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

Diego Armando Bolaños Anturi

Asesor:

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias Básicas, Tecnología E Ingeniería ECBTI

Especialización en seguridad informática

Diciembre 2025

Resumen

Este informe técnico tiene como objetivo relacionar el marco jurídico que se ocupa de la ciberseguridad en Colombia con la ejecución técnica de pruebas de penetración, abordando la revisión normativa de la Ley 1273 de 2009 y la Ley 1581 de 2012, además de la implementación práctica de las fases del hacking ético: reconocimiento, escaneo, explotación y mantenimiento, empleando herramientas como Metasploit en entornos virtuales; entre los resultados más destacados, se enfatiza la identificación de vulnerabilidades críticas en servicios web, como Rejetto, lo que permite verificar las técnicas de ataque, el escalamiento de privilegios y el movimiento lateral entre diferentes sistemas, subrayando la importancia de unir las habilidades técnicas ofensivas con tácticas defensivas (Blue Team), abarcando la adopción de soluciones SIEM y medidas de seguridad perimetral, permitiendo abordar generalidades sobre la protección de los activos de información, combinando rigurosidad técnica, la gestión de incidentes y un estricto cumplimiento de los principios éticos.

***Palabras clave*:** Blue teams, hacking, rejetto, SIEM, vulnerabilidades.

Abstract

This technical report aims to relate the legal framework governing cybersecurity in Colombia to the technical execution of penetration tests, addressing the regulatory review of Law 1273 of 2009 and Law 1581 of 2012, as well as the practical implementation of the phases of ethical hacking: reconnaissance, scanning, exploitation, and maintenance, using tools such as Metasploit in virtual environments. Among the most notable results, emphasis is placed on the identification of critical vulnerabilities in web services, such as Rejetto, which allows for the verification of attack techniques, privilege escalation, and lateral movement between different systems, underscoring the importance of combining offensive technical skills with defensive tactics (Blue Team), encompassing the adoption of SIEM solutions and perimeter security measures, allowing for a general approach to the protection of information assets, combining technical rigor, incident management, and strict compliance with ethical principles.

***Keywords*:** Blue teams, hacking, rejetto, SIEM, vulnerabilities.

Tabla de Contenido

Introducción 8

Justificación 9

Objetivos 10

Objetivo General 10

Objetivos Específicos 10

Tema 1 Principios de Operaciones Grupos Red Team y Blue Team 11

Pentesting 13

Herramientas de Ciberseguridad 15

Configuración banco de Trabajo 17

Tema 2 Escenario en el Marco de los Criterios Éticos y Legales 25

Tema 3 Hallazgo de Vulnerabilidades en un Sistema Informático mediante Técnicas de Intrusión 30

Escenario de Prueba 30

Tema 4 Gestión y Contención de Incidentes de Seguridad 45

Tema 5 Informe 49

Análisis del Vector de Ataque 49

Herramienta Principal: Metasploit Framework (MSFConsole) 49

Estrategia de Defensa y Respuesta 50

Erradicación y Recuperación 50

Conclusiones y Recomendaciones 52

Evidencia de Sustentación 53

Conclusiones 54

Recomendaciones 55

Referencias Bibliográficas 56

Apéndices.....60

Lista de Figuras

Figura 1 *Instalación máquina virtual virtualbox* 18

Figura 2 *Sistemas operativos instalados* 19

Figura 3 *Conexión parrot OS 6.4* 20

Figura 4 *Conexión maquinas A y B Windows* 21

Figura 5 *Configuración tarjeta de red máquina parrot* 22

Figura 6 *Configuración tarjeta de red (adaptador 1) máquina A windows* 23

Figura 7 *Configuración tarjeta de red (adaptador 2) máquina A windows* 24

Figura 8 *Conexión parrot OS a máquina Windows 7 A* 31

Figura 9 *Instalación de aplicación Rejetto* 32

Figura 10 *Msfconsole* 33

Figura 11 *Search rejetto* 34

Figura 12 *Vulnerabilidad 1* 35

Figura 13 *Autoroute* 36

Figura 14 *Portproxy* 37

Figura 15 *Sesión host B* 38

Figura 16 *Search eternalblue* 39

Figura 17 *Exploit eternalblue* 40

Figura 18 *Ipconfig host B* 41

Figura 19 *Net user host B* 42

Figura 20 *Evidencia usuario host B* 43

Figura 21 *Diagrama de flujo* 44

Lista de Apéndices

Apéndice A *Resultado de revisión en Turnitin* 60

Introducción

En el presente documento, conoceremos la importancia de los modelos que combinan tácticas tanto ofensivas como defensivas, administradas por el Red Team y el Blue Team, teniendo como objetivo establecer el contexto legal y ético necesario, en la correcta ejecución técnica de pruebas de penetración, asegurándose de que todas las actividades de seguridad se mantengan dentro del marco de la legalidad.

El Red Team actúa como el adversario, diseñando y realizando simulaciones de ataques para identificar vulnerabilidades importantes en las infraestructuras y procesos, con el fin de proporcionar una perspectiva realista y anticipada sobre los riesgos más cruciales, por otro lado, el Blue Team se enfoca en la detección, respuesta y mitigación de incidentes, fortaleciendo la habilidad de respuesta de la organización y reduciendo el tiempo de recuperación. La colaboración entre ambos es crucial para completar el ciclo de mejora continua: los hallazgos ofensivos del Red Team definen las prioridades de fortalecimiento del Blue Team, creando una estrategia defensiva basada en datos concretos.

Abordaremos las fases del hacking ético reconocimiento, escaneo, explotación y mantenimiento en un entorno virtual, incluyendo el uso de herramientas especializadas como Metasploit para identificar vulnerabilidades en servicios web como Rejetto y se presentarán los resultados más destacados, como la validación de métodos de ataque, el aumento de privilegios y el movimiento lateral. Finalmente, el informe resalta la importancia de las tácticas defensivas (Blue Team) mediante la implementación de soluciones SIEM y medidas de seguridad perimetral, concluyendo con un enfoque que integra la rigurosidad técnica y la gestión de incidentes.

Justificación

El presente informe articula el marco jurídico colombiano asociado a la ciberseguridad con la práctica técnica de las pruebas de penetración, requisitos legales que orientan las actividades propias del hacking ético, abordando pilares normativos que garantizan que las actividades de análisis de vulnerabilidades, explotación controlada y simulación de ataques se realicen con autorización, responsabilidad y respeto por los derechos de los titulares de la información, permitiendo fundamentar la pertinencia y obligatoriedad de integrar el componente legal en cualquier proceso técnico de evaluación de seguridad.

La ejecución de pruebas de penetración en entornos virtuales y los resultados obtenidos, la identificación de vulnerabilidades críticas en servicios web, entre ellos Rejetto, evidencia la relevancia de analizar escenarios reales donde es posible validar procedimientos de explotación, escalamiento de privilegios y el concepto de pivoting dentro de una infraestructura, generando hallazgos que no solo permiten confirmar la efectividad de las herramientas empleadas, sino que resaltan la importancia de conducir cada acción con rigurosidad y dentro del marco ético que demanda el ejercicio del pentesting.

Finalmente se destaca la necesidad de integrar las capacidades ofensivas con la perspectiva defensiva, entendiendo que el propósito último del hacking ético es mejorar la postura de seguridad de las organizaciones, incluyendo tácticas propias del Blue Team, tales como la adopción de soluciones SIEM, la puesta en marcha de medidas de seguridad perimetral y administración de incidentes, permitiendo consolidar un enfoque integral que abarca tanto la detección de amenazas como la protección de los activos de información.

Objetivos

Objetivo General

Evaluar el estado de la ciberseguridad en SecureNova Labs mediante pruebas reguladas, enmarcada en principios ético legales, además de medidas preventivas, reconociendo vulnerabilidades y sugiriendo mejoras en las tácticas del equipo Red Team y el Blue Team.

Objetivos Específicos

Abordar normativa legal para conocer la perspectiva ética y legal, que permita identificar los riesgos jurídicos asociados a la actividad.

Crear un entorno de prueba que a través de máquinas virtuales para evaluar estrategias ofensivas y defensivas.

Realizar pruebas de intrusión con el fin de analizar y explotar vulnerabilidades de un sistema operativo.

Crear estrategias de contención a la organización, como resultado de la evaluación de la infraestructura tecnológica propuesta.

Tema 1 Principios de Operaciones Grupos Red Team y Blue Team

En Colombia, las regulaciones que abordan los delitos electrónicos y la salvaguarda de la información personal se componen de leyes y decretos que supervisan los delitos en el ámbito digital, así como el manejo de datos personales por parte de entidades tanto del sector público como privado y una de las leyes más relevantes según el Congreso de la República de Colombia (2009), la Ley 1273 de 2009 establece medidas para la protección de la información y los datos; esta ley, modifica el Código Penal de Colombia al añadir un nuevo interés legal relacionado con la protección de la información y los datos, sancionando actos como el acceso indebido a sistemas informáticos, la interceptación de información digital, la utilización de programas maliciosos y la violación de la privacidad de datos personales y también toma en cuenta factores que pueden aumentar las penas cuando los delitos afectan a instituciones estatales, entidades del sector financiero o son cometidos por funcionarios públicos.

En lo que concierne a la salvaguarda de los datos personales, según la ley 1581 de 2012 (Congreso de la República de Colombia, 2012), conocida como la "ley estatutaria de protección de datos personales", tiene como objetivo promover el derecho esencial de las personas a acceder, actualizar y corregir los datos que se recopilan sobre ellas en bases de datos, así como asegurar demás derechos y libertades vinculados a la privacidad, buen nombre y libertad, aplicándose a la información personal que se guarda en bases de datos tanto de entidades públicas como privadas, tomando una mayor relevancia cuando el encargado del manejo de los datos se encuentra fuera del territorio nacional, pero está sujeto a normatividad nacional.

Según el Decreto 1377 de 2013 (Presidencia de la República de Colombia, 2013) complementa el marco de la Ley 1581 de 2012, pues establece regulaciones parciales a dicha ley y ofrece lineamientos sobre la autorización que debe otorgar el propietario de los datos, la

información de privacidad, así como definiciones de datos públicos, semiprivados y sensibles, detallando los procedimientos para que los titulares ejerzan sus derechos, estipulando que la recolección de datos debe limitarse a aquellos relevantes y adecuados para el propósito comunicado, requiriendo que esta recolección cuente con el consentimiento del titular, excepto en situaciones legítimas.

Otro aspecto relevante, tiene que ver con el sector financiero y comercial que está regido por una ley específica: la Ley 1266 de 2008 Congreso de la República de Colombia (2008), que condiciona normativamente el manejo de información en bases de datos financieras, créditos, comercio y servicios, así como la información que llega desde el exterior, con el objetivo de promover el derecho constitucional de hábeas data y en este campo particular, podemos resaltar que sus características más relevantes se encuentran el derecho de los propietarios de los datos a conocer, cambiar y corregir su información, además de la obligación de los gestores de bases de datos de garantizar la protección de estos derechos.

Congreso de la República de Colombia (2009), la Ley 1273 de 2009, en lo que respecta a las medidas punitivas relacionadas con los delitos cibernéticos, define varias acciones como ilegales, la cual incluye el acceso no permitido a sistemas de computación, la interrupción ilícita de sistemas informáticos o redes de comunicación, la captura de datos en espacios digitales, el deterioro de sistemas informáticos, el uso de software malicioso, la explotación de información personal de terceros, la creación de sitios web falsos para robar datos personales y la transferencia no autorizada de bienes mediante medios digitales, todas las consecuencias legales establecidas abarcan penas de cárcel y multas, las cuales cambian según la gravedad de la acción delictiva y las circunstancias que la agraven.

Todas estas normativas buscan asegurar la protección de la información personal, así como la integridad, accesibilidad y privacidad de los sistemas de información, reconociendo la existencia de un nuevo bien jurídico en el espacio digital: la información y los datos, puesto que se enfoca en resguardar los sistemas informáticos y la información que almacenan, alineándose con las leyes que protegen los datos personales, las cuales intentan ofrecer seguridad legal a quienes son dueños de esa información, haciendo parte del marco legal colombiano sobre delitos informáticos y la protección de datos personales.

Pentesting

En el ámbito de la ciberseguridad, las pruebas de penetración, comúnmente conocidas como pentesting,, IBM (s. f.) explica que son procedimientos metódicos orientados a evaluar la protección de sistemas, redes o aplicaciones mediante la simulación de ataques auténticos, propendiendo que los resultados de estas evaluaciones detecten vulnerabilidades antes de que puedan ser aprovechadas por tercero, lo que contribuye a la defensa de la organización asegurando un enfoque coherente y metódico, dividiendo en varias etapas, cada una con metas definidas, técnicas y elementos que facilitan su implementación.

La etapa inicial es la abarca recolección de información, donde el analista reúne la mayor cantidad de datos sobre un objetivo sin interactuar directamente, teniendo prioridad por la identificación de direcciones IP, dominios, correos electrónicos y otros servicios expuestos, componentes habituales que en esta fase son Whois, Jimeno García et al. (2008), permitiendo acceder a datos públicos de registro de dominios.

La segunda fase consiste en listar y escanear, realizando un examen minucioso de los sistemas para encontrar puertos abiertos, servicios que están disponibles y posibles fallas de seguridad, utilizando herramientas como Nmap, permitiendo identificar los dispositivos conectados a la red y brindando información detallada sobre sus servicios y versiones. También es común emplear Nessus, que facilita la identificación de vulnerabilidades conocidas y proporciona informes detallados sobre errores en la configuración.

La fase tres se centra en la explotación, IBM (s. f.) presenta que en la que el pentester se esfuerza por utilizar las vulnerabilidades identificadas para obtener acceso no autorizado al sistema; esta fase es fundamental porque su objetivo es demostrar la viabilidad de realizar un ataque real, destacando Metasploit como una herramienta muy utilizada, ya que proporciona un entorno adecuado para llevar a cabo exploits, crear sesiones remotas y desplegar cargas útiles controladas en el sistema que ha sido comprometido.

En la etapa de mantenimiento del acceso, se buscan estrategias para mantener la conexión y el control sobre el sistema comprometido de forma indetectable, con el propósito de emular cómo un atacante podría permanecer en ese entorno durante largos períodos sin ser detectado, empleando herramientas orientadas a la persistencia; en este sentido, Netcat se utiliza para establecer conexiones permanentes o túneles de comunicación entre el atacante y el sistema, comportamiento que se alinea con lo que menciona Alahmari y Duncan (2020) sobre las técnicas que permiten asegurar la continuidad del acceso en un entorno previamente comprometido.

Ya en la última etapa, correspondiente a la limpieza y la elaboración del informe, el pentester se encarga de eliminar cualquier rastro dejado durante la evaluación y de documentar en detalle los hallazgos, incluyendo las vulnerabilidades identificadas, la evidencia recopilada, el impacto potencial y las recomendaciones para su mitigación, conformando un documento

esencial para que las organizaciones reconozcan sus debilidades e implementen acciones correctivas, completando así el ciclo del pentesting, tal como señalan Salazar Mata et al. (2021) al describir la importancia de cerrar adecuadamente la fase final de estas evaluaciones.

Herramientas de Ciberseguridad

Las herramientas relacionadas con la ciberseguridad son cruciales y existen programas específicos que pueden ayudar en la labor diaria del profesional, es por eso que se hace necesario reconocer y definir las siguientes:

- Metasploit: Es un sistema modular y expandible destinado a realizar pruebas de penetración, que incluye exploits, cargas útiles, herramientas para la post-explotación y recursos para el diseño y ejecución de ataques controlados en sistemas, con el fin de validar vulnerabilidades y ser usado tanto por expertos en seguridad como por investigadores, facilitando la automatización de la explotación, el lanzamiento de cargas útiles (como Meterpreter), la administración de sesiones y la recopilación de pruebas, siempre con un enfoque ético y actuando con permiso en situaciones de evaluación o prueba, tal como menciona Kerner (2019) al explicar las mejoras y características nuevas en Metasploit Framework 5. 0, orientadas a reforzar las prácticas de pruebas de seguridad.

- Nmap: Se trata de una herramienta accesible que se utiliza para investigar y auditar redes, trabaja haciendo accesible la detección de dispositivos activos, puertos abiertos, servicios y sus versiones, junto con información sobre el sistema operativo y demás elementos de la red mediante varias técnicas de escaneo, valorándose en las etapas de reconocimiento y recopilación de información en pruebas de penetración, pues traza la superficie de ataque e identifica los vectores de riesgo, como lo mencionan Machap y otros (2024), Nmap es útil tanto

para aprender como para llevar a cabo pruebas de seguridad. Es crucial utilizar Nmap solo en entornos donde se tenga permiso y con la autorización adecuada.

- OpenVas: Kejiou y Bekaroo (2022) indican que se trata de una herramienta de código abierto destinada a escanear vulnerabilidades, que permite detectar automáticamente fallos en sistemas, aplicaciones y servicios, disponiendo de una base de datos de chequeos (NVTs) y herramientas para programar y manejar escaneos, clasificar los resultados, así como generar informes detallados que priorizan las reparaciones necesarias, utilizándose principalmente en la etapa inicial durante pruebas de penetración, así como en revisiones de seguridad regulares, con el objetivo de identificar software desactualizado, configuraciones no seguras y vulnerabilidades. Un ejemplo de su uso se puede ver a través de la interfaz web Greenbone Security Assistant (GSA), en este sitio se debe crear un objetivo, elegir un perfil de escaneo como "Completo y rápido" y comenzar la tarea, al finalizar, GSA entrega un informe que especifica la gravedad, evidencias halladas y las sugerencias para implementar.
- ExploitDB: Es un repositorio público con enfoque Offensive Security que recopila exploits, proof-of-concepts (PoC), vulnerabilidades y recursos relacionados para dispositivos y sistemas que sirve como referencia para investigadores de seguridad que buscan ejemplos públicos de explotación para validar vulnerabilidades durante un pentest, logrando el uso de repositorios abiertos de conocimiento ofensivo que se alinea con los enfoques modernos de análisis del comportamiento de las amenazas descritos en estudios recientes sobre ciberseguridad cognitiva y aprendizaje automático (Khan et al., 2025), contando además de la interfaz web con búsquedas por producto, ofrece la utilidad searchsploit que permite buscar y recuperar exploits localmente desde la línea de comandos.

- CVE: Se trata de un sistema globalmente estandarizado para la identificación y clasificación de vulnerabilidades en seguridad, gestionado por MITRE Corporation con la colaboración de diversas agencias y entidades internacionales, que busca que cada vulnerabilidad documentada se le asigna un código único, como el CVE-2024-12345, lo que facilita su utilización en reportes, bases de datos y herramientas de análisis, con el objetivo de establecer un lenguaje común que permita a fabricantes e investigadores correlacionar vulnerabilidades de manera uniforme, sin discriminar la fuente o el producto afectado, señalando la necesidad de evolucionar hacia modelos más transparentes y descentralizados para la divulgación y gestión de vulnerabilidades, como lo plantean Amirov et al. (2025) en su propuesta basada en blockchain con permisos, procurando en el entorno del pentesting y la gestión de riesgos, resaltando la utilidad de los CVE para identificar las vulnerabilidades presentes en los sistemas analizados, así como para comprobar la disponibilidad de parches o soluciones de mitigación.

Configuración banco de Trabajo

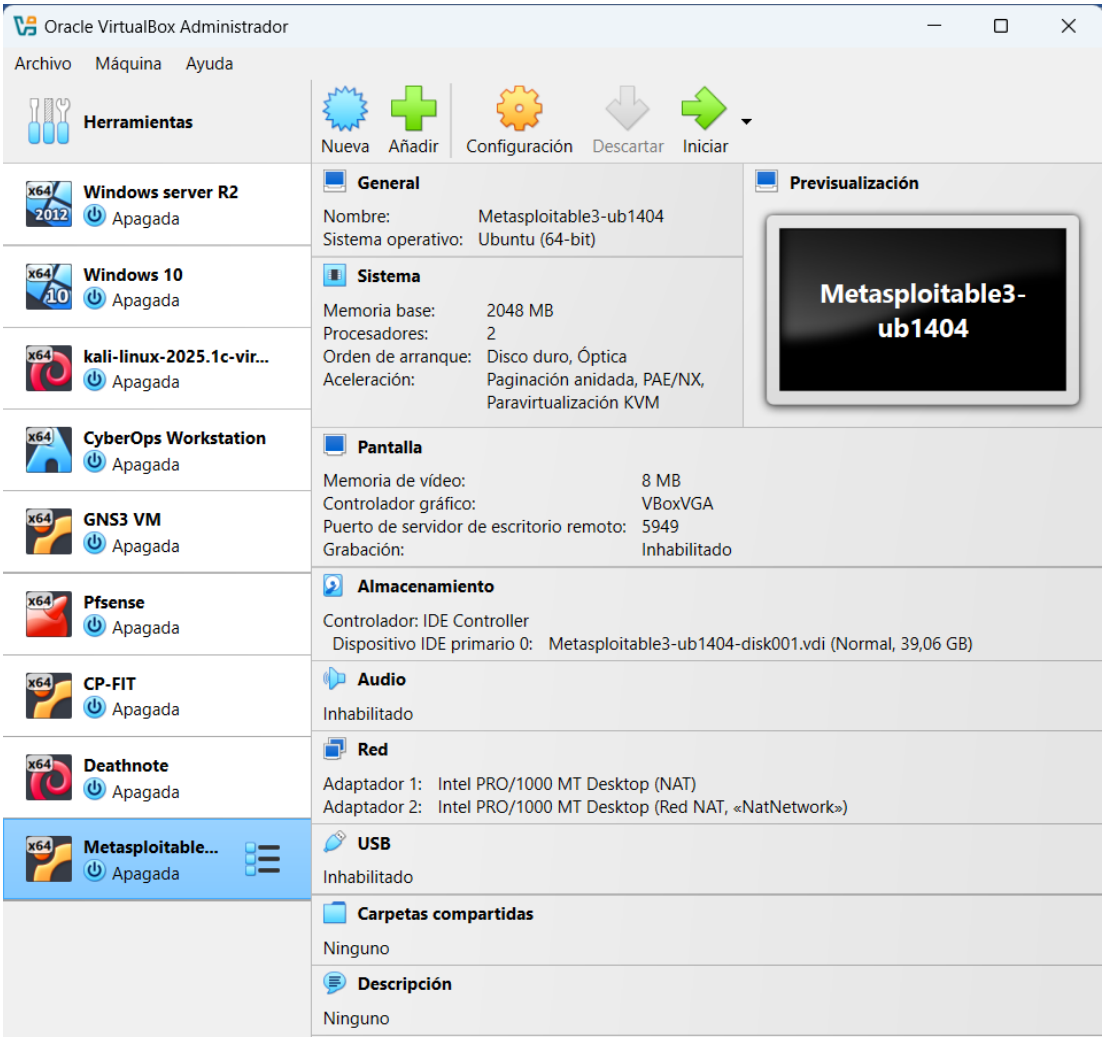
Una vez abordado el marco jurídico y los detalles de algunas herramientas importantes en el ámbito de la ciberseguridad, procederemos a configurar el banco de trabajo descargando la herramienta virtualizada, poniendo en marcha configuraciones iniciales y comprobando conexiones.

Es fundamental tener presente que, en la configuración que a continuación evidenciaremos, se resaltará la importancia de documentar cada paso del proceso, desde la instalación hasta la validación correcta de la operación, con el fin de mostrar los resultados y minimizar riesgos asociados a configuraciones o usos indebidos.

Es importante resaltar que se implementará un ejercicio simulado que pretende abordad principios básicos de ciberseguridad en torno al concepto de pivoting.

Figura 1

Instalación máquina virtual virtualbox

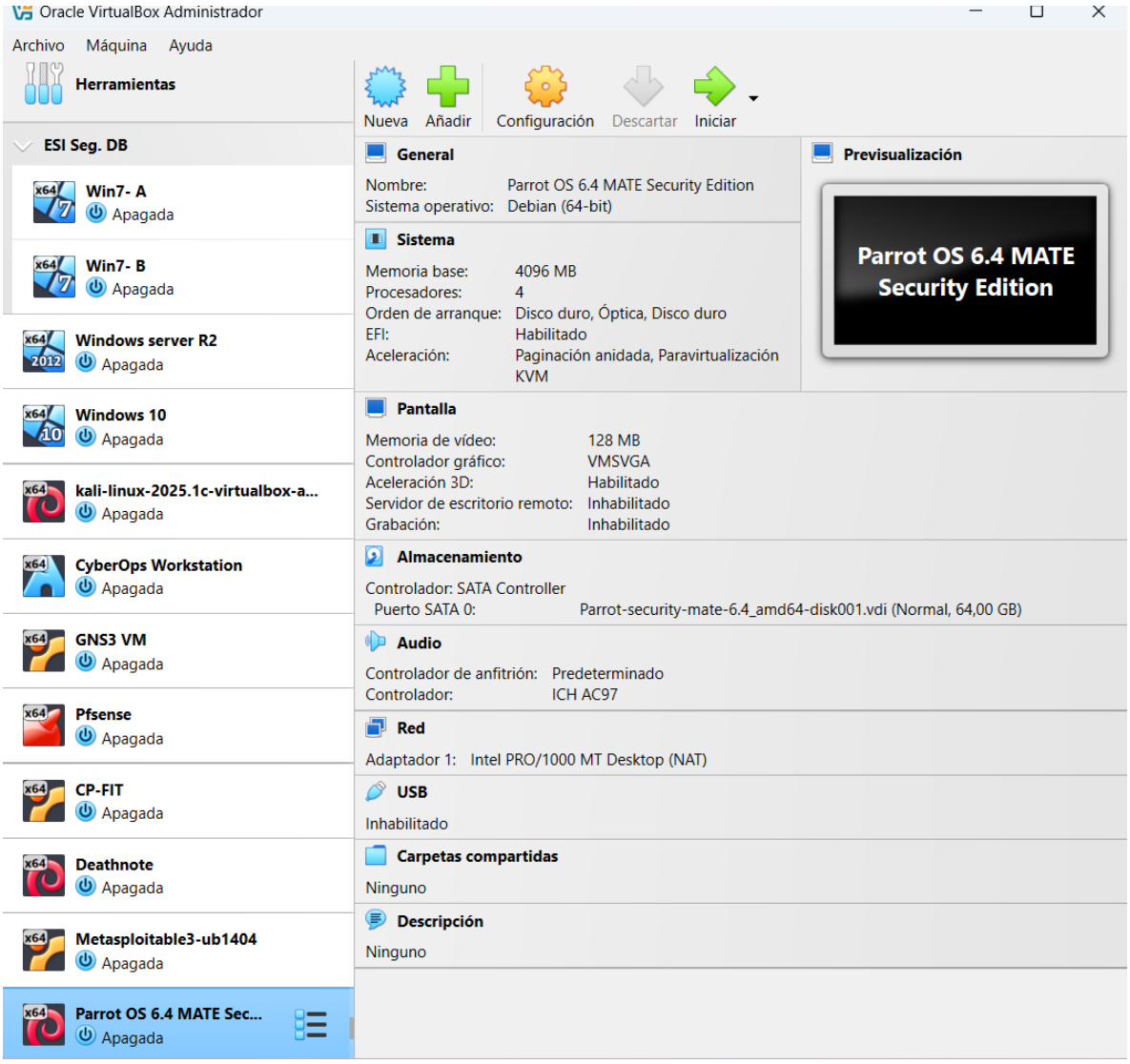


Fuente. Autoría Propia

Procedemos a instalar dos máquinas Windows A y B, OVA, sistema operativo Windows 7 (64 BIT) junto con Parrot OS 6.4; esta última se utilizará como escenario de ataque, en el que llevaremos a cabo el despliegue de instrucciones en el ejercicio de pivoting y pondremos en marcha las configuraciones y comandos necesarios que demuestren el desarrollo del ejercicio.

Figura 2

Sistemas operativos instalados

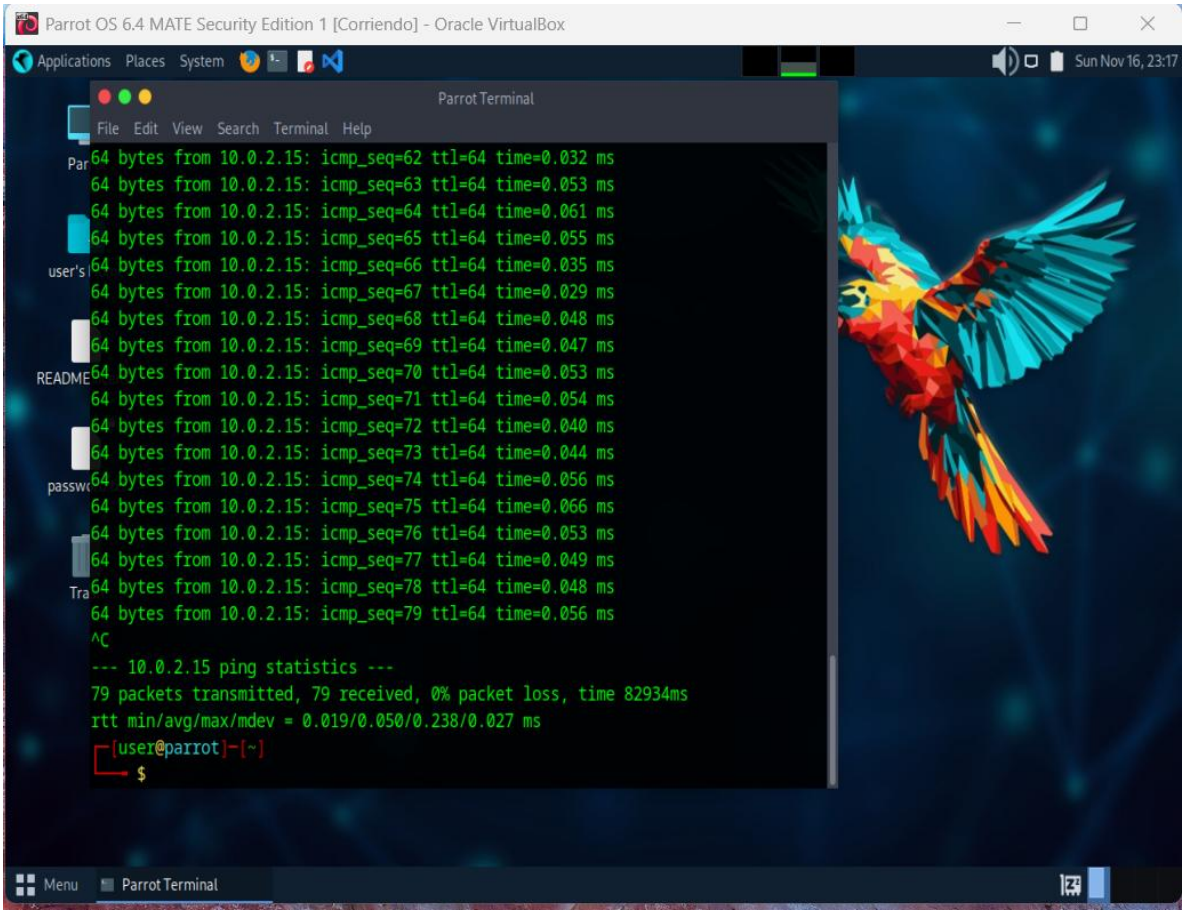


Fuente. Autoría Propia

Ponemos en marcha las máquinas y comprobamos conectividad:

Figura 3

Conexión parrot OS 6.4

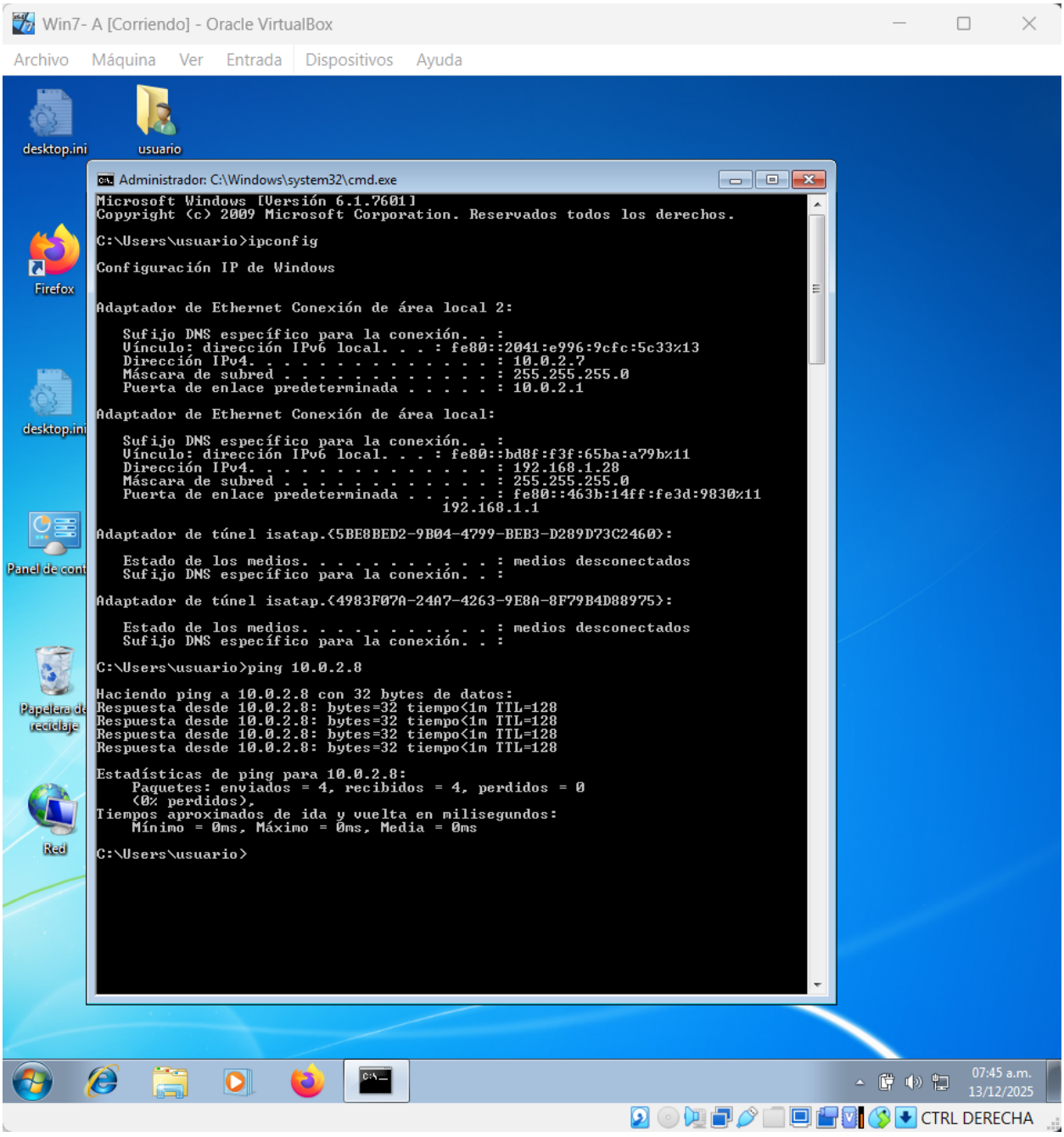


Fuente. Autoría Propia

Ejecutamos Ipconfig y ping entre la máquina A y B y comprobamos conexión:

Figura 4

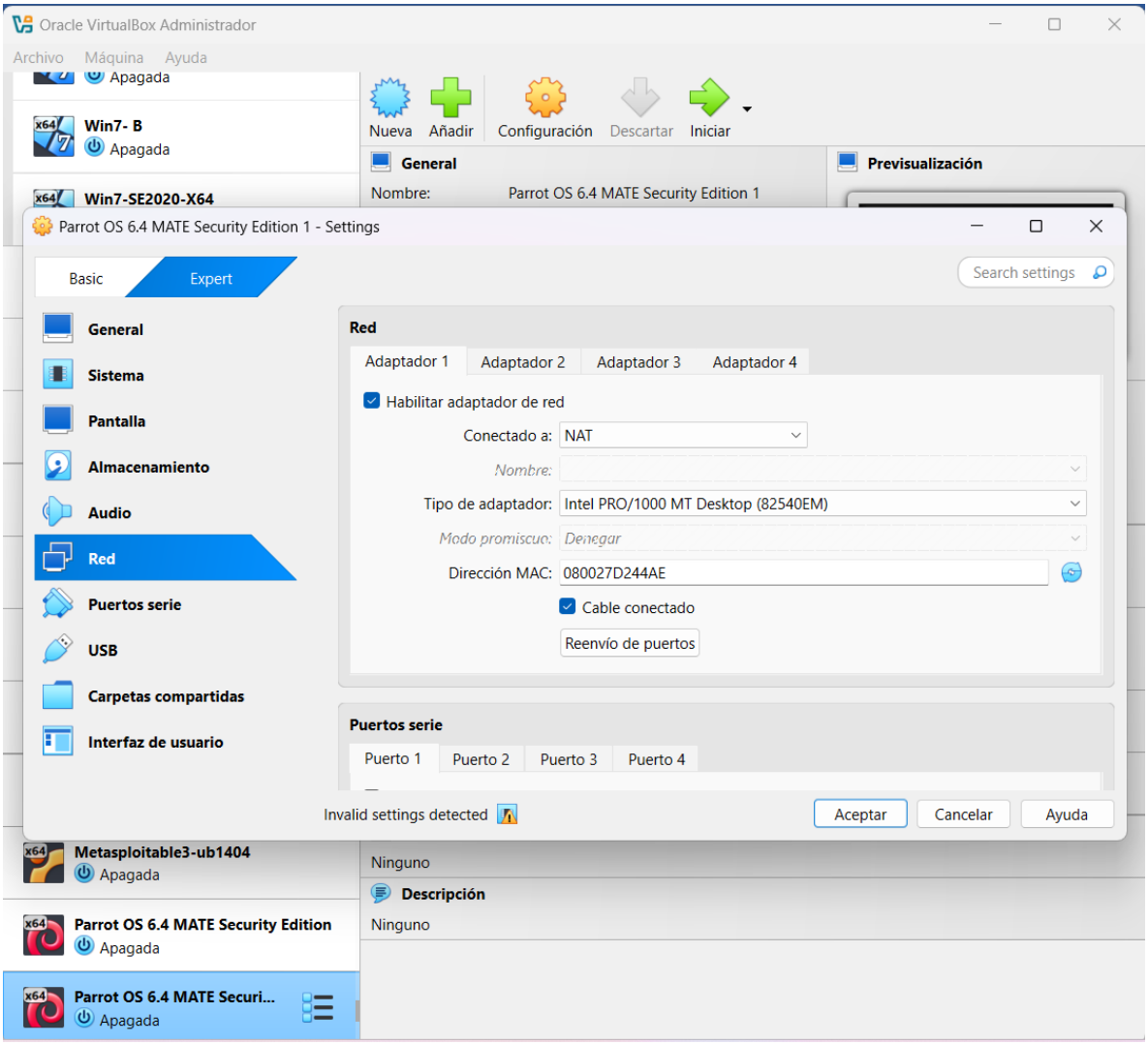
Conexión maquinas A y B Windows



Fuente. Autoría Propia

Figura 5

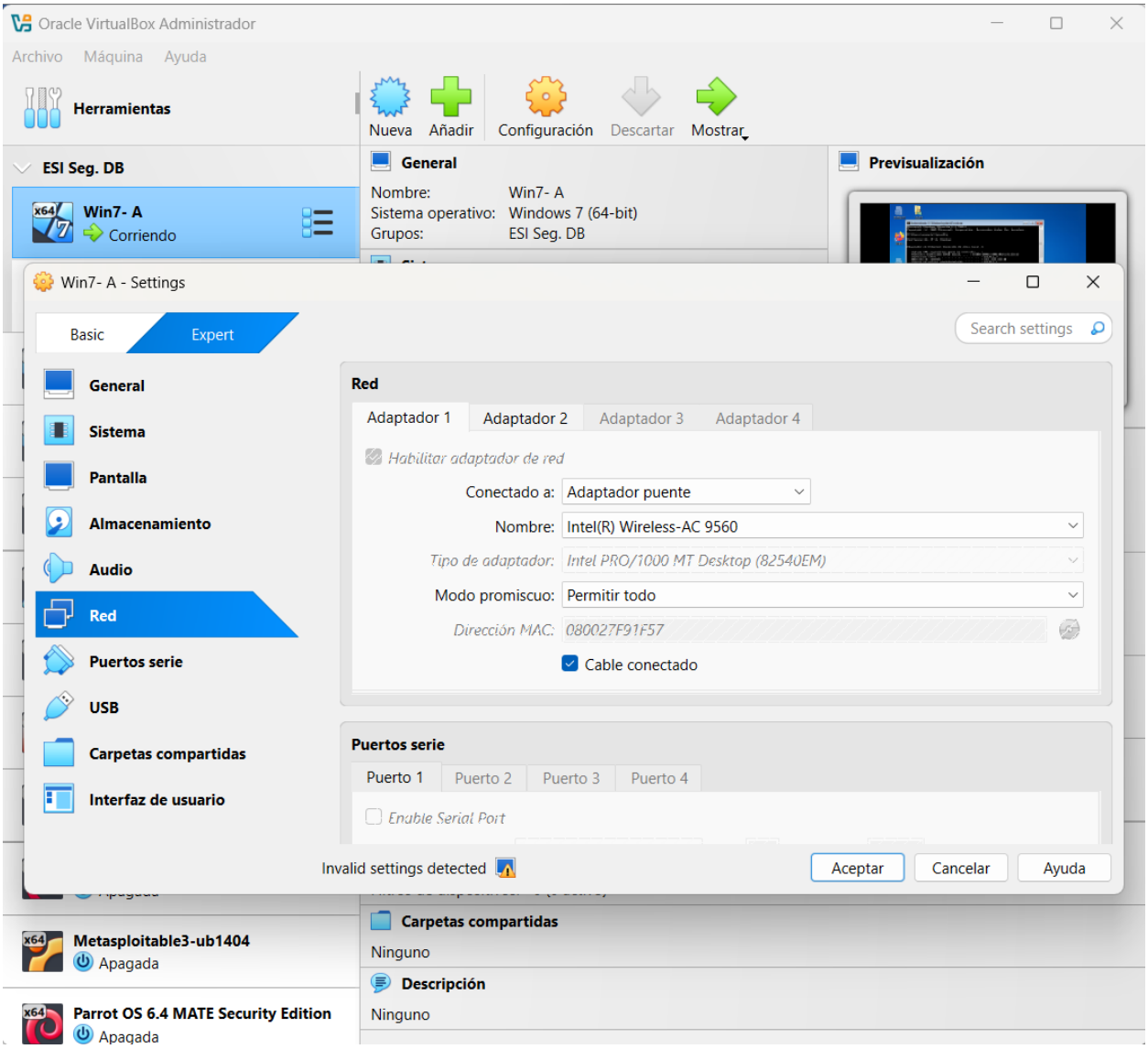
Configuración tarjeta de red máquina parrot



Fuente. Autoría Propia

Figura 6

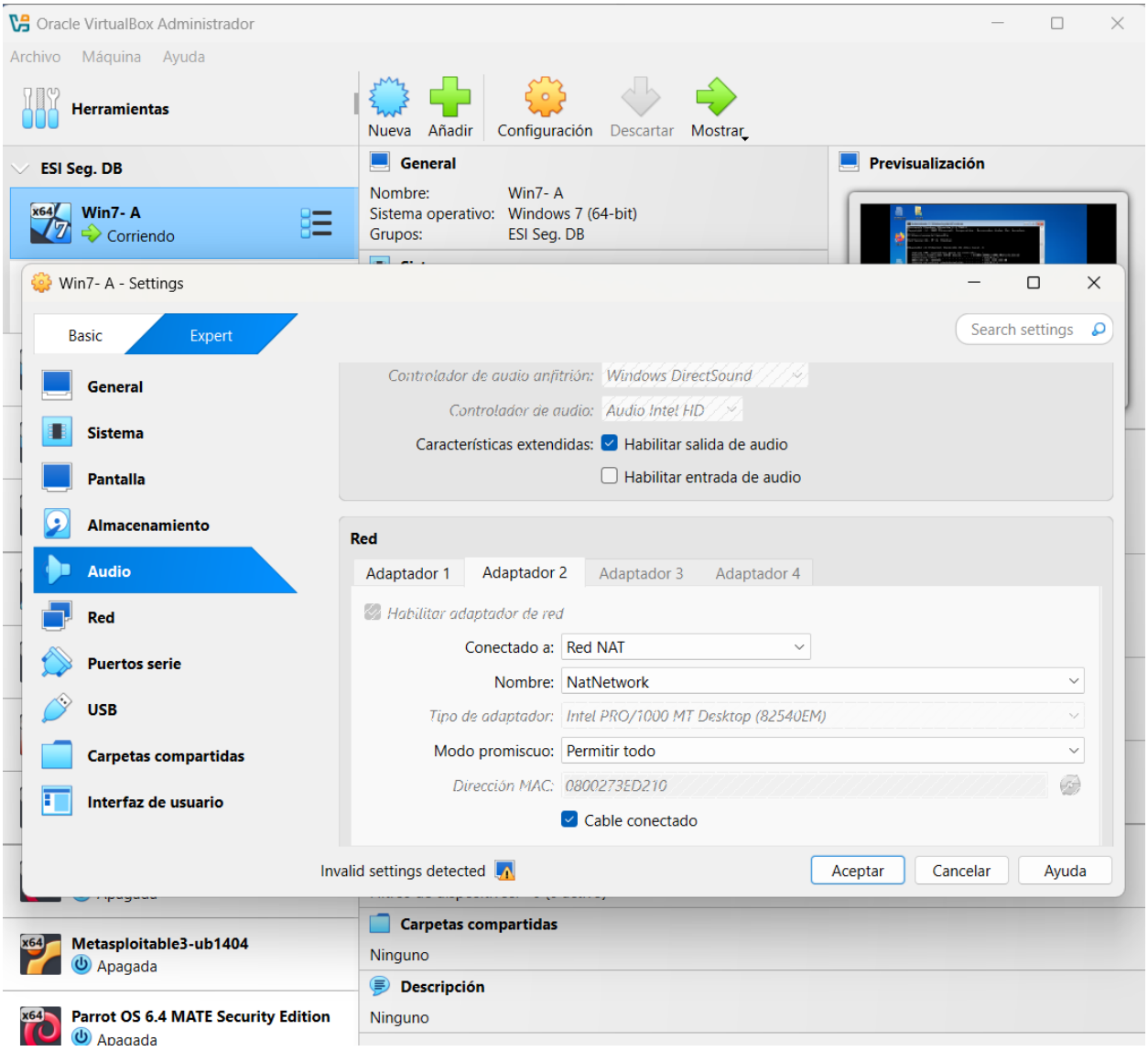
Configuración tarjeta de red (adaptador 1) máquina A windows



Fuente. Autoría Propia

Figura 7

Configuración tarjeta de red (adaptador 2) máquina A windows



Fuente. Autoría Propia

Tema 2 Escenario en el Marco de los Criterios Éticos y Legales

En este documento se escenifica una situación problema de la organización SecureNova Labs en la que se pretende reclutar talento humano para conformar los equipos de red team y blue team y para iniciar el proceso, la empresa da a los aspirantes un contrato y un acuerdo de confidencialidad, sin embargo, se evidencia que hay irregularidades y un margen poco ético en la gestión de datos sensibles, los cuales son:

- Que se entienda como información confidencial cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, datos secretos como “datos de chuzadas, interceptación de información, accesos abusivos a sistemas informáticos”.
- No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

Lo anteriormente expuesto nos lleva a desglosar nuevamente la Ley 1273 de 2009, “por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones”, norma que establece el marco penal para la protección de la información en Colombia y tipifica conductas relacionadas con el acceso abusivo, la interceptación de datos y los daños informáticos, tal como lo dispone el Congreso de la República de Colombia (2009).

Considerando lo anterior, y de acuerdo a esta ley, se estarían vulnerando los siguientes artículos:

- Artículo 269A: Acceso abusivo a un sistema informático.
- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

- Artículo 269C: Interceptación de datos informáticos.
- Artículo 269E: Uso de software malicioso (malware).
- Artículo 269F: Violación de datos personales.
- Artículo 269H: Hurto por medios informáticos y semejantes.
- Artículo 269I: Transferencia no consentida de activos.

Además, podría considerarse la omisión del deber de denuncia, toda vez que el artículo 441 del Código Penal colombiano tipifica el delito de "omisión de denuncia de particular", al establecer que, teniendo conocimiento de la comisión de un delito que deba perseguirse de oficio y no se denuncie ante la autoridad competente, incurrirá en sanción pecuniaria, conforme a lo dispuesto por el Congreso de la República de Colombia (2000).

De acuerdo con las condiciones previamente expuestas, como profesional en ciberseguridad considero que no sería pertinente aplicar a una vacante en SecureNova Labs en las condiciones mencionadas, puesto que, desde una perspectiva ética y profesional, implicaría renunciar a los principios fundamentales que he prometido respetar y que reflejan la integridad personal, pues estos valores, arraigados en la formación y los principios inculcados en el hogar, orientan el actuar y el compromiso con la responsabilidad y la rectitud en el ejercicio de la profesión.

Argumentando la respuesta, es importante citar la relevancia del Código de Ética para el ejercicio de la Ingeniería, el cual establece los principios y deberes que deben regir la actuación profesional, garantizando responsabilidad social, honestidad, la competencia técnica y el respeto por la ley en el ejercicio de la ingeniería y sus profesiones afines, conforme a lo dispuesto por el Consejo Profesional Nacional de Ingeniería (COPNIA, 2015).

Entre estos principios podemos destacar los de rectitud, probidad y honestidad consagrados para el ejercicio de la Ingeniería, invitando al profesional a desarrollar las prácticas de seguridad informática bajo criterios de legalidad, responsabilidad y transparencia, lo cual implica custodiar adecuadamente la información y los activos a cargo, evitar el uso indebido de estos, colaborar con las autoridades y órganos de control en el ejercicio de las funciones y denunciar cualquier delito, falta o contravención conocida en el marco de la ejecución profesional, enfatizando también en el deber de respetar y hacer respetar las disposiciones legales y reglamentarias aplicables, así como reportar sus transgresiones, reforzando la responsabilidad ética y legal del ingeniero en el manejo de la información y protección de sistemas tecnológicos, conforme a lo establecido por el Consejo Profesional Nacional de Ingeniería (COPNIA, 2015, arts. 31 y 35).

Durante una evaluación de seguridad, las empresas de ciberseguridad pueden necesitar acceder a información sensible de sus clientes, como configuraciones de red, bases de datos, contraseñas temporales o registros de actividad, ya que esta información es crucial para detectar vulnerabilidades, riesgos y sugerir métodos efectivos de mitigación, lo hace necesario que dicho acceso deba estar controlado rigurosamente mediante clausulas y políticas de privacidad que estipulen claramente el alcance, las restricciones y el propósito del uso de la información, así como los sistemas de supervisión y seguimiento todas las etapas del proceso, elementos que son esenciales para mantener la confianza entre el auditor y el cliente, tal como lo destacan Pina et al. (2024) al abordar las consideraciones éticas y de protección de datos en la gestión de información sensible.

Kostiuk et al. (2025) destacan que la efectividad de los controles de seguridad de la información depende en gran medida del uso adecuado de mecanismos de registro y supervisión, reflejándose en la necesidad de que las organizaciones establezcan controles técnicos, legales y éticos para evitar el mal uso de la información, incluyendo acuerdos de confidencialidad, clasificación del acceso según el rol, el registro y la supervisión de las actividades realizadas durante la auditoría, así como la eliminación segura de los datos una vez finalizado el proceso, conminando a que los profesionales involucrados actúen conforme al código de ética, fomentando el respeto por la privacidad de la información, de manera que solo a través de una gestión ética y controlada del acceso se garantice que las actividades de seguridad no se conviertan en un riesgo para la propia organización que está siendo auditada.

En Colombia, cuando se identifica que una empresa de ciberseguridad contratada ha estado involucrada en actividades de ciberespionaje, la respuesta institucional debe basarse, en primer lugar, en el marco penal que se establece con la Ley 1273 de 2009. Esta ley, como mencionamos antes, define los delitos informáticos y reconoce la información y los datos personales como bienes jurídicos protegidos, haciendo necesario llevar a cabo las acciones penales pertinentes por comportamientos como el acceso indebido o la violación de datos personales, de acuerdo con lo que se establecido por el Congreso de la República de Colombia (2009); complementariamente, deben intervenir las autoridades competentes, entre ellas la Fiscalía General de la Nación y la Policía Nacional a través del Centro Cibernético Policial, también la Superintendencia de Industria y Comercio cuando se vean comprometidos datos personales, en concordancia con lo establecido por la Ley 1581 de 2012 sobre protección de datos personales (Congreso de la República de Colombia, 2012), que en todo caso, resultaría indispensable suspender los contratos vigentes con la empresa involucrada, realizar auditorías

forenses independientes, adoptar medidas técnicas y administrativas orientadas a contener el incidente, previniendo una mayor filtración o uso indebido de la información afectada.

Para recuperar la confianza y asegurar que situaciones similares no vuelvan a ocurrir, las instancias administrativas correspondientes deben reforzar sus métodos de control, contratación y supervisión, de acuerdo con el Decreto 1377 de 2013, que es reglamentario de la Ley 1581 de 2012, así como las políticas que ha establecido el Ministerio de Tecnologías de la Información y las Comunicaciones en materia de seguridad digital, incluyendo recomendar y poner en marcha cláusulas de confidencialidad y sanciones por incumplimiento, exigir certificaciones de cumplimiento normativo y llevar a cabo procesos de auditoría regular conforme a la norma ISO/IEC 27001, resaltando de manera relevante, el fomento de la educación ética y la responsabilidad profesional en el campo de la ciberseguridad, ayudando a crear una cultura de integridad tecnológica, fortaleciendo la confianza en las instituciones y protegiendo los derechos digitales.

Tema 3 Hallazgo de Vulnerabilidades en un Sistema Informático mediante Técnicas de Intrusión

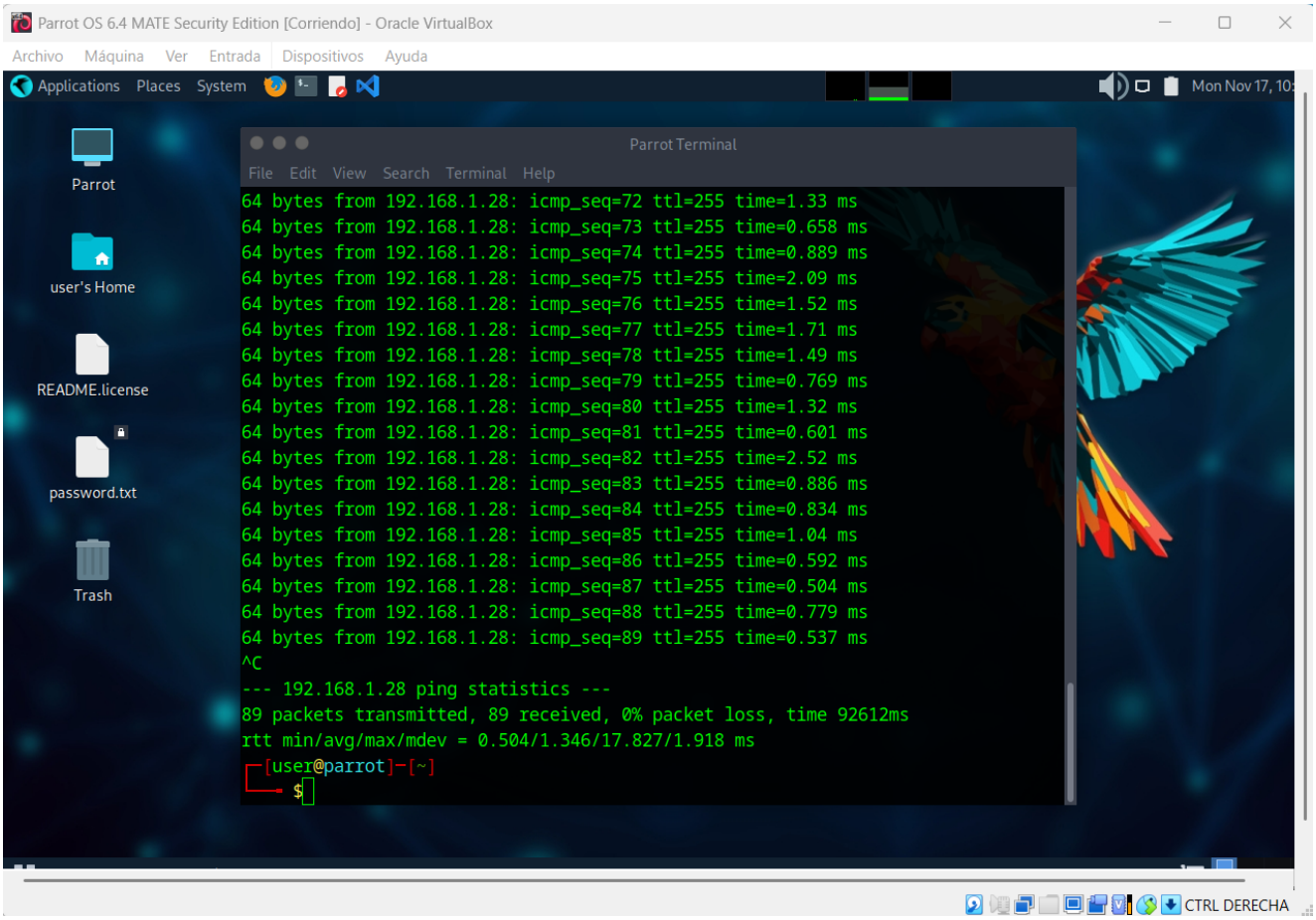
En esta etapa el análisis se centrará en torno a Host-A y Host-B ambos replicados en VirtualBox, junto con un host Parrot como entorno de trabajo y en el que identificaremos posible vector de fuga validando la explotación de una aplicación vulnerable, para confirmar un eventual escalamiento de privilegios y estudiar el movimiento lateral (pivoting), realizando la creación controlada de una cuenta administrativa en la imagen del Host-B, así como los criterios para la recolección de evidencias, la construcción del timeline forense y la formulación de recomendaciones, garantizando que todas las acciones sean documentadas y limitadas estrictamente al entorno autorizado.

Escenario de Prueba

Ejecutamos la máquina Parrot OS para verificar la conexión con el adaptador puente de la máquina Win7- A.

Figura 8

Conexión parrot OS a máquina Windows 7 A

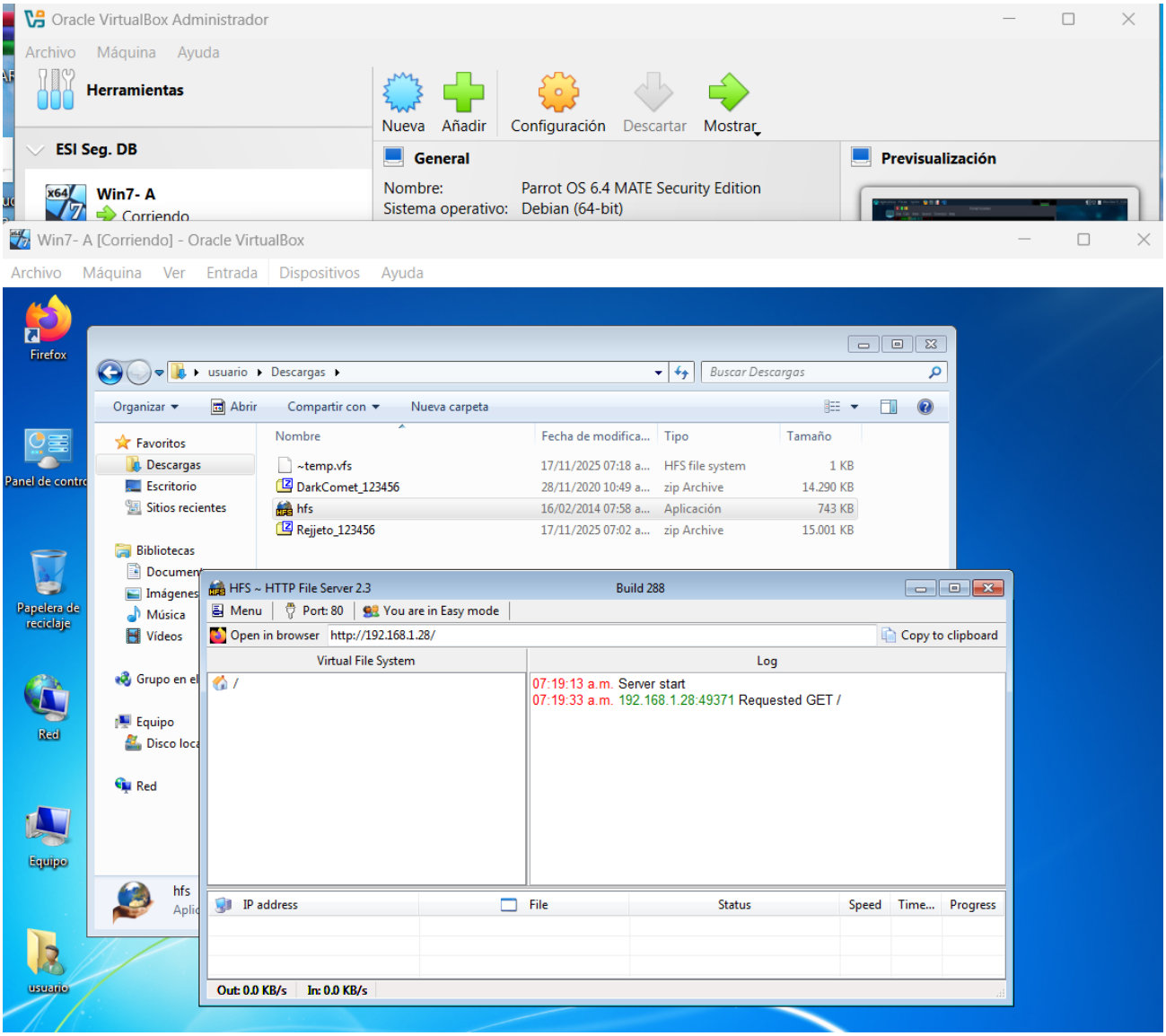


Fuente. Autoría Propia

Posteriormente volvemos al Win 7 – A y descargamos la aplicación Rejetto

Figura 9

Instalación de aplicación Rejetto

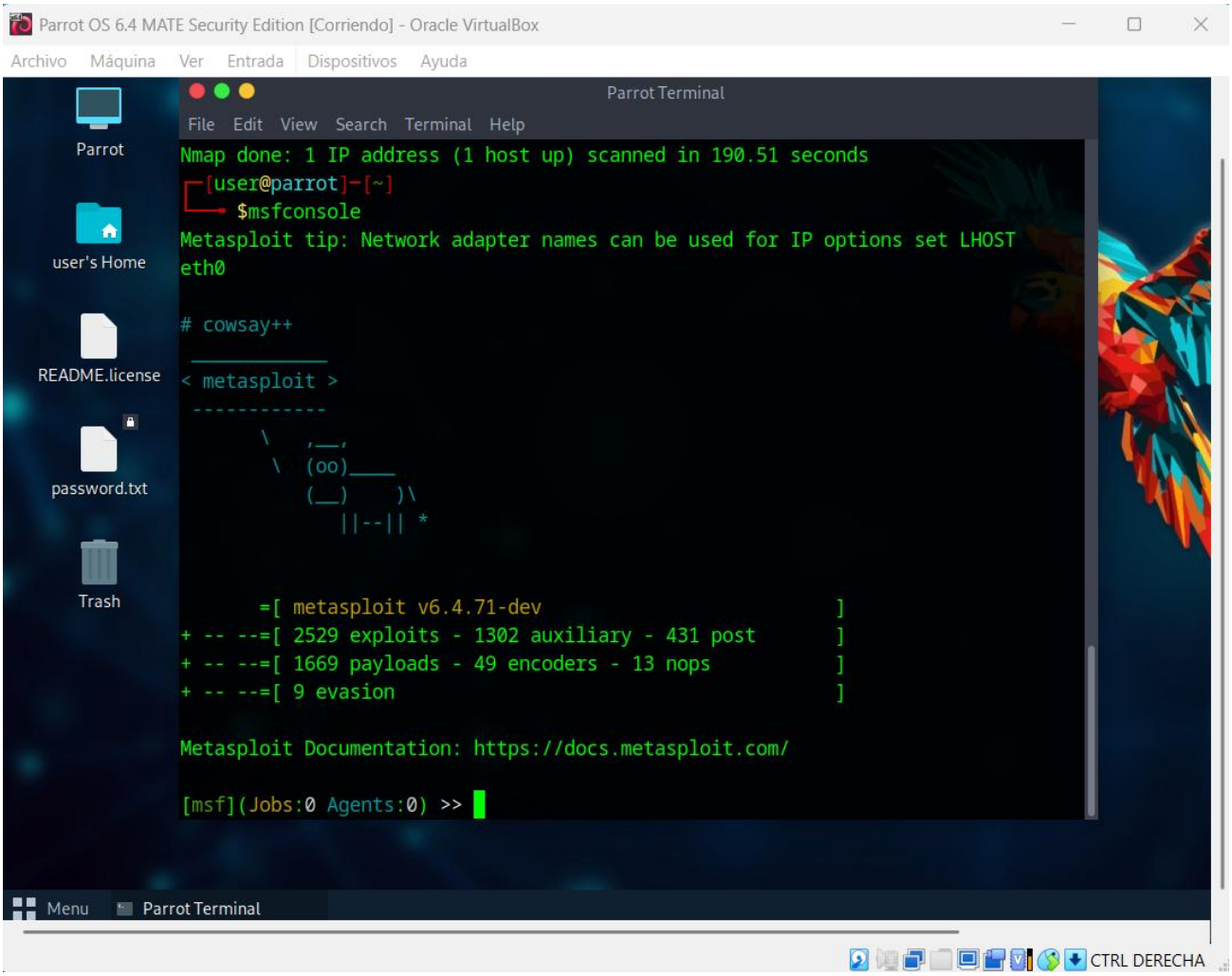


Fuente. Autoría Propia

Posteriormente nos dirigimos al host Parrot OS y ejecutamos msfconsole para poner en marcha la tarea de análisis.

Figura 10

Msfconsole



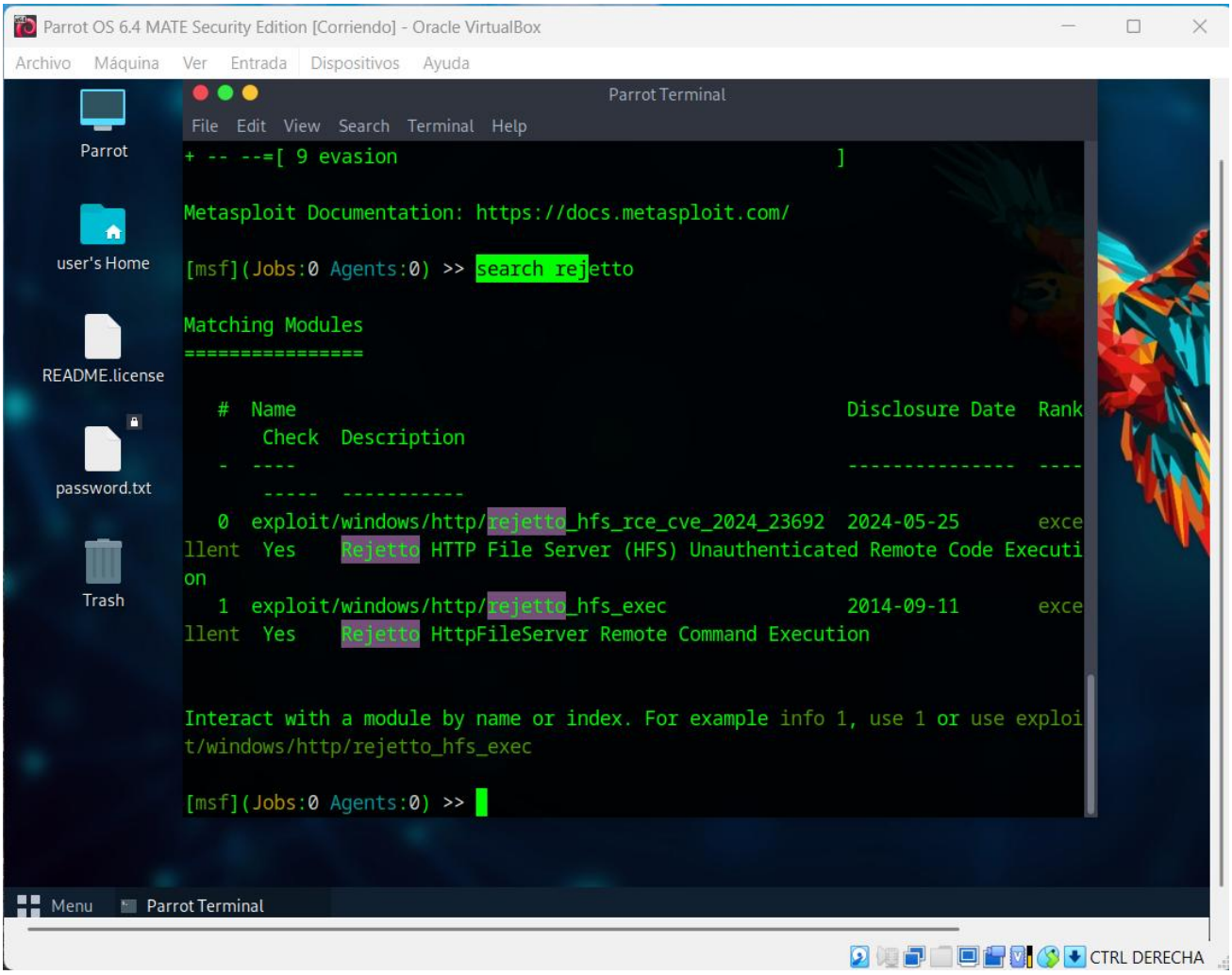
Fuente. Autoría Propia

Exploramos el aplicativo rejetto con el fin de que nos arroje las vulnerabilidades del servicio, a través del comando:

Search rejetto

Figura 11

Search rejetto

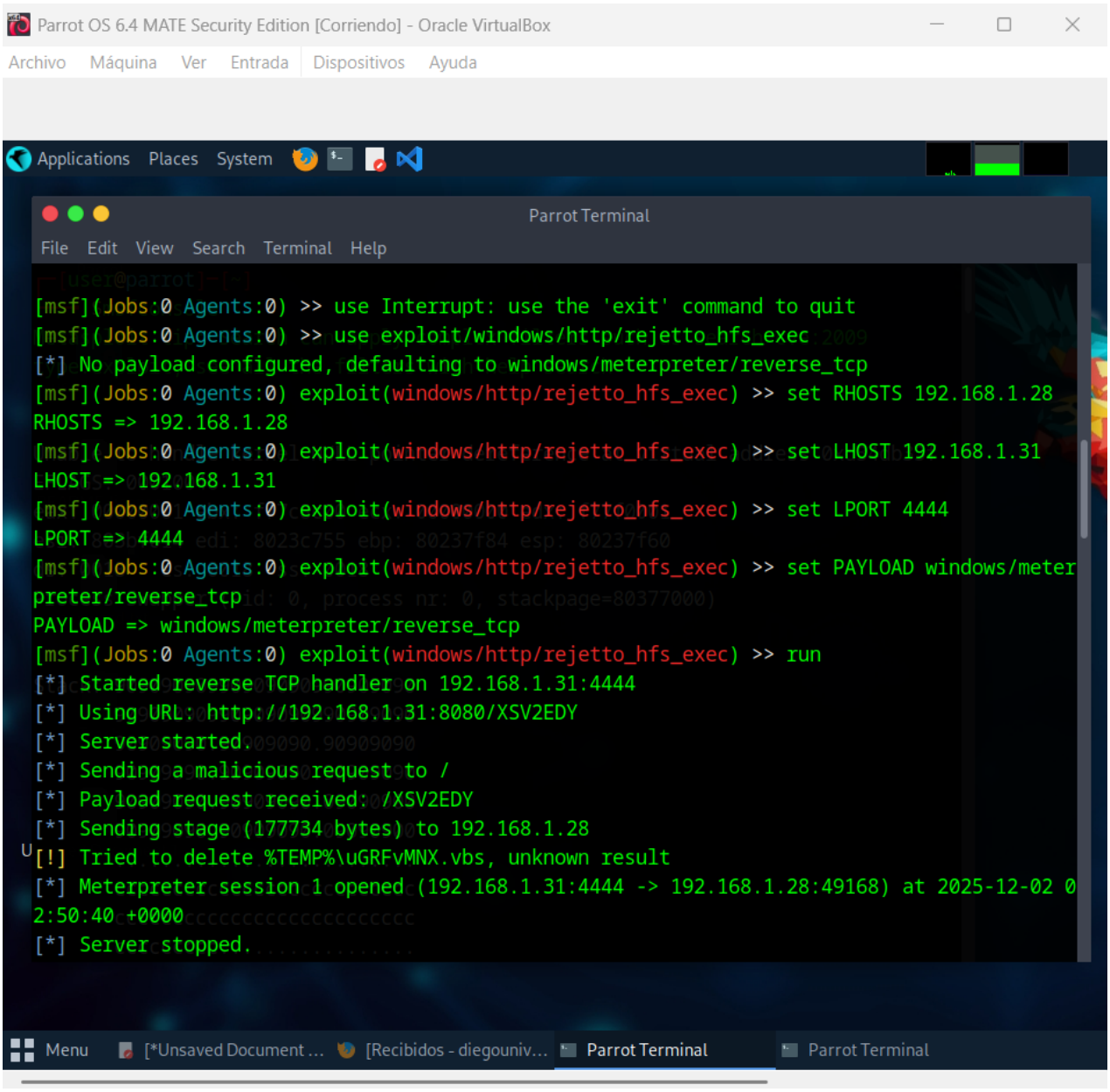


Fuente. Autoría Propia

Usamos la vulnerabilidad 1: use exploit/Windows/http/rejetto_hsfs_exe, fijamos IP local y remota, fijamos puertos local y remoto, fijamos PAYLOAD y ejecutamos utilizando el comando run:

Figura 12

Vulnerabilidad 1

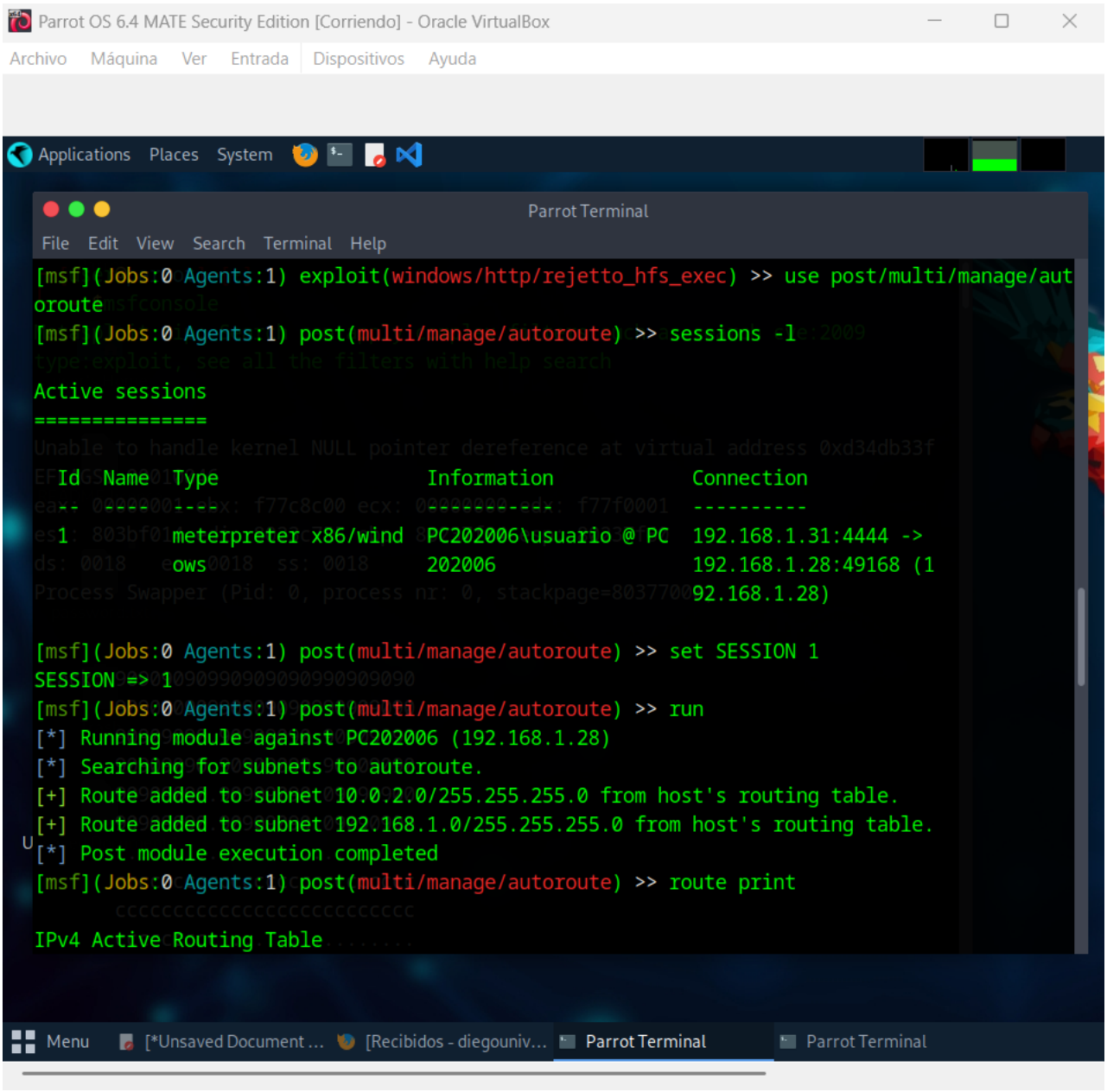


Fuente. Autoría Propia

Utilizamos el comando autoroute para enrutar la red:

Figura 13

Autoroute

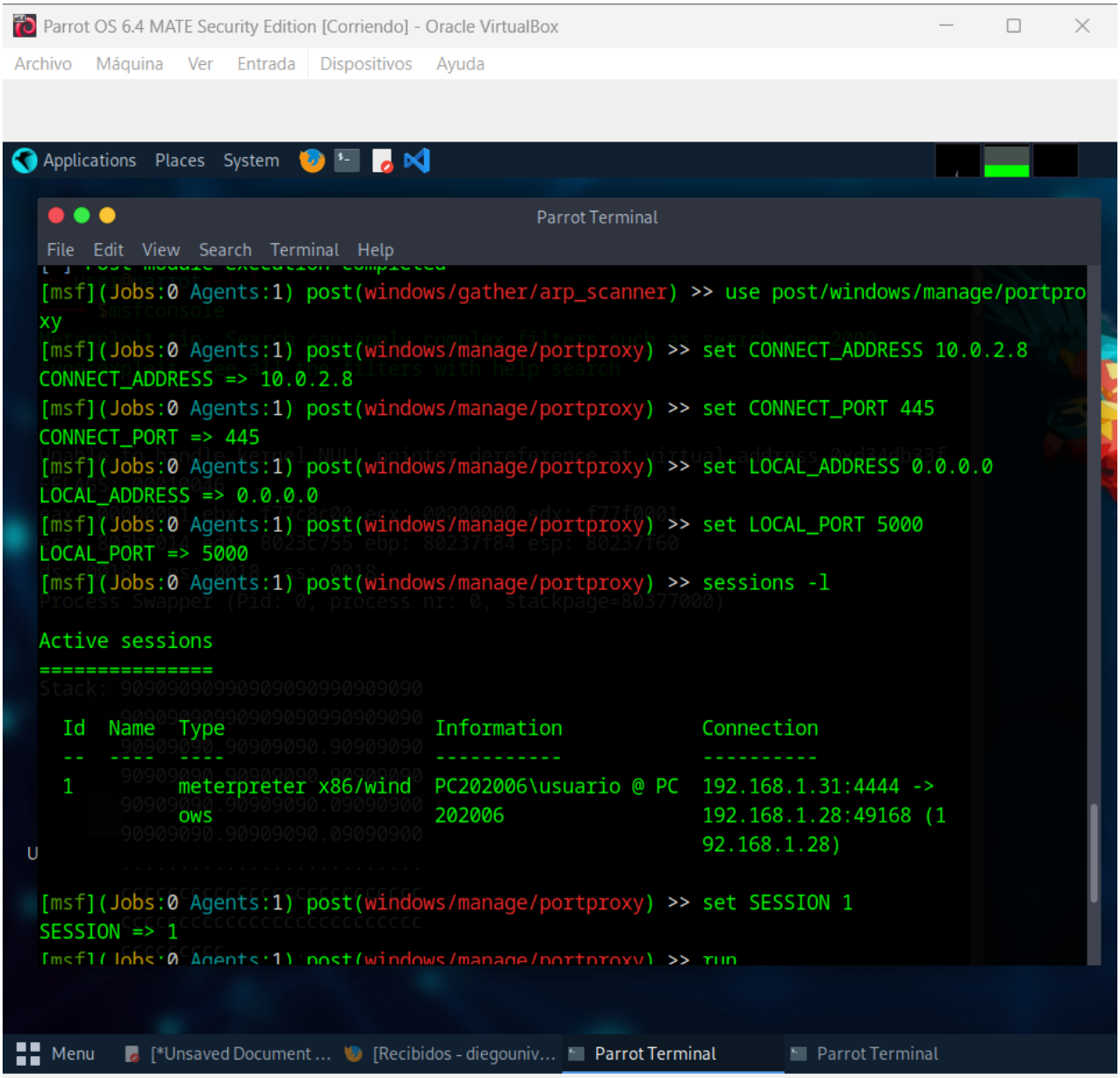


Fuente. Autoría Propia

A continuación, utilizamos el comando portproxy para asegurarnos una ruta al host B

Figura 14

Portproxy

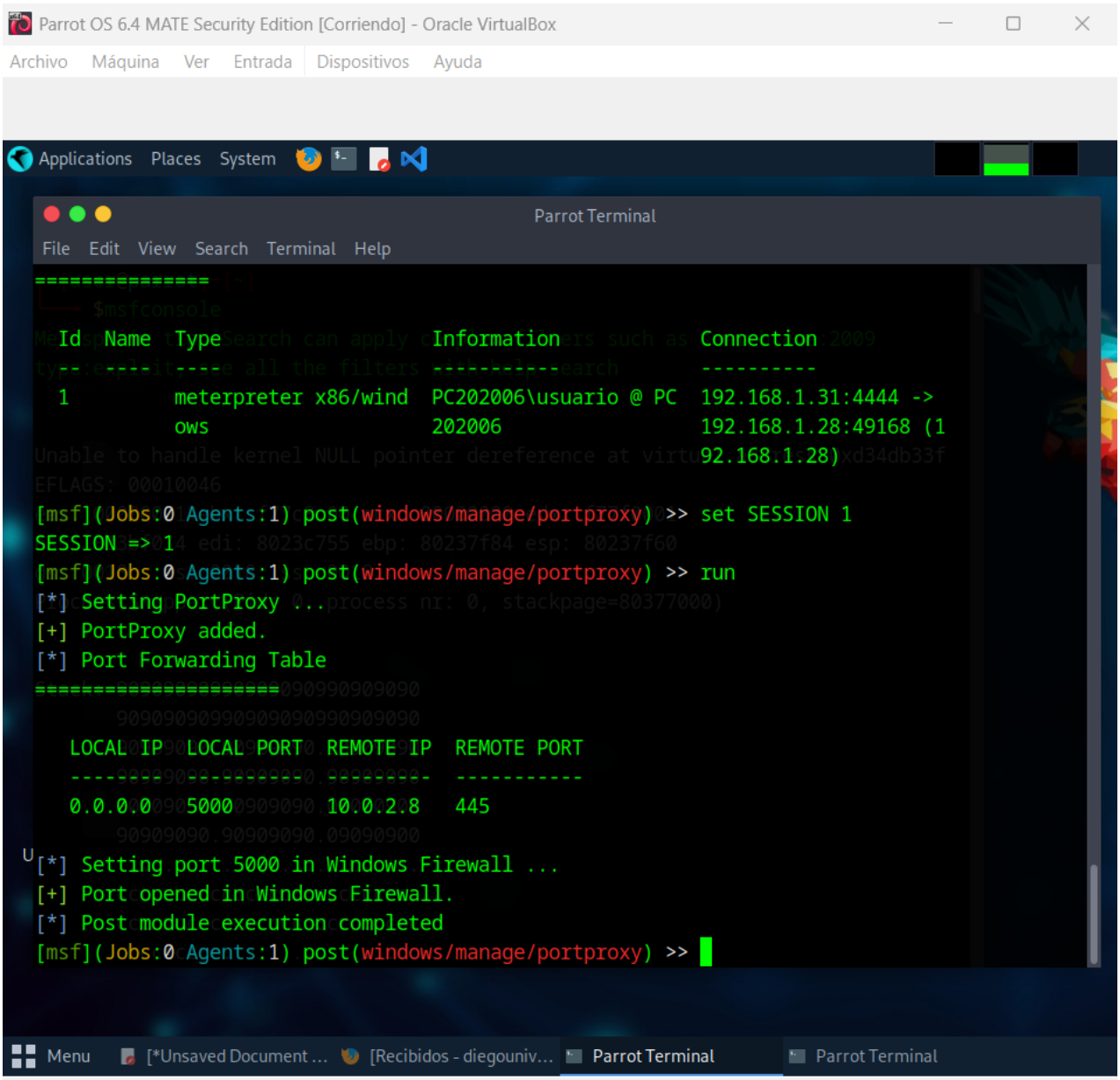


Fuente. Autoría Propia

Logrando la sesión en el host B.

Figura 15

Sesión host B

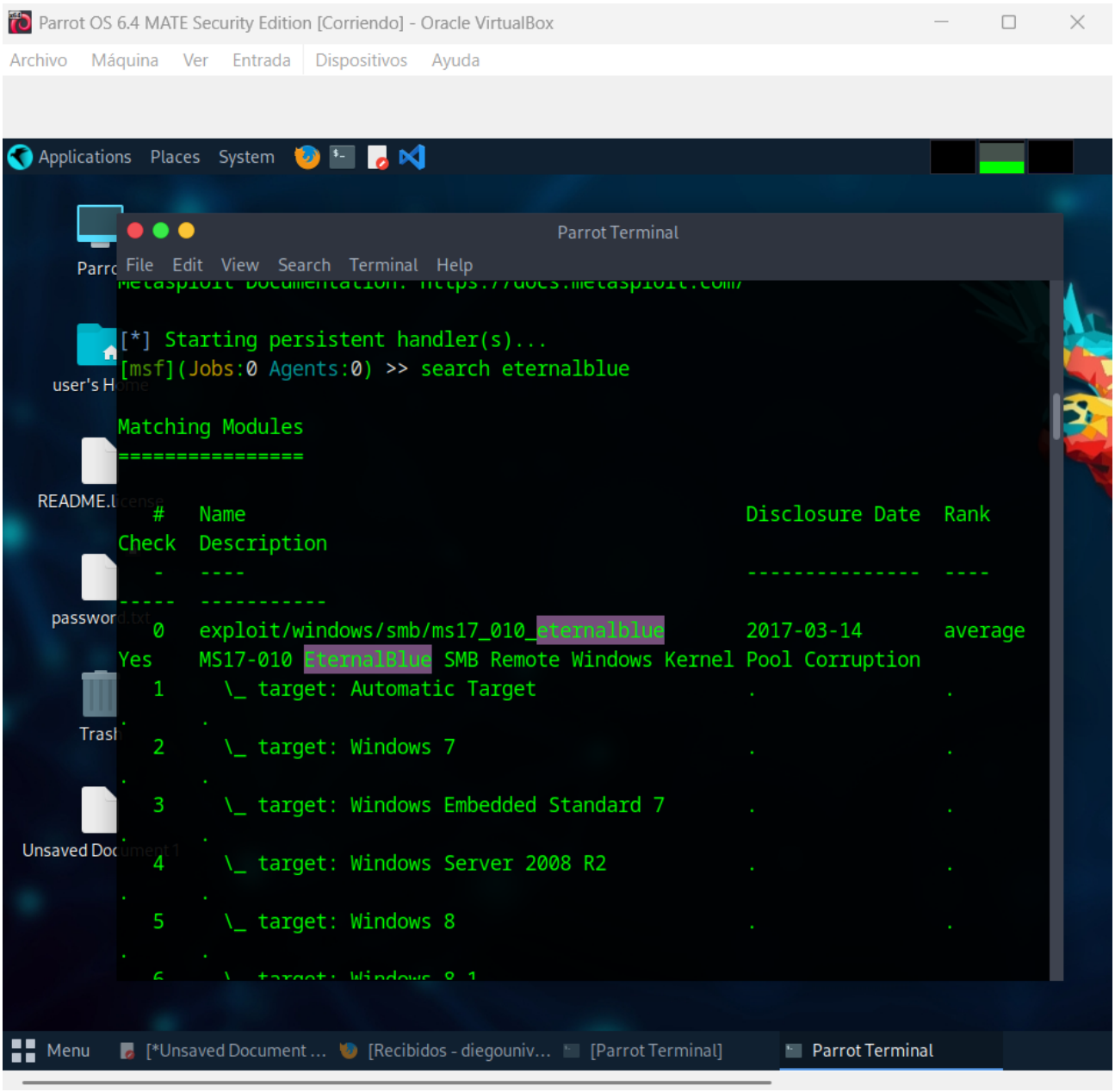


Fuente. Autoría Propia

Por otro lado, abrimos otra ventana de comando y ejecutamos msfconsole y desplegamos Search eternalblue

Figura 16

Search eternalblue

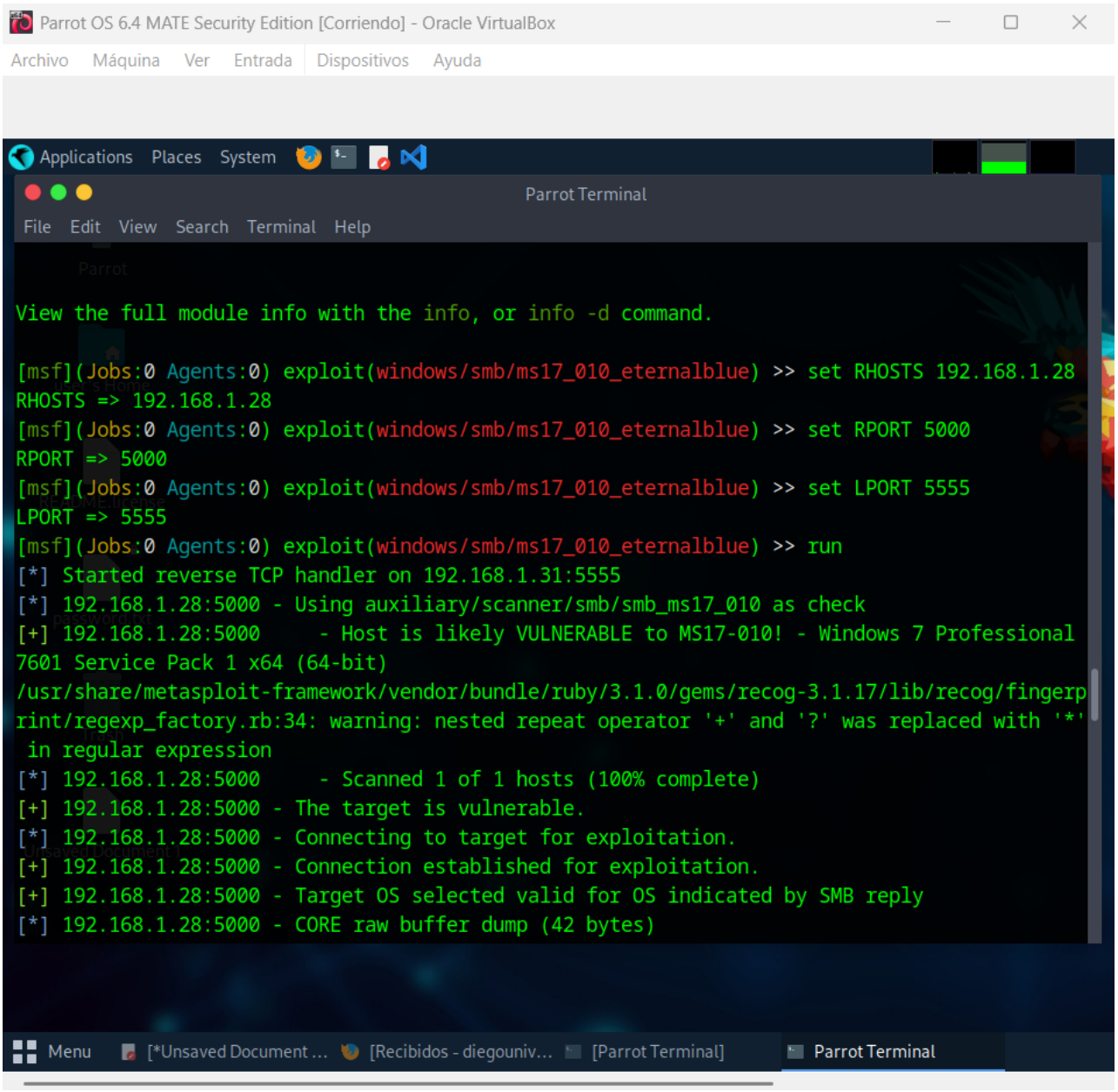


Fuente. Autoría Propia

Utilizamos use exploit/Windows/smb/ms17_010_eternalblue, fijamos los puertos y ejecutamos.

Figura 17

Exploit eternalblue

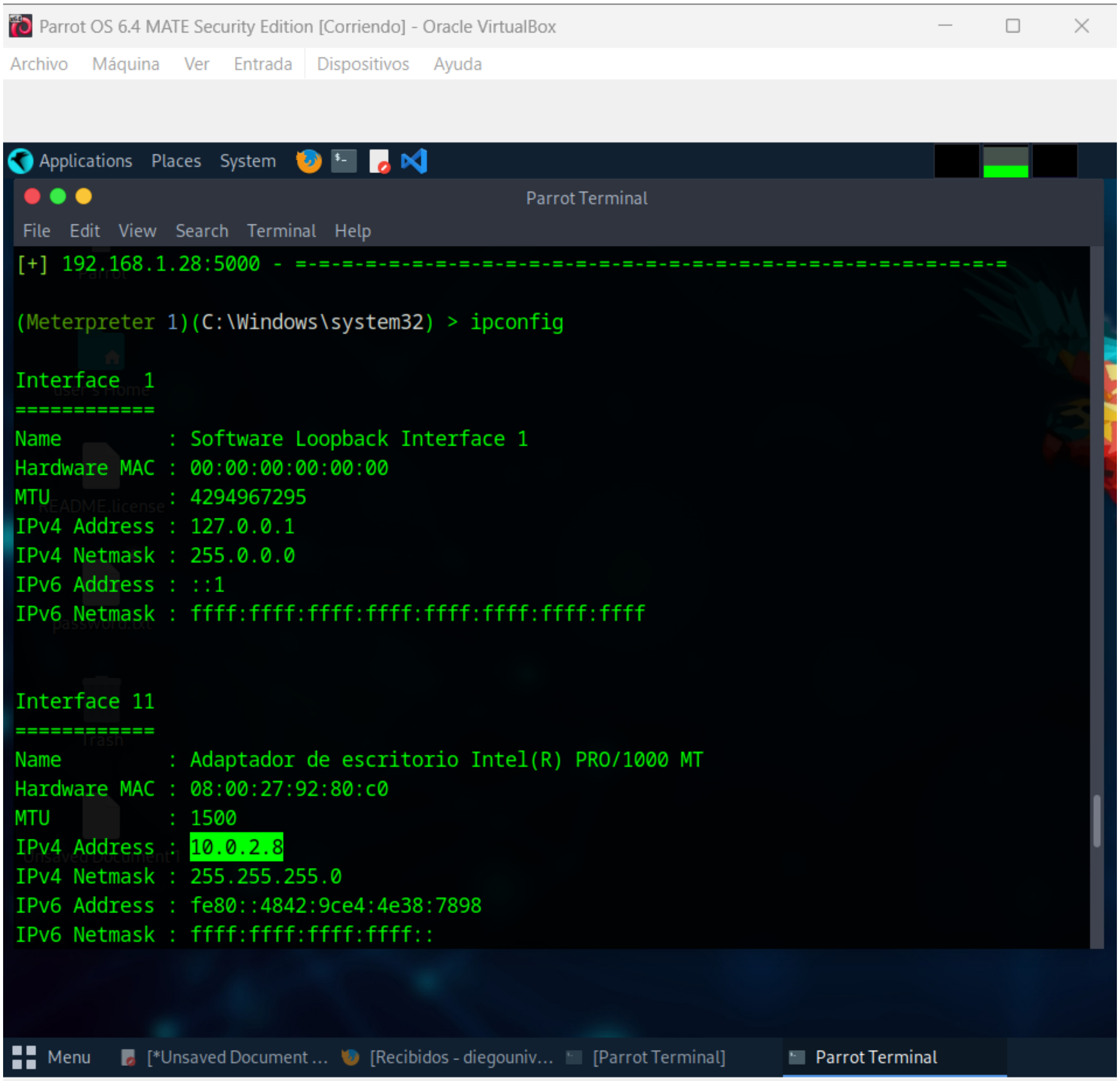


Fuente. Autoría Propia

Para comprobar nuestro ingreso al host B ejecutamos ipconfig y verificamos la ip:

Figura 18

Ipconfig host B

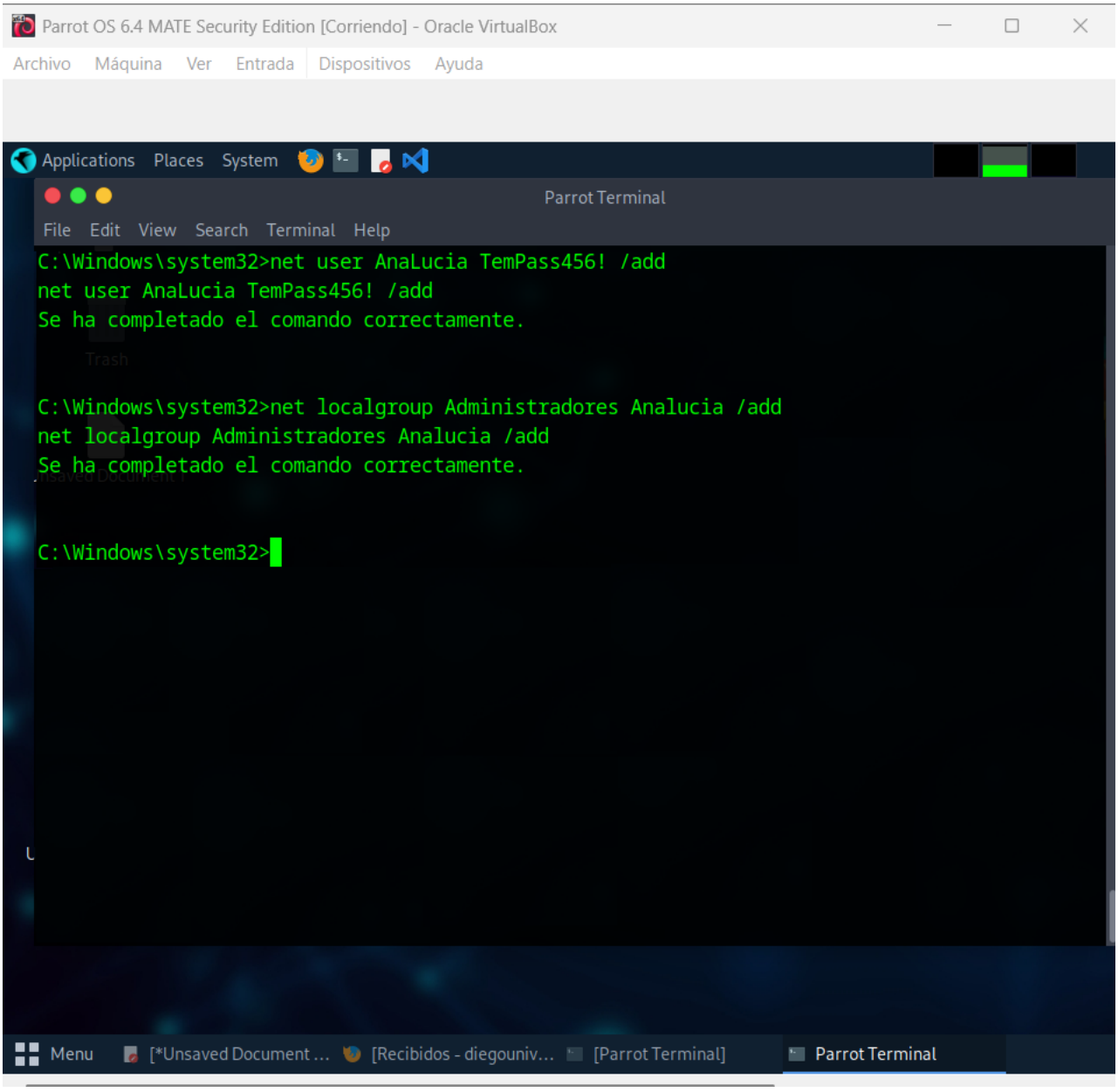


Fuente. Autoría Propia

Ejecutamos el comando net user para crear el usuario:

Figura 19

Net user host B

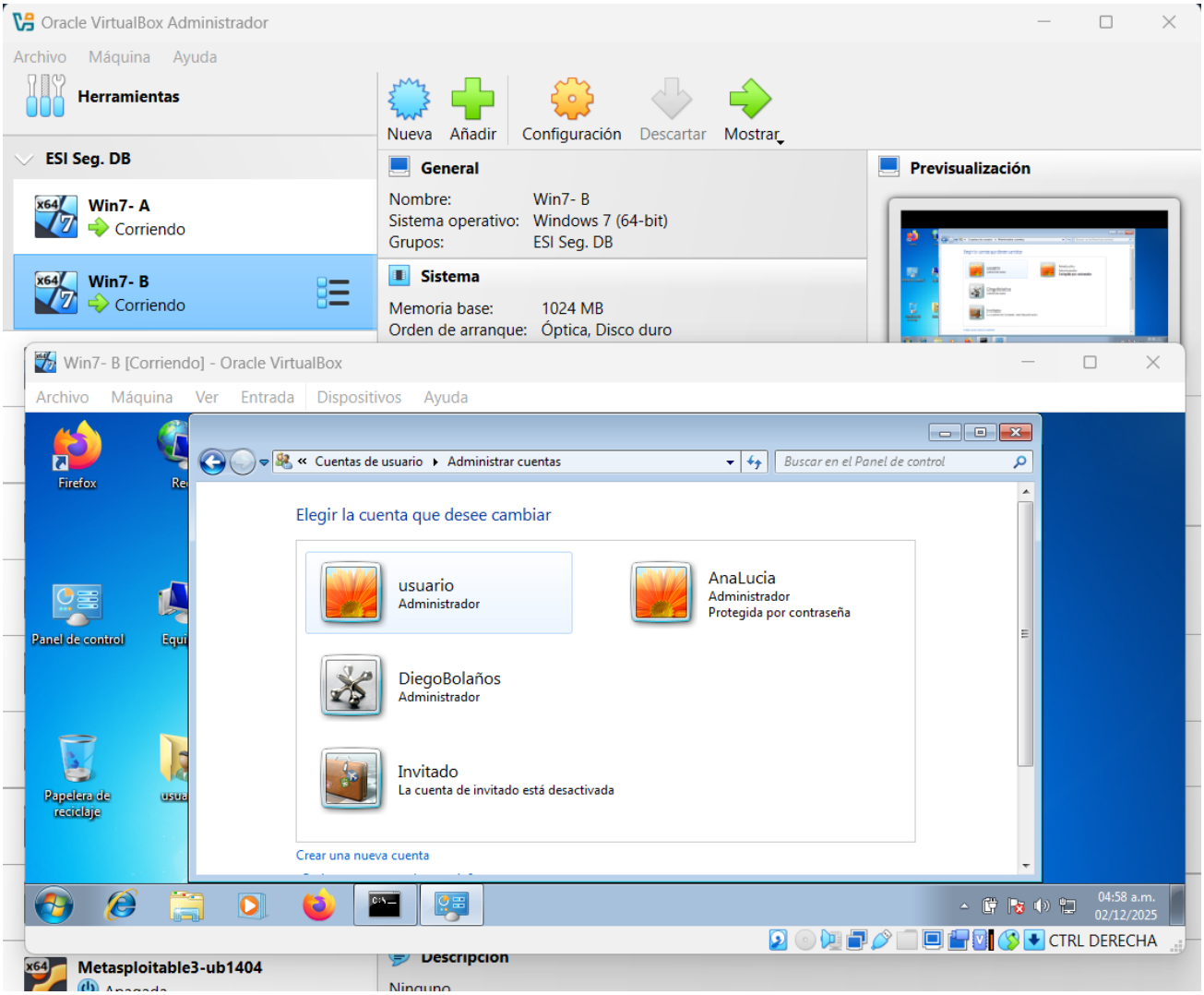


Fuente. Autoría Propia

Y evidenciamos en el host B la creación del usuario, designado como administrador:

Figura 20

Evidencia usuario host B



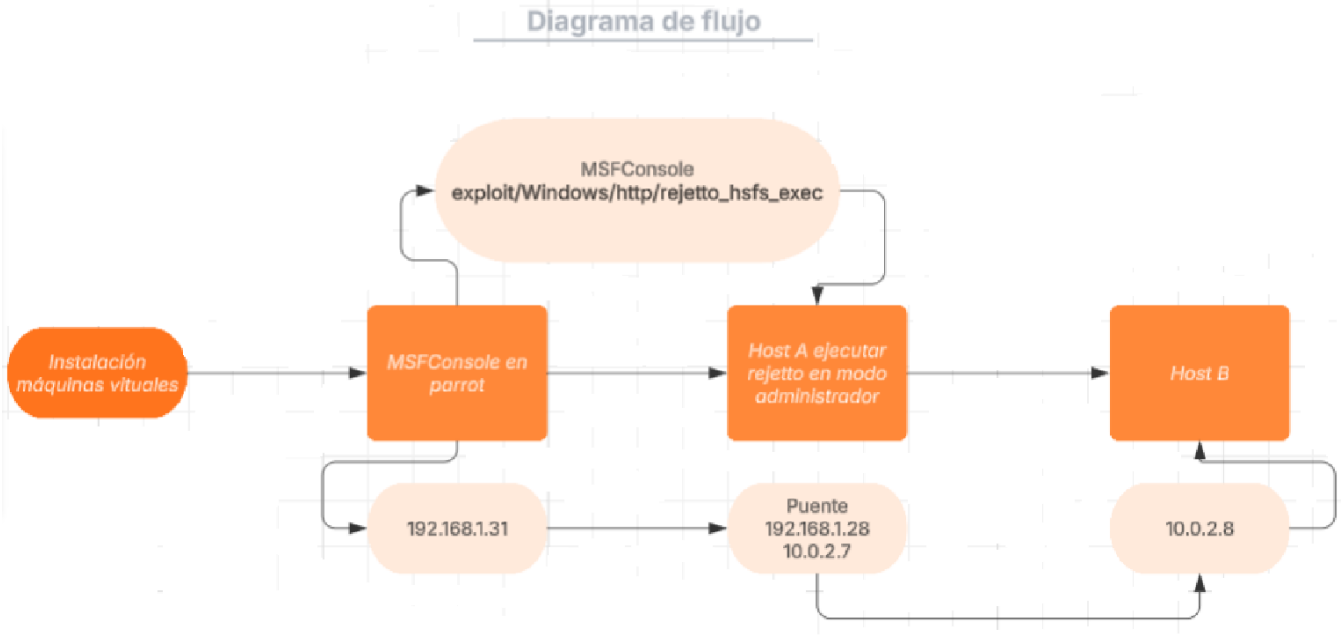
Fuente. Autoría Propia

Es fundamental que se describa la ejecución de la aplicación, ya que a través del software Rejetto se escalaron privilegios al host A para que fueran ejecutados en el escenario descrito y debido al escalamiento de privilegios, se logra crear un usuario en el host B, determinando el vector de fuga.

A través de MSFConsole se dio búsqueda con el comando search a las vulnerabilidades listadas para el aplicativo Rejetto, resultando use exploit/Windows/http/rejetto_hsfs_exec y fijando el puerto LHOST 4444 para el HOST A en el ejercicio.

Figura 21

Diagrama de flujo



Fuente. Autoría Propia

El ataque compromete inicialmente las máquinas con sistema operativo Windows mediante la explotación del aplicativo Rejetto, lo que permite el acceso no autorizado a los servicios web que este ejecuta, partiendo de esta vulneración, se establece el primer host comprometido (Host A), desde el cual es posible escalar privilegios, permitiendo que la intrusión se extienda hacia la segunda máquina (host B) mediante técnicas de movimiento lateral (pivoting), aprovechando una vulnerabilidad del sistema Windows y utilizando un túnel previamente configurado, lo que finalmente permite la creación de un usuario no autorizado en la máquina objetivo.

Tema 4 Gestión y Contención de Incidentes de Seguridad

Ante el escenario presentado, lo primero que se debe indagar, en la principal tarea al manejar un incidente de seguridad en tiempo real es detener la amenaza, lo que significa desconectar el sistema de la red para evitar el movimiento lateral y la fuga de información, después, recolectar la evidencia volátil. (National Institute of Standards and Technology [NIST], 2012).

El segundo paso es realizar un escaneo profundo de procesos para identificar persistencias y capturar el tráfico de red en la LAN para evidenciar paquetes maliciosos, así mismo, iniciar el análisis forense de la memoria RAM para evaluar posibles procesos y detectar traza de código oculto (López Delgado, 2007).

Es por eso que dentro de las medidas de hardenización que se propone implementar son aquellas que buscan en primer lugar gestionar el acceso a la red, lo que significa una gestión administrativa con el proveedor de internet local, con el fin de evaluar la configuración de los equipos receptores de la señal y definir la segmentación interna de la LAN, seguido de la implementación de un proxy, que suponga un obstáculo para cualquier intento de incursión pues a través de él, se redefiniría el tráfico de la red optimizando los recursos y dedicando todo el flujo hacia los sitios preestablecidos y objeto de trabajo por parte de la organización.

De acuerdo a la planificación propuesta, es importante contar con equipos altamente preparados, como el Blue team y un equipo de respuesta a incidentes informáticos, teniendo en cuenta que el primero se encarga de diseñar y escenificar posibles amenazas, disponiendo de los recursos cotidianos para prever las posibles amenazas que podrían penetrar la estructura informática de la organización, mientras un equipo de incidentes informáticos es un grupo

reactivo ante situaciones presentadas, lo que equivale a maniobras de contención y estabilización operativa de los equipos con los que cuenta la organización.

Teniendo en cuenta lo anteriormente mencionado, se hace razonable conocer más de cerca los lineamientos del Center for Internet Security (CIS), estos pueden emplearse para implementar procesos de hardening que adopten los más altos estándares de seguridad, aplicando controles críticos orientados a la prevención de ciberataques, permitiendo la adopción sistemática de los CIS Benchmarks como referencia para el fortalecimiento de sistemas, se alinea con las prácticas descritas por H. A. P. y Sujatha (2024), quienes destacan su eficacia para reducir la superficie de ataque mediante configuraciones seguras y estandarizadas.

Es aquí donde es relevante conceptos como el SIEM Security Information and Event Management o Gestión de la Información y Eventos de Seguridad y Cinque, Cotroneo y Pecchia (2018) mencionan que esta herramienta, es crucial en el ámbito de la ciberseguridad, ya que unen principalmente dos tareas importantes: la Gestión de la Información de Seguridad y la Gestión de Eventos de Seguridad.

El objetivo principal de un SIEM es ofrecer una perspectiva fundamentada y conectada sobre la situación de seguridad de toda la infraestructura tecnológica de una organización, lo que ayuda en la detección precoz, la evaluación y la respuesta rápida frente a amenazas e incidentes de seguridad.

En relación a la recolección de datos, el SIEM reúne información de diversas fuentes de registros y eventos de seguridad a través de la red, incluyendo cortafuegos, enrutadores, servidores, sistemas de detección de intrusiones, antivirus, bases de datos y aplicaciones. Esta información se obtiene en su forma original y luego se normaliza y convierte para que pueda ser analizada de manera uniforme y comparativa.

En lo que respecta al análisis, el sistema utiliza reglas de correlación para descubrir patrones y conexiones entre eventos que parecen aislados, identificando situaciones que de manera individual podrían parecer seguras, pero que en conjunto representan un peligro y para esto, se utilizan técnicas estadísticas y de detección de anomalías que ayudan a señalar comportamientos que se apartan de la actividad normal de la red.

Y en cuanto al monitoreo y la respuesta, cuando se detecta un comportamiento que viola alguna política o norma de seguridad, el SIEM emite alertas que pueden ser manejadas por el equipo Blue Team, facilitando la investigación forense, la creación de informes de cumplimiento y el análisis histórico de eventos, ya que guarda un registro central y permanente de los incidentes de seguridad.

Por otro lado, Tello Flores (2024) señala que la contención efectiva constituye un componente esencial en la respuesta ante incidentes de ciberseguridad, ya que permite minimizar el impacto del ataque y evitar su propagación dentro de la infraestructura tecnológica de la organización, resaltando la relevancia de los elementos de contención que pueden implementarse, dado que estos contribuyen directamente a reducir el efecto del incidente y a preservar la integridad de los sistemas, por lo tanto, es crucial destacar los principales mecanismos de contención que se pueden aplicar, entre los cuales se incluyen:

- Cortafuegos: Esta herramienta es fundamental para dividir la red según el tipo de tráfico, y tiene un papel importante en la contención de incidentes, permitiendo a los encargados de seguridad bloquear de inmediato el tráfico y aislar partes específicas de la red y en caso de un incidente, el equipo tiene la capacidad de ajustar las normas del cortafuegos para desconectar completamente una sección afectada del resto de la infraestructura, evitando que el intruso se desplace lateralmente.

- Herramientas de detección y respuesta en puntos finales (EDR): Las herramientas EDR son esenciales para gestionar amenazas en dispositivos, ya que ofrecen visibilidad en tiempo real de los acontecimientos que suceden en los puntos finales y permiten actuar de manera remota, a través de funciones de contención permitiendo aislar un dispositivo comprometido de la red con un solo clic, lo que ayuda a que se supervise en estado de cuarentena y se realicen análisis forenses, manteniéndolo desconectado tanto de la red de la organización como del sistema del atacante.
- Sistemas de Control de Acceso a la Red (NAC): Las soluciones de Control de Acceso a la Red (NAC) hacen posible gestionar de manera central cómo y quién puede conectarse a la red, los dispositivos autorizados y bajo qué condiciones, asegurando que solo los dispositivos que cumplen con las normas de seguridad establecidas puedan acceder a la red, limitando o bloqueando los que presentan comportamientos sospechosos; Cuando se halla un dispositivo con actividades inusuales a través de la telemetría del EDR o del SIEM, el NAC puede redirigir automáticamente ese dispositivo a una red de cuarentena con acceso nulo o restringido, sin necesidad de intervención manual en el cortafuegos principal, facilitando así una respuesta rápida y automatizada.

Tema 5 Informe

Análisis del Vector de Ataque

Luego de configurar las máquinas virtuales, desde la perpectiva del red team se llevó a cabo una serie de acciones con el objetivo de escalar privilegios y lograr permanencia en la red interna, detectando que el Host A estaba utilizando el servicio Rejetto HTTP File Server (HFS), una aplicación que presenta fallas de seguridad en versiones que no están actualizadas.

Herramienta Principal: Metasploit Framework (MSFConsole)

- Vector de Entrada: Se seleccionó el exploit exploit/windows/http/rejetto_hfs_exec.
- Configuración: Se estableció el LHOST 192.168.1.31 y el puerto 4444 para recibir la conexión inversa.
- Ejecución: Al lanzar el exploit, se logró la ejecución remota de código debido a una falla en el análisis de las solicitudes web del aplicativo Rejetto, vulnerabilidad que permitió dio apertura al escalamiento del ataque y una vez comprometido el Host A, el atacante no se detuvo, sino que lo utilizó como "pivote" para alcanzar objetivos más profundos en la red LAN segmentada a través de tarjeta de red secundaria.
- Escalamiento: Se elevaron privilegios en el Host A para obtener control.
- Túnel/Pivote: Utilizando las capacidades de enrutamiento de Meterpreter, se estableció vía de acceso para redirigir el tráfico hacia el Host B.
- Objetivo Final: Se explotó una vulnerabilidad de Windows en el Host B para crear un usuario no autorizado, logrando que actuara como una backdoor, garantizando el acceso y determinando el vector de fuga de los datos alojados en la máquina.

Estrategia de Defensa y Respuesta

Con la realización exitosa del ataque, el grupo encargado de la defensa (Blue Team) y el Grupo de Respuesta a Incidentes (CSIRT) necesitan poner en marcha los procedimientos que rigen normas como las de NIST.

El SIEM debe generar la alerta sobre la ejecución maliciosa del proceso desde el servicio Rejetto (Host A), simultáneamente, la creación de un usuario local en el Host B fuera del horario de administración.

- Visibilización: Revisión de logs de Firewalls, Routers y servidores para auditar la IP origen del ataque. La prioridad es detener la fuga de datos y el movimiento lateral.
- Aislamiento vía EDR: Utilizando la solución de Endpoint Detection and Response (EDR), se procede a aislar lógicamente los Hosts A y B. Esto corta la comunicación con la red y el atacante, pero mantiene la máquina encendida para el análisis forense.
- Bloqueo vía NAC: El Network Access Control (NAC) identifica el comportamiento anómalo y mueve los dispositivos afectados a una VLAN de cuarentena automáticamente.
- Segmentación de Red (Firewall): Se aplican reglas de emergencia en el Firewall para bloquear el tráfico hacia/desde la IP externa del atacante (LHOST).

Erradicación y Recuperación

Ante la situación descrita, es crucial adoptar una estrategia completa que una esfuerzos técnicos de reacción ante el incidente con acciones que fortalezcan la seguridad y cumplan con la legislación vigente, pues en primer lugar, desde el enfoque del análisis forense, se requiere realizar un volcado de memoria para identificar y examinar el payload de Metasploit, que generalmente se encuentra ahí y puede no dejar huellas permanentes en el sistema, por otro lado,

la captura y análisis del tráfico de red ayudan a identificar qué tipo de información pudo haberse exfiltrado, además de reconstruir la comunicación que se estableció entre los sistemas afectados.

Dentro de las medidas de eliminación, se debe quitar el usuario no autorizado creado en el Host B, así como quitar cualquier archivo malicioso presente en los sistemas afectados, teniendo como objetivo restaurar el entorno y prevenir que el atacante mantenga métodos de persistencia.

Es esencial implementar acciones de endurecimiento que busquen disminuir la superficie de ataque y en este contexto, la gestión de vulnerabilidades implica actualizar o eliminar el software Rejetto HFS, que fue usado como medio de entrada inicial, además, el uso de un proxy web permite filtrar, auditar y controlar todo el tráfico que sale de la organización, lo que dificulta la creación de conexiones inversas no autorizadas y asegura que el flujo de datos se restrinja solamente a los destinos necesarios para el funcionamiento legítimo de la entidad.

Desde la perspectiva del marco legal y normativo, como experto en ciberseguridad, es importante señalar que las acciones mencionadas, si fueran llevadas a cabo por un individuo sin la debida autorización, serían consideradas crímenes graves según el Código Penal colombiano y en el entorno analizado, se observan posibles violaciones como el acceso indebido a un sistema informático, al comprometer el Host A mediante la explotación de Rejetto; el uso de software malicioso, por la ejecución de payloads de Metasploit y la creación de túneles ilegales; la interceptación de datos informáticos, resultante de la captura de tráfico o información a través del vínculo entre Host A y Host B y la violación de datos personales, en caso de que se accediera o alterara información de personas naturales almacenada en esos sistemas.

En lo que respecta a la protección de datos personales y el habeas data, conforme a la Ley 1581 de 2012 y la Ley 1266 de 2008, la entidad es responsable del manejo de la información, por

consiguiente, el incidente sugiere un posible incumplimiento del principio de seguridad requerido por la normativa y si se viesen comprometidos datos personales de empleados, clientes o información financiera, la organización podría enfrentar sanciones y multas impuestas por la Superintendencia de Industria y Comercio (SIC), a raíz de la falta de implementación de las medidas técnicas adecuadas y efectivas.

Es fundamental tener en cuenta que, al confirmarse un incidente real, hay una obligación legal de reportarlo y especialmente en casos de delitos que se investigan de manera oficial, como los que amenazan la seguridad digital, los bienes o la seguridad de la comunidad e ignorar la obligación de informar puede llevar a sanciones penales y multas para las directivas o quienes, al estar al tanto de la situación, eligen no revelarla.

Conclusiones y Recomendaciones

- Obsolescencia Tecnológica: El uso de software vulnerable como Rejetto HFS representa un riesgo inaceptable y se debe proceder a su retiro inmediato o actualización.
- Defensa en Profundidad: La implementación de CIS Controls es urgente pues no basta con un firewall y se requiere EDR en los endpoints y una gestión estricta de identidades.
- Cultura de Seguridad: Se recomienda mantener ejercicios periódicos de pentesting ético para identificar brechas, asegurando así el cumplimiento del principio de responsabilidad demostrada exigido por la normatividad.

Evidencia de Sustentación

En cumplimiento de los requisitos de la etapa 5 del seminario especializado, se presenta el video de sustentación disponible en el siguiente enlace:

https://youtu.be/XE2Bx5RTweg

Conclusiones

En conclusión el documento evidencia que una respuesta adecuada ante incidentes de ciberseguridad no debe restringirse solo a medidas técnicas (como contención, análisis forense o hardening), sino que tiene que estár en consonancia con el marco jurídico colombiano, propendiendo por la correcta identificación de conductas tipificadas en la Ley 1273 de 2009 y el respeto por las normas de protección de datos (Ley 1581 de 2012 y Ley 1266 de 2008) fortaleciendo la legitimidad y trazabilidad de las actuaciones realizadas durante un incidente.

Asimismo, la incorporación de prácticas como el volcado de memoria RAM, la captura de tráfico y la eliminación controlada de activos maliciosos demuestra que el análisis forense no solo permite comprender el alcance del ataque, sino que también respalda procesos legales, auditorías internas y mejoras posteriores en la postura de seguridad de la organización.

Finalmente, el trabajo confirma que la explotación de vulnerabilidades conocidas, como el uso de software desactualizado (Rejetto HFS), refleja fallas en la gestión de vulnerabilidades y la adopción de estándares como ISO/IEC 27001 y CIS Benchmarks, junto con equipos especializados como Blue Team y CSIRT, resulta fundamental para reducir la superficie de ataque y anticiparse a amenazas futuras.

Recomendaciones

Se recomienda que la organización documente y mantenga actualizado un plan de respuesta a incidentes basado en NIST, conformando roles claros, procedimientos de contención, análisis forense, protocolos para notificación a autoridades competentes y comunicación interna, garantizando coherencia técnica, legal y operativa.

Asimismo es prioritario implementar procesos periódicos de evaluación de vulnerabilidades, eliminación o parcheo oportuno de software obsoleto y aplicación sistemática de estándares generalmente aceptados, logrando que todas estas acciones deben complementarse con controles físicos de red como proxies, segmentación y monitoreo continuo mediante SIEM y EDR para detectar y contener amenazas en fases tempranas.

Finalmente se recomienda capacitar de forma continua al personal técnico y directivo en temas de ética profesional, deber de denuncia, confidencialidad y protección de datos personales, conforme al Código de ética profesional y la normativa de habeas data (además de la complementaria), reduciendo riesgos legales, sanciones y permitiendo el fortalecimiento de la confianza de clientes y partes interesadas.

Referencias Bibliográficas

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. En *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1–5). https://doi.org/10.1109/cybersa49311.2020.9139638

Amirov, N., Aliyev, N., & Bicakci, K. (2025). Decentralized vulnerability disclosure using permissioned blockchain: A secure and transparent alternative to centralized CVE management. En *2025 18th International Conference on Information Security and Cryptology (ISCTürkiye)* (pp. 1–6). IEEE. https://doi.org/10.1109/isctrkiye68593.2025.11224809

Cinque, M., Cotroneo, D., & Pecchia, A. (2018). Challenges and directions in security information and event management (SIEM). En *2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)* (pp. 95–99). IEEE. https://doi.org/10.1109/issrew.2018.00-24

Congreso de la República de Colombia. (2000, 24 de julio). *Ley 599 de 2000. Por la cual se expide el Código Penal*. Diario Oficial No. 44.097. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

Congreso de la República de Colombia. (2008, 31 de diciembre). *Ley 1266 de 2008. 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*. Diario Oficial No. 47.219. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34206

Congreso de la República de Colombia. (2009, 5 de enero). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado —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, y se dictan otras disposiciones*. Diario Oficial No. 47.223. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (2012, 17 de octubre). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=4998

Consejo Profesional Nacional de Ingeniería. (2015). *Código de ética para el ejercicio de la ingeniería en general y sus profesiones afines y auxiliares* (pp. 3–26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

H, A. P., & Sujatha, G. (2024). System hardening using CIS benchmarks. En *2024 International Conference on Advances in Computing, Communication and Automation (ACCAI)* (pp. 1–6). IEEE. https://doi.org/10.1109/accai61061.2024.10602274

IBM. (s. f.). *¿Qué son las pruebas de penetración?* IBM Think. https://www.ibm.com/es-es/think/topics/penetration-testing

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* (ISO/IEC Standard No. 27001). https://www.iso.org/standard/82875.html

Jimeno García, M. T., Míguez Pérez, C., Matas García, A. M., & Pérez Agudín, J. (2008). *Hacker (Edición 2008)*. Anaya Multimedia. https://books.google.com/books/about/hacker.html?id=nk19pgaacaaj

Kejïou, A., & Bekaroo, G. (2022). A review and comparative analysis of vulnerability scanning tools for wireless LANs. En *Proceedings of the 2022 3rd International Conference on Next Generation Computing Applications (NextComp)* (pp. 1–6). IEEE. https://doi.org/10.1109/nextcomp55567.2022.9932245

Kerner, S. M. (2019, 14 de enero). *Open-source Metasploit Framework 5.0 improves security testing*. eWEEK. https://www.eweek.com/security/open-source-metasploit-framework-5-0-improves-security-testing/

Khan, W., Ashoka, K., Razak, M. S. A., Kumar, M. V. M., & Naseer, R. (2025). A comprehensive survey on cognitive cyber security analysis using machine learning approaches. *IEEE Access*, *13*, pp. 169314–169326. https://doi.org/10.1109/cybersa49311.2020.9139638

López Delgado, M. (2007). *Análisis forense digital* (2.ª ed.). CriptoRed. https://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf

Machap, K., Shyan, L. K., & Nathan, Y. (2024). *A survey of Nmap command builder for learning penetration testing*. *AIP Conference Proceedings*, *3161*(1), 1–9. https://doi.org/10.1063/5.0230138

National Institute of Standards and Technology. (2012). *Computer security incident handling guide (NIST Special Publication 800-61 Rev. 2)*. U.S. Department of Commerce. https://doi.org/10.6028/nist.sp.800-61r2

Pina, E., Ramos, J., Jorge, H., Váz, P., Silva, J., Wanzeller, C., Abbasi, M., & Martins, P. (2024). *Data privacy and ethical considerations in database management*. *Journal of Cybersecurity and Privacy*, *4*(3), 494–517. https://doi.org/10.3390/jcp4030024

Presidencia de la República de Colombia. (2013, 27 de junio). *Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012* [Decreto reglamentario]. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53616

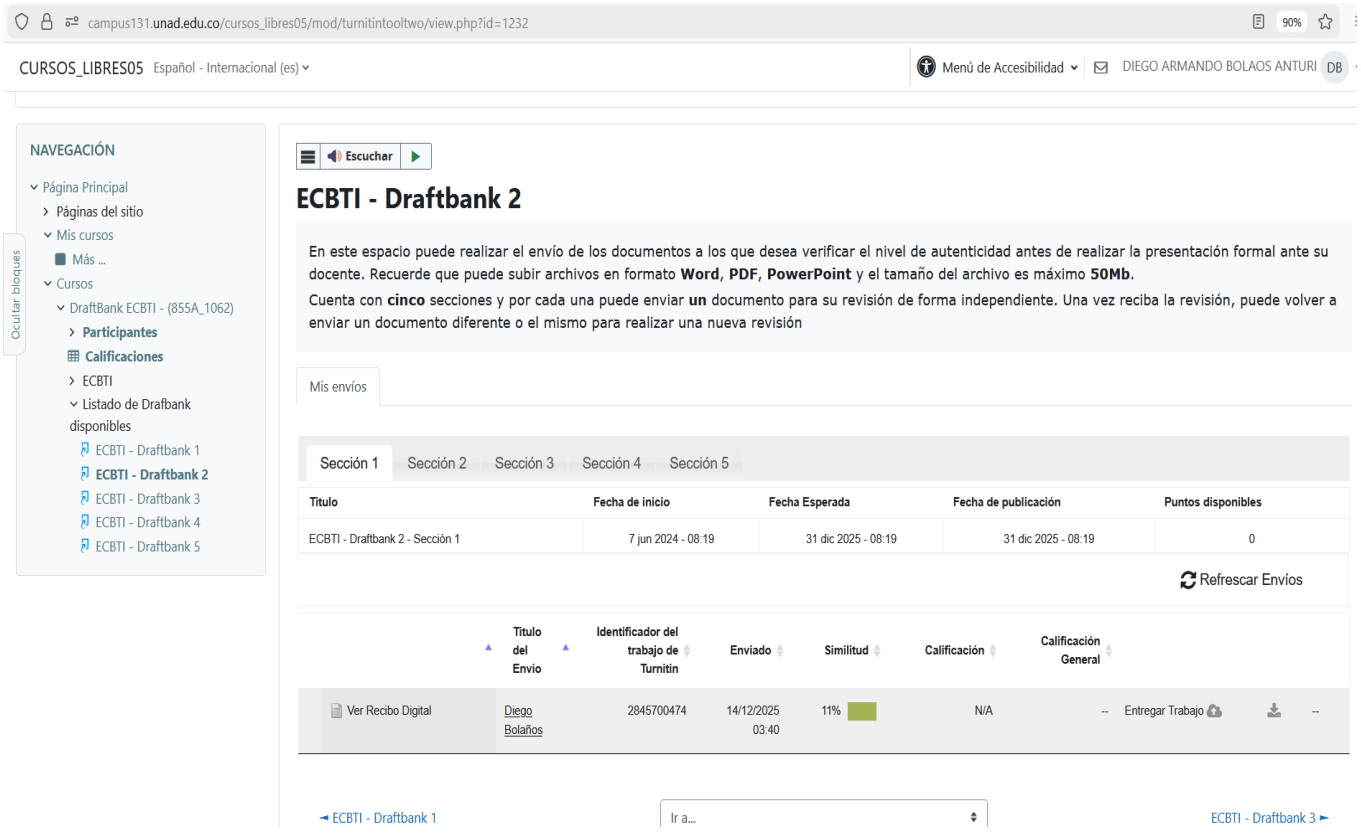
Salazar Mata, J. M., Balderas Sánchez, A. V., García Aldape, H., & Cruz Navarro, C. (2021). Implementación de una estrategia de pentesting con software libre / Implementation of a pentesting strategy with free software. *TECTZAPIC: Revista Académico-Científica, 7*(1), 22–30. https://dialnet.unirioja.es/servlet/articulo?codigo=8507628

Tello Flores, L. (2024). *Plataforma para la detección y control de puntos finales en la red usando tecnologías Zero Trust y NAC* (Trabajo de fin de máster, Universitat Oberta de Catalunya). https://hdl.handle.net/10609/149872

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Fuente. Autoría Propia