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

Hernán Augusto Herrera Rincón

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

Principalmente quiero dedicar este trabajo a mi querida esposa e hijos, que me apoyaron en aquellos momentos difíciles por los cuales he pasado, por brindarme esa paciencia, comprensión, amor y fortaleza que me impulsaron a continuar con mi crecimiento profesional y permitirme dar todo mi potencial con el fin de culminar este proceso académico satisfactoriamente. Infinitas gracias familia por estar presente en este proceso y ayudarme a cumplir mis sueños.

Agradecimientos

Quiero expresar mis agradecimientos especialmente a Dios quien me permitió vivir esta experiencia llena de conocimiento, a mi esposa Leidy Viviana Molina Rico por su apoyo constante con sus sabios consejos, agradezco a cada uno de los tutores de la Universidad Nacional Abierta y a Distancia UNAD que me acompañaron y apoyaron a lo largo de este camino brindándome asesorías y motivación en aquellos momentos complejos.

Resumen

Este informe técnico tiene como objetivo documentar el desarrollo del seminario especializado en la capacitación en ciberseguridad en el dominio Red Team y Blue Team, específicamente sobre el reconocimiento, análisis y mitigación de la toma de decisiones desde el enfoque ético y legal. Se describen aspectos básicos de la ciberseguridad, las etapas del pentesting y las herramientas que le corresponden. En la práctica realizada, el laboratorio trata sobre una máquina atacante, donde se utiliza Parrot OS, y dos máquinas Windows 7 (una como pivote y otra como víctima), allí se efectúa el reconocimiento y enumeración de servicios expuestos al ataque y se comprueba el HFS/Rejetto 2.3 como vía de ataque. Mediante la explotación controlada con Metasploit, se demuestra la falta de defensas contra el software obsoleto y el impacto de las configuraciones inseguras, la falta de controles de seguridad y la escasa vigilancia al software. Se pasan luego a las estrategias del Blue Team relacionadas con el Hardening, la segmentación, las pólizas de control de acceso a la información, el principio del mínimo privilegio, el control de acceso a la red por MFA/EDR, el SIEM, la detección y la respuesta en tiempo real. Finalmente, los resultados obtenidos se relacionan con los aspectos de los delitos informáticos y la protección de datos en la legislación colombiana, donde se destaca la importancia de solicitar autorización, cuidar la información, y la responsabilidad profesional que se debe tener en las actividades de seguridad ofensiva y defensiva.

***Palabras clave*:** BlueTeam, hardening, pentesting, RedTeam, SIEM.

Abstract

This technical report aims to document the development of a specialized cybersecurity training seminar in the Red Team and Blue Team domains, specifically focusing on the recognition, analysis, and mitigation of attack risks from an ethical and legal perspective. It describes basic cybersecurity principles, the stages of penetration testing, and the corresponding tools. The practical exercise involved an attacker machine running Parrot OS and two Windows 7 machines (one as the pivot and one as the victim). The analysis included the identification and enumeration of services exposed to attack and verified the HFS/Rejetto 2.3 attack vector. Through controlled exploitation with Metasploit, the report demonstrated the lack of defenses against outdated software, the impact of insecure configurations, the absence of security controls, and the insufficient software monitoring. The discussion then moves on to Blue Team strategies related to hardening, segmentation, information access control policies, the principle of least privilege, network access control via MFA/EDR, SIEM, and real-time detection and response. Finally, the results obtained are linked to aspects of cybercrime and data protection in Colombian legislation, highlighting the importance of requesting authorization, safeguarding information, and the professional responsibility required in offensive and defensive security activities.

***Keywords*:** BlueTeam, hardening, pentesting, RedTeam, SIEM.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team:

Equipo responsable de resguardar los activos informáticos de una organización frente a los ataques de ciberdelincuentes.

CSIRT:

Equipo de respuesta a incidentes de seguridad informática.

CVE:

Grupo de vulnerabilidades en seguridad informática.

Delito Informático:

Conducta ilegal donde se utiliza una herramienta informática como objetivo para cometer el delito.

Explotación (Exploit):

Procedimiento mediante el cual se aprovecha una vulnerabilidad para ejecutar acciones no autorizadas sobre un sistema.

Firewall:

Filtro de seguridad que tiene como finalidad controlar el tráfico de red que ingresa y sale de una maquina al resto de la internet.

Hacker:

Persona con cualidades informáticas muy altas capaz de superar cualquier obstáculo en un sistema informático.

Hardenizacion:

Técnicas o procedimientos que consisten en reducir vulnerabilidades en los sistemas informáticos.

HIDS:

Sistema con la funcionalidad de detención de intrusos.

Intrusión:

Acceso no autorizado a un sistema por medio de la explotación de una vulnerabilidad.

Metasploit:

Framework usado en la ciberseguridad para probar y validar vulnerabilidades en sistemas, redes y aplicaciones.

Meterpreter:

Payload de metasploit cuyo objetivo es aprovechar una explotación para lograr abrir una sesión de control remoto tipo Shell.

Parrot:

Distribución de Linux cuya funcionalidad está enfocada a la ciberseguridad, pentesting, forense y privacidad.

Pentesting:

Proceso autorizado cuya función es simular un ataque real contra un sistema y así evidenciar vulnerabilidades.

Pivoting:

Método empleado por un atacante para utilizar un equipo ya comprometido como puente hacia otros sistemas dentro de la red interna.

Red Team:

Equipo encargado de simular ataques reales para evaluar la postura de seguridad de la organización, utilizando técnicas ofensivas controladas.

Vulnerabilidad:

Fallo de seguridad en un sistema informático que compromete la seguridad de una infraestructura.

Introducción

Las organizaciones han digitalizado sus métodos de operación, almacenamiento y organización de la información. Como resultado, deben incluir la ciberseguridad en sus estrategias de protección y la protección de la información. Adoptando a Red Team y Blue Team que vienen a ser la parte complementaria de la ciberseguridad, donde tenemos en el primero la evaluación de la ofensa de manera controlada y en el segundo la ofensa mediante la ejecución de la defensa a través de la contención y el posterior fortalecimiento defensivo. Esta ciberseguridad y ética han establecido las bases para la elaboración de un informe.

Adoptando la metodología de una prueba, por lo que este documento responde al informe esperado. Este método es la definición del laboratorio, el análisis práctico del ataque que puede venir de una máquina preparada con un sistema operativo Parrot y la víctima que puede residir en cualquier sistema Windows 7. Se necesita una partición distinta en la máquina de Windows 7 que desempeñará el papel de Pivot. Desde las actividades de reconocimiento, enumeración de servicios, validación de la exposición y explotación controlada, sistemas con configuraciones vulnerables, falta de controles defensivos y configuraciones de sistemas obsoletos que aumentan significativamente la vigilancia.

Según los hallazgos, se implementarán estrategias de Blue Team centradas en el Hardening, la segmentación, el control de acceso y el uso de tecnologías como SIEM, EDR y MFA para reducir la superficie de ataque y mejorar la respuesta a incidentes.

Por último, el informe fusiona la parte del análisis técnico con las dimensiones éticas y legales relacionadas con el campo de la ciberseguridad, en particular la importancia del acceso, el manejo de pruebas, la protección de datos y el cumplimiento legal en Colombia. Por lo tanto, el informe busca crear una visión integral donde la eficacia técnica se encuentre con la responsabilidad profesional.

Justificación

El uso del laboratorio incorpora la práctica y una teoría a la práctica operativa donde se reconocen los servicios expuestos, se valida el efecto potencial de las configuraciones inseguras y se puede ver cómo una explotación puede, de forma controlada, dar lugar a acceso remoto, escalada de privilegios y persistencia. Esta experiencia es fundamental para la propuesta de medidas de defensa específicas como el Hardening, la segmentación de red, el principio de mínimo privilegio, y la centralización del monitoreo, orientadas a interrumpir la cadena de ataque con el fin de aumentar las capacidades de detección y respuesta.

Finalmente, el trabajo es pertinente, porque en ciberseguridad no es suficiente con poder ejecutar técnicas es necesario ejecutarlas con permisos, con límites, y con responsabilidad, de acuerdo con la normativa relacionada con delitos cibernéticos y a la protección de datos. Incorporar el componente legal y ético (autorizaciones, límites, evidencia, y privacidad) hace más sólida la práctica profesional, disminuye el riesgo a las organizaciones y evita que los ejercicios de seguridad sean conductas de incumplimiento. En conjunto, el informe establece las directrices que son de gran utilidad para el aprendizaje y la aplicación de la forma profesional de estrategias de Red Team y Blue Team en la práctica.

Objetivos

Objetivo General

Establecer criterios de aprendizaje en seguridad informática en el contexto de los enfoques Red Team y Blue Team durante un seminario especializado, con el fin de preparar a los participantes para identificar, analizar y mitigar vulnerabilidades del entorno digital, anticipar amenazas cibernéticas dirigidas a las organizaciones y fortalecer la toma de decisiones y el comportamiento ético, promoviendo prácticas responsables y el cumplimiento legal para la protección de la tecnología y la información.

Objetivos Específicos

Identificar los aspectos clave que aporten al desarrollo de estrategias para los equipos Red Team y Blue Team.

Definir estrategias operativas que fortalezcan y articulen el trabajo conjunto de Red Team ofensivo y Blue Team defensivo.

Establecer estrategias para el endurecimiento hardening de la seguridad de la información en la organización personas, procesos y tecnología.

Determinar herramientas y controles de detección, respuesta y contención que permitan mitigar y contener ataques informáticos preventivas, correctivas y de monitoreo.

Definir los aspectos legales y de cumplimiento que deben considerarse en el desarrollo de actividades de Red Team y Blue Team autorizaciones, alcance, evidencia, privacidad y normativa aplicable.

Sustentar documentar y presentar la propuesta mediante resultados, evidencia técnica, conclusiones y recomendaciones.

Desarrollo del Informe

En este informe técnico se plasmara cada etapa ejecutada en el seminario el cual está compuesta por las diferentes temáticas propuestas.

Estrategias Red Team

De acuerdo a la situación planteada en la fase 3 las estrategias Red Team se estructuran según el flujo de un pentest y el escenario del laboratorio propuesto, Parrot - Windows 7 Pivot – Windows 7 víctima con HFS/Rejetto. A continuación de enumeran cada una de las estrategias:

- **Planeación y reglas de juego:** Aquí se define el objetivo de alcance y nivel de autorización por parte de la organización para la ejecución de la prueba.
- **Reconocimiento:** El comando Nmap sirve para escanear puertos abiertos, y una manera de hacer un chequeo de seguridad. Este aplicativo realiza un escaneo full de los puertos abiertos en un dispositivo, lo que permite recopilar información para planear posibles ataques.
- **Enumeración:** La enumeración de servicios, versiones y sistemas operativos se puede hacer con Nmap. Esta herramienta es capaz de hacer un mapeo de la red, identificando qué servicios están corriendo, sus versiones y los sistemas operativos que corren en los dispositivos de la red. La información recopilada por Nmap puede usarse para encontrar posibles vulnerabilidades y tomar medidas de seguridad. Por lo cual su empleo es una práctica obligatoria en seguridad informática y administración de redes.
- **Priorización y selección del vector de ataque:** Este apartado, establece una relación entre el servicio identificado y la vulnerabilidad previamente documentadas, como CVE-2014-6287, que se considera el vector susceptible de explotación.
- **Explotación controlada:** Haciendo uso del framework Metasploit cumple la función de buscar y ejecutar el módulo correspondiente al exploit de la vulnerabilidad.

- **Post-explotación:** Aquí se define la verificación de acceso remoto total al sistema vulnerado por medio de usuarios, sistema y permisos de privilegios.
- **Movimiento lateral o pivot:** Habilitación del reenvió de IP en la maquina con Windows 7 pivot y ruta estática desde parrot con destino a la red interna vía pivot.
- **Reporte técnico y recomendaciones:** Por último se registran los hallazgos encontrados en el puerto vulnerado 80/tcp por medio de la vulnerabilidad explotada y el alcance logrado.

Estrategias Blue Team

Las estrategias del equipo Blue Team sobre el análisis de laboratorio se centraron en romper la cadena de ataque que fue posible gracias a la poca seguridad del Windows 7 obsoleto, y la exposición de HFS 2.3 (Rejetto) en 80/tcp, mala configuración del cortafuegos, pivote por reenvío de IP más falta de monitoreo/EDR. Para evitar futuras vulnerabilidades se tomara como refuerzo las siguientes estrategias:

- **Hardening para prevenir ataques:**

Tabla 1

Estrategias de hardening

Sustitución del SO Windows 7	El cambio a un SO actualizado reduce las probabilidades de vulnerabilidades.
Reglas de Firewall	Configuración de puertos necesario para la ejecución de las tareas en la organización.
Principio de mínimo privilegio	Evitar la ejecución de servicios como admin-System, limitar permisos y cuentas.
Control de aplicaciones	Prohibición de aplicaciones no autorizadas.

Segmentación de red	Impedir tránsito libre entre segmentos y limitar alcance del atacante.
Eliminar IP Forwarding en el Pivot	Con el propósito de finalizar el movimiento lateral que se habilito durante el laboratorio.
Implementación de EDR y MFA	Elevar detención y control de accesos no autorizados.
Routers y switches robustos	Controlar rutas y comunicaciones entre subredes

Nota. Tabla sobre las estrategias descriptivas de dureza aplicadas a la infraestructura tecnológica para mitigar los riesgos de seguridad mediante la actualización de sistemas, controles de privilegios, segmentación de red y mecanismos avanzados de detección y autenticación.

Monitoreo y detección: La implementación de monitoreo, alertas y un Sistema de Gestión de Eventos e Información de Seguridad (SIEM) para la correlación cruzada en tiempo real y la conciencia situacional (de usuarios, puntos finales, redes, cortafuegos, etc.) es una necesidad. El análisis destaca que un Sistema de Gestión de Información y Eventos de Seguridad (SIEM) constituye una herramienta fundamental para la generación de alertas en tiempo real, la correlación de datos, el seguimiento de incidentes, la asistencia en investigaciones forenses y el cumplimiento de normativas.

- **Estrategias de repuesta Blue Team:**

Tabla 2

Respuesta BlueTeam

Validación urgente	Mediante IoC monitorear conexiones inusuales como Powershell, reverse Shell, RDP, puertos no autorizados, elevación irregular y logs críticos.
Contención inmediata sin destruir evidencia	Aislar el host con el fin de deshabilitar el puerto en el switch, aislar con EDR y bloquear IPs en el Firewall para frenar el pivoting.
Identificación del vector	Identificación de servicios expuestos, vulnerabilidades ya conocidas y credenciales comprometidas.
Preservación forense	Recolección de logs con herramientas correspondientes para dicha tarea.
Erradicación y recuperación	Reparación, cierre del vector violado, revocación de credenciales y restauración controlada a un punto seguro.
Documentación	Finalización de cada fase.

Nota. La figura describe las fases iniciales de la finalización de la respuesta a incidentes del Equipo Azul, que incluyen la validación de los indicadores de compromiso (IoCs), la recopilación inmediata y sin interrupción de la evidencia, la identificación del vector de ataque, la preservación forense, la eliminación y restauración del sistema, y el cierre de la documentación del incidente.

Etapa 1 : Conceptos de equipos de seguridad

Marco legal en Colombia sobre delitos informáticos y protección de datos personales

Actualmente en Colombia se cuenta con varias legislaciones vigentes que tiene el propósito de mitigar delitos informáticos en las organizaciones.

Tabla 3 *Marco legislación en Colombia*

Ley	Función	Características
Ley 1581 de 2012	Busca desarrollar el derecho constitucional al hábeas data, lo que significa que todos los individuos tienen el derecho a saber, actualizar y corregir la información que se ha recopilado acerca de ellos en bases de datos o archivos. Además, salvaguarda las libertades y garantías vinculadas con el artículo 20 (derecho a la información) y el	• Principios para la protección de datos: Los datos personales tienen que ser gestionados bajo los principios de licitud, finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad.

	artículo 15 de la Constitución (derecho a ser respetado en lo íntimo y en su reputación).	• Derechos de los dueños: Los individuos tienen el derecho de enterarse sobre la información que las organizaciones o empresas tienen acerca de ellos, así como de actualizarla y corregirla. • Obligaciones de los comerciantes: Las compañías o entidades tienen que garantizar la confidencialidad de los datos y conseguir el permiso explícito, libre y previo de los dueños antes de recoger o procesar datos. • Registro nacional de bases de datos: Las bases de datos que contienen información

		sensible y que son gestionadas por grandes compañías o entidades públicas tienen la obligación de registrarse en la Superintendencia de la industria y el comercio. • Fundamentos: Establece la finalidad, la seguridad en el manejo de la información, la calidad, la transparencia, la libertad y la accesibilidad como principios. • Autoridad de supervisión: La Superintendencia de Industria y Comercio se establece como supervisora de la ley.

Ley 1273 de 2009	Esta ley representa un avance significativo en Colombia en la lucha contra los delitos informáticos. Se establece una categoría específica de delitos denominada "delitos contra la confidencialidad, la integridad y la disponibilidad de la información y de los sistemas informáticos	• Protección de datos: El acceso, la supresión, el uso o la alteración no autorizada de sistemas informáticos y datos personales están sujetos a castigo. • Delitos informáticos: son infracciones que comprenden la interceptación de datos, el acceso ilegal a sistemas de cómputo, el uso de malware (virus) y el fraude cibernético. • Consecuencias: Según la gravedad del delito, determina condenas que pueden ir de las multas hasta el encarcelamiento.

		• Pilar fundamental: Esta reglamentación es el primer paso para controlar los delitos cibernéticos en Colombia. • Creación de nuevas categorías para los delitos: Se definieron como delitos nuevos aquellos relacionados con la información y los datos, tales como la interceptación de datos, el acceso ilegal a sistemas informáticos o la eliminación de información. • Bien jurídico protegido: La protección de la información y los datos es un nuevo bien jurídico protegido.

Decreto 1377 de 2013 - Reglamentario de la Ley 1581 de 2012	Este decreto regula aspectos concretos de la Ley 1581 promulgada en el año 2012. Concentra sus regulaciones para la administración apropiada de información personal, definiendo deberes más precisos para las empresas e instituciones que manejan estos datos.	• Adquisición de consentimiento: Especifica cómo debe hacerse la solicitud y cómo se debe documentar el aprobación de los dueños de los datos. • Políticas de privacidad: Necesita que las compañías implementen políticas internas de la salvaguarda de datos, los cuales deben estar al alcance de los titulares. • Tiempos establecidos para la actualización de datos: Cuando el titular lo requiera, establece los procedimientos y plazos para la actualización, corrección o eliminación de datos.

Ley 1928 de 2018 - Protección frente a la utilización indebida de datos personales en bases de datos	Esta ley hace énfasis en los principios y reglas internacionales que tienen como finalidad proteger a todas las personas con respecto al uso indebido de los datos personales	- La protección a las personas frente a al uso de información especialmente cuando son usados por medio de sistemas automatizados como base de datos. - Garantizar el derecho a la privacidad de la información de cada persona. - Garantizar aquellos principios de responsabilidad para el personal que hace uso de la recolección de datos. - Regulación de los datos personales a nivel internacional. - Fortalecer los convenios internacionales para la protección de los datos.

Nota. De la tabla anterior se toman como comparativos los principales aspectos contenidos en la legislación colombiana en cuanto a la protección de datos personales y la seguridad de la información, tales como la Ley 1581 de 2012, que se ocupa de la protección del derecho fundamental al hábeas data y al tratamiento responsable de la información personal; la Ley 1273 de 2009, que se ocupa de los delitos informáticos y protege la confidencialidad, integridad y disponibilidad de los sistemas de información; así como la Ley 1928 de 2018 que complementa la normativa que protege el uso indebido de datos de carácter personal y busca la armonización de la legislación nacional con principios y estándares internacionales en materia de protección y seguridad de la información.

Etapas del pentesting en el entorno de la ciberseguridad

Antes de entrarnos a fondo en el tema del Pentesting es fundamental saber que significa este término, “El pentesting es una prueba de penetración, también conocida como prueba de lápiz, es un ciberataque simulado contra su sistema informático para comprobar si hay vulnerabilidades explotables. En el contexto de la seguridad de las aplicaciones web, las pruebas de penetración se utilizan comúnmente para aumentar un cortafuegos de aplicaciones web (WAF).” (Imperva, 2025)

“El proceso de prueba de penetración consta de múltiples fases que imitan ataques del mundo real. La definición exacta de las fases del proceso de prueba de penetración puede diferir entre las metodologías y los proveedores, pero las actividades combinadas de todas las fases son esenciales para un compromiso exitoso.” (AMATAS, 2024)

En el mundo de la ciberseguridad existen procesos definidos para poder ejecutar de forma organizada lo que se conoce como pruebas de penetración o pentesting; usted como futuro experto deberá redactar con sus palabras y definir cada una de las etapas del pentesting,

dentro de la definición incorporará un ejemplo de una herramienta que se utilice para cada una de las etapas del pentesting.

Fase de Recolección de Información: En esta fase el objetivo principal como su nombre lo indica es recolectar la mayor cantidad de información sobre la entidad a la cual se va realizar el pentesting (archivos, ip, dominios), este proceso se ejecuta sin dejar registro de la ip del equipo atacante en los registros del objetivo, para esta fase es conveniente el uso de aplicaciones pasivas que permita la extracción de datos con el mínimo contacto con el objetivo.

Dentro de las herramientas pasivas podemos usar **Google Dorking** que tiene como objetivo la búsqueda avanzada en distintos motores con hallazgos en índices públicos, como por ejemplo archivos, aquellas configuraciones que se encuentran expuestas, y paginas internas. Para la extracción de información **ExifTool** donde su función es la extracción de metadata de imágenes y archivos.

Fase de Enumeración*:* En esta fase se define el objetivo que se quiere atacar y los puntos críticos donde se evidencian las vulnerabilidades que se pueden llegar a controlar, en esta etapa se efectúa la recolección de información más específica, como el ingreso a los servidores para detectar equipos activos, sus sistemas operativos, servicios en línea y sus respectivas versiones, rangos de IP, DNS, Firewall, por medio de la herramienta **Nmap** que permite identificar hosts, puertos abiertos, servicios y versiones; muy práctico también por sus scripts (NSE) para la enumeración avanzada.

Fase de Análisis de Vulnerabilidades: En esta fase el objetivo es clasificar las posibles vulnerabilidades según la información recolectada en la fase anterior, por medio de la herramienta **Metasploit**, que permite comparar la información anteriormente recolectada con base de datos de vulnerabilidades ya establecida, de esta manera obteniendo como resultado las vulnerabilidades más críticas.

Fase de Explotación: Esta es la fase más importante del pentesting ya que es el momento donde se utiliza la información obtenida de las fases anteriores, y se aprovechan las vulnerabilidades evidenciadas en el sistema para lograr tomar control del equipo, y escalar privilegios con técnicas como ingeniería social, cracking de passwords, ejecución de exploits, ataques de denegación de servicios, actualizaciones maliciosas, todo por medio del framework de Metasploit.

Definición de las herramientas en ciberseguridad

Metasploit: "Es un framework de código abierto utilizado principalmente para realizar pruebas de penetración y desarrollar y ejecutar exploits." (Rapid7, s. f.)

Ventajas

1. Amplia Base de Datos de Exploits
2. Código Abierto y Comunidad Activa
3. Modularidad y Flexibilidad
4. Interfaz de Usuario Intuitiva
5. Metasploit Pro
6. Educación y Formación
7. Soporte y Documentación Extensiva
8. Actualizaciones Frecuentes
9. Entorno de Pruebas Seguro

Pruebas de penetración (Penetration Testing): Metasploit ayuda a imitar verdaderos ataques en una red y sistema para que los profesionales puedan identificar y corregir fallas antes de que un atacante real las explote.

Análisis de Vulnerabilidades: La herramienta utiliza sus bases de datos de exploits para intentar identificar debilidades en cualquier sistema y aplicación.

Monitoreo Continuo de Seguridad: Metasploit verifica para asegurarse de que no se introduzcan nuevas vulnerabilidades cada vez que se lanza una nueva versión o parche. De esta manera, se puede integrar en los procesos de CI/CD.

Desarrollo de Exploits: En un mundo de defensa cibernética en desarrollo, Metasploit puede ayudar a idear y probar nuevos exploits.

Capacitación y Desarrollo Profesional: Metasploit ofrece planificación práctica para ayudar a las personas a desarrollar habilidades de hacking ético, formando la base de muchos programas educativos en ciberseguridad.

Nmap: Es un programa de código abierto que sirve para efectuar rastreo de puertos. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas.

Características:

- Descubrimiento de servidores: Identifica computadoras en una red, por ejemplo listando aquellas que responden ping.
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determina qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como fingerprinting).
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

OpenVas: Open Vulnerability Assessment System) es un escáner de vulnerabilidades de uso libre que permite identificar y corregir fallas de seguridad, o debilidades en un activo, que pueden ser explotadas por una o más amenazas.

Características

Es un marco basado en servicios donde las herramientas pueden ser utilizadas individualmente o como parte de las herramientas de seguridad OSSIM (Gestión de Información de Seguridad de Código Abierto). Las distribuciones de Kali Linux vienen con esta herramienta preinstalada, aunque en el caso de Kali Linux 2023, debe ser completada para la instalación y configuración con el fin de ser utilizada a través de dos clientes, desde la línea de comandos (OpenVAS CLI) o una interfaz web (Asistente de Seguridad Greenbone).

Servicios en línea:

ExploitDB: Es una aplicación web que reúne bases de datos públicas con exploits para vulnerabilidades conocidas, en lo que contribuyen los usuarios. Dichos exploits pueden ser consultados, descargados y utilizados por pentesters de todo el mundo de forma gratuita para mejorar la calidad de sus auditorías de ciberseguridad. ∫Gracias a esta base de datos, los investigadores de seguridad cuentan con una fuente adicional para consultar la existencia de exploits para las vulnerabilidades que encuentren en un sistema.

CVE: De acuerdo con el CVE, las vulnerabilidades son errores en el código del software A que posibilitan que un atacante acceda de manera no autorizada y directa a redes y sistemas informáticos y difunda malware. Esto, por lo general, permite a los atacantes hacerse pasar por administradores o super usuarios del sistema que tienen acceso total a los recursos de la empresa. La CVE considera la exposición como fallas en la configuración o el código del software que posibilitan que un atacante acceda de manera indirecta a las redes y sistemas. Esto podría posibilitar que el asaltante aceche en las redes de computadoras y recoja de manera secreta datos delicados, credenciales de usuario e información del cliente. La meta primordial de CVE es asistir a las organizaciones en la mejora de sus defensas de seguridad. Lo realiza reconociendo y ofreciendo un catálogo de vulnerabilidades de firmware o software, el cual pone a la disposición del público como un diccionario gratuito. Un caso de uso común de CVE ofrece a las

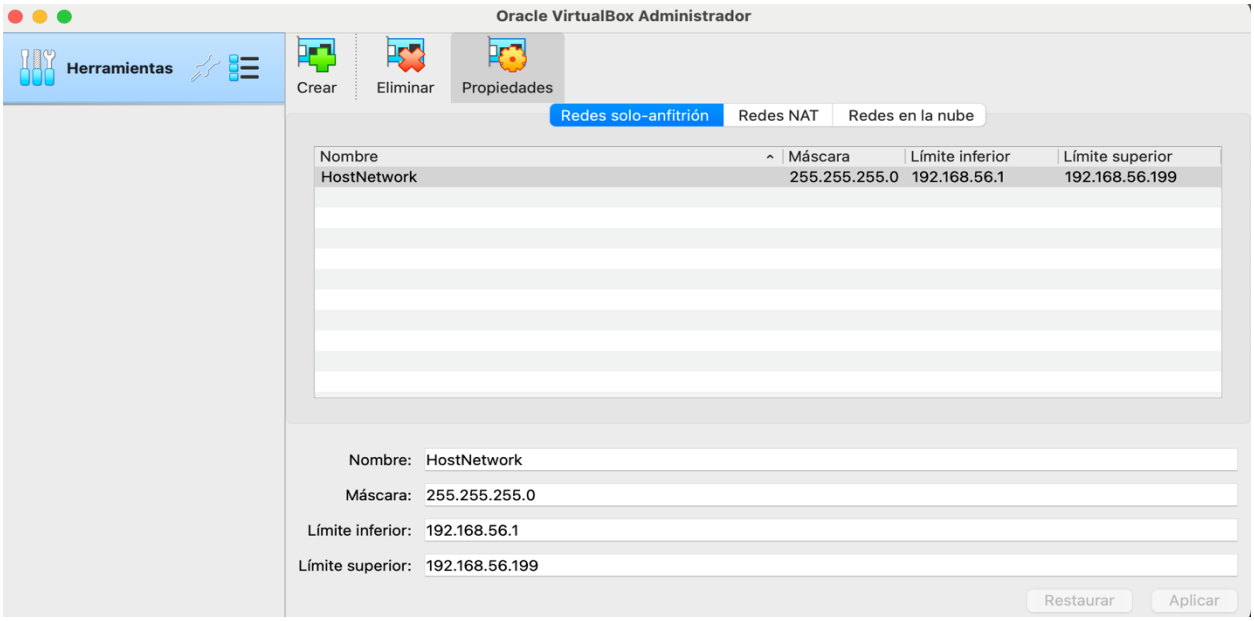
organizaciones múltiples ventajas, tanto en términos de uso como de comercialización de productos y servicios compatibles con CVE.

Configuración del banco de trabajo Anexo 1

Como se observa en la Figura 1, la configuración de red en VirtualBox se establece en modo solo-anfitrión, permitiendo la comunicación controlada entre las máquinas virtuales del laboratorio.

Figura 1

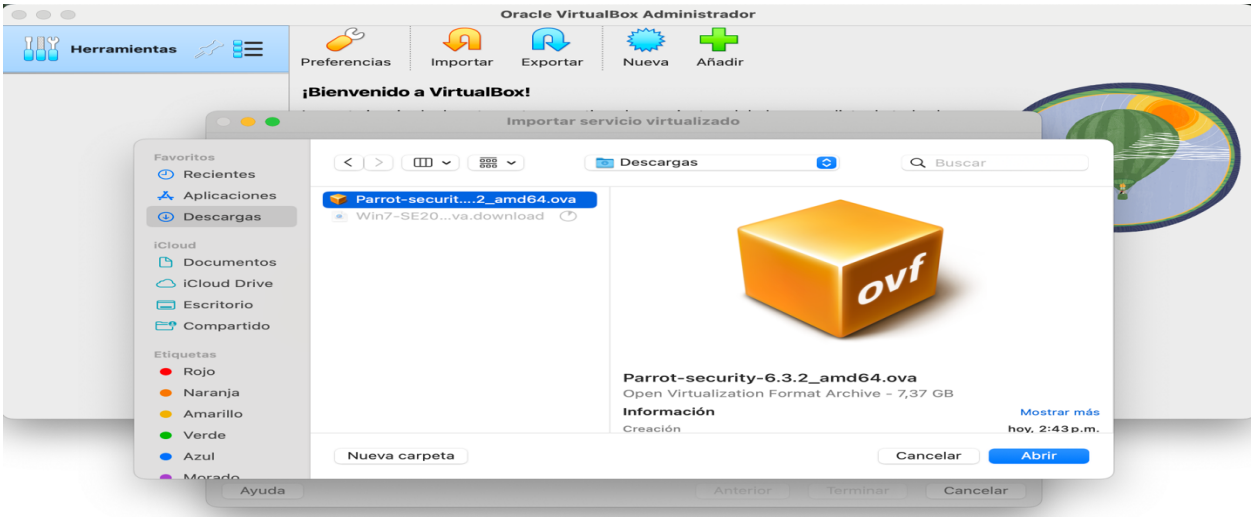
VirtualBox configuración red



Fuente. Autoría Propia

Figura 2

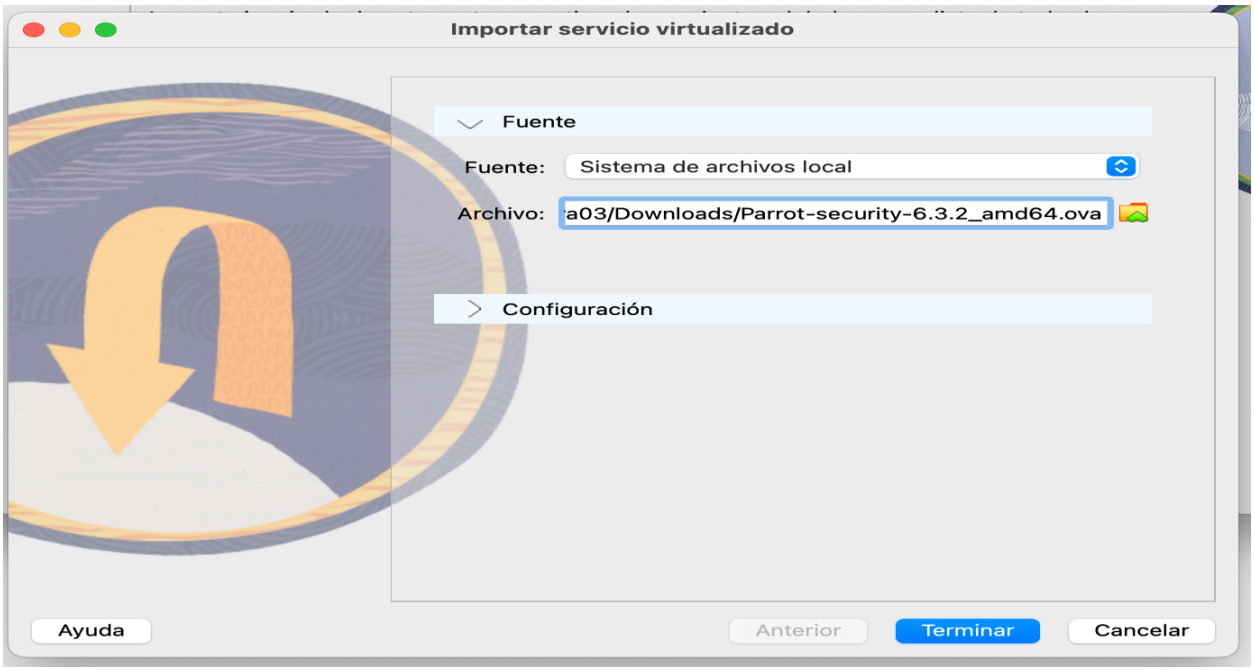
Instalación maquina parrot



Nota. La evidencia anterior confirma la importación de la máquina virtual parrot para lograr efectuar el laboratorio.

Figura 3

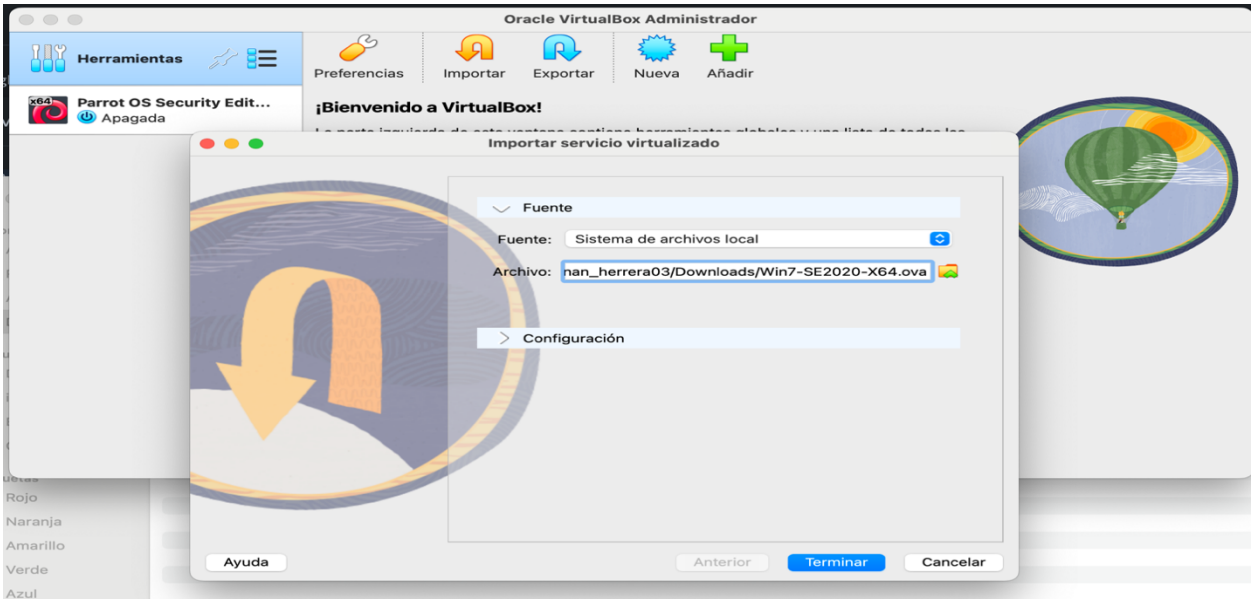
Importación de la Maquina



Fuente. Autoría Propia

Figura 4

Importación maquina win7



Fuente. Autoría Propia

Figura 5

Maquinas instaladas

Fuente. Autoría Propia

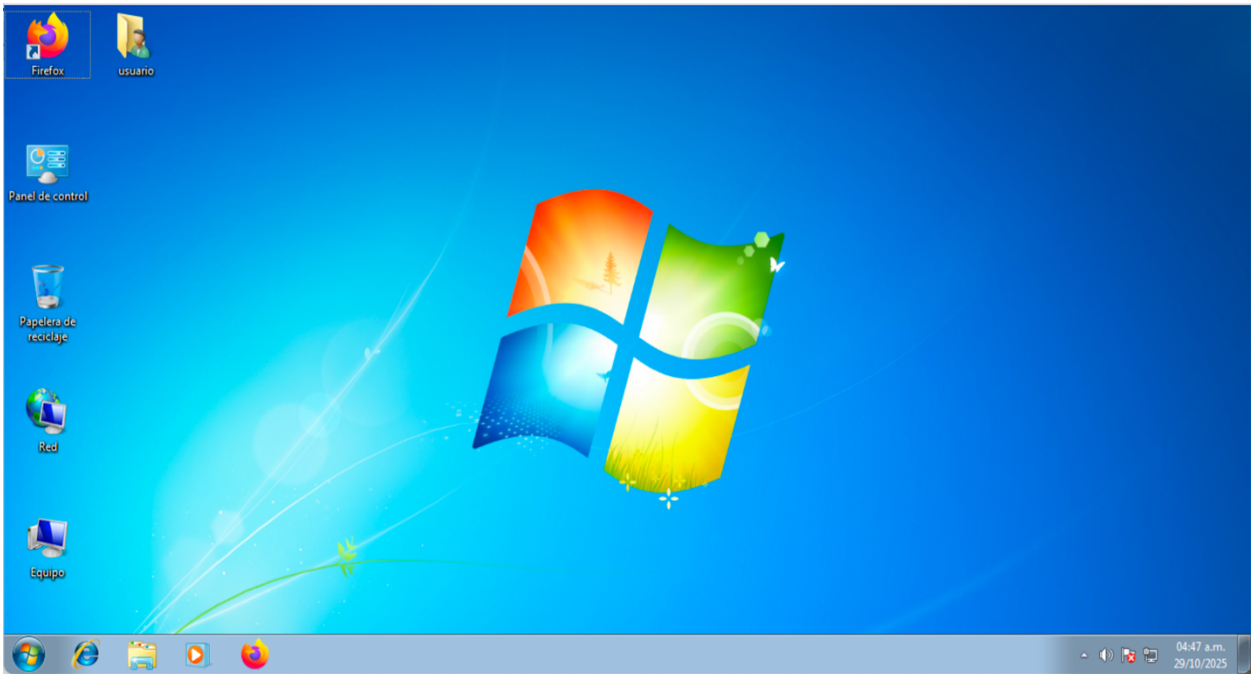
Figura 6

Maquina parrot corriendo

Fuente. Autoría Propia

Figura 7

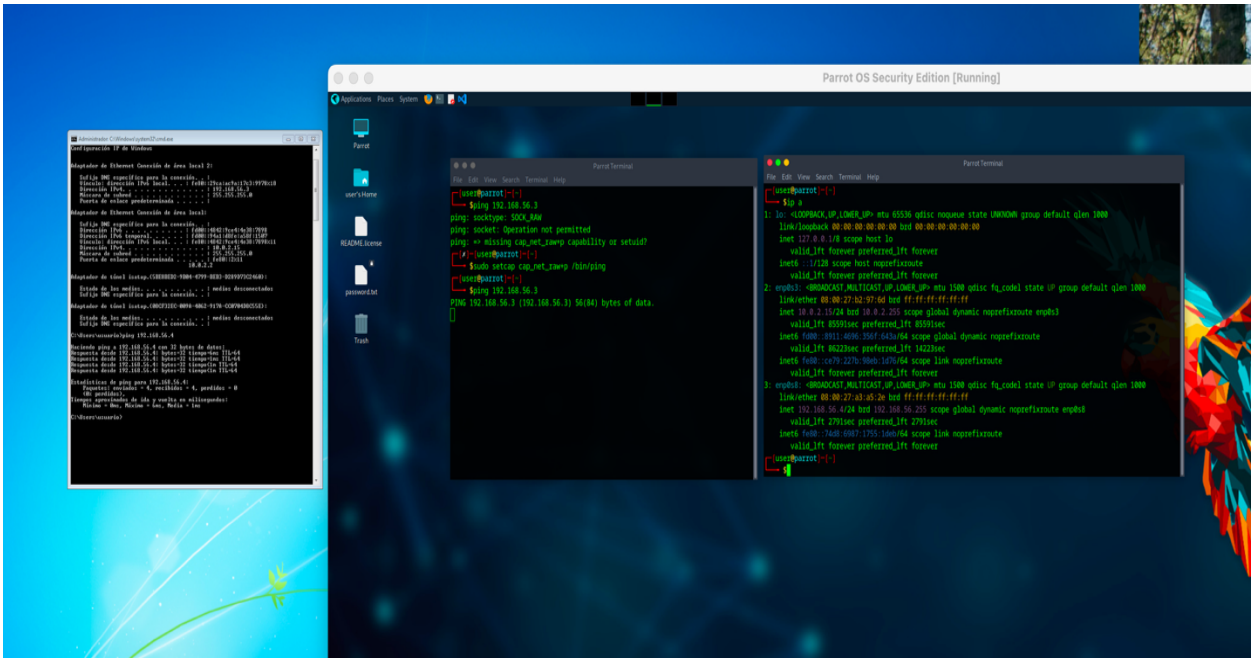
Maquina win7 corriendo



Fuente. Autoría Propia

Figura 8

Comunicación entre maquinas



Nota. Para validar la conectividad entre las máquinas del laboratorio, se efectuó una prueba de comunicación ICMP, cuyos resultados se presentan en la Figura 8.

Etapa 2: Actuación Ética y Legal

¿Una vez leído el anexo 2 – escenario 2 y el anexo 3 – Acuerdo usted logra evidenciar algún proceso ilegal y no ético que se esté estipulando en dicho acuerdo? Deberá argumentar su respuesta y señalar los fragmentos ilegales del anexo acuerdo en caso de existir alguna irregularidad.

Dando análisis al documento Anexo 2 se logra evidenciar una irregularidad ya que en el escenario que se plantea el contrato y los acuerdos fueron realizados por un abogado que ya había sido despedido por irregularidades en su trabajo, así mismo se concluye que la alta gerencia en ningún momento realizo la respectiva revisión del documento antes de ser entregado a los aspirantes. Lo anteriormente descrito se asocia a un riesgo legal y ético por parte de la

empresa por el simple hecho de firmar documentación potencialmente ilícita sin antes ser verificada por un ente jurídico.

En el Anexo 3 que es el acuerdo se evidencia irregularidades en la cuarta clausula numerales 3 y 4.

No denunciar ante las autoridades actividades sospechosas de espionaje o cualquier otro proceso en el cual intervenga la apropiación de información de terceros.

Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

Las cláusulas 3 y 4 dan a entender que no se pueden denunciar ni publicar irregularidades que se evidencien en el proceso y en teoría esto sería un delito informático por encubrir irregularidades. Si nos remitimos a la ley 1273 de 2009 allí evidenciamos los artículos 269A al 269J que nos hablan sobre delitos los cuales estaríamos violando al encubrir:

- 269A: Acceso abusivo a un sistema informático
- 269B : Obstaculización ilegal de sistema informático o red
- 269C: Interceptación de datos informáticos
- 269D: Daño Informático
- 269E: Uso de software malicioso
- 269F: Violación de datos personales
- 269G: Suplantación de sitios web

Además, contradicen el Código de Ética del Profesional en Seguridad Informática, que exige reportar vulnerabilidades o actos ilícitos a las autoridades competentes. Éticamente, promueven la cultura del silencio frente a delitos, lo que puede convertir al firmante en cómplice

por omisión. En el Anexo 3 en la cláusula segunda nos habla de información confidencial pero en el numeral 2 incumplen y es gravemente irregular.

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.

Las "chuzadas" o interceptaciones ilegítimas son un tipo de delito en Colombia (Código Penal artículos 192, 269A, 269B, 269E). La ilegalidad de obtener información de un delito no puede ser coartada o establecida en un acuerdo de confidencialidad. Proponer que estas actuaciones queden subsumidas en el concepto de "información confidencial" es ocultar el ejercicio de conductas delictuales y vulnerar garantías de orden legal, ético, y de Derechos Humanos, tales como el respeto a la intimidad, art. 15 de la Constitución.

En la cláusula octava hay un apartado que habla de “En caso que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a SecureNova Labs.” (Anexo 3. Universidad Nacional Abierta y a Distancia, 2023).

Esta cláusula está ajustada para dejar la responsabilidad penal al receptor (en este caso el estudiante o el empleado), liberando de esta manera a la empresa de cualquier responsabilidad penal. Esto es ilegal ya que nadie puede transferir la responsabilidad penal o eximirse contractualmente de los crímenes cometidos.

Ética y moralmente, ilustra una inequidad en la distribución del poder contractual, ya que la empresa presumiblemente está tratando de coaccionar al firmante para que asuma la responsabilidad de otra persona. También es contrario a los principios de la responsabilidad

objetiva de las personas jurídicas en la ley (Ley 2195 de 2022, art. 34A del Código Penal Colombiano).

Si la respuesta es afirmativa y usted encontró algún proceso ilegal en el anexo 3 – Acuerdo: acuerdo, deberá mencionar que artículos de la ley 1273 se podrían vulnerar en dicho acuerdo y especificar porqué vulnera artículos de la ley 1273.

En la segunda cláusula y la cuarta clausula se afecta la ley 1273: 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."

"Abstenerse de denunciar y publicar la información confidencial e ilegal que conozca, reciba o intercambie con ocasión de las reuniones sostenidas."

- **269A – Acceso abusivo a un sistema informático:**

"El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes." (Congreso de la República de Colombia, 2009)

La cláusula que reconoce como "confidencial" la información obtenida a través de "intercepción de información" o "acceso abusivo a sistemas informáticos" legitima comportamientos que califican como actos criminales. Ocultar o participar en tales acciones constituye complicidad o la provisión de asistencia al crimen.

- **269B – Obstaculización ilegal de sistema informático o red:**

“El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.” (Congreso de la República de Colombia, 2009)

El requisito de “no informar sobre actividades de espionaje o la apropiación de información de terceros” crea la posibilidad de que florezcan actos de sabotaje o interferencia no informados, lo que entra en el ámbito de este artículo.

- **269C – Interceptación de datos informáticos:**

“El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.” (Congreso de la República de Colombia, 2009)

Dentro del marco del contrato, la expresión “datos de chuzadas” o “intercepción de información” constituye el cruce de comunicaciones sin una orden judicial, un acto que esta norma establece como penal. En este caso, las interceptaciones en el contrato enmarcan la información como “confidencial”, lo que equivale a legalizar un acto ilícito.

- **269D – Daño informático:**

“El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en

multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.” (Congreso de la República de Colombia, 2009)

Al requerir una reserva de información por "accesos abusivos", el acuerdo pudiera implicar reconocimiento o validación de manipulación indebida de sistemas. Esto podría ser consecuencia de un daño informático o alteración ilegal de datos.

- **269E – Uso de software malicioso:**

“El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.” (Congreso de la República de Colombia, 2009)

El encubrimiento de espionaje y acceso abusivo podría implicar el uso de software malicioso (spyware, keyloggers, troyanos), lo que constituiría una violación directa de esta disposición.

- **269F – Violación de datos personales:**

“El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.” (Congreso de la República de Colombia, 2009)

El Acuerdo protege cierta información adquirida sin autorización (por ejemplo, información de terceros) bajo confidencialidad, constituyendo una violación de datos personales.

- **269H – Circunstancias de agravación punitiva:**

"Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere" (Congreso de la República de Colombia, 2009)

En el contexto de un acuerdo de confidencialidad respecto a la selección de empleo o personal, si el estudiante (empleado) acepta mantener silencio sobre actividades ilegales, esto aumentaría su responsabilidad penal.

¿Existiendo procesos poco confiables en el anexo 3 – Acuerdo, usted como experto en ciberseguridad aplicaría a este trabajo en SecureNova Labs, donde la organización dispone de un sueldo de $15.000.000 de pesos colombianos mensuales y contrato vitalicio? Debe argumentar su respuesta ya sea afirmativa o negativa y tener en cuenta en la argumentación que dispone COPNIA en su código de ética para ingenieros.

Rta. No aplicaría a esta oferta laboral

Para nadie es un secreto que un contrato como el que está ofreciendo la empresa SecureNova Labs con un salario tan amigable y además de eso vitalicio sería una grandiosa oportunidad laboral, pero por otro lado está presente la ética profesional de cada uno de los profesionales y en mi caso mi ética está por encima del dinero, ya que el contrato contiene muchas irregularidades que a largo plazo me va a generar problemas legales. El Código de Ética de COPNIA establece, de acuerdo con la Ley 842 de 2003, que la práctica profesional debe basarse en la honestidad, la responsabilidad, el respeto a la ley y el compromiso social. Involucrarse con una organización que aboga por el espionaje, la interceptación de datos o la ocultación de información ilegal (de acuerdo al Anexo 3) implicaría la violación de varias disposiciones del Código, incluyendo:

Trayendo a colación el **Articulo 31 que trata los deberes generales de los profesionales** allí se ordena “Denunciar los delitos, contravenciones y faltas contra este Código de Ética, de que tuviere conocimiento con ocasión del ejercicio de su profesión, aportando toda la información y pruebas que tuviere en su poder.” (COPNIA, 2015).En el acuerdo Anexo 3 ordena al estudiante o empleado “abstenerse de denunciar actividades ilegales o de espionaje”, lo que significa que va en contra del código de ética.

Por otro lado tenemos el Articulo 33 que trata sobre Deberes especiales con la sociedad, allí se establece que el profesional debe “proteger la vida y salud de los miembros de la comunidad, evitando riesgos innecesarios en la ejecución de los trabajos” (COPNIA, 2015). Al involucrarse en actividades ilegales o de interceptación en una compañía, el profesional afecta de manera negativa la privacidad, los derechos digitales y la integridad de las personas, ocasionando un incumplimiento de su responsabilidad social.

De acuerdo al **Artículo 34 Prohibiciones especiales a los profesionales respecto de la sociedad,** que habla sobre “ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación” (COPNIA, 2015). Teniendo en cuenta el anexo 3 donde se establecen cláusulas que van en contra de la ley 1273 de 2009 específicamente la interceptación o el acceso abusivo a sistemas, los profesionales en seguridad no deberían aceptar por ningún motivo este cargo inclusive así halla un incentivo económico bastante amigable.

En el **Articulo 35 deberes con la dignidad de la profesión** hace referencia a “respetar y hacer respetar todas las disposiciones legales y reglamentaras que incidan en actos de estas profesiones, así como denunciar todas sus transgresiones” (COPNIA, 2015). Una profesión es digna mientras se respete el principio de legalidad y el deber de denunciamiento. Trabajar para

una organización que normaliza delitos informáticos o que manipula la información confidencial de otras personas es una falta de respeto a la profesión.

La práctica de la ciberseguridad también involucra la dimensión ética de la custodia de la privacidad y los derechos informativos de los sujetos de datos. Asumir el rol bajo los términos del acuerdo constituiría una violación de la ley y del código ético que te expondría a medidas disciplinarias por ejemplo, suspensión o cancelación de la licencia profesional, que está establecido en el Art. 4 del Código de Ética código ética y responsabilidad penal. Con estos argumentos definitivamente diría NO a esta oferta laboral.

Deberá analizar el caso problema "Ciberespionaje y Ética en SecureNova Labs" (Anexo 2 - Escenario 2), redactar su punto de vista teniendo en cuenta las implicaciones legales y éticas que allí se pudieron generar y dar respuesta los siguientes interrogantes:

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

Las firmas de ciberseguridad deben acceder a información sensible de los clientes durante auditorías y pruebas de penetración. Este acceso determina vulnerabilidades y evalúa la seguridad de los sistemas para mejorar y salvaguardar los datos. Este acceso debe dirigirse al alcance de vulnerabilidades previamente aprobadas de una manera legal y éticamente razonable para la profesión. "La Ley 1581 de 2012 establece que los datos personales y la información sensible solo deben ser manejados con la autorización previa y explícita del titular de los datos, y para un objetivo legítimo y proporcional al propósito del tratamiento. En este caso de auditoría, esto significa que los datos para el análisis técnico deben implementarse dentro de un control legal y contractual que rodea al equipo de ciberseguridad." (Ley 1581 de 2012)

Además, la Ley 1273 de 2009, que regula la protección de la información y los datos

informáticos, clasifica como delitos el acceso abusivo cercano (Art. 269A), la interceptación ilegal (Art. 269C) y la violación de datos personales (Art. 269F). Por lo tanto, si una empresa actúa bajo una auditoría de datos con espionaje personalizado no autorizado, manipulación de datos o venta ilegal de datos, está cometiendo un delito informático. Un ejemplo de un contrato abusivo es el del Anexo 3 de SecureNova Labs, que establece: "no reportar espionaje o robo de datos de terceros." Esto es un claro abuso del contrato e ilustra la falta de cumplimiento con la ley y el uso indebido de la información.

Legalmente, la Ética de COPNIA (ley 842 de 2003), artículos 31, 33, 34, establece que un profesional debe actuar con honestidad, y con responsabilidad y respeto a la ley. Esto significa que el auditor de seguridad debe preservar el secreto profesional, pero además tiene el deber moral y legal de informar sobre cualquier actividad ilegal que surja en el transcurso de sus funciones.

Garantías para evitar explotación indebida del acceso, para que las empresas protejan la información sensible, deben implementar medidas de control éticas y técnicas, por ejemplo:

Consentimiento informado y contractual: Los clientes deben dar autorización por escrito sobre qué información será revisada y con qué propósito.

Principio de mínima exposición: El auditor solo debe acceder a la información absolutamente necesaria para la auditoría.

Registro y seguimiento de acceso: El rastro de auditoría de las acciones realizadas por el auditor debe ser accesible para su revisión.

Cláusulas éticas y de responsabilidad: Todo contrato debe especificar qué tipo de información no puede ser utilizada para propósitos distintos a la auditoría.

Destrucción y devolución de datos: Toda la recopilación de información para la auditoría debe obligatoriamente ser destruida o retornada al cliente.

Supervisión independiente: Entidades o auditores externos deben asegurar que la empresa cumpla con toda la normatividad vigente en cuestión de protección de datos.

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

Es de vital importancia que las empresas de ciberseguridad establezcan unas medidas que permitan el control y supervisión con el propósito de evitar análisis no autorizados; Entre estos mecanismo de control destacamos:

Políticas internas:

- Establecer un código de conducta con el objetivo de fijar responsabilidades y límites para el uso de las herramientas forenses en la empresa.
- Importante que existan cláusulas que permitan establecer normas para el acceso autorizado a los sistemas y datos, consentimientos informados por parte del cliente o dueño de la información, y el uso prohibido de herramientas con fines personales sin antes contar con una orden judicial.
- El entrenamiento continuado sobre capacitaciones en ética profesional, privacidad y legislaciones vigentes en Colombia.

Accesos y privilegios:

- Asignación de cuentas empresariales e intransferibles a los analistas para un estricto control de su uso.
- Implementación de un autentificador multifactor y principio de mínimo privilegio para cada funcionario de la empresa de seguridad, para lograr optimizar el control de registros de cada movimiento por empleado dentro del sistema.
- Resguardar todos los accesos mediante logs protegidos contra toda manipulación.

Auditorias técnicas y revisiones periódicas

- Implementación de auditorías internas y externas que permitan a la empresa la revisión del uso de herramientas forenses, uso de exploit y script.
- Implementación del uso de SIEM Security Information and Event Management con el objetivo de chequear en tiempo real cada proceso que realizan los analistas.

Continuo monitoreo y alertas automatizadas

- Implementación de herramientas Data Loss Prevention (DLP) y User Behavior Analytics (UBA) que permitan a la empresa de seguridad un control para evitar copias o transferencias de datos que no han sido autorizadas.
- Control en la ejecución de herramientas de pentesting fuera del horario laboral establecido.
- Monitoreo en conexiones o dispositivos usb sospechosos.

Seguridad en las cadenas de custodia digital

- Es muy importante que todo proceso de análisis forense quede documentado bajo el formato establecido por la empresa para la cadena de custodia, así mismo que indique fecha y hora del acceso, responsable del análisis, herramientas utilizadas, resultados y destino de la evidencia.

Capacitación legal

- Definir el apoyo hacia los analistas con las capacitaciones en la normativa vigente ley 1273 de 2009, código de ética profesional, ley 1581 de 2012, y buenas prácticas del Computer Security Incident Response Team (CSIRT).

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

Cuando un gobierno u organización detecta que su proveedor de ciberseguridad está realizando ciberespionaje, es necesario que la respuesta sea inmediata, transparente y verificable. Para restaurar la confianza y cerrar la oportunidad a que suceda de nuevo es necesario:

Respuesta Contener, preservar y escalar estimado de 0 a 72 horas:

- Definir un plan de respuesta a incidentes y así mismo crear una comitiva que este compuesta por miembros de los departamentos legales, seguridad, auditoría y comunicaciones.
- Restringir el acceso del proveedor Y revocar credenciales, tokens y acceso a VPN, rotar claves y secretos; y bloquear integraciones.
- Preservar evidencia como imágenes forenses, registros, correos electrónicos, tickets, evidencia de la cadena de custodia.
- Notificar a las autoridades en Colombia, para luego contactar a la fiscalía, la policía cibernética (DIJIN/CCIT) y la SIC si hay datos personales (Ley 1581) y problemas relacionados con ciberseguridad. Autoridades regulatorias sectoriales en finanzas, salud y otras industrias.
    - Cláusulas contractuales suspensión o terminación por incumplimiento grave, llamar a garantías y penalidades, y vulnerar el seguro de riesgo cibernético.
- Comunicación controlada expedir un comunicado sobre qué ocurrió, qué se está haciendo, y a quién contactar sin especulación infundada.

Investigación estimado de 3 a 30 días:

- Mapa de impacto — qué datos/sistemas, exfiltrados, impacto en el cliente, riesgos residuales.

- Acción correctiva tomada por el proveedor debido a CAPA (Acciones Correctivas y Preventivas) con hitos verificables.
- "Acciones legales denuncias penales ejemplo, Ley 1273 en Colombia: 269A, 269C, 269E, 269F, y sanciones administrativas." (Congreso de Colombia, 2009)
- Notificar a los titulares de los datos y la mitigación empleada para el monitoreo de robo de identidad, con el total apoyo dedicado.

Restauración de la confianza estimado de 30 a 90 días:

- Efectuar la publicación de las lecciones aprendidas del evento y los avances del modelo CAPA.
- Auditoría externa según norma ISO 27001.
- Programa para la estructuración técnica donde se realice entrega completa de credenciales y PKI, revocación de la integridad hashing en endpoints y servidores, y fortalecimiento de PoLP, MFA, segmentación y zero trust.

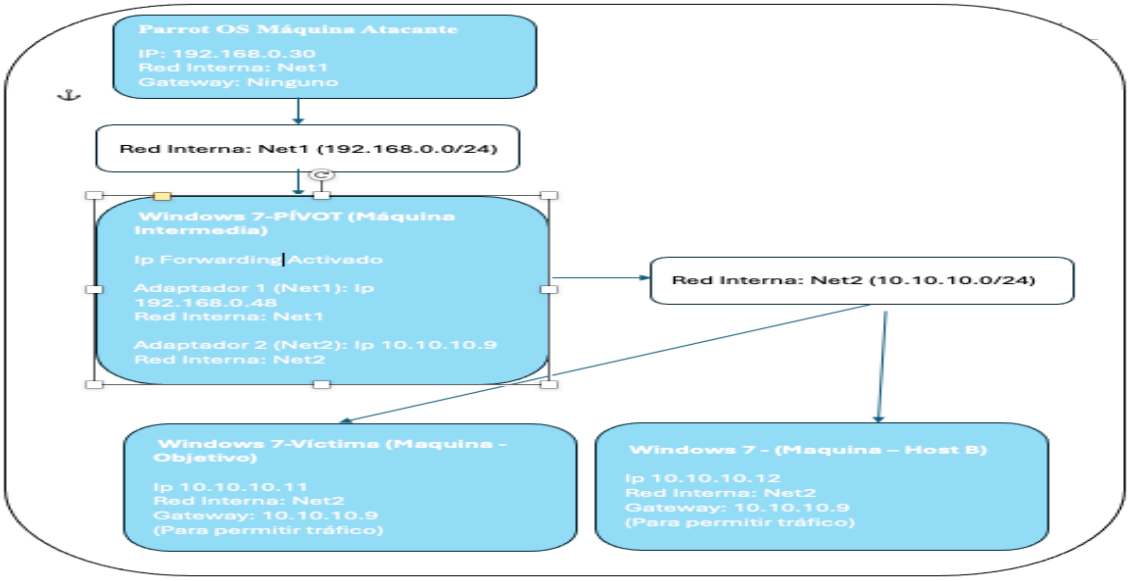
Etapa 3: Ejecución Pruebas de Intrusión

Describa de manera específica las herramientas software que utilizó para llevar a cabo el anexo 4 – escenario 3 enfocado a Redteam. Deberá adjuntar evidencia de los comandos utilizados y resultados que arrojó cada herramienta utilizada, estas herramientas deben estar clasificadas según los pasos de un pentesting.

En la figura 9 observamos la configuración de red del escenario de trabajo el cual se usara para lograr exitosamente el laboratorio planteado.

Figura 9

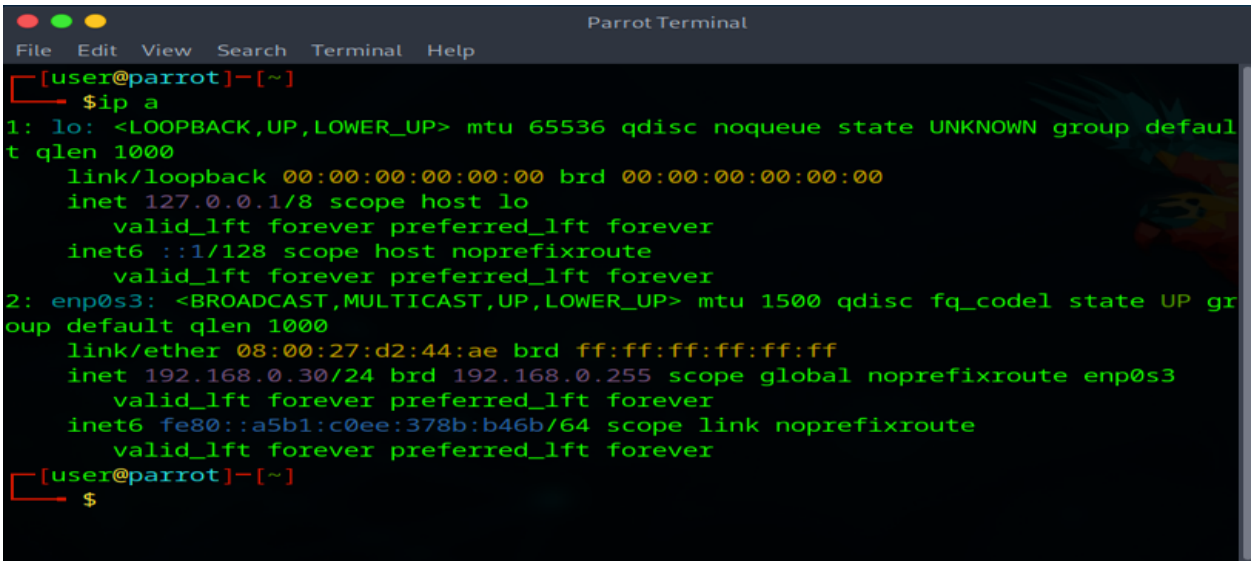
Diagrama de la red



Fuente. Autoría Propia

Figura 10

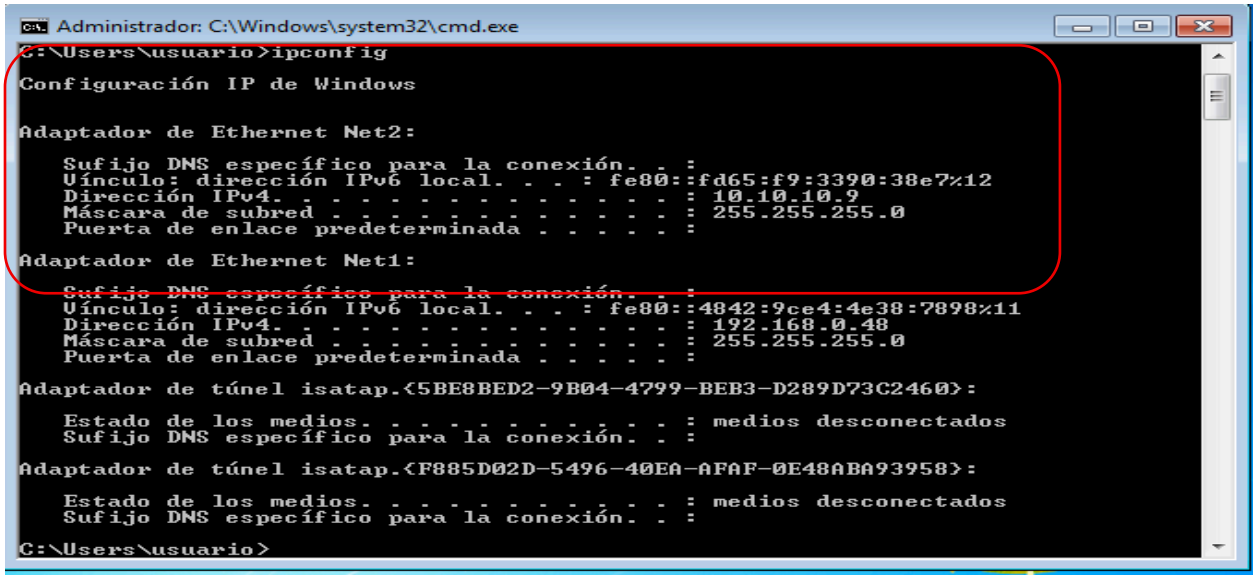
Configuración ip maquina parrot



Fuente. Autoría Propia

Figura 11

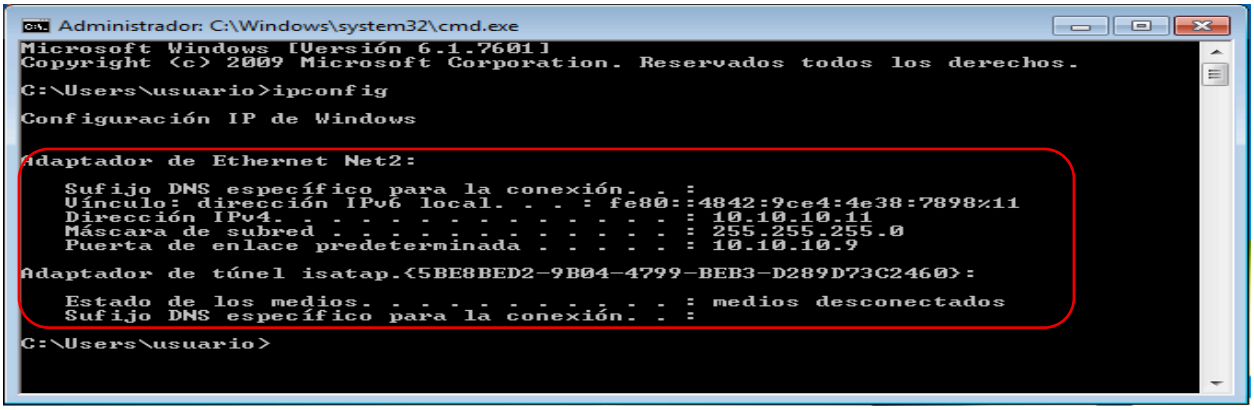
Configuración ip maquina windows 7 PIVOT



Fuente. Autoría Propia

Figura 12

Configuración ip maquina Windows 7 victima



Fuente. Autoría Propia

PASO 1 — Habilitar IP Forwarding en Windows 7 (PÍVOT)

Esto permite que Windows “pase” paquetes entre Net1 y Net2.

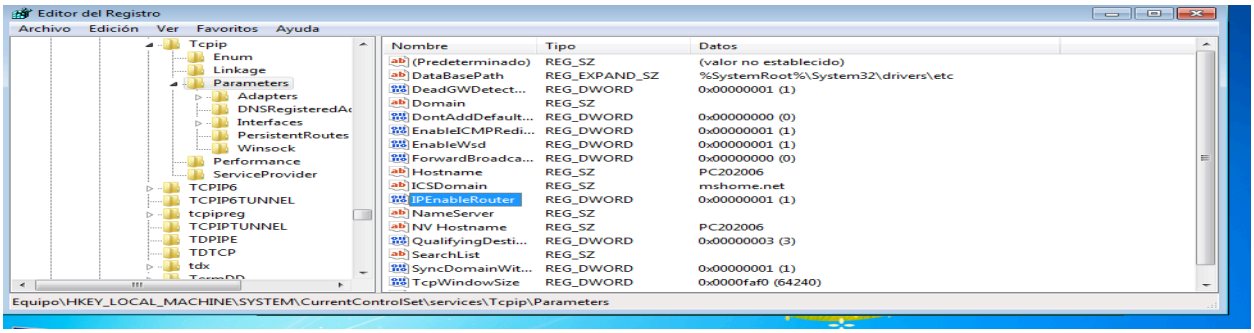
Ingresar en Regedit

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

IPEnableRouter = 1

Figura 13

Habilitación del servicio



Nota. En la figura anterior muestra el procedimiento para convierte al Windows 7 en un equipo capaz de reenviar tráfico entre sus dos interfaces.

PASO 2 — Configurar una ruta estática en Parrot OS

Parrot no sabe que la red 10.10.10.0/24 está “detrás” del PÍVOT. Así que se debe indicar la ruta.

sudo ip route add 10.10.10.0/24 via 192.168.0.48

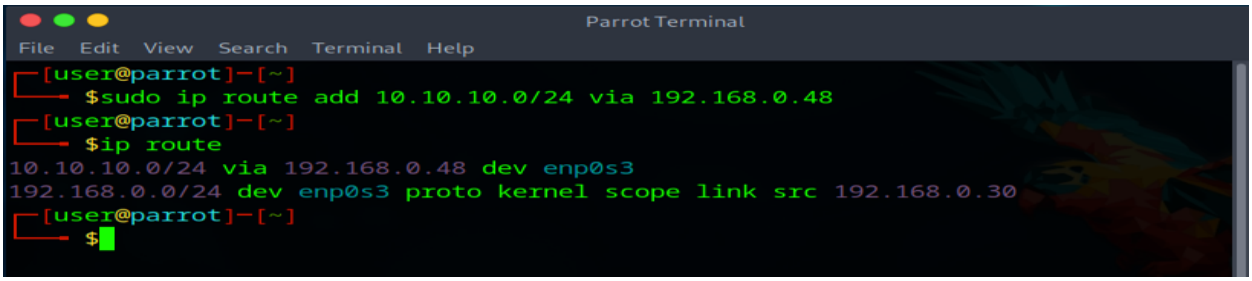
Esto significa:

“Para llegar a 10.10.10.x debes pasar por 192.168.0.48”.

ip route:

Figura 14

Ruta para la maquina parrot



Fuente. Autoría Propia

PASO 3 — Probar conectividad básica a la segunda red

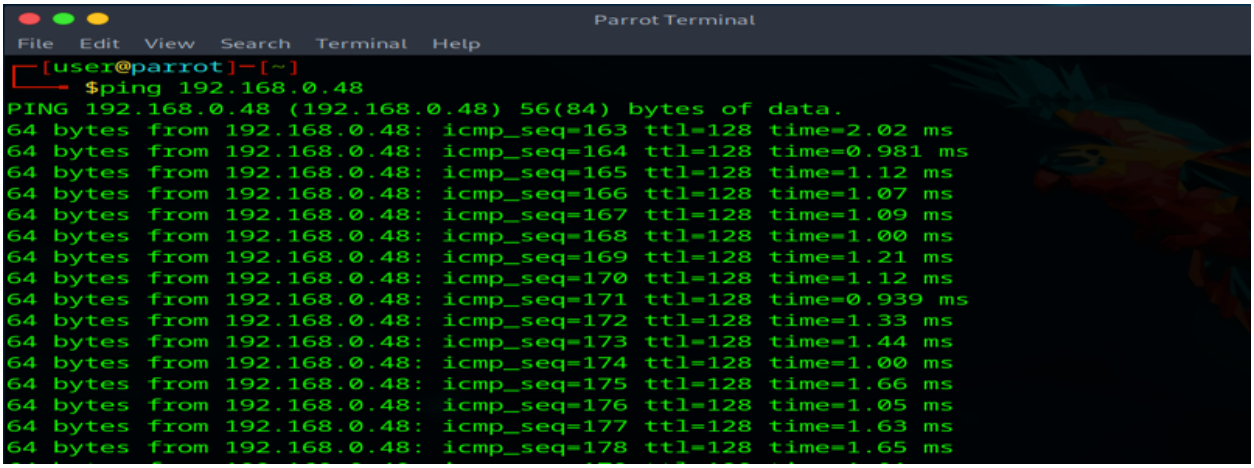
Ahora se intenta una conexión positiva desde Parrot:

Ping al PÍVOT desde la maquina Parrot (debe responder):

ping 192.168.0.48

Figura 15

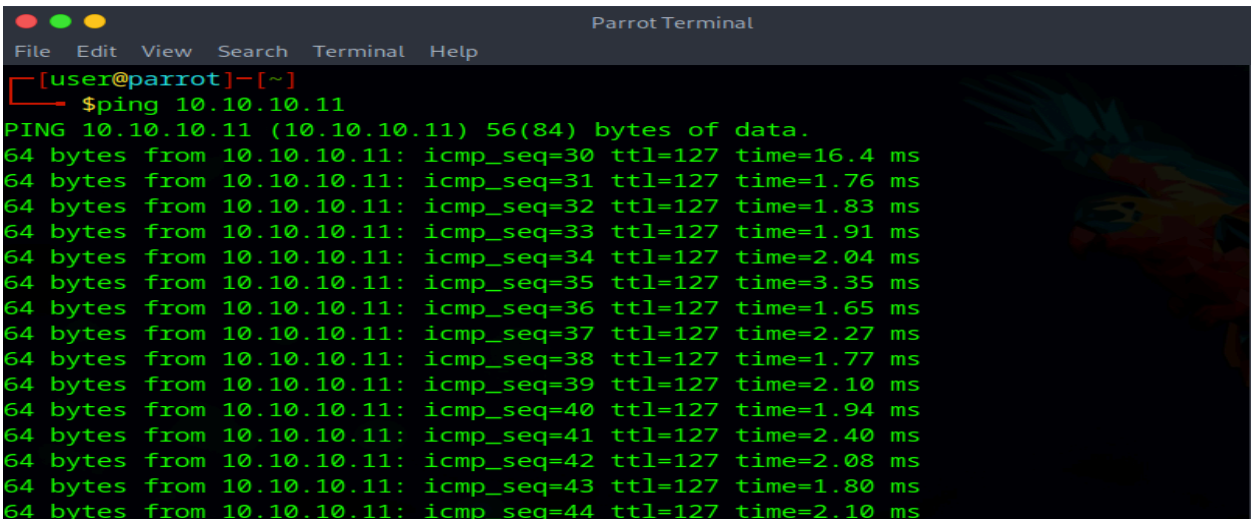
Conexión positiva desde parrot a máquina pívot



Fuente. Autoría Propia

Figura 16

Ping 10.10.10.11 positivo a la maquina víctima desde parrot



Fuente. Autoría Propia

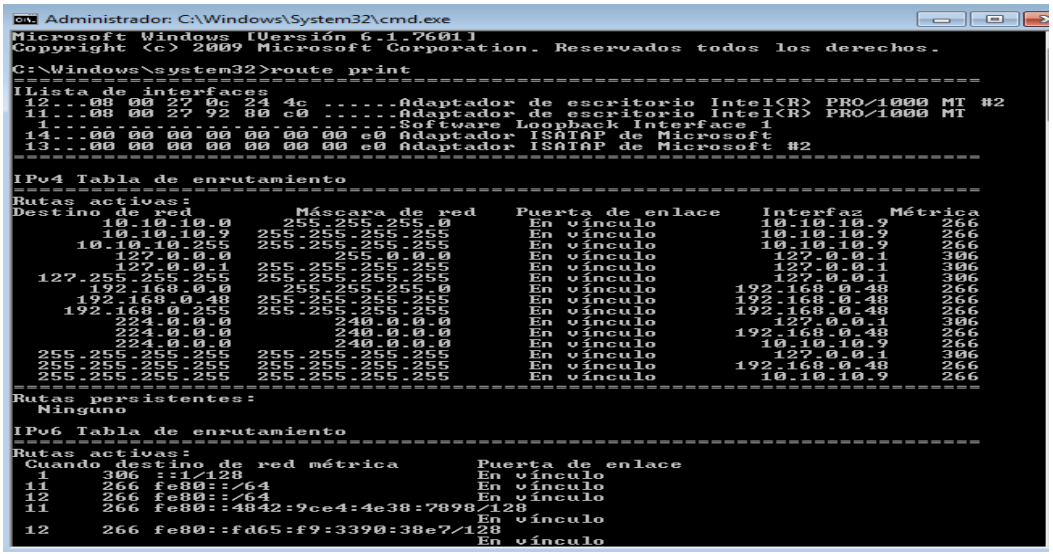
¿Qué logramos con esto?

Con estos tres pasos que se realizaron anteriormente se diseña una topología de red funcional:

- Parrot → solo está en red 192.168.0.0/24
- PIVOT → une esa red con 10.10.10.0/24
- Win7-victima → está oculto detrás del PIVOT
- El PIVOT reenvía paquetes (IP forwarding)
- Parrot tiene una ruta estática hacia la red oculta

Figura 17

Enrutamiento maquina pívot



Fuente. Autoría Propia

Con el comando route print en la maquina Pívot observaremos:

- Rutas hacia 192.168.0.0/24 (Net1)
- Rutas hacia 10.10.10.0/24 (Net2)
- Interfaz utilizada para cada red

- Métricas de enrutamiento
- Rutas de broadcast

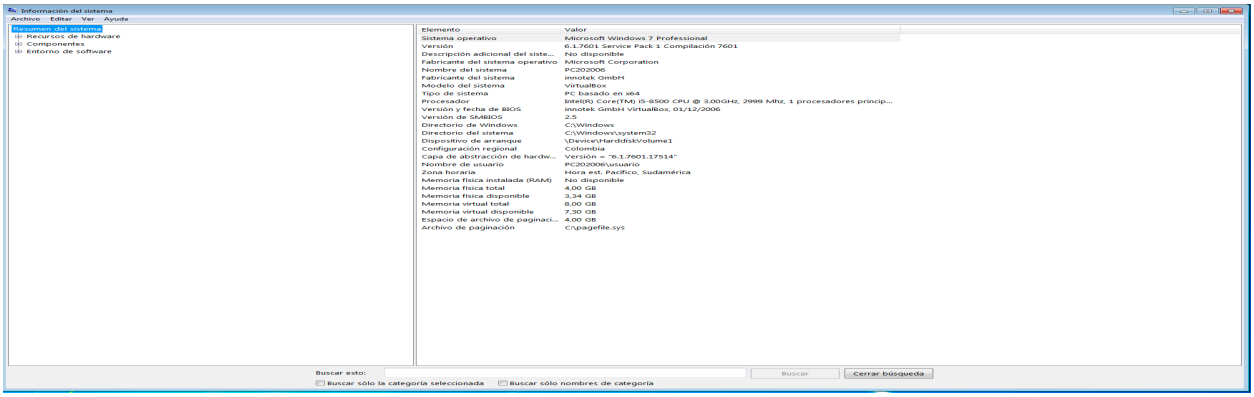
Fase de Reconocimiento:

En esta fase encontramos dos tipos de reconocimiento el Pasivo el cual no interactúa directamente con el objetivo, y el Activo el cual usaremos para este laboratorio cuyo objetivo es interacción directa en este caso con la maquina victima Windows 7, donde aplicaremos escaneos con el comando NMAP. Nota importante para este tipo de reconocimiento es necesario saber qué hay disponible antes de atacar en la maquina víctima.

Como se comentaba anteriormente las maquinas Windows 7 son sistemas ya obsoletos por su falta de actualizaciones, y cabe destacar que aún cuentan con su firewall activo por defecto que a su vez deja los puertos que pueden ser vulnerables asegurados y así se realice el escaneo con NMAP no logra detectar ningún puerto abierto; Para lograr este laboratorio se realizó la instalación del aplicativo Rejjeto_123456 en la maquina víctima la cual nos genera una vulnerabilidad para poder trabajar este laboratorio. “La función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (también conocido como HFS o HttpFileServer) 2.3x anterior a 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda.” (INCIBE-CERT, 2014)

Figura 18

Información de la maquina victima



Fuente. Autoría Propia

Fase de Enumeración Escaneo:

En esta fase se profundiza en los servicios encontrados, buscando versiones de software, usuarios, recursos, puertos secundarios, rutas y directorios ocultos. Dando continuidad al laboratorio realizamos un escaneo de la red por medio del comando nmap que permite identificar:

- Qué dispositivos están activos en la red 192.168.0.0/24 y 10.10.10.0/24.
- Qué servicios están corriendo y sus versiones en cada equipo
- Qué sistema operativo (aproximado) ejecuta cada host

Objetivo: Identificar qué hosts están activos (Host-A, Host-B) y qué servicios/puertos exponen con el siguiente comando desde la maquina atacante Parrot.

sudo nmap -sV -O 192.168.0.0/24

sudo nmap -sV -O 10.10.10.0/24

Nmap: Es la herramienta usada para reconocimiento de red.

- sV: Significa Service Version Detection, intenta identificar qué servicio y versión está corriendo en los puertos abiertos por ejemplo:

- Apache 2.4.41

- OpenSSH 8.2

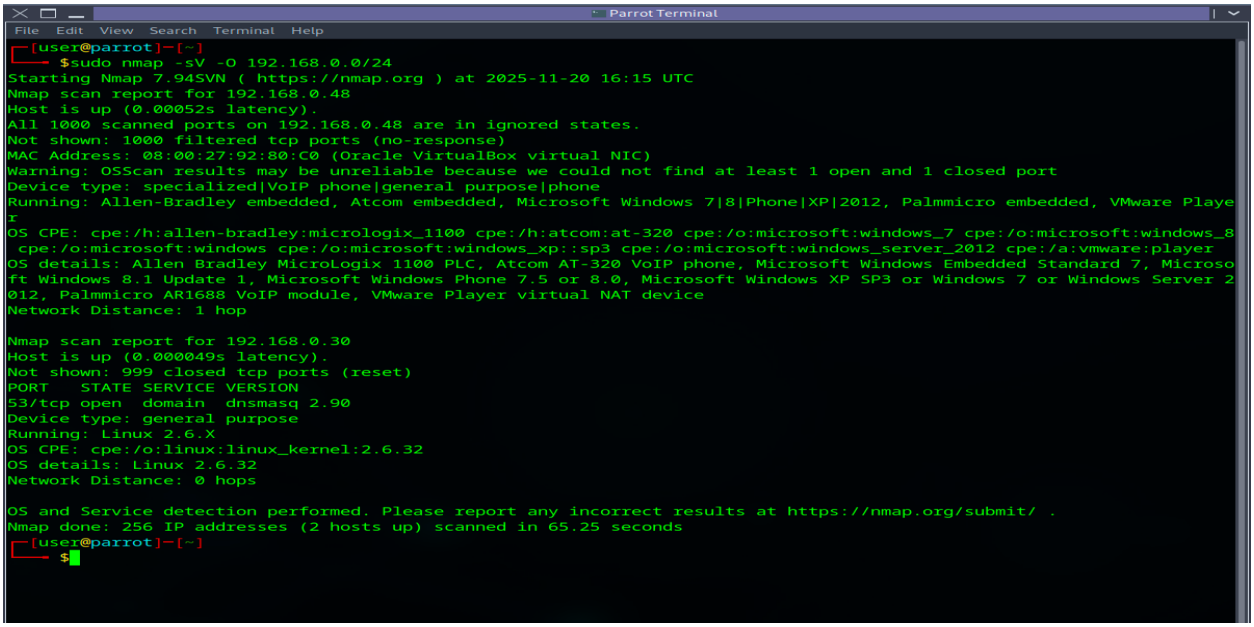
- Microsoft IIS 7.5

-O: Significa OS Detection con este comando se crea una huella de red (fingerprint) para estimar el sistema operativo del host, y cabe resaltar que la detección de SO es una estimación, no siempre exacta.

Los resultados del reconocimiento inicial mediante Nmap permiten identificar los servicios activos en la máquina víctima, tal como se evidencia en la Figura 19.

Figura 19

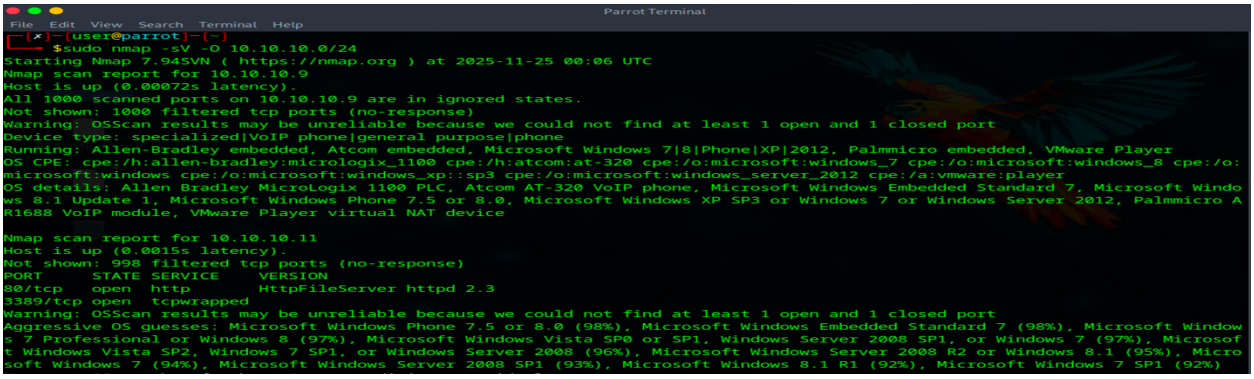
Escaneo a la IP 198.168.0.0/24



Nota. En el escaneo salen 1000 puertos filtrados, lo cual es típico cuando la máquina está viva, pero el firewall rechaza todos los puertos. Not shown: 1000 filtered tcp ports "Filtered" esto significa que el firewall está silenciosamente descartando conexiones. Para dar continuidad al laboratorio es necesario habilitar algunos puertos manualmente como:

Figura 20

Escaneo a la ip 10.10.10.0/24



Fuente. Autoría Propia

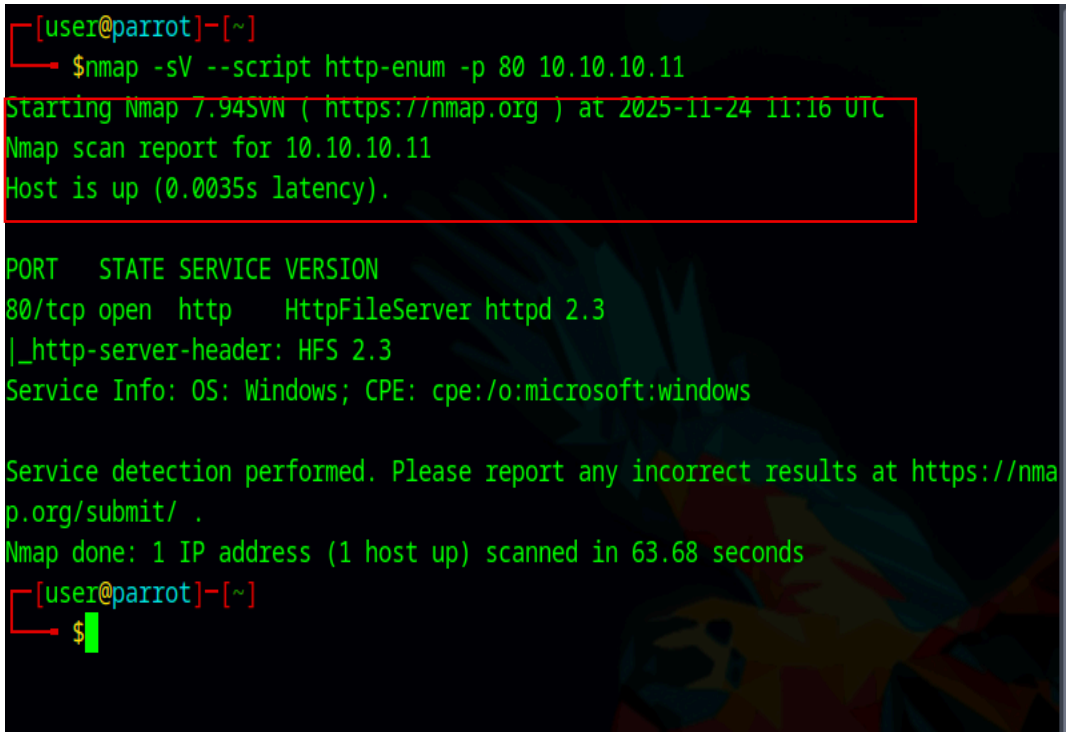
Se evidencia la máquina Pivot sin puertos abiertos ya que tiene en funcionamiento su Firewall, por otro lado se evidencia la maquina victima con Windows 7 donde tiene su Firewall activo pero a su vez está corriendo el aplicativo de Rejetto v2.3 que genera la evidencia del puerto 80/tcp ubicado con IP 10.10.10.11. Al ejecutarse este aplicativo se manifiesta una vulnerabilidad en la maquina victima la cual tiene como función correr el servicio "HttpFileServer httpd v 2.3" en el puerto 80/tcp.

De acuerdo al portal web incibe este servicio implementa la vulnerabilidad CVE-2014-6287 "La función findMacroMarker en parserLib.pas en Rejetto HTTP File Server (también conocido como HFS o HttpFileServer) 2.3x anterior a 2.3c permite a atacantes remotos ejecutar programas arbitrarios a través de una secuencia %00 en una acción de búsqueda" (INCIBE-CERT, 2025).

Estos ataques permiten a los delincuentes ejecutar programas en la máquina afectada que roban información, permiten un acceso adicional, crean nuevas cuentas con roles de administrador, configuran Shells inversas y muchas otras cosas perjudiciales.

Figura 21

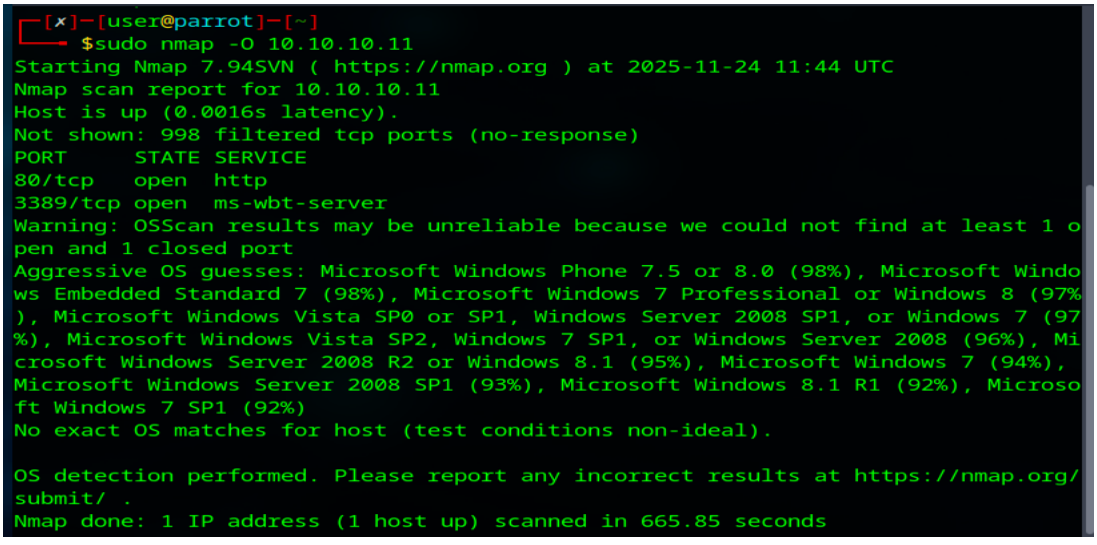
Nueva búsqueda con NMAP para más información



Fuente. Autoría Propia

Figura 22

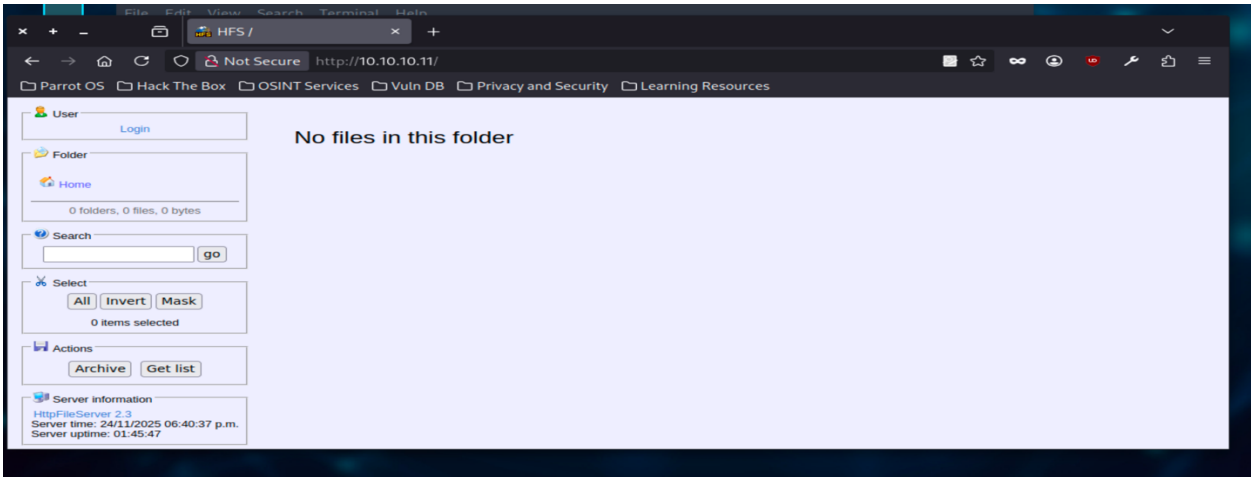
Comando para saber el SO



Nota. En esta figura el sistema muestra el sistema operativo de la Ip la cual se está revisando.

Figura 23

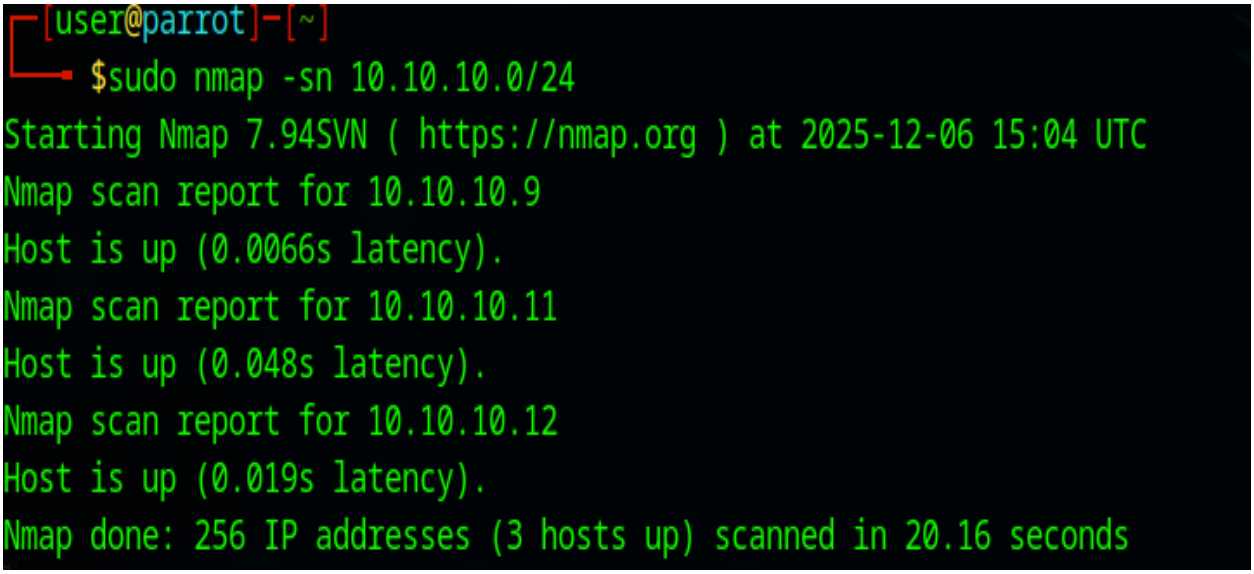
Servidor web de archivos HFS



Nota. En esta evidencia se observa que la dirección Ip de la maquina victima tiene un servicio web activo.

Figura 24

Escaneo de ip



Nota. Aquí se logra identificar que la maquina Parrot está viendo las tres maquinas del laboratorio Pivot, Víctima, y Host B para el cumplimiento de lo que se solicita en el anexo 4.

Para la ejecución del Pivoting el escenario se compone:

Parrot: 192.168.0.30

Win7 Pivot: 192.168.0.48 y 10.10.10.9 (doble NIC)

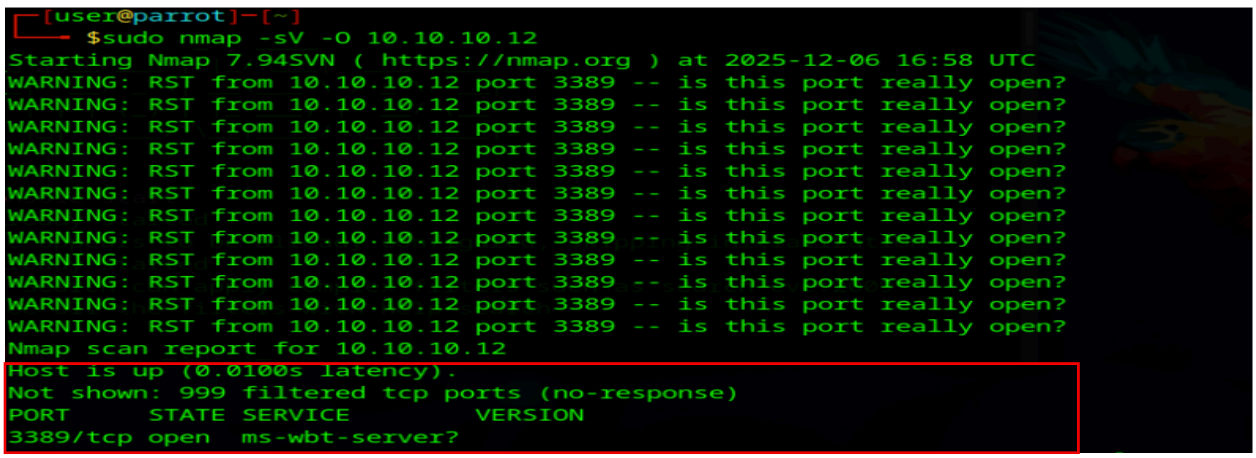
Host-A: 10.10.10.11 (vulnerable HFS)

Host-B: 10.10.10.12

La función del Pivoting es demostrar que tras afectar el Host-A (o usar el Pivot), se puede efectuar la enumeración efectiva de servicios en Host-B y/o interactuar con ellos, y que ese acceso depende del pivote.

Figura 25

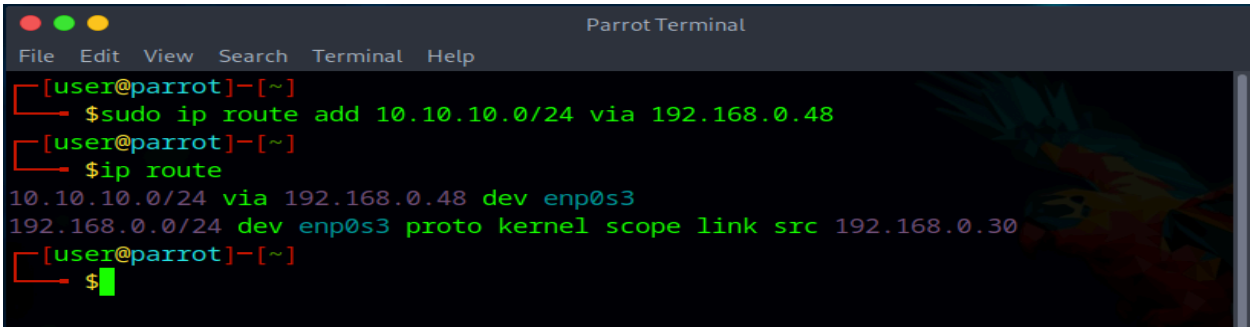
Escaneo de puertos en el Host B



Nota. Se logra evidenciar que el puerto 3389/tcp ms-wbt-server es el servicio RDP (Remote Desktop Protocol) de Microsoft. No es una vulnerabilidad por sí mismo, pero cuando está expuesto se convierte en una superficie de ataque muy común, y se asocia a CVE-2019-0708 (BlueKeep) “es una vulnerabilidad crítica de ejecución remota de código (RCE) en Remote Desktop Services (RDP) de Microsoft. Afecta a sistemas antiguos (incluido Windows 7 SP1) cuando RDP está habilitado y el sistema no está parcheado.” (CVEdetails.com, s. f.)

Figura 26

Camino del pivot



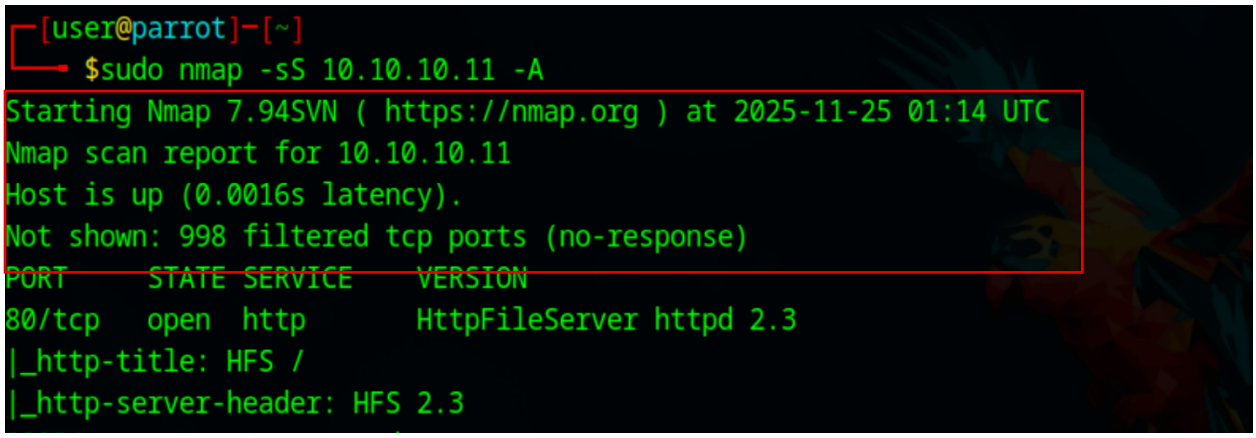
Fuente. Autoría propia

Fase de Explotación:

"Para la ejecución exitosa de este laboratorio fue necesario el apoyo de un ejercicio guiado de pivoting en entornos virtualizados, adaptado y replicado de manera controlada según una demostración práctica disponible en línea" (*TechEduca*, 2024). Con lo anteriormente descrito procedemos a correr nuestra maquina atacante la maquina parrot, donde se corre el comando sudo nmap -sS 10.10.10.11 para detectar el puerto vulnerable en la maquina víctima el cual sería el 80/tcp.

Figura 27

Puerto abierto

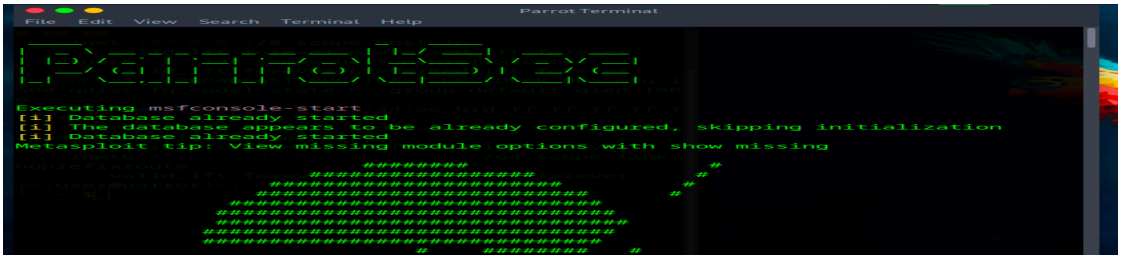


Nota. Se observa en la figura la información del puerto 80 de acuerdo al comando nmap.

Para esta fase se usará el framework Metasploit “es una herramienta desarrollada en Perl y Ruby en su mayor parte, que está enfocada a auditores de seguridad y equipos Red Team y Blue Team. Es una herramienta muy completa que tiene muchísimos exploits, que son vulnerabilidades conocidas, en las cuales tienen también unos módulos, llamados payloads, que son los códigos que explotan estas vulnerabilidades.” (Rizaldos, 2018)

Figura 28

Ingreso a la consola Metasploit

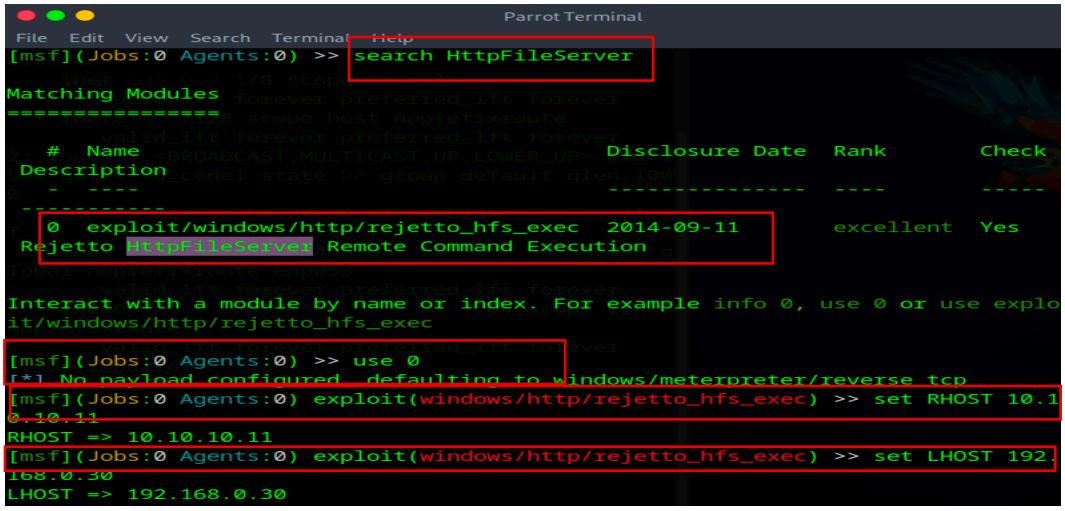


Nota. Aquí se observa la configuración e inicio del framework metasploit.

De acuerdo al análisis de la red ya tenemos el servicio del puerto 80/tcp que se quiere explotar, para esto procedemos a correr el siguiente comando para saber que exploit usar.

Figura 29

Búsqueda de exploit para el servicio

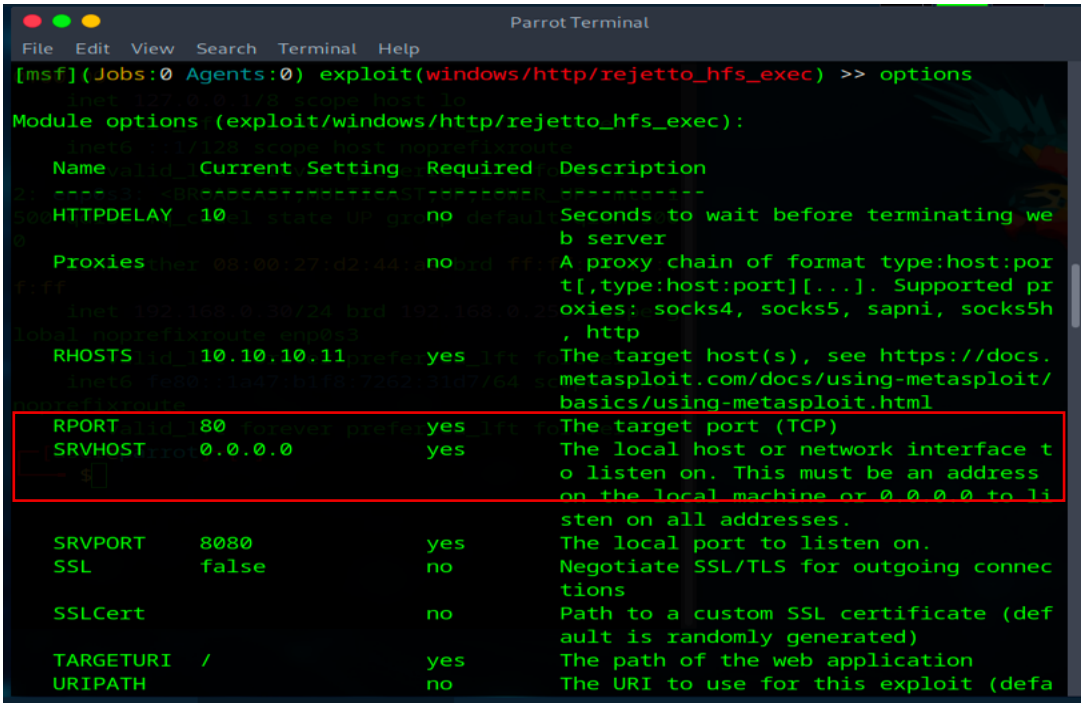


Nota. En la imagen anterior como primer paso buscamos el servicio del puerto en la base de

datos de metasploit para saber si existe algún exploit. Como se puede observar hay un exploit en la base de datos **exploit/Windows/http/rejetto_hfs_exec** el cual seleccionamos con el comando **use.** El paso a seguir es verificar con el comando options que parámetros obligatorios necesita tanto el exploit como el payload en este caso el RHOST del exploit con la ip de la maquina víctima y el LHOST payload con la ip de la maquina atacante. Para tener un poco más claro el tema de la función de un exploit, este término hace referencia a "programas utilizados por hackers de sombrero blanco y sombrero negro, con el fin de utilizar una vulnerabilidad informática para infiltrarse en un ordenador." (Cilleruelo, 2024)

Figura 30

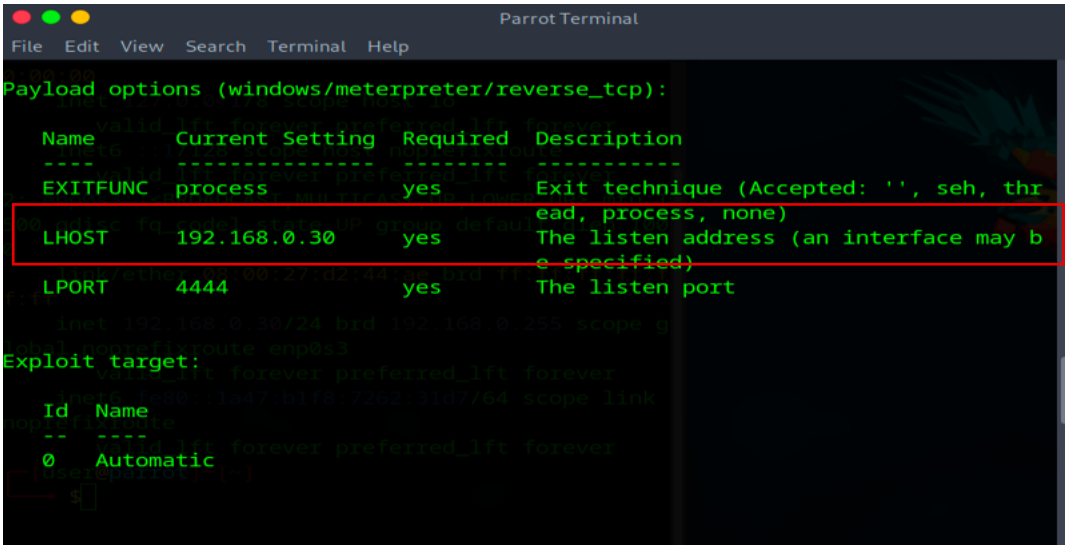
Opciones del exploit y payload



Nota. En esta figura se muestra la configuración del RHOST que es la maquina víctima.

Figura 31

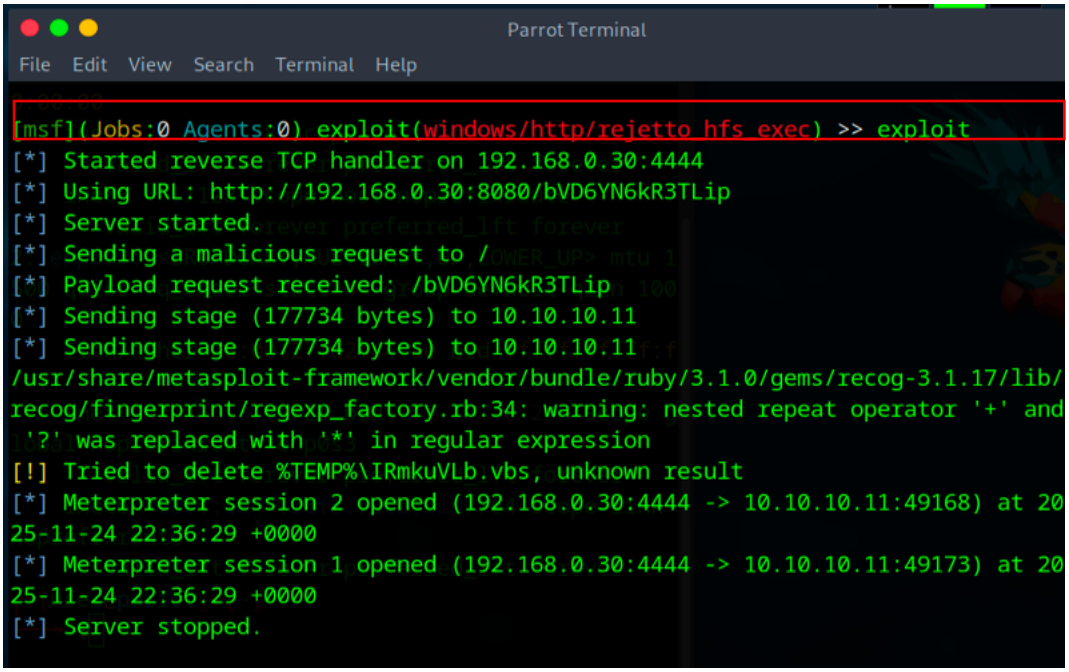
Opciones Payload



Nota. En esta figura se muestra la configuración del LHOST que es la maquina atacante.

Figura 32

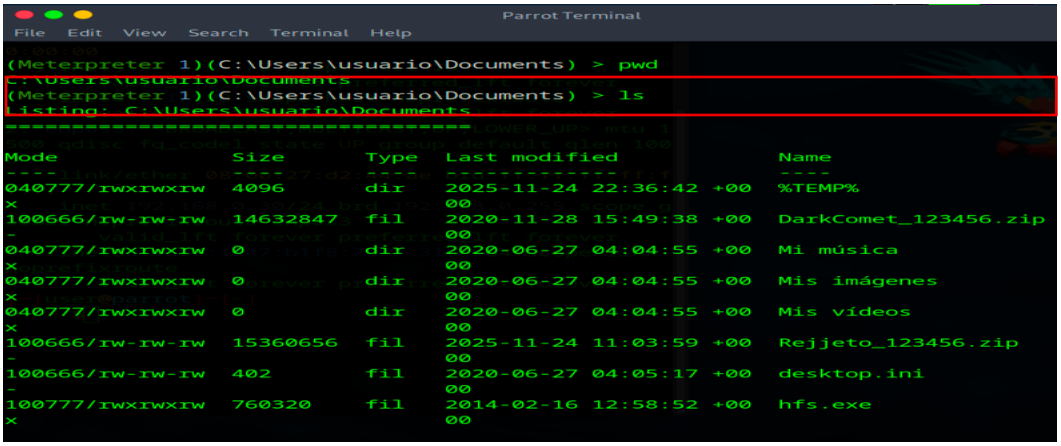
Correr el Exploit



Fuente. Autoría Propia

Figura 33

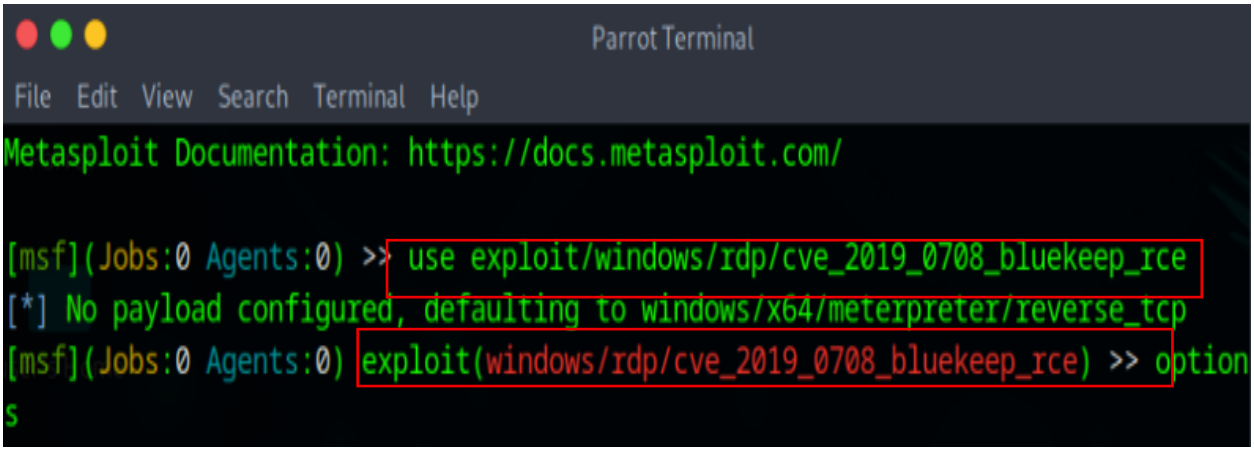
Ingreso del exploit usando Meterpreter



Nota. En la evidencia anterior se observa que la explotación se da inicio por medio del exploit y el payload precargados dando acceso a un Shell de comandos en el del módulo meterpreter, el cual tiene como función ser la interfaz entre la maquina atacante y la maquina víctima por medio de comandos de forma remota, de esta manera permitiendo extraer información, control de cámara, mouse, teclado, y creación de usuarios.

Figura 34

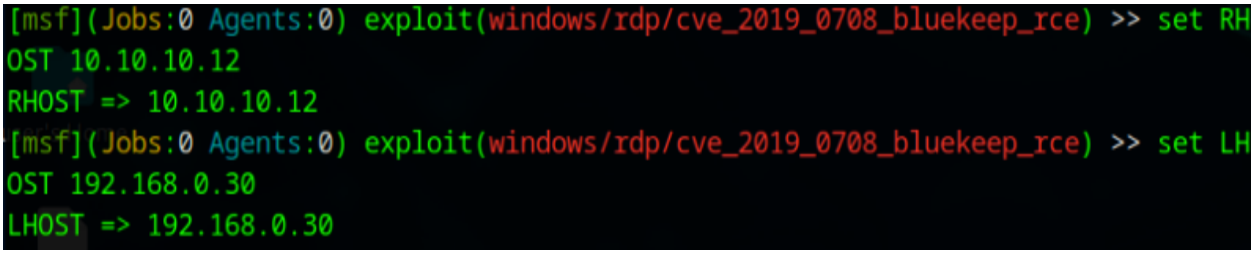
Configuración Exploit Maquina Host B



Nota. En la figura anterior se efectúa la selección del exploit el cual se va a utilizar para realizar la explotación de la vulnerabilidad asociada al puerto abierto en la maquina Host B.

Figura 35

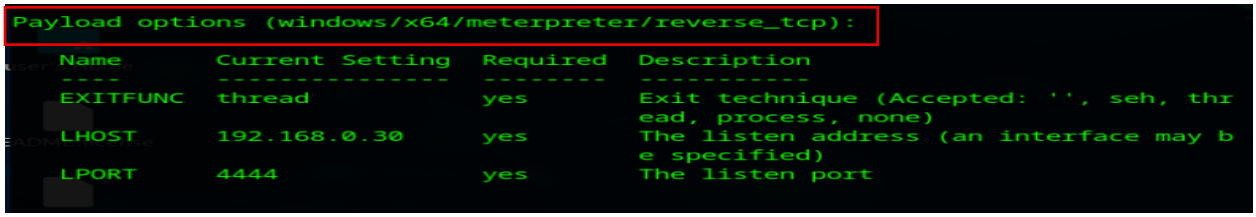
Configuración del RHOST y LHOST



Fuente. Autoría Propia

Figura 36

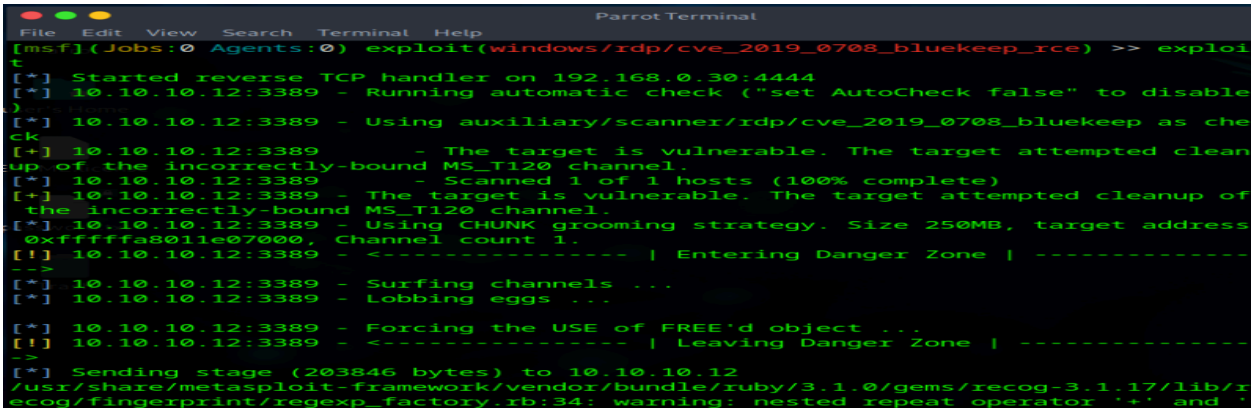
Payload para el Exploit



Fuente. Autoría Propia

Figura 37

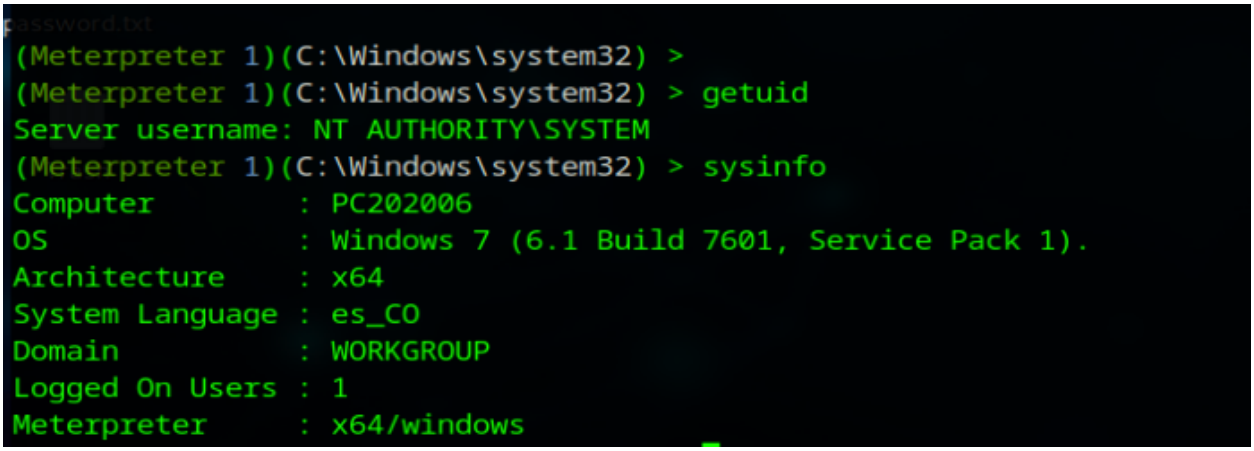
Ejecución del Exploit



Nota. En la figura anterior se confirma que el Pivot fue todo un éxito y se logró vulnerar la maquina Windows 7 Host B desde la maquina Parrot por medio del exploit seleccionado donde se explota CVE-2019-0708 (BlueKeep).

Figura 38

Shell con permisos de SYSTEM e información de la maquina vulnerada



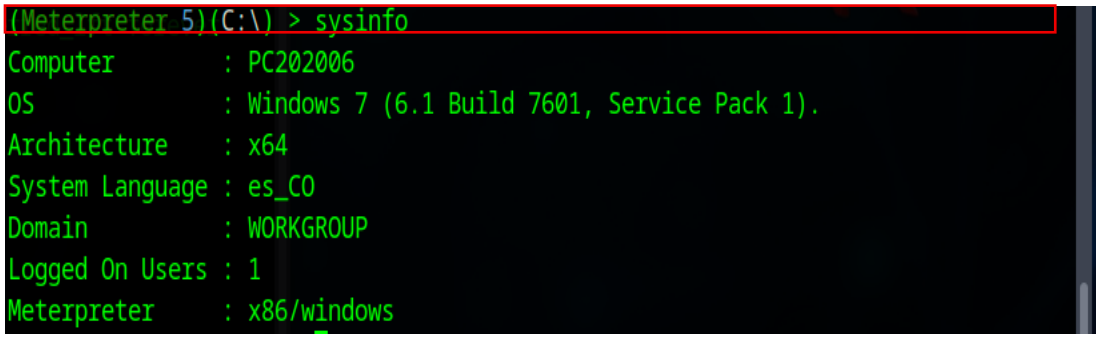
Nota. Con el paso anterior se evidencia que gracias al exploit y el framework Meterpreter fue posible vulnerar los permisos del sistema en la maquina host B como se muestra en la imagen anexa.

Fase de Post - Explotación:

Con el comando pwd se puede observar los archivos que se encuentran en la maquina víctima.

Figura 39

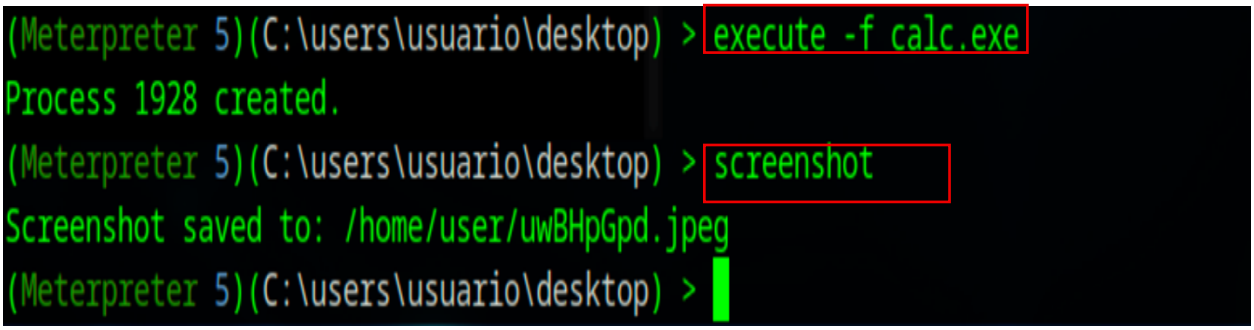
Comando para ver información del sistema



Nota. En esta figura se observa que el comando a utilizar para lograr saber la información del equipo a vulnerar es sysinfo.

Figura 40

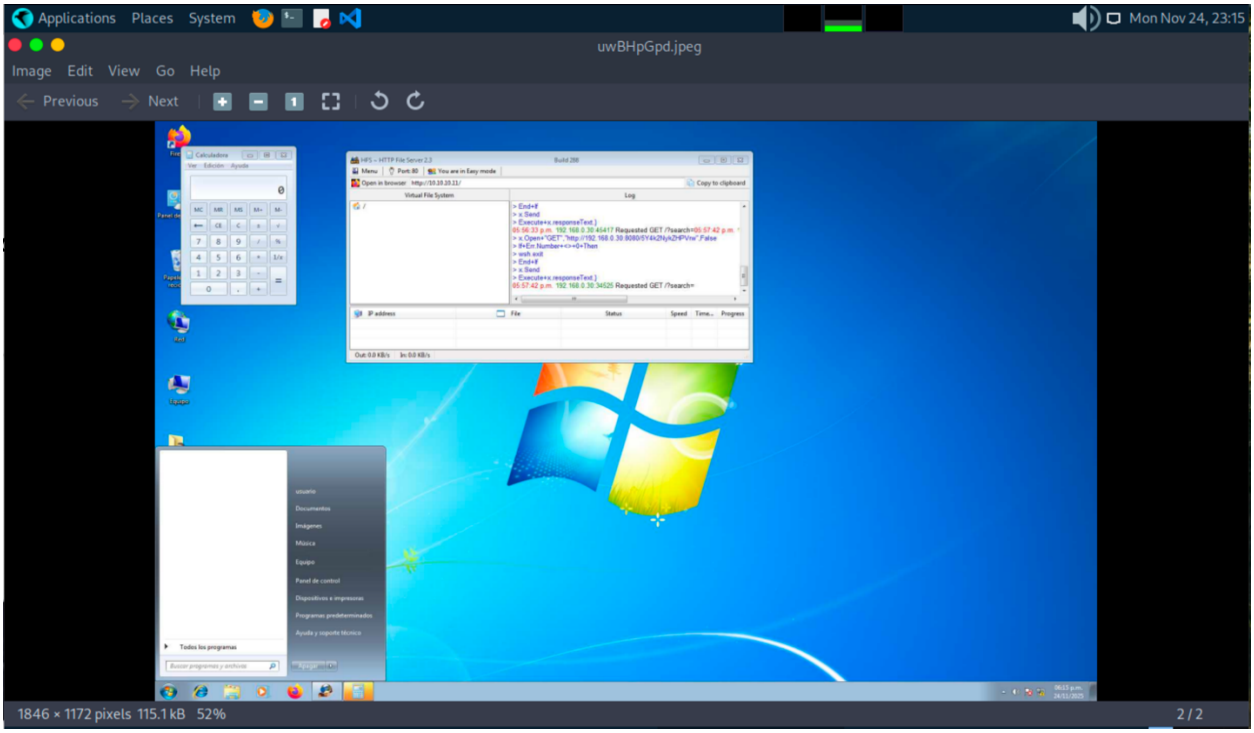
Comando para manipular calculadora y tomas de capturas



Nota. Con el comando execute -f cal.exe como se evidencia en esta figura se observa que es posible manipular el aplicativo de la calculadora de la maquina victima remotamente.

Figura 41

Captura del escritorio maquina victima

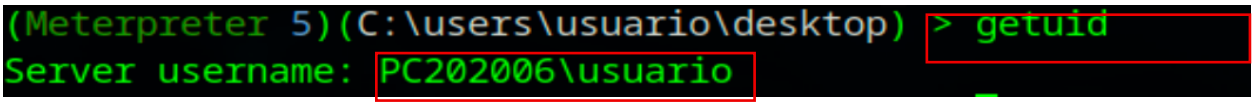


Fuente. Autoría Propia

Para esta fase con el comando getuid se observa que el sistema nos va a mostrar como resultado el nombre del usuario actual de la maquina víctima que en este caso es Usuario PC202006 como se evidencia en la figura 42.

Figura 42

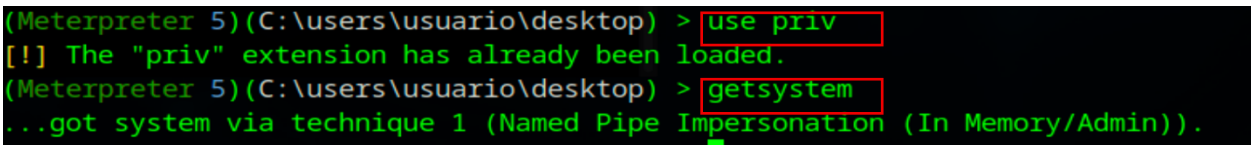
Comando getuid



Fuente. Autoría Propia

Figura 43

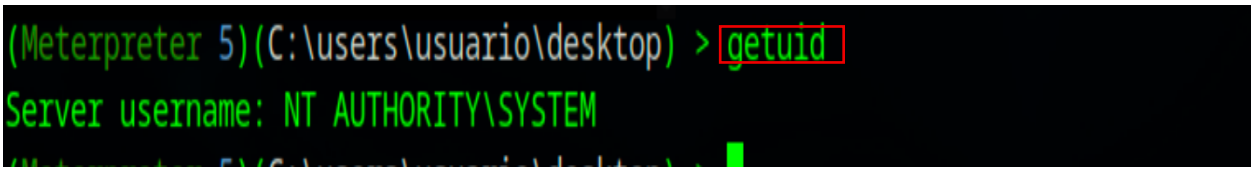
Comando para elevar privilegios con getsystem



Fuente. Autoría Propia

Figura 44

Privilegios system

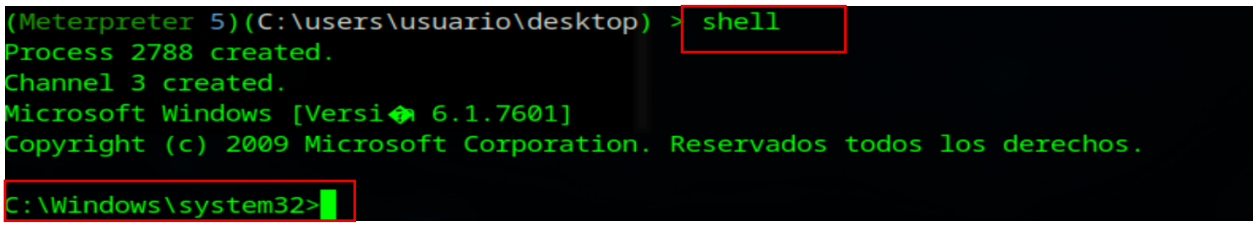


Fuente. Autoría Propia

Al aplicar estos comandos tendremos acceso total a la creación de usuarios con privilegios de administrador. Seguidamente se crea una Shell con el fin de obtener una interface idéntica a la de la maquina víctima para iniciar con el proceso de creación de usuarios.

Figura 45

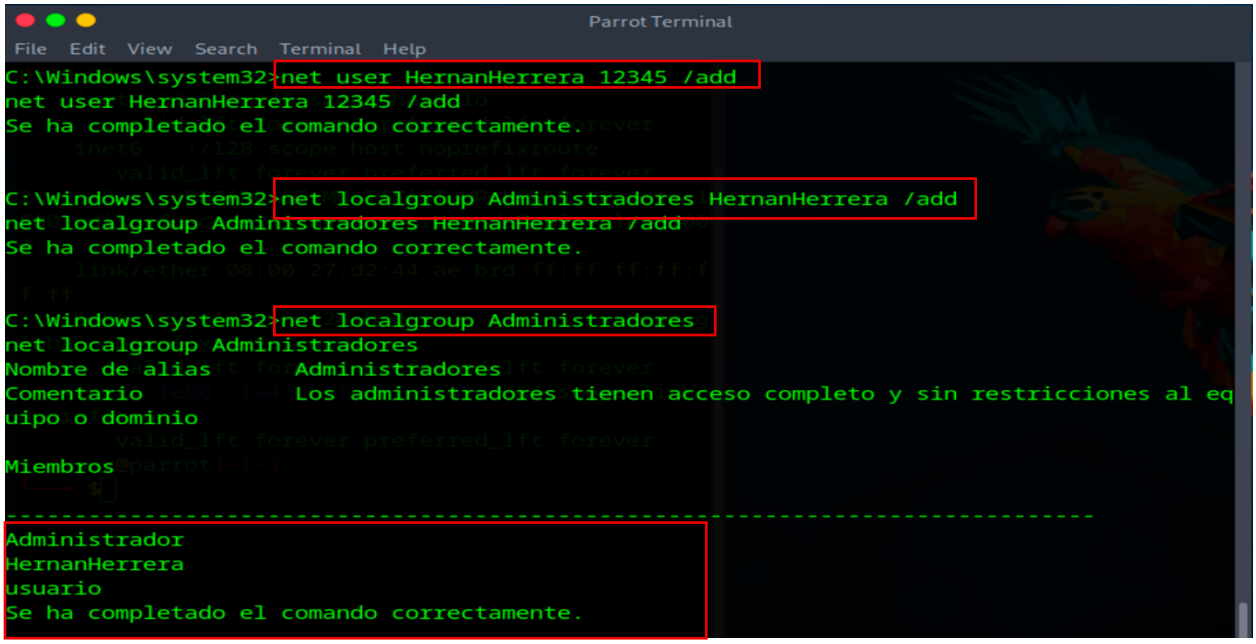
Creación de Shell



Nota. Con el comando Shell es posible ingresar a la terminal de la maquina víctima, de esta manera es posible la creación de usuario con privilegio como se muestra en la figura 46.

Figura 46

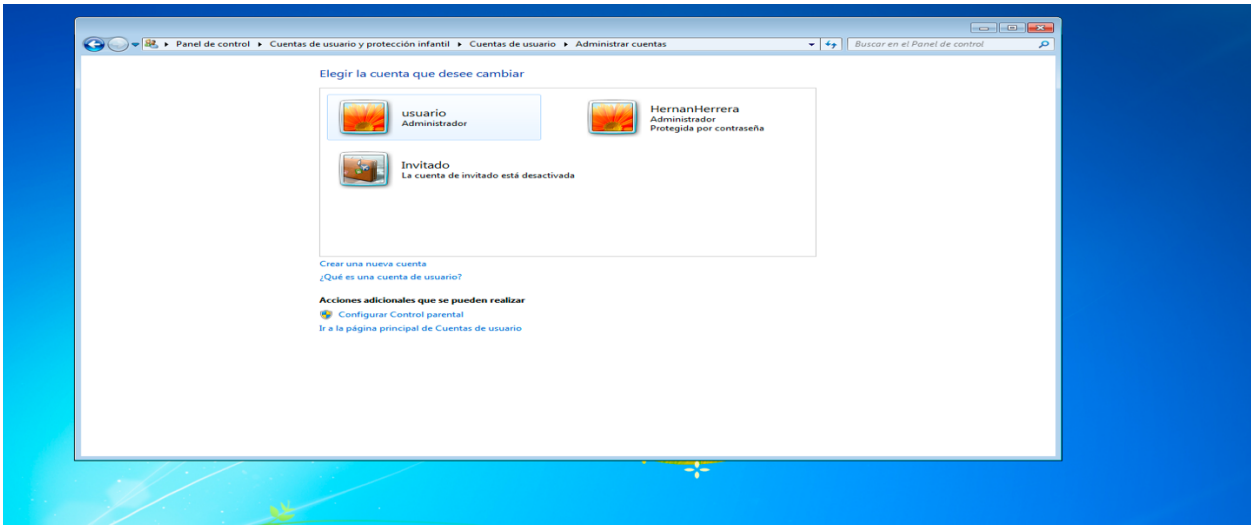
Creación de usuario con privilegio



Fuente. Autoría Propia

Figura 47

Usuarios



Fuente. Autoría Propia

A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la Máquina - 1 Windows.

En relación con la base de información del caso en la que hay evidencia de datos Fugas dentro de la organización con respecto a las fugas de datos dentro de un equipo específico, se procede a determinar que hay una máquina infectada que se ejecuta en Windows 7 x64 y ejecuta Rejetto V2.3.

Se inicia el proceso de identificación de puertos abiertos donde se observa que en el puerto 80 el servidor de archivos HTTP HFS 2.3 de Rejetto v2.3 se ejecuta, el cual es un servidor web para compartir archivos que están libres de malware, pero que tienen vulnerabilidades críticas donde los exploits de Shell se pueden ejecutar para obtener shells con Meterpreter. En este escenario crítico de tener acceso remoto, es un resultado de la mala administración de

políticas de seguridad dejando el cortafuegos desactivado, dejando Puertos TCP/IP expuestos que afectan gravemente a la corporación.

¿Qué herramienta utilizó para poder identificar los fallos de seguridad de la " Máquina - 1 Windows"? ¿Qué puerto abre la aplicación específica en el anexo?

Atreves de la maquina parrot por medio de la consola y con la configuración adecuada cómo se ha explicado a lo largo de este laboratorio, se utiliza la poderosa herramienta Nmap que nos permite identificar los puertos abiertos que se encuentran en toda la red en la cual están las maquinas del laboratorio por medio de los siguientes comandos:

sudo nmap -sV -O 10.10.10.0/24

sudo nmap -sV -O 10.10.10.11

Nmap permitió identificar la existencia del servicio HttpFileServer httpd 2.3 y el puerto asociado: 80/tcp abierto que coincide con la vulnerabilidad CVE-2014-6287.

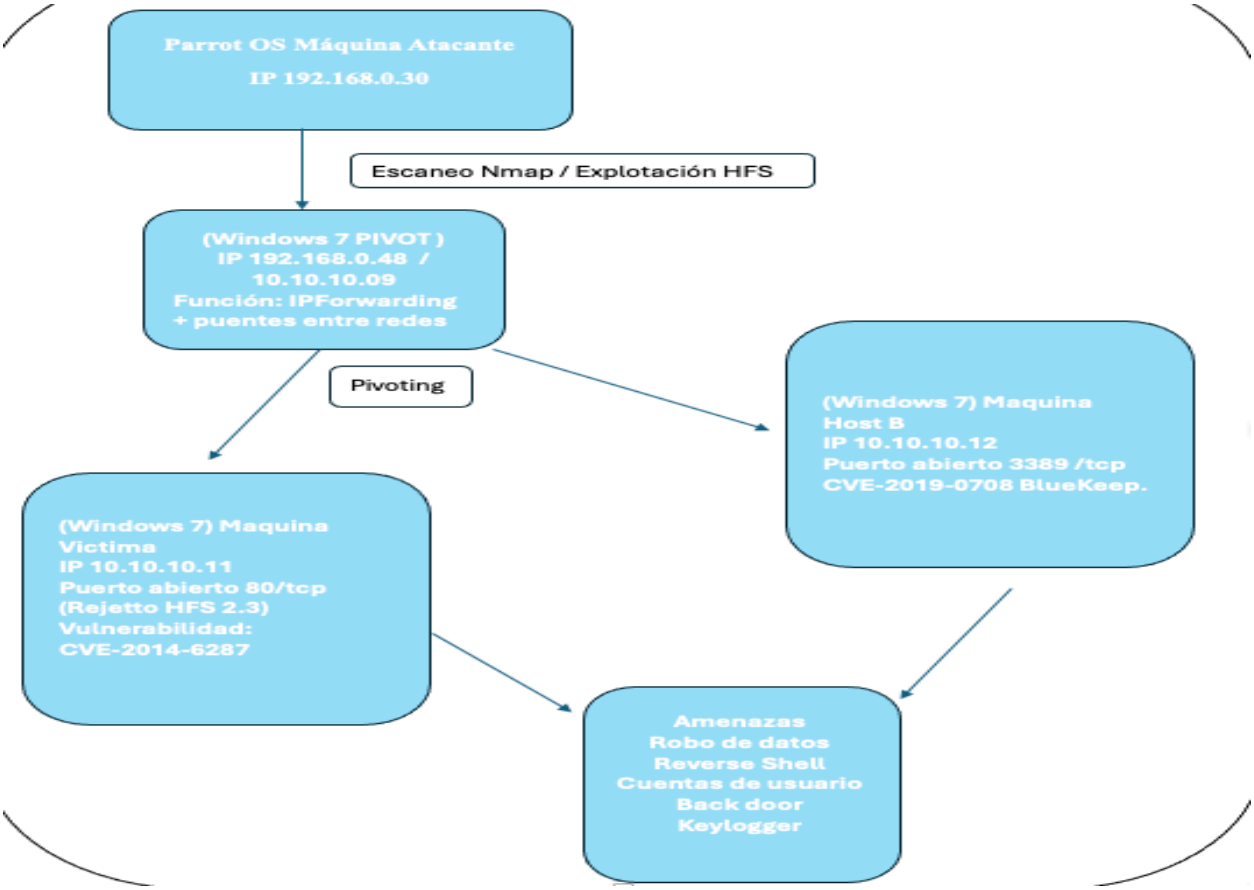
Explique con sus palabras y de manera específica cómo afecta el ataque a las máquinas (Windows) encontradas en la red: Haga uso de gráficos para explicar el ataque.

La explotación inicial en Host-A (Vicitma), el atacante puede ejecutar comandos arbitrarios a través de una carga útil maliciosa enviada mediante un payload vulnerable del software debido a la exposición del servidor HFS 2.3 en el puerto 80, permitiendo de esta manera acceso remoto al shell, ejecución de cargas útiles de Meterpreter, leer o escribir archivos en el sistema, instalación de la persistencia y creación de usuarios administradores.

Al entrar, el atacante toma comandos como getuid y luego getsystem, dando un control total sobre la máquina. El atacante utiliza Host-A como trampolín a Host-B debido al reenvío de IP en el Pivot, el enrutamiento estático en Parrot y el acceso de privilegios otorgado por la vulnerabilidad en Host-A.

Figura 48

Diagrama del ataque



Nota. En esta figura se muestra la configuración del ataque efectuado en el laboratorio.

Documente, cada uno de los pasos que ejecutó y las evidencias correspondientes para la validación de la vulnerabilidad en la máquina Windows; integre además la descripción del pivoting realizado hacia la segunda máquina.

Paso inicial configuración de la topología:

El escenario se compone de tres máquinas virtuales instaladas en virtualbox bajo la arquitectura de MacOS:

- Parrot OS (Atacante) – Red: 192.168.0.30/24
- Windows 7 PIVOT – Red 1: 192.168.0.48 | Red 2: 10.10.10.9

- Windows 7 Víctima (Host-A) – Red: 10.10.10.11

Primer paso:

Configuración para la habilitación de IP Forwarding en la maquina Windows 7 PIVOT con el propósito de permitir que Windows reenvié tráfico entre ambias redes para que actue como router.

- Modificación de los parámetros por medio del comando Regedit.

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

  IPEnableRouter = 1

Segundo paso:

Configuración de la red estática en parrot

- Parrot solo tenía visibilidad de 192.168.0.30/24.
- Para acceder a 10.10.10.0/24 se añadió:

sudo ip route add 10.10.10.0/24 via 192.168.0.48

Figura 49

Captura del comando ip route correcta.

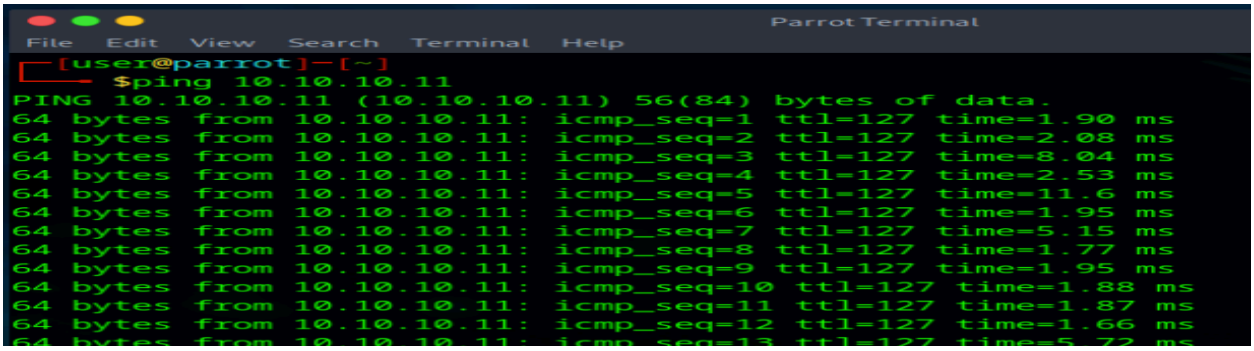
Fuente. Autoría Propia

Tercer paso:

Ping desde parrot a las maquinas PIVOT y víctima.

Figura 50

Ping maquina victima



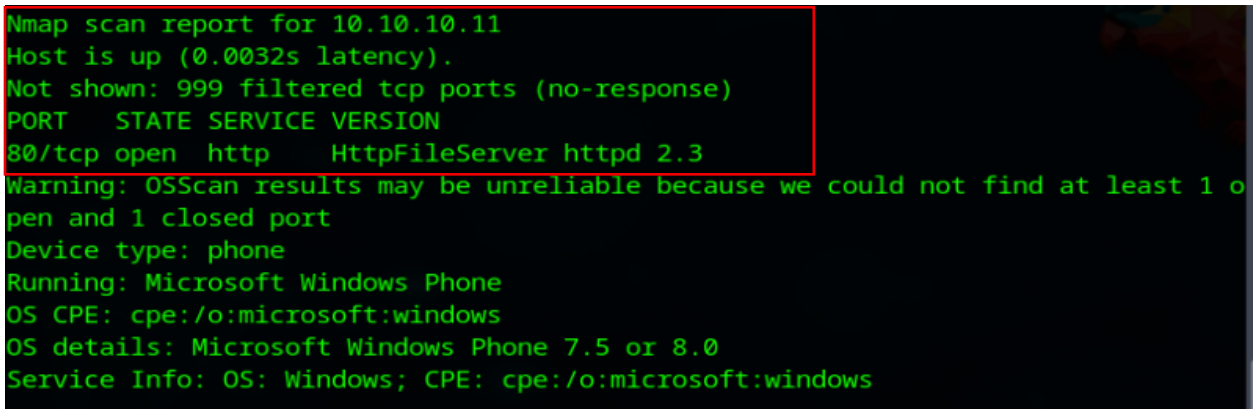
Fuente. Autoría Propia

Cuarto paso Reconocimiento:

Reconocimiento con el comando Nmap, en este apartado al efectuar la búsqueda con el comando sudo nmap -sV -O 192.168.0.0/24 evidenciamos que muestra las IP de la maquina parrot y maquina pivot sin puertos abiertos, y en la red 10.10.10.0/24 encontramos las IP de la maquina pivot que es el puente a la maquina víctima, parta esta máquina victima si se evidencia el puerto 80/tcp abierto en la dirección 10.10.10.11.

Figura 51

Puerto abierto



Fuente. Autoría Propia

Quinto paso fase explotación:

Se corre metasploit con el comando msfconsole:

Figura 52

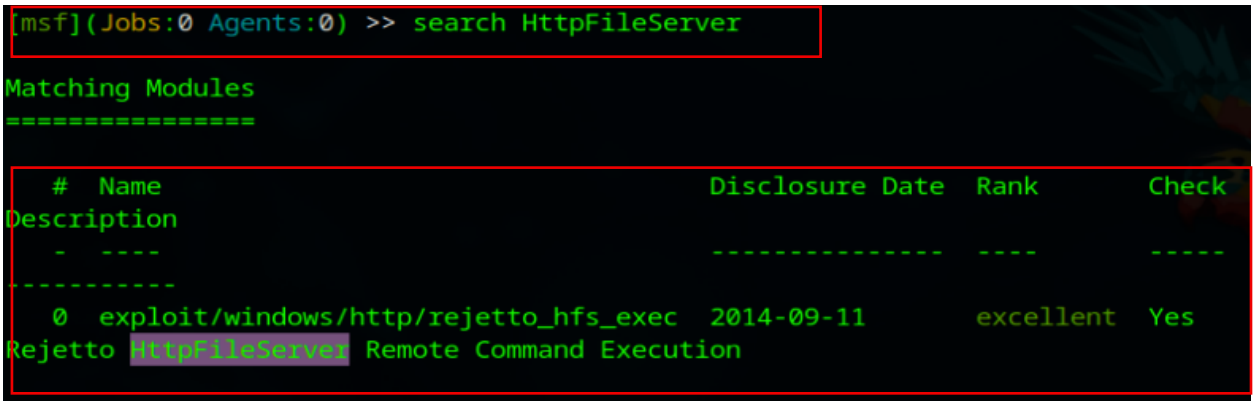
Inicio de metasploit

Fuente. Autoría Propia

Con la referencia e información del puerto abierto buscamos el exploit el cual se va utilizar para explotar la vulnerabilidad y esto se realiza con el comando search.

Figura 53

Búsqueda del exploit

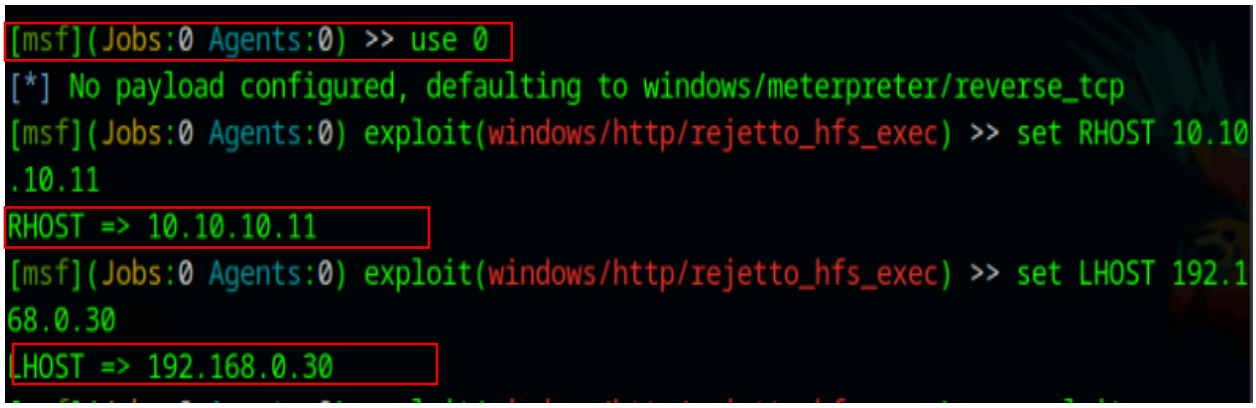


Nota. En la imagen anterior se evidencia que el comando search busca el exploit referente a la

vulnerabilidad del puerto abierto el cual tiene que ver con rejetto, aplicativo que está corriendo en la maquina víctima.

Figura 54

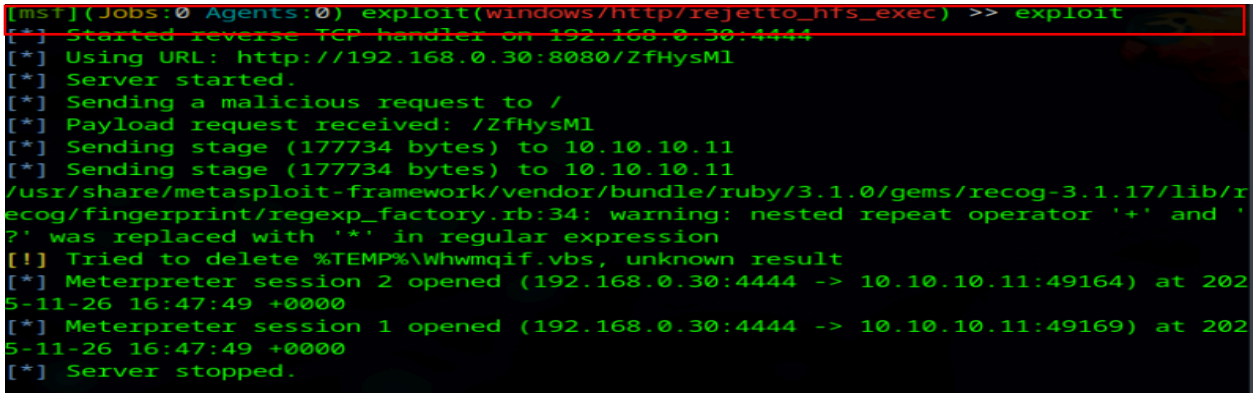
Selección del exploit



Nota. Con el comando use 0 seleccionamos el exploit y se procede a revisar la configuración de este, el cual se efectúa con el comando options. En la mayoría de los casos los exploit solicita que se configure RHOST que hace referencia a la dirección Ip de la maquina víctima 10.10.10.11 y LHOST que hace parte del payload y se refiere a la dirección Ip de la maquina atacante 192.168.0.30.

Figura 55

Ejecución del exploit

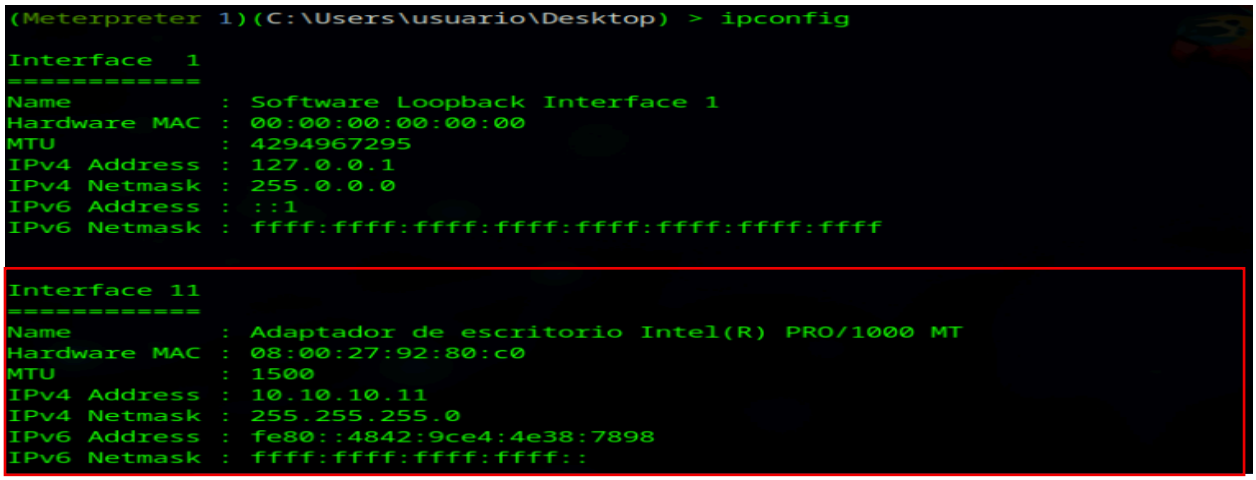


Nota. Como se observa, la maquina atacante con Parrot logra establecer conexión con la víctima

al 10.10.10.11 donde seguidamente se ejecuta el Shell de Windows, que me permite ejecutar comandos dentro de la maquina victima con el payload Meterpreter. Para demostrar que hay un control positivo de la maquina víctima se efectúa un ipconfig para saber la Ip de la máquina.

Figura 56

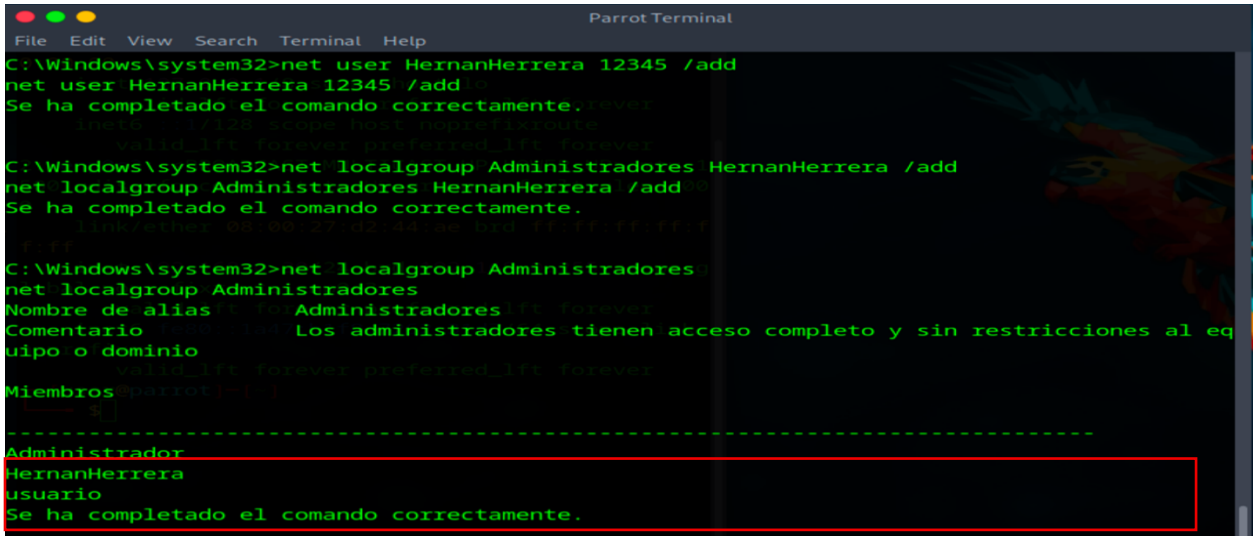
Dirección Ip de la maquina víctima desde Parrot



Fuente. Autoría Propia

Figura 57

Creación de usuarios escalando privilegios



Nota. Claramente se observa que atreves del software Rejetto v2.3 con exploit, se permite el

acceso a través del puerto :80, y hay una seguridad de privacidad, y una filtración de los datos de la organización según el anexo 4 escenario 3, al estar abierto el puerto :80 se puede ejecutar un ataque exitoso. Se logra ejecutar una la explotación de la vulnerabilidad creando un usuario con privilegios de grupo administrativo local con el siguiente nombre del estudiante: HERNAN y primer apellido: HERRERA, con esto se resume que hay fallas en la seguridad informática de la empresa y es importante que los altos ejecutivos tomen acción junto al aérea de seguridad.

Etapa 4: Contención ante Incidentes de Seguridad

De manera individual usted deberá leer el problema que se encuentra en el anexo 5 escenario 4 referente a equipo Blueteam y por medio del banco de trabajo configurado en la actividad anterior deberá dar respuesta a las siguientes preguntas orientadoras:

A continuación se plasmara una matriz de trazabilidad con el objetivo de tener presente las evidencias actuales identificadas en el laboratorio de la fase 3, y así fortalecer la conexión entre acciones propuestas y vulnerabilidades.

Tabla 4

Matriz de Trazabilidad

Hallazgo (Fase 3)	Evidencia (laboratorio)	Impacto observado (ataque ejecutado)	Acción propuesta (contención/mitigación)	Cómo corta la cadena del ataque
Servicio vulnerable HFS/Rejett	Identificación del servicio en	Acceso inicial mediante	Bloqueo inmediato de 80/tcp desde redes no autorizadas (NGFW/ACL).	Evita el vector de entrada y

Hallazgo (Fase 3)	Evidencia (laboratorio)	Impacto observado (ataque ejecutado)	Acción propuesta (contención/mitigación)	Cómo corta la cadena del ataque
o 2.3 expuesto por 80/tcp	escaneo (HTTP File Server 2.3)	explotación (RCE) y obtención de sesión remota	Retiro del servicio o actualización/migración. WAF/reverse proxy si es requerido	la ejecución remota inicial
Ejecución remota y persistencia local tras explotación	Sesión tipo Meterpreter/ejecución de payload	Permite control del host, descarga de herramientas y persistencia	Aislamiento del endpoint (EDR “network isolation”) + bloqueo de hashes/IoCs + kill de procesos maliciosos	Detiene la sesión activa y evita que el host sea plataforma de post-explotación
Escalada de privilegios a SYSTEM	Comando/acción tipo “getsystem”	Permite acciones administrati	Revocación de tokens/sesiones, revisión de privilegios, hardening local,	Reduce impacto y evita

Hallazgo (Fase 3)	Evidencia (laboratorio)	Impacto observado (ataque ejecutado)	Acción propuesta (contención/mitigación)	Cómo corta la cadena del ataque
		vas (cambios de configuración, cuentas)	reglas EDR para detección de técnicas de elevación	cambios persistentes de alto privilegio
Creación de usuario administrador(persistencia)	Alta de usuario y pertenencia a grupo admin	Mantiene acceso aun si se cierra la sesión inicial	Deshabilitar/bloquear cuenta sospechosa, rotación de credenciales, auditoría de cuentas y grupos privilegiados	Elimina persistencia basada en cuentas y corta reingresos
Pivoting habilitado por IP forwarding + rutas	IPEnableRouter=1 y rutas hacia 10.10.10.0/24	Movimiento lateral hacia red interna “oculta”	Deshabilitar IP forwarding, ACL intersegmento, control de rutas, segmentación/microsegmentación	Corta el movimiento lateral y el alcance

Hallazgo (Fase 3)	Evidencia (laboratorio)	Impacto observado (ataque ejecutado)	Acción propuesta (contención/mitigación)	Cómo corta la cadena del ataque
				del atacante
Exposición de RDP 3389/tcp en host interno	Puerto 3389 abierto	Riesgo de acceso remoto no autorizado y escalamiento lateral	Bloqueo 3389 desde segmentos no autorizados, acceso vía VPN + MFA, bastion/jump server, políticas de lockout	Reduce superficie de ataque y limita vectores de lateralidad

Nota. La figura resume los hallazgos durante el escenario de ataque. La evidencia obtenida en laboratorios, el impacto generado y las acciones de contención y mitigación tomadas demuestran cómo las medidas de seguridad implementadas interrumpen la cadena de ataque y reducen el impacto.

¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Al detectar un ataque en tiempo real, lo primero que hay que hacer no es actuar por

impulso, sino confirmar, contener y comprender. En ciberseguridad, una acción inicial atroz puede destruir la evidencia, interrumpir las operaciones e incluso actuar a favor del atacante.

Primer paso: La validación inmediata del ataque, es importante corroborar que si efectivamente se trate de una vulneración del sistema en tiempo real, basándonos en indicadores de compromiso.

- Conexiones inusuales (RDP, SMB, Powershell remota, reverse shells).
- Procesos que sean desconocidos en cmd.exe lanzando *powershell.exe, wscript.exe*
- Puertos abiertos sin autorización (80, 443, 4444, 3389, etc.).
- Actividad irregular de elevación de permisos hacia direcciones no autorizadas.

También es muy importante tener presente el tema de Logs críticos como:

- Registros EDR / SIEM
- Alertas de Firewall
- Windows Event Logs (Security, System, PowerShell, Sysmon).

Segundo paso: Contención inmediata del ataque, pero muy importante no se debe destruir la evidencia. Para este paso se procede aislar el host de la red:

- Switch deshabilitar puerto físico
- EDR aislar el equipo de la red
- Firewall aquí bloquear Ip de origen – destino

Con los anteriores pasos descritos aislar evita que el atacante pueda moverse lateralmente (pivoting), así mismo que siga exfiltrando datos valiosos, y que mantenga sesiones activas por medio de Meterpreter, reverse shells.

Tercer paso: Identificación del vector de ataque en tiempo real ya que con el ataque

contenido se logra identificar que brechas está aprovechando el atacante. Por medio de la revisión de vectores comunes se puede identificar:

- Servicios expuestos
- Vulnerabilidades conocidas
- Credenciales comprometidas
- Puertos abiertos por la inyección de malware

Cabe resaltar que la comprensión del vector permite saber si el ataque permanece activo, sí hay puertas traseras o si se creó persistencia.

Cuarto paso: Preservación de los datos forenses sin alteración de estas antes de erradicar el malware o suspender los servicios. Para estos procesos más conocidos como volcado de memoria RAM y registros existen herramientas muy completas que brindan información verídica:

- FKT Imager
- Volatility
- Magnet RAM Capture

Registros

- Event Logs
- SRUM
- Historial de PowerShell

La RAM contiene shells activos, payloads, claves de cifrado y conexiones. Perderla significa perder al atacante.

Quinto paso: Erradicación y recuperación controlada en este apartado se incluye:

- Parches actualizados
- Cerrar el vector vulnerado

- Revocar credenciales
- Realizar una restauración de la maquina a un punto seguro

Sexto paso: Documentación necesaria de cada paso ejecutado

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team, qué medidas de hardenización propondría para que el ataque no se repita?

El ataque realizado en el laboratorio fue exitoso debido a una combinación de fallos críticos:

- Uso de un SO obsoleto (Windows 7).
- Servicio vulnerable (HFS 2.3) expuesto en el puerto 80.
- Firewall mal configurado permitiendo tráfico no autorizado.
- Falta de segmentación y control en el PIVOT.
- Falta de monitoreo y ausencia de medidas de protección como EDR.
- La mitigación requiere aplicar defensa en profundidad, endureciendo el sistema operativo, los servicios, la red y los controles de acceso.

Para evitar que se vuelva a repetir un ataque se propone las siguientes medidas de hardenización:

- Remplazar Windows 7 ya que es un sistema sin soporte
- Configuración de Firewall con reglas estrictas donde se permitan puertos necesarios
- Establecer el principio de mínimo privilegio esto quiere decir que se debe evitar la ejecución de servicios como administrador o system
- Prohibición de aplicaciones no autorizadas
- Establecer segmentación de la red
- Eliminación de IP Forwarding en el PIVOT
- Establecer ACLs robustas en switches y routers

- Implementación de un EDR
- Control robusto de usuarios y privilegios por medio de la implementación MFA
- Monitoreo, alertas y SIEM

¿Describa con sus palabras las diferencias entre un equipo BlueTeam y un equipo de respuesta a incidentes informáticos?

Funciones del equipo BlueTeam:

- Fortificación del sistema y del servidor (endurecimiento).
- Configuración de cortafuegos, EDR, antivirus y controles de seguridad.
- Implementación de políticas de seguridad y gestión de acceso (IAM).
- Monitoreo de red en tiempo real (SOC, SIEM).
- Detección temprana de amenazas.
- Llevar a cabo auditorías internas, escaneos de vulnerabilidad y evaluaciones de riesgos.
- Documentar y revisar el marco de ciberseguridad.

Funciones del equipo de respuesta a incidentes informáticos:

- Determinar si un incidente es real (triaje).
- Detener la incursión (aislar dispositivos, cuentas de usuario, sesiones de eliminación, etc.).
- Elimine cualquier malware persistente o acceso no autorizado.
- Examine la RAM, las unidades de disco y los registros para la ciencia forense digital.
- Establecer el vector de ataque y la contención.
- Gestionar la coordinación interna (y, para casos graves, externa legal o ejecutiva).
- Restablecer los servicios y restaurar la continuidad del negocio.
- Realizar informes posteriores a incidentes.

Tabla 5

Diferencias BlueTeam y Equipo de Respuesta a Incidentes

BlueTeam	**Equipo de Respuesta a Incidentes**
Preventivo - Proactivo	Reactivo - Correctivo
Continuo Trabajo 24/7	Presente en incidentes confirmados
Protege y endurece la infraestructura	Contiene, erradica y analiza incidentes
Monitoreo, hardening	Forense, contención, y recuperación
Evita que ocurra los eventos	Actúa cuando se presente el ataque
Análisis de vulnerabilidades	Aísla las máquinas y se encarga de una respuesta rápida

Nota. La figura muestra las diferencias entre un enfoque preventivo y proactivo (Blue Team) y uno reactivo y correctivo (equipo de respuesta a incidentes).

¿Si dentro de un equipo BlueTeam le indican que debe trabajar con CIS "Center For Internet Security", usted lo utilizaría para qué fin?

El CIS (Centro de Seguridad en Internet) es una de las partes más importantes de cualquier BlueTeam porque proporciona estándares probados, guías y configuraciones de seguridad para la protección de sistemas y redes. Lo utilizaría con el propósito de aplicar CIS Benchmarks más conocidas como guías de hardening, CIS publica guías técnicas detalladas con el fin de asegurar Windows, Linux, macOS, servidores apache, sql server y servicios en la nube. Adicional sirve para deshabilitar servicios inseguros, configurar permisos correctamente, y endurecer los sistemas de acuerdo con buenas prácticas. Con la ayuda del CIS permitirá al BlueTeam garantizar el cumplimiento de las normativas vigentes, como la ISO 27001, y NIST.

Los CIS controls que son 18 controles críticos que se encargan de cubrir toda la defensa

organizacional:

- Inventario y control de activos
- Gestión de vulnerabilidades
- Configuración segura
- Control de accesos
- Monitoreo continuo
- Protección de datos
- Defensa en profundidad

Explique y redacte las funciones y características principales de lo que es un SIEM.

Es una herramienta de software que permite a las organizaciones identificar, evaluar y responder a las amenazas de seguridad mediante la recopilación y correlación de datos en tiempo real de eventos de seguridad en todo el entorno de TI.

"Los principios fundamentales de todo sistema SIEM son agregar datos relevantes de múltiples fuentes, identificar desviaciones de la norma y tomar las medidas pertinentes. Por ejemplo, al detectar un posible problema, un sistema SIEM puede registrar información adicional, generar una alerta e instruir a otros controles de seguridad para que detengan el progreso de una actividad. Los sistemas SIEM pueden recopilar datos de dispositivos de usuario, servidores, equipos de red, firewalls, programas antivirus y otro software de seguridad." (Gillis & Rosencrance, 2025)

Función

"En su nivel más básico, un sistema SIEM puede basarse en reglas o emplear un motor de

correlación estadística para conectar las entradas del registro de eventos. Su funcionamiento se divide en tres pasos principales: gestión de registros, correlación y análisis de eventos, y monitorización de incidentes y alertas de seguridad.” (Gillis & Rosencrance, 2025)

Características

- Consolidación de datos: Se ocupan de recopilar y supervisar información de aplicaciones, bases de datos, servidores y redes.
- Correlación: Por lo general, en el contexto de la gestión de eventos de seguridad (SEM) dentro de una herramienta SIEM, se conoce como correlación el trabajo de encontrar similitudes entre diferentes sucesos.
- Paneles: Para evitar que eventos críticos se ignoren, los datos se recopilan y consolidan a partir de aplicaciones, bases de datos, redes y servidores; luego se muestran gráficamente para ayudar a identificar patrones.
- Alertas: Si se identifica un incidente de seguridad, las herramientas SIEM pueden notificar a los usuarios.
- Automatización: Algunos programas SIEM pueden incluir la evaluación automática de incidentes de seguridad y las respuestas automatizadas a estos eventos.
- Informes de ejecución: Los informes producidos por herramientas SIEM pueden ayudar a cumplir con los marcos regulatorios.
- Análisis forense y respuesta a incidentes: Las herramientas de SIEM son capaces de documentar cronogramas de incidentes, lo cual simplifica la vigilancia y la reacción ante los sucesos vinculados a la seguridad.
- Vigilancia del acceso a servidores y bases de datos: Los instrumentos SIEM tienen la habilidad de identificar accesos no permitidos y otras anomalías en bases de datos y servidores.

- Identificación de amenazas tanto internas como externas: Las herramientas SIEM pueden detectar amenazas que provengan de dentro o fuera de la entidad.
- Seguimiento en tiempo real: El software SIEM ofrece en tiempo real la supervisión, correlación y análisis de amenazas en diversos sistemas y aplicaciones.
- Supervisión de la actividad del usuario: El programa SIEM es capaz de monitorear la conducta del usuario para detectar comportamientos anormales o incumplimientos.

Defina por lo menos 3 herramientas de contención de ataques informáticos "hardware o software", recuerde que las herramientas de contención son diferentes a las herramientas de detección.

Herramientas Contención:

EDR con funcionalidad de Aislamiento de Red/Contención de Host

- **Acción de Contención:** Poner el host comprometido en aislamiento (manteniendo solo el canal de gestión) que permite finalizar procesos maliciosos y poner en cuarentena artefactos.
- **Justificación con el ataque ejecutado:** Aislar el endpoint después de detectar una sesión remota debido a RCE habría detenido cualquier actividad posterior de explotación (enumeración, descarga de herramientas y escalada de privilegios).
- **Resultado Esperado:** Detención inmediata del progreso, contención del impacto y preservación controlada para análisis forense.

NGFW perimetral e interno para bloqueo de puertos, IPs y IoCs

- **Acción de contención**: Bloqueo inmediato del tráfico que hay en los puertos, o de servicio, se ejecutan líneas de denegación de servicio y control de interdicción con esta herramienta.

- **Justificación con el ataque ejecutado:** El acceso inicial fue concedido por la explotación de un servicio HTTP desprotegido; este cortafuegos de enrutamiento permite un "cierre" inmediato del servicio mientras se aplican parches. Además, con un evidente movimiento lateral hacia la red 10.10.10.0/24, las reglas/ACL internas en inter-VLANs pueden contener el movimiento lateral.
- **Resultado Esperado:** Disrupción del acceso inicial y reducción del alcance lateral (contención a nivel de red).

Contención en capa 2/3 por medio de un Switch gestionable VLAN de cuarentena

- **Acción de contención**: Deshabilitar el puerto del switch en el equipo afectado y trasladarlo a una VLAN de cuarentena o en su defecto denegar la conexión a endpoint.
- **Justificación con el ataque ejecutado:** Si un host actúa como un pivote (por ejemplo, habilitando el reenvío IP y el enrutamiento), la contención más rápida puede ser física/lógica: "apagar el puerto" o poner en cuarentena el dispositivo para cortar la comunicación lateral sin depender del sistema operativo del host.
- **Resultado Esperado:** Definitivamente un aislamiento inmediato del pivot, y un corte del movimiento lateral acompañado de la reducción del riesgo de propagación.

Herramientas Detención

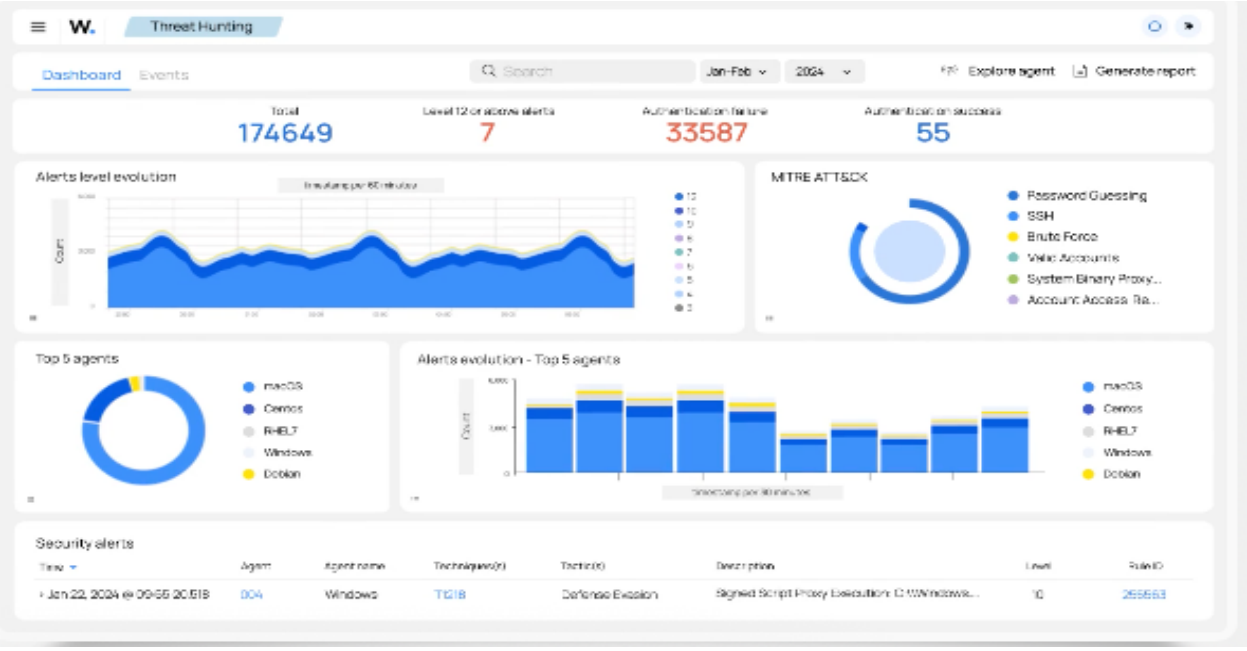
WAZUH

Es una plataforma Open Source de seguridad y monitoreo de infraestructura. Ofrece detección de amenazas, monitoreo de integridad, análisis de logs, y cumplimiento normativo, todo desde una única solución centralizada. Cabe resaltar que es un software que recolecta y analiza logs en Windows, Linux, App con el fin de detectar un comportamiento sospechoso. Este software normalmente está compuesto por un Wazuh Agent en cada equipo el cual se requiere vigilar, y la maquina principal de mando y control se despliega:

- Wazuh server
- Wazuh indexer
- Wazuh dashboard

Figura 58

WAZUH Herramienta de Contención



Nota. Plataforma de ciberseguridad open source para detención, monitoreo y respuesta que tiene la funcionalidad de combinar las capacidades de SIEM.

https://www.imagunet.com/servicio/wazuh/

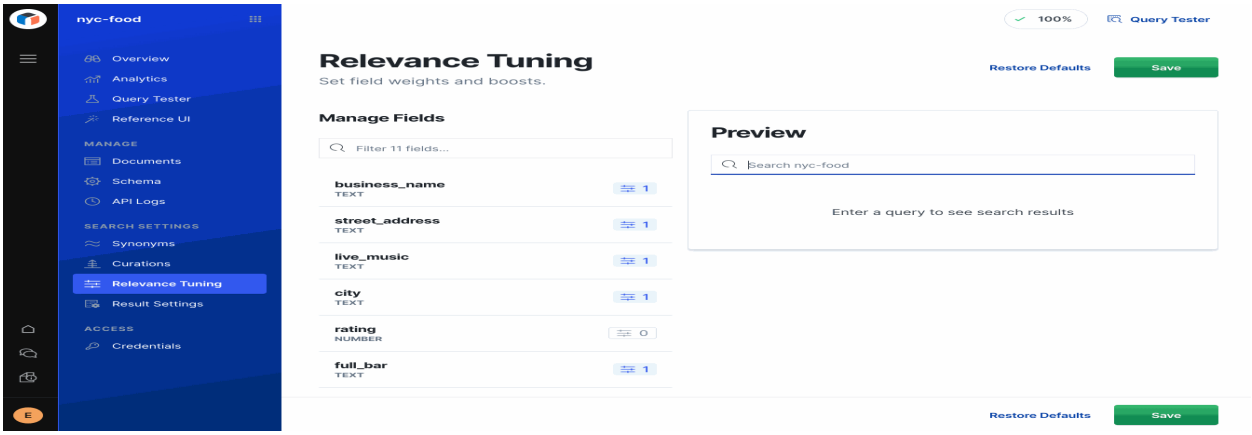
ELASTICSEARCH

"Es un motor de búsqueda y analíticas distribuido open source desarrollado para aplicaciones de velocidad, escalabilidad y AI. Como plataforma de recuperación, almacena datos estructurados, no estructurados y vectoriales en tiempo real, al ofrecer búsquedas híbridas y vectoriales rápidas, impulsar la analítica de seguridad y observabilidad, y habilitar aplicaciones impulsadas por AI con alto rendimiento, precisión y relevancia." (Elastic, s. f.)

Características

"Desde seguridad de nivel empresarial y API fácil de usar para los desarrolladores hasta machine learning y analítica de grafo, el Elastic Stack se envía con características (algunas previamente incluidas como parte de X-Pack) para ayudarte a ingestar, almacenar, analizar, buscar y visualizar todos los tipos de datos a escala." (Elastic, s. f.)

Figura 59 *Software Elastic*

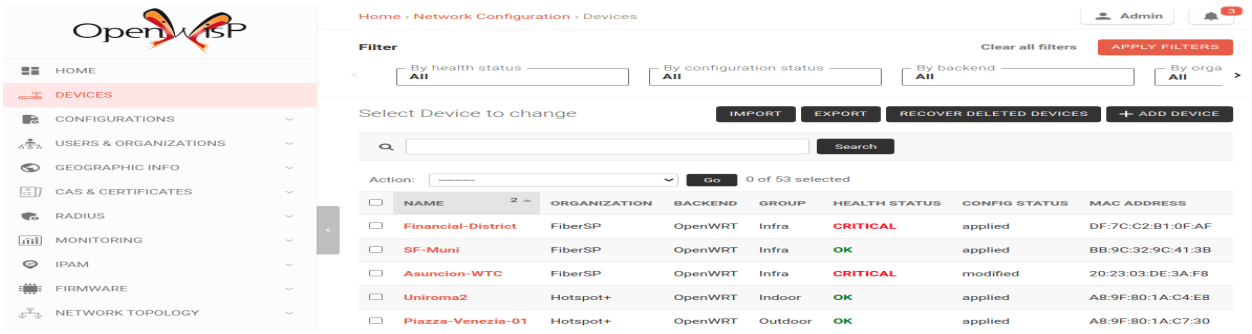


Nota. Plataforma encargada de búsqueda, observabilidad y seguridad basada en el Elastic Stack. https://www.elastic.co/es/blog/elastic-app-search-a-free-product-for-building-great-search-experiences

OPENWIPS

Figura 60

Software Openwips



Nota. Plataforma open source que se dedica a la prevención de intrusiones inalámbricas https://openwisp-org.translate.goog/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Es una solución de código abierto para la implementación, el monitoreo y la administraciones eficientes de redes de TI. Este aplicativo ofrece una gran cantidad de funciones que se componen de distintos módulos con código reutilizable que permite al administrador ayudar para satisfacer aquellas necesidades de administración de la red como:

- Plantillas de configuración
- Aprovisionamiento automático
- Túneles VPN automáticos
- Monitoreo de la red
- Alertas y notificaciones
- Actualizaciones de firmware
- Topología de red
- Puntos de acceso y wifi publico
- Redes de malla

Relación con aspectos legales y éticos

Como parte de sus actividades, el RedTeam y el BlueTeam deben tener en cuenta los siguientes aspectos legales:

Consentimiento informado: Se requiere autorización previa de la organización o del cliente antes de realizar cualquier tipo de prueba de seguridad y/o prueba de penetración

Limitaciones legales: Deben conocer los estatutos aplicables con respecto a las pruebas de seguridad, para no cometer ningún delito.

Protección de datos: Deben conocer la legislación de protección de datos y tener cuidado de no incluir ningún dato personal o confidencial durante las pruebas.

Propiedad intelectual: Tienen que asegurarse de que la organización no tenga sus derechos de propiedad intelectual violados durante la realización de cualquier prueba de intrusión.

Confidencialidad: Con respecto a los detalles de las pruebas de seguridad, especialmente en relación con la información confidencial, no deben revelar la información durante la prueba de seguridad

Responsabilidad: El equipo de profesionales debe asumir el rol con responsabilidad sobre las acciones ejecutadas con el fin de no causar ningún daño a la organización durante el curso de la realización de pruebas de intrusión.

Es muy importante que antes de cualquier movimiento el RedTeam y BlueTeam tengan en claro la actualización de las normatividades vigentes que apliquen, con el fin de ejecutar una satisfactoria prueba en la organización.

Evidencias 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:

Video de sustentación del informe final:

https://youtu.be/s81mNwLzJOQ

Conclusiones

La producción de este informe se destaca la combinación de software obsoleto, configuraciones inseguras y una falta de controles defensivos apropiados que continúa representando un factor crítico que aumenta considerablemente el riesgo de que una infraestructura tecnológica sea comprometida. Específicamente, se confirmó que la exposición de servicios y la falta de segmentación de la red contribuyen al acceso inicial y al movimiento lateral de un atacante dentro del entorno.

Desde la perspectiva del TeamRed, los resultados indican que una infraestructura con debilidades de seguridad básicas permite la ejecución efectiva de ataques controlados, que incluyen, el acceso remoto no privilegiado, la escalada de privilegios y la persistencia. Estos hallazgos subrayan la importancia de adoptar una postura preventiva en lo que respecta a la gestión de vulnerabilidades y el ciclo de vida del software, especialmente con sistemas no mantenidos.

En lo que respecta al TeamBlue, el análisis muestra que la falta de mecanismos de detección y respuesta, como EDR, monitoreo centralizado y segmentación apropiada, amplifica el impacto de los ataques una vez que se ha violado el perímetro de seguridad. Incorporar medidas de endurecimiento, controles de acceso, defensa en profundidad y monitoreo continuo es fundamental para interrumpir la cadena de ataque y limitar el impacto de incidentes potenciales.

Desde el punto de vista ético y jurídico, el trabajo sostiene que las actividades de ciberseguridad tienen que llevarse a cabo en los márgenes de las regulaciones vigentes y los principios de responsabilidad profesional. El consentimiento informado, la protección de los datos personales y el deber de denuncia constituyen bases materiales para asegurar que el

ejercicio de la ciberseguridad no sólo evite la práctica de ilícitos, sino que también no se deriven de los ejercicios prácticos responsabilidades penales o disciplinarias.

Analizando en conjunto el trabajo de los equipos de Red y Blue, se puede afirmar que el dominio técnico de las ciberseguridades no es la única variable que determina la efectividad de las estrategias. La efectividad de las estrategias en estas ciberseguridades también se explica por la existencia de controles organizacionales, normativos y éticos. Se debe entender que para una adecuada reducción de brechas y protección de la información, el ejercicio del profesional debe estar amparado en la responsabilidad ética y el deber de cumplir con las normas en el ámbito de la ciberseguridad.

Recomendaciones

De acuerdo a los hallazgos del análisis técnico y las conclusiones del estudio, se da como recomendación las siguientes sugerencias agrupadas en ejes temáticos con el fin de facilitar su aplicación y comprensión integral.

Técnicas

Se aconseja mantener todos los sistemas operativos y servicios relevantes actualizados con mantenimiento continuo y regular, incluyendo la aplicación de parches de seguridad para limitar las ventanas de exposición a vulnerabilidades conocidas. Además, para mitigar riesgos, se deben implementar medidas de endurecimiento con respecto a los sistemas desactivando características y servicios que no son necesarios y asegurando todas las configuraciones que se dejan en sus valores predeterminados para garantizar que su implementación y configuración no creen problemas de seguridad.

Además, se sugieren mejoras en la segmentación de la red que involucran la implementación de VLANs así como cortafuegos internos para separar los diversos entornos que consisten en usuarios, servidores y servicios críticos, para mitigar los efectos del movimiento lateral causado por intrusiones no autorizadas.

Por último, se recomienda la adopción de soluciones de monitoreo que sean capaces de correlacionar y responder a incidentes de seguridad, como sistemas SIEM o EDR, para garantizar que se detecten comportamientos anormales y puedan responder de manera oportuna.

Organizacionales

Viendo la situación desde una perspectiva organizacional, recomendamos mejorar las políticas internas de seguridad para clarificar y fortalecer el papel, responsabilidades y niveles de acceso de los usuarios especificados y detallados en las políticas internas de seguridad que deben

ser desarrolladas para la organización, incluyendo comunicarlas y actualizarlas de manera regular para asegurar que permanezcan relevantes y actuales.

De igual manera, se sugiere realizar auditorías de seguridad internas y externas con el objetivo de identificar vulnerabilidades adicionales y verificar el cumplimiento de las medidas de protección en torno al sistema.

Legal y contractual

En el lado legal del espectro, es recomendable revisar y editar los contratos que se tienen con los proveedores de servicios tecnológicos, asegurando que contengan disposiciones clave relacionadas con la protección de datos, la confidencialidad y la gestión de incidentes de seguridad.

Además, es vital asegurarse de que se respeten e implementen las regulaciones relacionadas con la protección de datos y la privacidad, con reglas definidas en cuanto al procesamiento, almacenamiento y acceso de los datos sensibles.

Referencias Bibliográficas

AMATAS. (2024, julio 22). Penetration testing phases. AMATAS. https://amatas.com/blog/penetration-testing-phases/

Basic Exploitation with Metasploit: Windows: HTTP File Server, (2021), https://www.youtube.com/watch?v=YQUcyQ4WT6w

Cilleruelo, C. (2024, 31 de julio). ¿Qué es ExploitDB? KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-exploitdb/

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 -– denominado "de la protección de la información y de los datos" – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Congreso de la República de Colombia. (2012, 17 de octubre). Ley Estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales [Ley estatutaria]. Diario Oficial No. 48.587. Recuperada de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Consejo Profesional Nacional de Ingeniería – COPNIA. (s. f.). Código de ética. COPNIA. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CVE Details. (s. f.). CVEdetails.com: CVE security vulnerability database. Security vulnerabilities, exploits, references and more. Recuperado el 5 de diciembre de 2025, de https://www.cvedetails.com/

Elastic. (s. f.). Elasticsearch: el motor oficial de búsqueda y analíticas distribuido. Recuperado el 2 de diciembre de 2025, de https://www.elastic.co/es/elasticsearch

Gillis, A. S., & Rosencrance, L. (2025, 2 julio). What is SIEM (security information and event management)? TechTarget. https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM

Imagunet. (s. f.). Wazuh, ciberseguridad open source de nueva generación. Imagunet. https://www.imagunet.com/servicio/wazuh/

Imperva. (2025). Penetration testing: Step-by-step process & methods. Imperva. https://www.imperva.com/learn/application-security/penetration-testing/

INCIBE-CERT. (2014, octubre 22). Vulnerabilidad en la función findMacroMarker en Rejetto HTTP File Server (CVE-2014-6287). Instituto Nacional de Ciberseguridad (INCIBE). https://www.incibe.es/index.php/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-6287

Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [LEY_1273_2009]. (s/f). Senado de la República de Colombia. Recuperado el 14 de octubre de 2024, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

OpenWISP. (s. f.). Features: OpenWrt controller, RADIUS. OpenWISP. https://openwisp.org/features/

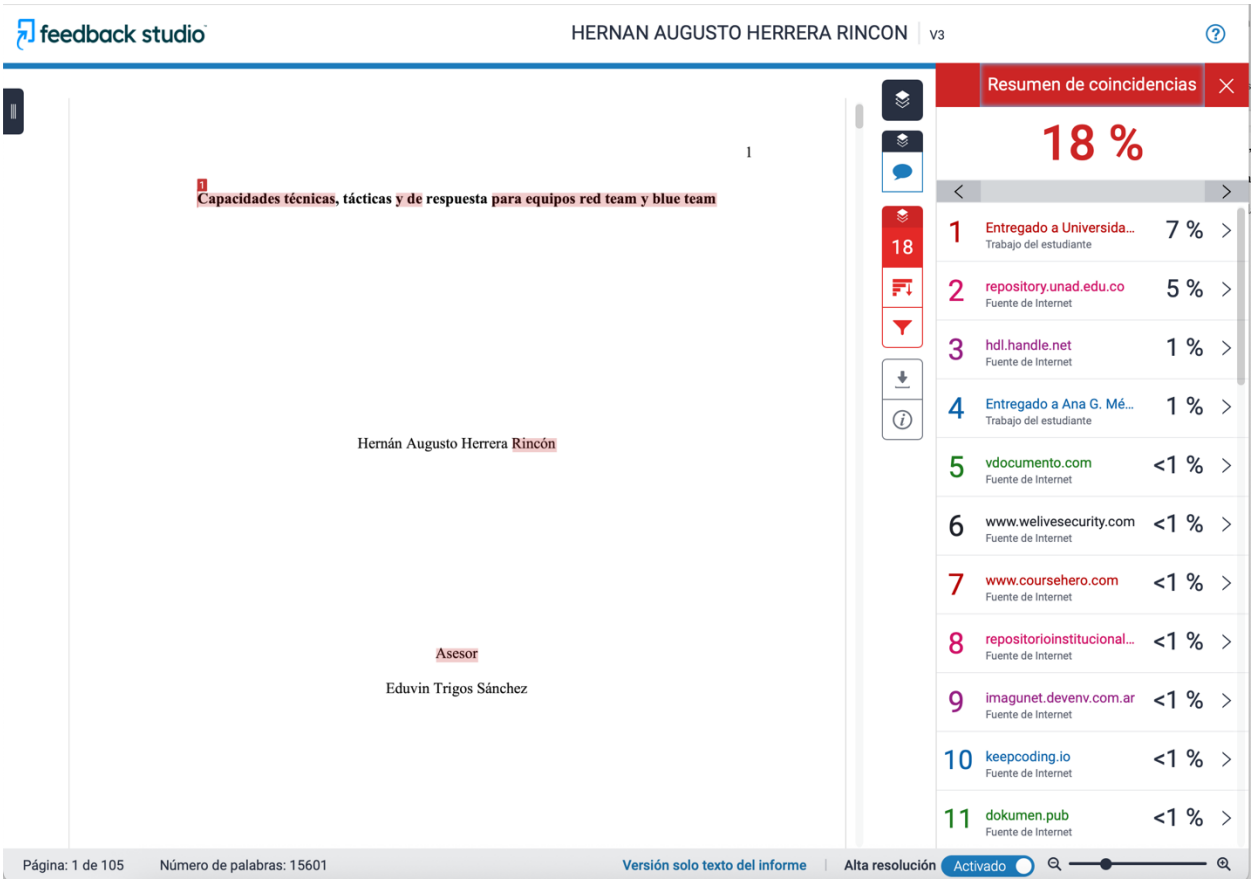
Rapid7. (2012). Metasploitable 2. Metasploit. https://metasploit.help.rapid7.com/docs/metasploitable-2

Rizaldos, H. (2018, 22 octubre). Qué es Metasploit framework. OpenWebinars. https://openwebinars.net/blog/que-es-metasploit/

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Fuente. Autoría Propia