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

Juan Pablo Ayala Ortiz

Asesor

Jenny Fernanda Restrepo Santacruz

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnologías e Ingenierías ECBTI

Especialización en seguridad informática

2025

Resumen

Este informe resume lo que descubrimos durante el seminario especializado en equipos Red Team y Blue Team, donde exploramos de manera ética, legal y técnica diferentes escenarios de ciberseguridad, tanto desde el ataque como desde la defensa. En concreto, nos centramos en la Fase 3 del laboratorio, que se dedicó a detectar y explotar una vulnerabilidad grave en el servicio HTTP File Server (HFS) versión 2.3 de Rejetto.

Con un enfoque práctico y en un entorno controlado, describimos paso a paso cómo se llevó a cabo la explotación, incluyendo cómo se lograron extraer datos sensibles usando técnicas de ataque ofensivo. También explicamos los métodos de ataque utilizados, las herramientas que empleamos y los resultados que obtuvimos, mostrando así las habilidades de los equipos y el impacto que esta vulnerabilidad podría tener en un entorno real.

Por último, el informe subraya lo crucial que es contar con defensas sólidas para reducir riesgos y fortalecer la seguridad de las infraestructuras tecnológicas, haciendo que sean más resistentes frente a posibles ciberataques.

***Palabras clave*:** Ciberseguridad, Exfiltración de Datos, HFS 2.3, Blue Team, Red Team, Vulnerabilidad.

Abstract

This report summarizes what we discovered during the Red Team and Blue Team specialized seminar, where we explored in an ethical, legal and technical way different cybersecurity scenarios, both from the attack and the defense. Specifically, we focused on Phase 3 of the lab, which was dedicated to detecting and exploiting a serious vulnerability in Rejetto's HTTP File Server (HFS) version 2.3 service.

Using a hands-on approach and in a controlled environment, we describe step-by-step how the exploitation was carried out, including how sensitive data was successfully extracted using offensive attack techniques. We also explain the attack methods used, the tools we employed and the results we obtained, thus showing the skills of the teams and the impact this vulnerability could have in a real environment.

Finally, the report underlines how crucial it is to have solid defenses in place to reduce risks and strengthen the security of technological infrastructures, making them more resilient against possible cyber-attacks.

Keywords**:** Cybersecurity, Data Exfiltration, HFS 2.3, Blue Team, Red Team, Vulnerability.

Índice

Tabla de Figuras

Glosario

Blue Team

Grupo responsable de la defensa cibernética de una organización, encargado de detectar, responder y mitigar ataques o intrusiones utilizando un enfoque defensivo.

Ciberseguridad

Es un conjunto de métodos, herramientas y acciones que se usan para proteger equipos, redes y datos contra accesos no permitidos, daños o ciberataques.

Exfiltración de datos

Proceso mediante el cual información sensible o confidencial es extraída de un sistema sin autorización, generalmente por medio de técnicas maliciosas o vulnerabilidades explotadas.

HFS (HTTP File Server)

Software ligero que permite compartir archivos a través de HTTP.

Mitigación

Conjunto de acciones implementadas para reducir la probabilidad que ocurra una amenaza o vulnerabilidad dentro de una red, equipo o sistema informático.

Monitoreo activo

Supervisión constante de redes y sistemas con herramientas automatizadas para detectar comportamientos anómalos, intrusiones o amenazas en tiempo real.

Penetración controlada (Pentesting)

Es una técnica que simula un posible ataque real en contra e un sistema informático, el objetivo principal es el de identificar vulnerabilidades y de evaluar la seguridad de manera ética y legal.

Postura de Ciberseguridad

Nivel general de preparación, resistencia y capacidad de respuesta de una organización frente a amenazas y riesgos cibernéticos.

Red Team

Equipo de profesionales de ciberseguridad encargados de simular ataques reales para evaluar la eficacia de las defensas de una organización, utilizando un enfoque ofensivo.

Vulnerabilidad

Es cualquier debilidad o fallo dentro de un sistema informático el cual puede ser aprovechado por actores maliciosos para comprometer los datos o integridad de los sistemas.

Introducción

En un contexto donde la tecnología es parte esencial de la vida diaria, la ciberseguridad se vuelve fundamental para resguardar la confidencialidad, integridad y disponibilidad de la información. El seminario especializado en equipos Red Team y Blue Team brinda una experiencia formativa integral, combinando teoría con ejercicios prácticos que simulan ataques reales y tácticas defensivas. Más allá de las habilidades técnicas, también impulsa la reflexión sobre los principios éticos y legales que rigen la seguridad digital.

Este informe se centra en los hallazgos obtenidos durante la Fase 3 del laboratorio, donde se identificó y explotó una vulnerabilidad crítica en el servicio HTTP File Server (HFS) versión 2.3 de Rejetto. A través de un entorno controlado, se demostró cómo un atacante podría aprovechar esta falla para acceder a información sensible si no se cuenta con medidas de seguridad adecuadas. Se describen los pasos del ataque, las herramientas empleadas y los riesgos identificados, subrayando la necesidad de contar con defensas proactivas y bien estructuradas para salvaguardar los sistemas digitales.

Objetivos

Objetivo General

Desarrollar un informe técnico que documente de manera clara las actividades realizadas durante el seminario, evidenciando el papel fundamental de las estrategias Red Team & Blue Team en la protección de redes, equipos y sistemas informáticos. También la necesidad de fortalecer continuamente las capacidades técnicas y profesionales de quienes participan en la defensa y evaluación de entornos digitales.

Objetivos Específicos

- Describir las actividades prácticas realizadas durante el curso, mostrando cómo se aplicaron las metodologías dentro de los equipos tanto de Red como de Blue Team dentro de entornos simulados de ciberseguridad.

- Analizar los resultados de los ejercicios de ataque y defensa, evaluando qué técnicas funcionaron mejor y cómo ayudaron a descubrir vulnerabilidades reales en los sistemas.

- Reflexionar sobre la colaboración entre ambos equipos, destacando por qué un enfoque coordinado, ético y proactivo es clave para responder eficazmente a las amenazas.

- Proponer recomendaciones para mejorar tanto las estrategias técnicas como la comunicación y el trabajo en equipo, asegurando que todos los profesionales en Ciberseguridad estén preparados para afrontar desafíos actuales en ciberseguridad.

Desarrollo del Informe

Marco Legal Colombiano

debe tener en cuenta todo el Marco Legal de nuestro pais para empezar con las pruebas de Pentesting y análisis forense, esto garantiza que se actúe bajo los términos de la ley y se alineen los procedimientos con los estandarizados bajo normas tanto locales como internacionales. Dentro de las más importantes en nuestro pais tenemos:

Ley 1273 de 2009: Esta ley introduce cambios al Código Penal y establece un nuevo derecho protegido: la "protección de la información y los datos". Su propósito se centra en tres aspectos fundamentales: salvaguardar la información y los sistemas frente a ataques o delitos informáticos, imponer sanciones a quienes cometan actos como el acceso no autorizado a sistemas, el robo de datos o la distribución de software malicioso, y regular la ciberseguridad y la protección de datos personales en Colombia. Todo esto se desarrolla a través de las siguientes disposiciones clave:

- Acceso abusivo a un sistema informático (Artículo 269A): Penaliza el acceso no autorizado a sistemas informáticos.
- Obstaculización indebida de un sistema informático o red de telecomunicaciones (Artículo 269B): Castiga legalmente a quienes interfieran de manera injustificada con el funcionamiento normal de sistemas informáticos o redes, afectando su disponibilidad o rendimiento.
- Interceptación de datos (Artículo 269C): Se penaliza toda interceptación no autorizada o sin consentimiento de datos desde orígenes informáticos.

- Daño a un Activo Informático (Artículo 269D): Penaliza toda destrucción, daño, borrado, deterioro, alteración o eliminación de datos en un dispositivo informático.
- Uso de software malicioso (Artículo 269E): Penaliza la producción, tráfico, adquisición, distribución, venta, envío, introducción o extracción de software malicioso.
- Violación de datos personales (Artículo 269F): Penaliza la obtención, compilación, sustracción, oferta, venta, intercambio, envío, compra, interceptación, divulgación, modificación o empleo de datos personales sin autorización.
- Suplantación de sitios web para capturar datos personales (Artículo 269G): Penaliza la creación y uso de sitios web falsos para capturar datos personales.
- Circunstancias de agravación punitiva (Artículo 269H): Establece que las penas se aumentarán si la conducta se cometiere bajo ciertas circunstancias agravantes

Ley 1581 de 2012 (Ley de Protección de Datos Personales): Esta ley establece normas para el manejo de datos personales y tiene como objetivo asegurar que cada persona pueda acceder, corregir o actualizar la información que se haya recopilado sobre ella en bases de datos o archivos.

Sus características principales incluyen:

- Principios para el tratamiento de datos: Establece principios como la legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad sobre la información de las personas como son sus nombres, direcciones, número de teléfono, datos financieros Etc.
- Derechos de los titulares: Los titulares de los datos tienen derechos como conocer, actualizar, rectificar y eliminar sus datos personales.

- Obligaciones de los responsables del tratamiento: Los responsables del tratamiento de datos deben garantizar la protección de los datos personales y cumplir con las disposiciones legales.

Sanciones: Establece sanciones para quienes incumplan las normas de protección de datos disposiciones en la ley.

Etapas del Pentesting.

Para llevar a cabo unas pruebas exitosas, estas deben estar alineadas a estándares internacionales. Para conocer que etapas se abordarán en las pruebas, es necesario conocer el estándar de ejecución de pruebas PTES el cual se explica a continuación:

Bajo el marco de ejecución de pruebas de penetración (PTES) se ha definido un marco de trabajo con los siguientes pasos y procedimientos para que pueda llevarse a cabo de manera exitosa, efectiva y segura un Pentesting:

Interacciones Previas: En esta etapa se crea tanto la planificación como la definición del alcance de la prueba de penetración. Estableciendo los objetivos, las reglas y los límites que va a tener la prueba.

Recopilación de Información: En esta etapa se realiza la recopilación de información sobre el objetivo. Esto incluye datos sobre la infraestructura, los sistemas, las aplicaciones y los empleados.

Modelado de Amenazas: En esta etapa se plantean y analizan las posibles amenazas que podrían afectar al objetivo definido. Se evalúan los riesgos y se priorizan las vulnerabilidades.

Análisis de Vulnerabilidades: Dentro de esta etapa se realiza la búsqueda y el análisis de todas las vulnerabilidades en el sistema. Se utilizan herramientas para el escaneo y detección de fallos de seguridad y se organiza la viabilidad de explotación de las vulnerabilidades encontradas.

Explotación: Una vez identificadas las vulnerabilidades, se realiza la explotación para comprobar si realmente pueden ser utilizadas para comprometer el sistema y comprobar su nivel de alcance.

Post-Explotación: Después de explotar las vulnerabilidades, se evalúa el impacto en línea con el objetivo planteado y se intenta asegurar el acceso al sistema comprometido. Se recopila información que pueda obtener la fase anterior y establecer el cómo se puede llegar a utilizar.

Reportes: Finalmente, se documentan todos los hallazgos y se elabora un informe de manera detallado el cual incluya todas las vulnerabilidades encontradas, las técnicas que se utilizaron y todas las recomendaciones para mitigar los riesgos encontrados.

Fases para llevar el proceso de Pentesting

Fase de reconocimiento / análisis de vulnerabilidades:

NMap: Es una herramienta gratuita y de código abierto que se usa para explorar redes y revisar su seguridad. Con ella, puedes escanear a fondo los puertos y servicios de un sistema o red, descubriendo qué dispositivos están activos y qué servicios están ofreciendo.

Figura 01

Comando nmap -A <IP> para ejecutar escaneo de puertos en host víctima.

Nota: Elaboración Propia.

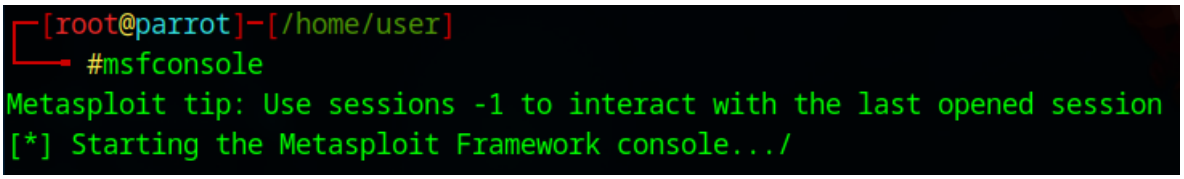
Explotación:

Metasploit: Metasploit es una plataforma muy popular que sirve para crear y lanzar ataques contra sistemas remotos. Proporciona un conjunto de herramientas para ejecutar esos ataques, diseñar Payloads y aprovechar los sistemas que han sido vulnerados.

VERSIÓN: METASPLOIT V6.4.58-DEV

Figura 02

Comando “msfconsole” para ejecutar interfaz de metasploit



Nota: Elaboración Propia.

ExploitDB: Base de datos pública la cual cuenta con amplia información sobre exploits y vulnerabilidades públicamente conocidas, incluyendo detalles y descripciones. Es un recurso clave para Pentesters, ofreciendo exploits específicos y datos sobre vulnerabilidades, como CVE y requisitos para explotarlas.

Figura 03

Pagina Exploit Database donde documentarse sobre Exploits

EXPLOIT DATABASE

Date	D	A	V	Title	Type	Platform
2021-02-23	⬇		✕	HFS (HTTP File Server) 2.3.x - Remote Command Execution (3)	Remote	Windows
2020-06-10	⬇		✕	HFS Http File Server 2.3m Build 300 - Buffer Overflow (PoC)	Remote	Multiple
2016-01-04	⬇	⬇	✓	Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)	Remote	Windows
2015-08-27	⬇	⬇	✓	FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution	Remote	Windows
2011-03-21	⬇		✓	Apple Mac OSX 10.6.x - HFS Subsystem Information Disclosure	Local	OSX

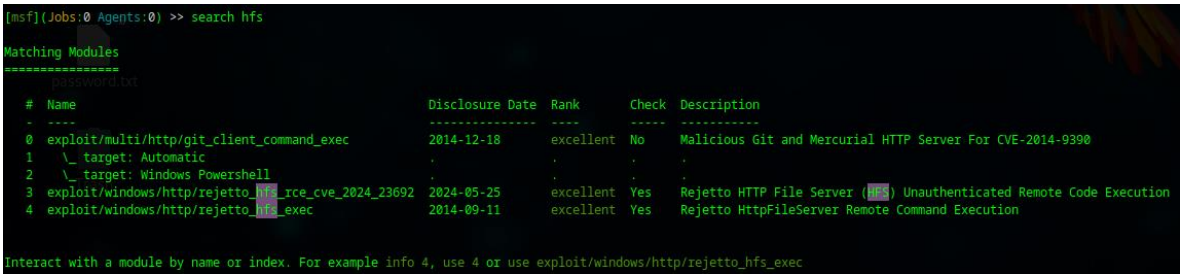
Nota: Elaboración Propia.

Post-Explotación:

Payloads: es el código malicioso que se activa tras explotar una vulnerabilidad, diseñado para ejecutar acciones específicas en un sistema comprometido, como establecer conexiones remotas (shell inversos), ejecutar comandos con privilegios elevados o instalar malware persistente (rootkits). Su complejidad varía desde funciones básicas hasta técnicas avanzadas de evasión.

Figura 04

Comando “Search” para búsqueda de Exploits y Payloads

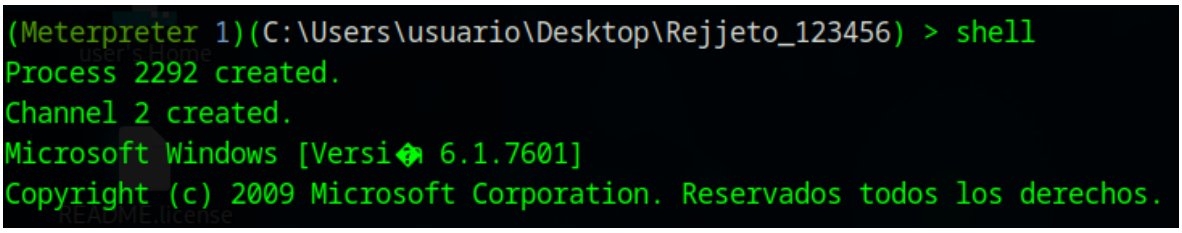


Nota: Elaboración Propia.

Webshell: Un web shell es un script malicioso que se introduce en un servidor web vulnerado, habilitando al atacante para ejecutar comandos en el servidor mediante una interfaz web. Es una herramienta frecuente en ataques contra aplicaciones web y servidores con deficiente protección.

Figura 05

Comando “shell” para ejecutar comandos de sistema en Windows.



Nota: Elaboración Propia.

Rejetto HFS: Rejjeto HFS es un servidor HTTP diseñado para compartir archivos de forma simple y rápida. Sin embargo, puede ser explotado por atacantes para cargar archivos maliciosos, como scripts o malware, en sistemas comprometidos a través de su interfaz web. Como HTTP File Server (HFS), esta herramienta puede servir como un medio para transferir Payloads.

Figura 06

Version de Rejjeto HFS 2.3 la cual es vulnerable

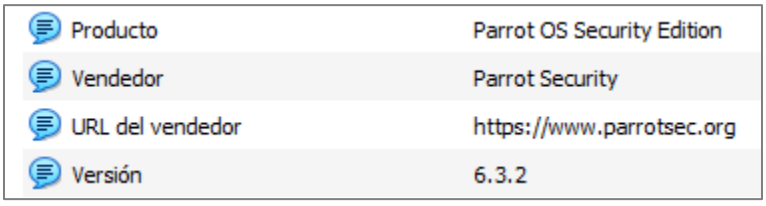
Nota: Elaboración Propia.

Análisis Forense / Documentación:

Parrot OS: Distribución del sistema operativo Linux que fue creada específicamente para pruebas de Ethical Hacker o Pentesting, análisis forense y actividades relacionadas a la ciberseguridad. Este sistema contiene una amplia colección de herramientas de ciberseguridad ya instaladas, estas son ideales para auditar tanto redes, aplicaciones, como sistemas informáticos.

Figura 07

Nombre del Sistema operativo Parrot OS y versión.

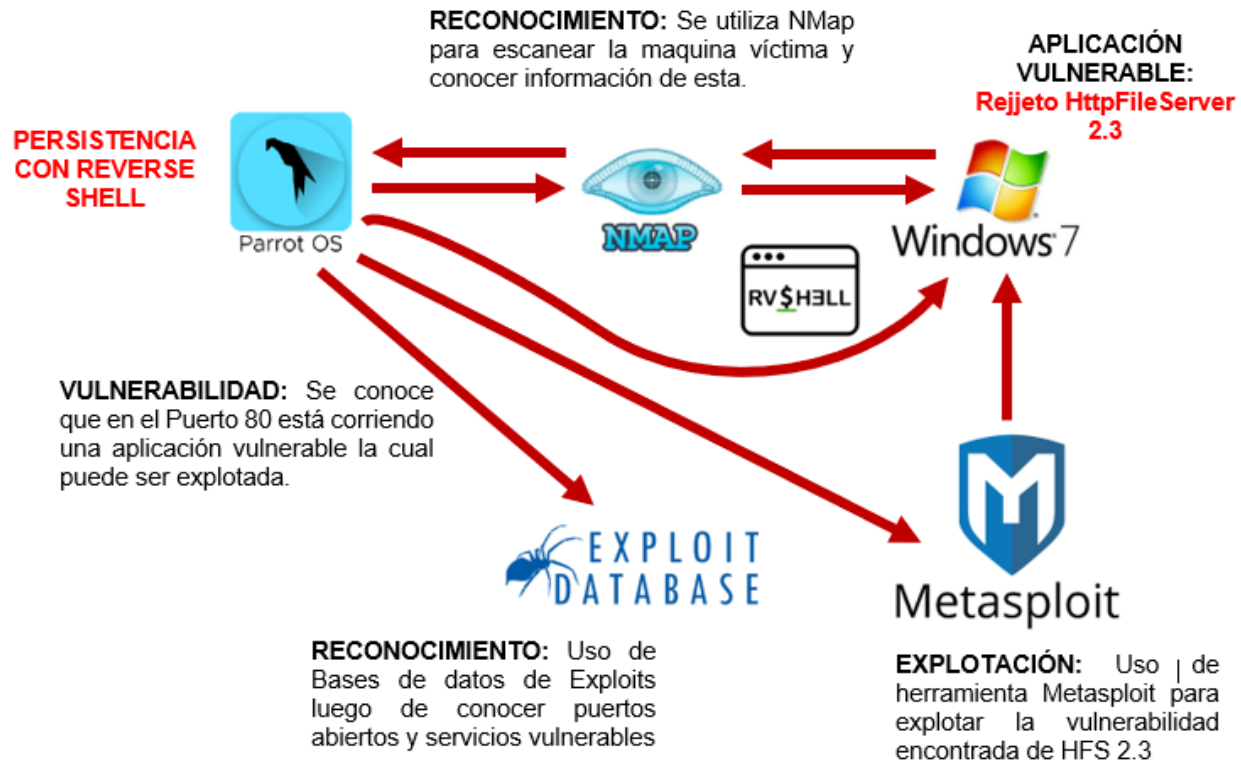


Nota: Elaboración Propia.

Grafica De Explicación Del Ataque

Figura 08

Diagrama que explica el ataque a la maquina Windows 7 con Rejjeto Vulnerable

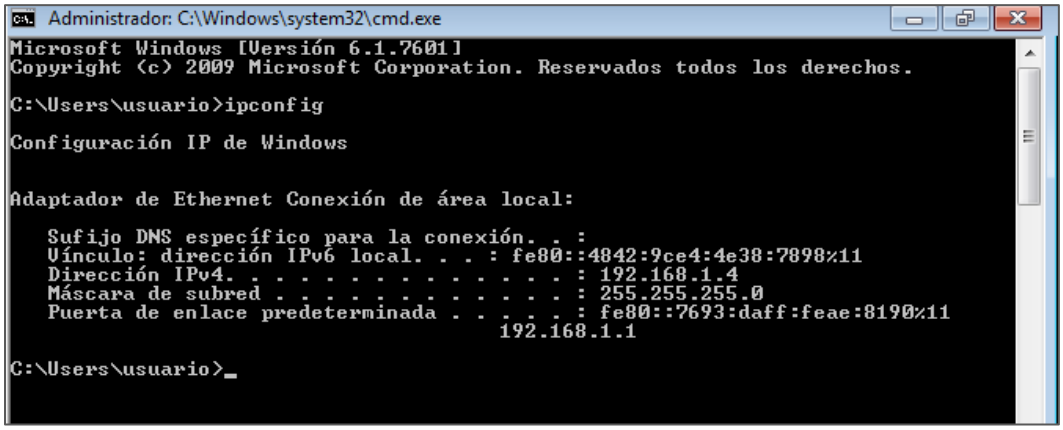


Nota: Elaboración Propia.

Pasos Ejecutados para Explotación de la Maquina Windows 7

Figura 09

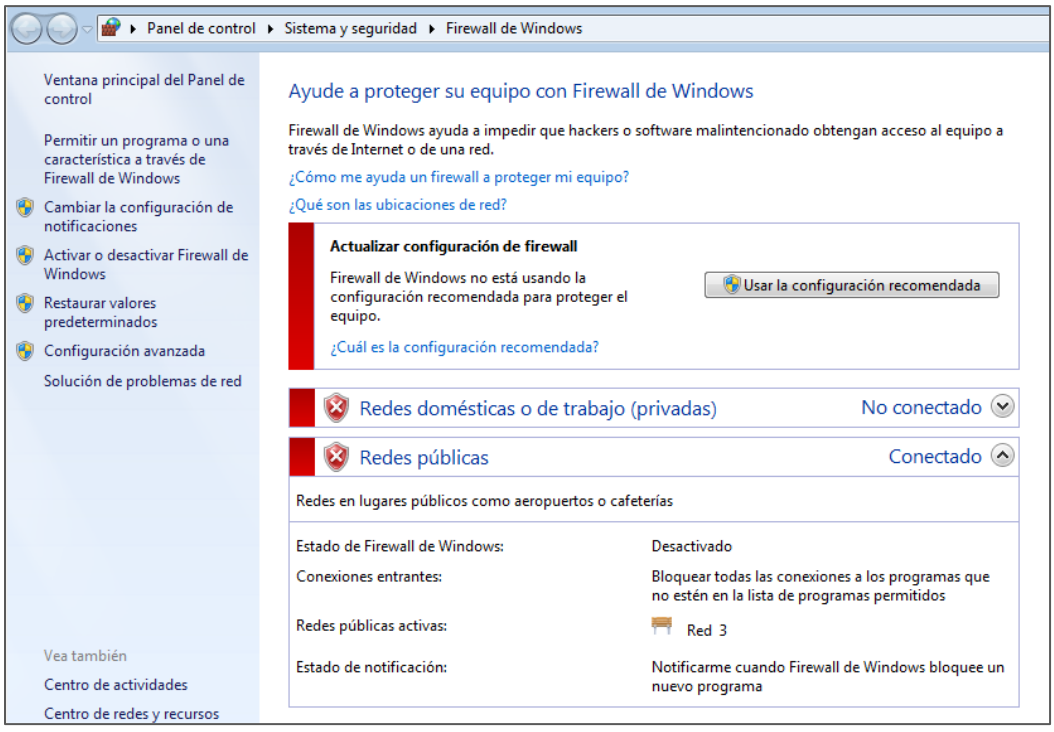
Dirección IP de la maquina víctima con Windows 7



Nota: Elaboración Propia.

Figura 10

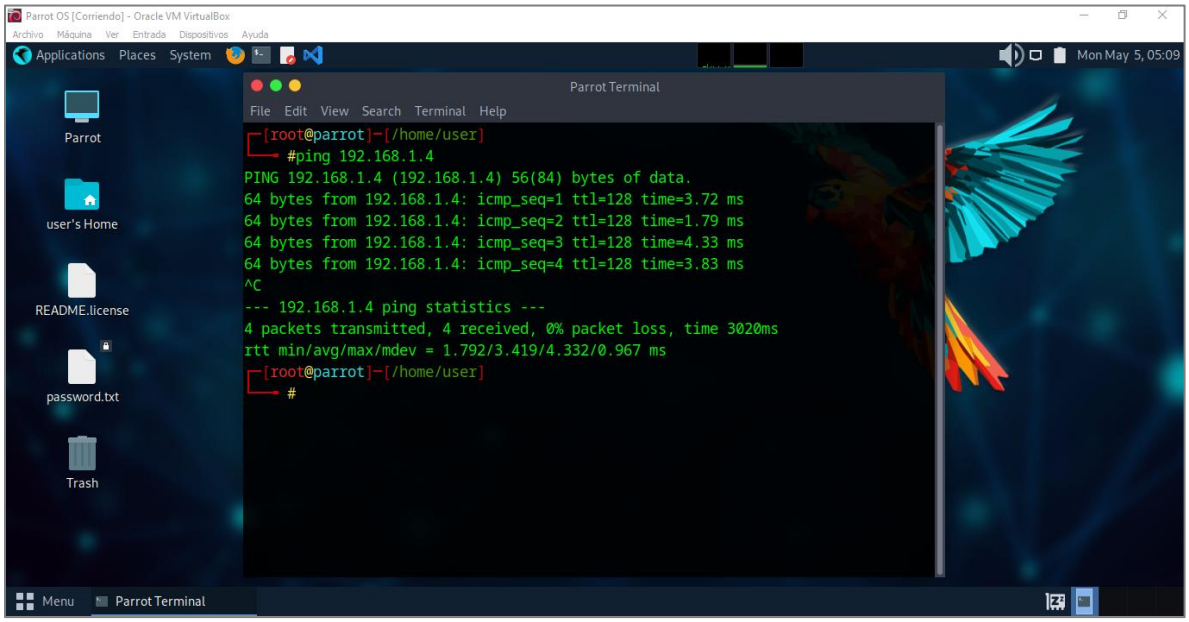
Desactivación de Firewall de la maquina víctima.



Nota: Elaboración Propia.

Figura 11

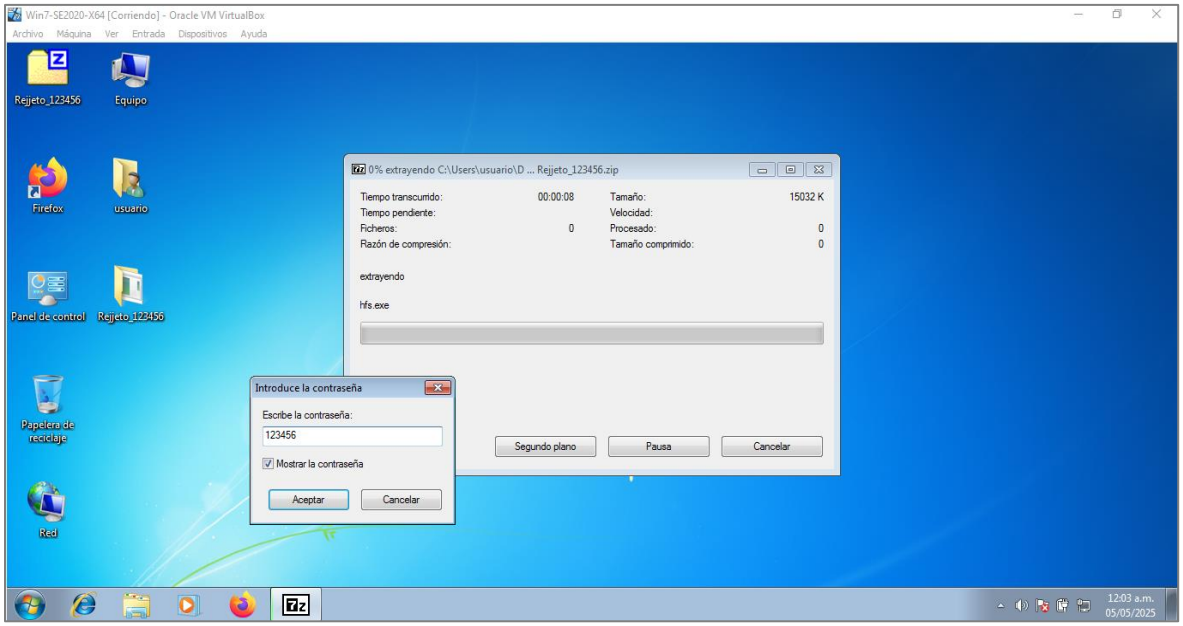
Prueba de Ping exitosa entre las dos maquinas



Nota: Elaboración Propia.

Figura 12

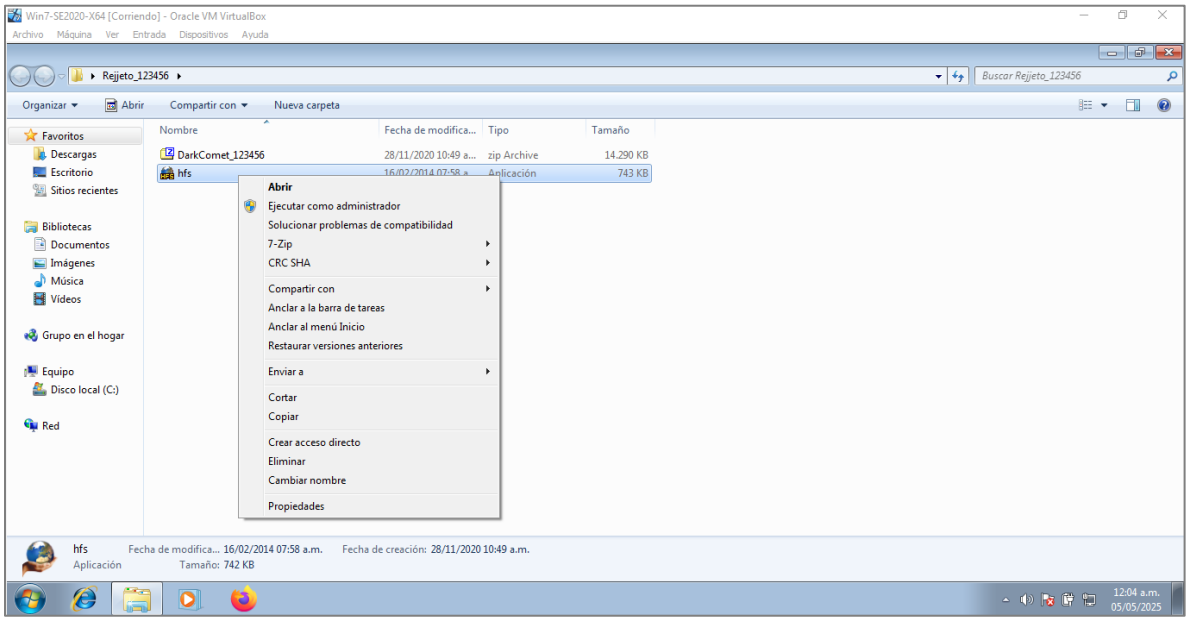
Descompresión de programa Rejjeto para las pruebas de RCE



Nota: Elaboración Propia.

Figura 13

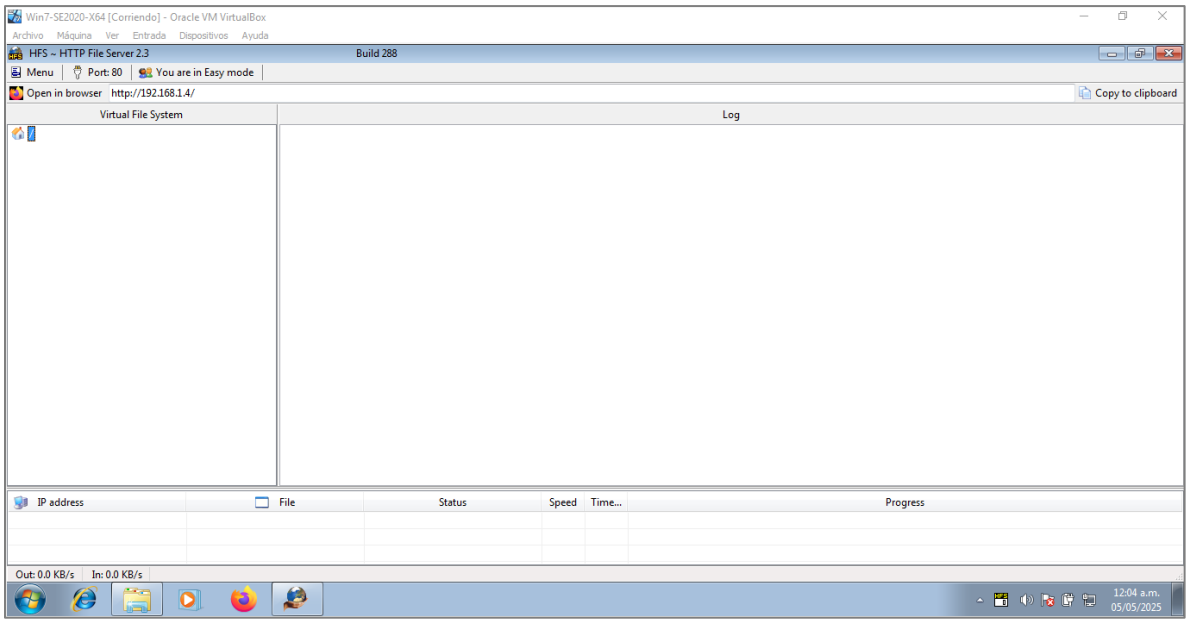
Apertura de Programa Rejjeto para inicio de pruebas.



Nota: Elaboración Propia.

Figura 14

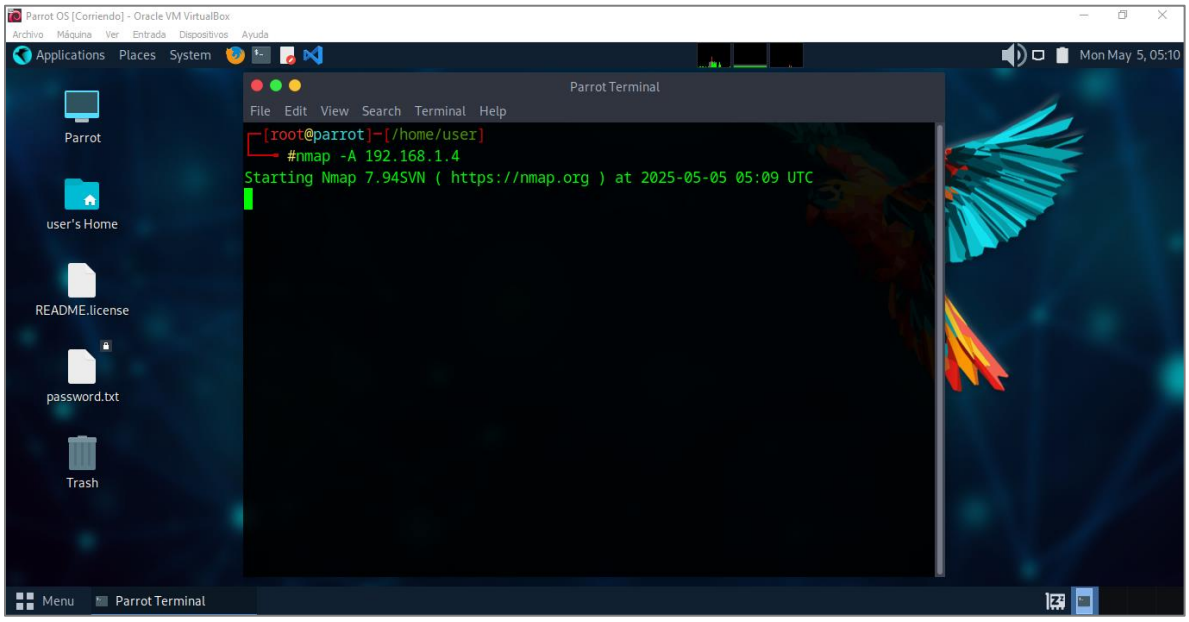
Vista de la interfaz del programa Rejjeto HFS.



Nota: Elaboración Propia.

Figura 15

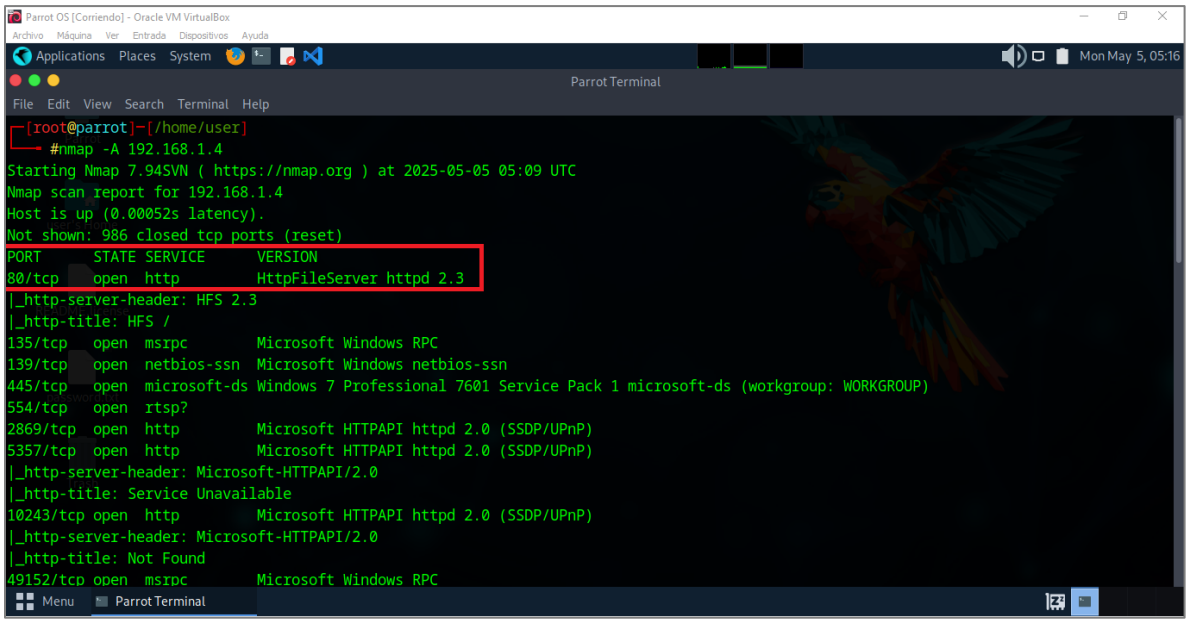
Inicio de Nmap a la IP del host Victima para escaneo de Puertos.



Nota: Elaboración Propia.

Figura 16

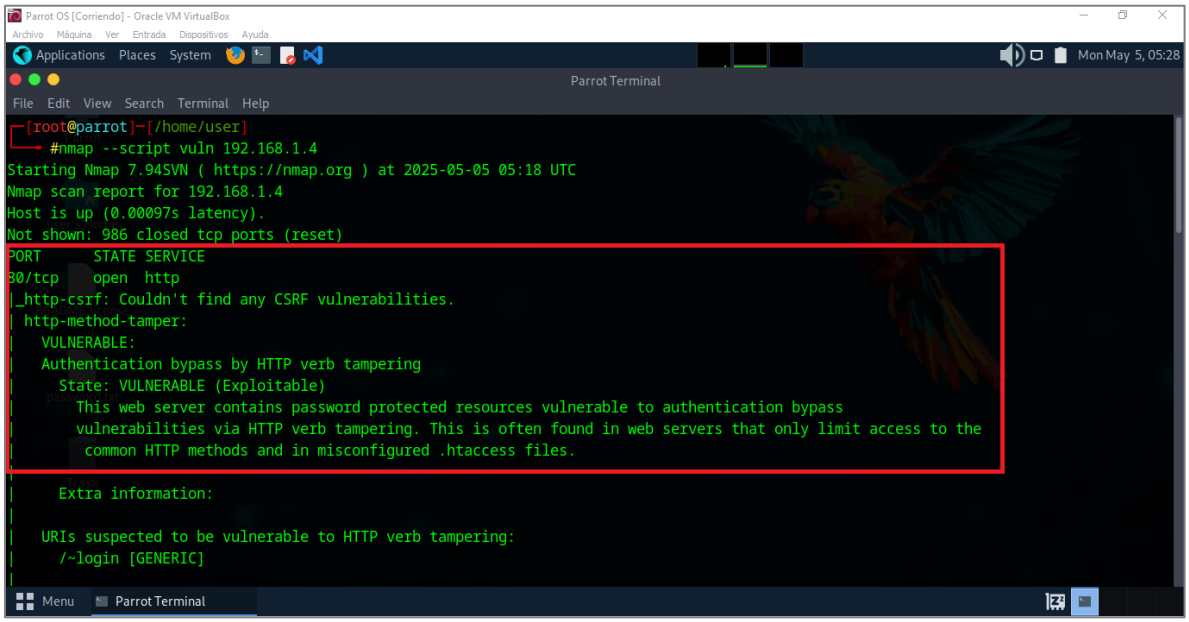
Hallazgo de puerto 80 vulnerable con el servicio HttpFileServer 2.3 corriendo.



Nota: Elaboración Propia.

Figura 17

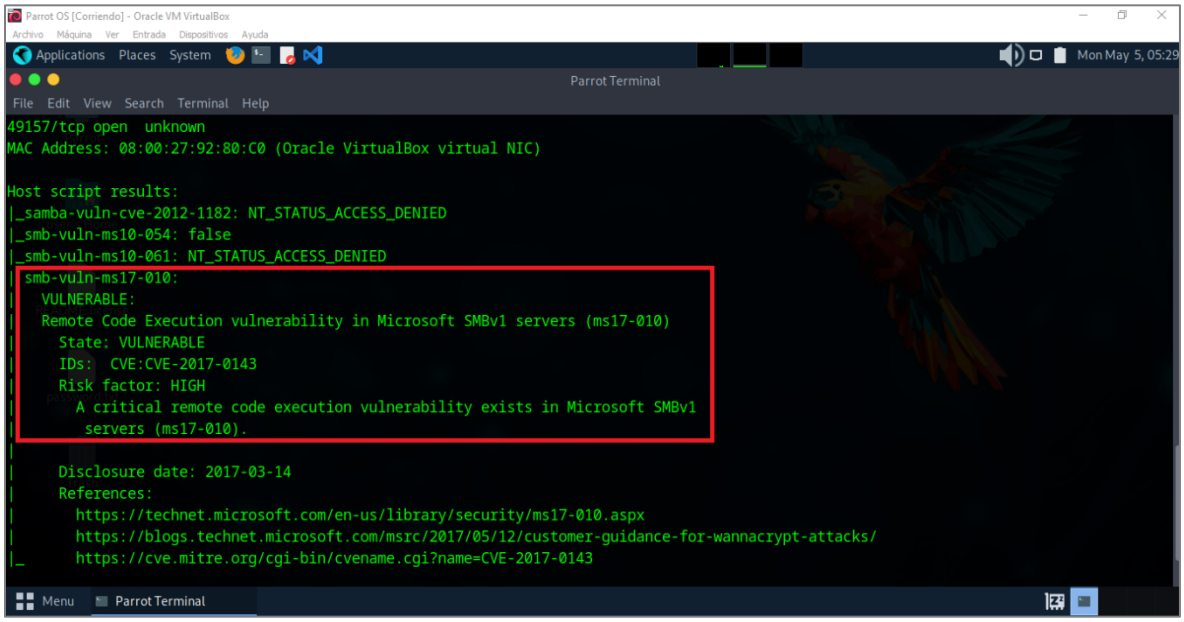
Hallazgo de vulnerabilidad de puerto 80 servicio HttpFileServer 2.3 (Explotable).



Nota: Elaboración Propia.

Figura 18

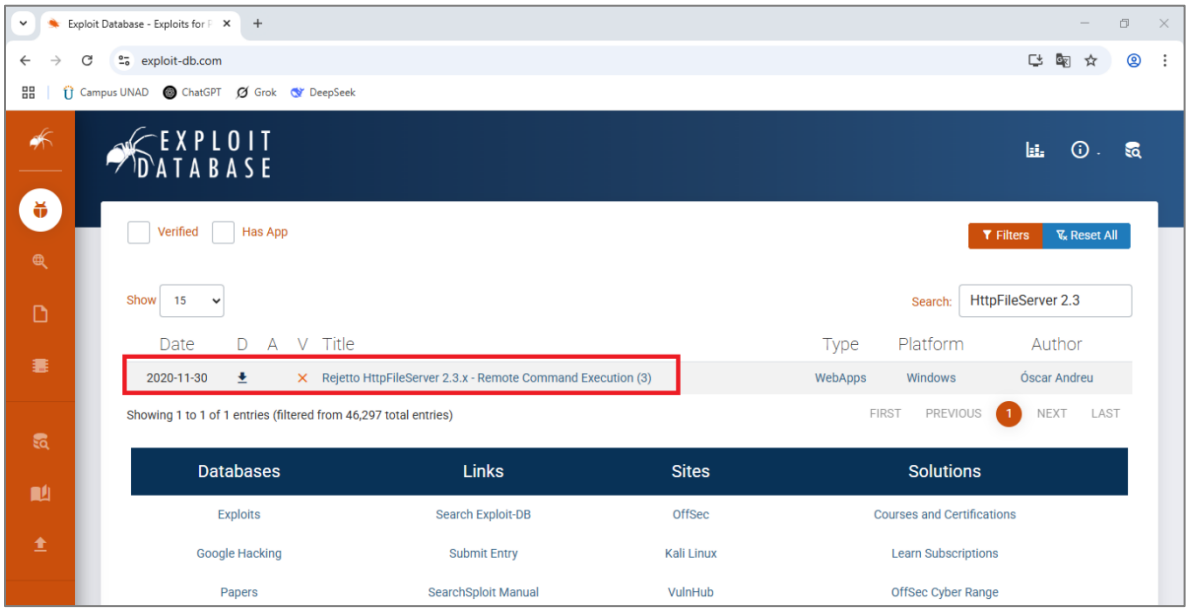
Otra Vulnerabilidad RCW en SMBv1 con CVE-2017-0143



Nota: Elaboración Propia.

Figura 19

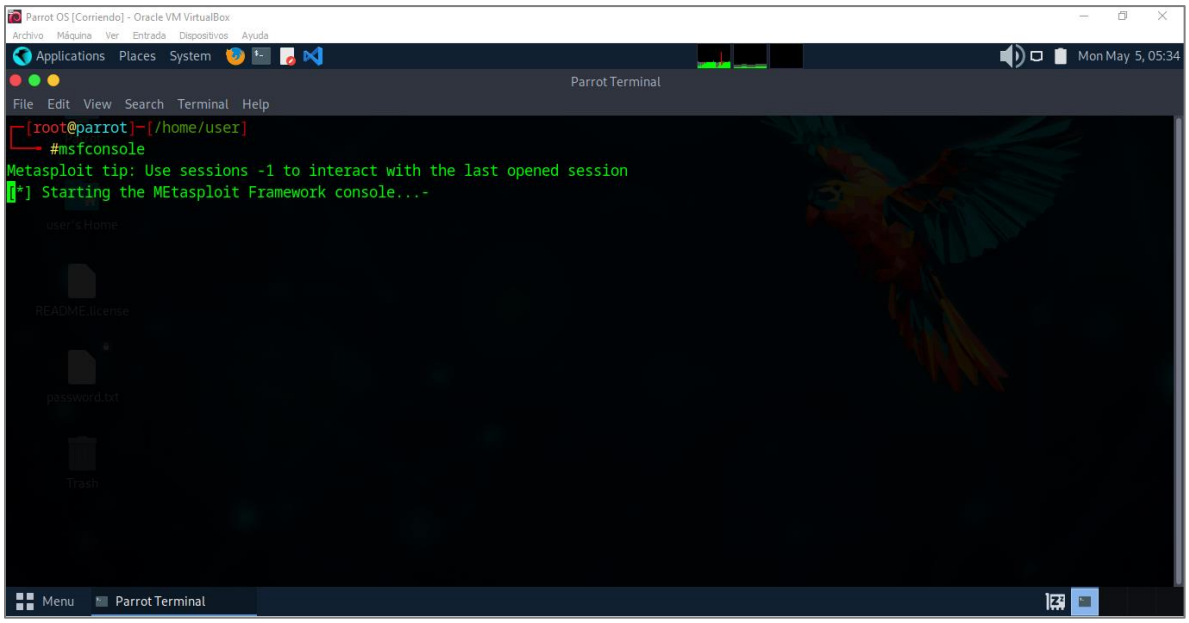
Revisión de base de datos de exploits sobre servicio HttpFileServer 2.3.



Nota: Elaboración Propia.

Figura 20

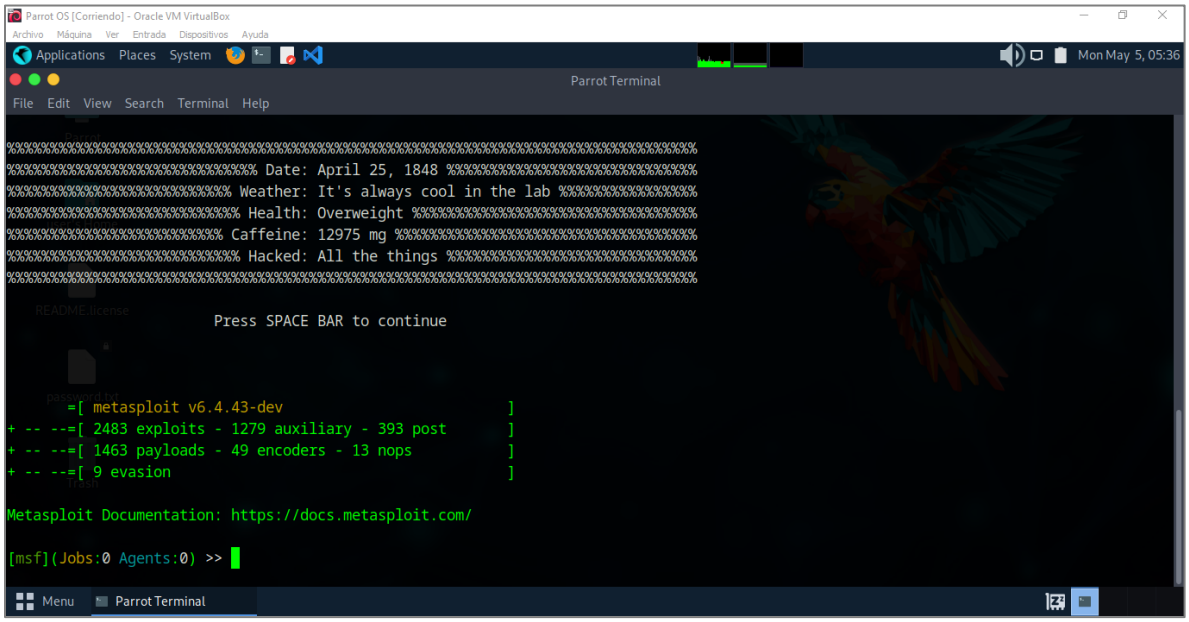
Apertura de herramienta Metasploit para explotación de vulnerabilidad.



Nota: Elaboración Propia.

Figura 21

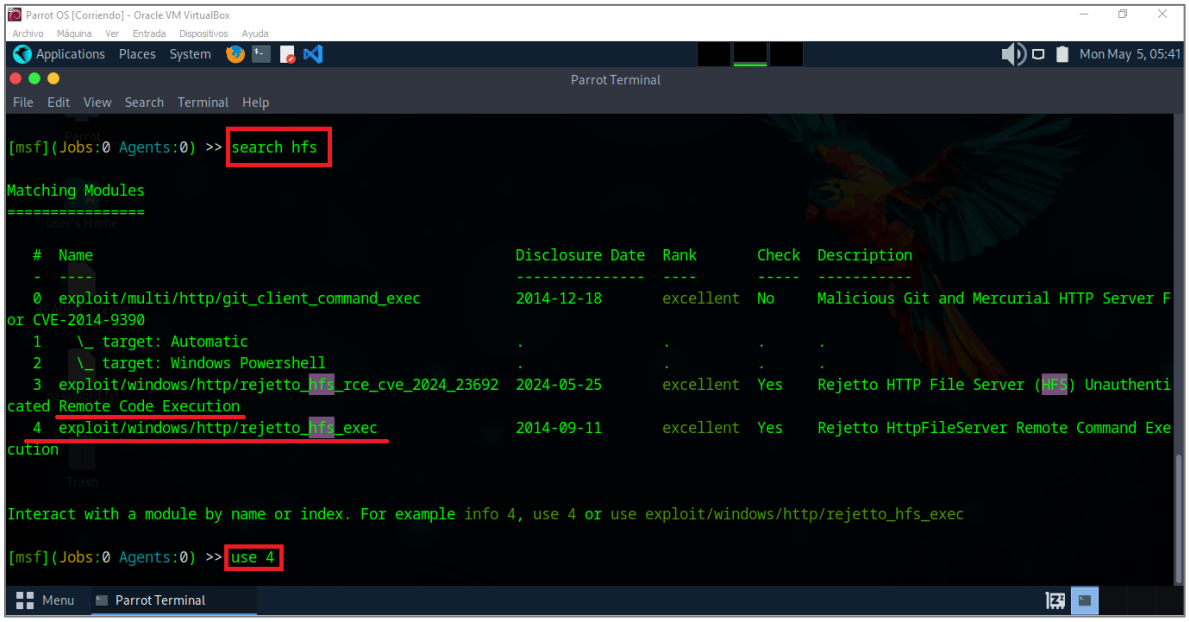
Aplicación Metasploit corriendo.



Nota: Elaboración Propia.

Figura 22

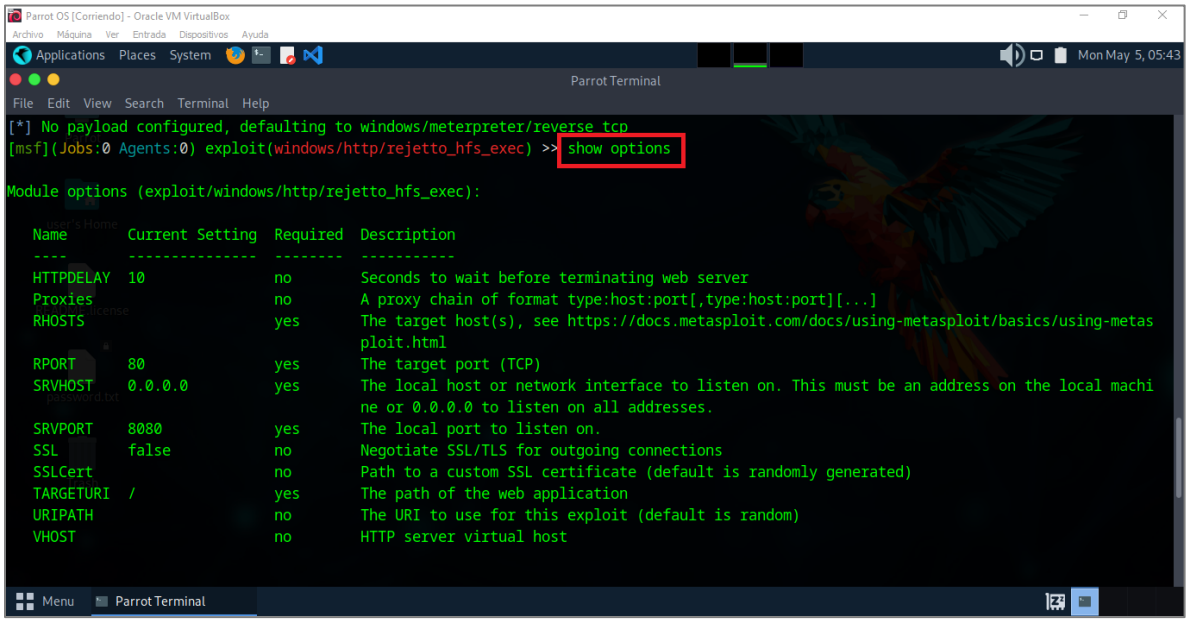
Búsqueda con comando “Search” de exploits para “HFS” y uso de modulo 4.



Nota: Elaboración Propia.

Figura 23

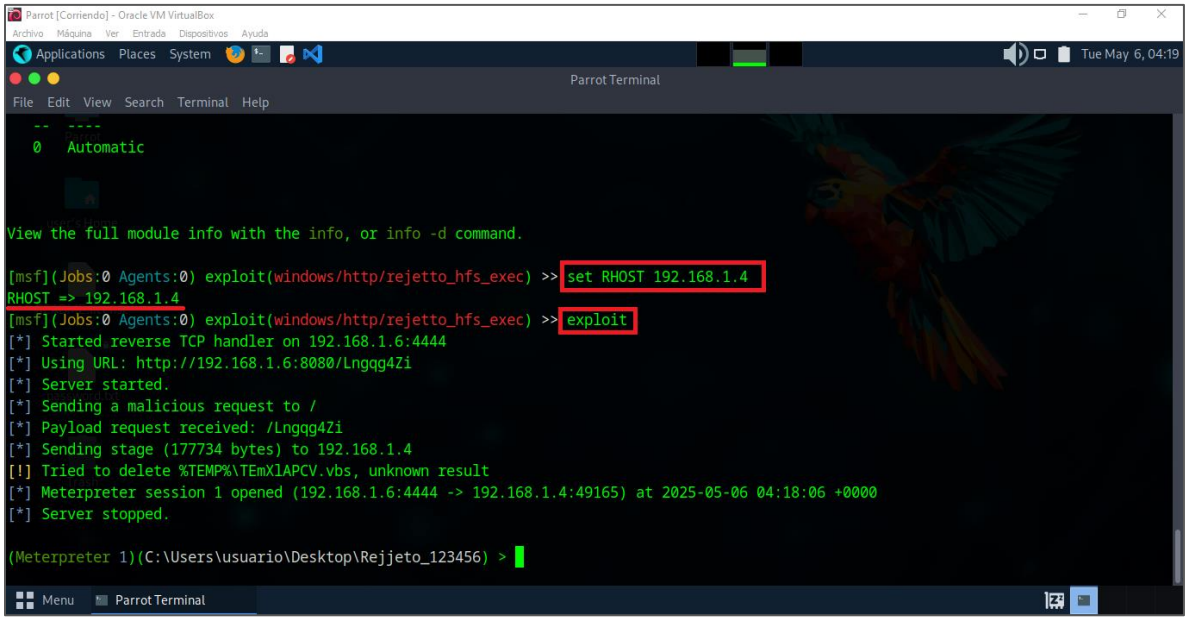
Vista de configuración para establecer parámetros al Exploit.



Nota: Elaboración Propia.

Figura 24

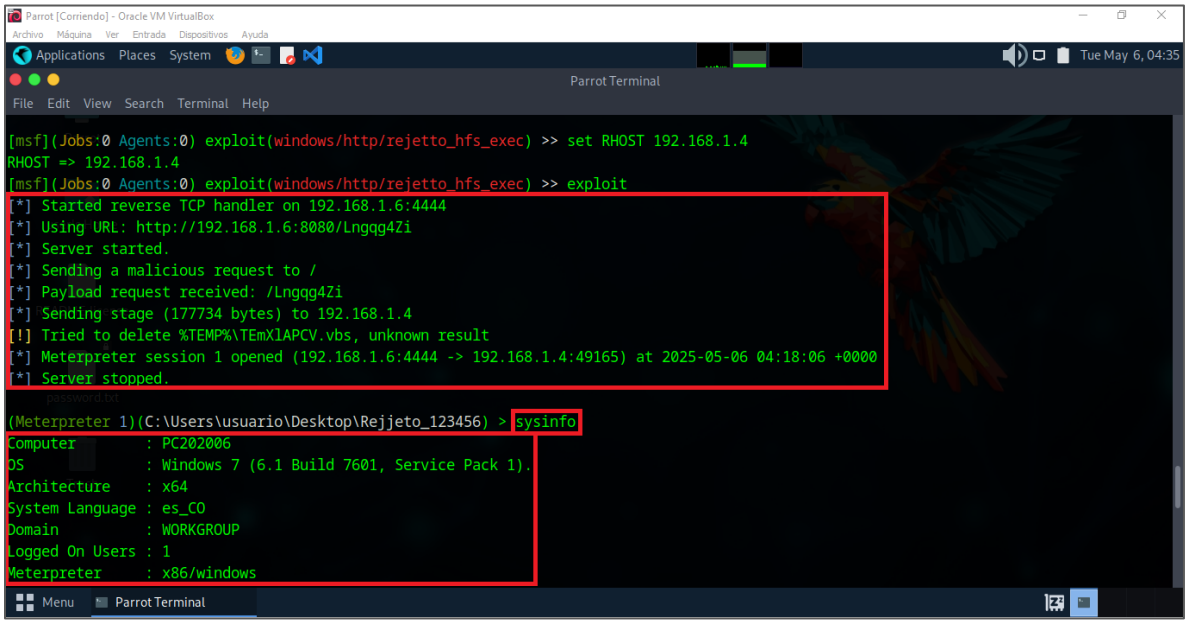
Establecimiento de Host víctima y comando para iniciar el Exploit.



Nota: Elaboración Propia.

Figura 25

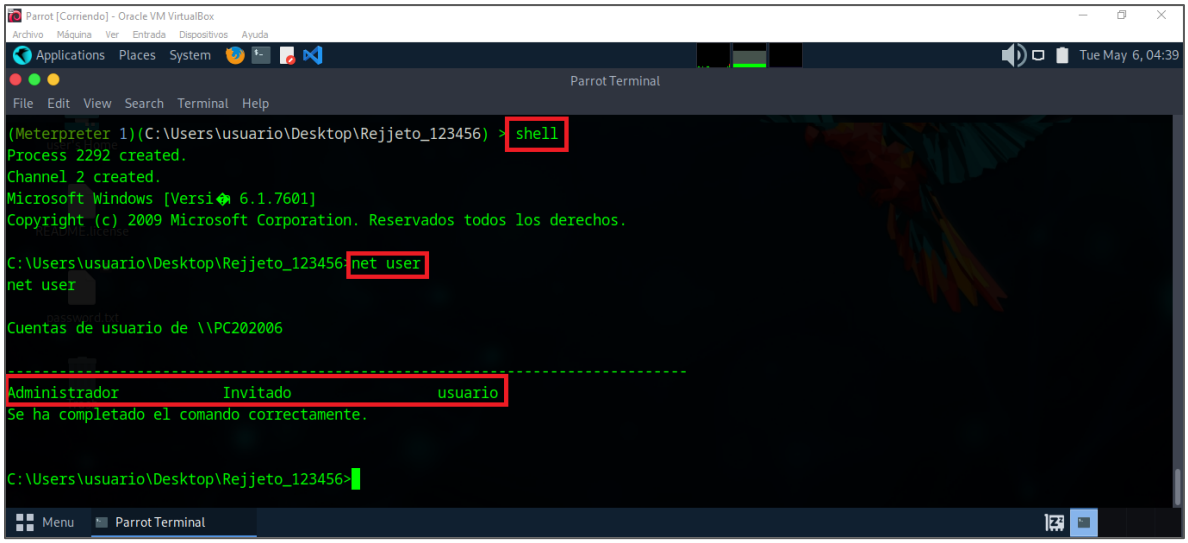
Explotación exitosa y conexión a equipo remotamente, uso de comando de “Sysinfo”



Nota: Elaboración Propia.

Figura 26

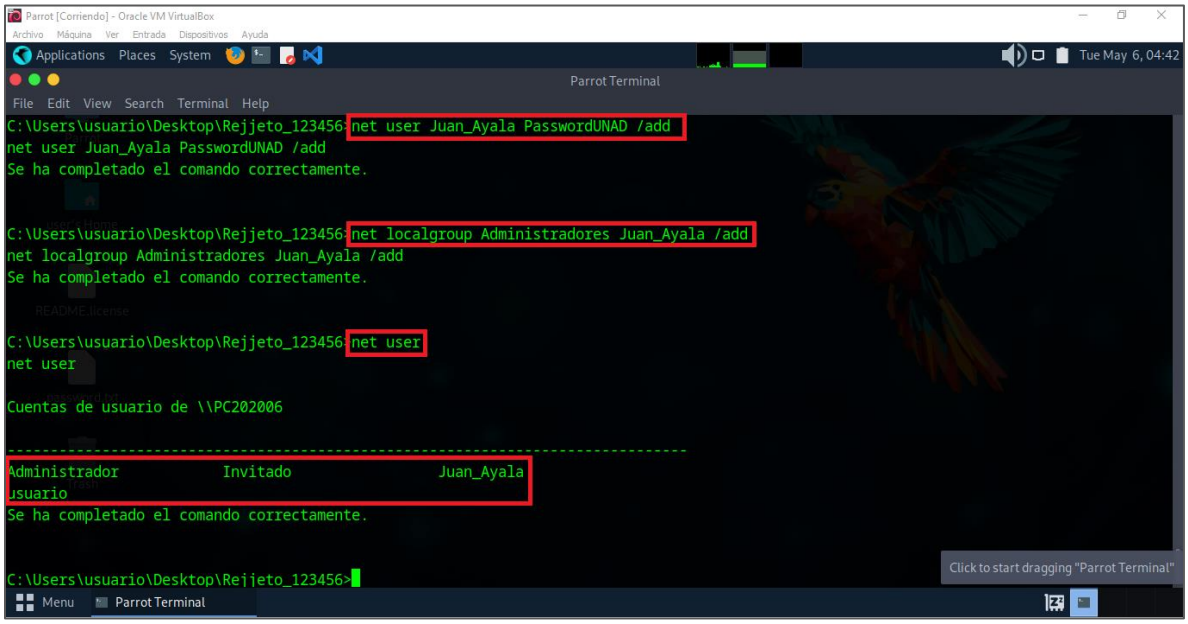
Comando Shell para ejecutar comandos de sistema en la maquina Víctima y vista de usuario del sistema.



Nota: Elaboración Propia.

Figura 27

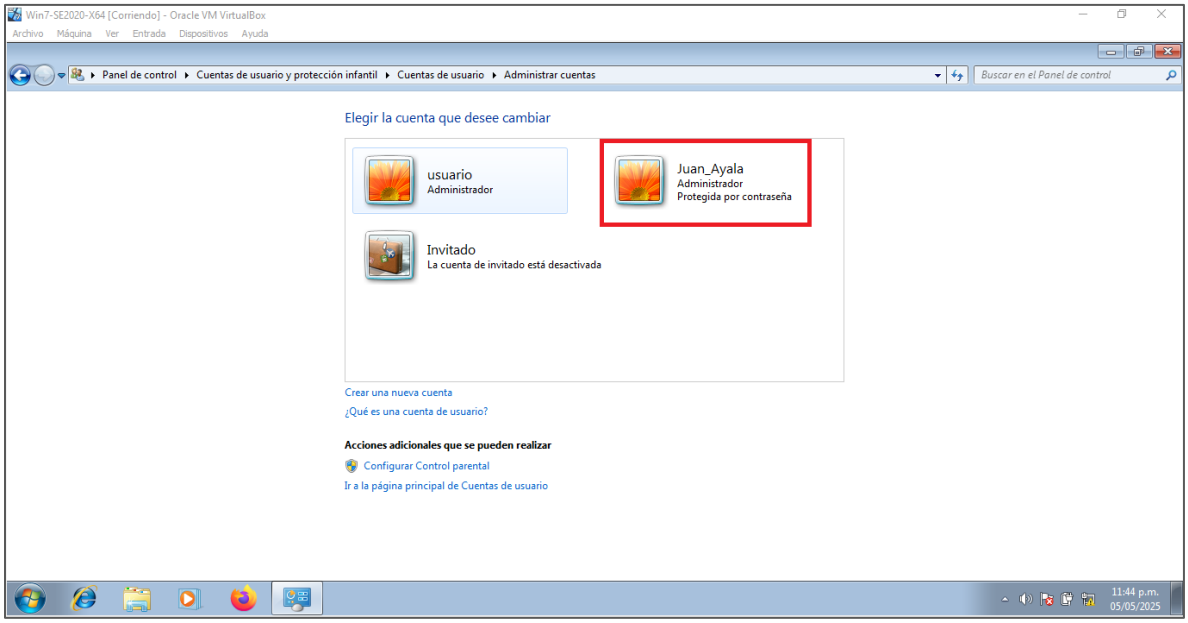
Comando para creación de usuario con contraseña y de tipo Administrador.



Nota: Elaboración Propia.

Figura 28

Vista desde Windows 7 de cuenta creada desde Parrot.



Nota: Elaboración Propia.

Figura 29

Cierre de sesión en maquina Parrot después de la creación del usuario administrador por RCE en vulnerabilidad de HttpFileServer 2.3 de Rejjeto.

Nota: Elaboración Propia.

Se puede observar que la vulnerabilidad presente en Rejetto HttpFileServer 2.3 permite llevar a cabo un ataque de Ejecución Remota de Código (RCE), mediante el cual es posible ejecutar comandos del sistema a través de una shell, esto permite, por ejemplo, utilizar el comando NET USER para crear nuevos usuarios y asignarles privilegios de administrador.

De esta forma, un atacante puede obtener acceso persistente al equipo comprometido y ejecutar diversas acciones que afectan tanto al sistema como a la red, los usuarios y los datos, comprometiendo la disponibilidad, integridad y confidencialidad de la información. Este laboratorio permite comprender cómo funciona un exploit que aprovecha una vulnerabilidad específica, así como las condiciones necesarias en la máquina víctima para que el ataque sea exitoso y se pueda tomar control total del sistema.

Identificación de Ataque en tiempo real y respuesta de Blue Team

Como profesionales especializados en seguridad informática debemos tener siempre algunos puntos clave para identificar y actuar ante un ataque en tiempo real. Alguno de estos son los siguientes tres:

Identificar El Ataque En Tiempo Real

- Se debe confirmar la existencia de una intrusión activa en la máquina comprometida, para esto se deben revisar las conexiones de red activas, esto va a permitir que se encuentren conexiones inusuales a IP's externas o desde puestos que no son estándar o utilizados. Cuando se detectan estas conexiones inusuales se debe validar la cantidad de conexiones, ya que demasiadas desde o hacia la misma IP es indicio de un posible escaneo o exfiltración de datos.

  En el caso del equipo comprometido, se puede analizar el comportamiento y el tráfico del puerto 80 el cual es el puerto utilizado por la aplicación Rejjeto HFS

- Analizar los procesos que se estén ejecutando también juega un papel muy importante a la hora de identificar un ataque en tiempo real, se pueden usar herramienta GLP p Free como "Process Hacker" el cual puede identificar y alertar sobre procesos sospechosos bien sea por sus nombres o por rutas inusuales donde se ejecutan, en la maquina comprometida podría

detectarse algunos procesos como los usados por el Powershell o algunos que haya involucrado lo archivos temporales en la carpeta del Rejjeto o procesos anormales de HFS.exe, se puede también tener en cuenta el uso del performance de la maquina tal como la CPU o de memoria, ya que puede ocasionar picos elevados en el trabajo de estos cuando se ejecutan procesos maliciosos o no legítimos.

- Monitorear actividad de red también es indispensable para la identificación de ataques, herramientas como TCPView puede verificar si los procesos como el de HFS.exe tiene conexiones activas a IPs remotas desconocidas, también se puede identificar mediante esta actividad de monitoreo si se están ejecutando Shells, scripts o archivos no legítimos o no autorizados por medio de red.

Contener El Ataque

El objetivo de esta fase es interrumpir toda actividad maliciosa, pero sin destruir evidencia crítica que sirva para investigaciones futuras, se pueden ejecutar las siguientes actividades:

- Aislar la máquina de la red, esto se puede realizar mediante comandos, agentes o de manera física desconectando el cable de red para que sea imposible seguirlo tomando de manera remota

- Detener procesos maliciosos también es una actividad a realizar en esta actividad, comandos como “taskkill” o desde el GUI del administrador de tareas puede permitir

finalizar procesos que permitan una conexión remota a un atacante, sin embargo, esta opción no es la más confiable ya que se pueden ejecutar tareas programadas que permitan al atacante volver a conectarse a futuro a la máquina.

Preservar Evidencia

Siempre es necesario preservar la evidencia en un ataque, esta permite estudiar la manera en que el equipo fue comprometido de manera que pueda ser remediado a futuro y evitar comprometer nuevamente la información o la red, esto también permite generar Indicadores de compromiso (IoC) los cuales puedan ser compartidos a los equipos de respuesta de incidentes o CSIRT los cuales compartan la información para evitar que otros sean atacados de la misma manera.

Se pueden realizar muchas actividades para exportar la data suficiente que permita una investigación posterior al compromiso, dentro de estos tenemos:

- Exportar lista de procesos: tasklist > <Ruta>\reporte_procesos.txt
- Exportar conexiones de red: netstat -ano > <Ruta>\reporte_netstat.txt

Indicadores De Compromiso (Ioc)

Se puede definir como evidencias observables que indican que una red, sistema o dispositivo puede haber sido comprometido por una amenaza o ataque cibernético. Los IoC pueden incluir direcciones IP maliciosas, dominios sospechosos, hashes de archivos maliciosos, firmas de malware o patrones inusuales de comportamiento en el sistema.

Algunas ventajas del uso de IoC en la detección de ciberataques son los siguientes:

- Permiten identificar ataques en sus primeras etapas, reduciendo el impacto potencial.
- Facilitan una acción inmediata al proporcionar información específica sobre la amenaza.
- Integración con herramientas de seguridad para bloquear automáticamente elementos maliciosos.
- Fortalecer la inteligencia colectiva contra ataques comunes si se comparten los IoCs entre organizaciones.

Realizar un volcado de memoria RAM utilizando herramientas gratuitas como Belkasoft RAM Capturer, para análisis posterior con Volatility.

Es fundamental evitar el movimiento lateral y la persistencia del atacante, quien podría estar intentando expandirse o mantener el acceso al sistema.

Preservar la evidencia forense es clave para comprender cómo ocurrió el ataque y qué se vio comprometido. Este análisis inicial permite determinar si se ha explotado una vulnerabilidad de ejecución remota (RCE), si hay una shell activa y qué comandos o herramientas están siendo utilizadas por el atacante.

Medidas para que el ataque no se repita

Las medidas de endurecimiento o Hardenización en inglés, que tomaría para que este ataque no se repita en la infraestructura comprometida seria la siguiente:

Eliminar O Reemplazar El Software Vulnerable

- Desinstalar la aplicación HFS 2.3 previamente identificada como brecha de seguridad, si necesariamente se debe mantener por requerimientos internos, se debe actualizar a la versión más reciente sin vulnerabilidades conocidas, sin embargo, sería más conveniente reemplazar HFS por un servidor web más seguro, como Apache o Nginx.

Restringir La Exposición Del Servicio

- Configurar el servidor HFS para que escuche únicamente en la dirección IP local o en una subred específica.
- Usar reglas de firewall para permitir el acceso solo desde IPs internas autorizadas y bloquear accesos externos.

Configuración Del Firewall En Windows 7

- Crear reglas para bloquear el puerto del servidor (por defecto el puerto 80) desde direcciones externas.
- Cerrar todos los puertos innecesarios y mantener un enfoque de denegación por defecto.
- Asegurarse de que solo los servicios requeridos estén accesibles desde la red.

Control De Aplicaciones

- Utilizar herramientas gratuitas o funciones del sistema operativo para restringir qué aplicaciones pueden ejecutarse.
- Prevenir que procesos como cmd.exe o powershell.exe puedan ser lanzados por aplicaciones web u otros procesos no autorizados.
- Usar listas blancas de ejecución para limitar el uso del sistema a software previamente aprobado.

Supervisión De Procesos

- Implementar herramientas como Process Hacker o OSSEC para monitorear todos los procesos en tiempo real los cuales se pueden estar ejecutando en el sistema.
- Configurar alertas cuando se detecten procesos anómalos, ejecución de scripts o invocación de comandos del sistema por parte de procesos no autorizados.

Hardenización Del Sistema Operativo

- Desactivar todos los servicios innecesarios, como Telnet, Escritorio Remoto, SNMP, entre otros.
- Aplicar todas las actualizaciones de seguridad posibles, utilizando parches manuales si es necesario, dado que Windows 7 ya no recibe soporte oficial.
- Configurar políticas de grupo para restringir la ejecución desde rutas como AppData, Temp, o el escritorio del usuario.
- Desactivar funciones de ejecución automática de scripts y macros.

Aislamiento Del Servicio

- Ejecutar HFS en una máquina virtual dedicada, sin acceso directo a recursos compartidos de la red interna.
- Establecer el servicio con una cuenta de usuario con permisos mínimos, sin privilegios administrativos.
- Implementar Sandboxing o contenedores para limitar el impacto de una posible explotación.

Supervisión Y Alertas

- Instalar un sistema de detección de intrusos como Snort o Suricata para detectar patrones de ataque conocidos y tráfico sospechoso.
- Configurar alertas para eventos como acceso al puerto del servidor desde direcciones desconocidas o ejecución de comandos del sistema.
- Centralizar los registros del sistema y la red usando herramientas como Wazuh o ELK Stack.

Restricción De Powershell Y CMD

- Limitar el uso de PowerShell a usuarios específicos.
- Registrar y auditar todos los scripts ejecutados mediante funciones de transcripción.
- Aplicar restricciones mediante políticas locales para prevenir su uso desde aplicaciones no confiables.

Conclusiones

Este seminario de especialización nos aportó un pensamiento más crítico y una mejor comprensión de los desafíos y momentos en los cuales los equipos de Red y Blue Team intervienen para ayudar en la protección de organizaciones, para esto los equipos deben tener claro los conceptos tanto éticos como legales en los cuales puedan verse involucrados, también por medio de laboratorios pudimos poner en práctica y en escenarios reales, un ataque a una maquina a través de una aplicación vulnerable, la cual permitió por medio de una ejecución de Código remoto la creación de usuarios administradores los cuales posiblemente pudieron realizar exfiltración de datos, con base a lo anterior se pueden formular estrategias de red y blue team que mejoren la postura de ciberseguridad y evitar estos problemas a futuro.

Recomendaciones

Recomendaciones Técnicas:

1. **Actualizar y parchear regularmente los sistemas y servicios:**

Mantener siempre actualizados el servicio HTTP File Server (HFS) y demás aplicaciones para corregir vulnerabilidades conocidas.

2. **Implementar controles de acceso estrictos:**

Restringir los permisos administrativos únicamente a usuarios autorizados, aplicando mecanismos robustos de autenticación y monitoreando la creación o modificación de cuentas con privilegios elevados.

3. **Despliegue de monitoreo activo y de sistemas de detección de intrusiones:**

Utilizar herramientas que permitan un monitoreo continuo para la identificación de comportamientos anómalos, tales como intentos de explotación o acceso no autorizado, permitiendo una respuesta oportuna.

4. **Implementar segmentación de redes y defensa en profundidad:**

Dividir la red en segmentos diferentes para limitar que un ataque se propague y de esta manera aplicar múltiples acciones de seguridad que protejan los activos críticos.

Recomendaciones Organizativas:

1. **Fomentar cultura organizacional de ciberseguridad en la organización:**

Promover conciencia y responsabilidad en ciberseguridad a todos los niveles de la organización, incentivando prácticas seguras y una comunicación fluida entre equipos.

2. **Capacitar continuamente al equipo de seguridad:**

Hay que asegurar que tanto el equipo Blue Team como el Red Team, reciba formación actualizada en técnicas y herramientas que permitan una mejor respuesta ante ataques.

3. **Documentar y mantener actualizadas las políticas de seguridad:**

Establecer y revisar periódicamente las políticas para que estas estén claras en el manejo y gestión de vulnerabilidades, control de accesos, respuesta a incidentes y mejores prácticas de seguridad, estas deben estar alineadas con estándares internacionales y política organizativa.

Recomendaciones Procedimentales:

1. **Realizar simulaciones periódicas de ataques controlados (Equipos de Red Team):**

Programar periódicamente ejercicios los cuales permitan evaluar la efectividad de todas las defensas y detectar posibles puntos débiles en el sistema.

2. **Fortalecer las capacidades del equipo de respuesta (Blue Team):**

Desarrollar planes de respuesta rápida ante incidentes, buenas prácticas de análisis forense digital y planes para mitigación de ataques con el objetivo de minimizar el impacto.

3. **Establecer procesos continuos de evaluación y mejora:**

Implementar revisiones constantes basados en resultados de auditorías, pruebas de penetración y monitoreos para ajustar y mejorar estrategias de seguridad presentes.

Referencias Bibliográficas

Bardají, E. (2025). Red Team vs Blue Team: Simulaciones de ciberataques para fortalecer la seguridad empresarial. ESEDsl. Recuperado de https://www.esedsl.com/blog/red-team-vs-blue-team-simulaciones-de-ciberataques-para-fortalecer-la-seguridad-empresarial

Bejarano Alarcón, J. C. (2024). Capacidades técnicas, legales y de gestión para equipos blue team y red team. Universidad Nacional Abierta y a Distancia. Recuperado de https://repository.unad.edu.co/handle/10596/62788

Check Point Software. (2025). Red Team vs. Blue Team. Cyber Hub. https://www.checkpoint.com/cyber-hub/cyber-security/red-team-vs-blue-team/

Cilleruelo, C. (2024). El Red Team y las simulaciones de ataques. KeepCoding. Recuperado de https://keepcoding.io/ciberseguridad/el-red-team-y-las-simulaciones-de-ataques/

Codemotion. (2024). Red Team vs Blue Team: Simulating Cyber Attacks. Codemotion Magazine. https://www.codemotion.com/magazine/cybersecurity/red-team-vs-blue-team-exercise-its-role-in-finding-your-cybersecurity-flaws/

Enoch, S. Y., Huang, Z., Moon, C. Y., Lee, D., Ahn, M. K., & Kim, D. S. (2020). HARMer: Cyber-attacks Automation and Evaluation. arXiv. Retrieved from https://arxiv.org/abs/2006.14352

Fortra. (2025). Guía: Red, Blue y Purple Team. Recuperado de https://www.fortra.com/es/recursos/guias/purple-blue-red-teaming

GTD. (2024). Purple Team: maximizando la colaboración entre Red y Blue Team. GTD Talks. Recuperado de https://blog.gtdcompany.com/2024/10/08/purple-team-maximizando-la-colaboracion-entre-red-y-blue-team/

Intelequia. (2025). Red Team y Blue Team - Funciones y Diferencias en Ciberseguridad. Recuperado de https://intelequia.com/es/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

Ley 1273 de 2009 - Gestor Normativo. (2015). Funcionpublica.gov.co. Recuperado de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Observatorio Nacional de Ciberseguridad. (2025). Claves estratégicas de las pruebas avanzadas de simulación de ciberataques. Recuperado de https://observatoriociber.org/claves-estrategicas-de-las-pruebas-avanzadas-de-simulacion-de-ciberataques/

Penetration Testing Execution Standard (PTES) : What is. Qualysec. (2024, April 2). https://qualysec.com/penetration-testing-execution-standard/#:~:text=PTES%20es%20una%20metodolog%C3%ADa%20de,a%20proveedores%20de%20servicios%20externos.

S2GRUPO. (2025). Blue team en ciberseguridad: definición, funciones y herramientas. Recuperado de https://s2grupo.es/blue-team-en-ciberseguridad-definicion-funciones-y-herramientas/

Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., & Kambhampati, S. (2019). A Survey of Moving Target Defenses for Network Security. arXiv. Recuperado de https://arxiv.org/abs/1905.00964

SentinelOne. (2024). Red Team Exercises in Cybersecurity: Benefits & Examples. SentinelOne. https://www.sentinelone.com/cybersecurity-101/services/red-team-exercise-in-cybersecurity/

UNIR. (2020). Red Team, Blue Team y Purple Team: funciones y diferencias. UNIR Revista. Recuperado de https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/

WebSecurityPulse. (2024). Red Team vs. Blue Team: Enhancing Cyber Defense Through Simulated Attacks. WebSecurityPulse. https://www.websecuritypulse.com/guides/red-team-blue-team-enhancing/

Anexos (URL Video)

URL Video de publicación de la sustentación del desarrollo del seminario especializado:

- URL VIDEO
- https://youtu.be/Gp8PBY9NiJE

Evidencia de Video Cargado a plataforma YouTube: