la matrícula profesional por faltas gravísimas. Por ello, rechazo de forma rotunda cualquier participación en actividades que puedan poner en riesgo mi ejercicio profesional, mi libertad y mi reputación.

Punto 4

De acuerdo con el anexo 7, la empresa CyberFort Technologies incurrió en prácticas fuera de la ética durante la auditoría de seguridad que realizó en sistemas gubernamentales. Lo critico de este incidente es que, además de la vulneración ética, los expertos de esta empresa abusaron del acceso privilegiado otorgado durante la auditoría para incurrir en ciber espionaje, accediendo a documentos clasificados que involucraban temas de vital importancia para el estado que contrató a la empresa. Este tipo de prácticas representa una grave violación de la confianza depositada en la empresa por parte del gobierno, comprometiendo no solo la seguridad de los sistemas auditados, sino también la integridad de la información sensible y la soberanía del estado. En Colombia, este tipo de actividades serían consideradas delitos tipificados en la Ley 1273 de 2009, que regula los delitos informáticos y de ciberseguridad.

Para evitar que empresas de ciberseguridad accedan de manera indebida a información confidencial, es esencial establecer medidas de supervisión rigurosa en el proceso de auditoría. Estas medidas incluyen la redacción de contratos claros que especifiquen los límites exactos del acceso a la información sensible, la implementación de cláusulas de confidencialidad estrictas y el monitoreo constante de todas las actividades realizadas durante el análisis forense. Además, se debe garantizar que solo el personal autorizado tenga acceso a los sistemas sensibles y que dicho acceso quede registrado y auditado en todo momento. También es importante dentro de las buenas prácticas que se deben ejercer durante el ejercicio de una auditoria, la formación continua de los auditores a nivel de las políticas de confidencialidad y el uso de herramientas que briden seguridad para la protección y el manejo de la información, así como también gestionar los procesos de destrucción segura de la información una vez finalice el proceso de autoría (Auditool, 2024).

Punto 5

Casos como el presentado en el anexo 7 no están alejados de la realidad y reflejan la necesidad urgente de establecer mecanismos estrictos de supervisión y control dentro de las empresas de ciberseguridad. Para evitar este tipo de incidentes, es fundamental que los empleados cumplan rigurosamente con las políticas internas, tanto en términos éticos como en el uso adecuado de herramientas tecnológicas.

Deben existir controles de acceso bien definidos y registros detallados (logs) de auditoría que permitan rastrear cualquier acción realizada sobre los sistemas y datos sensibles. Estos mecanismos deben garantizar que los expertos solo accedan a la información necesaria y dentro del alcance autorizado de su labor, sin desviarse de los contextos previamente establecidos.

Asimismo, las organizaciones deben implementar monitoreo constante sobre la labor de los auditores, bajo la supervisión de áreas clave como Seguridad de la Información, Riesgo Operativo o Cumplimiento, según la estructura de la empresa. Este control cruzado ayuda a detectar comportamientos anómalos o posibles desviaciones éticas antes de que se conviertan en incidentes mayores.

Es indispensable también que los empleados conozcan en profundidad los códigos de ética institucional y participen regularmente en programas de capacitación que refuercen su compromiso con la integridad profesional. Estas capacitaciones deben incluir ejemplos reales, actualizarse con frecuencia y destacar claramente las consecuencias disciplinarias, legales y reputacionales a las que podrían enfrentarse en caso de incurrir en conductas indebidas.

Punto 6

En primera instancia, los gobiernos y organizaciones deben activar los mecanismos judiciales pertinentes para que las autoridades competentes investiguen y sancionen a los

responsables de los actos delictivos cometidos por la empresa de ciberseguridad. Esto debe incluir una evaluación conjunta con las entidades encargadas de la seguridad nacional, con el fin de determinar el alcance e impacto de los actos de ciber espionaje sobre los intereses estratégicos del país.

A partir de este análisis, deben implementarse medidas de mitigación del riesgo, incluyendo la participación de auditorías externas independientes, que puedan ofrecer una evaluación objetiva del incidente y de los controles internos fallidos. Con base en estos hallazgos, se deben aplicar correctivos estructurales que impidan que situaciones similares vuelvan a ocurrir o escalen a escenarios más complejos.

Además, es fundamental revisar y fortalecer los procedimientos y políticas de contratación y supervisión, asegurando que incluyan cláusulas claras sobre la ética profesional, el uso responsable de herramientas forenses y el respeto por la privacidad de la información. Estos nuevos lineamientos deben estar alineados con el cumplimiento de la triada de la seguridad de la información (confidencialidad, integridad y disponibilidad), así como con controles estrictos para su verificación continua. El gobierno debe comunicar de manera clara y transparente a la ciudadanía las acciones emprendidas, reafirmando su compromiso con la ciberseguridad nacional y la protección de los datos e infraestructuras tecnológicas vitales para el país.

Etapa 3: Ejecución Pruebas de Intrusión

Punto 1

Para desarrollar la actividad, fue necesario comprender en mayor profundidad el rol de los equipos Red Team, conformados por profesionales y expertos en ciberseguridad que llevan a cabo ejercicios de hacking ético. Estos equipos simulan ataques reales con el objetivo de ayudar a las organizaciones a identificar vulnerabilidades que podrían pasar desapercibidas para las

áreas de TI. A partir de estos hallazgos, las organizaciones pueden implementar acciones correctivas y preventivas que minimicen el riesgo, reduciendo así la probabilidad de que se materialicen incidentes de ciberseguridad provocados por adversarios (IBM, 2024).

A nivel de las herramientas necesarias para realizar el laboratorio propuesto en el Anexo 4 – Escenario 3) y teniendo en cuenta las etapas del pentesting se tiene lo siguiente:

Obtención de información inicial y precontrato:

Para esta fase, se toma como referencia el Anexo 4 – Escenario 3, donde se plantea un incidente de seguridad que debe ser abordado por el equipo Red Team. El objetivo es identificar la causa de una fuga de información detectada en un equipo con sistema operativo Windows 7, el cual tiene instalada una aplicación vulnerable que, como se analizará más adelante, constituye una de las fallas de seguridad que propiciaron el evento y la escalación de privilegios. Para el desarrollo de la actividad, se cuenta con la autorización formal de la organización, así como con una copia forense de la máquina afectada, suministrada por el equipo especializado en análisis forense.

Enumeración:

Para esta fase se inicia con el uso del banco de trabajo previamente configurado, el cual se compone de la máquina afectada (Windows 7) con la IP 108.52.76.17 y la máquina con el sistema operativo (Parrot) con la IP 108.52.76.18. Es importante tener en cuenta que se debe actualizar los repositorios del sistema operativo Parrot, ya que de no hacer este proceso herramientas como Metasploit pueden fallar en los procesos requeridos.

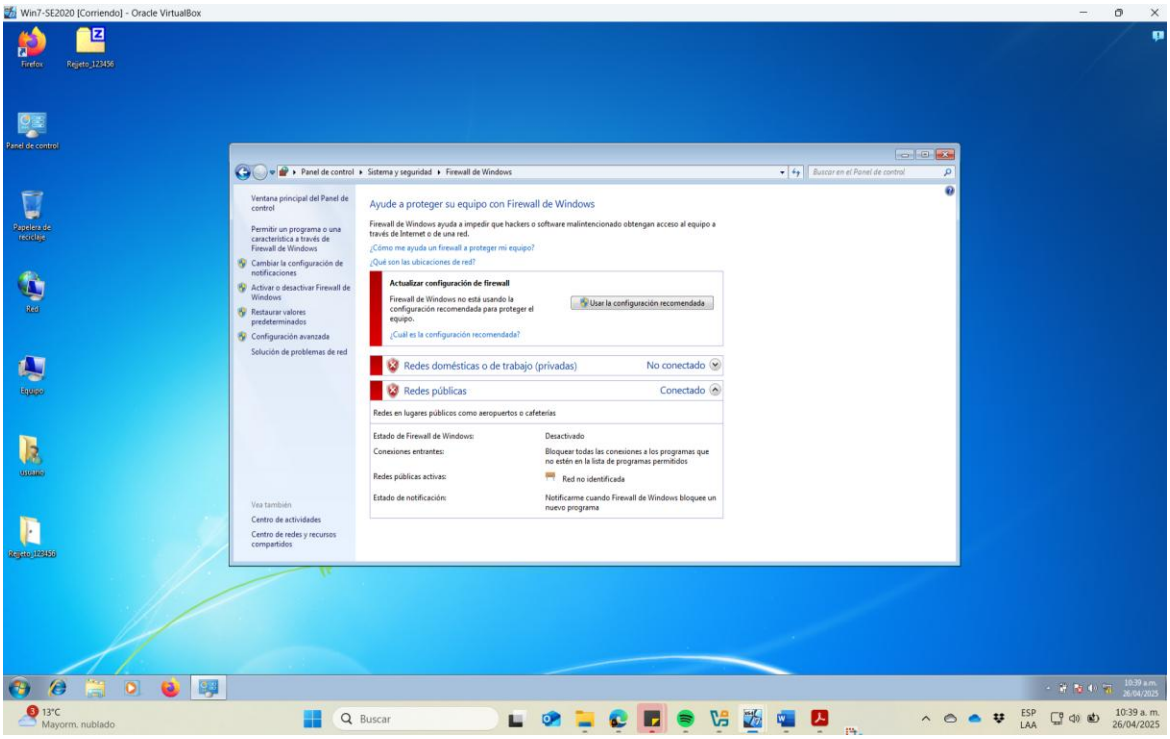
Esta fase es conocida por las tareas que se realizan para identificar información en la máquina afectada sobre los puertos, servicios y protocolos que se encuentran en uso, de tal manera que permitan obtener datos vitales para conocer y mapear los posibles vectores de

ataque. Desde la máquina Parrot se utilizó la herramienta NMAP realizando un escaneo exhaustivo de puertos y servicios abiertos, lo que proporcionó una visión clara de la infraestructura expuesta y facilitó la identificación de vulnerabilidades potenciales.

Para efectos del análisis fue necesario desactivar el firewall de la máquina Windows 7 como se observa a continuación.

Figura 8

Firewall desactivado en la máquina Windows 7



Fuente. Autoría propia.

Se ejecutó el comando: nmap – sS – A -sC -sV -p- --min rate 5000 108.52.76.17, a partir del cual se obtuvo la información requerida sobre los puertos abiertos, los servicios que se encuentran corriendo y las versiones de estos. En la siguiente tabla se encuentran relacionados con mayor detalle:

Tabla 1

Identificación de puertos y servicios abiertos con Nmap

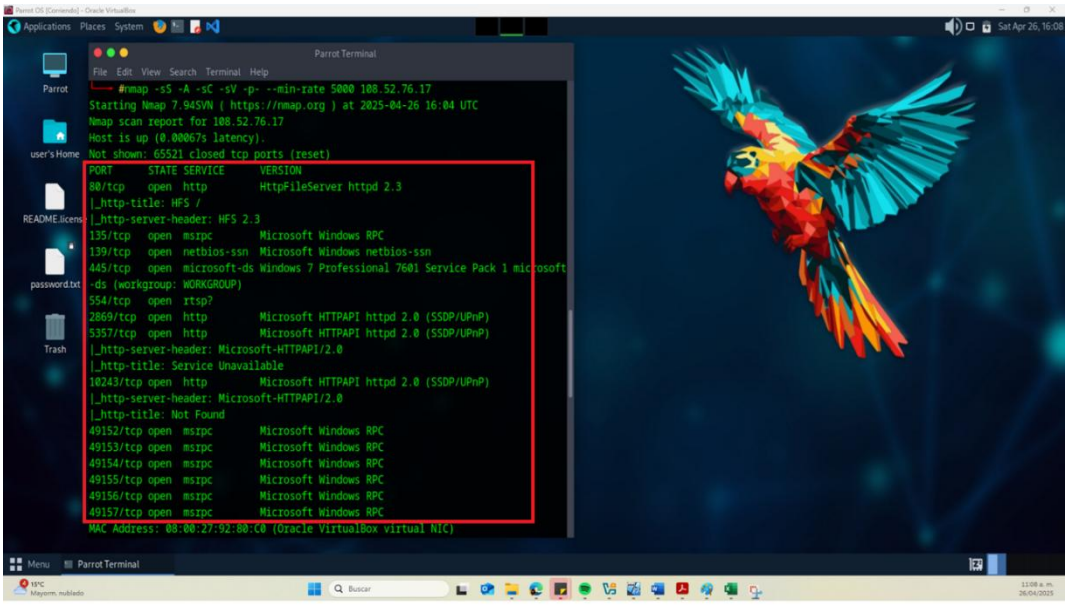
Puerto	Estado	Servicio	Versión
80 /tcp	open	http	HttpFileServer httpd 2.3
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Windows 7 Professional 7601 Service Pack 1
554/tcp	open	rtsp?	(Versión no identificada claramente)
2869/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp	open	msrpc	Microsoft Windows RPC
49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	msrpc	Microsoft Windows RPC
49156/tcp	open	msrpc	Microsoft Windows RPC
49157/tcp	open	msrpc	Microsoft Windows RPC

Fuente. Autoría propia

A continuación, se pueden observar los datos obtenidos desde la máquina Parrot, incluyendo los datos del sistema operativo, nombre de la máquina y grupo de trabajo.

Figura 9

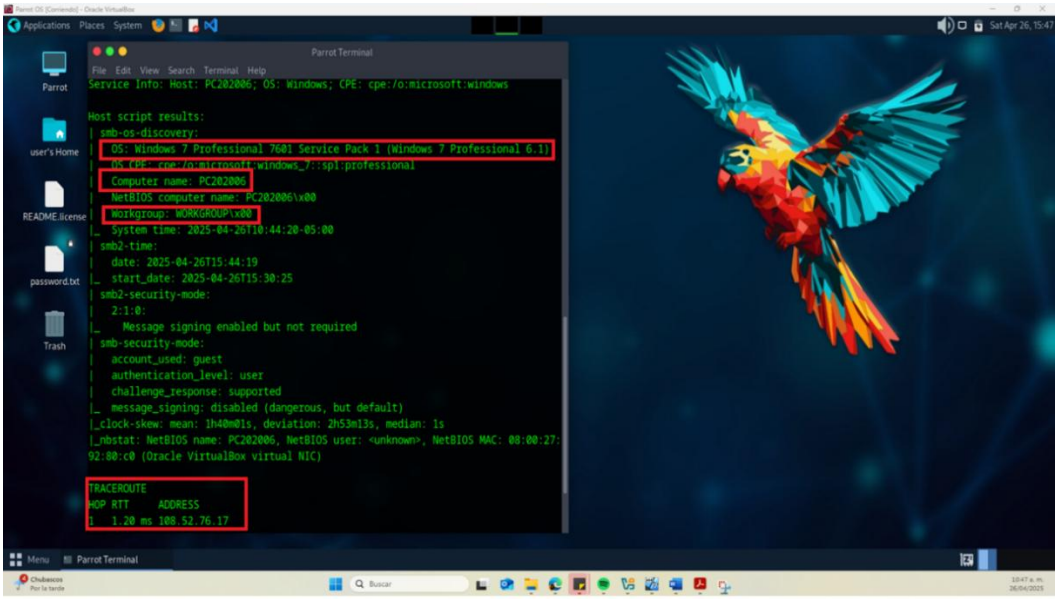
Resultados obtenidos con NMAP parte 1



Fuente. Autoría propia.

Figura 10

Resultados obtenidos con NMAP parte 2



Fuente. Autoría propia.

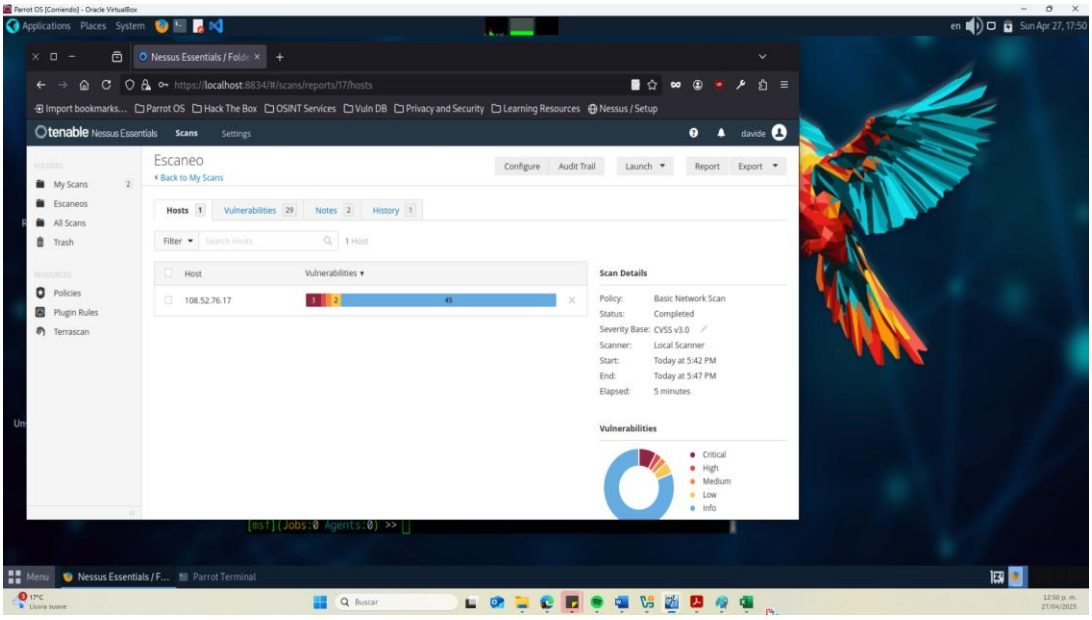
Al ejecutar este comando es importante destacar que NMAP nos arroja códigos CVE Una vez que se identifican estos códigos CVE, es fundamental realizar la consulta en sitios como CVE o INCIBE para obtener más detalles sobre la naturaleza de la vulnerabilidad, las recomendaciones de mitigación y, en algunos casos, los parches de seguridad que pueden aplicarse para corregir el problema.

Es importante tener en cuenta que, para llevar a cabo un análisis exhaustivo y efectivo, los profesionales de ciberseguridad deben apoyarse en una variedad de herramientas especializadas. Estas herramientas no solo permiten identificar vulnerabilidades, sino también evaluar el riesgo asociado a cada una de ellas y sugerir soluciones adecuadas. En el contexto de la investigación abordada por el equipo Red Team, una herramienta destacada es Nessus. Esta herramienta se destaca por su capacidad de identificar y evaluar vulnerabilidades en sistemas, redes y aplicaciones. Su principal función es realizar escaneos detallados que detectan una amplia gama de problemas, como por ejemplo inconvenientes de configuración en sistemas operativos, software desactualizado o la falta de parches de seguridad (Tenable, s. f.).

Al ejecutar el escaneo por medio de Nessus se identificaron veintinueve (29) vulnerabilidades, pero especialmente una que apunta a la aplicación Rejetto HTTP File Server (HFS), para lo cual se debe tener en cuenta el código CVE-2024-23692.

Figura 11

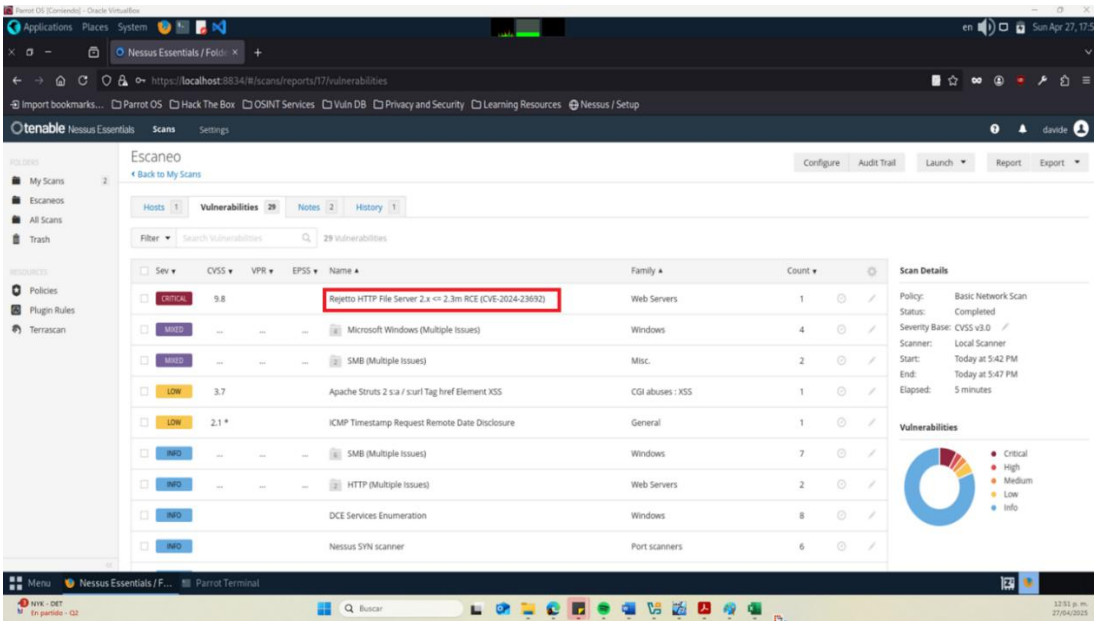
Vulnerabilidades identificadas con Nessus



Fuente. Autoría propia.

Figura 12

Vulnerabilidad critica identificada con Nessus



Fuente. Autoría propia.

En el punto número 3 de la actividad se aborda con más detalle las vulnerabilidades de seguridad asociadas a los códigos CVE-2007-6750, CVE-2017-0143 y CVE-2024-23692.

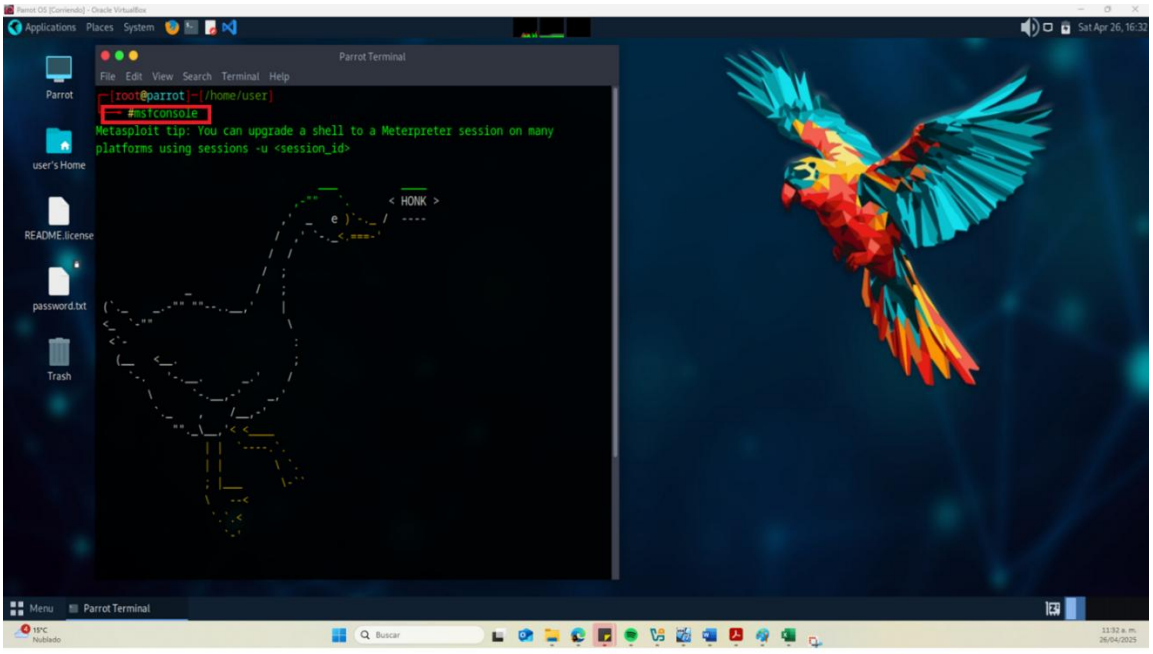
Explotación de vulnerabilidades:

Una vez con el contexto claro del escenario y se ha realizado el análisis correspondiente en la fase previa, con todos estos datos se procede a utilizar herramientas para explotar las vulnerabilidades detectadas, a través de Metasploit Framework.

A través del comando msfconsole se procedió a iniciar la explotación de vulnerabilidades.

Figura 13

Ejecución de Metasploit desde la máquina Parrot



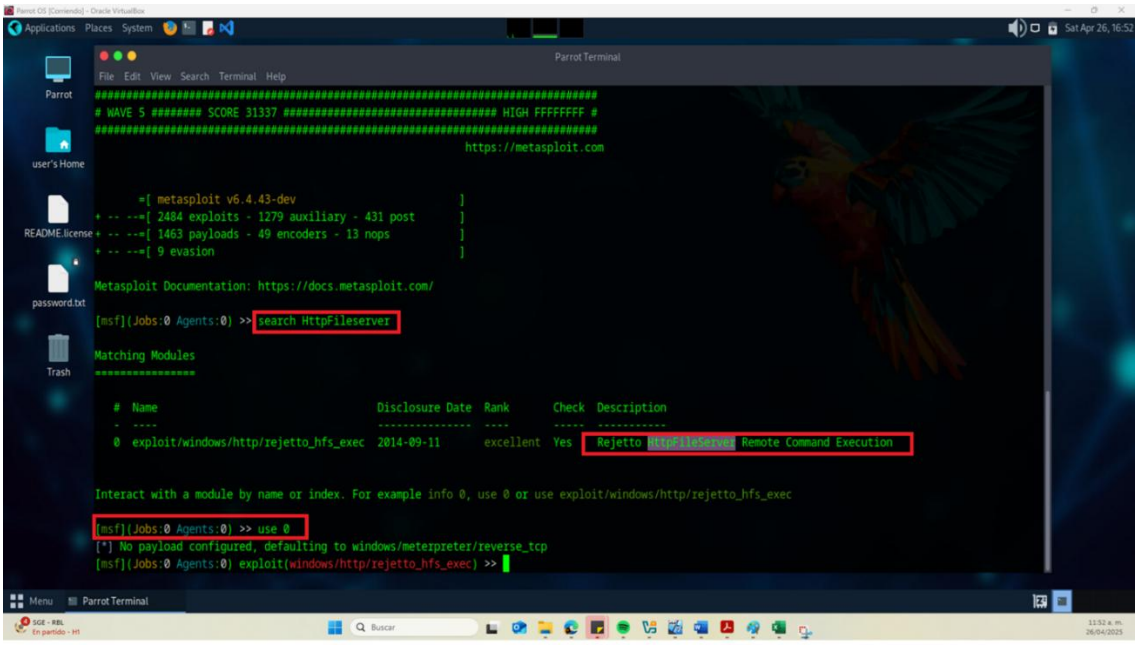
Fuente. Autoría propia.

Considerando la vulnerabilidad detectada en la aplicación Rejetto HTTP File Server (HFS), se utilizó el comando search HttpFileServer en Metasploit, lo que permitió identificar varios módulos de explotación disponibles. Entre ellos, sobresalió el módulo

exploit/windows/http/rejetto_hfs_exec, el cual está específicamente diseñado para explotar una vulnerabilidad de ejecución remota de código (RCE) en versiones afectadas de HFS. Este exploit posibilita la ejecución de comandos arbitrarios en el sistema objetivo a través de solicitudes HTTP modificadas, facilitando así el acceso inicial a la máquina comprometida.

Figura 14

Búsqueda y ejecución del módulo en Metasploit



Fuente. Autoría propia.

Posteriormente, se procedió a verificar los parámetros necesarios para la ejecución del exploit a través del comando show options. Fue indispensable configurar dos valores clave: RHOST y LHOST. En cuanto al payload se dejó por defecto.

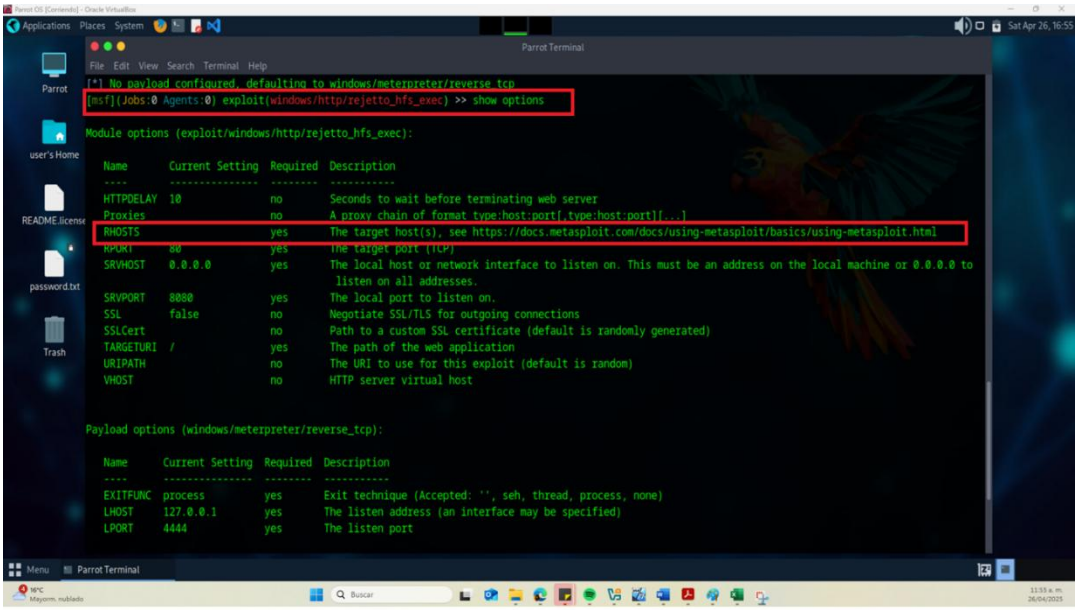
RHOST (Remote Host) se asignó con la dirección IP 108.52.76.17, correspondiente a la máquina objetivo Windows 7 en la que se detectó la vulnerabilidad.

LHOST (Local Host) se configuró con la dirección IP 108.52.76.18, perteneciente a la máquina desde la cual se realizó el ejercicio de pentesting.

Esta configuración permitió establecer la comunicación entre el atacante y el sistema comprometido, asegurando que, al ejecutar el exploit, la sesión remota se redirigiera correctamente hacia el equipo de control del Red Team.

Figura 15

Consulta de parámetros de configuración en Metasploit



Fuente. Autoría propia.

Figura 16

Configuración del parámetro RHOST en Metasploit

Fuente. Autoría propia.

Figura 17

Configuración del parámetro LHOST en Metasploit

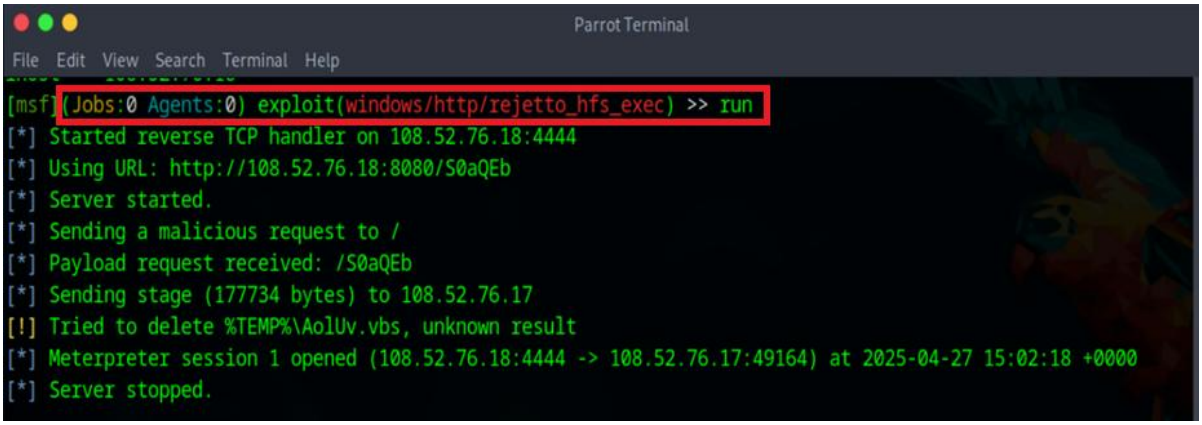
```
[msf](Jobs:0 Agents:0) exploit(windows/http/rejetto_hfs_exec) >> set LHOST 108.52.76.18
LHOST => 108.52.76.18
```

Fuente. Autoría propia.

Con los parámetros previamente configurados, se procedió a ejecutar el exploit mediante el comando run. Cabe destacar que, en Metasploit, también es posible iniciar la explotación utilizando el comando exploit, ya que ambos comandos cumplen la misma función: lanzar el módulo seleccionado y comenzar el proceso de ataque contra el objetivo. Al ejecutar el comando, se logró establecer una sesión remota exitosa con la máquina Windows 7.

Figura 18

Ejecución del exploit en Metasploit



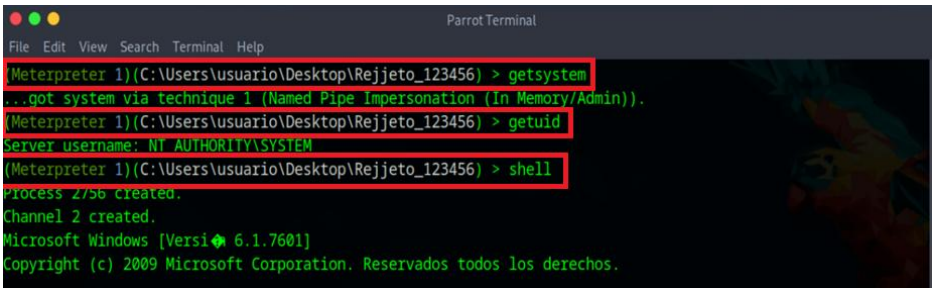
Fuente. Autoría propia.

Una vez establecida la sesión en la máquina comprometida mediante Meterpreter, una herramienta avanzada de Metasploit que opera en memoria para facilitar el control remoto, se procedió a ejecutar comandos clave para validar el acceso. Se utilizó getuid para identificar el usuario actual con el que se había ingresado al sistema, getsystem para realizar la escalación de privilegios y obtener permisos de nivel SYSTEM, y shell para abrir una consola de comandos

tradicional como la que se conoce como cmd en sistemas Windows. Estas acciones permitieron confirmar el nivel de acceso alcanzado y preparar el entorno para realizar tareas de post-explotación de forma efectiva.

Figura 19

Ejecución remota de comandos

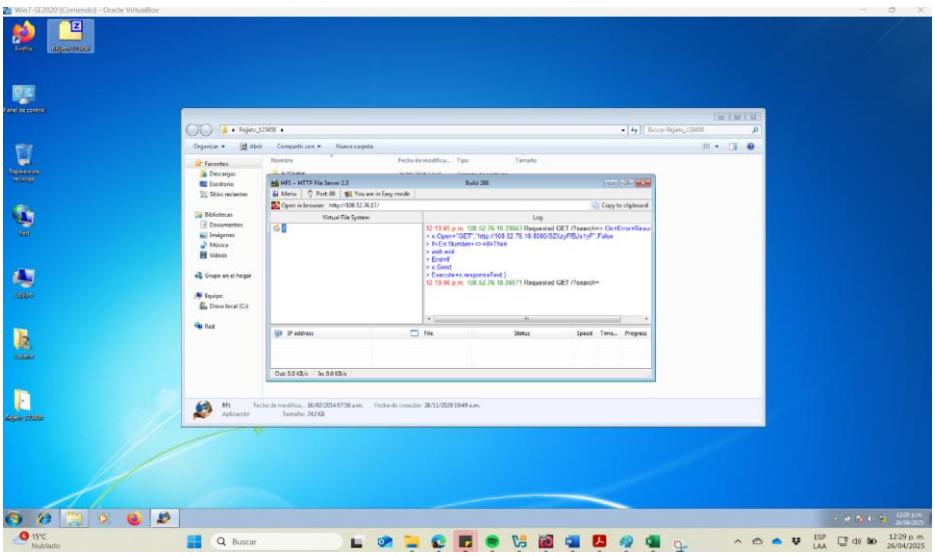


Fuente. Autoría propia

En la máquina Windows 7 se verificó la conexión establecida, confirmando la ejecución exitosa del exploit a través de la aplicación vulnerable Rejetto HTTP File Server (HFS).

Figura 20

Verificación en la máquina Windows 7

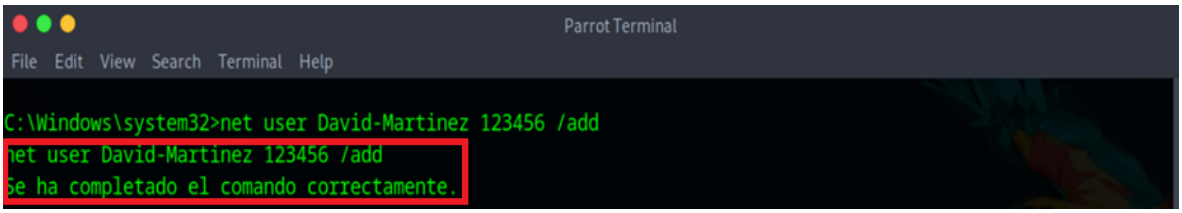


Fuente. Autoría propia

De acuerdo con la solicitud realizada por la alta dirección de la organización, se procedió a la creación de un nuevo usuario en la máquina comprometida. Para ello, se ejecutó el comando net user David-Martinez 123456 /add, el cual permitió registrar un nuevo usuario en el sistema con la contraseña especificada. Posteriormente, mediante el comando net localgroup administradores David-Martinez /add, se añadió dicho usuario al grupo de administradores locales, otorgándole privilegios elevados. Esta acción permitió demostrar la explotación exitosa de la vulnerabilidad y la posibilidad de escalamiento de privilegios, cumpliendo así con la prueba de concepto (PoC) solicitada.

Figura 21

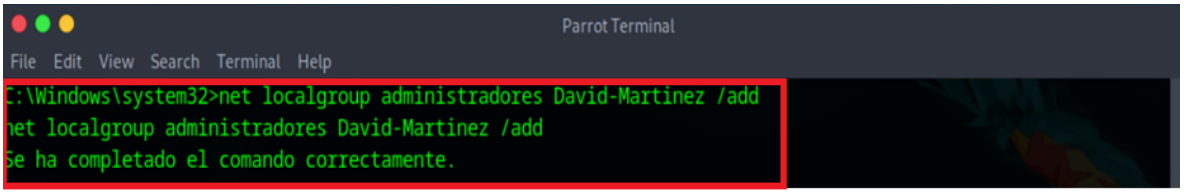
Creación del usuario en la máquina Windows 7 desde Metasploit



Fuente. Autoría propia

Figura 22

Asignación de permisos de usuario administrador al usuario creado

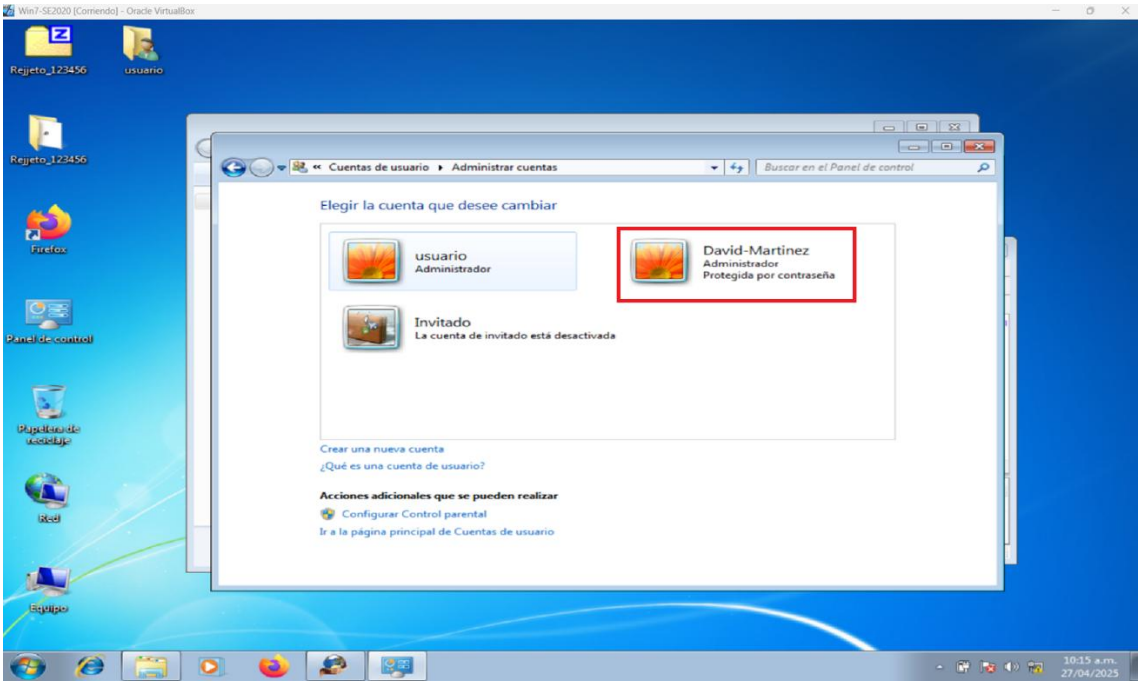


Fuente. Autoría propia

Desde la máquina Windows 7 se verificó la creación del usuario David-Martinez con el permiso de administrador.

Figura 23

Verificación del usuario creado con permisos de administrador en Windows 7



Fuente. Autoría propia

Documentación y evidencias de resultados:

Para esta fase, se recopilan todas las evidencias obtenidas durante el proceso de pentesting realizado a la máquina Windows 7. Con el fin de cumplir los objetivos de la actividad, el presente documento se estructura para compilar y presentar de manera organizada dichas evidencias, incluyendo los comandos ejecutados, los resultados obtenidos, las capturas de pantalla relevantes y el análisis técnico correspondiente. De esta manera, se garantiza la trazabilidad de cada acción realizada, así como la demostración clara de la explotación de la vulnerabilidad, la escalación de privilegios y el cumplimiento de la prueba de concepto solicitada por la organización.

Punto 2

El Anexo 4 – Escenario 3 es un documento valioso para el ejercicio realizado, teniendo en cuenta que presenta elementos claves para el ejercicio de análisis para identificar el motivo por el cual se presentó la fuga de información y la escalación de privilegios.

Elementos que describe el anexo:

Sistema operativo afectado: Se menciona que la máquina comprometida cuenta con el sistema operativo Windows 7, enfocando el análisis a este sistema operativo.

Aplicación vulnerable: Se describe que la máquina cuenta con una aplicación vulnerable, que tras realizar el proceso de pentesting y explotación, se determina que es Rejetto HTTP FileServer (HFS). Esta información es fundamental para la búsqueda de exploits específicos en Mestasploit.

Tipo de incidente: El anexo describe la ocurrencia de una fuga de información, lo que inicialmente orientó la investigación hacia la posible explotación de vulnerabilidades. Esta hipótesis fue confirmada al concluir el ejercicio de pentesting, donde se evidenció que existían fallos de seguridad que permitieron el acceso no autorizado a la información como también la creación de usuarios con permisos de administrador.

Acceso a la evidencia: El anexo también especifica que el equipo de análisis forense de la organización proporcionó una copia de la máquina afectada, lo cual otorga un marco de legalidad y validez al proceso de análisis. Este detalle es fundamental, ya que asegura que las actividades de pentesting y explotación se realizan sobre una imagen controlada, preservando la integridad de la evidencia digital y respetando los procedimientos adecuados de manejo de incidentes.

Punto 3

Como se mencionó en el punto 1, las herramientas empleadas para identificar los fallos de seguridad en la máquina Windows 7 fueron Nmap y Nessus. Nmap permitió detectar los puertos y servicios abiertos, mientras que Nessus realizó un análisis detallado que reveló vulnerabilidades críticas activas en el sistema. Entre las más relevantes se identificaron:

CVE-2007-6750: Vulnerabilidad en servidores HTTP Apache (versiones 1.x y 2.x), que permite a un atacante generar una denegación de servicio (DoS) mediante el envío de solicitudes HTTP parciales. Su detección alerta sobre posibles vectores de ataque si la máquina tuviera servicios Apache activos (INCIBE, 2011).

CVE-2017-0143: Falla crítica en el protocolo SMBv1 presente en múltiples versiones de Windows. Esta vulnerabilidad permite ejecución remota de código (RCE) a través de paquetes especialmente diseñados, y fue ampliamente utilizada por el exploit EternalBlue en ataques como WannaCry. Su presencia representa un riesgo elevado de seguridad en entornos que aún utilizan este protocolo obsoleto (INCIBE, 2017).

CVE-2024-23692: Afecta a Rejetto HTTP File Server (HFS) hasta la versión 2.3m. Permite a un atacante remoto no autenticado ejecutar comandos arbitrarios a través de una inyección de plantillas mediante solicitudes HTTP manipuladas. Durante el ejercicio de pentesting, esta vulnerabilidad fue identificada y aprovechada con éxito para lograr acceso no autorizado al sistema (INCIBE, 2024).

En cuanto al puerto asociado a la aplicación vulnerable descrita en el Anexo 4 – Escenario 3, se estableció que Rejetto HTTP File Server (HFS) opera sobre el puerto 80/TCP, ya que actúa como servidor HTTP. Este hecho facilitó el acceso y posterior explotación remota de la vulnerabilidad detectada en dicha aplicación.

Punto 4

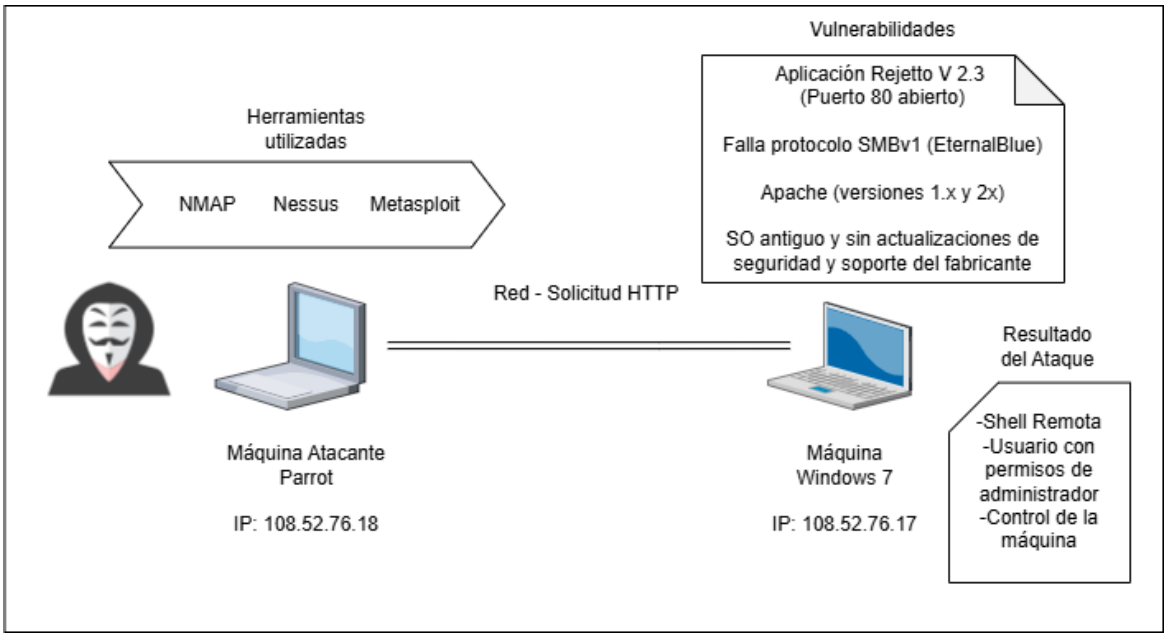
El ataque comprometió la máquina con sistema operativo Windows 7 al explotar una vulnerabilidad crítica en la aplicación Rejetto HTTP File Server (HFS), expuesta a través del puerto 80. Esta falla permitió a un atacante remoto ejecutar comandos arbitrarios mediante una sesión Meterpreter, lo que derivó en un acceso no autorizado. A partir de esta intrusión, se logró una escalación de privilegios, permitiendo tomar control total del sistema. Este acceso puede comprometer la confidencialidad de la información, facilitar la instalación de malware o incluso provocar una denegación de servicio.

Por lo tanto, la vulnerabilidad explotada afecta gravemente la confidencialidad, integridad y disponibilidad del sistema comprometido. La confidencialidad se ve comprometida al permitir la ejecución remota de comandos sin autenticación, lo que facilita el acceso a información sensible almacenada en el sistema, como archivos confidenciales o configuraciones críticas. La integridad se afecta porque el atacante puede modificar, reemplazar o eliminar archivos alojados, alterar configuraciones del sistema o inyectar contenido malicioso, generando consecuencias funcionales o legales. Finalmente, la disponibilidad se ve amenazada ya que se pueden ejecutar acciones que interfieren con el funcionamiento normal del sistema operativo, como la sobrecarga de procesos, la interrupción de servicios o incluso el uso de la vulnerabilidad como vector para ataques de denegación de servicio o instalación de ransomware. Esta afectación conjunta evidencia el riesgo crítico que representa no aplicar medidas de prevención y mitigación adecuadas.

A continuación, se encuentra la topología de red del ataque:

Figura 24

Topología de red del ataque



Fuente. Autoría propia

Punto 5

Como se evidenció en el punto inicial de la actividad, una vez se contó con la identificación de las vulnerabilidades en la máquina Windows 7 y teniendo en cuenta lo requerido en el Anexo 4 – Escenario 3, se enfocó la actividad en la explotación de la vulnerabilidad (CVE-2024-23692) mediante Metasploit.

Para ello fue necesario ejecutar los comandos:

msfconsole: Para iniciar la consola principal de Metasploit y de esta forma gestionar exploits, payloads y sesiones.

search HttpFileServer: Con el fin de buscar los módulos relacionados con "HttpFileServer" dentro de la base de datos de exploits de Metasploit.

use exploit/windows/http/rejetto_hfs_exec: Para seleccionar el módulo de explotación específico para la vulnerabilidad en Rejetto HFS.

set RHOST 108.52.76.17: Para definir la dirección IP del host remoto objetivo (la máquina Windows 7 vulnerable).

set LHOST 108.52.76.18: Para definir la IP local del atacante, donde se recibirá la conexión inversa (reverse shell).

run: Ejecuta el módulo configurado para lanzar el exploit contra el objetivo.

A partir del análisis realizado, se concluye que es fundamental fortalecer la seguridad de la infraestructura tecnológica de la organización. Esto permitirá mitigar los riesgos asociados a vulnerabilidades no gestionadas y reducir significativamente la ventana de oportunidad que los adversarios pueden aprovechar para ejecutar ataques, comprometer sistemas críticos o acceder a información sensible.

A continuación, se encuentran algunas recomendaciones que se sugiere aplicar para evitar que se materialicen incidentes como el analizado:

Auditorías periódicas de seguridad: Realizar evaluaciones de seguridad y análisis de vulnerabilidades de forma continua para identificar equipos con sistemas operativos obsoletos o software sin soporte.

Actualización de sistemas operativos y parches de seguridad: Sustituir equipos con Windows 7 u otros sistemas sin soporte, y mantener siempre actualizado el software con los últimos parches de seguridad.

Implementación de soluciones EDR/XDR: Utilizar tecnologías avanzadas de detección y respuesta ante amenazas (EDR – Endpoint Detection and Response, XDR – Extended Detection and Response) para identificar comportamientos anómalos y bloquear ataques en tiempo real.

Segmentación de red mediante VLANs: Dividir la red en segmentos lógicos para limitar la propagación lateral en caso de compromiso, reduciendo así el alcance de un atacante.

Implementación de controles de red: Configurar la seguridad perimetral mediante firewalls, así como sistemas de detección (IDS) y prevención de intrusos (IPS) para monitorear y responder ante eventos anómalos. Se recomienda restringir el acceso al puerto 80 mediante firewall o listas de control de acceso (ACL).

Gestión de accesos: Controlar y auditar el uso de cuentas con privilegios administrativos. Políticas de backups regulares y cifrados: Implementar copias de seguridad automáticas, fuera de línea y cifradas, con planes de recuperación ante desastres.

Etapa 4: Contención de Ataques Informáticos

Punto 1

Para contextualizar la etapa cuatro del seminario, es crucial comprender el rol del Blue Team: un equipo de expertos en ciberseguridad dedicado a la defensa proactiva de la organización contra adversarios. Su función primordial es proteger los activos mediante un análisis exhaustivo del estado de seguridad, implementando estrategias como la supervisión continua, el análisis de registros, la evaluación de vulnerabilidades y la respuesta a incidentes para identificar debilidades, reforzar controles y asegurar la protección integral de sistemas, datos y operaciones frente a amenazas reales (IBM, 2023).

Es fundamental que las organizaciones dispongan de un plan de respuesta ante incidentes de ciberseguridad, el cual actúe como una guía estructurada para todos los equipos involucrados. Este plan permite mitigar eficazmente los ataques, asegurar la continuidad del negocio y minimizar los impactos negativos, tanto en la pérdida de información como en los aspectos

económicos y reputacionales. De acuerdo con Parra (s. f.) el plan se debe desarrollar en cuatro fases que son: preparación, detección y análisis, respuesta y acciones post incidente.

Asumiendo que las herramientas de monitoreo y detección administradas (Nessus), por un Centro de Operaciones de Seguridad (SOC) o por un Equipo de Respuesta ante Incidencias de Seguridad Informáticas (CSIRT), alertaron sobre un incidente en la máquina con el sistema operativo Windows 7, es necesario profundizar en la fase de detección y análisis.

De tal manera que se debe identificar con prioridad con qué tipo de ataque se está lidiando, para ello se deben utilizar herramientas como Wireshark, la cual permite analizar el tráfico de red en tiempo real, detectando actividades sospechosas como intentos de intrusión, tráfico malicioso o fuga de datos (Wireshark, s. f.).

Una vez detectado el compromiso, la siguiente fase es la contención inmediata. En este contexto, se debe aislar completamente el sistema afectado para evitar la propagación del ataque dentro de la red corporativa. Este aislamiento puede lograrse de forma física, desconectando el cable de red, o de manera lógica, deshabilitando la interfaz de red desde el sistema operativo. Adicionalmente, si se detecta que el firewall perimetral o de la máquina presenta una configuración inadecuada, se deben aplicar reglas de contención específicas, bloqueando IPs maliciosas y cerrando puertos vulnerables, particularmente aquellos asociados al servicio comprometido (en este caso, el puerto 80 utilizado por Rejetto HFS).

Tan pronto se haya realizado la contención, es fundamental proceder con la preservación de la evidencia digital, lo cual da inicio formal a una investigación donde el equipo de análisis forense debe realizar un proceso que incluye:

Captura de la memoria RAM: Mediante herramientas como por ejemplo Belkasoft RAM, la cual permite extraer de forma segura la evidencia volátil como procesos en ejecución,

contraseñas en memoria, comandos ejecutados y sesiones activas (como una posible sesión de Meterpreter).

Copia bit a bit del disco duro del sistema comprometido: Se puede generar a través de herramientas como FTK Imager. A partir de la cual, y por medio de herramientas como Autopsy se puede analizar en profundidad archivos del sistema, logs, posibles malware persistentes, y cambios en el sistema de archivos.

También es importante correlacionar estos artefactos con la captura de tráfico de red, previamente realizada mediante Wireshark. Esta correlación es crucial para reconstruir la línea de tiempo del ataque, identificar los vectores de entrada y salida, y asociar acciones observadas en el sistema con eventos de red específicos.

Otro aspecto fundamental que deben liderar las áreas de riesgos y auditoría de la organización es la definición y seguimiento de un plan de acción correctivo, el cual debe ser ejecutado por el área de tecnología dentro de un plazo previamente establecido. Este plan debe contemplar medidas específicas orientadas a remediar las vulnerabilidades identificadas, fortalecer los controles de seguridad y prevenir la recurrencia de incidentes de este tipo. A continuación, se encuentran algunas medidas de hardenización para contribuir con este plan.

Punto 2

Teniendo en cuenta el ejercicio realizado desde el equipo Red Team y partiendo de que se cuenta con el análisis del ataque realizado, es vital reducir la superficie de ataque mediante el endurecimiento de la seguridad de los sistemas operativos y equipos de red, aplicando los controles y las actualizaciones proporcionadas por los fabricantes. Por lo tanto, se debe:

Desinstalar la aplicación Rejetto HTTP File Server (HFS) en todos los equipos de la organización, ya que está aplicación cuenta con una vulnerabilidad y se debe sustituir por una

aplicación segura y actualizada o por otros medios para compartir información como por ejemplo One Drive para la empresa, la cual permite gestionar adecuadamente los accesos mediante control de permisos, autenticación multifactor (MFA) y cifrado de datos en tránsito y en reposo.

Actualizar los equipos a nivel de hardware compatible con el sistema operativo Windows 11, considerando que Windows 7 es un sistema obsoleto y Windows 10 dejará de recibir soporte oficial de seguridad en 2025. Utilizar sistemas operativos sin soporte representa un riesgo crítico, ya que quedan expuestos a nuevas vulnerabilidades sin posibilidad de corrección.

Implementar políticas de control de software, contraseñas y privilegios de usuarios, mediante Directivas de Grupo (GPO) en Active Directory. Las políticas deben restringir la instalación de software solo al personal autorizado del área de TI, establecer contraseñas robustas (combinación de longitud, complejidad y periodicidad de cambio), y limitar el uso de cuentas con privilegios administrativos solo cuando sea estrictamente necesario. Todo lo anterior debe ejecutarse en alineación con las directrices del área de Seguridad de la Información, asegurando el cumplimiento de los procedimientos internos y normativas vigentes.

Configurar adecuadamente el firewall de Windows en todos los equipos, o implementar un firewall perimetral centralizado, con reglas que bloqueen puertos innecesarios como el puerto 80 y permitan únicamente conexiones hacia y desde direcciones IP previamente autorizadas y monitoreadas.

Verificar que el software instalado en los equipos corresponda estrictamente a la línea base autorizada, previamente definida y aprobada por el área de TI y Seguridad de la Información.

Instalar soluciones de seguridad de nueva generación como EDR (Endpoint Detection and Response) o XDR (Extended Detection and Response). Estas herramientas permiten detectar

y responder a ataques sofisticados, incluso aquellos que utilizan técnicas de evasión y herramientas potenciadas por inteligencia artificial. La administración de estos agentes debe realizarse desde una consola central, que permita aplicar políticas de filtrado web, control de dispositivos extraíbles y análisis de comportamiento.

Implementar software DLP (Data Loss Prevention) en los equipos, para prevenir la filtración de información confidencial y garantizar el cumplimiento normativo en el tratamiento de datos sensibles. Esta solución debe ser configurada para monitorear el uso, movimiento y copia de archivos dentro y fuera de la organización, permitiendo alertas o bloqueos ante comportamientos no autorizados.

Es vital contar con un sistema de detección y prevención de intrusiones (IDS/IPS) correctamente implementado y configurado en la infraestructura de red de la organización. Teniendo en cuenta en Anexo 5 – Escenario 4, Snort puede ser una opción válida para detección y bloqueo de amenazas en tiempo real.

Punto 3

A continuación, se encuentran algunos conceptos clave para entender las diferencias entre equipos Blue Team y equipos de respuesta a incidentes de seguridad informática, teniendo en cuenta lo descrito por IBM (2023) y Microsoft (s. f.).

Tabla 2

Diferencias entre Blue Team y CSIRT

Aspecto	**Equipo Blue Team**	**Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT)**
Enfoque	Proactivo	Reactivo
Objetivo	Defender a los activos de la organización para evitar ataques cibernéticos	Responder de manera estructurada y eficaz a incidentes de seguridad ya ocurridos, con el fin de minimizar su impacto y restaurar la operación normal

	mejorando la postura de seguridad.	
Funciones	Monitorear continuamente sistemas, redes y eventos.	Identificar, contener y eliminar las amenazas activas para restaurar la operación.
	Gestionar vulnerabilidades y configuraciones para reducir la superficie de ataque.	Realizar análisis forenses para determinar las causas de los incidentes de seguridad
	Participar en simulacros de defensa (Blue vs Red Team).	Coordinar la respuesta a los incidentes con las áreas clave de la organización
	Capacitar al personal en ciberseguridad y concienciación	Documentar los incidentes y generar planes de acción y de mejora.
Tipo de Equipo	Conformado por profesionales o expertos en seguridad informática de la organización, normalmente parte del área de tecnología o de seguridad informática	Equipo multidisciplinar conformado por personal interno y/o externo (proveedores), involucrando áreas como tecnología, legal, riesgos y cumplimiento
Herramientas utilizadas	SIEM, IDS/IPS, EDR/XDR, gestores de vulnerabilidades	Consolas de respuestas a incidentes, herramientas de análisis forense, playbooks de respuesta, sistemas de gestión de incidentes entre otros
Trabaja con	Equipos Red Team, áreas de tecnología, seguridad informática e infraestructura.	Áreas de seguridad informática, tecnología, legales, cumplimiento, gestión de riesgos y proveedores externos de ciberseguridad.

Fuente. Autoría propia

Punto 4

Si dentro de un equipo Blue Team se indica la necesidad de trabajar con el Center for Internet Security (CIS), esto representa una señal clara de que se busca fortalecer la postura de seguridad de la organización mediante la implementación de estándares y buenas prácticas

reconocidas internacionalmente, con el propósito de proteger los activos tecnológicos y de información frente a las amenazas cibernéticas actuales. Estas amenazas incluyen un espectro cada vez más sofisticado de técnicas y tácticas empleadas por adversarios, muchas de ellas potenciadas por el uso de inteligencia artificial (Center for Internet Security, s. f.).

En este contexto, emplearía los CIS Controls para aplicar mejores prácticas enfocadas en la optimización de la defensa proactiva, la priorización de controles basados en riesgos, y el cumplimiento normativo. Asimismo, utilizaría los CIS Benchmarks como guías técnicas para la configuración segura de dispositivos de red y de sistemas operativos tanto en estaciones de trabajo como en servidores, incluyendo entornos en la nube como Microsoft Azure o Amazon Web Services (AWS), por mencionar algunos.

Complementariamente, trabajaría en conjunto con el área de Seguridad de la Información para alinear las políticas y procedimientos institucionales con los lineamientos del CIS, asegurando que las medidas implementadas respondan tanto a los requerimientos operativos como a los estándares exigidos por las auditorías internas y externas, que suelen ser cada vez más exhaustivas en materia de ciberseguridad.

Punto 5

De acuerdo con lo señalado por IBM (s. f.), un SIEM (Security Information and Event Management) es una solución integral de seguridad que permite a las organizaciones mejorar la detección, el análisis y la respuesta ante amenazas cibernéticas, mediante la recolección centralizada, en tiempo real, y la correlación de grandes volúmenes de datos y eventos provenientes de múltiples fuentes dentro de una infraestructura de TI. Estas fuentes incluyen equipos de usuario final, firewalls, dispositivos de red, servidores, aplicaciones empresariales y entornos en la nube, entre otros.

Las soluciones SIEM de última generación integran capacidades avanzadas de analítica de datos, inteligencia artificial (IA) y aprendizaje automático, lo que permite detectar comportamientos anómalos, automatizar tareas de monitoreo y respuesta, y reducir significativamente los tiempos de detección y reacción ante incidentes de seguridad. Estas funcionalidades convierten al SIEM en un elemento clave dentro de los SOC, al ofrecer una visibilidad centralizada del entorno tecnológico, alertas enriquecidas con contexto y herramientas para facilitar el cumplimiento de normativas regulatorias. En un escenario real, el SIEM cumple un papel estratégico al correlacionar múltiples eventos dispersos a lo largo de la infraestructura tecnológica para reconstruir la secuencia de un ataque, permitiendo identificar desde accesos no autorizados y ejecución de scripts maliciosos hasta tráfico inusual hacia direcciones IP externas, lo que fortalece la capacidad de respuesta, el análisis forense y a minimizar el riesgo cibernético.

Entre las funciones más importantes de un SIEM se tiene:

Gestionar y analizar registros: Mediante la recopilación centralizada de eventos de seguridad desde múltiples dispositivos y sistemas.

Correlacionar eventos: A partir de análisis potenciados por la inteligencia artificial y el aprendizaje automático, para detectar patrones o actividades sospechosas que se pueden considerar una amenaza de seguridad y de esta manera mitigar rápidamente el riesgo.

Monitorear y generar alertas: Por medio de la emisión de alertas en tiempo real ante comportamientos inusuales o violaciones de políticas de seguridad, lo que permite a los equipos de TI y de seguridad actuar de forma precisa para evitar o contener posibles incidentes.

Contribuir al cumplimiento normativo y auditoría: Una solución SIEM permite generar informes automáticos y en tiempo real que se encuentren alineados con normativas internacionales, reduciendo la carga operativa de los equipos de TI y seguridad.

Apoyar el análisis forense: Debido a que aportan datos de incidentes de seguridad que sirven como apoyo para el análisis histórico de eventos, contribuyendo a la identificación de la causa raíz y a la mejora continua de los controles de seguridad.

Punto 6

Contener ataques informáticos mediante el uso de herramientas nativas de Windows o soluciones de código abierto ofrece una amplia variedad de opciones efectivas para responder en tiempo real a incidentes de seguridad. De tal manera que se permitan bloquear conexiones sospechosas, aislar los sistemas comprometidos, monitorear comportamientos maliciosos, y aplicar controles de acceso de forma automatizada entre otras funcionalidades. A continuación, se proponen tres opciones:

Firewall de Windows: El sistema operativo Windows incorpora de forma nativa un firewall avanzado que, al ser configurado correctamente, permite establecer reglas precisas para controlar el tráfico de red entrante y saliente. Esta herramienta resulta clave para contener amenazas, ya que permite bloquear puertos específicos, restringir direcciones IP sospechosas, y limitar el acceso de aplicaciones a servicios de red. En el contexto del caso de estudio, por ejemplo, el Firewall de Windows podría utilizarse para bloquear el puerto 80, utilizado por la aplicación vulnerable Rejetto HTTP File Server (HFS), con el fin de evitar su exposición y reducir el riesgo de explotación remota.

Suricata: Esta herramienta de código abierto se utiliza para detección y prevención de intrusiones (IDS/IPS), de tal manera que permite monitorear el tráfico de la red en tiempo real y bloquear automáticamente conexiones sospechosas, lo que la convierte en una herramienta eficaz para contener amenazas activas. En escenarios como la explotación de la vulnerabilidad en la aplicación Rejetto HTTP File Server (HFS) a través del puerto 80, esta herramienta sería capaz

de identificar y bloquear patrones de ataque conocidos asociados a esa explotación, evitando la ejecución remota de código o la escalación de privilegios desde un acceso no autorizado.

PowerShell: Es una herramienta nativa avanzada del sistema operativo Windows que permite ejecutar acciones de administración y respuesta ante incidentes mediante comandos y scripts personalizados. Esta utilidad facilita la creación de reglas de firewall, el cierre de procesos sospechosos, la desactivación de servicios vulnerables y la revocación de privilegios a usuarios comprometidos, todo sin depender de software de terceros. En el caso específico de la aplicación vulnerable Rejetto HTTP File Server (HFS), PowerShell puede utilizarse para detener el proceso activo de HFS, bloquear su puerto de escucha (80) y eliminar el ejecutable del sistema. Estas acciones permiten contener rápidamente la amenaza y limitar el acceso no autorizado antes de que se materialice un mayor compromiso de seguridad.

Aspectos que Aportan al Desarrollo de Estrategias Red Team y Blue Team

Entre los aspectos clave que se deben considerar para garantizar un aporte significativo en el desarrollo de estrategias de los equipos Red Team y Blue Team en las organizaciones, destacan los siguientes:

Compromiso desde la alta dirección: Es imprescindible que exista una voluntad firme por parte de la alta dirección para respaldar la conformación y funcionamiento de los equipos Red Team y Blue Team. Esto implica asignar recursos tecnológicos adecuados, presupuesto y personal especializado, así como promover una cultura organizacional orientada a la ciberseguridad proactiva.

Capacitación continua y especializada del personal: Dada la evolución constante de las amenazas y las tecnologías, los integrantes de estos equipos deben recibir formación continua en el uso de herramientas avanzadas, gestión de hardware y software, y en marcos de referencia

reconocidos internacionalmente como MITRE ATT&CK, NIST y CIS Controls. Esta capacitación debe ser pertinente y adaptada a los nuevos desafíos que enfrenta la seguridad informática.

Retroalimentación continua e integración interdepartamental: Los hallazgos obtenidos en las actividades y análisis realizados por los equipos Red Team y Blue Team deben compartirse de manera constante y estructurada con otras áreas clave de la organización, como Gestión de Riesgos, Seguridad Informática, Seguridad de la Información, y TI. Esta sinergia permite implementar planes de mejora efectivos, actualizar políticas de seguridad, fortalecer controles y garantizar una postura de seguridad integral, alineada con las necesidades reales del entorno organizacional.

Incorporación de indicadores de rendimiento (KPIs): Es necesario definir métricas que permitan evaluar de forma precisa la efectividad de las actividades tanto ofensivas como defensivas. Estos indicadores deben estar estrechamente vinculados a los objetivos estratégicos de la organización y facilitar el monitoreo de aspectos clave como el tiempo de detección de incidentes, la velocidad de respuesta, la cantidad de vulnerabilidades identificadas y el grado de cumplimiento de las políticas de seguridad establecidas.

Conclusiones

El desarrollo de las actividades realizadas durante el seminario especializado evidenció que la adopción de estrategias fundamentadas en la dinámica operativa de los equipos Red Team y Blue Team resulta clave para el fortalecimiento integral de la ciberseguridad en las organizaciones. Mientras el Red Team simula ataques reales para descubrir vulnerabilidades y evaluar la capacidad de respuesta, el Blue Team se encarga de la detección, contención y mitigación de incidentes. Para que estas estrategias sean efectivas, es indispensable que las organizaciones conformen formalmente estos equipos con profesionales altamente especializados y dedicados exclusivamente a sus funciones, lo que permite anticiparse a amenazas reales, reducir riesgos y proteger de manera proactiva los activos críticos de información.

Las actividades prácticas, como el laboratorio de pentesting en entornos virtualizados, evidenciaron que la integración de enfoques ofensivos y defensivos, apoyados en herramientas como Nmap, Nessus y Metasploit, permite identificar y corregir brechas de seguridad de forma efectiva. Este tipo de ejercicios es clave para mitigar riesgos y fortalecer la infraestructura de TI, contribuyendo a una defensa más robusta en las organizaciones.

Contar con profesionales de ciberseguridad capacitados, éticamente comprometidos y legalmente actualizados, es un factor determinante en el despliegue exitoso de estrategias Red Team y Blue Team. La sinergia entre estos equipos y las distintas áreas de la organización no solo facilita la gestión proactiva de amenazas, sino que también permite implementar medidas como la hardenización de sistemas, el monitoreo continuo, la respuesta inmediata a incidentes y el cumplimiento normativo. Esto fortalece de forma integral la resiliencia digital institucional frente a un entorno de amenazas en constante evolución.

Recomendaciones

Se recomienda que las organizaciones institucionalicen la metodología Red Team y Blue Team mediante la designación formal de personal idóneo y especializado. Además, es fundamental ejecutar pruebas de penetración periódicas que permitan simular ataques controlados para identificar vulnerabilidades no detectadas, evaluar la eficacia de los controles de seguridad y mejorar la capacidad de respuesta. La realización constante de estos ejercicios de simulación y evaluación fortalece de manera integral la postura de seguridad organizacional.

Es fundamental implementar soluciones SIEM que proporcionen monitoreo proactivo y visibilidad centralizada de la infraestructura de seguridad, permitiendo la correlación de eventos y la generación de alertas en tiempo real. Esto facilita la detección temprana de amenazas, la respuesta rápida a incidentes y la mejora continua de la postura de seguridad organizacional, apoyando de manera efectiva el trabajo tanto de los equipos Blue Team como Red Team, así como de las áreas de seguridad informática en la gestión integral de riesgos y la coordinación de acciones defensivas y ofensivas.

Se recomienda que las organizaciones desarrollen y mantengan un plan de respuesta a incidentes de ciberseguridad robusto, acompañado de políticas y procedimientos estructurados, actualizados y alineados con estándares y normativas internacionales. Estas directrices deben ser diseñadas, difundidas y supervisadas por el área de Seguridad de la Información, garantizando su cumplimiento obligatorio en toda la organización. De esta forma, se asegura una gestión efectiva ante incidentes y se minimizan riesgos legales y operativos, transformando las auditorías internas y externas en oportunidades de mejora continua, en lugar de identificar hallazgos críticos.

Resulta clave fortalecer la hardenización de sistemas mediante una gestión rigurosa y constante de parches y actualizaciones, asegurando que todos los componentes de hardware y

software estén protegidos contra vulnerabilidades conocidas. Además, es fundamental promover la capacitación continua del personal de TI, adaptándola a las nuevas tecnologías y amenazas emergentes. Tanto el equipo Blue Team como el Red Team deben contar con especialización constante para manejar eficazmente las herramientas y técnicas necesarias para defender y evaluar la infraestructura tecnológica, garantizando una protección integral y actualizada.

Referencias Bibliográficas

ARFASA Abogados. (2024). La importancia de la revisión de contratos para evitar contingencias legales [Publicación en LinkedIn]. LinkedIn. https://www.linkedin.com/pulse/la-importancia-de-revisi%C3%B3n-contratos-para-evitar-contingencias-yzc9e/

Auditool. (2024). La importancia de la confidencialidad en auditoría: Manteniendo la ética profesional. Auditool. https://www.auditool.org/blog/auditoria-interna/la-importancia-de-la-confidencialidad-en-auditoria-manteniendo-la-etica-profesional

Campus Internacional de Ciberseguridad. (2024). La guía definitiva de Metasploit [Publicación]. LinkedIn. https://www.linkedin.com/pulse/la-gu%C3%ADa-definitiva-de-metasploit-campusdeciberseguridad-gcnwf/

Center for Internet Security. (s. f.). About us. https://www.cisecurity.org/about-us

Consejo Profesional Nacional de Ingeniería (COPNIA). (2003). Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares. https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Departamento Nacional de Planeación. (2020). Política nacional de confianza y seguridad digital (Documento CONPES No. 3995). https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

ESET. (s. f.). Evaluación de vulnerabilidades usando OpenVAS. WeLiveSecurity. https://www.welivesecurity.com/es/recursos-herramientas/evaluacion-vulnerabilidades-openvas/

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

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

Función Pública. (2013). Decreto 1377 de 2013. Departamento Administrativo de la Función Pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

IBM. (s. f.). ¿Qué es el pentesting? IBM. https://www.ibm.com/mx-es/topics/penetration-testing

IBM. (s. f.) ¿Qué es la gestión de eventos e información de seguridad (SIEM)? IBM. https://www.ibm.com/mx-es/topics/siem

IBM. (s. f.). ¿Qué son las vulnerabilidades y exposiciones comunes (CVE)? IBM. https://www.ibm.com/es-es/think/topics/cve

IBM. (2023) ¿Qué es el equipo azul? IBM. https://www.ibm.com/mx-es/topics/blue-team

IBM. (2024) ¿Qué es el equipo rojo? IBM. https://www.ibm.com/mx-es/think/topics/red-teaming

INCIBE-CERT. (2011). CVE-2007-6750: Vulnerabilidad en Apache. INCIBE. https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2007-6750

INCIBE-CERT. (2017). CVE-2017-0143: Vulnerabilidad en servidor SMBv1 en múltiples productos Microsoft. INCIBE. https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2017-0143

INCIBE-CERT. (2024). CVE-2024-23692: Vulnerabilidad en Rejetto HTTP File Server. INCIBE. https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2024-23692

Microsoft. (s. f.). ¿Qué es la respuesta a incidentes? https://www.microsoft.com/es-co/security/business/security-101/what-is-incident-response

Ministerio de Tecnologías de la Información y las Comunicaciones. (2024). Resolución 2239 del 24 de junio de 2024. https://www.mintic.gov.co/portal/715/articles-2627_Resolucion_2239_de_2024.pdf

Nmap. (s. f.). Guía de referencia de Nmap. Nmap. https://nmap.org/man/es/index.html

Nuñez Alcalá, C. (2021). Penetration testing: Auditoría profesional [Trabajo de grado, Universidad Abierta de Cataluña]. Repositorio Institucional. https://openaccess.uoc.edu/bitstream/10609/132609/8/carlosnTFG0621memoria.pdf

Offensive Security. (2025). Acerca de la base de datos de exploits. Exploit Database. https://www.exploit-db.com/about-exploit-db

Parra, F. (s. f.). ¿Qué hacer en caso de un ciberataque? Netdata Networks. https://blog.netdatanetworks.com/que-hacer-en-caso-de-un-ciberataque

Policía Nacional de Colombia. (s. f.). Normatividad sobre delitos informáticos. https://www.policia.gov.co/normatividad-sobre-delitos-informaticos

Secretaría del Senado. (1991). Constitución política de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991_pr001.html

Secretaría del Senado. (2004). Ley 906 de 2004. http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004_pr001.html

Tenable (s. f.). Tenable Nessus: La herramienta primordial en su conjunto de herramientas de ciberseguridad. https://es-la.tenable.com/products/nessus

Wireshark (s. f.). About Wireshark. https://www.wireshark.org/about.html

Anexos

Anexo A

Sustentación

Link del video: https://youtu.be/ue_KkcB-hLE