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

Jefferson Torres Murillo

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Resumen

En este documento que es un informe técnico se pone en contexto las acciones realizadas en las fases de la 1 a la 4 relacionadas con la ciberseguridad. En estas fases se analizaron acuerdos y cláusulas desde una perspectiva ética y legal identificando los posibles riesgos que pueden existir por el incumplimiento de las normas legales. También se configuró un entorno virtual simulando uno real para la realización de pruebas de seguridad identificando las vulnerabilidades encontradas. Igualmente se identificaron las acciones implementadas por los equipos de seguridad. Al final se realizaron las recomendaciones correspondientes para fortalecer la ciberseguridad de SecureNova Labs.

Palabras clave: exploit, mitigación, pentesting, protección, vulnerabilidad.

Abstract

This technical report contextualizes the actions taken in phases 1 through 4 related to cybersecurity. These phases involved analyzing agreements and clauses from an ethical and legal perspective, identifying potential risks that could lead to penalties for non-compliance with laws and regulations. A virtual environment simulating a real-world scenario was also configured to conduct security tests and identify vulnerabilities. The actions implemented by the security teams were also documented. Finally, corresponding recommendations were made to strengthen the cybersecurity of SecureNova Labs.

Keywords: exploit, mitigation, pentesting, protection, vulnerability.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Glosario

Blue Team:

Es un equipo encargado de la ciberseguridad para proteger los sistemas informáticos y responder ante los incidentes de seguridad.

Ciberseguridad:

Estrategias y prácticas de proteger los sistemas informáticos y los datos en contra de los ciberataques.

Firewall:

Sistema de seguridad de tipo hardware o software que protege la red privada controlando el tráfico entrante y saliente.

Metasploit: Herramienta de ciberseguridad que permite crear exploits y es muy utilizada para pruebas de penetración.

MS17_010:

Vulnerabilidad del sistema operativo Windows 7 utilizada en diferentes ataques como el ransomware WannaCry.

Parrot OS:

Sistema operativo de tipo Linux con gran conjunto de herramientas especializadas en la ciberseguridad ofensiva y defensiva.

Pentesting:

Prueba de penetración para examinar la seguridad de un sistema informático permitiendo identificar las vulnerabilidades existentes.

Red Team:

Equipo de ciberseguridad encargado de simular ataques para encontrar vulnerabilidades y fallas de seguridad en un sistema informático.

Introducción

La ciberseguridad es uno de los pilares fundamentales en la protección de los datos de la era digital en la que nos encontramos debido al aumento desmedido de la cibercriminalidad. La gran cantidad de ataques digitales que ocurren cada año han llevado a las organizaciones a tomar acciones que busquen contrarrestar las acciones realizadas por los ciber delincuentes y que les permita salvaguardar los activos e información con la que operan estas organizaciones.

En este informe técnico se recopilan las acciones realizadas en las fases de la 1 a la 4 según los lineamientos del documento Anexo 6 – Escenario 5. Este informe contiene un panorama que evidencia la seguridad actual de SecureNova Labs mediante una prueba simulada de un ataque donde fue comprometida la seguridad.

La construcción de este informe se realiza en solicitud para su análisis por los Senior de la seguridad de la organización con miras a fortalecer los procesos y acciones que implementa SecureNova Labs en busca de mitigar o eliminar las brechas de seguridad para salvaguardar los activos y proteger el sistema informático de los posibles ciberataques.

Justificación

En la actualidad, la ciberseguridad es un factor clave en la protección de los datos personales ante el aumento desmedido de los ataques informáticos a las organizaciones. La gestión en ciberseguridad les permite a las organizaciones implementar acciones que salvaguarden la información confidencial respondiendo oportunamente ante la ocurrencia de un incidente que ponga en peligro la integridad, confidencialidad y disponibilidad de los datos contenidos en un sistema informático. Es por ello que adoptar medidas de protección que permitan detectar de manera temprana un incidente de seguridad e implementar acciones para contener los ataques informáticos logrará salvaguardar al máximo los activos de las organizaciones.

Identificar la ocurrencia de un incidente de seguridad de manera temprana es un factor de gran importancia porque logra que se minimicen los posibles daños en el sistema informático al poner en práctica acciones que permitan responder de manera eficaz ante la amenaza impidiendo al máximo que se comprometa algún activo crítico del sistema.

La respuesta para la contención de ataques debe ser rápida para evitar que los ciberdelincuentes logren sus objetivos. Ante un incidente de seguridad, se deben realizar acciones que aíslen un activo comprometido evitando la propagación del ataque logrando proteger la infraestructura crítica del sistema.

No se debe dejar de lado la etapa de análisis forense les permite a las organizaciones evaluar el ataque sufrido recopilando la información necesaria que logre identificar qué activos y qué información fue comprometida, así como el vector de ataque y las acciones que realizaron los ciberdelincuentes para el acceso al sistema con el objetivo de mitigar las brechas de seguridad e impedir que se repita el ataque.

Para la protección de los datos las organizaciones implementan equipos de profesionales en ciberseguridad quienes aúnan esfuerzos para mantener a salvo los sistemas informáticos de intrusiones no deseadas cumpliendo las políticas y las normas vigentes concernientes a la seguridad de la información. Estos equipos trabajan en coordinación para detectar las vulnerabilidades existentes e identificar las brechas en la seguridad informática que deben ser mitigadas y les permite fortalecer sus conocimientos para fortalecer las estrategias implementadas para la defensa de los sistemas.

Objetivos

Objetivo General

Realizar una prueba de pentesting controlada buscando analizar la seguridad digital de SecureNova Labs identificando las vulnerabilidades existentes y realizar un análisis ético de las acciones de los equipos de ciberseguridad.

Objetivos Específicos

Analizar documento de acuerdo para identificar las cláusulas contractuales desde la perspectiva ética profesional.

Utilizar software especializado en prueba controlada de pentesting sobre máquinas virtuales simulando un entorno real.

Identificar y explotar alguna vulnerabilidad existente en un sistema informático para la extracción de información.

Desarrollo

Estrategias de los Equipos de Ciberseguridad

Red Team

Acciones de Ingeniería Social. Implementar acciones para llevar taques de ingeniería social en la organización con herramientas como Wifiphisher o Maltego debido a que en la ciberseguridad el eslabón más débil es el ser humano.

Recopilación y Análisis de Información. Hacer uso de motores de búsqueda como Censys y SpiderFoot que es una herramienta de recopilación de datos con el objetivo de correlacionar la información obtenida y planificar ataques.

Creación o Modificación de Exploits. Hacer uso de la inteligencia artificial (IA) y el aprendizaje automático (Maching Learning) para crear o modificar exploits que permitan probar la seguridad de la organización logrando traspasar las barreras de seguridad.

Blue Team

Formación en Ciberseguridad. Realizar capacitaciones a los empleados de la organización para que éstos puedan identificar los vectores de ataques y estén preparados al máximo ante los posibles ciberataques.

Monitoreo Continuo. Implementar y configurar herramientas SIEM para monitoreo de la red buscando que se generen alertas tempranas ante eventos sospechosos que permiten responder oportunamente ante las amenazas (Rajendran et al., 2011).

Cronograma de Auditorías. Crear un cronograma de auditorías permitirá detectar a tiempo las vulnerabilidades y posibles brechas de seguridad que existan para que éstas sean

corregidas a la mayor brevedad y así evitar incidentes que pongan en peligro los activos con los que cuenta la organización.

Inteligencia de Amenazas. Recopilar información sobre las amenazas emergentes permitirá que el equipo de ciberseguridad implemente acciones que logren robustecer la seguridad y los prepare ante los posibles ataques.

Entrenamiento Continuo. En busca de mejorar la seguridad, se realizarán simulaciones de ataques con la ayuda del equipo Red Team para mejorar los tiempos de detección y respuesta ante los ataques informáticos (Chindrus & Caruntu, 2023).

Fase 1. Fundamentos de Operaciones Red Team y Blue Team

Leyes y Decretos en Colombia sobre Delitos Informáticos

Teniendo en cuenta la altísima transferencia de datos que transitan en internet, deben implementarse las leyes sobre protección de los datos en cada país teniendo en cuenta los derechos a la intimidad de todas las personas (MINTIC, s. f.). Para la protección de los datos personales en Colombia existe la ley 1581 de 2012 que establece los derechos de cada persona para conocer, actualizar y rectificar sus datos (MINAMBIENTE, s. f.). La implementación de esta ley también establece los principios y las obligaciones de cada entidad de carácter pública o privada en la protección de los datos con los que operan.

También existe el decreto 1377 de 2013 que reglamenta todo lo concerniente a la autorización de las personas para el tratamiento de sus datos y las políticas que se deben cumplir con los mismos (Función Pública, s. f.).

Otro decreto es el 886 de 2014 que da instrucciones sobre la mínima información que se requiere para que las bases de datos sean inscritas en el Registro Nacional de Bases de Datos regulando el proceder del tratamiento de datos personales para proteger los derechos de los titulares (VLEX, 2014).

Etapas del Pentesting y las Herramientas Utilizadas

Para la realización de la prueba de penetración o pentesting se siguen un conjunto de pasos o etapas que son las siguientes:

Planificación y Alcance. En esta fase es donde se realiza la planificación de los objetivos, las restricciones, los activos a probar y el alcance del proyecto. También es importante cumplir con las reglas de compromiso y se debe redactar un documento firmado por el titular

dando la respectiva autorización legal al pentester para la realización de la prueba. En esta fase solo se necesita un editor de texto como herramienta.

Reconocimiento. Etapa donde se realiza la recolección de información útil referente al sistema que será atacado. Esta recolección se puede realizar de manera pasiva donde no se tiene contacto directo con el sistema y de manera activa donde se interactúa con el mismo (IBM, 2023). Como ejemplo de la fase de reconocimiento se buscaría información sobre los servicios y puertos abiertos del sistema utilizando la herramienta nmap y el comando "*nmap -Ss -Sv -O <IP/RED>*" que realiza un escaneo silencioso de una IP o red para encontrar los dispositivos activos, el sistema operativo que ejecutan y encontrar los puertos abierto. Algunas de las herramientas utilizadas para esta fase son Wireshark, Nmap, Google Hacking y sistemas operativos como Kali Linux, entre otros.

Detección de Vulnerabilidades. Es la fase donde se identifican las vulnerabilidades, servicios, credenciales y todo tipo de información que permita acceder al sistema objetivo para su posterior explotación. Las vulnerabilidades identificadas deben ser investigadas en bases de datos públicas para saber si estas han sido corregidas o se trata de un falso positivo. Un ejemplo de esta fase sería obtener credenciales válidas para acceder al sistema. Algunas herramientas utilizadas para esta fase son Greenbone/OpenVAS y Nessus (Lopez, 2025).

Explotación. Fase donde se llevan a cabo las acciones necesarias que permitan explotar las vulnerabilidades halladas en la fase anterior con el objetivo de acceder a recursos críticos del sistema. En esta fase se deben registrar todas las actividades realizadas teniendo en cuenta las restricciones planteadas en la fase inicial para no afectar el sistema y poder restaurarlo a su condición inicial cuando finalice la prueba. Un ejemplo de la explotación sería acceder a la base de datos de una organización. Un framework muy útil a utilizar es Metasploit.

Post-explotación. Es en esta fase donde se busca extraer información valiosa y sensible del sistema objetivo. También se busca la escalada de privilegios para tener un control total del sistema, así como realizar acciones que permitan acceder al sistema de manera posterior (Cilleruelo, 2022b). Es muy importante proteger la información de cualquier cambio permanente para lo cual es importante utilizar funciones hash y logs para tener claridad de todos los cambios realizados. Un ejemplo de lo que se puede realizar en esta fase sería el volcado de datos que residen en base de datos de una compañía. Entre las herramientas que se pueden utilizar para obtener éxito en esta fase están Metasploit, PowerSploit y SilentTrinity, debido a que estas herramientas pueden ejecutar código y recopilar gran cantidad de información privilegiada, se debe tener total control de lo realizado en esta fase sin apartarse de la ética profesional.

Elaboración de Informe. En esta última etapa se elabora un informe detallado sobre los hallazgos encontrados en el sistema objetivo. Este informe debe incluir un resume con las vulnerabilidades encontradas y su priorización de acuerdo al riesgo e impacto sobre los activos, un plan para mitigarlas, las capturas de pantalla, los comandos utilizados, el estampado de tiempo, la metodología utilizada, información pública de las vulnerabilidades encontradas, y las recomendaciones que busquen fortalecer la seguridad digital. La redacción del informe debe ser consistentes y fácilmente entendible por todas las personas que tengan la oportunidad de leerlo.

Las herramientas que permiten crear informes automatizados son Blackstone y PWNDoc.

Algunas Herramientas de Ciberseguridad

- **Metasploit**: Poderosa herramienta de código abierto que es un framework ampliamente utilizado en pentesting. Esta herramienta recopila una gran variedad de exploits

contenidos en una muy amplia base de datos. Es una herramienta modular lo cual permite que se puedan añadir o modificar módulos ampliando su rango de acción (Alhamed & Rahman, 2023).

- **Nmap**. Software open source para exploración y auditorias de seguridad de red. Permite analizar grandes conjuntos de redes permitiendo conocer los equipos que están disponibles, los servicios que ofrecen y el sistema operativo ejecutado en los mismos (Genuino Cloud, 2023).

- **Greenbone/OpenVas**. Scanner de vulnerabilidades muy completo que permite realizar pruebas autenticadas y no autenticadas, además esta optimizado para escaneos a gran escala y permite evaluar protocolos industriales y de internet (Greenbone, s. f.).

Servicios en Línea:

- **ExploitDB**. Información contenida en una Base de datos acerca de exploits y vulnerabilidades de seguridad informática con fines educativos que puede ser usada por investigadores de seguridad (Cilleruelo, 2022a). Esto permite que cualquier persona pueda descargar y probar los exploits para mejorar la seguridad informática.

- **CVE**. Es una base de datos con un identificador único y estandarizado para las vulnerabilidades detectadas en la seguridad informática. Las siglas CVE (Common Vulnerabilities and Exposures) significan vulnerabilidades y exposiciones comunes (FMS, 2023). A cada vulnerabilidad detectada se le da in ID CVE (como ejemplo CVE-2023-12345) que permite que sea identificada por las organizaciones de ciberseguridad.

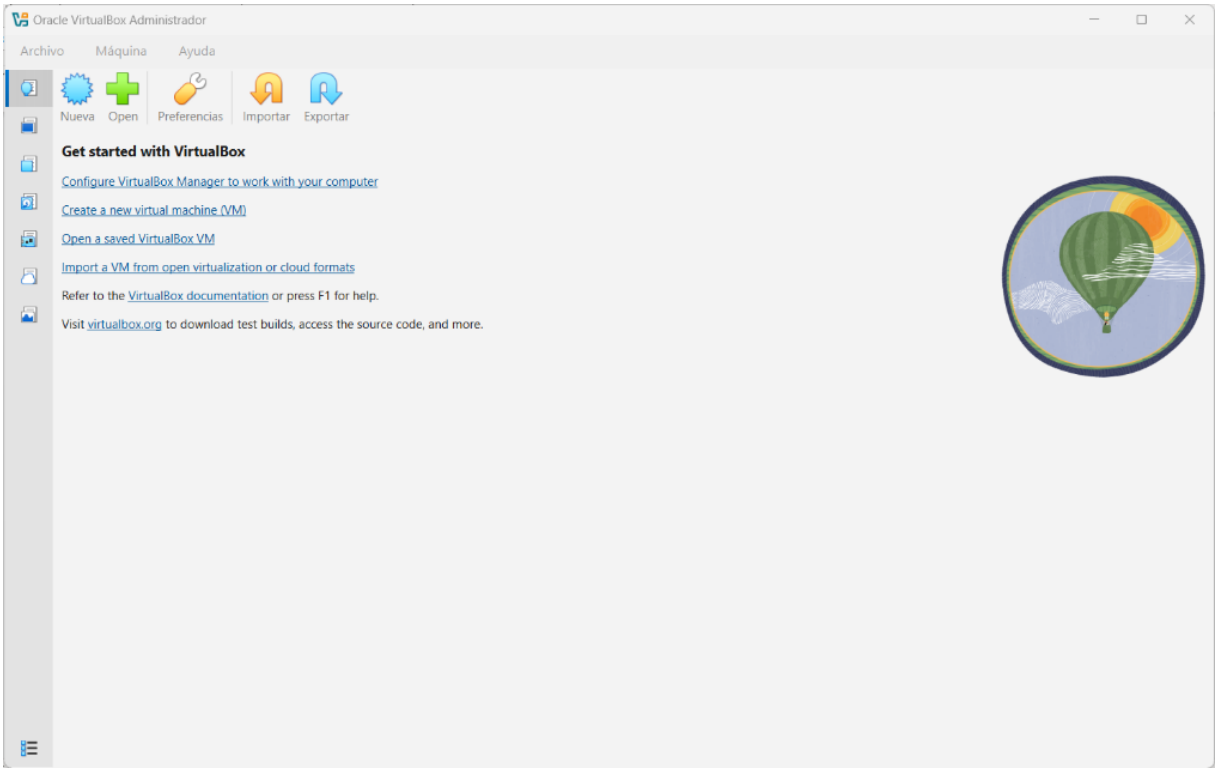
Configuración y Montaje del Banco de Trabajo

- Paso A: Descargar la herramienta virtualizadora “VirtualBox” en su última versión. Para ello nos dirigimos a la página https://www.virtualbox.org/ buscando realizar la

correspondiente descarga del archivo de instalación. Una vez descargado el archivo realizamos la instalación del software en nuestra máquina.

Figura 1

Instalación de VirtualBox en su última versión.

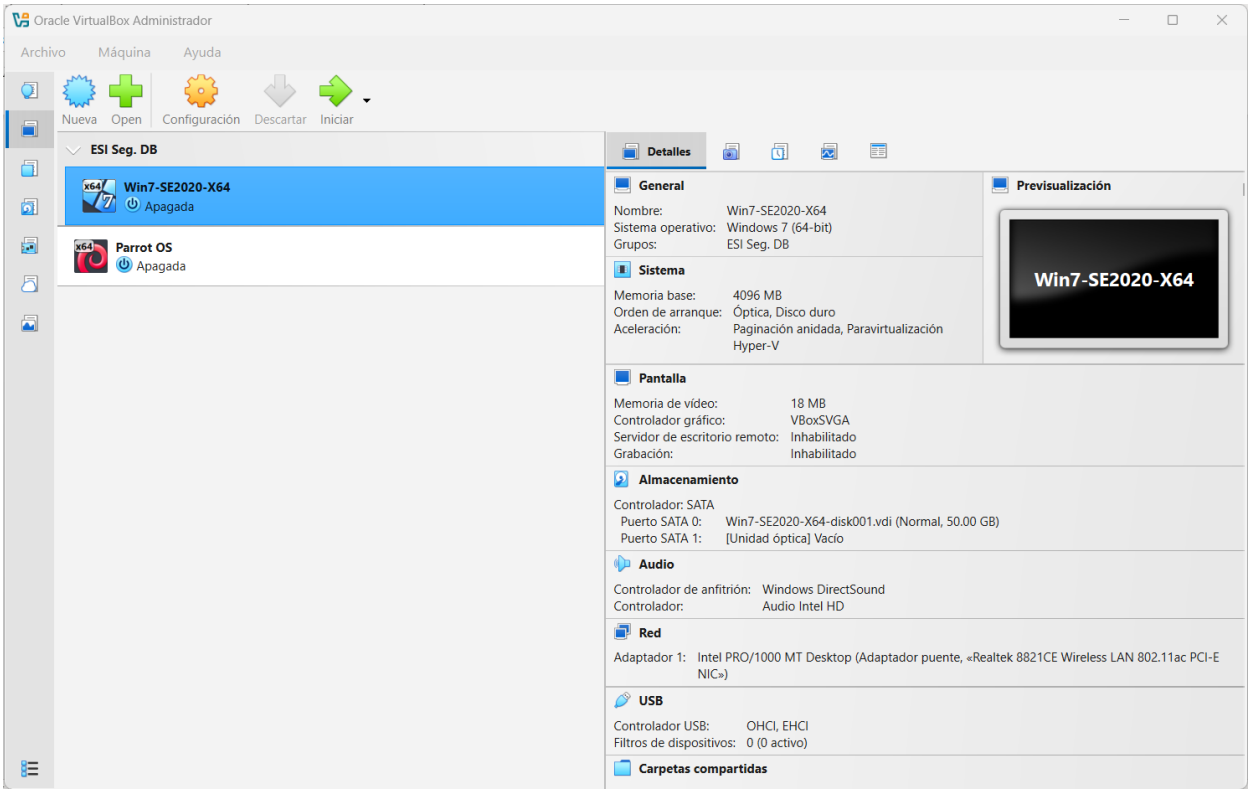


Fuente. Autoría Propia.

- Paso B: imágenes en formato *.OVA: Un sistema operativo Windows y un sistema operativo Parrot OS. Una vez descargadas las imágenes de los sistemas operativos, hacemos la importación en VirtualBox para tener la configuración del banco de trabajo.

Figura 2

*Instalación de las imágenes *.OVA en VirtualBox.*

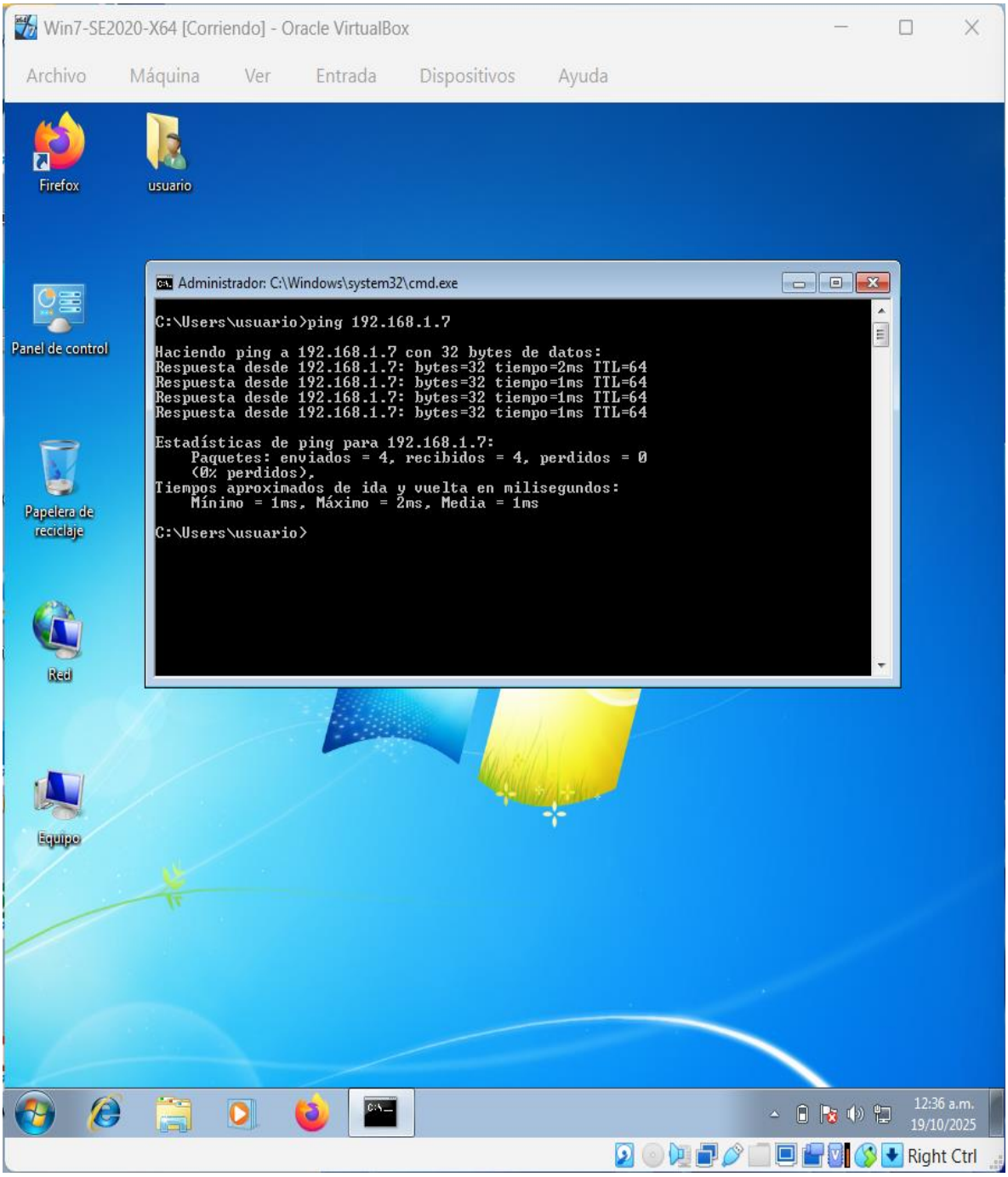


Fuente. Autoría Propia.

- Paso C: Validar que exista comunicación entre cada una de las máquinas. Esto se consigue configurando los adaptadores de red en VirtualBox buscando la comunicación entre las maquinas ejecutadas. Si no se realiza una correcta configuración, las maquinas no se podrán comunicar entre sí.

Figura 3

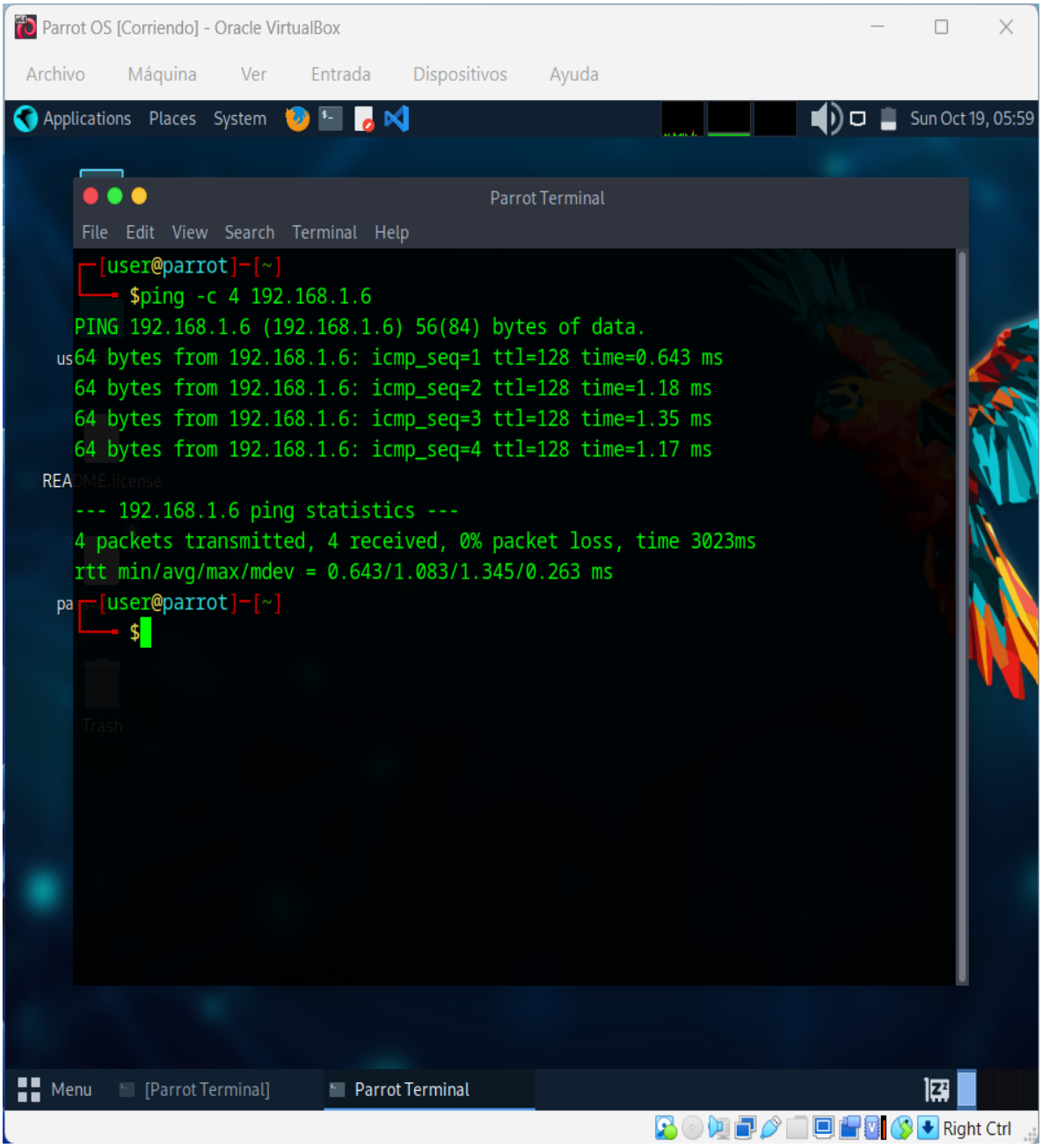
Ping desde Windows 7 a Parrot OS.



Fuente. Autoría Propia.

Figura 4

Ping desde Parrot OS a Windows 7.

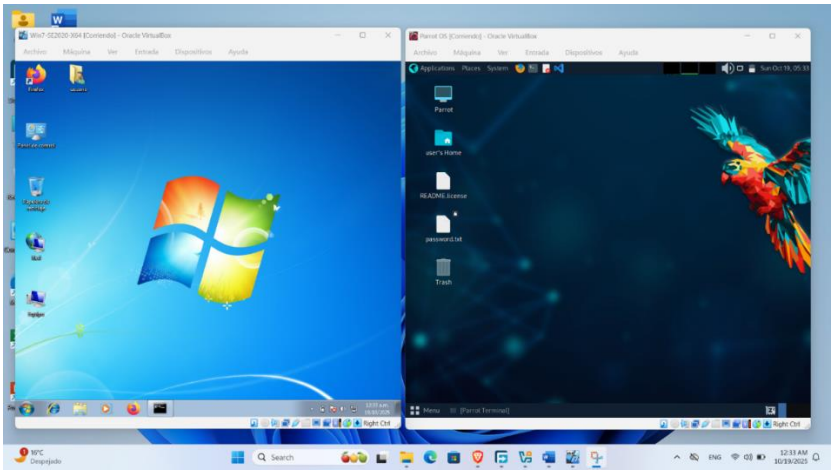


Fuente. Autoría Propia.

- Paso D: Evidenciar con printscreen el montaje del banco de trabajo y explicar cómo se encuentra desplegado “características técnicas de hardware”.

Figura 5

Máquinas virtuales en ejecución.



Fuente. Autoría Propia.

El hardware asignado a las máquinas virtuales es el mostrado en la siguiente tabla.

Tabla 1

Hardware asignado a las máquinas virtuales.

Característica	Windows 7	Parrot OS
Núcleos de procesador	1	2
Memoria RAM	4 GB	8 GB
Memoria de Video	18 MB	128 MB
Disco Duro	50 GB	64 GB
Espacio en disco utilizado	7.97 GB	9.42 GB
Tarjeta de red	Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC	Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC

Nota. Recursos de hardware que le fueron asignados a las máquinas Windows 7 y Parrot OS utilizadas en el banco de trabajo con VirtualBox. *Fuente*. Autor.

Fase 2. Ética Profesional y Marco Normativo en Operaciones de Seguridad

Procesos Ilegales y No Ético Estipulados en Acuerdos de Confidencialidad

Una vez leídos los documentos Anexo 2 – escenario 2 y el Anexo 3 - Acuerdo, se observan errores procedimentales que pueden traer graves consecuencias legales a la organización y miembros de los equipos seguridad que hagan parte de ella.

El primer error se presenta en la falta de revisión de los contratos que se le otorgan al personal que quiera hacer parte de la organización. Esta falta en el procedimiento de contratación expone a la organización a incidentes graves que pueden afectar gravemente el buen funcionamiento y reputación de la organización debido a que no hay completa certeza de que los contratos estén de acuerdo a las normar y leyes del país.

El segundo error que es igualmente gravísimo se presenta en la primera clausula donde se obliga a los firmantes del contrato a la no divulgación de ningún tipo de información, aunque esté relacionada con "procesos ilegales" dentro de la organización. Este tipo de clausula va en contra de la ética profesional contenida en el código de ética del Consejo Profesional Nacional de Ingeniería (COPNIA). Esta misma situación se presenta en la cláusula 4 en los puntos 3, 4 y 9.

La no divulgación de información sobre procesos ilegales va en contra vía de lo estipulado en el artículo 31 numeral F del código de ética para la ingeniería en general donde se insta a los individuos a realizar las correspondientes denuncias de los posibles delitos relacionados con la profesión (Copnia, 2015). Las personas que quieran hacer parte de los equipos de seguridad de la organización no deberían firmar el presente contrato hasta que este

sea totalmente corregido quitando aquellas cláusulas que buscan encubrir los posibles delitos que se puedan presentar.

Artículos de la Ley 1273 que se Podrían Vulnerar en Acuerdo de Confidencialidad

Observado con detenimiento el documento sobre los acuerdos, se puede concluir que existe violaciones de algunos artículos de la ley 1273 los cuales se explican a continuación.

Artículo 269A: Acceso Abusivo a un Sistema Informático. El documento de acuerdos clasifica los datos obtenidos mediante el acceso abusivo a un sistema de información como clasificados y prohíbe a los firmantes del mismo la divulgación de este tipo de información. Esto es claramente un delito porque no se debe acceder a un sistema informático sin la debida autorización (Función Pública, s. f.).

Artículo 269C: Interceptación de Datos Informáticos. El documento de acuerdos viola este artículo porque clasifica los "datos de chuzadas" como información confidencial y prohíbe poner en conocimiento de las autoridades este tipo de prácticas. Esta es una clara violación de la ley porque no se pueden obtener datos de manera ilegal y es un deber de los profesionales la divulgación de este tipo de delito a las autoridades competentes (Función Pública, s. f.-b).

Ética Profesional Frente a Sueldos

Como profesionales de la carrera de ingeniería y afines, debemos contar con una ética profesional que nos defina y que esté acorde a las leyes, normas y decretos que rigen a nuestra nación. Es por ello que como profesionales debemos ser personas íntegras y evitar cualquier tipo de corrupción poniendo en primer lugar la ética profesional que nos rige antes que los beneficios económicos que podamos obtener.

Como profesional de carrera NO aplicaría para este trabajo porque la ética no se vende, aunque esté de por medio un jugoso contrato en cuanto a dinero se refiere. Es necesario actuar en todo momento de manera trasparente recordando que las leyes se deben obedecer y que existen unas exigencias profesionales que se deben cumplir independientemente del salario devengado.

El acuerdo ofrecido por la organización va en contra de la moral de las personas y de la ética profesional porque obliga a los expertos en ciberseguridad a ser testigos silenciosos de los posibles delitos que se puedan presentar en el interior de la organización y a ser participantes de los mismos lo cual va en contravía de las leyes de nuestro país. La ética y dignidad de las personas debe estar por encima de los salarios.

Cuando se antepone la ética profesional frente a los contratos y salarios jugosos, podemos estar seguros de que somos personas íntegras en todo momento que no se dejaran sobornar de ningún modo.

Acceso a Información Sensible de Clientes Durante una Auditoría de Seguridad

Las auditorias de seguridad buscan evaluar la seguridad de una organización con miras a fortaleces los procesos que mitiguen o eliminen las brechas que puedan ser explotadas para la filtración de los datos. Este es un proceso fundamental en la era digital en que vivimos y es por ello que las organizaciones necesitan contratar empresas de ciberseguridad para la detección de fortalezas y debilidades en los procesos y activos utilizados para salvaguardar la información. Por la naturaleza de la auditoria, las empresas de ciberseguridad deben tener acceso a la información sensible, pero esto se puede limitar a través de los acuerdos establecidos entre las partes porque las empresas de ciberseguridad deben operar de manera transparente a los clientes

informándoles clara y explícitamente los tipos de datos sensibles a los que se tendrá acceso. Los datos a los cuales se accedan deben ser solo los necesarios para la auditoria respetando en todo momento la privacidad de todos los clientes y aunando esfuerzos en proteger este tipo de información para que no sea divulgada bajo ninguna circunstancia, respondiendo de manera legal ante la posible filtración de estos datos.

La manera en que se puede garantizar que este proceso no sea explotado de manera indebida es contratar personal con ética profesional intachable que realice los procesos de auditoría de manera transparente utilizando solo las herramientas de software necesarias para dicha actividad y que permitan el cumplimiento de los acuerdos establecidos. También se debe contar con software especializado que registre en todo momento las actividades realizadas para constancia de un proceso transparente que brinde confianza a los clientes y a los supervisores de la auditoria.

Mecanismos de Supervisión y Control en las Empresas de Ciberseguridad

Entre los mecanismos de supervisión que se deben implementar están los controles internos que permitan vigilar continuamente las actividades de los profesionales de la ciberseguridad identificando la herramienta, hora y tiempo utilizado.

Igualmente se deben establecer controles de acceso basado en roles para establecer qué personal tiene acceso a determinada herramienta. Esto permite controlar el uso de las herramientas para que estas sean utilizadas solo por el personal calificado lo cual debe estar estipulado estrictamente en los contratos establecidos entre las partes donde se especifique el uso y las sanciones que se aplicarán en caso del uso irregular.

Contar con un mecanismo de denuncia confidencia es crucial para que otros empleados que sean testigos de la mala utilización de herramientas avanzadas puedan reportar las irregularidades que permitan identificar a los responsables del posible delito o la práctica de acciones de ética cuestionable.

Respuesta de los Gobiernos y Organizaciones Ante el Ciberespionaje

Cuando se comprueba la ocurrencia de un caso de espionaje, es fundamental que los gobiernos actúen con prontitud, severidad e imparcialidad donde se debe seguir el debido proceso para no caer en malos procedimientos (Guarnizo Portela, 2024). Se debe denunciar el caso ante las autoridades competentes teniendo en cuenta las leyes colombianas con la 1273 de 2009 que establece las sanciones a este tipo de delitos.

Otro tipo de medida es la cancelación de todas las operaciones de la empresa de ciberseguridad hasta que se llegue a un veredicto para evitar posibles delitos futuros que puedan afectar a otras organizaciones que requieran auditorias de seguridad. Igualmente se deben realizar las investigaciones necesarias para establecer responsabilidades de carácter grupal e individual con el fin de establecer las sanciones pertinentes.

Por último, se deben aplicar las normas a las que haya lugar para establecer las multas económicas por daños y perjuicios ocasionados dejando un precedente para evitar que esto ocurra en vigencias futuras.

Medidas Adecuadas para Restaurar la Confianza Ante el Ciberespionaje

La confianza es uno de los pilares del buen trabajo y es fundamental en los procesos que se realicen referidos a salvaguardar la información con que trabajan las organizaciones. Debido a

lo anterior se hace necesario que las empresas de ciberseguridad aumenten los requisitos en la contratación de personal exigiendo certificados internacionales para el manejo de información como la norma ISO/IEC 27001 y 27002. También es fundamental contar con los lineamientos nacionales del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Por último, se deben realizar actualizaciones periódicas de los conocimientos adquiridos por los profesionales para estar a la vanguardia en temas de ciberseguridad.

Fase 3. Prueba de Intrusión del Equipo Red Team en Ambiente Controlado

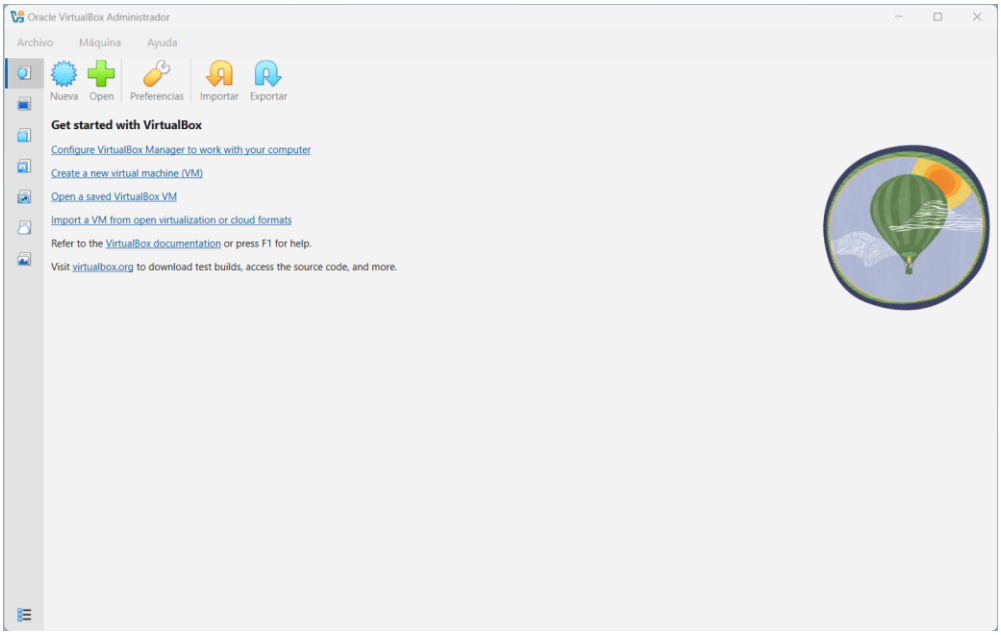
Herramientas Utilizadas para la Práctica de Pentesting

Para la realización de esta prueba de penetración se utilizaron las siguientes herramientas:

VirtualBox 7.2.2 r170484 (Qt6.8.0): Software de código abierto utilizado en la virtualización de sistemas operativos que permite probar diferentes configuraciones sin afectar la maquina anfitriona.

Figura 6

Software de virtualización VirtualBox.

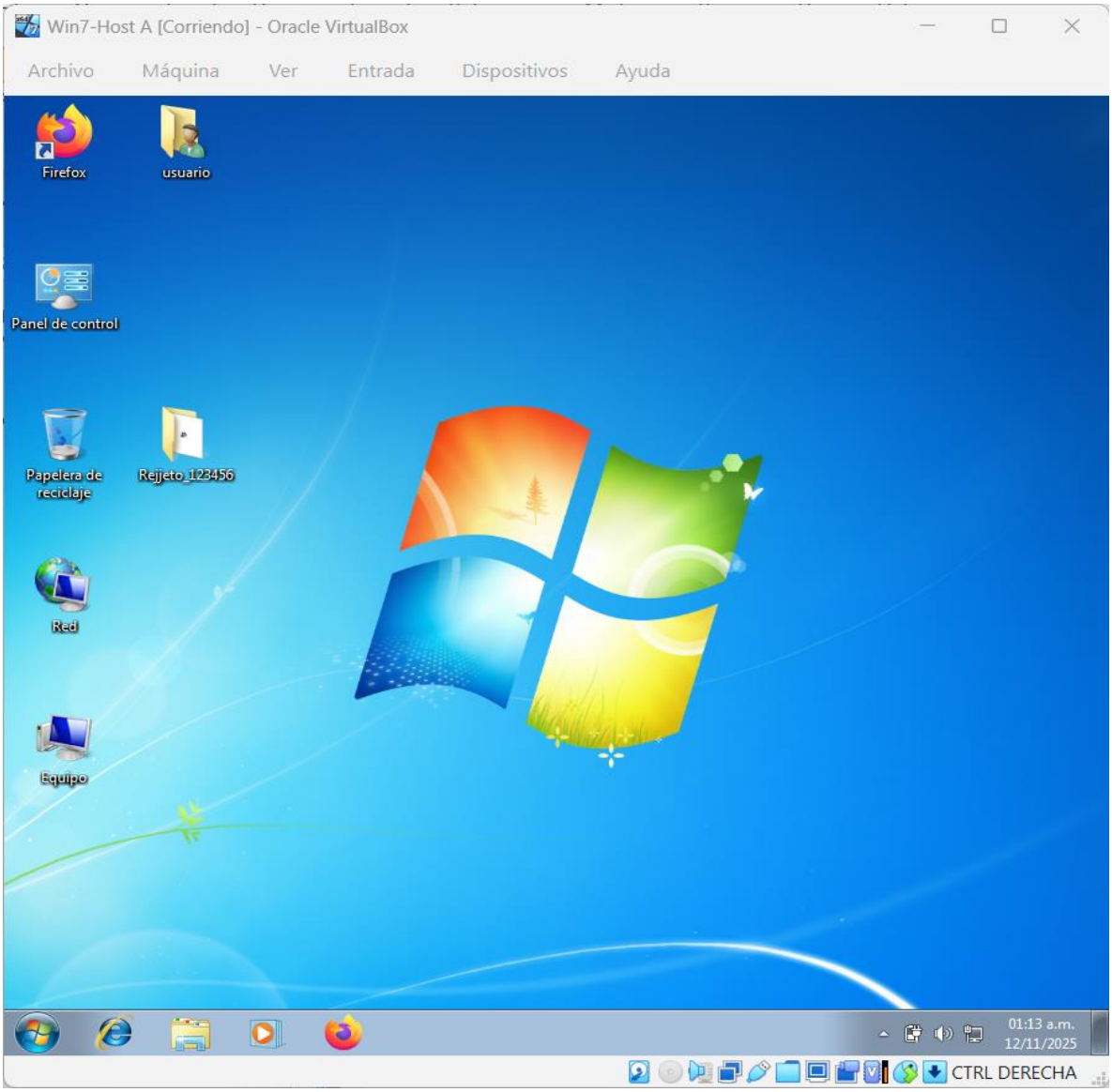


Fuente: Autoría Propia.

Windows 7: Sistema operativo de pago con interfaz mejorada e intuitiva con optimizaciones en el rendimiento perteneciente a la corporación Microsoft el cual salió en el año 2009 y tuvo soporte hasta el año 2020.

Figura 7

Sistema operativo Windows 7.

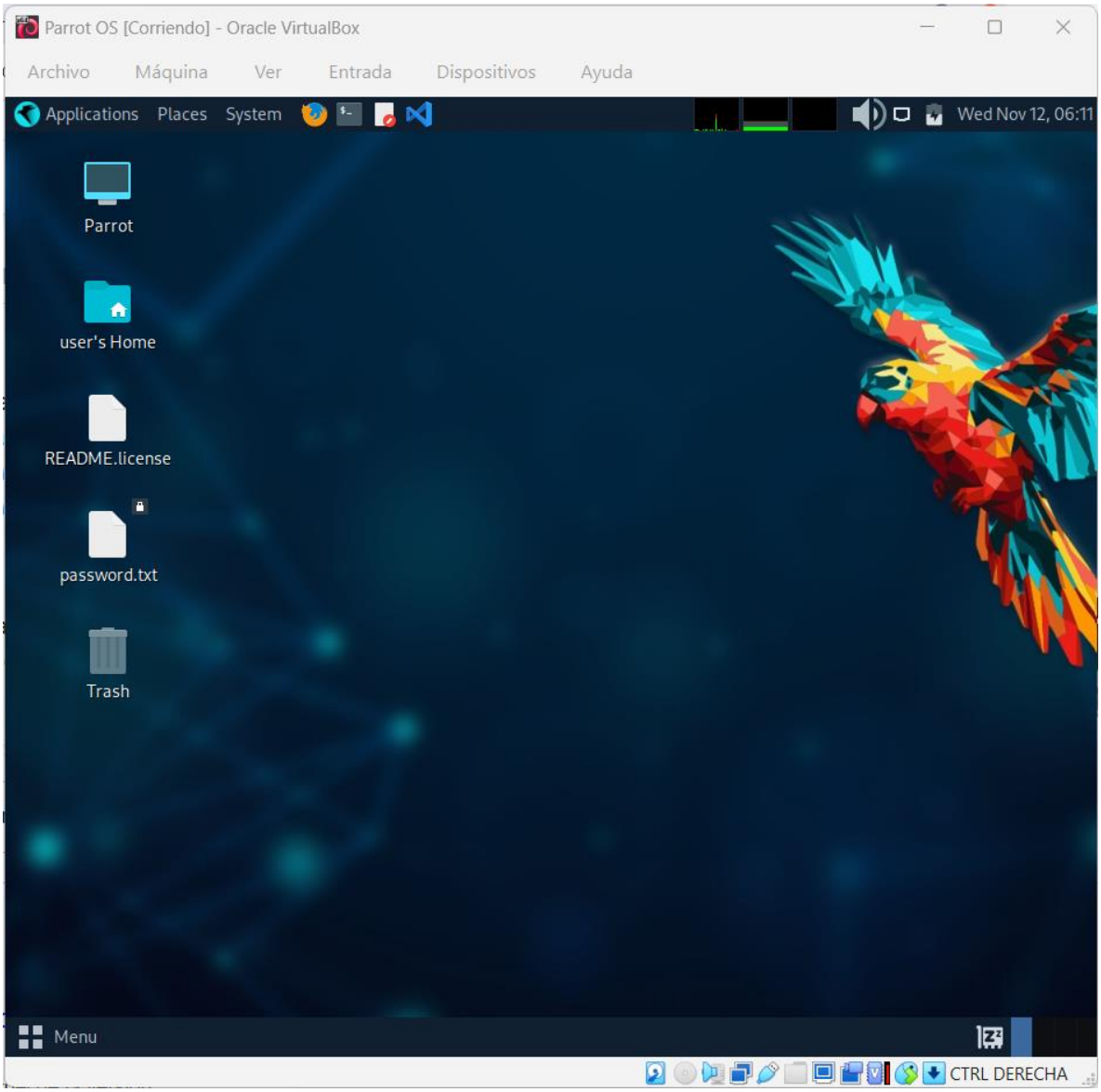


Fuente: Autoría Propia.

Parrot OS 6.3: Sistema operativo de tipo Linux utilizado principalmente para la seguridad ofensiva y defensiva especialmente en las auditorias de seguridad a sistemas informáticos. `

Figura 8

Sistema operativo Parrot 6.3 de tipo Linux.



Fuente: Autoría Propia.

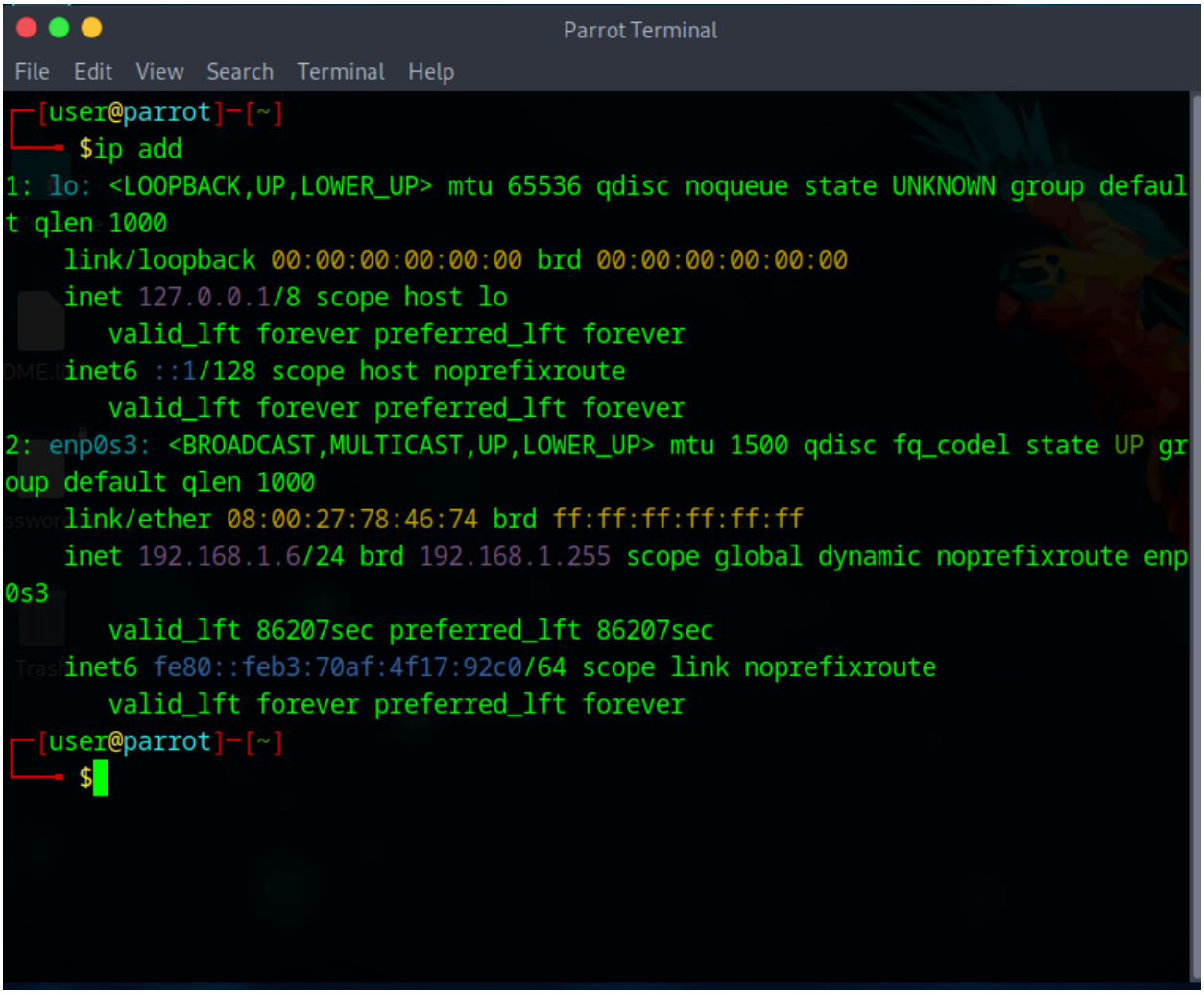
Reconocimiento

Después de poner en ejecución las tres máquinas virtuales, se procedió a conocer la dirección IP de la máquina atacante que en este caso es Parrot OS. Esto se realizó con el

comando <***ip add***> el cual arrojó el resultado mostrado en la **Figura 4** como se muestra a continuación.

Figura 9

IP de la máquina Parrot OS.

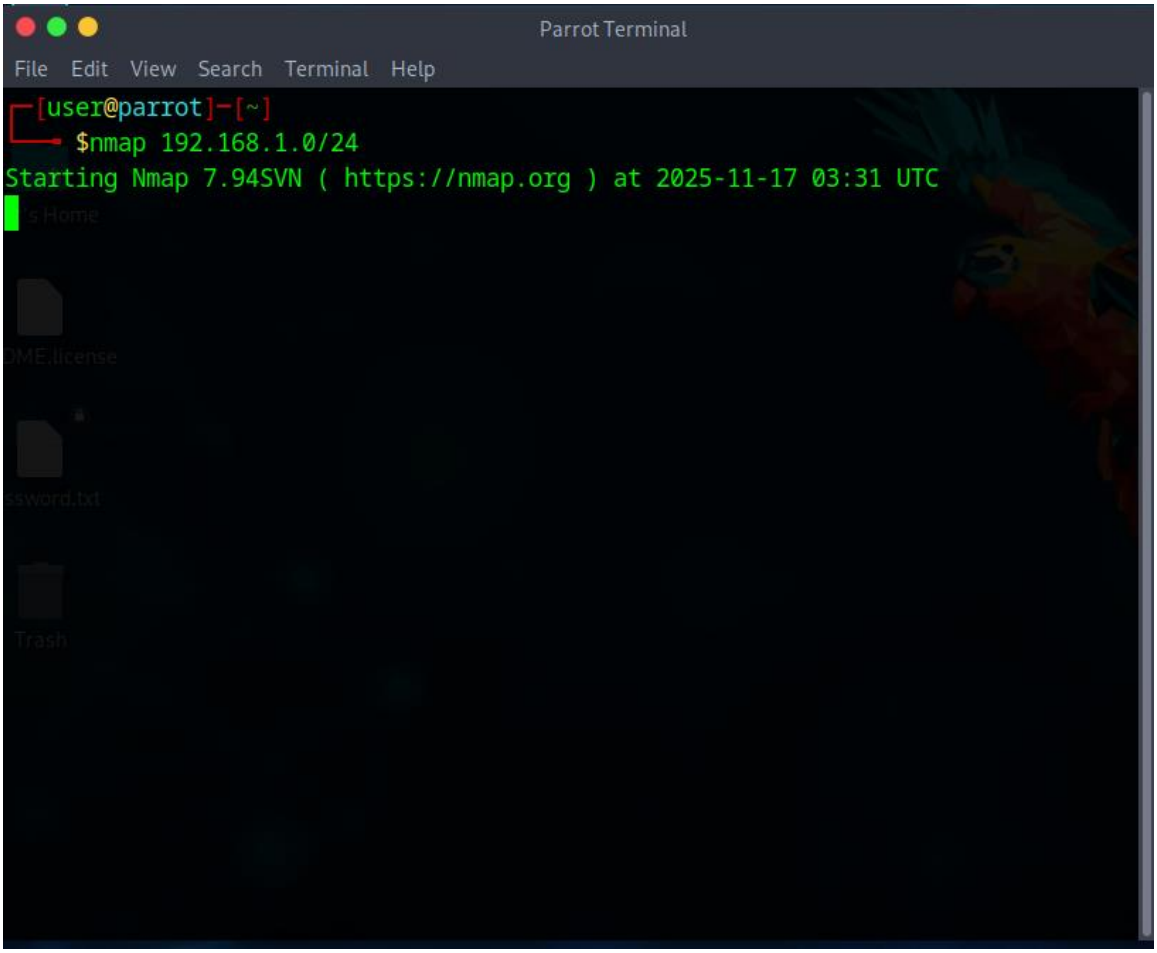


Fuente. Autoría Propia.

Para la fase de reconocimiento se utilizó la herramienta **Nmap** con el objetivo de conocer los equipos que están conectados a la red perteneciente a la máquina Parrot OS. Para este caso se utilizó el comando <***nmap 192.168.1.0/24***> como se muestra a continuación.

Figura 10

Escaneo de la red con Nmap.

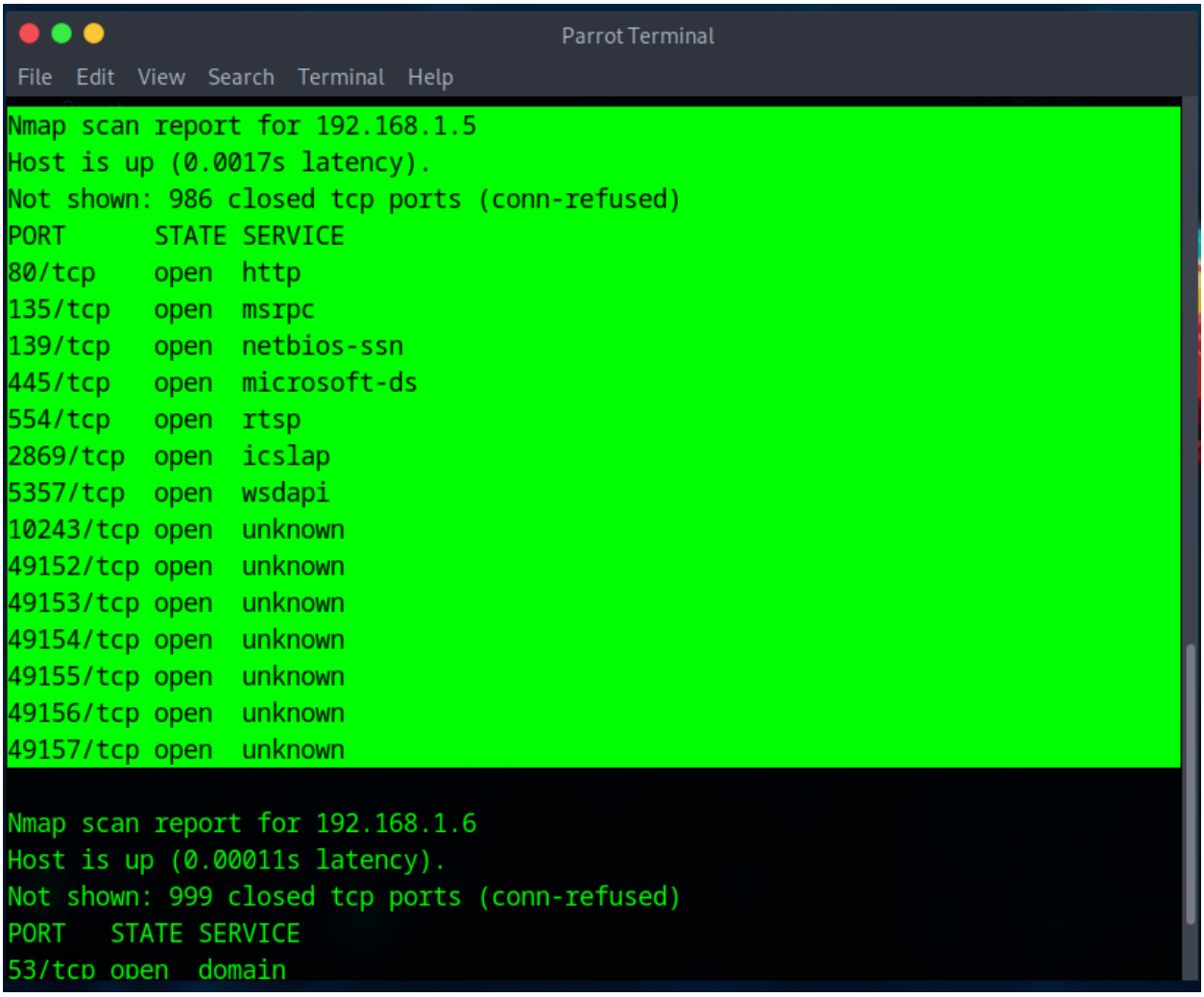


Fuente. Autoría Propia.

Una vez utilizado el comando antes mencionado, se observa que se encuentra un equipo con la dirección 192.168.1.5 que está ejecutando el servicio HTTP por el puerto 80 como observamos a continuación.

Figura 11

Host encontrado en el escaneo de red con Nmap.

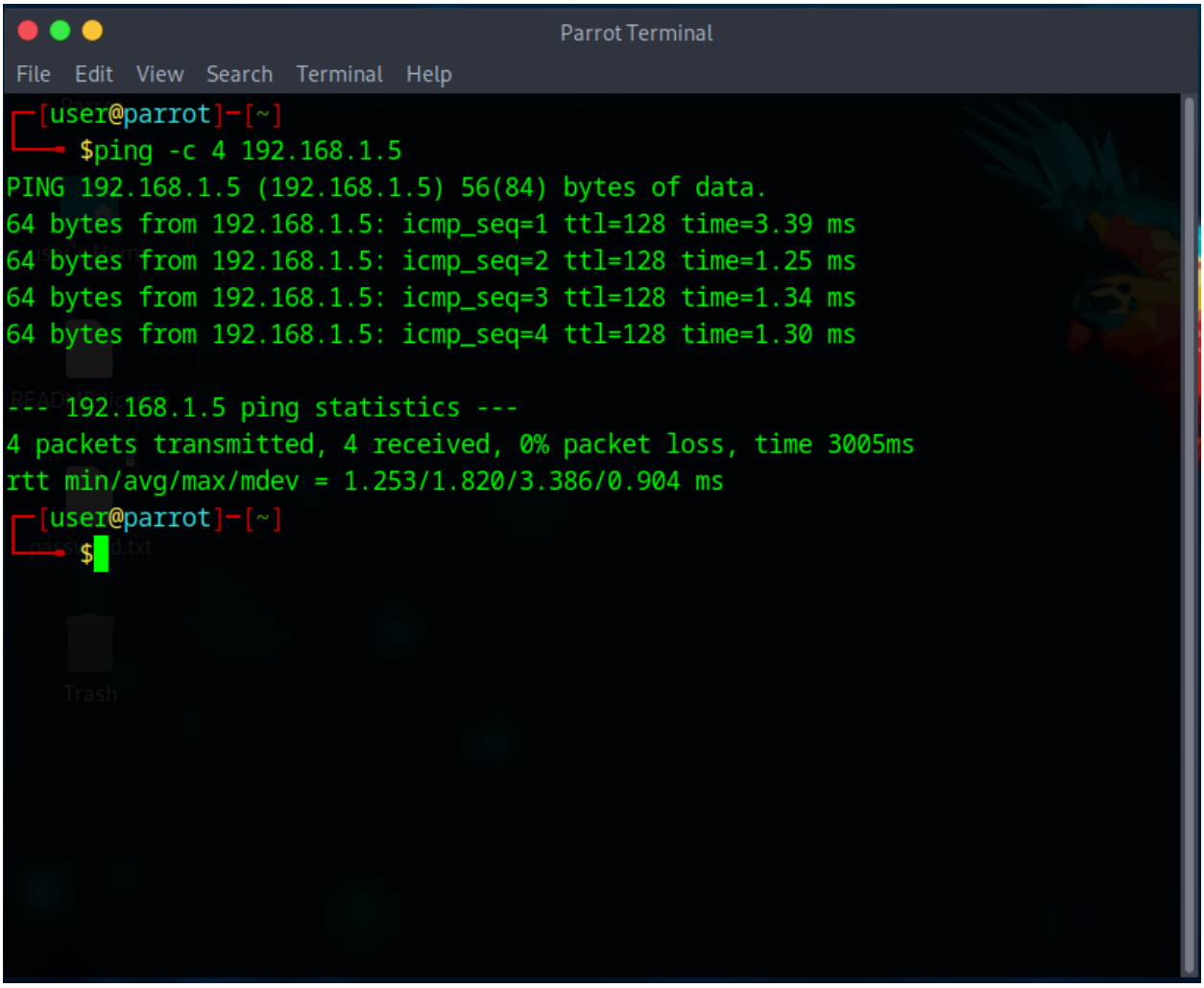


Fuente. Autoría Propia.

Para conocer en más detalle el Host encontrado, realizamos un Ping a la dirección del equipo para saber si hay respuesta del mismo. Esto lo realizamos con el comando <***ping -c 4 192.168.1.5***> el cual enviará 4 paquetes a la dirección IP seleccionada.

Figura 12

Ping desde Parrot hasta el Host encontrado.



Fuente. Autoría Propia.

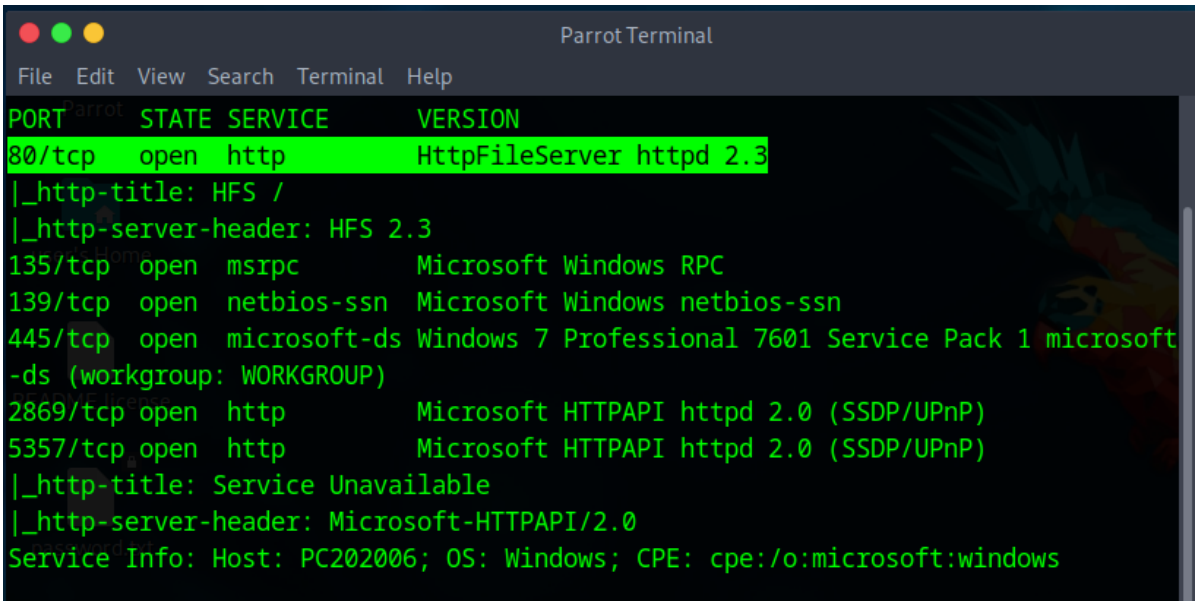
La ejecución del comando Ping nos muestra una respuesta con TTL de 128 lo cual nos confirma que es un Host con el sistema operativo Windows.

Detección de Vulnerabilidades

Teniendo en cuenta la información recopilada, realizamos un escaneo para conocer en detalle los puertos y servicios que se están ejecutando en la máquina Windows con el comando <***nmap -A 192.168.1.5***> como se muestra a continuación.

Figura 13

Servicio y versión ejecutado en el puerto 80 del Host Windows.

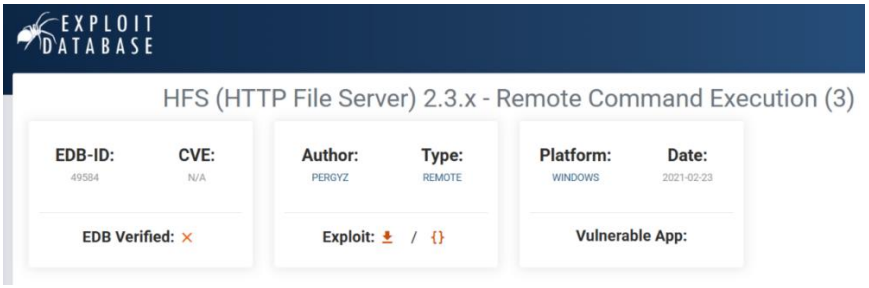


Fuente. Autoría Propia.

Ahora nos dirigimos a la dirección https://www.exploit-db.com/ con el objetivo de investigar si existe alguna vulnerabilidad para HFS (HTTP File Server) 2.3.x y se observa que existe la vulnerabilidad <***EDB-ID: 49584***> que nos permitirá ejecutar comando de manera remota.

Figura 14

Identificación de la vulnerabilidad para HFS.



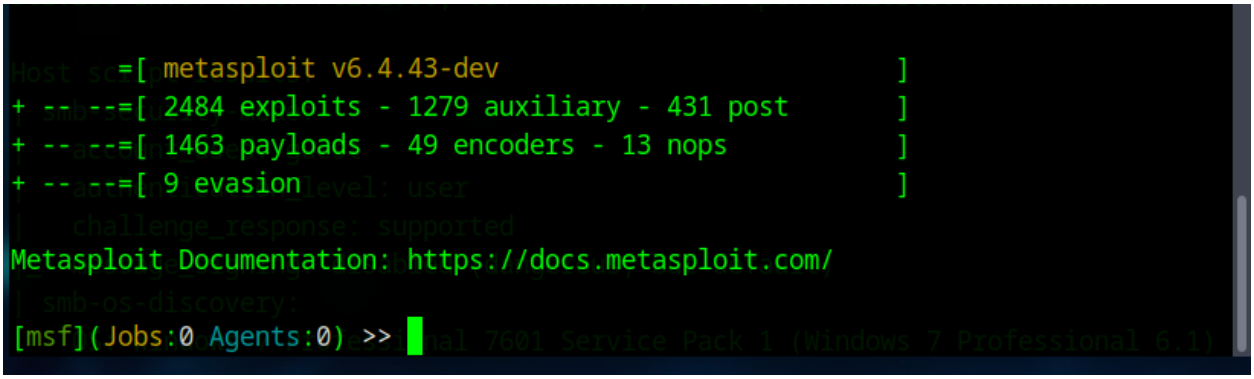
Fuente. Autoría Propia.

Explotación

Para la explotación de esta vulnerabilidad utilizamos Metasploit utilizando en la consola el comando <***msfconsole***>. Esto permitirá trabajar con la consola de Metasploit para explotar la vulnerabilidad encontrada.

Figura 15

Consola de Metasploit.

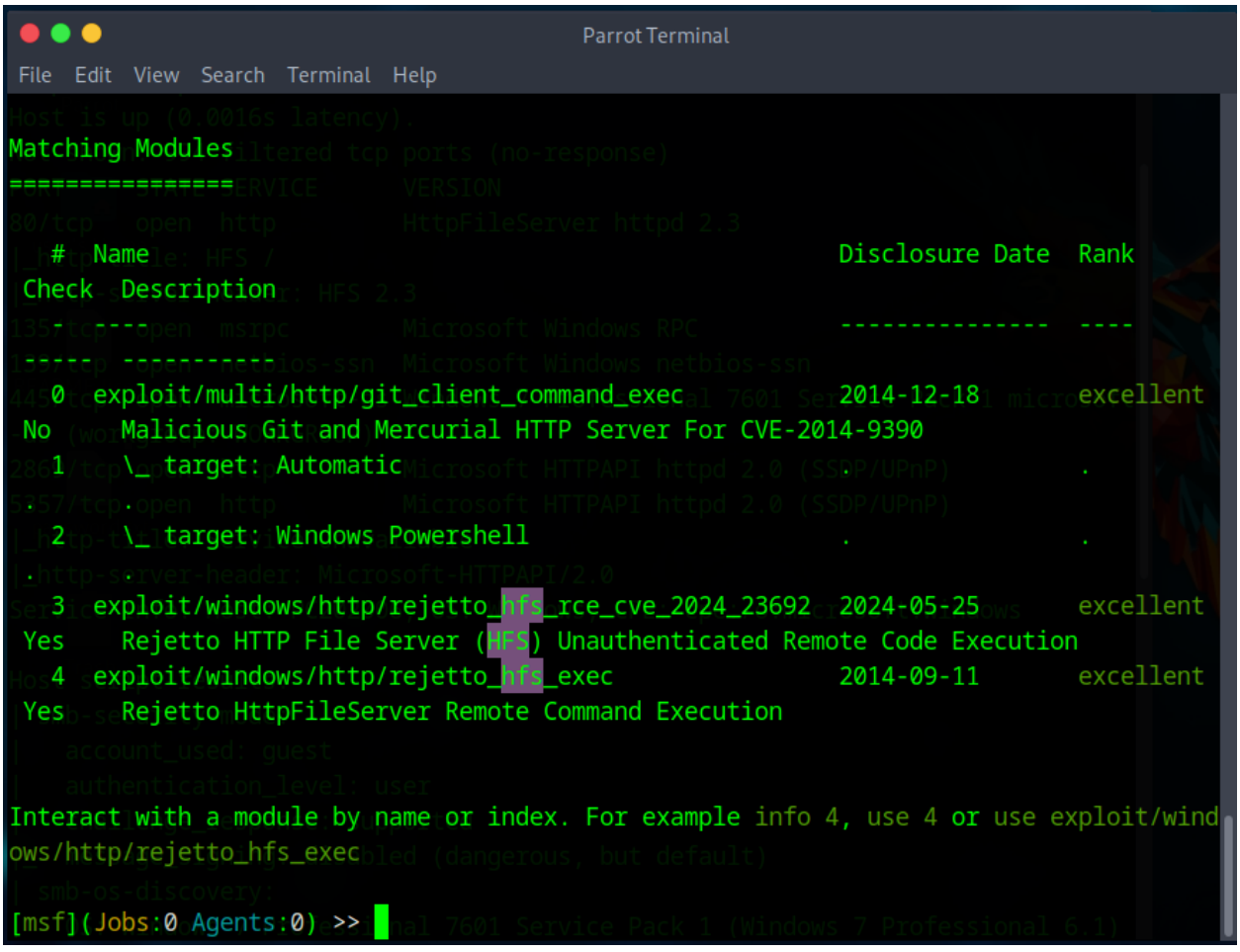


Fuente. Autoría Propia.

A continuación, buscamos un exploit que nos pueda servir para la explotación de la vulnerabilidad encontrada para la aplicación Rejetto 2.3 que se ejecuta en el puerto 80 del Host A. Para esto utilizamos el comando <***search hfs***> que nos permitirá iniciar una sesión en el Host A como muestra la siguiente salida.

Figura 16

Búsqueda de exploits para HFS.

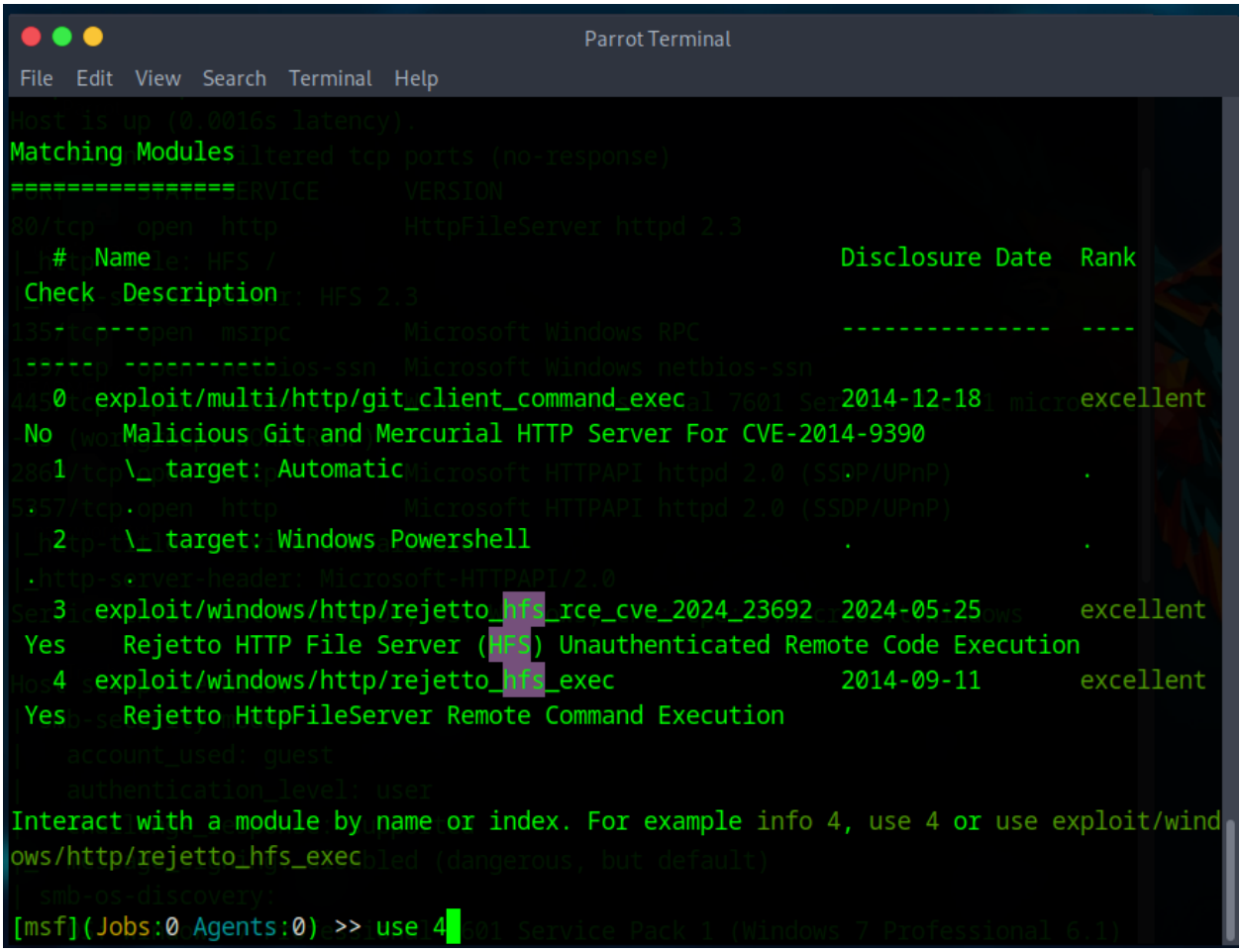


Fuente. Autoría Propia.

De la lista que encontramos, podemos observar que el exploit que nos permitirá la ejecución remota de comandos es "*exploit/windows/http/rejetto_hfs_exec*". Lo seleccionamos con el comando <***use 4***>.

Figura 17

Selección del exploit para HFS.

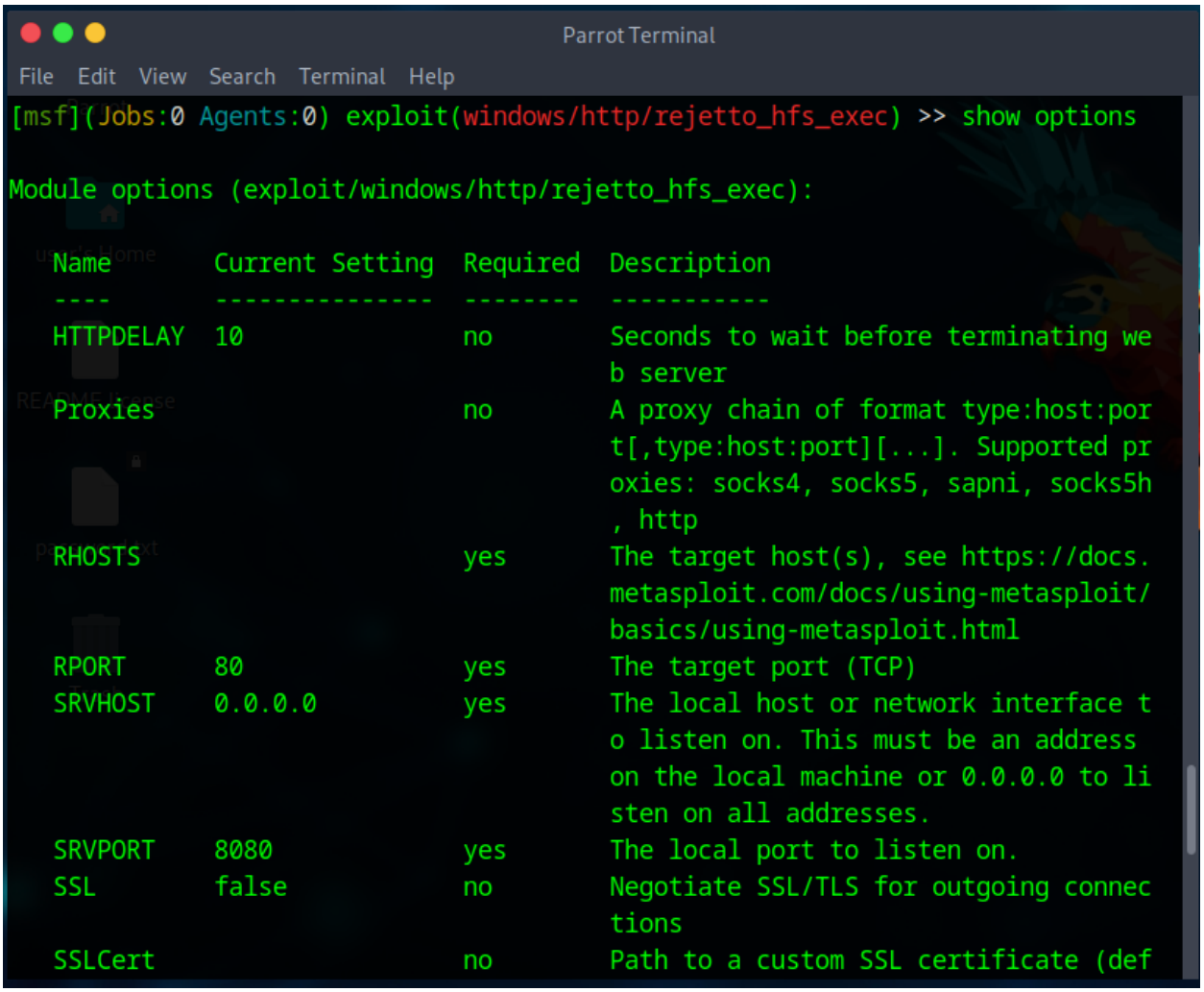


Fuente. Autoría Propia.

Una vez seleccionado el exploit adecuado, nos aseguramos de conocer los parámetros que se necesitan para su ejecución. Para ello mostramos las opciones ingresando el comando <***show options***>.

Figura 18

Parámetros necesarios para ejecutar el exploit.

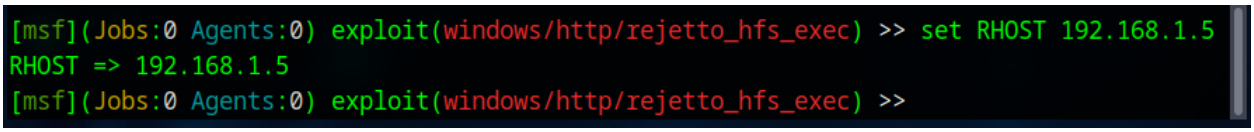


Fuente. Autoría Propia.

A continuación, ingresamos los parámetros necesarios correspondientes a la dirección IP del Host A en el cual se ejecutará el exploit para explotar la vulnerabilidad. Esto se consigue con el comando <***set RHOST 192.168.1.5***>.

Figura 19

Seleccionando la IP para la ejecución del exploit.

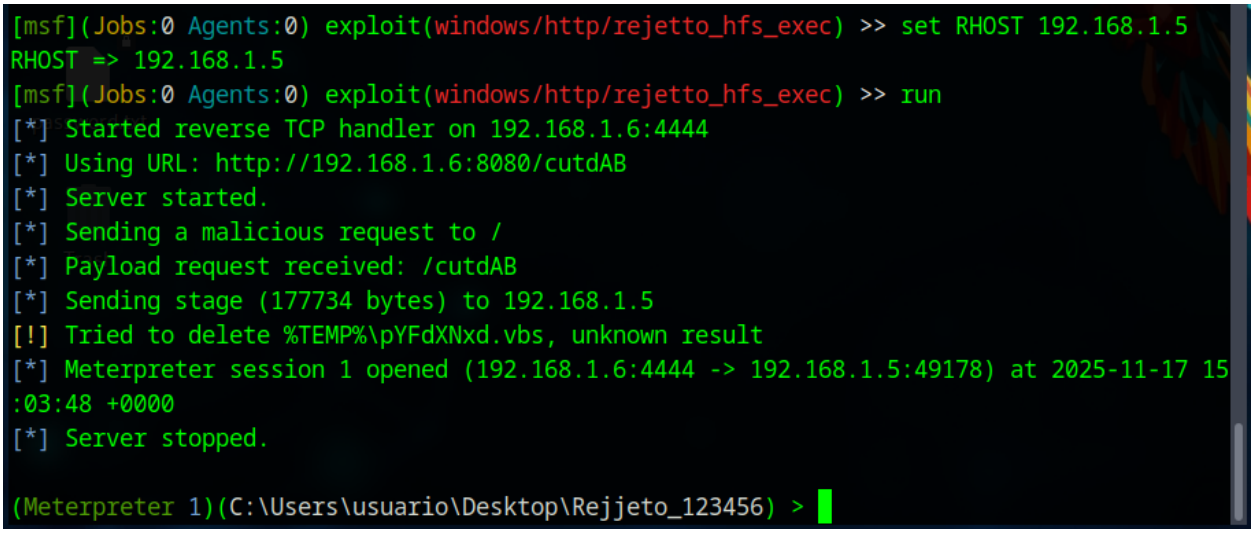


Fuente. Autoría Propia.

Habiendo realizado el paso anterior, procedemos a ingresar el comando <***run***> para ejecutar el exploit.

Figura 20

Ejecución del exploit.



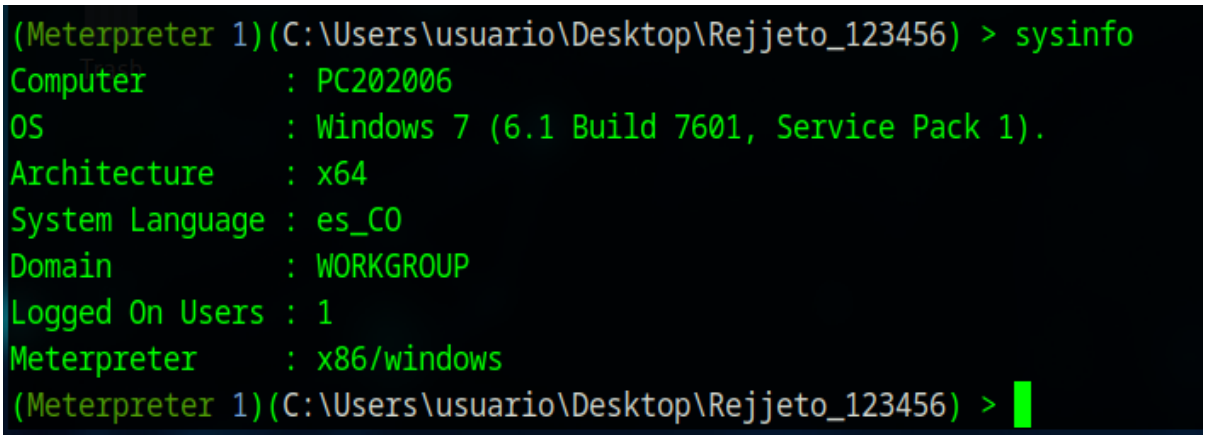
Fuente. Autoría Propia.

La ejecución del exploit nos permite abrir una sesión en el Host A desde donde podemos hacer el Pivoting al Host B.

Para comprobar que estamos dentro del Host A ingresamos el comando <***sysinfo***> que nos desplegará información por pantalla referente al sistema operativo accedido.

Figura 21

Información del Host A.



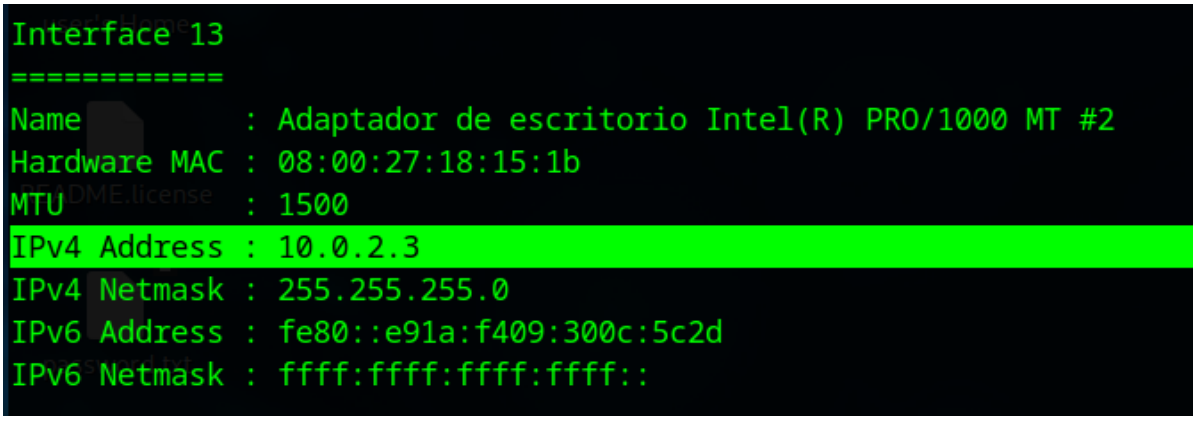
Fuente. Autoría Propia.

Post-explotación

Ahora comprobamos cuantas direcciones IP tiene el Host A para identificar las redes y los posibles Host pertenecientes a ellas. Para conseguir esto utilizamos el comando <***ipconfig***>.

Figura 22

Nueva IP del Host A

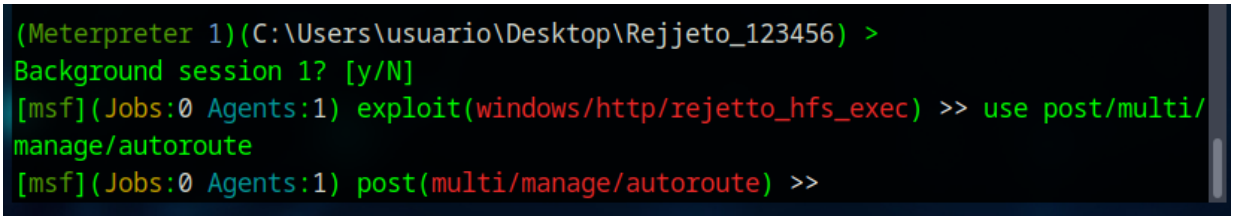


Fuente. Autoría Propia.

El siguiente paso a realizar es establecer la auto ruta hacia la red interna del Host A. Salimos momentáneamente de la sesión con <**Ctrl + Z**> para enrutar el tráfico hacia la maquina atacante. Ingresamos el comando <***use post/multi/manage/autoroute***>

Figura 23

Cargando el exploit autoroute

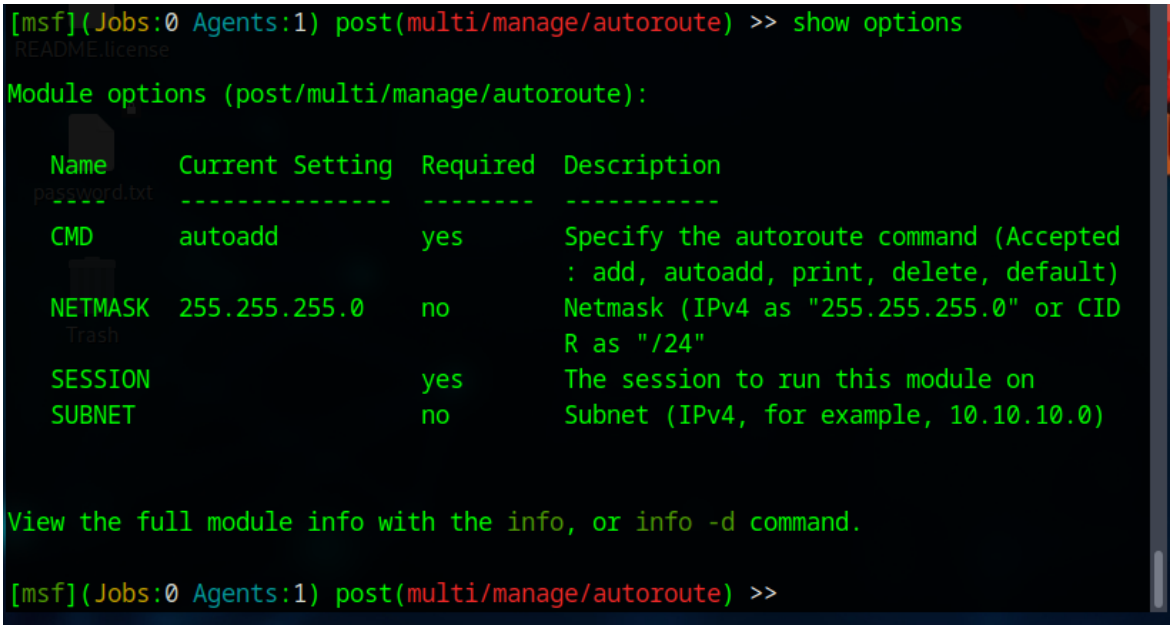


Fuente. Autoría Propia.

Con el comando <***show options***> podemos conocer los parámetros necesarios que se deben ingresar para ejecutar el exploit.

Figura 24

Parámetros para el autoroute.

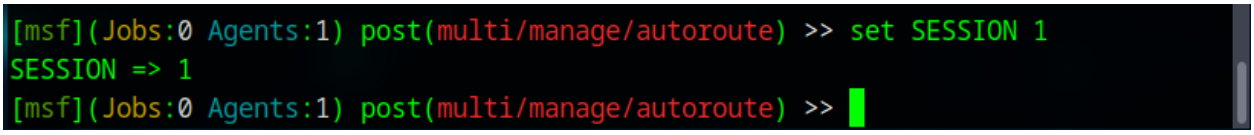


Fuente. Autoría Propia.

La información en pantalla nos muestra que solo se necesita como parámetro la sesión que se está ejecutando. Con el comando <***set SESSION 1***> ingresamos el dato que se nos pedía.

Figura 25

Estableciendo la sesión para autoroute

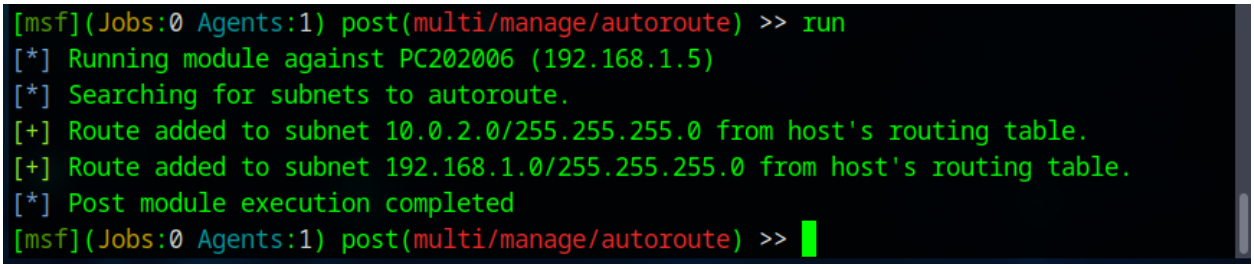


Fuente. Autoría Propia.

Seguidamente ejecutamos el exploit con el comando <***run***>. Esto permite enrutar el tráfico de la máquina objetivo a la maquina atacante.

Figura 26

Ejecutando el exploit de autoroute

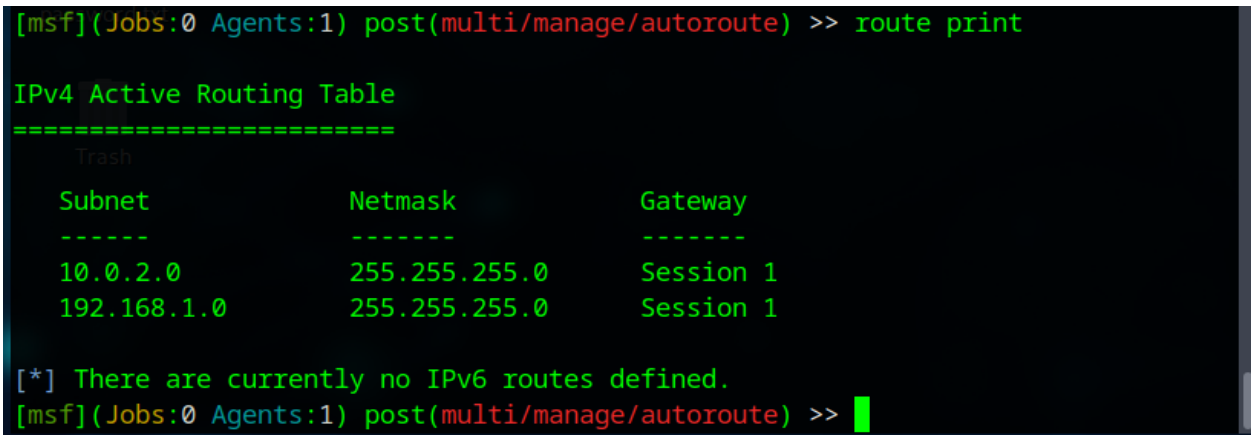


Fuente. Autoría Propia.

Una vez ejecutado el exploit, procedemos a comprobar el enrutamiento ingresando el comando <***route print***> como se muestra a continuación.

Figura 27

Comprobación del enrutamiento.

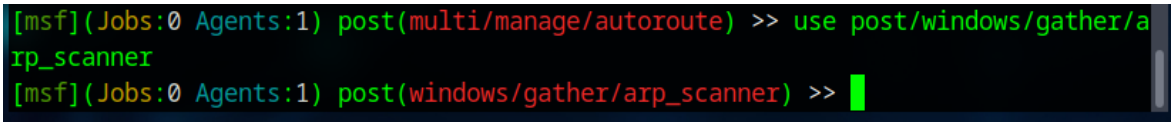


Fuente. Autoría Propia.

Esto nos muestra que el tráfico de la red interna del Host A será dirigido hacia la red de la máquina atacante. A continuación, necesitamos conocer los Host que pertenecen a la red interna del Host A buscando conocer la dirección IP del Host B que será la máquina objetivo del ataque. Para realizar esto debemos utilizar un exploit que nos sirva para tal fin. Cargamos el exploit arp scanner haciendo uso del comando <***use post/windows/gather/arp_scanner***>.

Figura 28

Cargando el exploit arp_scanner.

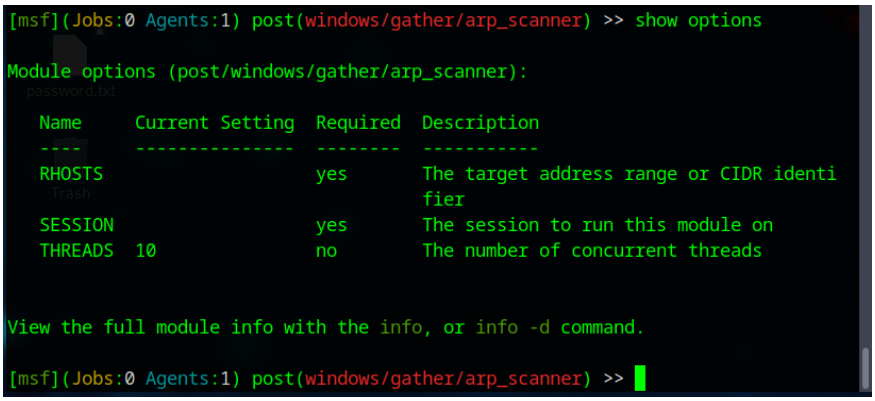


Fuente. Autoría Propia.

Ingresando el comando <***show options***> nos informamos de los parámetros necesarios que se deben ingresar para ejecutar el exploit.

Figura 29

Parámetros necesarios para arp_scanner.

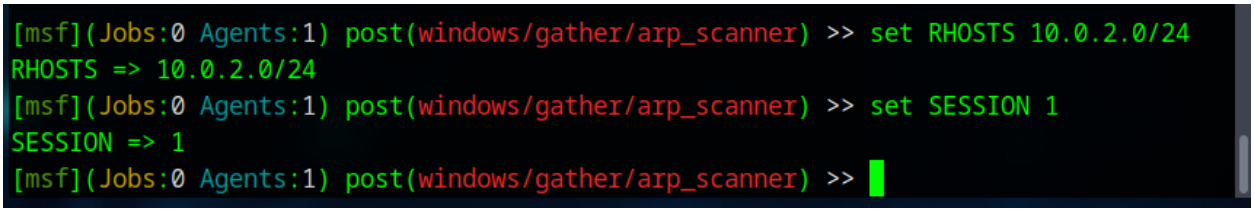


Fuente. Autoría Propia.

Ahora procedemos a ingresar los parámetros que nos piden para la ejecución del exploit con los comandos <***set RHOSTS 10.0.2.0/24***> y <***set SESSION 1***>

Figura 30

Ingreso de parámetros para arp_scanner.

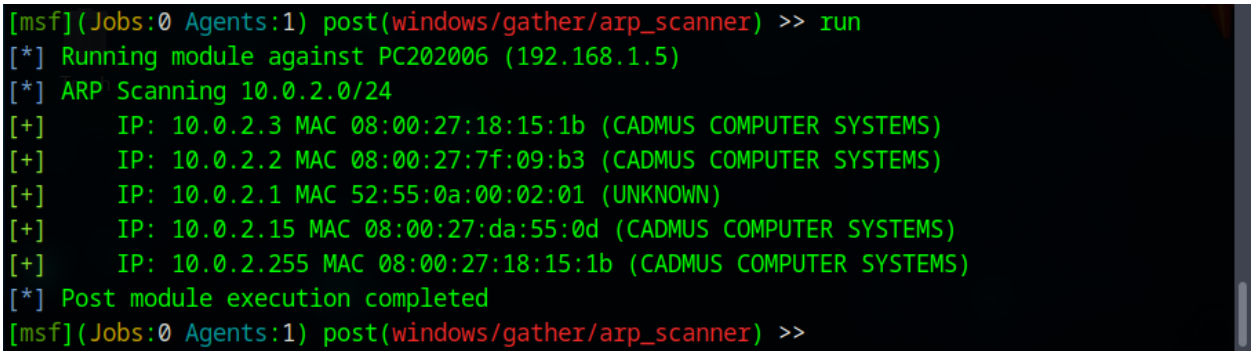


Fuente. Autoría Propia.

Seguidamente procedemos a ejecutar el exploit con el comando <***run***> para que se nos escanee la red y podamos encontrar los equipos pertenecientes a ella.

Figura 31

Ejecución del exploit arp_scanner.



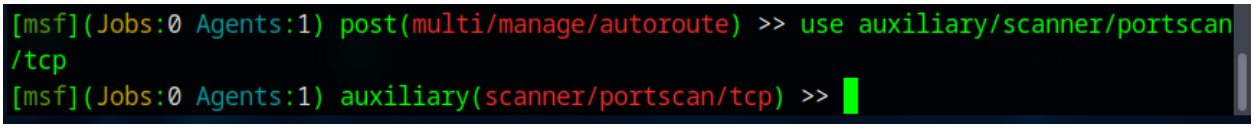
Fuente. Autoría Propia.

Se puede observar que se ha hallado la dirección IP 10.0.2.15 que pertenece al Host B que se buscaba.

Continuando con el proceso, realizamos un escaneo de los puertos abiertos del Host B cargando el módulo tcp_scanner con el comando <***use auxiliary/scanner/portscan/tcp***>

Figura 32

Carga del módulo PortScan

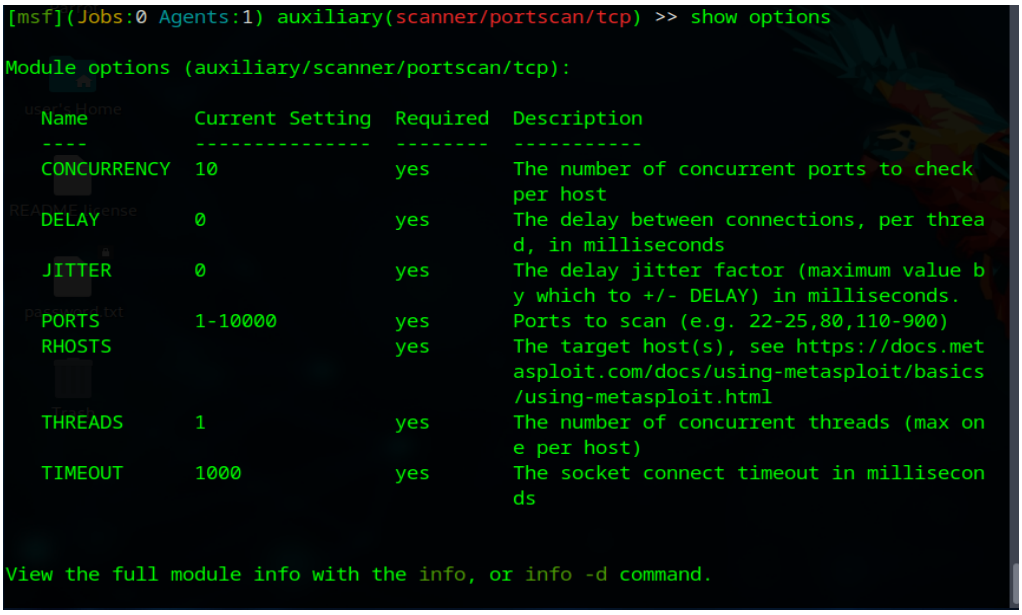


Fuente. Autoría Propia.

Seguidamente consultamos las opciones para conocer los campos obligatorios que son necesarios para la ejecución del módulo. Ingresamos <***show options***>

Figura 33

Opciones de PortScan

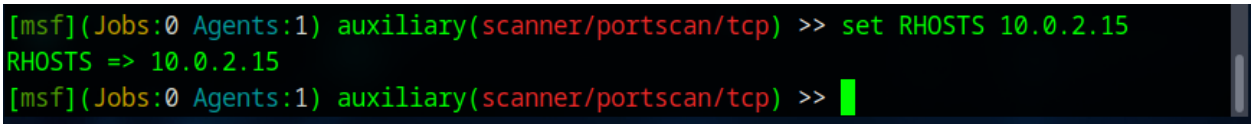


Fuente. Autoría Propia.

Luego ingresamos todos los parámetros obligatorios que fueron consultados.

Figura 34

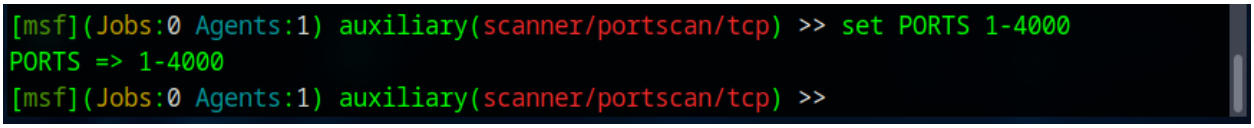
Configurando el Host para el escaneo



Fuente. Autoría Propia.

Figura 35

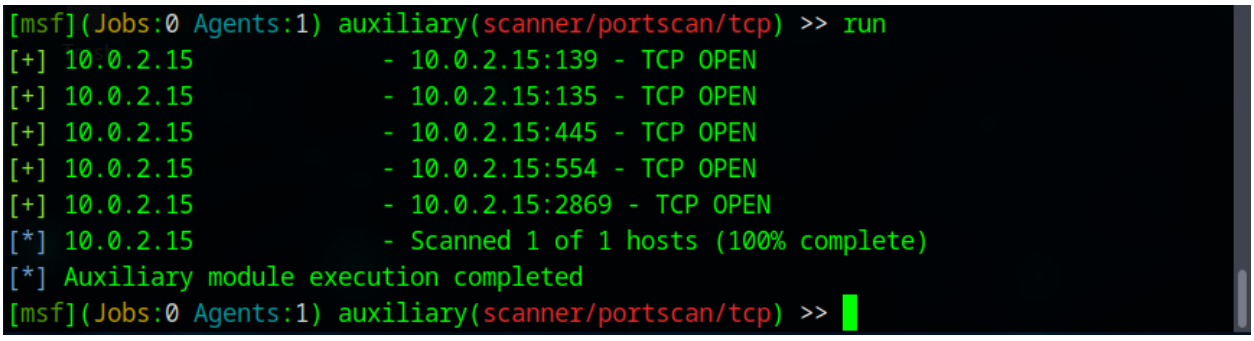
Selección de 4000 puertos a escanear



Fuente. Autoría Propia.

Figura 36

Ejecutando PortScan

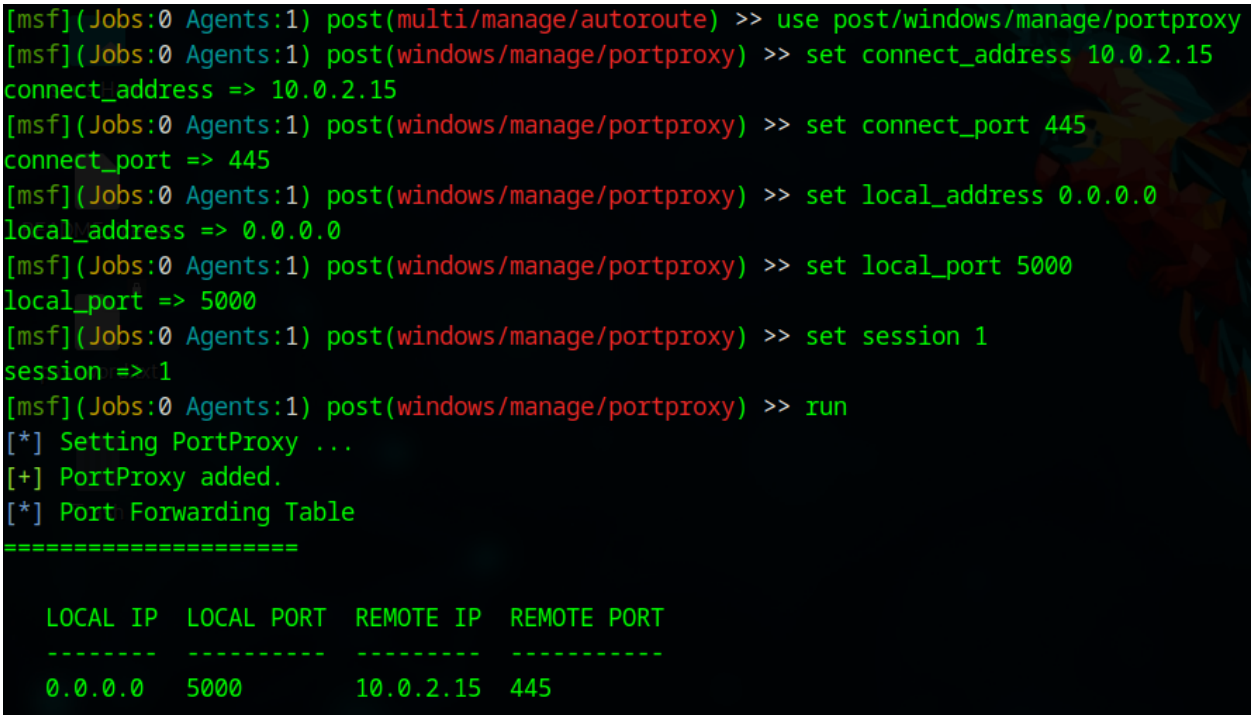


Fuente. Autoría Propia.

Ahora podemos configurar los puertos de escucha con PortProxy. PortProxy permitirá que todo el tráfico de la máquina atacante se dirija a un puerto específico del Host B para poder acceder al mismo. Cargamos el módulo con el comando <***use auxiliary/scanner/portscan/tcp***>. Después de cargar el módulo, ingresamos los parámetros obligatorios para su posterior ejecución. Entre estos parámetros obligatorios encontramos la dirección IP del Host al cual nos queremos conectar que en este caso sería la dirección IP del Host B, el puerto de conexión, la dirección local, el puerto de conexión local y la sesión que se está utilizando.

Figura 37

Configuración y ejecución de PortProxy



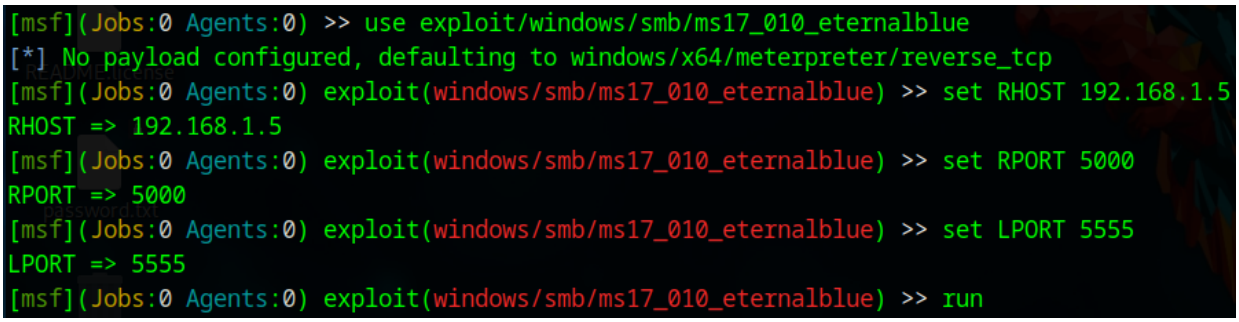
Fuente. Autoría Propia.

Después de ejecutar el comando anterior, debemos ejecutar un exploit que nos permita acceder al Host B. Este módulo es ms17_010 conocido como EternalBlue que nos dará acceso a la maquina atacada usando como puente el Host A.

En la **Figura 38** se nos muestran los comandos necesarios para cargar, configurar y ejecutar el exploit.

Figura 38

Configuración y ejecución de ms17_010



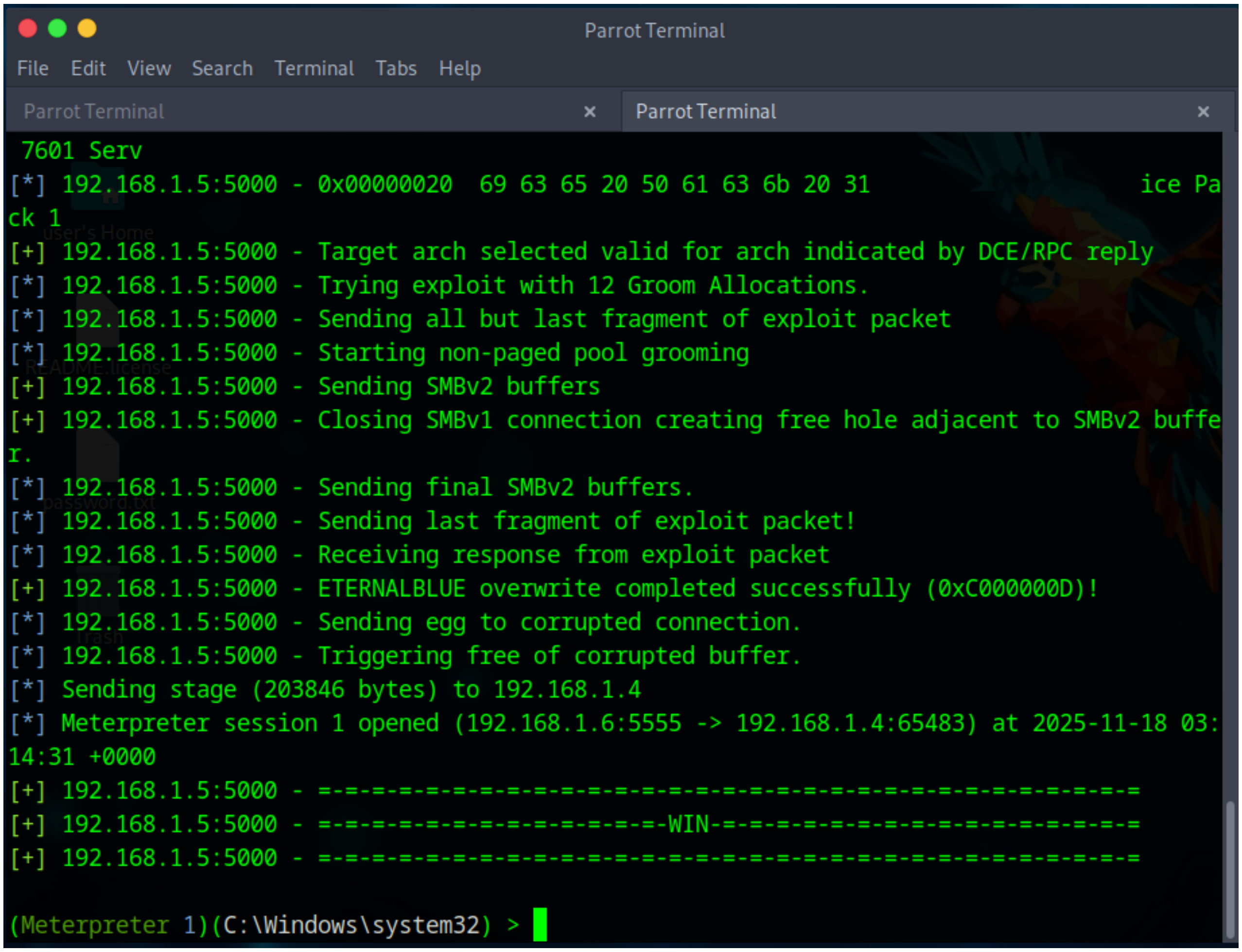
Fuente. Autoría Propia.

Entre los parámetros que se deben ingresar para que el exploit tenga éxito está la dirección IP y el puerto remoto que se desea atacar, también se debe ingresar el puerto local de escucha. Luego de haber ejecutado el exploit tendremos acceso al Host B. En la **Figura 39** podemos ver el resultado de la ejecución. Hemos logrado acceder al Host B utilizando de pivoting al Host A.

Ahora podemos llevar cabo todas las acciones que queramos porque ya tendremos iniciada una sesión que nos permitirá ejecutar comandos remotamente.

Figura 39

Acceso al Host B.

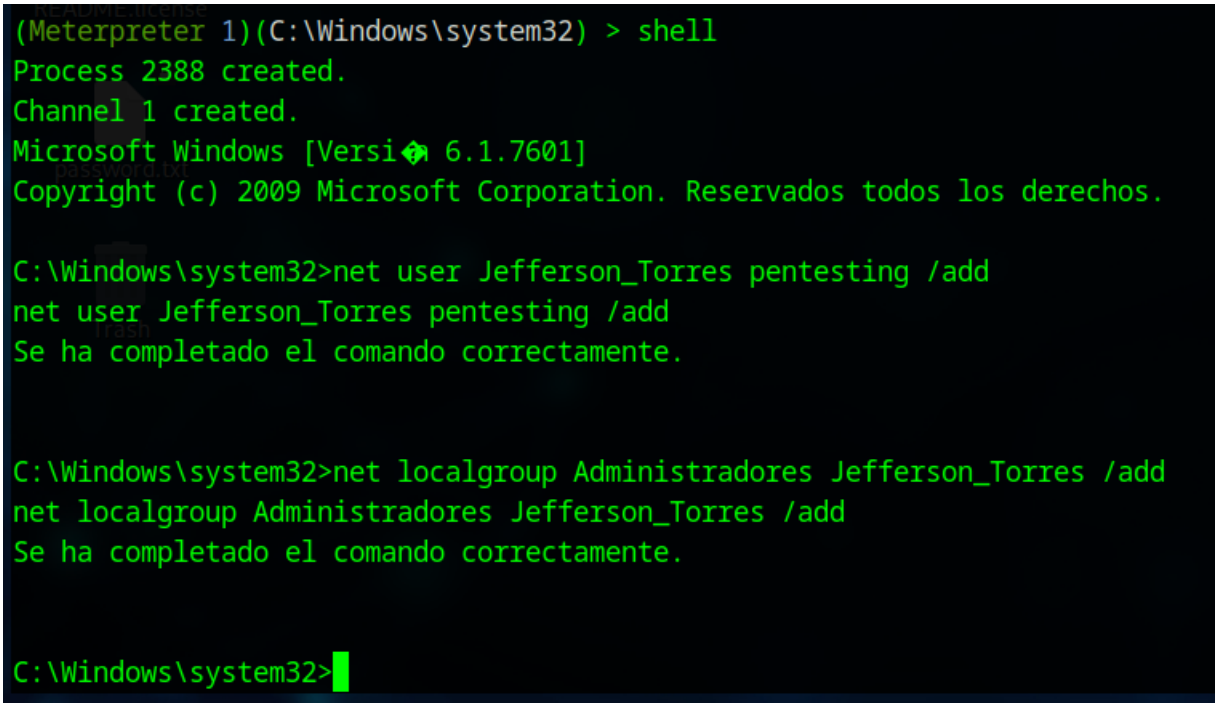


Fuente. Autoría Propia.

Una vez tenemos acceso a la maquina objetivo, realizaremos las acciones necesarias para crear un usuario temporal. Esto lo hacemos a través de una Shell de Windows para crear el usuario

Figura 40

Creación del usuario en el Host B.

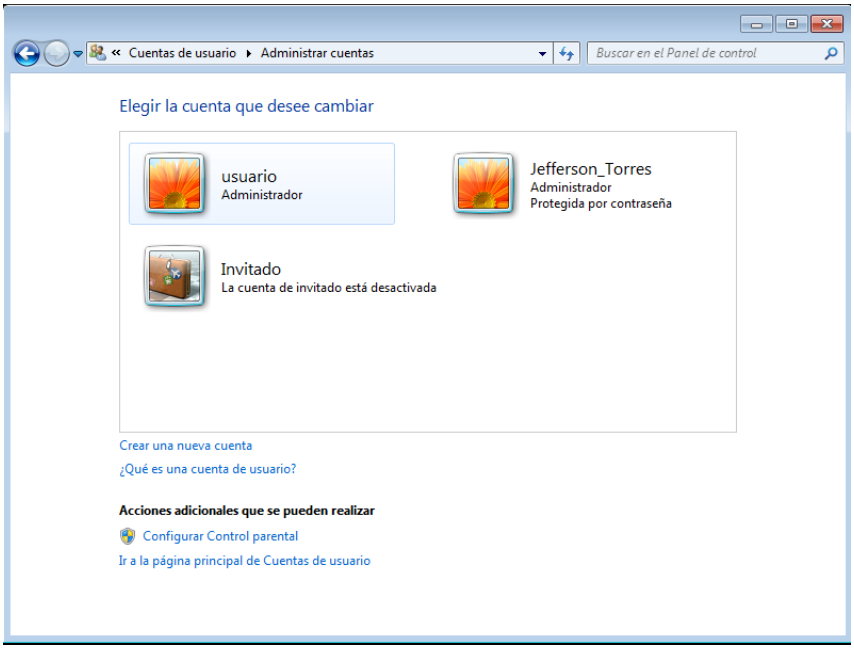


Fuente. Autoría Propia.

Una vez creado el usuario, procedemos a realizar la comprobación en la maquina objetivo donde se observa el éxito de la operación.

Figura 41

Evidencia de la creación de cuenta de usuario.



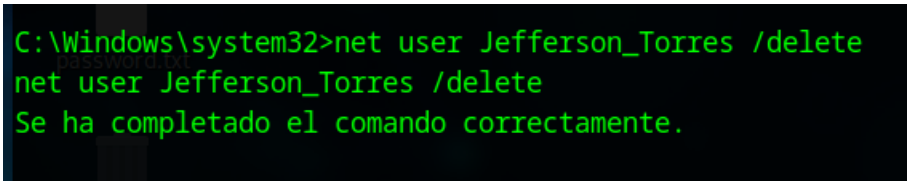
Fuente. Autoría Propia.

Eliminación de Huellas

Como último paso procedemos a eliminar la cuenta creada para la eliminación de rastros sobre la operación realizada.

Figura 42

Eliminación de la cuenta temporal.



Fuente. Autoría Propia.

Datos que Permitieron Identificar las Fallos de Seguridad

Los datos que permitieron identificar el fallo de seguridad se listan a continuación.

Aplicación Vulnerable

Este dato permitió conocer que, a través de la ejecución de una aplicación con fallas de seguridad, se estableció una brecha en la seguridad que le permitió al atacante ejecutar comandos de manera remota que le permitieran acceder a la máquina víctima utilizando un Shell que le sirviera para escalar privilegios y realizar el Pivoting.

Creación de Usuario Administrativo

Este es un dato de suma importancia porque revela que hubo un acceso ilegal a la máquina atacada donde se creó un usuario con altos privilegios con el objetivo de realizar actividades ilegales que permitieron la fuga de información.

Registros

Los registros fueron los datos que evidenciaron las actividades ilegales que se realizaron en el Host A para acceder al Host B donde se pudo comprobar que se utilizó al Host A fue utilizado como trampolín para el acceso al Host B donde residía la información que fue hurtada.

Herramientas Utilizadas para Identificar los Fallos de Seguridad

Una vez replicadas las actividades ilegales en una prueba controlada, se pudieron identificar los fallos de seguridad utilizando las siguientes herramientas.

Nmap

Esta herramienta permitió que se identificaran los puertos abiertos y los servicios que se ejecutaban en la máquina Windows. Al conocer el servicio en ejecución, se pudo comprobar que

se estaba ejecutando una versión que no estaba actualizada y que contenía un fallo de seguridad muy grave.

Metasploit

Herramienta utilizada para la explotación de la vulnerabilidad encontrada en la máquina Windows y que permitía acceder al Host A obteniendo una Shell para la ejecución de comandos de manera remota.

Puerto que Abre la Aplicación

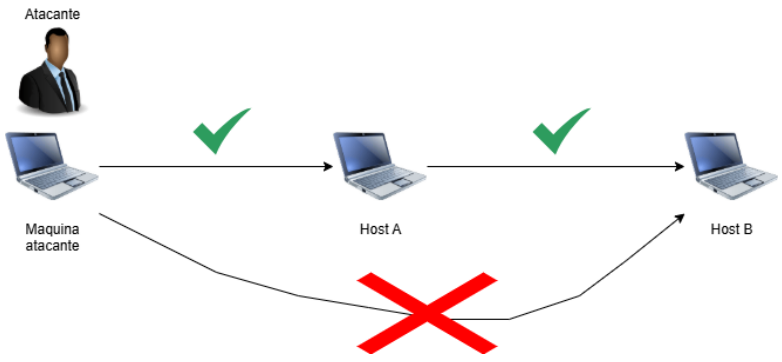
La aplicación utilizada en la máquina Windows es “rejetto 2.3” que cuando se ejecuta abre el puerto 80 para la comunicación ftp y que en este caso fue el puerto utilizado para la intrusión en el Host A.

Afectación del ataque a las máquinas (Windows) encontradas en la red

En primer lugar, tenemos el escenario desde el comienzo donde el atacante no tiene acceso directo al Host B que es la maquina objetivo del ataque.

Figura 43

Escenario inicial del ataque.

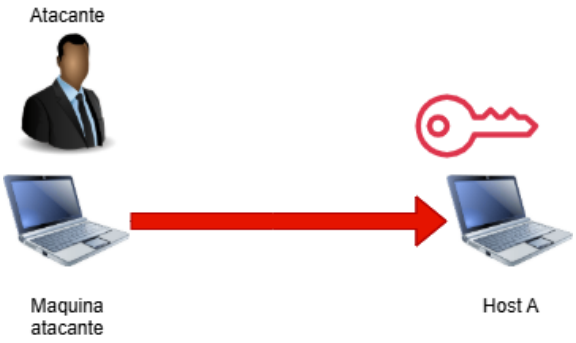


Fuente. autoría Propia.

Luego tenemos la afectación del Host A por medio de una vulnerabilidad encontrada en la aplicación Rejetto 2.3 que le permitió al atacante el acceso a la máquina. En este caso el Host A quedo bajo el control del atacante quien lo uso de puente para llegar al Host B.

Figura 44

Acceso al Host A por la maquina atacante.

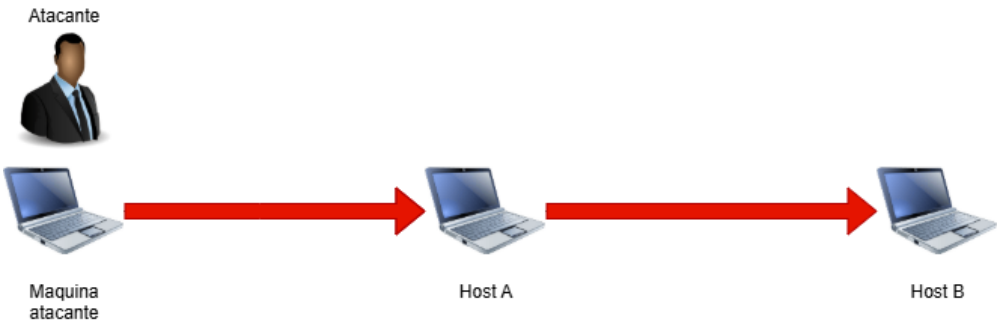


Fuente. Autoría Propia.

Una vez obtenido el control del Host A, el atacante realizo un movimiento lateral para llegar hasta el Host B con el objetivo de tener acceso y escalar privilegios.

Figura 45

Conexión al Host B por la maquina atacante.

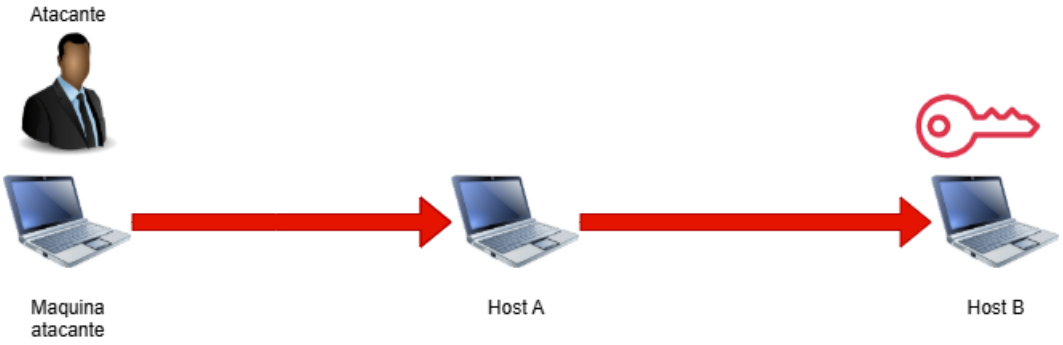


Fuente. Autoría Propia.

Es aquí donde se crea una cuenta con permisos administrativos que le da control al atacante para realizar las acciones delictivas.

Figura 46

Acceso al Host B por la maquina atacante.

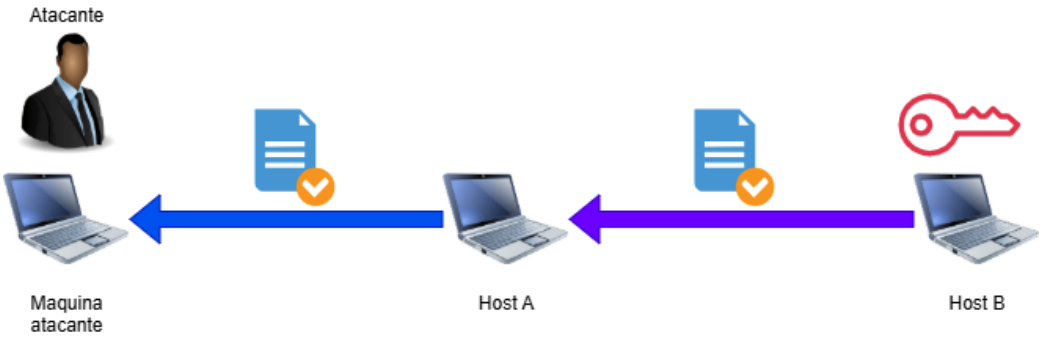


Fuente. Autoría Propia.

Una vez se escalaron los privilegios, el atacante procedió a realizar la extracción de información privilegiada que afecto a la organización a la cual pertenecen los activos atacados.

Figura 47

Extracción de información del Host B.



Fuente. Autoría Propia.

Este tipo de ataque afecta a las maquinas Windows encontradas debido a que estas no se encuentran en su versión más actualizada donde se han corregido multitud de vulnerabilidades que fueron explotadas en este caso.

Pasos para Validación de la Vulnerabilidad en la Máquina Windows

Los pasos ejecutados para la validación de la vulnerabilidad encontrada en la maquina Windows consistieron en lo siguiente:

Escaneo de Red

Utilizando el software Nmap se escaneo la red a la cual pertenecía la IP de la maquina atacante para encontrar los equipos pertenecientes a la misma. Esto permitió identificar el Host A que sería usado posteriormente como puente para acceso al host B.

Escaneo de Puertos y Servicios

Utilizando el mismo software anteriormente (Nmap) se escaneo la dirección IP del Host A para encontrar los puertos abiertos y los servicios ejecutados en ellos. Este escaneo permitió identificar que en el puerto 80 se estaba ejecutando un servicio HTTP con un software que contaba con una vulnerabilidad que ya estaba corregida en versiones posteriores.

Explotación de Vulnerabilidades

Haciendo uso del software Metasploit se explotó la vulnerabilidad encontrada en el servicio ejecutado para el acceso al Host A.

Movimiento Lateral

Estando dentro del Host A se procedió a realizar el salto a la subred en la cual se encontraba el Host B. En este paso se realizó nuevamente el escaneo de red al igual que el de

puertos y servicios para identificar la IP del Host B y los puertos que serían atacados para obtener acceso.

Escalada de Privilegios

Habiendo tenido acceso al Host B, se realizaron acciones para escalar privilegios. Esto se logró creando una cuenta con permisos administrativos para acceder a la información privilegiada.

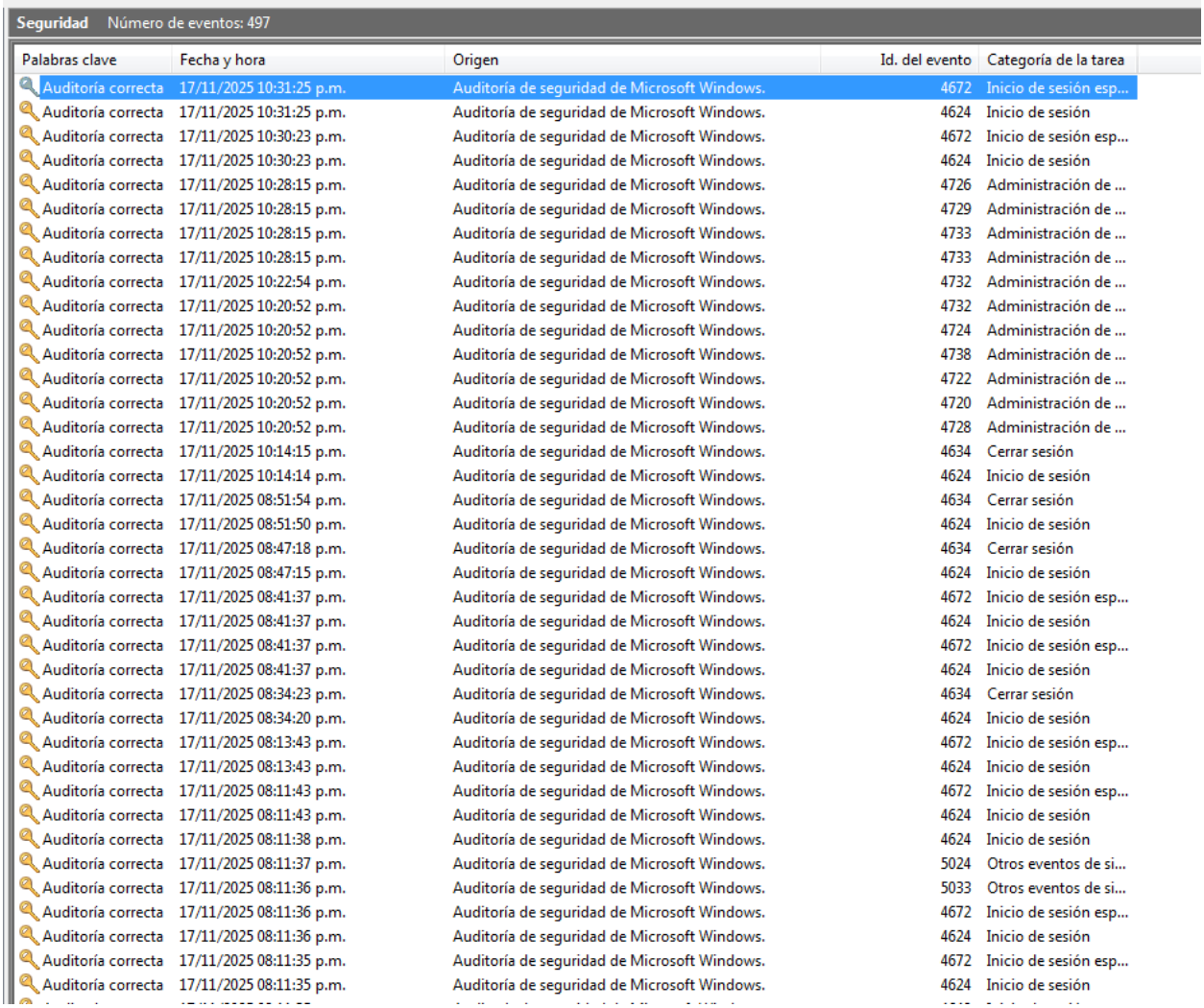
Eliminación de Huellas

Como último paso se eliminó la cuenta administrativa con el objetivo de borrar las huellas del acceso al Host B.

Los Logs de la maquina atacada muestran las acciones realizadas que permiten comprobar que hubo una vulneración de la seguridad.

Figura 48

Registros de la maquina atacada



Seguridad Número de eventos: 497

Palabras clave	Fecha y hora	Origen	Id. del evento	Categoría de la tarea
Auditoría correcta	17/11/2025 10:31:25 p.m.	Auditoría de seguridad de Microsoft Windows.	4672	Inicio de sesión esp...
Auditoría correcta	17/11/2025 10:31:25 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión
Auditoría correcta	17/11/2025 10:30:23 p.m.	Auditoría de seguridad de Microsoft Windows.	4672	Inicio de sesión esp...
Auditoría correcta	17/11/2025 10:30:23 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión
Auditoría correcta	17/11/2025 10:28:15 p.m.	Auditoría de seguridad de Microsoft Windows.	4726	Administración de ...
Auditoría correcta	17/11/2025 10:28:15 p.m.	Auditoría de seguridad de Microsoft Windows.	4729	Administración de ...
Auditoría correcta	17/11/2025 10:28:15 p.m.	Auditoría de seguridad de Microsoft Windows.	4733	Administración de ...
Auditoría correcta	17/11/2025 10:28:15 p.m.	Auditoría de seguridad de Microsoft Windows.	4733	Administración de ...
Auditoría correcta	17/11/2025 10:22:54 p.m.	Auditoría de seguridad de Microsoft Windows.	4732	Administración de ...
Auditoría correcta	17/11/2025 10:20:52 p.m.	Auditoría de seguridad de Microsoft Windows.	4732	Administración de ...
Auditoría correcta	17/11/2025 10:20:52 p.m.	Auditoría de seguridad de Microsoft Windows.	4724	Administración de ...
Auditoría correcta	17/11/2025 10:20:52 p.m.	Auditoría de seguridad de Microsoft Windows.	4738	Administración de ...
Auditoría correcta	17/11/2025 10:20:52 p.m.	Auditoría de seguridad de Microsoft Windows.	4722	Administración de ...
Auditoría correcta	17/11/2025 10:20:52 p.m.	Auditoría de seguridad de Microsoft Windows.	4720	Administración de ...
Auditoría correcta	17/11/2025 10:20:52 p.m.	Auditoría de seguridad de Microsoft Windows.	4728	Administración de ...
Auditoría correcta	17/11/2025 10:14:15 p.m.	Auditoría de seguridad de Microsoft Windows.	4634	Cerrar sesión
Auditoría correcta	17/11/2025 10:14:14 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión
Auditoría correcta	17/11/2025 08:51:54 p.m.	Auditoría de seguridad de Microsoft Windows.	4634	Cerrar sesión
Auditoría correcta	17/11/2025 08:51:50 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión
Auditoría correcta	17/11/2025 08:47:18 p.m.	Auditoría de seguridad de Microsoft Windows.	4634	Cerrar sesión
Auditoría correcta	17/11/2025 08:47:15 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión
Auditoría correcta	17/11/2025 08:41:37 p.m.	Auditoría de seguridad de Microsoft Windows.	4672	Inicio de sesión esp...
Auditoría correcta	17/11/2025 08:41:37 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión
Auditoría correcta	17/11/2025 08:41:37 p.m.	Auditoría de seguridad de Microsoft Windows.	4672	Inicio de sesión esp...
Auditoría correcta	17/11/2025 08:41:37 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión
Auditoría correcta	17/11/2025 08:34:23 p.m.	Auditoría de seguridad de Microsoft Windows.	4634	Cerrar sesión
Auditoría correcta	17/11/2025 08:34:20 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión
Auditoría correcta	17/11/2025 08:13:43 p.m.	Auditoría de seguridad de Microsoft Windows.	4672	Inicio de sesión esp...
Auditoría correcta	17/11/2025 08:13:43 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión
Auditoría correcta	17/11/2025 08:11:43 p.m.	Auditoría de seguridad de Microsoft Windows.	4672	Inicio de sesión esp...
Auditoría correcta	17/11/2025 08:11:43 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión
Auditoría correcta	17/11/2025 08:11:38 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión
Auditoría correcta	17/11/2025 08:11:37 p.m.	Auditoría de seguridad de Microsoft Windows.	5024	Otros eventos de si...
Auditoría correcta	17/11/2025 08:11:36 p.m.	Auditoría de seguridad de Microsoft Windows.	5033	Otros eventos de si...
Auditoría correcta	17/11/2025 08:11:36 p.m.	Auditoría de seguridad de Microsoft Windows.	4672	Inicio de sesión esp...
Auditoría correcta	17/11/2025 08:11:36 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión
Auditoría correcta	17/11/2025 08:11:35 p.m.	Auditoría de seguridad de Microsoft Windows.	4672	Inicio de sesión esp...
Auditoría correcta	17/11/2025 08:11:35 p.m.	Auditoría de seguridad de Microsoft Windows.	4624	Inicio de sesión

Fuente. Autoría Propia.

Fase 4. Respuesta y Contención ante Incidentes de Seguridad

Indagaciones ante un Ataque en Tiempo Real

En la actualidad, existen diferentes tipos de ataques informáticos que pueden comprometer seriamente la seguridad del sistema informático de SecureNova Labs. Existe los ataques de tipo ransomware que se caracteriza por encriptar la información de un sistema para posteriormente pedir un rescate económico por la información, los ataques de tipo DoS que buscan inhabilitar un servicio determinado enviando un gran número de peticiones a un servidor para que este no las pueda responder a todas y se bloquee, los ataques de tipo inyección SQL que se vale de un conjunto de técnicas para acceder de manera ilegal a la información que reside en una base de datos. Debido a la gran variedad de ataque se debe tener claro que es lo que está ocurriendo en todo momento para que la reacción sea oportuna.

Ante un ataque informático en tiempo real lo primero que la organización SecureNova Labs debería investigar es el tipo de ataque que se está llevando a cabo para implementar las medidas correctivas que permitan su contención. Conocer el tipo de ataque permitirá que se pueda identificar la técnica utilizada por los atacantes para alcanzar su objetivo y así reaccionar de manera efectiva para la mitigación del mismo. Cabe destacar que la indagación del tipo de ataque es de mucha premura, pues entre más tiempo este comprometido el sistema de la organización, mayores serán las consecuencias producto del ataque.

Medidas de Hardenización para Evitar que se Repita el Ataque

Para el fortalecimiento de la ciberseguridad del sistema informático de SecureNova Labs se hace necesario implementar algunas acciones que robustezcan la seguridad y logren salvaguardar la información y los activos de la organización. Entre estas medidas tenemos:

Actualización del Sistema Operativo. Contar con la última versión del sistema operativo Windows utilizado en SecureNova Labs brindará mayor seguridad al sistema informático debido a que las versiones más actualizadas corrigen errores críticos que afectan la seguridad digital.

Actualización de Software. SecureNova Labs debe implementar un cronograma para la actualización de software porque un software desactualizado puede contener fallas de seguridad (Souppaya & Scarfone, 2021). Esto se hace evidente en la utilización de Rejetto 2.3 que cuenta con una vulnerabilidad crítica que ante un ciberataque facilita el acceso a la información sensible poniendo en riesgo los procesos operativos de las organizaciones.

Implementar Firewalls de Última Generación. Los firewalls son dispositivos que brindan seguridad perimetral y son la primera barrera entre una red privada y una pública como internet. SecureNova Labs debe implementar este tipo de herramienta que ayuda a restringir el acceso no autorizado logrando bloquear ataques maliciosos.

Administración de Puertos. SecureNova Labs debe administrar correctamente los puertos de comunicación con los que cuenta sistema informático para fortalecer la seguridad. Esto requiere que los puertos que no son usados por ninguna aplicación o servicio sean cerrados para evitar el acceso no autorizado.

Implementar IDS/IPS. Como medida adicional en la capa de seguridad digital de SecureNova Labs es necesario la implementación de sistema de detección de intrusiones robusto que monitoree en tiempo real las actividades que se realicen para evitar el acceso no autorizado y en caso de detectar actividades maliciosas se puedan tomar acciones inmediatas que mitiguen la falla de seguridad.

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

El equipo de ciberseguridad Blue Team se encarga de tomar las medidas necesarias para proteger los activos y los sistemas informáticos de las organizaciones a las que estos pertenecen implementando las técnicas más efectivas para tal fin. Blue Team establece controles, realiza un continuo monitoreo de la red e implementa acciones que le permitan estar preparados en todo momento para contener un ataque informático (Kotwani et al., 2023). En base a este objetivo, las acciones realizadas por Blue Team se enfocan tanto en la prevención como en la contención de incidentes de seguridad.

Un equipo de respuesta a incidentes informáticos enfoca todos sus esfuerzos en la contención de incidentes de seguridad buscando en todo momento limitar los daños a los sistemas e implementar acciones para evitar que el ataque se propague a los activos que aún no están comprometidos. El objetivo primordial de este equipo de ciberseguridad es la contención, erradicación y la recuperación ante la ocurrencia de un ataque informático.

La principal diferencia que existe entre Blue Team y un equipo de respuesta a incidentes de seguridad radica en que Blue Team realiza acciones proactivas y reactivas, mientras que el equipo de contención de incidentes solo implementa acciones reactivas.

Utilización de CIS "Center For Internet Security" en un Equipo Blue Team

Cuando hablamos de CIS (Center For Internet Securit) nos referimos a un conjunto de prácticas que tienen como objetivo reducir las probabilidades de ataques a un sistema informático (Arredondo, 2024). Debido a la continua actualización de CIS, en SecureNova Labs se pueden mitigar grandemente las brechas de seguridad para tener protección ante las amenazas emergentes (Armis, 2021).

Dentro de un equipo de seguridad Blue Team en SecureNova Labs se utilizaría CIS para los siguientes aspectos:

Cumplir con la Normativa Actual. Los controles CIS van alineados con otras normativas como la NIST y la GDPR que facilitan a la organización SecureNova Labs que puedan poner en ejecución procesos regulatorios para evitar posibles sanciones por incumplimientos en proteger la información.

Robustecer la Seguridad. Al implementar recomendaciones de seguridad SecureNova Labs fortalecerá el sistema de información contra los posibles ataques permitiendo que se identifiquen y se corrijan las vulnerabilidades más conocidas robusteciendo los mecanismos de defensa.

Minimizar las Vulnerabilidades. Una vez implementadas las recomendaciones de seguridad SecureNova Labs tendrá un sistema más seguro mitigando las brechas de seguridad y minimizando los posibles ataques que pueden traer consecuencias legales, financieras y aquellas que tienen que ver con la reputación de la organización.

Optimizar Programas de Seguridad. Los controles CIS ayudan a que la organización SecureNova Labs mejore la eficiencia operativa estableciendo una guía de medidas de seguridad que sean de obligatorio cumplimiento para todos los empleados y colaboradores.

Mejorar la Administración de Recursos. La aplicación de CIS en SecureNova Labs permitirá identificar aquellas áreas que requieren mayor protección y que tienen un gran impacto en la seguridad de los activos y el sistema informático. Esto permitirá que la asignación de recursos de la organización se realice de manera eficiente dirigidos a las áreas de mayor importancia.

Funciones y Características Principales de un SIEM

Un SIEM (Securiry Information and Event Management) es un solución de gestión de eventos e información de seguridad clave en la ciberseguridad que permite recopilar, agregar y administrar amplios volúmenes de información contenida en diferentes dispositivos como servidores, dispositivos y datos de aplicación en tiempo real permitiéndole a los profesionales de la ciberseguridad detectar, investigar y responder a las ataques e incidentes de seguridad de manera oportuna para salvaguardar los sistemas de información (Microsoft, s. f.).

Las funciones principales son las siguientes:

Gestión de Registros. Los SIEM recopilan y analizan los registros de toda la infraestructura del sistema de información como los servidores, cortafuegos, dispositivos de red, puntos finales, datos de hardware y de software (IBM, 2023). El objetivo es identificar en tiempo real anomalías que indiquen una posible amenaza.

Correlación de Eventos. Una vez recopilados los datos, estos se analizan en busca de patrones que una vez correlacionados permitan detectar actividades que por sí solas parecen normales, pero que cuando se combinan con otras pueden indicar que existe un riesgo de seguridad. Un ejemplo de ello puede ser que se detecte que hay una cuenta comprometida, así como un tráfico inusual en la red, lo que un SIEM podría indicar que hay una relación entre estos dos eventos y generar una alerta de seguridad para que los equipos de seguridad realicen la correspondiente investigación (Microsoft, s. f.).

Respuesta a Incidentes y Monitorización. Las soluciones SIEM monitorean continuamente los sistemas informáticos y muestran su análisis en un panel central que le permite a los equipos de seguridad supervisar las actividades, clasificar las alertas, identificar las

amenazas y responder ante las mismas. Algunos SIEM puede responder automáticamente a las amenazas según las reglas establecidas por el SOC. Por ejemplo, ante la identificación de un malware un SIEM podría aislar el sistema comprometido según las reglas predefinidas.

Herramientas de Contención de Ataques Informáticos

Ante la ocurrencia de un ataque informático, se hace necesario implementar acciones que permitan contener el mismo. Para la contención de ataques informáticos tenemos las siguientes herramientas:

pfSense. Firewall Open Source de última generación basado en FreeBSD con funcionalidades avanzadas como balanceo de carga, servidor DHCP, VPN, cortafuegos de borde, entre otras características (Netgate, s. f.). Se puede utilizar para contener un ataque informático porque permite bloquear tráfico malicioso y aislar segmentos de red.

OPNsense. Firewall Open Source de última generación que es la alternativa a pfSense con funcionalidades comparables a las de los firewalls comerciales que ofrece entre sus funciones filtrado de paquetes en tiempo real, VPN, balanceo de carga, entre otras características (Luz, 2017). Se puede utilizar para contener un ataque informático porque permite bloquear tráfico malicioso

Wazuh. Plataforma de ciberseguridad open source que unifica XDR y SIEM en una única solución que permite detectar amenazas y responder a los incidentes de seguridad para su contención. Entre las funciones de esta herramienta tenemos que permite bloquear IPs, aislar host, aplicar reglas de cortafuegos (Wazuh, s. f.).

ModSecurity. Cortafuego para aplicaciones web (WAF) open source que ofrece seguridad a los sitios web y las aplicaciones contra ataque maliciosos como los de inyección SQL y XSS. Permite contener ataques porque bloquea en tiempo real las peticiones o respuestas sospechosas según las reglas predefinidas (Moreno, 2022).

Evidencias de sustentación

A continuación, en el siguiente enlace se relaciona el video de sustentación con el objetivo de cumplir con el requisito establecido en la Fase 5 del Seminario Especializado:

Video de sustentación del informe final: https://youtu.be/cwye2CkKOqw

Conclusiones

Como conclusión del informe se detalla que la ética profesional es un pilar fundamental en la carrera de ciberseguridad la cual debe estar por encima de salarios jugosos porque se podrían firmar acuerdos que infrinjan las normas legales vigentes lo cual es un delito muy grave. El documento de acuerdos ofrecido por la organización SecureNova Labs incumple las normas colombianas vigentes para la protección de los datos personales.

Igualmente, este informe detalla que a través de una prueba controlada donde se replicó un ataque de Pivoting, se pudo demostrar el proceder del atacante para el acceso a la maquina objetivo. En esta prueba se utilizó una máquina Parrot como máquina atacante la cual pudo comprometer una máquina Windows 7 (Host A) y utilizarla como puente para llegar a la máquina atacada (Host B) con Windows 7 donde se comprometió la seguridad y la información contenida en la misma.

Esta prueba revelo graves fallas de seguridad en SecureNova Labs que permitieron que algunas vulnerabilidades fueran explotadas para el acceso remoto a la maquina atacada. Entre las vulnerabilidades se encontraba la utilización de un software desactualizado utilizado para la comunicación. Adicionalmente se detectó el uso de un sistema operativo (Windows 7) desactualizado y sin soporte que contaba con una vulnerabilidad crítica que permitía al acceso a la máquina.

Estas brechas de seguridad en la organización permitieron que se vulnerara el sistema y se accediera a información privilegiada porque los controles establecidos no eran rigurosos debilitando las barreras de ciberseguridad que se deben implementar para la protección de los sistemas informáticos.

Es imprescindible que los equipos de profesionales en ciberseguridad tomen acciones que aborden el tema sobre las brechas en la seguridad de SecureNova Labs para mitigar o eliminar los posibles incidentes implementando software especializado para fortalecer los procesos llevados a cabo por SecureNova Labs.

Recomendaciones

Después del análisis realizado, se pudo comprobar que la seguridad en SecureNova Labs no es un factor prioritario y que los controles implementados no permiten salvaguardar de manera efectiva la información sensible del sistema informático. Las pruebas realizadas demostraron que existen brechas de seguridad críticas que permiten a los atacantes sobrepasar los controles establecidos y acceder a la información privilegiada de la organización.

Igualmente se subraya la importancia de adoptar medidas que aborden la seguridad de los activos de la organización como es el cifrado de información en tránsito y en reposo buscando que, ante cualquier intrusión al sistema, la información obtenida por los delincuentes no pueda ser divulgada

También se deben realizar inversiones que permitan implementar dispositivos hardware y software que brinden protección adicional al sistema como los cortafuegos de última generación y los IDS/IPS logrando que los equipos de ciberseguridad monitoreen continuamente la red para evitar al máximo los accesos no autorizados.

Por último, es importante que se realicen periódicamente simulaciones de ataques para que los equipos de respuesta a incidentes mejoren los controles de seguridad establecidos y se mitiguen las brechas de seguridad (Hernández, 2025). Entre las acciones que se deben implementar para el fortalecimiento de la seguridad está la formación en ciberseguridad para que los empleados de la organización pongan en práctica los conocimientos adquiridos.

Bibliografía

Alhamed, M., & Rahman, M. M. H. (2023). A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Applied Sciences, 13*(12), 6986. https://doi.org/10.3390/app13126986

Armis. (2021). What are the CIS Controls? *Armis*. https://www.armis.com/faq/what-are-the-cis-controls/

Arredondo, O. (2024, diciembre 4). *Controles CIS: Qué Son y Cómo Aplicarlos en tu Empresa*. https://www.deltaprotect.com/blog/controles-cis-ciberseguridad-empresa

Chindrus, C., & Caruntu, C.-F. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. *Information, 14*(11), 587. https://doi.org/10.3390/info14110587

Cilleruelo, C. (2022a, octubre 4). *¿Qué es ExploitDB?* https://keepcoding.io/blog/que-es-exploitdb/

Cilleruelo, C. (2022b, octubre 14). *5 Herramientas de postexplotación: Características y usos*. https://keepcoding.io/blog/herramientas-de-postexplotacion/

Copnia. (2015). *Código de ética*. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

FMS, P. (2023, diciembre 22). ¿Qué es CVE (Common Vulnerabilities and Exposures)? *Pandora FMS*. https://pandorafms.com/es/it-topics/que-es-cve/

Función Pública. (s. f.). *Decreto 1377 de 2013—Gestor Normativo*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Función Pública. (s. f.). *Ley 1273 de 2009—Gestor Normativo*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Genuino Cloud. (2023, enero 16). *¿Qué es NMAP?* https://genuinocloud.com/blog/que-es-nmap/

Greenbone. (s. f.). *OPENVAS - Open Vulnerability Assessment Scanner*. https://www.openvas.org/

Guarnizo Portela, M. P. (2024). *La naturaleza jurídica de los delitos informáticos en Colombia*. http://repository.unad.edu.co/handle/10596/41392

Hernández, J. (2025, abril 22). *Pentest, ¿qué es y por qué es tan importante para las empresas?* https://impactotic.co/ciber-seguridad/pentest-que-es-y-por-que-es-tan-importante/

IBM. (2023, enero 24). *¿Qué son las pruebas de penetración?* https://www.ibm.com/mx-es/think/topics/penetration-testing

IBM. (2023, junio 23). *¿Qué es SIEM?* https://www.ibm.com/es-es/think/topics/siem

Kotwani, B., Sawant, M. R., & Chopra, D. S. (2023). *Red Teaming vs. Blue Teaming: A Comparative Analysis of CyberSecurity Strategies in the Digital Battlefield – IJSREM*. https://ijsrem.com/download/red-teaming-vs-blue-teaming-a-comparative-analysis-of-cybersecurity-strategies-in-the-digital-battlefield/

Lopez, V. (2025, marzo 10). Pentesting: Qué es, para qué sirve y cómo realizar una prueba de penetración. *S2GRUPO*. https://s2grupo.es/pentesting-que-es-y-para-que-sirve/

Luz, S. D. (2017, febrero 4). *OPNsense: Conoce este completo firewall gratuito para instalar en tu red doméstica o empresa*. RedesZone. https://www.redeszone.net/2017/02/04/opnsense-conoce-este-completo-firewall-gratuito-instalar-red-domestica-empresa/

Microsoft. (s. f.). *¿Qué es SIEM?* https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

MINAMBIENTE. (s. f.). *Política de Protección de Datos Personales*. https://www.minambiente.gov.co/politica-de-proteccion-de-datos-personales/

MINTIC. (s. f.). *Políticas de Privacidad y Condiciones de Uso*. MINTIC Colombia. https://www.mintic.gov.co/portal/715/w3-article-2627.html

Moreno, M. (2022, junio 22). *ModSecurity: Qué es y cómo funciona—Cdmon*. https://www.cdmon.com/es/blog/mod-security-seguridad-para-tu-servidor

Netgate. (s. f.). *pfSense—World's Most Trusted Open Source Firewall*. https://www.pfsense.org/

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. *2011 IEEE 29th International Conference on Computer Design (ICCD)*, 285-288. https://doi.org/10.1109/ICCD.2011.6081410

Souppaya, M., & Scarfone, K. (2021). *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-40r4-draft

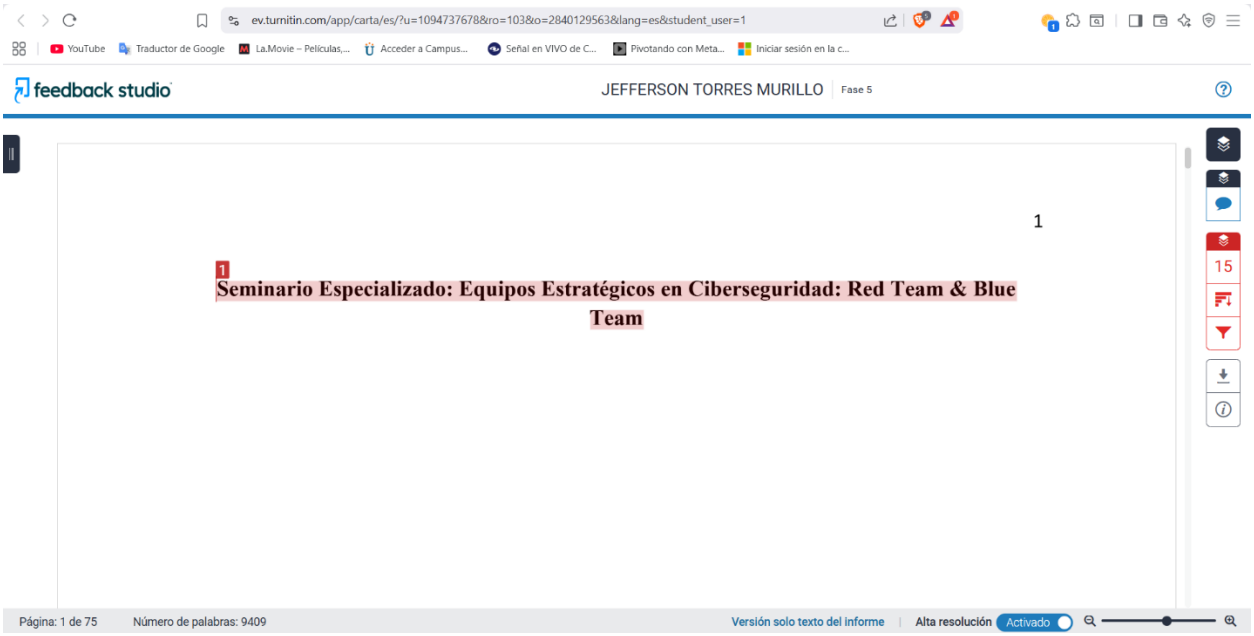
VLEX. (2014, mayo 13). *Decreto número 886 de 2014, por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos*. vLex. https://vlex.com.co/vid/2014-reglamenta-arta-culo-bases-datos-510980942

Wazuh. (s. f.). Overview. *Wazuh*. https://wazuh.com/platform/overview/

Apéndices

Apéndice A

Porcentaje Turnitin



Nota. Resultado arrojado por la herramienta Turnitin del documento que muestra el porcentaje de similitud con otras fuentes. *Fuente*. Autoría Propia.