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

Jonathan Moncada Ramírez

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI)

Especialización en Seguridad Informática

2025

Resumen

El presente trabajo desarrolla un ejercicio práctico de análisis ofensivo y defensivo en un entorno controlado, aplicando técnicas propias de los equipos Red Team y Blue Team. Para ello se emplearon dos máquinas Windows configuradas como Host-A y Host-B, junto con un sistema Parrot OS como estación atacante. Durante la fase ofensiva se identificaron vulnerabilidades críticas en Host-A, entre ellas una explotación remota del servicio Rejetto HFS 2.3 y un vector adicional asociado a EternalBlue, lo que permitió obtener acceso privilegiado y posteriormente ejecutar un movimiento lateral hacia Host-B por medio de pivoting. Una vez comprometido el segundo equipo, se procedió a recrear el impacto potencial mediante la creación controlada de un usuario administrativo. Desde la perspectiva del Blue Team se efectuó una revisión de los eventos generados, se analizaron las trazas de comportamiento y se estableció una ruta probable de intrusión. A partir de ello se diseñó un conjunto de acciones de contención y medidas de endurecimiento para mitigar futuros incidentes. El trabajo evidencia la importancia de realizar pruebas ofensivas en laboratorio y fortalecer la capacidad de respuesta ante amenazas reales.

Palabras clave: BlueTeam, forense, pivoting, RedTeam, vulnerabilidades.

Abstract

This paper presents a practical exercise in offensive and defensive analysis in a controlled environment, applying techniques specific to Red Team and Blue Team environments. Two Windows machines, configured as Host-A and Host-B, were used, along with a Parrot OS system as the attacker station. During the offensive phase, critical vulnerabilities were identified on Host-A, including remote exploitation of the Rejetto HFS 2.3 service and an additional vector associated with EternalBlue. This allowed for privileged access and subsequent lateral movement to Host-B via pivoting. Once the second machine was compromised, the potential impact was simulated by the controlled creation of an administrative user account. From the Blue Team perspective, a review of the generated events was conducted, behavioral traces were analyzed, and a probable intrusion path was established. Based on this analysis, a set of containment actions and hardening measures were designed to mitigate future incidents. This paper highlights the importance of conducting offensive tests in a laboratory setting and strengthening response capabilities against real-world threats.

Keywords: BlueTeam, forensics, pivoting, RedTeam, vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Blue Team:

Grupo responsable de monitorear, detectar, contener y remediar incidentes de seguridad dentro de una organización.

EternalBlue:

Exploit que aprovecha una falla crítica en SMBv1, permitiendo la ejecución remota de código en versiones antiguas de Windows.

Hardening:

Conjunto de medidas destinadas a reducir la superficie de ataque de un sistema operativo o servicio.

Meterpreter:

Shell avanzado de Metasploit que facilita el control remoto de una máquina comprometida.

Movimiento lateral:

Acción mediante la cual un atacante avanza dentro de la infraestructura una vez obtiene presencia en un equipo inicial.

Pivoting:

Técnica que permite a un atacante utilizar un equipo comprometido como puente para acceder a otros sistemas dentro de la red.

Rejetto HFS 2.3:

Aplicación que funciona como un servidor HTTP liviano, conocida por vulnerabilidades que permiten ejecución remota de código.

Red Team:

Equipo encargado de simular ataques reales para comprobar la resistencia de un entorno tecnológico ante amenazas externas o internas.

Introducción

El análisis de seguridad informática requiere comprender tanto las tácticas empleadas por un atacante como las acciones necesarias para detectarlo y contenerlo. Con este propósito, el presente trabajo recrea un escenario de ataque y respuesta en un entorno virtual diseñado para simular condiciones reales sin afectar sistemas productivos. El ejercicio involucra dos dominios de actuación: el Red Team, encargado de ejecutar técnicas ofensivas para comprometer sistemas vulnerables, y el Blue Team, responsable de analizar la intrusión, determinar su alcance y establecer medidas de remediación.

Durante la práctica se utilizó una máquina con Parrot OS como atacante y dos máquinas Windows representando sistemas internos. A través de técnicas de escaneo, explotación y pivoting, se demostró cómo un atacante puede escalar privilegios y desplazarse lateralmente dentro de la infraestructura. Posteriormente, se analizó el incidente desde la óptica defensiva para establecer la ruta de compromiso, identificar el ataque y aplicar controles técnicos orientados a prevenir ataques similares en el futuro. Este enfoque integral refuerza la importancia del entrenamiento práctico en escenarios de ciberseguridad.

Justificación

La creciente dependencia de las organizaciones en infraestructuras digitales hace que las amenazas informáticas evolucionen con rapidez y se vuelvan cada vez más sofisticadas. Por ello, resulta indispensable que los profesionales en formación desarrollen competencias tanto ofensivas como defensivas para comprender de manera integral cómo se originan, ejecutan y mitigan los ataques cibernéticos. El presente trabajo se justifica en la necesidad de simular escenarios reales que permitan identificar debilidades técnicas, evaluar el comportamiento de los sistemas ante incidentes y fortalecer la capacidad analítica del estudiante frente a situaciones de riesgo.

Mediante la ejecución de ejercicios controlados de Red Team y Blue Team, es posible reconocer de primera mano cómo una vulnerabilidad no corregida puede convertirse en un punto de entrada para un atacante, facilitando desde la escalación de privilegios hasta el movimiento lateral dentro de una red. Al mismo tiempo, la revisión desde el enfoque defensivo permite comprender la importancia del monitoreo, el análisis forense y la implementación de controles que reduzcan el impacto de esas amenazas.

Este enfoque práctico contribuye a desarrollar una visión más completa del ciclo de un ataque y a formar profesionales capaces de anticipar, detectar y responder ante cualquier incidente de seguridad, fortaleciendo la preparación técnica para enfrentar desafíos del mundo real.

Objetivos

Objetivo General

Realizar un análisis integral ofensivo y defensivo en un entorno de laboratorio mediante técnicas de Red Team y Blue Team, con el fin de identificar vulnerabilidades, explotar fallas controladamente, evaluar el movimiento lateral y aplicar medidas de remediación que fortalezcan la seguridad del sistema.

Objetivos Específicos

Identificar y analizar vulnerabilidades presentes en Host-A mediante herramientas de reconocimiento y enumeración.

Explotar fallas críticas como Rejetto HFS V2.3 y EternalBlue para obtener acceso remoto controlado.

Ejecutar técnicas de pivoting desde Host-A hacia Host-B para demostrar movimiento lateral.

Recrear de manera segura el impacto potencial mediante la creación de un usuario administrativo en Host-B.

Evaluar la intrusión desde la perspectiva del Blue Team mediante análisis de eventos y trazas de actividad.

Diseñar e implementar medidas de contención y hardening orientadas a reducir riesgos futuros.

Documentar el proceso completo, relacionando acciones ofensivas con respuestas defensivas.

ETAPA 1: Fundamentos de operaciones Red Team y Blue Team

Describa con sus propias palabras que legislación a nivel de leyes y decretos existen actualmente en Colombia sobre delitos informáticos.

LEY 1273 DE 2009

Esta ley fue creada con el fin de modificar el código penal con el fin de proteger la información, los datos y la preservación integral de todos los sistemas que hagan uso de las tecnologías de la información (Función Pública, 2009).

Características:

Se divide en 2 capítulos, los cuales abordan los atentados contra la triada de la información y los atentados informáticos y otras infracciones.

Capítulo I: De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Se divide en 7 artículos los cuales mencionare a continuación:

Artículo 269A: Acceso abusivo a un sistema informático. Habla del uso sin autorización de un sistema informático, este o no protegido y la pena que esta acción puede generar.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. Menciona la pena que se generaría para aquellos que sin tener facultad para hacerlo impida el funcionamiento normal a un sistema informático.

Artículo 269C: Interceptación de datos informáticos. Habla de la pena que se impondrá aquellos que intercepten datos informáticos en su origen, destino o el interior.

Artículo 269D: Daño Informático. Quien no este facultado para ello, destruya, dañe, borre, deteriore o altere cualquier sistema de tratamiento de información o sus componentes lógicos.

Artículo 269E: Uso de software malicioso. El que sin tener la facultad produzca, trafique o distribuya programas maliciosos u otros programas de computación de efectos dañinos.

Artículo 269F: Violación de datos personales. Quien con provecho propio o de un tercero realice alguna acción sobre los datos personales contenidos en ficheros o bases de datos.

Artículo 269G: Suplantación de sitios web para capturar datos personales. Habla sobre el ilícito y sin facultades para diseñar, vender o ejecutar, programé o envié páginas electrónicas, enlaces o ventanas emergentes.

Artículo 269H: Circunstancias de agravación punitiva: Los artículos descritos anteriormente aumentaran dependiendo sobre donde se genere el delito, entre las opciones aparecen algunas tales como: Redes informáticas, por servidor público, aprovechando la confianza depositada, entre otras.

Capitulo II: De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. Este artículo habla sobre cuando una persona roba información o bienes usando medios informáticos. Es decir, de si alguien logra entrar o superar las medidas de seguridad de un sistema, red o computadora, y desde ahí manipula datos o suplanta a otro usuario para obtener algo que no le pertenece.

Artículo 269J: Transferencia no consentida de activos. Este artículo se refiere a cuando alguien, con intención de ganar dinero, utiliza un truco o manipulación informática para mover o transferir dinero u otros bienes que no son suyos, perjudicando a otra persona.

LEY 1928 DE 2018: Convenio de Budapest

Obliga a Colombia a tener estándares mínimos de tipificación de delitos como el acceso ilícito a sistemas, la interceptación de datos informáticos, interferencia en los datos, interferencia en los sistemas, abuso de los dispositivos, falsificación y fraude informático, delitos relacionados

con pornografía infantil, entre otros para sumar un total de 48 artículos que hacen parte de este convenio de Budapest el cual Colombia adopto y fue promulgada el 24 de julio de 2018. (Sistema Único de Información Normativa, 2018)

Ley 1581 de 2012: Protección de datos personales

Esta ley busca desarrollar un derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar toda información que haya sido recolectada sobre ella en las bases de datos o archivos o como se conoce este derecho el habeas data.

Características principales:

Aplica tanto a entidades públicas como privadas y establece principios como:

- Finalidad
- Libertad (requiere consentimiento)
- Veracidad
- Seguridad
- Confidencialidad

Obliga a las empresas a solicitar autorización previa para tratar datos personales y crea la figura del responsable y encargado del tratamiento, y exige la adopción de políticas de protección de datos. (Función Pública, 2012)

Decreto 1377 de 2013 – Reglamentación de la Ley 1581

Este decreto reglamenta parcialmente la Ley 1581. Específicamente, detalla cómo deben obtenerse las autorizaciones para el uso de datos personales que ya existían antes de la ley, y cómo deben las entidades avisar a los titulares.

Puntos clave:

Permite que empresas continúen tratando datos recolectados antes de 2012, si notifican adecuadamente al titular.

Obliga a tener políticas claras de tratamiento de datos. (Función Pública, 2013)

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.

¿Qué es el Pentesting?

El Pentesting (Prueba de Penetración) es un proceso controlado en el que un profesional de ciberseguridad simula un ataque real contra un sistema, red o aplicación, con el fin de descubrir vulnerabilidades antes de que lo hagan atacantes maliciosos.

Estas pruebas permiten que el evaluador verifique los aspectos funcionales de un modelo, de tal manera que puede determinar el grado de vulnerabilidad de un objetivo ante ataques de intrusión y su nivel de seguridad. (Garg & Bansal, 2021)

Este proceso se realiza en etapas definidas, para asegurar que los resultados sean precisos, éticos y útiles, apoyándose del uso de herramientas destinadas para este fin.

Etapas del Pentesting

Reconocimiento

En esta etapa se recolecta toda la información posible sobre el objetivo. El pentester acuerda con el cliente qué sistemas se pueden analizar, en qué horarios y con qué objetivos. El objetivo puede ser una red, una web, una empresa o una persona. Esta información puede ser pública (como dominios, correos, servidores) o privada si se usa ingeniería social.

Herramienta, Shodan

para encontrar qué servicios de la empresa están expuestos a Internet.

Escaneo

Una vez se tiene información básica, el pentester empieza a "tocar" el sistema para ver qué está activo y cómo responde.

En esta fase se aplican diferentes aplicaciones, herramientas y técnicas de escaneo para escanear redes, dispositivos y servicios. Identifica una unidad compartida abierta, puertos FTP abiertos, servicios que se están ejecutando, etc. Los métodos de escaneo se dividen en escaneo estático y escaneo dinámico. (Sarker, 2023)

Herramienta, Nmap

Es una herramienta muy usada para descubrir qué servicios están funcionando en una máquina, qué puertos están abiertos y qué sistemas operativos están corriendo.

Enumeración o análisis de vulnerabilidades

Es una extensión del escaneo, pero más profundo. Aquí se trata de extraer información detallada de los servicios detectados (usuarios, nombres de máquina, versiones de software, etc.).

Herramienta, Enum4linux

Enum4linux sirve para obtener información de sistemas Windows o Linux, permite obtener información como (usuarios, grupos, políticas de seguridad).

Explotación

Esta es la parte en que se aprovechan las vulnerabilidades encontradas para obtener acceso no autorizado a los sistemas. El objetivo de esta fase no es dañar, si no demostrar si una de estas vulnerabilidades puede ser usada en un ataque real.

Herramienta, Metasploit Framework

Metasploit es uno de los frameworks más conocidos. Permite automatizar muchos tipos de ataques y probar exploits contra servicios vulnerables.

Escalada de privilegios

Si el atacante obtuvo acceso limitado (por ejemplo, como usuario), intentará aumentar sus privilegios para tener control total del sistema (por ejemplo, como administrador o root).

Herramienta, LinPEAS / WinPEAS

buscan formas de obtener privilegios más altos.

Mantenimiento del Acceso

Se configura una forma de mantener el acceso sin ser detectado, como dejar una puerta trasera o un usuario oculto, simulando lo que haría un atacante persistente.

Esto se puede hacer dejando un rockit en el sistema, que es un tipo de programa maligno con gran habilidad para ocultarse.

Limpieza

Después de terminar las pruebas, el pentester borra cualquier rastro de su actividad para dejar el sistema igual que antes.

Esto incluye eliminar usuarios de prueba, archivos cargados o registros creados durante la prueba.

Se puede hacer mediante scripts o comandos del sistema operativo para eliminar archivos y usuarios temporales o incluso de manera manual

Informe

Por último, el pentester prepara un informe detallado con todos los hallazgos.

Incluye qué vulnerabilidades encontró, cómo las explotó, qué impacto tendrían y cómo solucionarlas.

Se entrega normalmente un informe técnico (para el equipo de TI) y uno ejecutivo (para la dirección).

Herramienta, Dradis

permite organizar los hallazgos técnicos y convertirlos en reportes para equipos de seguridad o ejecutivos

Las herramientas de ciberseguridad son fundamentales para analizar, proteger y evaluar sistemas. Como futuro profesional, es importante que puedas definir y explicar el uso de las herramientas más relevantes del entorno:

Metasploit

es como una "caja de herramientas" para probar si una vulnerabilidad realmente puede aprovecharse. Incluye exploits (que es lo que usamos para aprovechar la falla), payloads (lo que queda ejecutando en el equipo objetivo) y utilidades para automatizar pruebas y explorar sistemas tras ingresar al sistema.

Metasploit nos permite validar que una vulnerabilidad detectada es explotable, simular ataques controlados y realizar tareas de post-explotación (inspeccionar qué se puede acceder desde dentro).

Un ejemplo de esto sería, si se detecta un puerto vulnerable en el sistema objetivo, Metasploit permite ejecutar un exploit conocido contra él y abrir una sesión para demostrar el impacto.

Se recomienda siempre usar en ambientes controlados y con autorización del objetivo si es fuera de un laboratorio de prueba.

Nmap

Nmap es una de las herramientas más utilizadas en entornos de ciberseguridad para examinar y analizar redes. Su nombre proviene de *Network Mapper*, y su desarrollo ha sido liderado por Gordon Lyon, también conocido como Fyodor, quien ha mantenido y ampliado la herramienta a lo largo del tiempo (Machap et al., 2024)

Nmap nos permite mapear la superficie de ataque, saber exactamente qué hay expuesto hacia Internet o dentro de una red para de esta manera hacernos una idea de que podemos atacar.

Como ejemplo, podríamos lanzar con un comando que nos permita escanear una IP o rango y obtener una lista de puertos abiertos y servicios detectados.

Al igual que el Metasploit se recomienda ejecutar en entornos controlados, ya que la inspección puede alertar los sistemas.

OpenVAS (Greenbone Vulnerability Manager)

es un escáner automatizado de vulnerabilidades. Revisa sistemas buscando fallos conocidos y te devuelve un reporte con severidades y referencias a CVE.

Está diseñado para ser un escáner de vulnerabilidades completo con una variedad de pruebas integradas y una interfaz web diseñada para que la configuración y la ejecución de los escáneres de vulnerabilidades sean rápidas y sencillas, al tiempo que ofrece un alto nivel de configurabilidad por parte del usuario. (Afif Saktiansyah, 2022)

Ante este tipo de evaluaciones se debe siempre hacer una validación manual ya que los hallazgos pueden tener falsos positivos.

Servicios en línea:

ExploitDB (Exploit Database)

Es un repositorio público de exploits y pruebas de concepto (PoC) mantenido por Offensive Security. Es el lugar donde encontrarás código de ejemplo para vulnerabilidades públicas.

ExploitDB se usa para ver si existe un exploit público o un PoC que demuestre cuando explotarla, luego de obtener una o las vulnerabilidades luego de un escaneo.

Como usarla, se busca por CVE o por el nombre del software y revisar el PoC para entender la técnica o reproducirla en un laboratorio controlado.

CVE (Common Vulnerabilities and Exposures)

es la lista estándar de vulnerabilidades públicas: cada falla documentada recibe un identificador único (por ejemplo, CVE-2024-12345) y una descripción breve. Es la forma aceptada de nombrar vulnerabilidades para que todos hablen el mismo idioma.

Nos facilita buscar información, parches y referencias (por ejemplo, en NVD, ExploitDB, avisos de fabricantes). Si un escáner devuelve un CVE, se puede buscar rápidamente detalles, mitigaciones y exploits relacionados.

Por ejemplo, un reporte de un escaner como Nessus incluirá CVE en sus hallazgos; con ese número se busca la información oficial y las recomendaciones del proveedor.

Para cerrar esta actividad, es necesario que el estudiante identifique, configure y analice el "banco de trabajo" descrito en el Anexo 1 – Escenario 1, ya que sobre este entorno se desarrollarán las tareas técnicas asignadas

a. Descargar la herramienta virtualiza dora "VirtualBox" en su última versión.

Figura 1

Descarga de VirtualBox

Nota. Autoría propia, descarga de la aplicación VirtualBox en su última versión

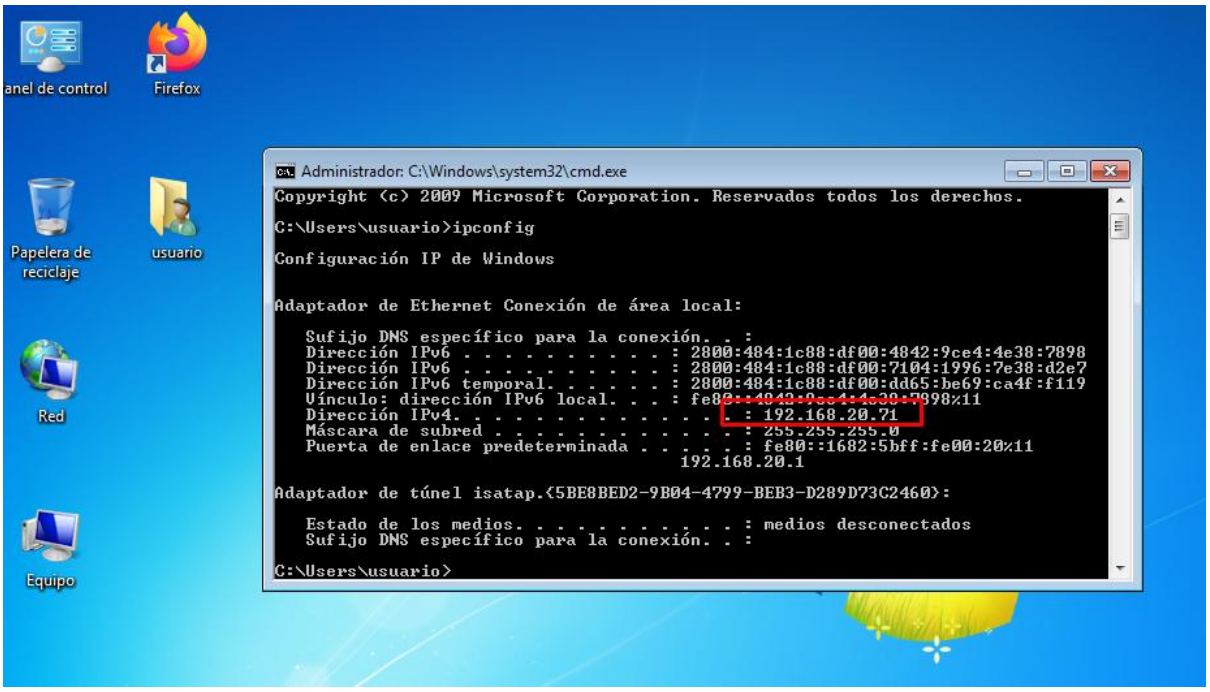
Figura 2

Comprobación de Ovas

Nota. Autoría propia, conexión con el repositorio para la descarga de los OVAS de trabajo.

Figura 3

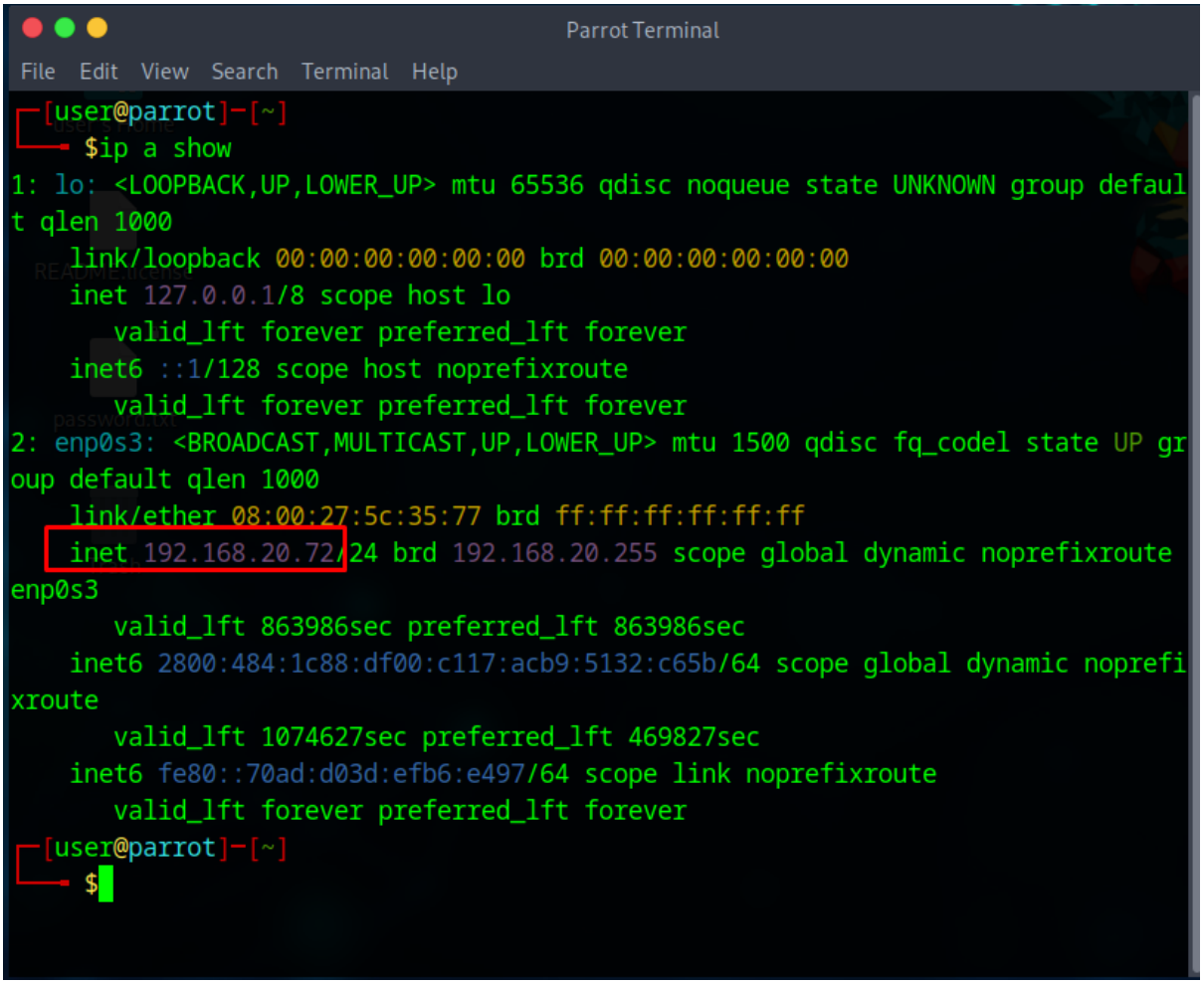
Conexión a la máquina WIN 7: 192.168.20.71



Nota. Autoría propia, se confirma el direccionamiento tomado por la máquina Win 7, ya que debe ser el mismo segmento de red que tiene el equipo con Parrot OS.

Figura 4

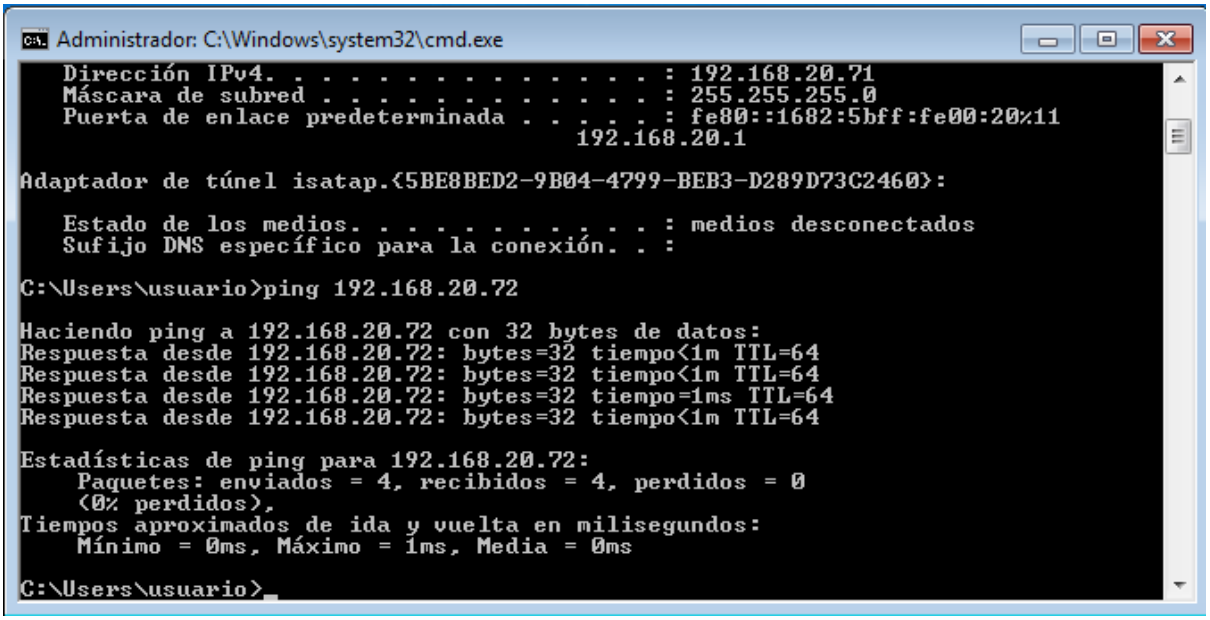
Conexión al equipo con Parrot OS: 192.168.20.72



Nota: Autoría propia, se valida direccionamiento de red para que las pruebas que se realizaran después funcionen correctamente.

Figura 5

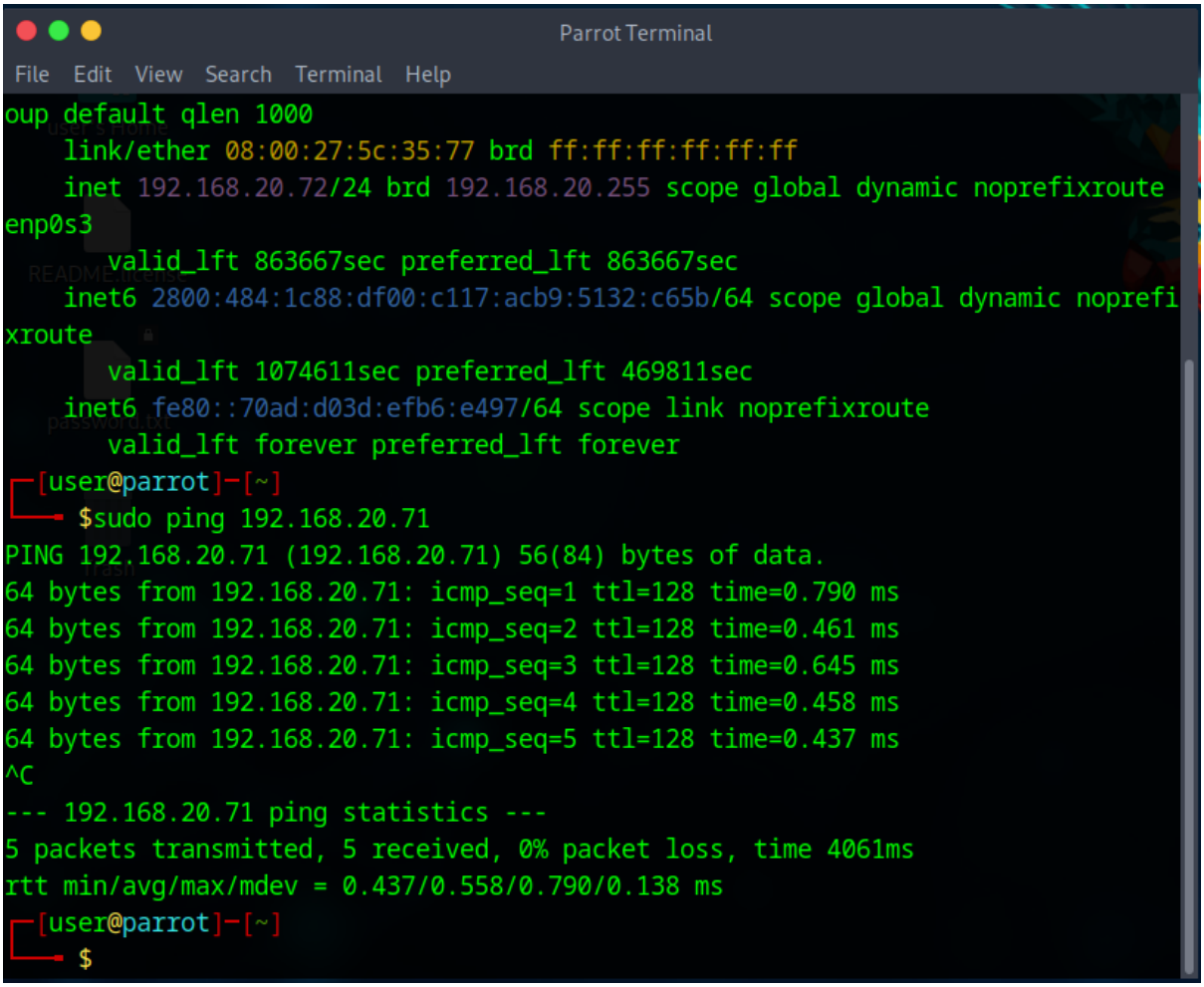
Prueba de conexión del equipo Win 7 al Parrot OS



Nota. Autoría propia, se lanza un ping desde el equipo Win7 con IP 192.168.20.71 hacia el Parrot OS con IP 192.168.20.72 para garantizar que se ven.

Figura 6

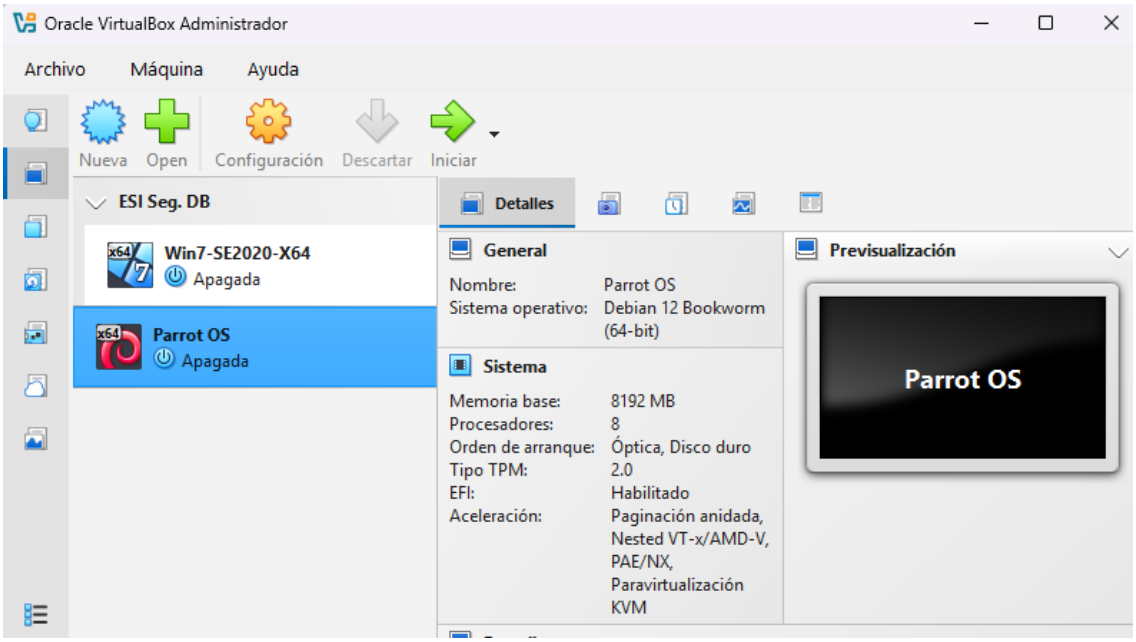
Prueba de conexión del equipo Parrot OS al Win7



Nota. Autoría propia, se lanza prueba de conexión desde el equipo Parrot Os con IP 192.168.20.72 al Win7 con IP 192.168.20.71 para garantizar el alcance entre los 2 equipos.

Figura 7

Banco de trabajo sobre VirtualBox



Nota. Autoría propia, se realiza montaje de las máquinas virtuales, sobre el virtualizados VirtualBox, mediante el uso de OVAS proporcionadas para el desarrollo de este ejercicio práctico.

El banco de trabajo fue desplegado sobre una máquina anfitriona con sistema operativo Windows 11 que actúa como hipervisor mediante VirtualBox. Las características técnicas del equipo anfitrión son las siguientes: procesador Intel Core i5 (12ª generación), 32 GB de RAM y 1.84 TB de almacenamiento en disco. Sobre esta máquina se instalaron dos máquinas virtuales provisionales importadas desde archivos OVA preconfigurados: una VM con Parrot OS y otra con Windows 7. La configuración asignada a las máquinas virtuales es:

- Parrot OS (VM): 8 GB de RAM asignada, interfaz de red en modo adaptador de puente, disco virtual preconfigurado desde OVA y herramientas de pentesting instaladas.
- Windows 7 (VM): 4 GB de RAM asignada, disco virtual importado desde OVA y configuraciones iniciales ya aplicadas.

El flujo operativo del banco de trabajo consiste en ejecutar las pruebas y herramientas de seguridad desde la VM Parrot OS, conduciendo escaneos y técnicas de explotación contra la VM Windows 7 cuando corresponda. La máquina anfitriona Windows 11 se utiliza para gestionar VirtualBox, almacenar instantáneas (snapshots) y mantener copias de seguridad de los OVA.

Figura 8

Capacidades del equipo anfitrión

Nota. Autoría propia, se realiza montaje sobre un equipo con capacidades suficientes que garantizan el correcto y optimo funcionamiento del laboratorio.

ETAPA 2: Ética Profesional Y Marco Normativo En Operaciones De Seguridad

¿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.

Si se encontraron procesos ilegales dentro del anexo 3, los cuales relaciono a continuación y subrayo en rojo:

1. Primera. Objeto: en virtud del presente acuerdo de confidencialidad, la parte receptora, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, autoridades legales, asesores o cualquier

persona relacionada con ella, la información confidencial o sobre procesos ilegales dentro de SecureNova Labs no podrán ser divulgados.

Argumento: Ningún acuerdo de confidencialidad puede impedir la denuncia de delitos y la colaboración con las autoridades, por lo cual la firma del contrato no puede prohibir cooperar con las mismas.

La firma del acuerdo debería excluir la denuncia de procesos ilegales porque iría en contra de los principios de transparencia y cooperación con los entes legales.

2. 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".

Argumento: En este punto se pretende considerar las actividades ilícitas como información confidencial que ante la ley colombiana están consideradas como delito grave, ya que vulnera delitos básicos como derecho a la intimidad.

3. Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el proceso de selección de personal y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Argumento: la información personal compartida en los procesos de selección como la hoja de vida, entre otros, son considerados datos personales y sensibles. Por lo que esta información no puede considerarse confidencial ya que son del candidato.

El mencionar que "independiente de su fuente o soporte" indicaría que no diferencia la forma en que se obtenga la información y esta podría ser pública o incluso obtenida de manera ilegal.

4. Proteger la información confidencial, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma SecureNova Labs, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla

Argumento: En este punto no se establece un límite de la obtención de la información y por ende no es posible indicar que SecureNova es la legitima poseedora de la información la cual puede proceder de terceros y se puede incurrir en el delito por obtener información sin permiso.

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

Argumento: En Colombia se tiene el deber de denunciar cualquier delito a las autoridades competentes, por lo que este punto vulnera el derecho a la moral, sin contar los delitos que promueve encubrir de la ley 1273 .

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

Argumento: En este punto se prohíbe denunciar sobre la información ilegal lo que lleva al empleado a omitir la denuncia de un delito, lo que limita el derecho de este a colaborar con la justicia colombiana.

7. La parte receptora se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la información confidencial o ilegal sin el previo consentimiento por escrito por parte SecureNova Labs.

Argumento: en este punto SecureNova Labs mantiene su posición de prohibir al empleado la participación y denuncia de eventos ilegales que pueda encontrar dentro de la organización, lo cual es derecho de todo colombiano.

Si se identifican prácticas irregulares dentro del anexo 3, es necesario señalar qué artículos de la Ley 1273 podrían estar siendo infringidos y explicar cómo cada cláusula del acuerdo vulnera dichas disposiciones.

Artículo 269A – Acceso abusivo a un sistema informático

Este artículo sanciona a quien acceda sin autorización a sistemas informáticos protegidos.

En el acuerdo se mencionan prácticas relacionadas con “procesos ilegales” y “acceso o interceptación de información”, las cuales podrían implicar la obtención o manipulación de datos ajenos sin permiso.

Permitir o encubrir estas acciones dentro de una organización equivale a autorizar un acceso indebido, lo cual vulnera directamente este artículo. (Función Pública, 2009)

Artículo 269B – Obstaculización ilegítima de sistemas informáticos o redes

Se vulnera este artículo cuando se interfiere, manipula o altera el funcionamiento normal de un sistema informático.

Las cláusulas que prohíben denunciar actividades sospechosas de espionaje o apropiación de datos fomentan el encubrimiento de acciones que pueden alterar o interferir redes y sistemas, lo cual se considera una violación al espíritu de este artículo. (Función Pública, 2009)

Artículo 269C – Interceptación de datos informáticos

Sanciona a quien intercepte comunicaciones digitales o flujos de información sin consentimiento.

En el acuerdo se menciona la existencia de "datos de chuzadas e interceptación de información", lo cual representa una conducta claramente tipificada como delito. Si una empresa mantiene o protege este tipo de información bajo el pretexto de confidencialidad, estaría encubriendo prácticas de interceptación ilícita, infringiendo así este artículo. (Función Pública, 2009)

Artículo 269D – Daño informático

Este artículo protege la integridad de los datos frente a alteraciones, borrado o daño.

Si el acuerdo impide denunciar irregularidades o mal uso de la información, se obstaculiza la identificación de alteraciones o destrucción intencional de datos, lo que indirectamente favorece la comisión del delito de daño informático. (Función Pública, 2009)

Artículo 269E – Uso de software malicioso

Sanciona la producción, distribución o tenencia de programas destinados a cometer delitos informáticos.

Al incluir referencias a procesos ilegales o manipulación de sistemas, y exigir silencio sobre ello, el acuerdo podría encubrir el uso de herramientas o programas con fines delictivos, vulnerando este artículo. (Función Pública, 2009)

Artículo 269H – Violación de datos personales

Protege los datos personales frente a la recolección o divulgación sin autorización.

Algunas cláusulas obligan a guardar silencio frente a la apropiación de información de terceros, lo que implica una violación a la privacidad y confidencialidad de datos personales.

Aceptar el no reportar o denunciar estos actos sería una infracción directa de este artículo. (Función Pública, 2009)

¿Al ver los procesos que no son del todo confiables en el Anexo 3, aplicaría al trabajo propuesto por SecureNova Labs, viendo que el salario es de $15.000.000 con contrato vitalicio?

No aplicaría posterior a la lectura del anexo lo rechazaría.

Argumente su respuesta ya sea afirmativa o negativa teniendo en cuenta el código de ética de COPNIA.

El artículo 31, literal b, señala como deber del profesional "custodiar y cuidar los bienes, valores, documentación e información que por razón del ejercicio de su profesión se le hayan encomendado, impidiendo su uso indebido". Si dentro del acuerdo laboral se promueven prácticas que puedan vulnerar la confidencialidad o manipular información de manera inapropiada, el profesional debe abstenerse de participar en dichas actividades. (Copnia, 2003)

De igual forma, el artículo 34, literal a, prohíbe "aceptar trabajos en contra de las disposiciones legales vigentes o que excedan la incumbencia que le otorga su título". Por tanto, si el ejercicio profesional dentro de esa empresa pudiera involucrar actos contrarios a la ley como la manipulación indebida de datos o la omisión de denuncias ante conductas ilícitas, aceptar el cargo sería una falta ética grave. (Copnia, 2003)

El artículo 35, literal b, establece el deber de "respetar y hacer respetar todas las disposiciones legales y denunciar sus transgresiones", lo cual refuerza la obligación moral y legal de no ser parte de actividades contrarias al orden jurídico, sin importar el beneficio económico ofrecido. (Copnia, 2003)

En el artículo 37, literal d, establece “respetar y reconocer la propiedad intelectual de los demás profesionales sobre sus diseños y proyectos”. El contrato menciona la prohibición de informar ante la ley la apropiación de información de terceros lo cual vulnerara lo descrito en este artículo. (Copnia, 2003)

El artículo 38, literal a, indica la prohibición a “utilizar sin autorización de sus legítimos autores y para su aplicación en trabajos profesionales propios, los estudios, cálculos, planos, diseños y software y demás documentación perteneciente a aquellos, salvo que la tarea profesional lo requiera, caso en el cual se deberá dar aviso al autor de tal utilización”. Este artículo al igual que el anterior conlleva a no reconocer a los propietarios legítimos de la información obtenida. (Copnia, 2003)

Y finalmente en el artículo 43, literal a, menciona que “los profesionales que se dispongan a participar en un concurso o licitación por invitación pública o privada y consideren que las bases pudieren transgredir las normas de la ética profesional, deberán denunciar ante el Consejo Profesional respectivo la existencia de dicha transgresión”. Lo cual me permite denunciar el ofrecimiento realizado por SecureNova Labs. (Copnia, 2003)

Dicho lo anterior la decisión de rechazar la oferta de los 15 millones de pesos, no tiene una base económica si no el deber ético que tengo como ingeniero el cual me lleva a actuar con honestidad y respeto por la ley y aceptar esta oferta no solo compromete mi integridad como profesional si no también la dignidad de la ingeniería como profesión.

Analice el caso problema "Ciber espionaje y Ética en SecureNova Labs" (Anexo 2 - Escenario 2), y desarrolle una redacción los interrogantes:

¿Las empresas de ciberseguridad que tanto acceso deben tener a la información sensible de cada uno de sus clientes y de qué forma es posible garantizar que el acceso no sea usado de manera incorrecta?

El acceso a información sensible por parte de una empresa de ciberseguridad durante una auditoría debe limitarse estrictamente al principio de necesidad operacional. Esto significa que solo se debe acceder a los datos indispensables para cumplir los objetivos definidos en el alcance del proyecto, sin exceder los límites técnicos, legales ni éticos establecidos por el cliente y la normativa vigente.

Para aumentar su nivel de seguridad y evitar que la información sea usada de manera indebida, las organizaciones deben implementar controles técnicos y administrativos sólidos, como pueden ser:

Segmentación de privilegios, registro y monitoreo de actividades, entornos controlados de prueba, cláusulas contractuales específicas y auditorías cruzadas o revisiones de terceros.

¿De qué manera se puede evitar que los empleados usen herramientas de ciberseguridad avanzadas con fines no autorizados?

Las empresas de ciberseguridad pueden y necesitan acceder a información sensible solo a netamente necesario para cumplir el alcance de la auditoría o servicio. El acceso debe basarse en mínimos permisos, propósito documentado y consentimiento informado del cliente.

Y para garantizar su uso legítimo deberían cumplirse algunas condiciones como: definición clara de alcance, usar en lo posible datos que sean copias de los reales, asignación de permisos mínimos, realizar las pruebas en ambientes controlados, toda actividad realizada debe

quedar documentada con los tiempos en el que se realiza cualquier acción, revisión del contrato por parte del área legal antes de proceder con cualquier actividad y la transparencia con el cliente.

¿Cuál debería ser la respuesta tanto de gobiernos como organizaciones al descubrir que una empresa de ciberseguridad la cual fue contratada cometió actos de ciber espionaje?¿De qué manera se puede restaurar la confianza y asegurar que este tipo de incidente no se repita?

Realizar una contención técnica, donde involucre, desconectar, aislar y preservar evidencias; evitar que se borren logs o se destruya cualquier información que será clave para la investigación posterior.

Se debe llevar a cabo una investigación forense, acá se debe contratar un tercero imparcial para auditar el alcance del incidente y se debe separar la investigación legal de la correctiva.

Se debe realizar la notificación a autoridades competentes, denunciando formalmente ante las autoridades regulatorias.

Se deben suspender los accesos que tiene la empresa implicada, revocando las credenciales y acceso a las infraestructuras críticas.

Y se debe tener una comunicación transparente e informar a los clientes y partes afectadas con hechos confirmados sin la necesidad de revelar información sensible y ofrecer medidas de mitigación y canales de apoyo.

Las medidas que deberían tomarse abarcan:

El aplicar penalidades contractuales, reclamar responsabilidad civil por daños y apoyar procedimientos penales si corresponde.

Se deben exigir auditorías externas, rectificación de controles y certificaciones previas a cualquier recontratación.

Realizar revisiones regulatorias ya que el regulador puede imponer condiciones administrativas, multas o inhabilitaciones para operar en ciertos contratos.

Seguro y compensación a víctimas, activando coberturas de seguro cibernético y definiendo esquemas de compensación para afectados.

Incorporar cláusulas más estrictas (derecho de auditoría, supervisión en vivo, control de acceso federado, retención de logs en custodia del cliente).

Publicar los resultados de la investigación (respetando límites legales) y un plan de remediación verificable por terceros.

ETAPA 3: Componente práctico

Que herramientas de software utilizó para el desarrollo del escenario 3, descríbalas y adjunte la evidencia de los comandos usados, dichas herramientas deben seguir la clasificación según los pasos del pentesting.

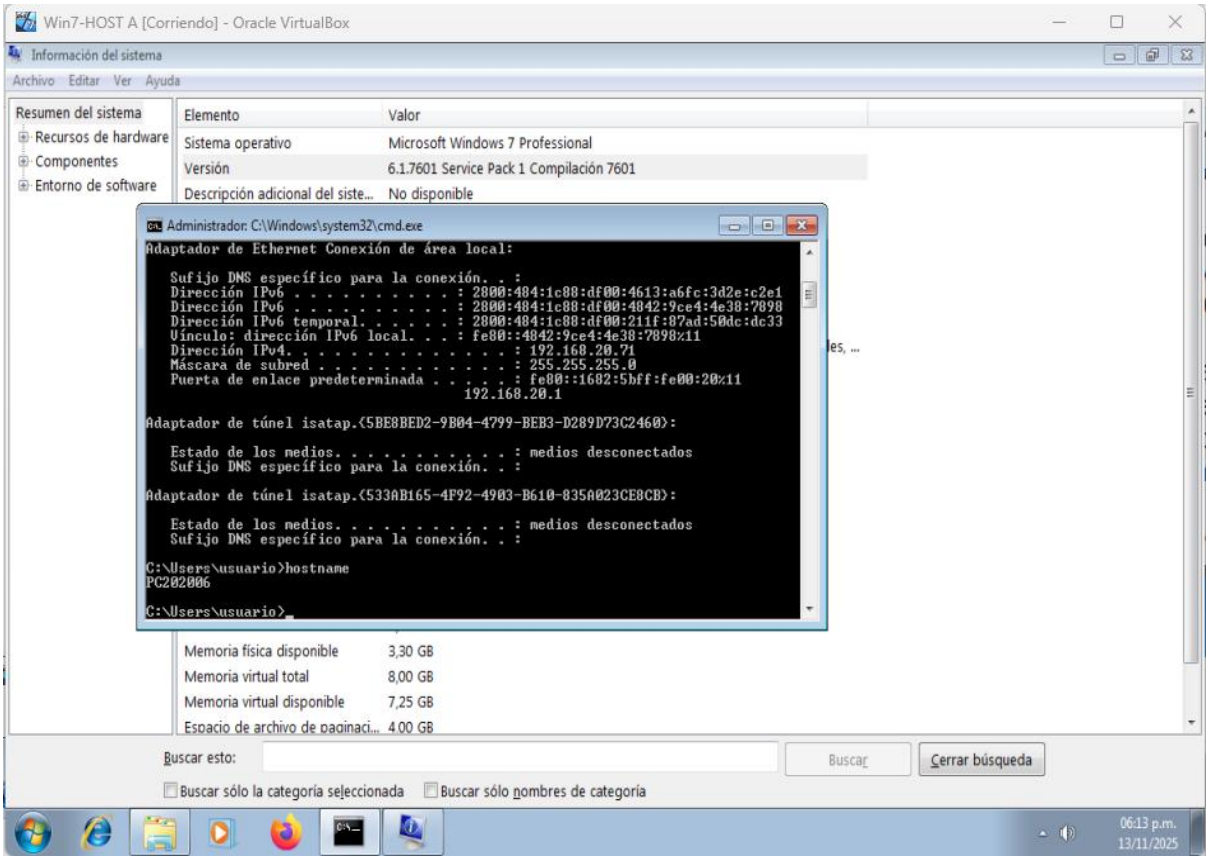
Recolección de información (Reconocimiento)

En la fase inicial se realizó un primer acercamiento desde el equipo atacante, ejecutando Parrot OS dentro del laboratorio. Durante esta exploración se identificó un dispositivo activo en la red interna con dirección IP 192.168.20.71, correspondiente a un sistema operativo Windows 7 Professional (versión 6.1.7601).

Para efectos del ejercicio, este sistema será referido como HOST A

Figura 9

Comprobación direccionamiento IP en el HOST A



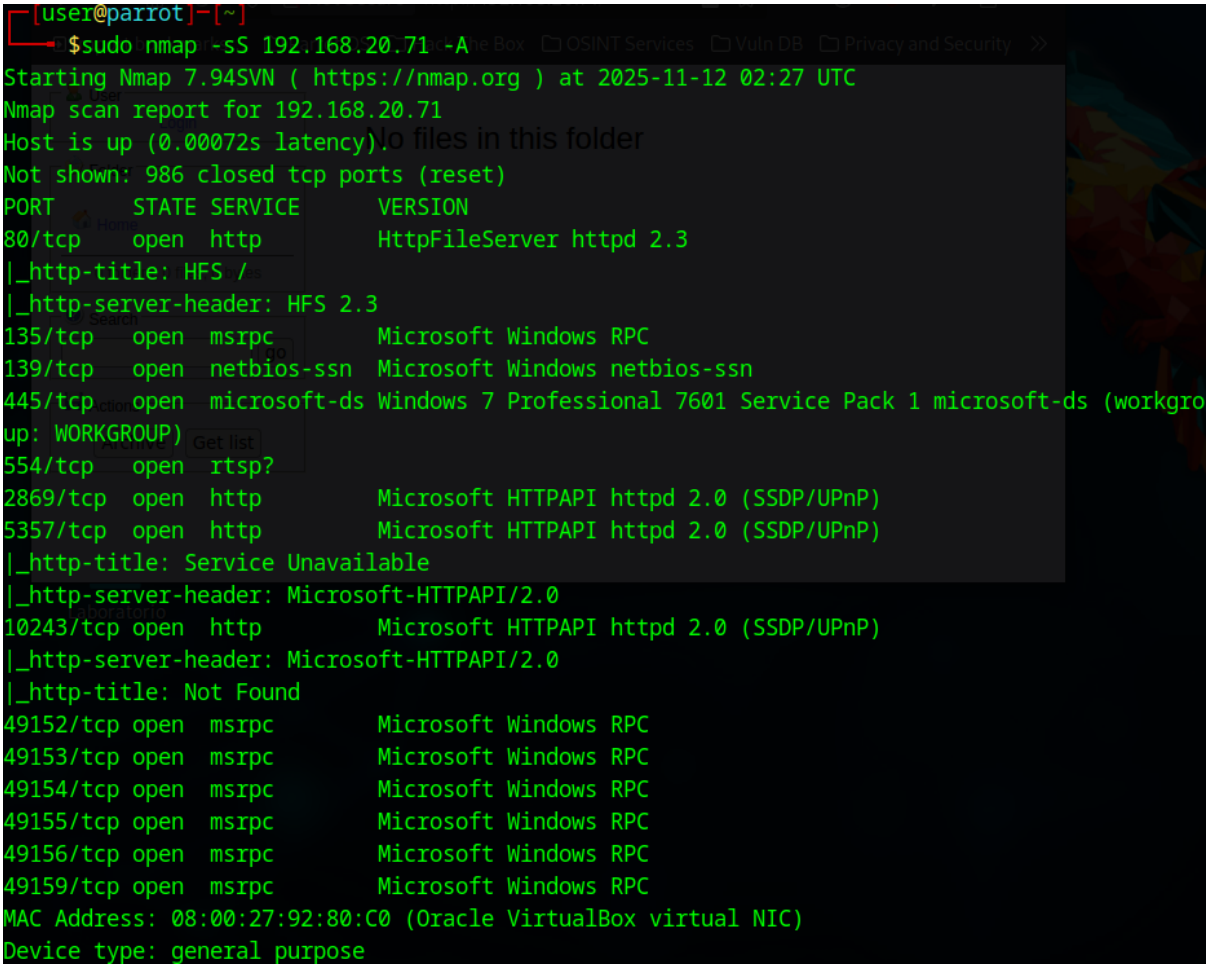
Nota. Autoría propia, se confirma que el direccionamiento IP en el HOST A este dentro del segmento de red asignado.

Enumeración

Posteriormente, desde el equipo atacante se utilizó la herramienta Nmap con el fin de identificar servicios expuestos en el HOST A. El análisis permitió descubrir puertos abiertos y aplicaciones en ejecución que podrían representar puntos de entrada para el laboratorio. Esta información resulta clave para orientar las etapas posteriores del ejercicio ofensivo.

Figura 10

Escaneo desde el equipo atacante al HOST A



Nota: Autoría propia, se realiza escaneo al HOST A usando el comando NMAP desde nuestra máquina atacante.

Análisis de vulnerabilidades

Tomando como referencia la documentación proporcionada para el desarrollo del laboratorio y los resultados obtenidos durante su ejecución, en la enumeración se identificó que el HOST A ejecuta Rejetto HFS versión 2.3, la cual presenta una vulnerabilidad conocida que permite ejecución remota de código.

Dicha falla ha sido catalogada como un riesgo crítico y está documentada en reportes públicos de seguridad, como el emitido por INCIBE-CERT.

Figura 11

Comprobación del CVE detectado durante el escaneo

Nota: Fuente INCIBE https://www.incibe.es/index.php/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-6287

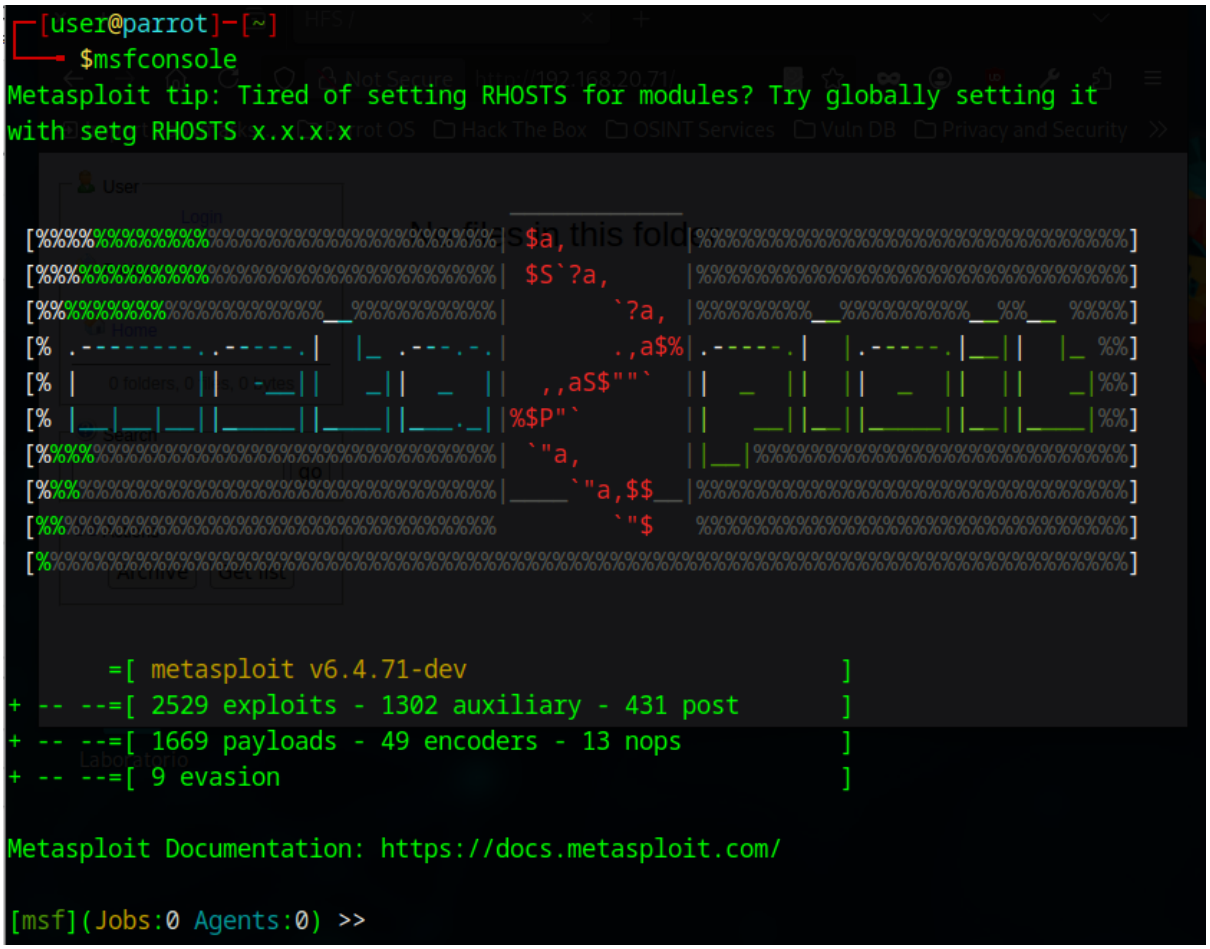
Explotación

Para aprovechar esta vulnerabilidad dentro del entorno controlado, se utilizó Metasploit Framework, herramienta diseñada para realizar pruebas de penetración en laboratorios autorizados.

A través del módulo correspondiente a Rejetto HFS, se estableció una sesión remota con el HOST A, permitiendo obtener acceso en el contexto del usuario vulnerable de la máquina objetivo.

Figura 12

Ejecutando por primera vez el Metasploit sobre el HOST A.

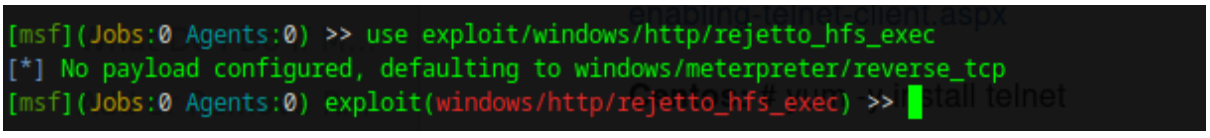


Nota. Autoría propia, se realiza el lanzamiento Metasploit para aprovechar la vulnerabilidad detectada en el HOST A.

Hacemos uso de alguno de los exploit disponibles con el comando use/exploit/windows/http/rejetto_hfs_exec

Figura 13

Llamando el exploit: exploit/windows/http/rejetto_hfs_exec

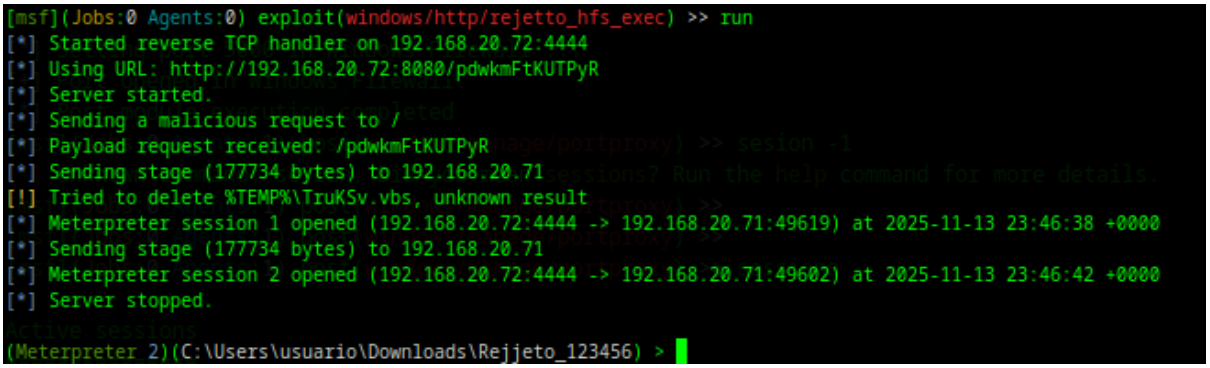


Nota. Autoría propia lanzando el comando del exploit para poder configurarlo antes de lanzarlo sobre el HOST A, que es nuestra máquina objetivo.

El cual con el comando run se ejecuta y permite la conexión con el HOST A

Figura 14

Ejecutando exploit rejetto_hfx_exec



Nota. Autoría propia, posterior a su configuración el exploit se ejecuta para que alcance el HOST A, que es nuestra máquina objetivo.

Escalada de privilegios

Con la sesión activa, se habilitó un entorno interactivo mediante Meterpreter, lo cual permitió ejecutar funciones avanzadas sobre el sistema comprometido.

Desde esta posición, se verificaron opciones de interacción, reconocimiento interno y gestión de usuarios, incluyendo acciones como la creación de cuentas locales y su asignación a grupos de privilegios elevados dentro del entorno exclusivo del laboratorio.

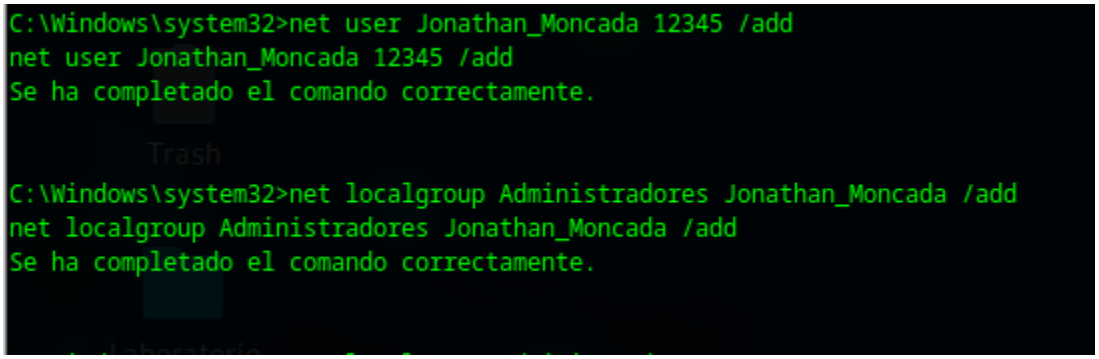
Algunos de los comandos que pueden ser ejecutados para elevar privilegios:

net user Jonathan_Moncada 12345 /add –> que nos permite crear usuarios

net localgroup Administradores → el cual nos permite agregar el usuario al grupo de administradores locales de la máquina objetivo.

Figura 15

Muestra del escalamiento de privilegios luego de la explotación



Nota. Autoría propia, tras lograr la conexión hacia nuestra máquina objetivo final, se comprueba que se puede realizar un escalamiento de privilegios creando un usuario administrador local en la máquina.

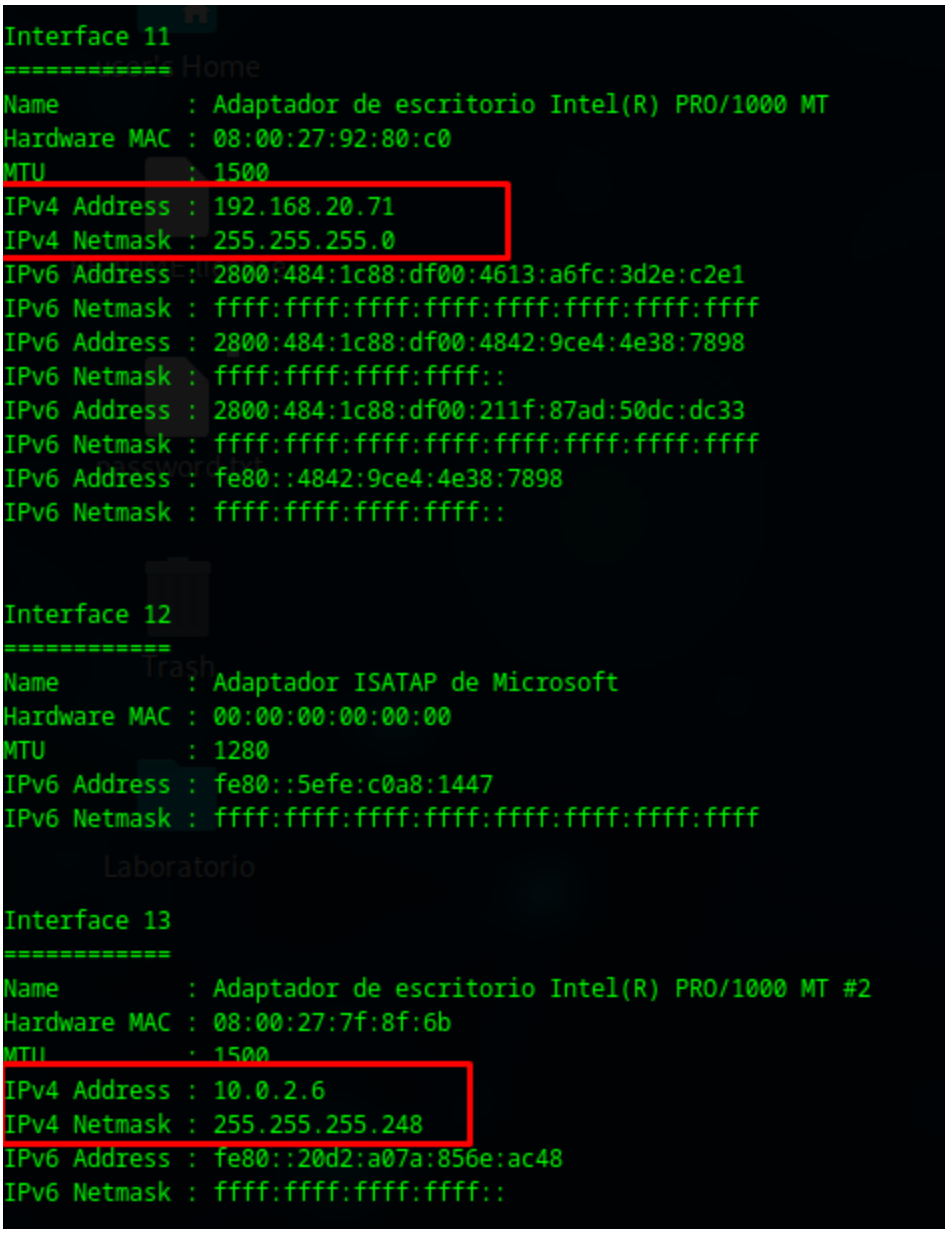
Movimiento lateral / Persistencia

Una vez dentro del HOST A, se identificó que el sistema posee múltiples interfaces o rutas de red disponibles.

Esto sugiere que podría actuar como punto de pivote (pivoting) hacia otros dispositivos del entorno, lo cual abriría la posibilidad de explorar redes adicionales o establecer mecanismos de persistencia, siempre dentro de las limitaciones y autorizaciones del laboratorio.

Figura 16

Sacando el IPCONFIG del HOST A por medio del Shell desde la máquina atacante



Nota. Autoría propia, tras poder ingresar a nuestra primera máquina aprovechando su vulnerabilidad podemos ver que esta tiene alcance a otras redes lo que nos permite crear ataques de movimiento lateral hacia otras redes que no vemos desde el equipo atacante.

Esto lo podemos aprovechar para escalar si queremos generar una persistencia usando el HOST A como pivoting hacia otros dispositivos.

Documentación y Reporte

1. Registro de actividades

Durante el laboratorio se llevó una bitácora en la que se consignaron las acciones principales realizadas, indicando:

Noviembre 13 del 2025

Se utilizo un equipo con Windows 10, 32 en RAM y 2 teras en disco duro sobre el cual se realizó el montaje de las máquinas virtuales que permitieron la ejecución del laboratorio

Objetivo observable de cada fase

Recolección de información (Reconocimiento

Objetivo:

Identificar qué equipos están activos en la red y obtener información básica del sistema objetivo.

Resultado observable:

Se detecta un equipo activo con IP 192.168.20.71.

Se identifica que ejecuta Windows 7 Professional.

El dispositivo se clasifica como HOST A.

Enumeración

Objetivo:

Descubrir los puertos abiertos, servicios activos y características técnicas del HOST A.

Resultado observable:

El escaneo muestra que el HOST A tiene servicios accesibles desde la red interna.

Se identifica la presencia del servidor Rejetto HFS.

Se observan puertos abiertos que confirman exposición innecesaria.

Análisis de vulnerabilidades

Objetivo:

Determinar si los servicios detectados presentan fallas conocidas que pueden ser explotadas.

Resultado observable:

Se confirma que Rejetto HFS 2.3 es vulnerable a ejecución remota de código (CVE publicado).

La aplicación vulnerable coincide con información suministrada en la guía del laboratorio.

Explotación

Objetivo:

Aprovechar la vulnerabilidad identificada para obtener acceso remoto autorizado dentro del laboratorio.

Resultado observable:

Se logra establecer una sesión remota con el HOST A mediante Metasploit.

El sistema responde y permite ejecutar acciones en el contexto del usuario víctima.

El atacante obtiene un canal de comunicación activo.

Escalada de privilegios

Objetivo:

Obtener privilegios más altos dentro del HOST A para tener mayor control del sistema.

Resultado observable:

Meterpreter permite interactuar con funciones avanzadas del sistema.

Se pueden consultar configuraciones del equipo, listar usuarios y ejecutar comandos.

Se demuestra la posibilidad de manipular cuentas (crear, listar o asignar permisos) dentro del laboratorio.

Movimiento lateral / persistencia

Objetivo:

Explorar si el HOST A puede utilizarse como punto de pivote hacia otras redes o sistemas internos.

Resultado observable:

HOST A revela la existencia de más de una interfaz o ruta de red.

Se verifica la posibilidad de usarlo como puente hacia otros equipos.

Se evidencia que un atacante podría permanecer o escalar su posición en un entorno real si no existieran controles adecuados.

2. Evidencias recopiladas

A lo largo de cada fase se capturaron pantallas y datos relevantes para sustentar los hallazgos, entre ellos:

Identificación del HOST A y su dirección IP.

Resultados del escaneo de servicios visibles en la red interna.

Información sobre la vulnerabilidad detectada en Rejetto HFS.

Evidencias del acceso a información del sistema comprometido.

Estas evidencias se almacenaron de forma ordenada y se adjuntaron para consulta.

3. Análisis de hallazgos

El análisis se centró en tres puntos clave:

Exposición innecesaria de servicios vulnerables, como Rejetto HFS 2.3.

Debilidad por desactualización del sistema operativo, lo cual incrementa la superficie de ataque.

Posibilidad de movimiento lateral, evidenciada por la presencia de múltiples rutas de red desde el HOST A.

El impacto potencial de estas debilidades fue clasificado como alto dentro del contexto del laboratorio.

4. Recomendaciones derivadas

Como resultado de la revisión técnica se emitieron las siguientes recomendaciones:

Retirar o actualizar aplicaciones vulnerables.

Migrar hacia sistemas operativos soportados y actualizados.

Restringir el acceso a puertos y servicios que no sean estrictamente necesarios.

Implementar controles de monitoreo, roles y privilegios mínimos.

Segmentar la red para limitar el alcance de un posible compromiso.

Estas medidas buscan prevenir escenarios similares en entornos reales.

5. Conclusión del reporte

La documentación generada proporciona una visión clara de cómo un sistema vulnerable puede ser comprometido mediante un proceso estructurado de pentesting. El registro, las evidencias y las recomendaciones resultan útiles para fortalecer las capacidades de defensa y comprender de manera práctica la importancia de minimizar la superficie de ataque.

Describa los datos e información escenario 3 que fueron de utilidad identificar el fallo de seguridad específico sobre el cual puede atacar al host A.

El anexo 4 proporcionó información clave para reconstruir el incidente y entender cuál fue el fallo de seguridad que permitió comprometer la Máquina 1 (Host-A).

El anexo señalaba que la estación Windows comprometida tenía instalada una aplicación con historial de fallas de seguridad y que probablemente había sido el punto inicial de

explotación. Esto me permite centrar el análisis en un componente específico, reduciendo el alcance de investigación y orientando la búsqueda hacia aplicaciones conocidas por permitir ejecución de código o abuso remoto.

La imagen forense indicaba que el sistema había recibido comandos no generados por el usuario legítimo, lo que apuntaba a la presencia de una sesión remota activa durante el incidente. La presencia de ejecución de comandos de forma externa confirma que el atacante no solo accedió al sistema, sino que logró interacción directa con el sistema operativo.

El anexo mencionaba que se detectó un usuario nuevo incorporado al grupo de administradores locales sin justificación operativa. Este hallazgo demuestra que, después de obtener acceso inicial, el atacante realizó escalamiento de privilegios, lo cual encaja con el comportamiento que normalmente sigue una explotación real. También es una señal clara de persistencia o preparación para movimiento lateral.

El anexo señalaba una actividad lateral desde Host-A hacia un servidor secundario, lo cual coincidía con patrones típicos de pivoting. Esto permitió entender que la intrusión no se limitó al equipo inicial, sino que el atacante utilizó Host-A como plataforma de salto para alcanzar otros sistemas más valiosos.

¿Con que herramienta logro identificar el fallo de seguridad del host A? ¿Qué puerto se muestra abierto por la aplicación Rejetto?

Desde el equipo con sistema operativo Parrot OS se usó la herramienta NMAP la cual es usada para el escaneo de redes y descubrir en ellas los dispositivos, puertos y servicios que en estos se estén ejecutando.

Con el comando sudo nmap -sS 192.168.20.71 -A se hace un escaneo sobre el equipo HOST A y este nos trae la información relacionada con el fallo de seguridad el cual se ejecuta sobre el puerto 80 y nos permite hacer la explotación sobre el mismo.

Figura 17

Escaneo de puertos sobre la 192.168.20.71 para ver los puertos activos generados por la utilización del Rejetto V2.3

Nota. Autoría propia, se realiza el escaneo con Nmap para validar los puertos abiertos sobre la máquina objetivo.

Diseñe un gráfico para explicar el ataque y explique cómo el mismo afecta a las máquinas con sistema operativo Windows.

Durante el laboratorio se simuló un ataque paso a paso para entender cómo un sistema Windows puede ser comprometido. En la red que fue atacada tenía Windows 7 en sus dos equipos objetivos, lo que hoy ya es un sistema viejo que ya no recibe actualizaciones y lo hace más vulnerable.

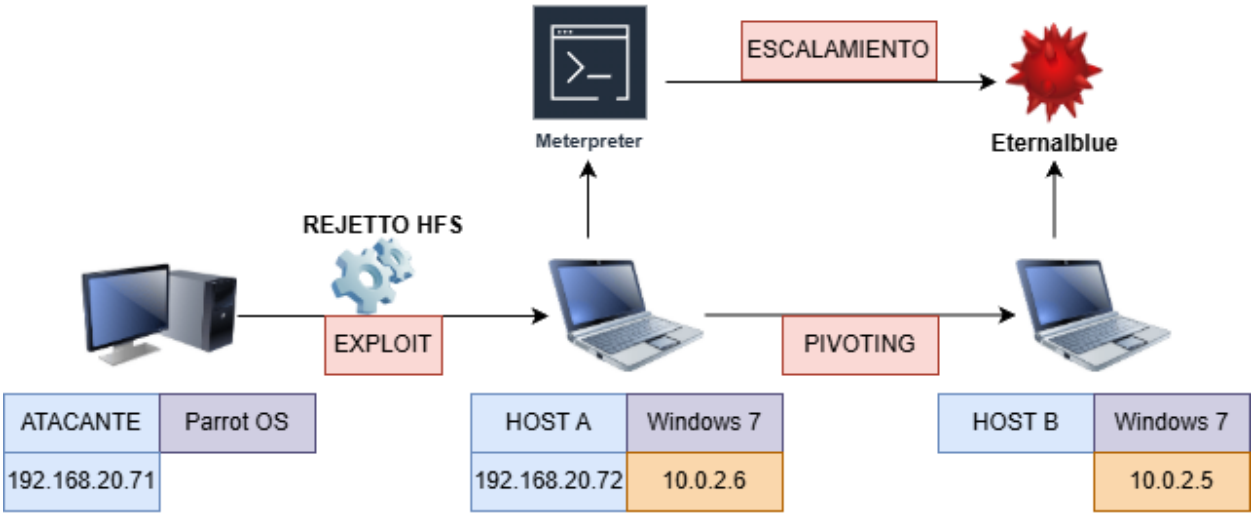
Sumado a lo ya mencionado, el uso de herramientas que son conocidas por tener fallas de exposición no debería permitirse, ya que aumenta el nivel de riesgo de los sistemas como en este caso el equipo Windows HOST A que tenía la aplicación Rejett V2.3. Esto abre la puerta al atacante para que pueda en esta máquina ver todo tipo de información y ejecutar comandos en el mismo sin ningún problema y para finalizar siendo aún más grave para la red, el atacante tiene la

posibilidad de ver todo en el equipo y esto incluye todos los equipos que hagan parte de las redes a las que el equipo infectado tenga alcance, permitiéndole realizar ataques de movimiento lateral y como lo logramos demostrar, poder ejecutar comandos sin ningún tipo de restricción.

Al final esto se resume en aumento en la vulnerabilidad de las máquinas Windows si no están actualizadas, fácil control por medio de servicios inseguros, solo se requiere un solo equipo comprometido para poner en riesgo toda la red y que, si el ataque cuenta con el conocimiento, puede alojarse en el sistema el tiempo que lo desee sin ser detectado.

Figura 18

Diagrama del ataque



Nota. Autoría propia, se muestra el diseño de cómo se estaba ejecutando el ataque.

Describa el paso a paso de lo ejecutado para validar la vulnerabilidad del host A sin dejar de lado el cómo logro hacer el pivoting hacia el host B.

Luego de realizado el análisis forense se tienen identificadas la máquina atacante con la IP 192.168.20.72 y el primer equipo denominado HOST A con la IP 192.168.20.71 con una

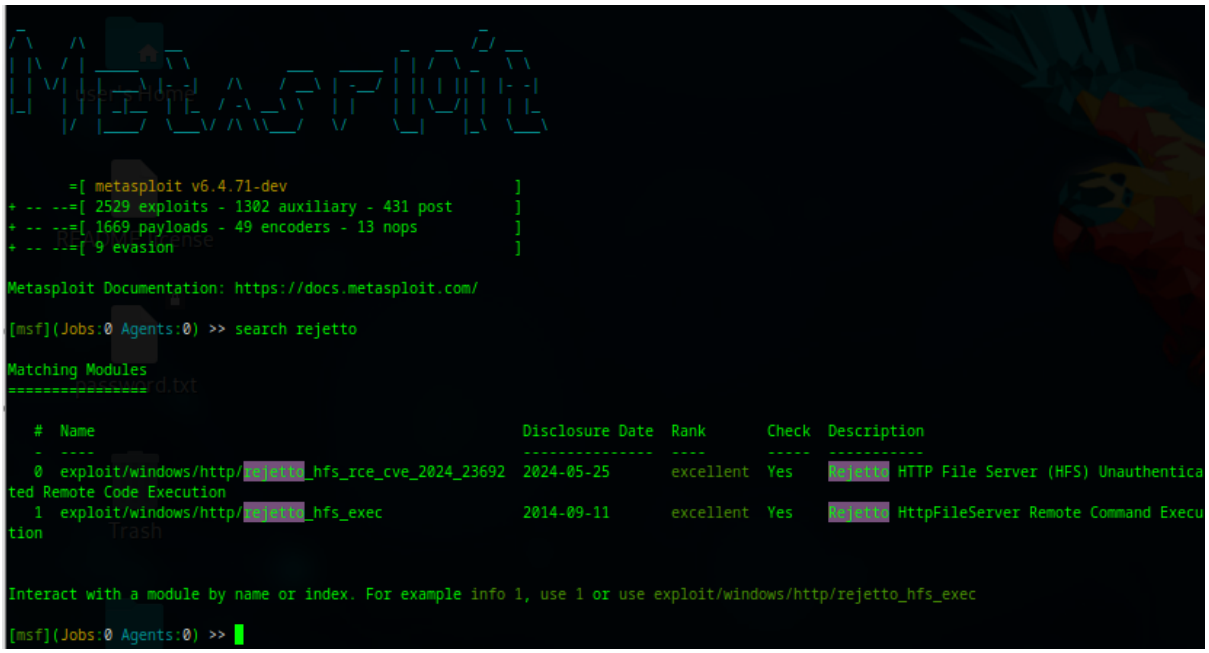
vulnerabilidad por el puerto 80 generada por la utilización del programa Rejetto V2.3, que será nuestro equipo Pivot para encontrar el siguiente dispositivo.

Lo primero será iniciar la herramienta Metasploit con el comando msfconsole y posterior a su arranque podemos identificar que exploits están disponibles para usar.

Usamos el comando *search Rejetto* y veremos las opciones disponibles

Figura 19

Uso del Metasploit para buscar las vulnerabilidades asociadas al uso del Rejetto



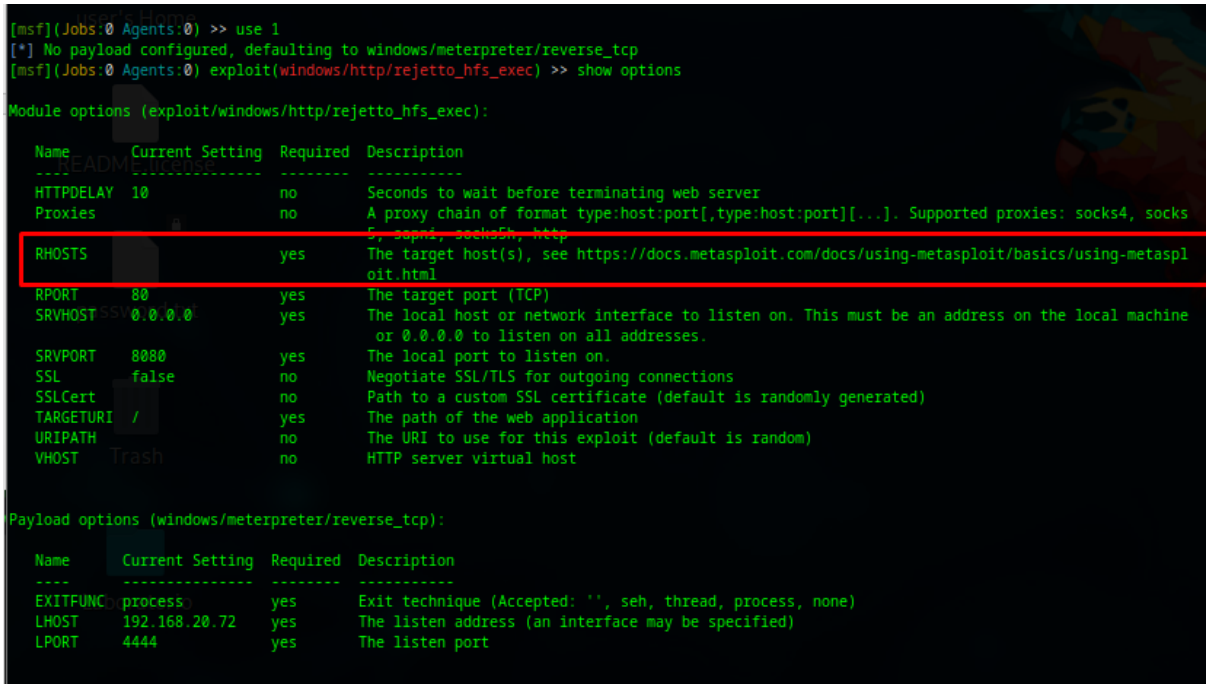
Nota. Autoría propia, ejecución del Metasploit e identificación de exploit disponibles relacionadas con Rejetto

Ahora de ver estas dos opciones disponibles seleccionamos la opción que deseamos probar, para este evento usaremos el exploit “exploit/Windows/Rejetto_hfs_exec” y lo podemos lanzar con 2 comandos y cualquiera es funcional:

Use 1 (el 1 hace referencia al identificador del exploit) o con el comando *use exploit/Windows/Rejetto_hfs_exec*, posterior a su ejecución lanzamos el comando *show options* para ver qué debemos configurar en el exploit y poder ejecutarlo hacia el HOST A.

Figura 20

Uso del módulo Windows/http/rejetto_hfs_exec y el comando show options

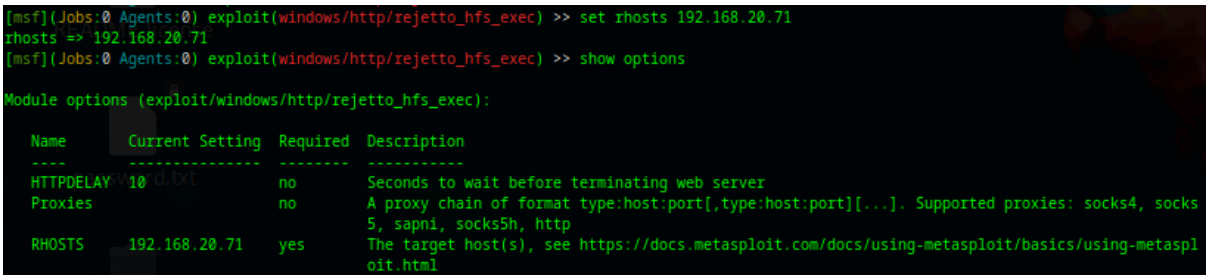


Nota. Autoría propia, se ejecuta dentro del Metasploit el exploit que vamos a usar y se configura para que alcance nuestra primer maquina objetivo.

Como se muestra en la imagen anterior, el único dato que vamos a necesitar para esta prueba es el host objetivo (RHOSTS), el cual agregamos escribiendo el comando *set RHOSTS 192.168.20.71* y confirmamos que quedará guardado escribiendo nuevamente *show options*.

Figura 21

Parámetros de configuración el módulo Windows/http/rejetto_hfs_exec

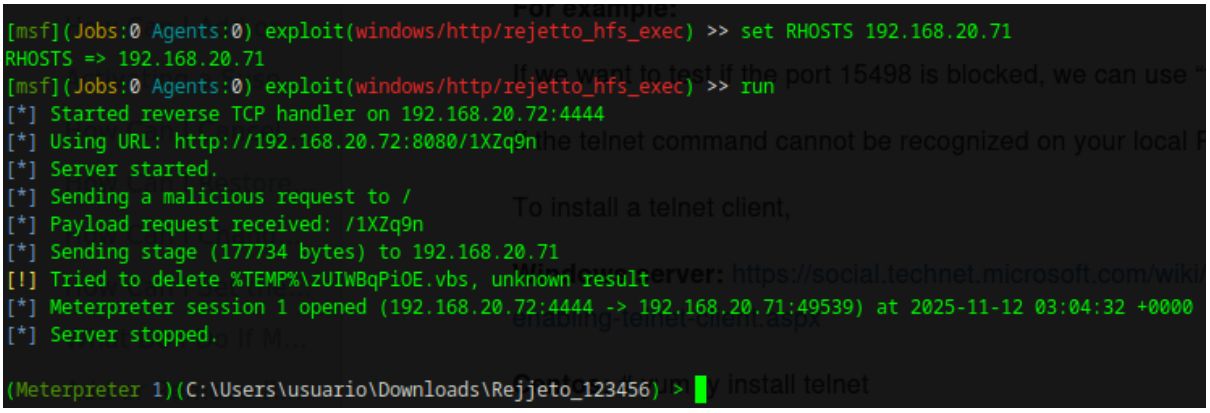


Nota. Autoría propia, se debe confirmar que los datos obligatorios dentro de los campos de configuración estén con información relevante para nuestro ataque como las direcciones IP.

Ya luego de guardados los cambios, ejecutamos el comando *run* para ejecutar el exploit y si está configurado correctamente este generará la conexión con el equipo HOST A.

Figura 22

Ejecución del módulo Windows/http/rejetto_hfs_exec y conexión al HOST A desde la máquina atacante



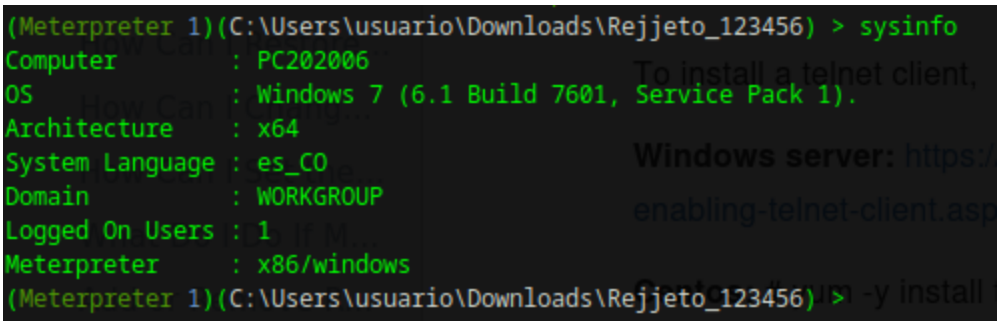
Nota. Autoría propia, se puede confirmar que la conexión se generó correctamente con la apertura de la sesión del Meterpreter sobre una ubicación distinta.

Ya una vez conectados al HOST A podemos tener acceso la consola de la máquina escribiendo el comando escribiendo *Shell* y desde allí lanzar algunos comandos básicos pero que nos ayudaran a confirmar que estamos en la ubicación que queremos estar que es el HOST A.

Algunos de estos comandos que nos ayudan con la validación es el comando *sysinfo* el cual nos deja ver la información del equipo al que nos hemos conectado.

Figura 23

Comando sysinfo para confirmar la máquina en la que estamos conectados

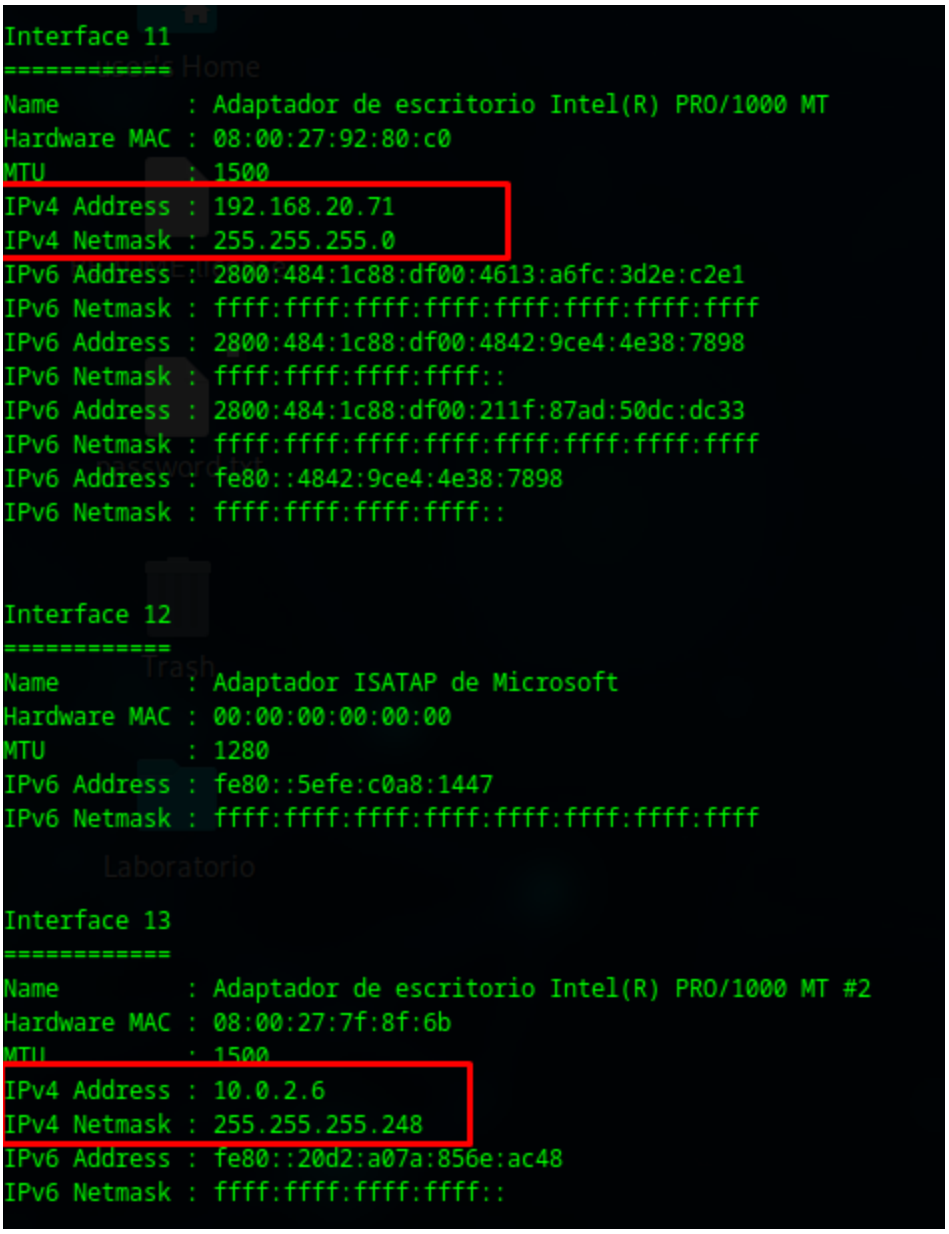


Nota. Autoría propia, el comando nos trae la información básica del equipo como el sistema operativo, el dominio en el que esta la máquina y la cantidad de usuarios logueados en el momento.

Y también podemos lanzar un *ipconfig* y ver la configuración de IP que tiene el HOST A

Figura 24

Validando las IPS que toma el HOST A, por medio del Shell que se abre al conectarse desde la máquina atacante



Nota. Autoría propia, como parte de las validaciones esenciales es confirmar la dirección IP que está tomando esa máquina, y podemos ver que efectivamente está tomando la IP 192.168.20.71, lo que nos dice que si hicimos nuestro primer ataque de manera correcta.

Como vemos en la imagen anterior tenemos dos direcciones IP en el HOST A, esto quiere decir que no solo este equipo tiene alcance a la red 192.168.20.0/24 sino que además hace

parte de una red 10.0.2.0/29 a la que seguramente también tiene alcance y debemos validar si vemos algo sobre esta red.

Descripción del Pivoting

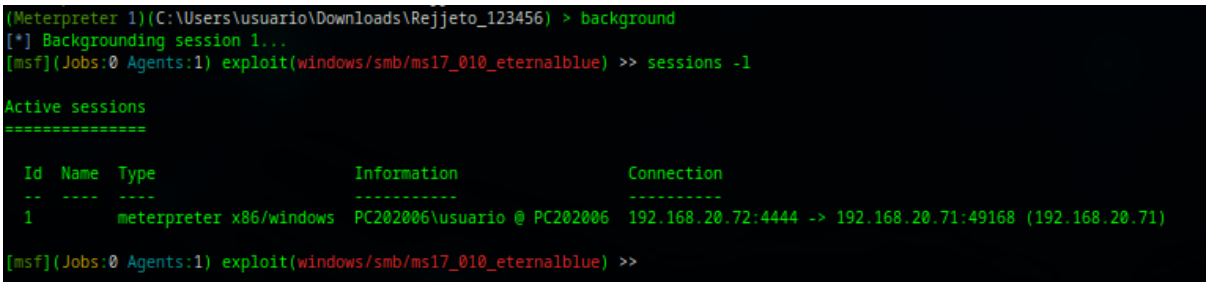
Lo primero es entender que el pivoting se refiere a la posibilidad que tiene un atacante de saltar de una red a otra, aunque desde la suya no lo lograra hacer y para esto existen posiblemente varias maneras las cuales se van descubriendo en la medida en que se va desarrollando el ataque o el ejercicio controlado.

Ahora continuando con el ejercicio lo que podemos hacer para poder detectar si hay más equipos en la red es buscar la forma de lanzar sobre esa red un escaneo de esta y para esto aprovecharemos las herramientas que nos brinda en Metasploit, como primera medida nos saldremos de la sesión actual generada al HOST A por medio del Meterpreter y esto lo haremos sin cerrar la sesión, esto lo haremos con el comando *background*.

Para confirmar las sesiones activas podemos escribir el comando *sessions -l*

Figura 25

Background para salir de la sesión activa sin cerrarla

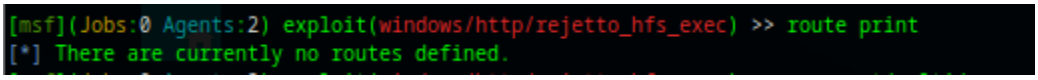


Nota. Autoría propia, debemos volver a la sesión del Metasploit para allí buscar módulos que nos permitan continuar con nuestro ataque y el comando *sessions -l* podemos validar las sesiones activas del Meterpreter.

Ahora vamos a ver las rutas que ve el equipo atacante con el comando *route print*.

Figura 26

Validando las rutas que reconoce el equipo atacante

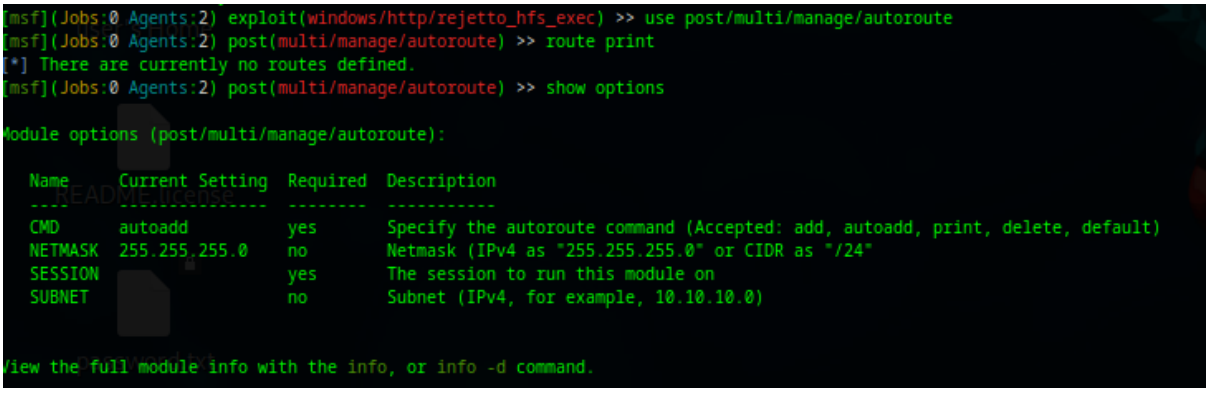


Nota. Autoría propia, comandos que nos ayudan a ver que estamos alcanzando a detectar desde nuestra maquina atacante.

Como vemos no se muestra nada y es porque solo tenemos alcance a lo que conoce el equipo, acá es donde usaremos las bondades del pivote para lograr alcanzar el segmento 10.0.2.0/29 desde nuestro equipo atacante por medio del HOST A. Y para lograr hacer esto usaremos un módulo que nos permitirá cargar la nueva ruta que solo estamos viendo a través del HOST A, el comando para llamar este módulo es *use post/multi/manage/autoroute*

Figura 27

Uso del módulo post/multi/manage/autoroute

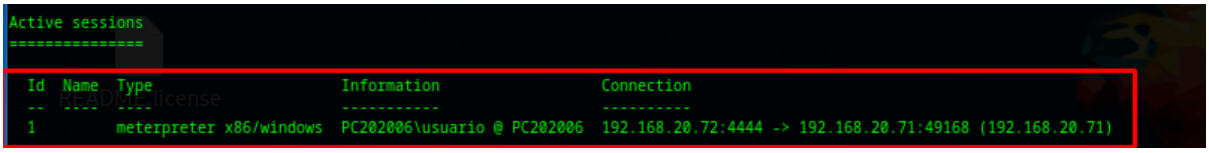


Nota. Autoría propia, lanzamos el módulo de Metasploit que nos permitirá agregar las rutas desconocidas pero alcanzables desde nuestro equipo atacante.

Con *show options* vemos las opciones que debemos y las que podemos agregar adicionales que no son obligatorias, ya que este módulo agrega las rutas automáticamente el único valor que nos pide obligatorio es la SESSION, el cual podemos confirmar con el comando *sessions -l.*

Figura 28

Confirmando las sesiones activas

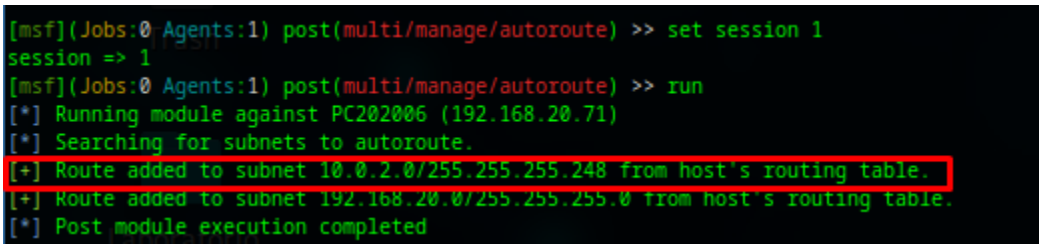


Nota. Autoría propia, confirmando que la sesión abierta por medio de Meterpreter y que es la sesión que usaremos para realizar el agregado de las rutas siga activa.

Escribimos *set SESSION 1* para asignar el dato que nos pide el módulo y posterior el comando *run* para ejecutarlo y vemos que nos carga las dos rutas, 192.168.20.0/24 y la ruta que no veíamos si no solo desde el HOST A 10.0.2.0/29

Figura 29

configuración del módulo multi/manage/autoroute

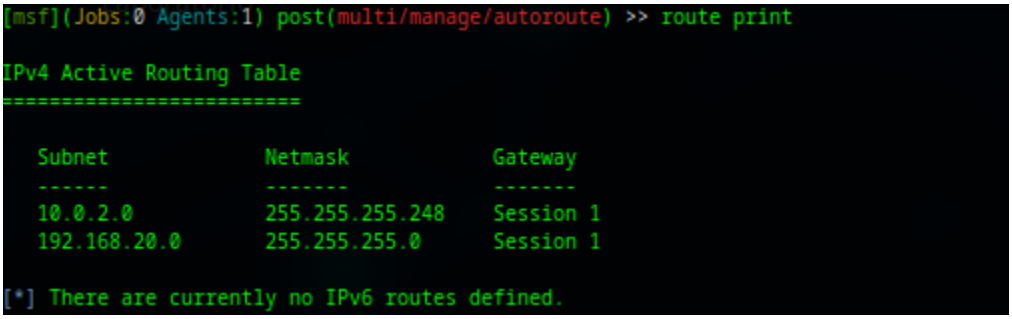


Nota. Autoría propia, se agregan las rutas por medio del módulo de Metasploit lo que nos permitirá alcanzar la red que anteriormente era desconocida y la cual encontramos gracias al primer equipo atacado.

Con el comando *route print* podemos ver las rutas aprendidas y como estas tienen como Gateway la sesión que seleccionamos para llamarlas poderlas aprender en el equipo atacante.

Figura 30

route print para validar las rutas aprendidas.



Nota. Autoría propia, confirmando que desde el equipo atacante ahora si alcanza a ver la ruta que aprendimos gracias a la técnica de pivoting ejecutada.

Ahora para poder ver qué equipos están en ese segmento de red 10.0.2.0/29 vamos a cargar un módulo nuevo con el comando *use post/windows/gather/arp_scanner*. Y con el *show options* vemos las opciones que necesitamos diligenciar para ejecutar el módulo, que para este caso son el RHOST con su máscara y la sesión que usamos del meterpreter.

Figura 31

Uso del módulo post/Windows/gather/arp_scanner

```
[msf](Jobs:0 Agents:2) post(multi/manage/autoroute) >> use post/windows/gather/arp_scanner
[msf](Jobs:0 Agents:2) post(windows/gather/arp_scanner) >> show options

Module options (post/windows/gather/arp_scanner):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   SESSION                   yes       The session to run this module on
   THREADS  10               no        The number of concurrent threads


View the full module info with the info, or info -d command.
```

Nota. Autoría propia, sin la información necesaria requerida la ejecución de los módulos no es posible.

Acá nos mostrará la información de los equipos conectados en esa red.

Figura 32

Ejecución del módulo Windows/gather/arp_scanner

```
[msf](Jobs:0 Agents:1) post(windows/gather/arp_scanner) >> set rhosts 10.0.2.0/29
rhosts => 10.0.2.0/29
[msf](Jobs:0 Agents:1) post(windows/gather/arp_scanner) >> set session 1
session => 1
[msf](Jobs:0 Agents:1) post(windows/gather/arp_scanner) >> run
[*] Running module against PC202006 (192.168.20.71)
[*] ARP Scanning 10.0.2.0/29
[+]     IP: 10.0.2.1 MAC 52:55:0a:00:02:01 (UNKNOWN)
[+]     IP: 10.0.2.3 MAC 08:00:27:35:f7:71 (CADMUS COMPUTER SYSTEMS)
[+]     IP: 10.0.2.5 MAC 08:00:27:92:80:c0 (CADMUS COMPUTER SYSTEMS)
[+]     IP: 10.0.2.6 MAC 08:00:27:7f:8f:6b (CADMUS COMPUTER SYSTEMS)
[+]     IP: 10.0.2.7 MAC 08:00:27:7f:8f:6b (CADMUS COMPUTER SYSTEMS)
[*] Post module execution completed
[msf](Jobs:0 Agents:1) post(windows/gather/arp_scanner) >>
```

Nota. Autoría propia, Se configuran los parámetros necesarios los cuales se agregan el comando set: *set rhost 10.0.2.0/29* y *set session 1.* Posterior a agregar la información se ejecuta el comando *run* para ejecutarlo y que este nos muestre la información que buscamos.

Se logra ejecutar el módulo según lo esperado y este nos trae información valiosa para ahora lograr realizar ataques de movimiento lateral gracias al pivoting realizado.

De las IPS encontradas, sabemos que 10.0.2.1 es la puerta de enlace de esa red y que 10.0.2.6 es la IP del HOST A, y podemos descartar la 10.0.2.7, ya que tiene la misma MAC del HOST A.

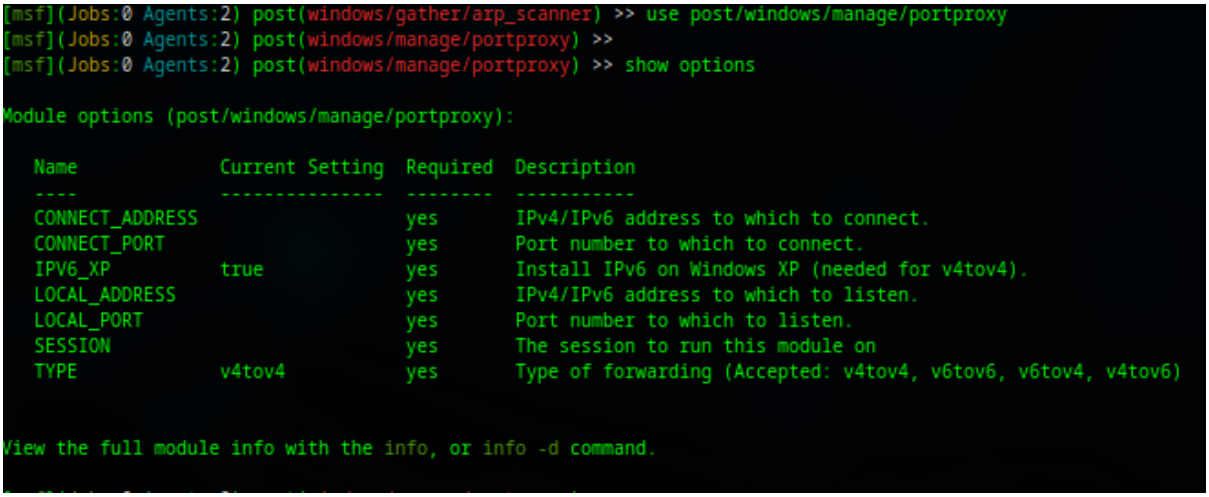
Para este ejercicio sabemos que la IP que tiene el HOST B que es nuestra máquina objetivo final es la 10.0.2.5 la cual aparece en el escaneo de red realizado.

Ahora lo que vamos a hacer es traer un puerto de la máquina HOST B hacia el HOST A y desde allí poder atacarlo desde nuestra máquina atacante.

Esto lo haré con el comando *use post/windows/manage/portproxy* y posterior un show options para ver lo que me pide modificar para lograr alcanzarla.

Figura 33

Uso del módulo post/windows/manage/portproxy



Nota. Autoría propia, validando los parámetros necesarios de configuración y diligenciando la información requerida para su ejecución.

Los datos que vamos a diligenciar son:

CONNECT_ADDRESS: La IP de la máquina objetivo final es decir la del HOST B 10.0.2.5

CONNECT_PORT: El puerto que vamos a traer del HOST B y por defecto sabemos que ya viene activo el 445

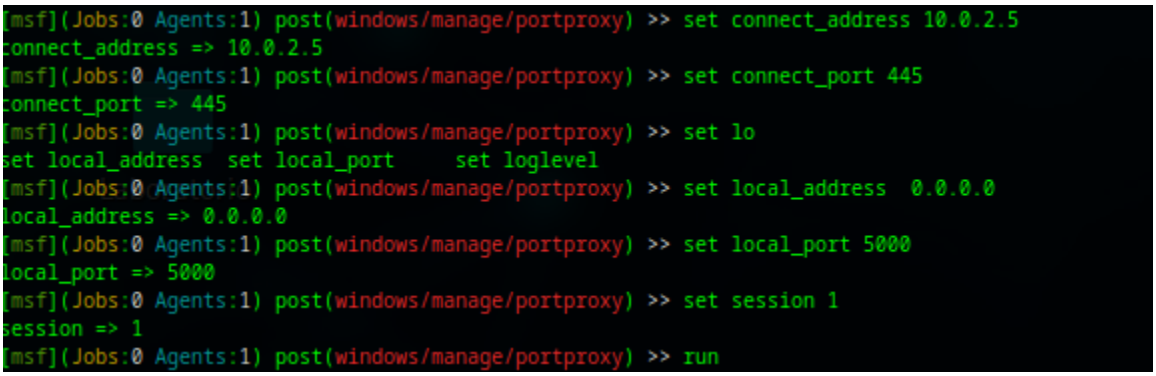
LOCAL_ADDRESS: Usaremos la 0.0.0.0

LOCAL_PORT: Acá va el puerto a donde vamos a traer el puerto 445 usaremos el 5000

SESSION: Y la sesión de meterpreter que estamos usando en este caso la 1

Figura 34

Configuración del módulo portproxy

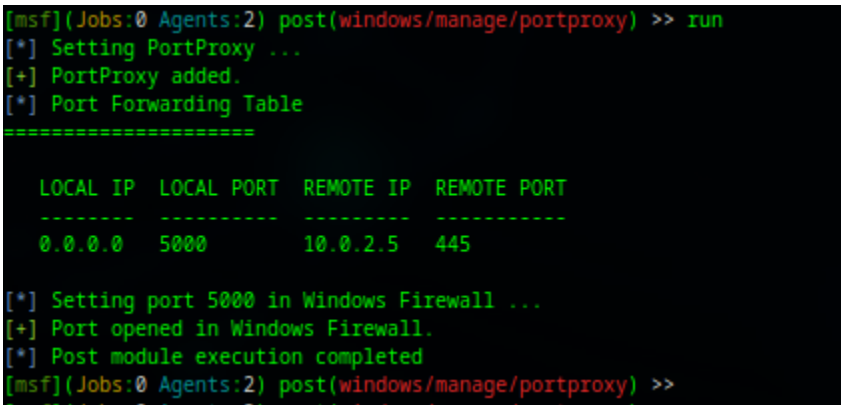


Nota. Autoría propia, se configuran los parámetros requeridos y se ejecuta el módulo para poder crear el portproxy.

Ejecutamos el comando *run* para que tome los cambios y nos confirma que trae la información como la hemos configurado

Figura 35

Ejecución del módulo Windows/manage/portproxy



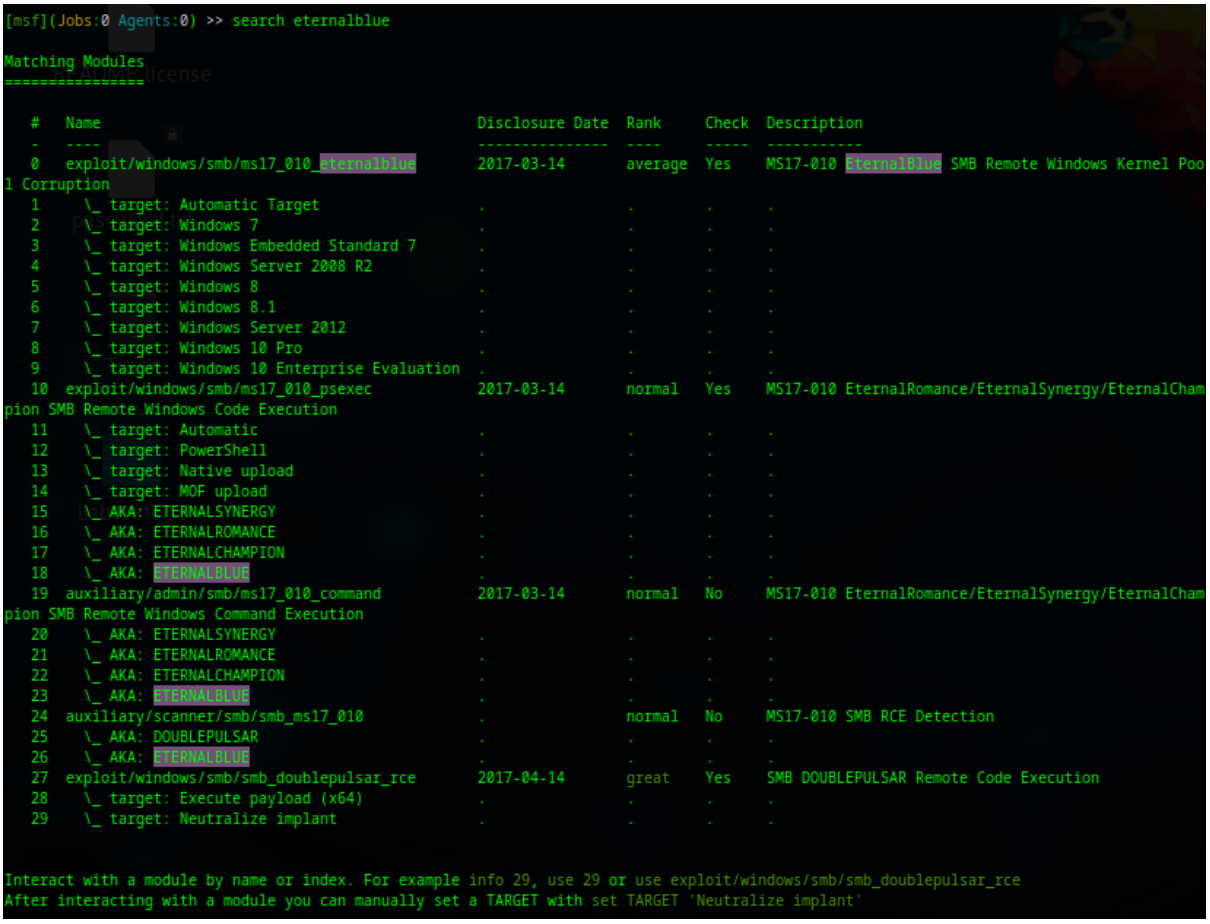
Nota. Autoría propia, el módulo ejecutado nos muestra que la configuración realizada ya fue lanzada.

Ya que hemos logrado crear un túnel desde la maquina atacante hacia el HOST B por medio del pivote realizado usando el HOST A, creamos el port proxy para traer la información que el HOST B nos muestre por el puerto 445 y esto lo aprovecharemos sabiendo que el eternalblue usa ese puerto de comunicación. Para esto vamos a ejecutar desde el Metasploit el módulo que nos permita explotar esa vulnerabilidad.

Desde una consola de Metasploit ejecutamos search eternalblue

Figura 36

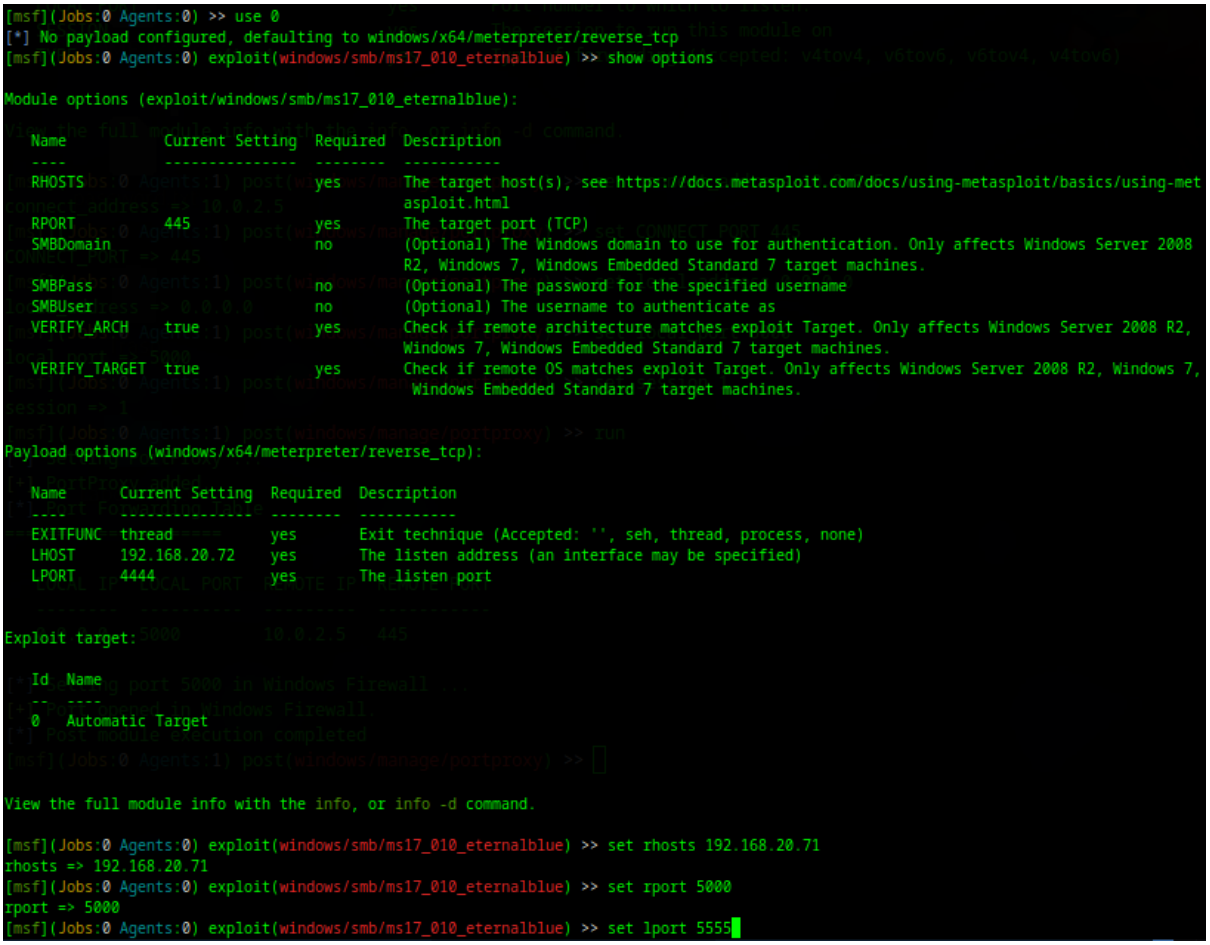
Buscando exploit asociados al eternalblue



Nota. Autoría propia, seleccionamos la primera opción (0) y damos *use 0* y posterior un *show options* para identificar que parámetros debemos modificar.

Figura 37

Ejecución del show options del exploit eternalblue.



Nota. Autoría propia, se validan los parámetros que deben ser configurados con el comando *show options.*

Para esta configuración editaremos:

RHOSTS que es la IP de nuestro equipo intermedio, es decir el HOST A 192.168.20.71, ya que es el que usaremos para hacer le pivoting hacia el HOST B.

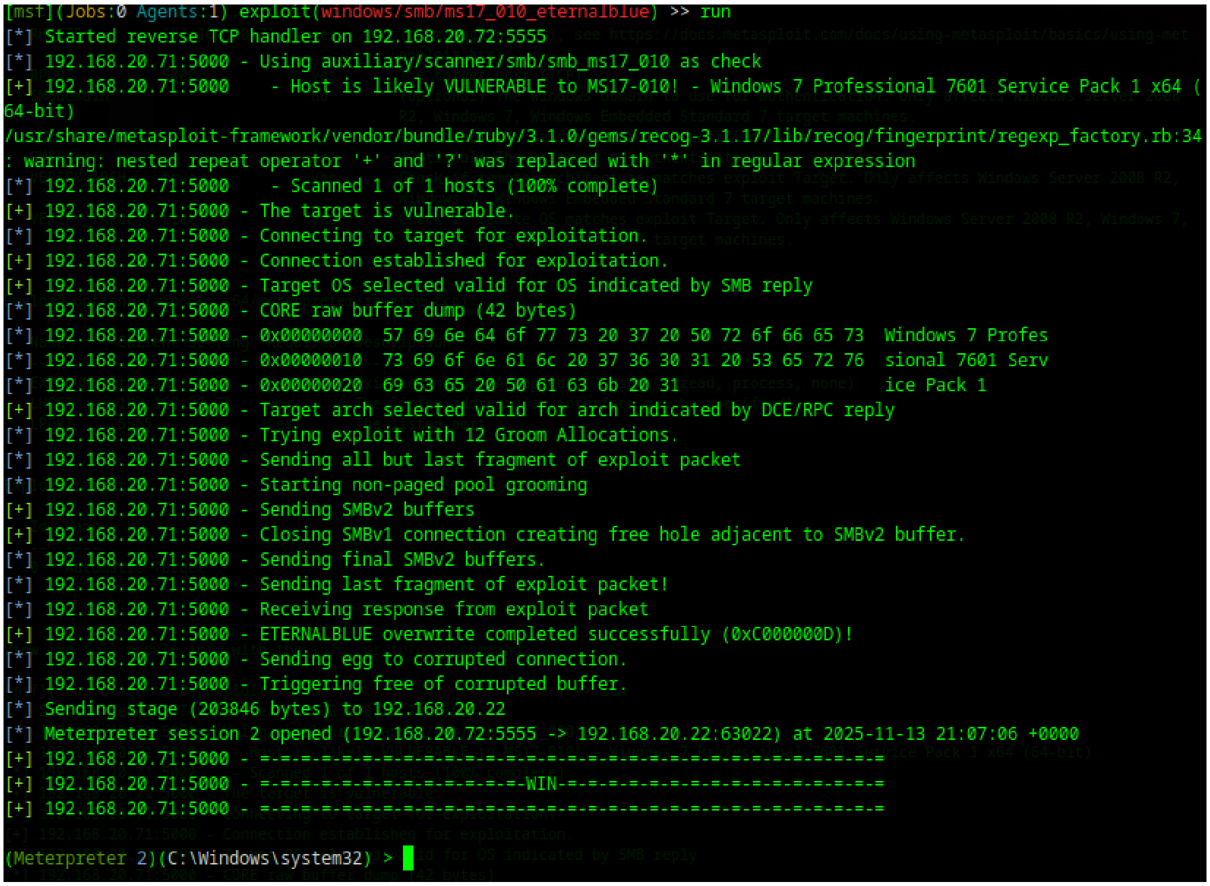
RPORT que es el puerto que trae el puerto del HOST B, en este caso el 5000

Y LPORT que es un puerto cualquiera donde recibiremos el tráfico en nuestra máquina atacante para este ejercicio lo haremos con el 5555.

Posterior a la configuración ejecutamos el *run*.

Figura 38

Ejecución del eternalblue

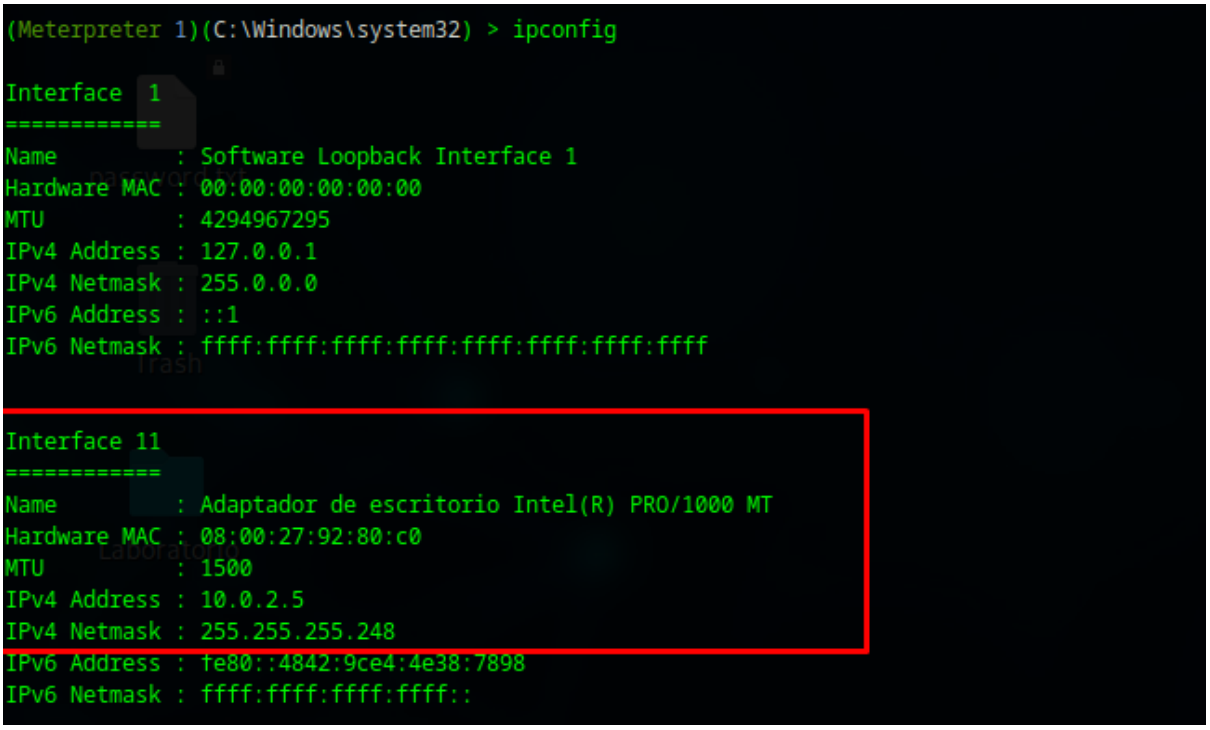


Nota. Autoría propia, tras lanzar el comando *run,* se ejecuta el eternalblue y esperamos que procese, si la configuración es correcta y se logra alcanzar el equipo veremos un mensaje que dice "WIN" confirmando así la conexión con el HOST B.

Posterior a lograr la conexión a la máquina objetivo el HOST B podemos comprobar que si estamos conectados de manera correcta ejecutando comandos como *ipconfig* para confirmar que si estamos en el equipo correcto.

Figura 39

Lanzamiento del comando ipconfig en el HOST B.



Nota. Autoría propia, se debe asegurar que estamos en el equipo que deseábamos alcanzar y no quizá nos quedamos en el HOST A.

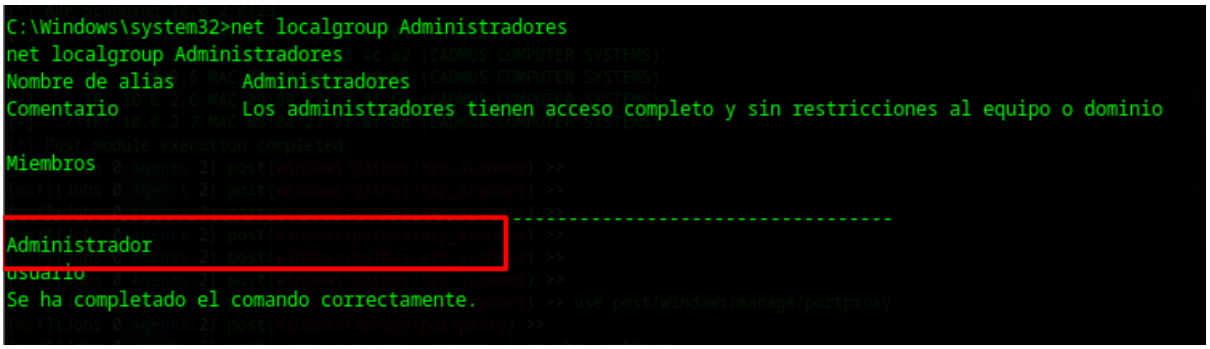
Ahora que ya confirmamos que estamos dentro de la máquina objetivo, vamos a ejecutar el comando *Shell* para poder ejecutar comandos del sistema que nos permitan hacer algo más que un ipconfig.

Para esto vamos a crear un usuario administrador llamado Jonathan_Moncada.

Lo primero será confirmar, mediante comandos, los usuarios administradores que existen; lo haremos con el comando *net localgroup Administradores*, y vemos que solo aparece un usuario llamado Administrador.

Figura 40

Confirmando los usuarios administradores del HOST B.



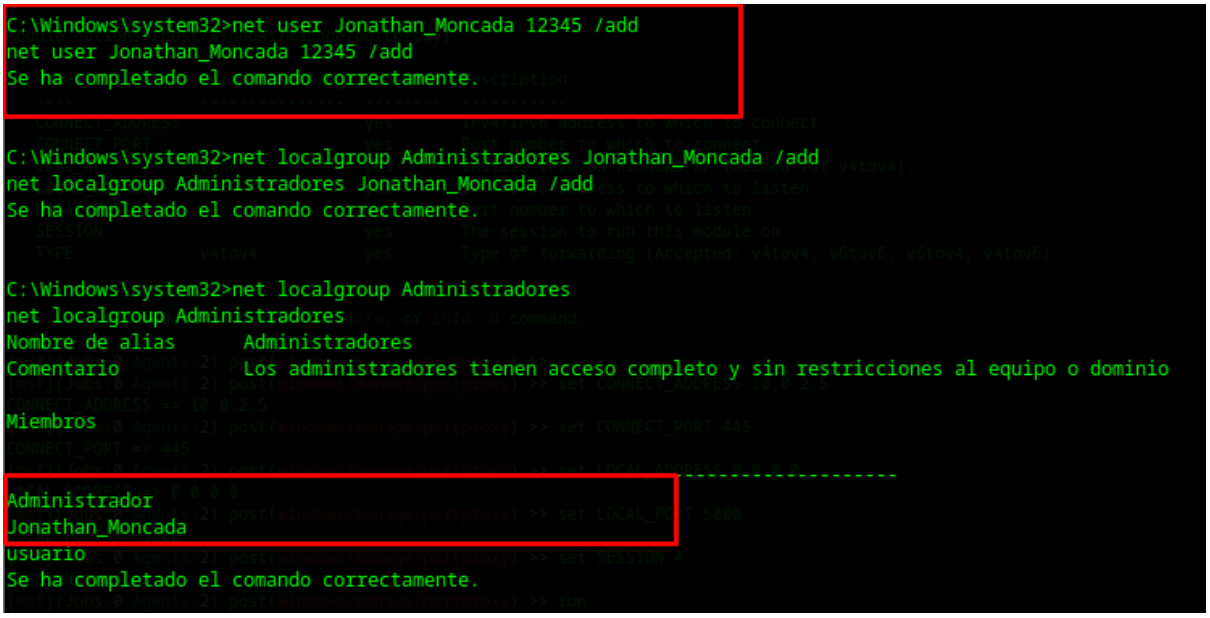
Nota. Autoría propia, se confirma mediante el comando indicado la cantidad de usuarios administradores dentro de la máquina para posteriormente empezar a desarrollar el escalamiento de privilegios en nuestro ataque.

Para crear el usuario, ejecutaremos el comando net user Jonathan_Moncada 12345 /add, donde 12345 es la contraseña.

Y también el comando *net localgroup Administradores Jonathan_Moncada /add* para agregar el usuario al grupo de administradores.

Figura 41

Escalando privilegios, creando usuario administrador Jonathan_Moncada.

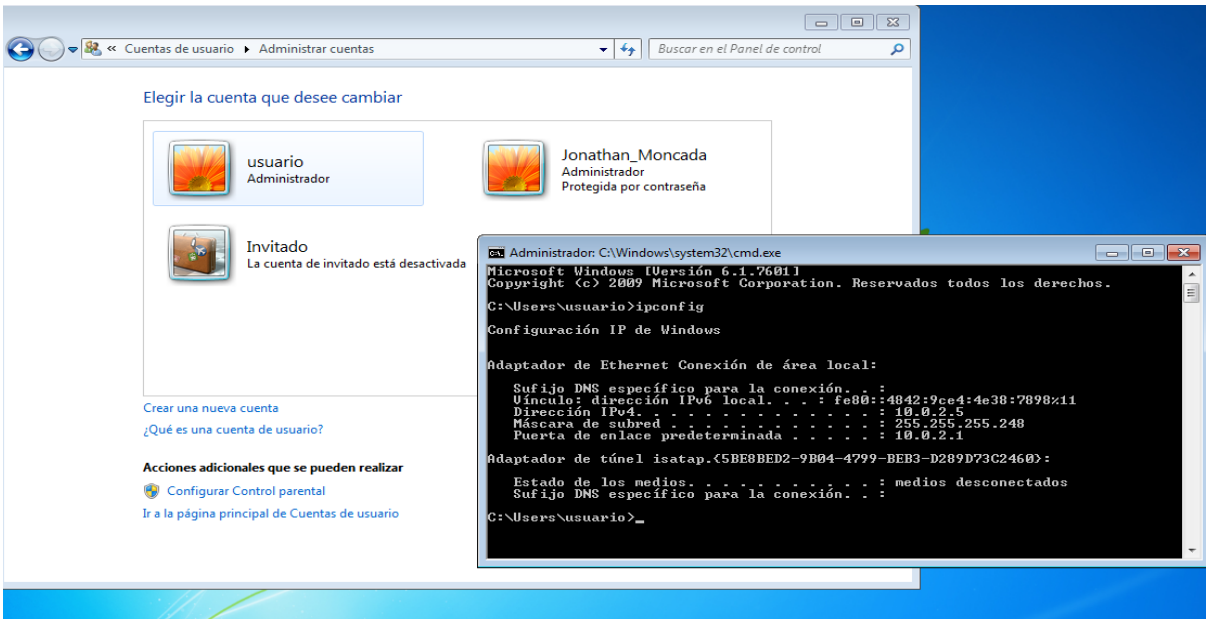


Nota. Autoría propia, dentro del desarrollo de este ejercicio controlado se tiene como objetivo desarrollar el escalamiento de privilegios creando un usuario administrador local.

Podemos confirmar que el cambio lo toma al ingresar al HOST B e ir a la edición de los usuarios, veremos una nueva cuenta llamada Jonathan_Moncada con perfil de administrador

Figura 42

Confirmando la creación del usuario



Nota. Autoría propia, aprovechando que es un ejercicio controlado y tenemos acceso a las máquinas confirmamos de manera gráfica que se creó el usuario Jonathan_Moncada con perfil de administrador.

Y para finalizar el desarrollo de esta actividad controlada y como parte de las buenas prácticas, eliminaremos el usuario creado para no dejar rastros de nuestra incursión, para lo cual usaremos el comando *net user Jonathan_Moncada /delete*

Figura 43

Borrando el usuario Administrador Jonathan_Moncada

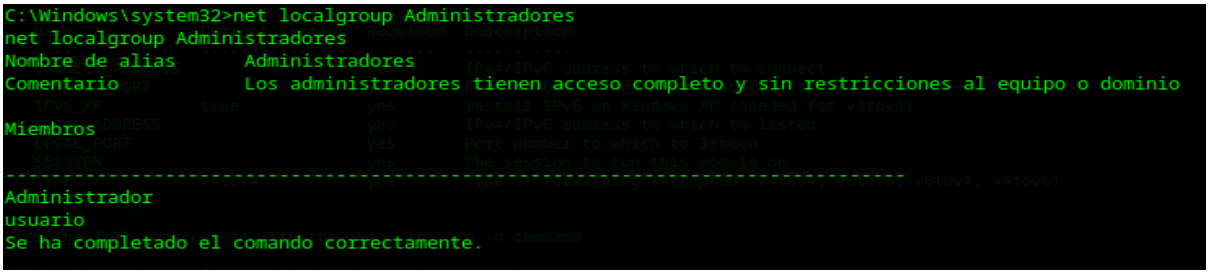
```
C:\Windows\system32>net user Jonathan_Moncada /delete
net user Jonathan_Moncada /delete
Se ha completado el comando correctamente.


C:\Windows\system32>
```

Nota. Autoría propia, dentro de la fase de post-explotación se deben borrar las huellas para eliminar toda evidencia de la intrusión.

Figura 44

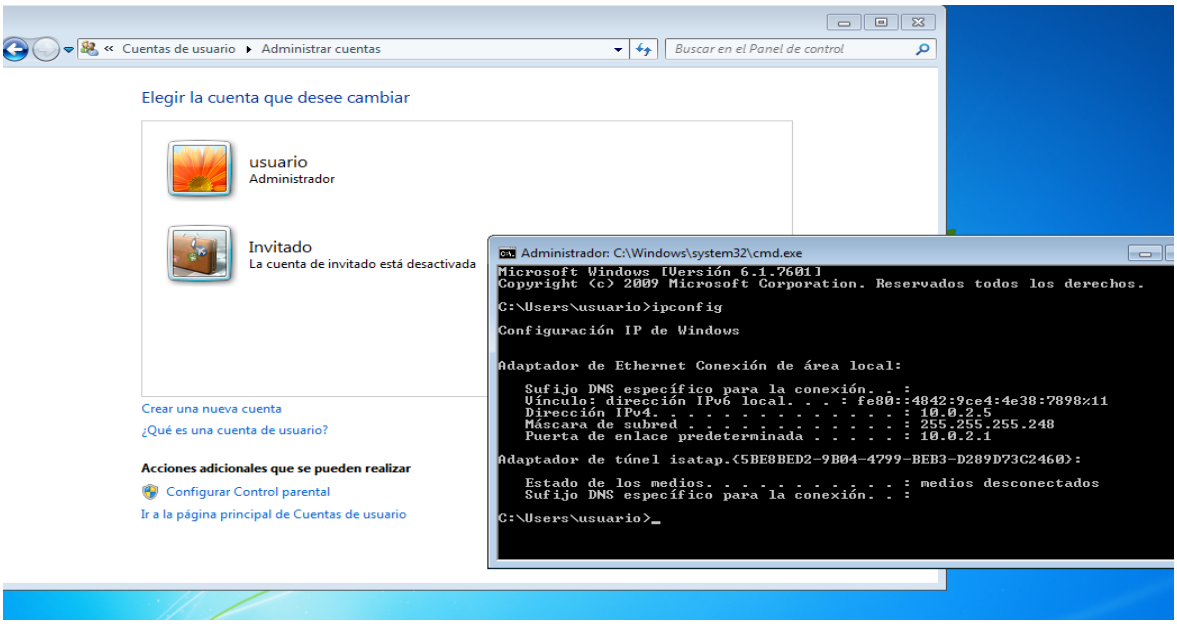
Confirmación del borrado del usuario



Nota. Autoría propia, se puede usar el comando *net localgroup Administradores* para confirmar que el usuario Jonathan_Moncada se halla borrado de manera correcta.

Figura 45

Usuario eliminado exitosamente



Nota. Autoría propia, se confirma directamente sobre el equipo HOST B que el borrado se hiciera de manera correcta.

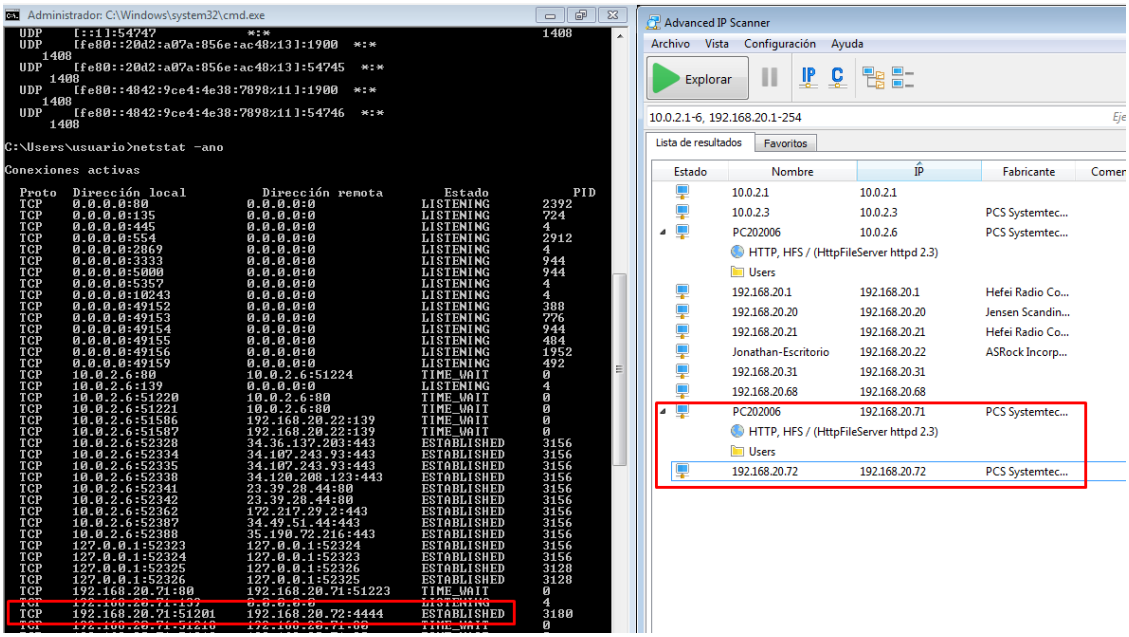
ETAPA 4: Respuesta y Contención ante Incidentes de Seguridad

Se identificó actividad anómala en el Host A derivada de la explotación de Rejetto HFS V2.3. Mediante herramientas nativas del sistema y análisis de conexiones activas se determinó que el atacante mantenía un canal remoto. Posteriormente, se detectó que el Host B también había sido comprometido mediante explotación de SMBv1 (Microsoft, 2025) (Eternalblue, s.f.), lo que confirmó la capacidad del adversario para realizar movimiento lateral.

Contención del ataque

Figura 46

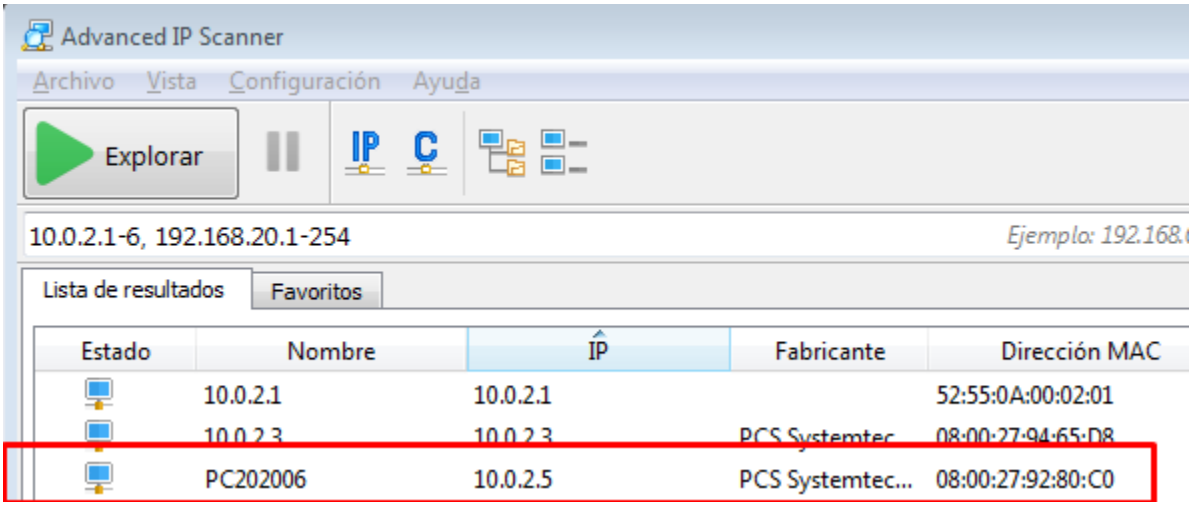
Detección de la conexión del equipo atacante al HOST A.



Nota. Autoría propia, los recursos nativos son bastante útiles para detectar conexiones anómalas en los equipos, pero si nos apoyamos de herramientas adicionales están nos mostraran información que puede ser de utilidad como la dirección MAC del equipo.

Figura 47

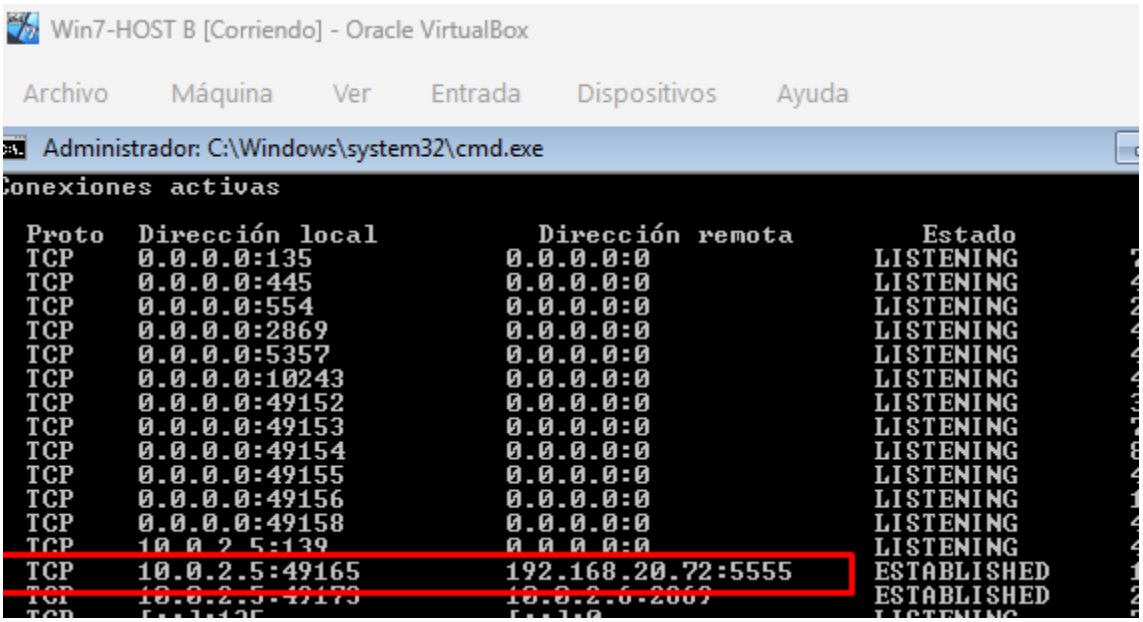
Rastreo de la conexión al HOST B.



Nota. Autoría propia, también vemos que en la red vemos un equipo con IP 10.0.2.5 y MAC 08:00:27:92:80:C0 y al hacer seguimiento con los datos obtenidos nos dirá información relevante para su identificación, para el laboratorio realizado sabemos que es un equipo que también tiene Windows 7. Lo que haremos con esa información es dirigirnos a esa máquina para poder ver si también está comprometida.

Figura 48

HOST B revisión con el comando netstat -ano

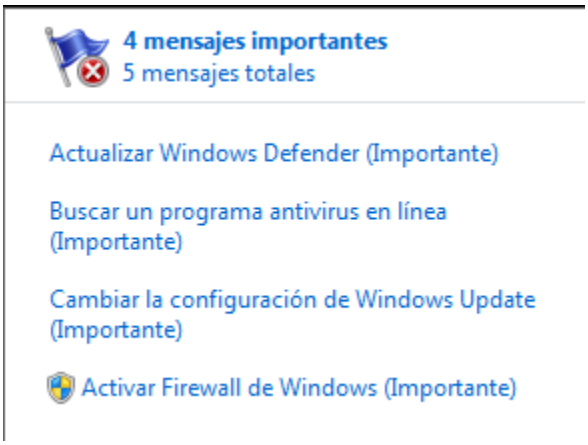


Nota. Autoría propia, tras validar en el HOST B vemos que este también ha sido comprometido y actualmente tiene una conexión establecida desde el equipo con IP 192.168.20.72 con lo cual ya sabemos que actualmente el atacante hizo un movimiento lateral sobre la red para alcanzar otros dispositivos.

Ahora ya que identificamos las máquinas que están impactadas debemos iniciar la contención del incidente, la cual vamos a realizar directamente sobre los equipos.

Figura 49

Revisión del HOST A

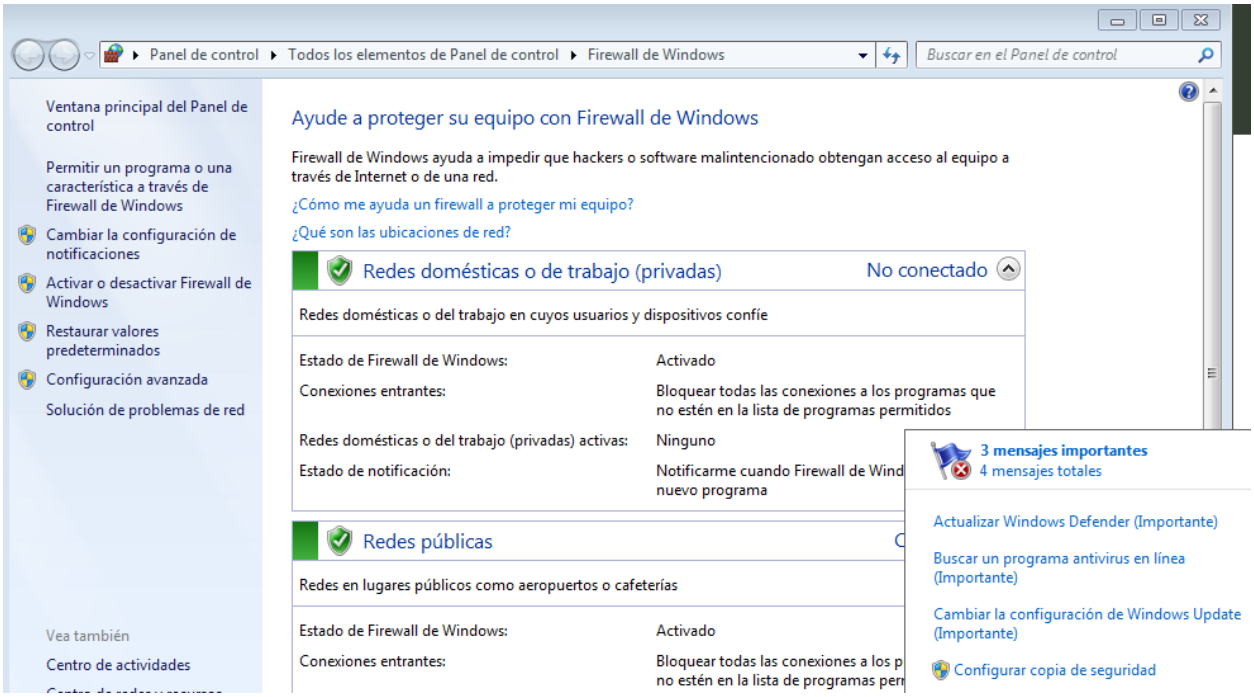


Nota. Lo primero que vamos a buscar es las posibles brechas de seguridad que tiene la primera máquina afectada y que fue el punto de salto para alcanzar la otra red expuesta.

Al ver los mensajes generados por el sistema se observa que el mismo hace recomendaciones de seguridad que muestran un descuido en los controles y pudieron ser la causa de que la brecha de seguridad fuera aún mayor.

Figura 50

Activación firewall de Windows



Nota. Se encontró que él firewall de Windows no estaba activo por lo que se procede a su activación y así activar unas de las principales capas de protección que tienen estos hosts.

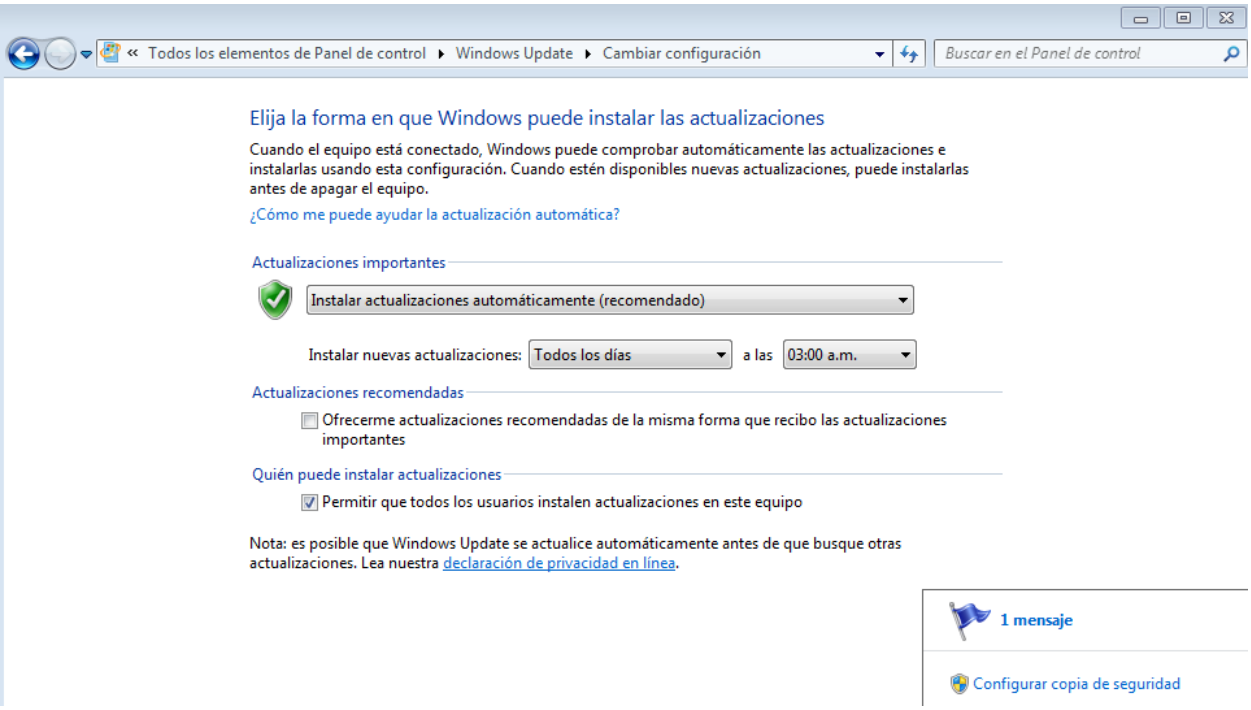
Figura 51

Instalación antivirus

Nota. Autoría propia, se realiza la instalación del antivirus que en conjunto con el firewall del sistema proporcionaran diferentes capas de protección al sistema.

Figura 52

Cambiando configuración del Windows Update



Nota. Autoría propia, se activa la actualización automática del sistema ya que las actualizaciones mismas nos ayudan a proteger el sistema al corregir vulnerabilidades que surgen diariamente, mejoran el rendimiento le proporcionan mayor estabilidad al sistema.

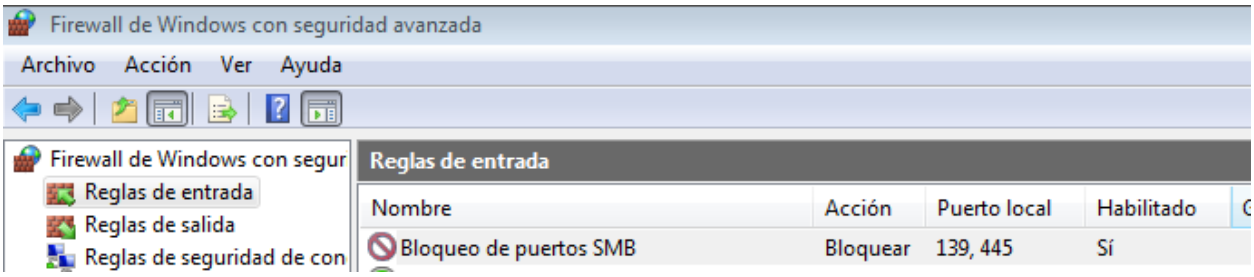
Ahora como vimos se logró hacer un ataque a un segundo equipo aprovechando una vulnerabilidad conocida llamada Eternalblue, “la herramienta de explotación EternalBlue fue filtrada por el grupo "The Shadow Brokers" el 14 de abril de 2017, en su quinta filtración, "Lost in Translation". Esta filtración incluía varias herramientas entre las que se mencionaba EternalBlue, basadas en múltiples vulnerabilidades en la implementación del protocolo SMB en

Windows. EternalBlue funciona en todas las versiones de Windows anteriores a Windows 8. Estas versiones contienen un recurso compartido de comunicación entre procesos que permite una sesión nula. Esto significa que la conexión se establece mediante un inicio de sesión anónimo y la sesión nula está permitida por defecto. (Eternalblue, s.f.)

Entendido lo anterior y tomando de referencia el ejemplo dado en el desarrollo del laboratorio, en casos como este que se tiene un sistema vulnerable como lo es el Windows 7, vamos a aumentar su nivel de seguridad configurando una regla en el firewall de Windows para evitar que los puertos usados SMB por esta vulnerabilidad estén expuestos.

Figura 53

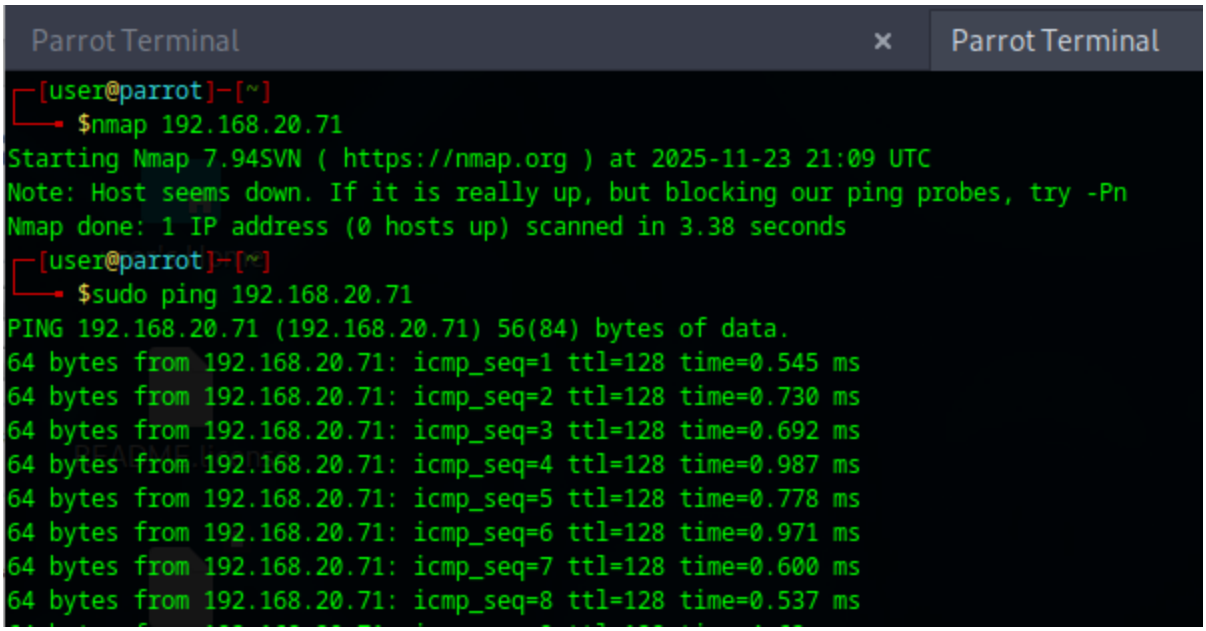
Creando regla de bloqueo puertos 139 y 445 TCP



Nota. Autoría propia, crear la regla manualmente para el sistema nos ayuda a garantizar que este tenga mayor nivel de protección, ahora si esto debe aplicarse a nivel general para una compañía se puede lanzar este parche utilizando una GPO (objeto de directiva de grupo).

Figura 54

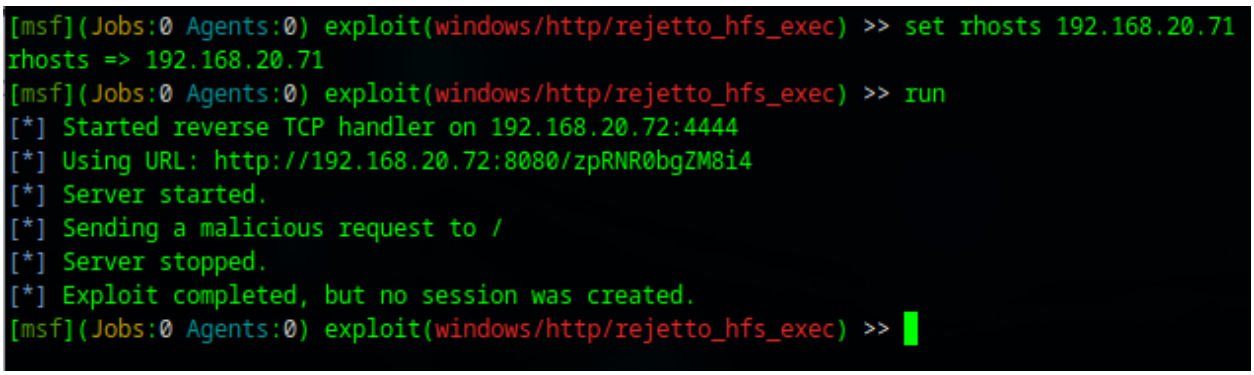
Prueba de contención.



Nota. Autoría propia, en la imagen anterior podemos ver que luego de lanzarle nuevamente un *nmap* a la maquina 192.168.20.71 que llamamos HOST A, este no nos muestra ya puertos abiertos que puedan presentar una brecha de seguridad, pero si se tiene alcance al dispositivo. Ya para finalizar se puede aislar el equipo si se quiere indagar más en los eventos que se hayan logrado efectuar sobre él y así garantizar que el ataque recibido no tenga un mayor alcance y esté totalmente contenido.

Figura 55

Lanzando exploit Rejetto para prueba



Nota. Autoría propia, se intenta lanzar nuevamente el exploit para demostrar que ya no hay forma de atacar dicha vulnerabilidad luego de las acciones realizadas para asegurar la red.

¿Si se encuentra con un ataque en tiempo real cual sería el primer paso o lo primero que indagaría? Especifique su respuesta con argumentos técnicos.

Lo primero que debe hacer un miembro del Blue Team cuando identifica un ataque en tiempo real es obtener una comprensión precisa y rápida de lo que está ocurriendo. Antes de tomar cualquier acción técnica profunda o correctiva, es fundamental confirmar que el ataque sigue activo y determinar su alcance inicial. En incidentes como el del laboratorio, donde se ha explotado una vulnerabilidad conocida en un servicio expuesto (Rejetto HFS 2.3) y posteriormente se ha utilizado la máquina comprometida para alcanzar un segundo objetivo mediante EternalBlue, la prioridad es identificar la actividad anómala que indica la presencia y el avance del atacante dentro de la red.

La primera indagación consiste en analizar el comportamiento del sistema comprometido desde una perspectiva de red y de procesos internos, ya que estas dos áreas son las que más rápidamente muestran evidencia de que un intruso mantiene control sobre la máquina. Verificar las conexiones activas del equipo permite identificar si existe comunicación con un origen externo no autorizado, si se han establecido canales persistentes hacia direcciones ajenas al entorno interno y si se observa tráfico característico de un “reverse shell” o un túnel utilizado para moverse lateralmente. Esta visibilidad inicial es indispensable para determinar si el compromiso es reciente, si el atacante continúa operando dentro del host o si ya ha establecido mecanismos de persistencia.

Paralelamente, es esencial revisar la actividad de todos aquellos procesos que se puedan estar ejecutando en el sistema. Cuando se explotan servicios como el Rejetto HFS, el proceso

asociado al servicio suele presentar comportamientos atípicos, como un consumo inesperado de recursos o la aparición de ejecuciones que no forman parte de su operación legítima. En el mismo sentido, una explotación como EternalBlue suele evidenciar alteraciones en servicios críticos de Windows o actividad inusual asociada al manejo del tráfico SMB. La correlación entre estas anomalías permite confirmar si el atacante está utilizando la máquina como punto de apoyo para avanzar hacia otras redes, particularmente si el sistema cuenta con varias interfaces o se encuentra conectado a segmentos distintos como en el caso del Host A del escenario.

Una vez confirmado que el ataque está en curso, la primera acción prioritaria es preservar la integridad del sistema y evitar que el intruso continúe expandiéndose, lo cual no implica apagar el equipo ni eliminar archivos, ya que esto destruiría evidencia crítica para el análisis posterior. La respuesta inicial debe centrarse en contener la propagación del ataque aislando temporalmente la máquina del resto de la red, sin afectar su estado interno. Esta contención temprana es esencial para impedir que el atacante siga enviando cargas maliciosas, mantenga sesiones activas o logre alcanzar el siguiente objetivo dentro del entorno interno.

Posteriormente, con el sistema aislado y sin el riesgo inmediato de propagación, se puede iniciar un análisis más profundo para identificar el vector inicial de acceso, evaluar si se han creado mecanismos de persistencia, revisar modificaciones sospechosas en archivos o configuraciones críticas y determinar si se produjo un movimiento lateral hacia otros segmentos.

Esto se puede desarrollar con un paso a paso detallando rápidamente lo que se debería hacer:

Tabla 1

Paso a paso en caso de ataque

Paso	Descripción
Confirmación del incidente	Se verifica que el comportamiento observado corresponde realmente a un ataque activo y no a una falla técnica, validando señales claras de compromiso como conexiones inusuales o procesos inesperados.
Identificación del origen y del alcance inicial	Se analiza desde qué red, host o servicio proviene la actividad maliciosa y qué parte del sistema se encuentra comprometida. Esto ayuda a determinar si el ataque es aislado o si se está expandiendo.
Análisis del comportamiento del sistema	Se revisa cómo están operando los procesos y servicios del host afectado, detectando comportamientos anómalos, modificaciones recientes o patrones que indiquen explotación o ejecución remota.
Evaluación del riesgo de propagación	Se determina si el atacante puede desplazarse hacia otros segmentos de red o activos internos, especialmente cuando el host comprometido tiene múltiples interfaces o conexiones.
Contención inmediata no destructiva	Se corta el acceso del atacante al sistema sin reiniciar, formatear ni eliminar evidencia, asegurando que la actividad maliciosa no continúe mientras se preserva el estado del sistema.
Estabilización del entorno	Se comprueba que el atacante ya no mantiene acceso y que no existen procesos activos que puedan restablecer la intrusión o facilitar nuevas etapas del ataque.
Documentación temprana del incidente	Se registran los hallazgos iniciales, tiempos, comportamientos anómalos y evidencias observadas antes de que cambie el estado del sistema debido a acciones defensivas.
Preparación para el análisis profundo	Se prepara el entorno para continuar con una investigación detallada que permita entender el vector inicial, evaluar el impacto y definir la siguiente fase de respuesta.

Nota. Autoría propia, se da un paso a paso de lo que haría en caso tal de presentarse un ataque en tiempo real en el cual deba intervenir como parte de un equipo de Blue Team.

¿Después de ejecutado la labor desde Red Team, qué medidas podrían implementarse a nivel de hardenización para que el ataque no se repita?

Tras desarrollar el ejercicio desde el lado de Red Team y comprender las vulnerabilidades explotadas, la prioridad de hardenización debe centrarse en reducir la superficie de ataque, eliminar configuraciones inseguras y fortalecer los mecanismos que impidan la ejecución remota no autorizada. En este caso, el ataque se apoyó en dos debilidades críticas: un servicio vulnerable expuesto sin control (Rejetto HFS 2.3) y un sistema operativo sin parches capaz de ser comprometido mediante EternalBlue. Por lo tanto, las medidas deben abordar tanto el vector inicial como el movimiento lateral que permitió la escalada del ataque.

En primer lugar, es fundamental evitar que aplicaciones obsoletas y vulnerables se encuentren expuestas a la red, especialmente cuando actúan como servicios accesibles desde múltiples segmentos. El servicio HFS 2.3 es ampliamente conocido por tener vulnerabilidades de ejecución remota y, por ende, no debe ser utilizado en entornos productivos ni de pruebas sin los mecanismos de aislamiento adecuados. Lo mejor sería reemplazarlo por una alternativa segura, y en caso de que su uso sea estrictamente necesario, operarlo dentro de un entorno completamente segmentado, con listas de control que limiten quién puede interactuar con él.

En segundo lugar, es importante mantener los sistemas operativos actualizados y libres de vulnerabilidades conocidas. El ataque EternalBlue solo fue posible porque los equipos Windows 7 que utilizamos en el ejercicio no contaban con los parches de seguridad necesarios, sin mencionar que hoy en día ya es un sistema operativo obsoleto que no cuenta con el soporte del fabricante desde el año 2020. Dentro de un proceso de hardening formal, los parches de seguridad deben aplicarse de manera sistemática y oportuna, priorizando cualquier

vulnerabilidad de ejecución remota que afecte servicios críticos como SMB. Esto implica también deshabilitar versiones antiguas de protocolos inseguros.

Como tercera medida importante consiste en limitar el movimiento lateral mediante una segmentación de red adecuada. En el ejercicio, logramos pivotar desde el Host A hacia el Host B porque ambos compartían acceso simultáneo a una red secundaria (10.0.2.0/29). Esta falta de separación interna permitió que lográramos el host comprometido como puente. Una política correcta sería aplicar segmentación estricta entre VLANs, restringir quién puede comunicarse con cada red y evitar que equipos expuestos en una DMZ o en redes menos confiables tengan acceso directo a segmentos internos. La segmentación actúa como una barrera natural que frena el avance del atacante, incluso si logra comprometer una máquina inicial.

Además, se debe reforzar la superficie de red mediante un firewall interno correctamente configurado. Todo servicio que no sea estrictamente necesario debe estar deshabilitado o bloqueado, y aquellos que requieran ser accesibles deben operar con reglas explícitas que controlen origen, destino y tipo de tráfico. En el caso de SMB, únicamente debe permitirse entre sistemas que realmente lo utilicen, evitando que cualquier host pueda iniciar conexiones arbitrarias hacia otros. Este tipo de restricción habría evitado la explotación de EternalBlue aun si el Host A hubiera sido comprometido.

Finalmente, el entorno debe complementarse con mecanismos de detección temprana, como un IDS/IPS de red o un HIDS de host, que puedan alertar en tiempo real sobre patrones de tráfico o comportamientos típicos de explotación, tales como incrementos súbitos en conexiones salientes, intentos de comunicación con redes no autorizadas, creación de procesos no firmados o actividad inusual en puertos críticos. Aunque esto no evita por sí mismo la vulnerabilidad, sí permite cortar el ataque en sus primeras etapas, reduciendo sustancialmente el impacto.

¿Cuáles son las diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos?

Los dos hacen parte fundamental dentro del ecosistema de ciberseguridad, pero el equipo BlueTeam se encarga permanentemente a monitorear, proponiendo políticas, monitoreo y hardenización en todo momento buscando fortalecer, vigilar y detectar cualquier amenaza. Su momento de acción es antes, durante y después y su enfoque es mas de prevención.

En cambio, el equipo de respuesta a incidentes actúa durante y después del incidente es decir cuando existe evidencia de un ataque, por lo cual su momento de acción es cuando la prevención ya no es suficiente para contener un ataque.

¿Si debe usar CIS "¿Center For Internet Security", trabajando en un equipo de Blue Team para que fin lo pudiera ser usado?

Primero conozcamos que es CIS, "son un conjunto prescriptivo, priorizado y simplificado de mejores prácticas que puede utilizar para fortalecer su estrategia de ciberseguridad. Hoy en día, miles de profesionales de la ciberseguridad de todo el mundo utilizan los Controles CIS o contribuyen a su desarrollo mediante un proceso de consenso comunitario". (CIS - Center for Internet Security, s.f.)

CIS ofrece guías muy detalladas para asegurar Windows, Linux, redes, servicios en la nube y equipos de usuario. Lo que me permite endurecer la configuración de los equipos, cerrar puertos innecesarios, ajustar políticas de seguridad, entre otros. Adicional a lo ya mencionado CIS este framework divide las medidas de seguridad en niveles, lo que me permitiría saber que controles implementar primero y organizar un plan de mejora.

CIS fue desarrollado pensando en las amenazas reales por lo que sus controles van enfocados en evitar explotación de vulnerabilidades, fortalecer credenciales e identidades y proteger redes y endpoints.

Como aplicaría el rol del CIS en el laboratorio desarrollado.

El primer aporte del CIS en el laboratorio es permitir mapear las debilidades identificadas con los controles específicos que fueron vulnerados durante el ataque. Esto facilita comprender por qué el adversario tuvo éxito y qué elementos de la infraestructura carecían de controles adecuados. En el escenario del laboratorio se evidenciaron tres fallas críticas que se alinean directamente con los CIS Controls v8:

Exposición de servicios vulnerables (Rejetto HFS 2.3)

Esta falla corresponde directamente a deficiencias en:

- CIS Control 2 – Inventory and Control of Software Assets (Center for Internet Security, 2021)
- CIS Control 4 – Secure Configuration of Enterprise Assets and Software (Center for Internet Security, 2021)

El software Rejetto HFS 2.3, conocido por múltiples vulnerabilidades RCE, no estaba inventariado, controlado ni sujeto a un proceso de validación o actualización. Su sola presencia como servicio accesible representa una violación a los controles CIS, pues cualquier software no gestionado se convierte en un punto de exposición significativo.

Sistemas sin parches y uso de protocolos inseguros (EternalBlue, SMBv1)

Esta situación refleja incumplimientos en:

- CIS Control 7 – Continuous Vulnerability Management (Center for Internet Security, 2021)

- CIS Control 4 – Secure Configuration of Enterprise Assets and Software (Center for Internet Security, 2021)

Los equipos Windows 7 utilizados en el laboratorio carecían de parches de seguridad y mantenían habilitado SMBv1, un protocolo obsoleto y vulnerable. La explotación de EternalBlue fue posible exclusivamente por esta ausencia de actualización continua, demostrando que la gestión de vulnerabilidades no estaba implementada de acuerdo con los lineamientos del CIS.

Falta de segmentación y controles de red que permitieron el movimiento lateral

Esta debilidad se asocia con:

- CIS Control 12 – Network Infrastructure Management (Center for Internet Security, 2021)
- CIS Control 13 – Network Monitoring and Defense (Center for Internet Security, 2021)

Ambos hosts, aun perteneciendo a redes distintas, tenían visibilidad mutua sin ningún mecanismo de filtrado, listas de control de acceso o segmentación efectiva. Esto permitió que el atacante, ya posicionado en un host inicial, pudiera pivotar hacia la segunda máquina sin restricciones, aprovechando la ausencia de políticas "deny by default" y la inexistencia de monitoreo avanzado.

Implementación de controles CIS aplicados directamente al laboratorio

Una vez identificadas las debilidades que hicieron posible el ataque, el siguiente paso consiste en implementar los CIS Controls como medidas concretas de hardening. Esto permite transformar los hallazgos del laboratorio en acciones operativas que reducen la superficie de ataque y fortalecen la postura defensiva.

Eliminación y control de software no autorizado (CIS 2 y CIS 4)

Aplicación directa en el laboratorio:

- Retirar completamente Rejetto HFS 2.3 o reemplazarlo por un servicio seguro.
- Incluir todos los servicios expuestos en un inventario oficial.
- Establecer un proceso formal que prohíba instalar software no autorizado o sin evaluación de riesgos.

Aplicación continua de parches, gestión de vulnerabilidades y endurecimiento del sistema (CIS 4 y CIS 7)

Acciones necesarias:

- Deshabilitar definitivamente SMBv1 en todos los hosts.
- Aplicar parches acumulativos que corrigen EternalBlue y otras vulnerabilidades críticas.
- Configurar plantillas de seguridad alineadas a CIS Benchmarks.

Segmentación efectiva y control estricto del tráfico interno (CIS 12 y CIS 13)

Implementación recomendada:

- Separar cada host en segmentos de red independientes con permisos mínimos.
- Configurar ACLs entre VLANs.
- Limitar completamente conexiones SMB entre máquinas que no lo requieran.
- Implementar monitoreo continuo.

Funciones y características principales de un SIEM.

Un elemento clave dentro de la ciberseguridad es el uso de soluciones SIEM, ya que permiten centralizar y analizar eventos relacionados con la seguridad. Estos sistemas integran tanto la gestión de la información como la de los eventos de seguridad, combinando en una sola plataforma las funciones SIM y SEM para ofrecer una visión unificada del entorno tecnológico (Fortinet, s.f.).

“Estos tipos de soluciones recopilan, agregan y analizan grandes volúmenes de datos de aplicaciones, dispositivos, servidores y usuarios en toda la organización en tiempo real”. (MICROSOFT - ¿Qué es SIEM?, s.f.).

Las características principales de un SIEM son:

1. Visibilidad total del entorno

Centraliza y consolida la información de seguridad para que nada pase desapercibido.

2. Capacidad de procesar grandes volúmenes de datos

Está diseñado para manejar miles o millones de eventos por minuto sin perder rendimiento.

3. Flexibilidad e integración

Se conecta con prácticamente cualquier dispositivo o aplicación que genere logs.

4. Automatización

Dependiendo del SIEM, puede ejecutar respuestas automáticas, como:

- bloquear una IP,
- deshabilitar una cuenta,
- aislar un host comprometido.

5. Escalabilidad

Permite crecer conforme aumenta la infraestructura y los requisitos de seguridad.

Y sus funciones principalmente son:

1. Recolección centralizada de logs

El SIEM reúne en un solo lugar todos los registros de seguridad que generan los sistemas, servidores, aplicaciones, firewalls, etc. Esto evita tener que analizarlos por separado y mejora la visibilidad.

2. Correlación y análisis de eventos

El SIEM compara y relaciona eventos para identificar patrones sospechosos. Lo que por separado parece normal, combinado puede evidenciar un ataque. Esta función es clave para detectar amenazas avanzadas.

3. Detección y generación de alertas en tiempo real

Cuando encuentra actividad anómala o potencialmente maliciosa, el SIEM genera alertas para que el equipo de seguridad actúe rápidamente. Esto ayuda a responder antes de que el ataque escale.

4. Almacenamiento y trazabilidad de eventos

Guarda registros por largos periodos, lo que permite realizar análisis forense, auditorías y reconstrucción de incidentes. Es fundamental para entender qué ocurrió y quién lo hizo.

5. Visualización y reportes

Ofrece paneles e informes que muestran el estado de la seguridad, eventos críticos y tendencias. Esto facilita la toma de decisiones y el seguimiento de la postura de seguridad.

Como aplicaría el rol del SIEM en el laboratorio desarrollado.

Explotación de Rejetto HFS:

El SIEM habría generado alertas por comportamiento irregular en el servicio HTTP, ejecución de procesos no asociados al servicio (cmd.exe o powershell desde hfs.exe) y patrones de ejecución remota característicos de un RCE.

Uso de la sesión Meterpreter:

La comunicación reverse shell hacia Parrot OS habría generado eventos asociados a conexiones salientes no autorizadas, apertura de sockets persistentes y tráfico cifrado inusual.

Enumeración de redes y pivoting:

La aparición de consultas ARP, rutas nuevas o conexiones hacia una red que el Host A no utiliza normalmente habría sido correlacionada por el SIEM como actividad propia de un movimiento lateral.

Explotación de EternalBlue:

Eventos SMBv1 inusuales, intentos de ejecución remota y fallos en el servicio lsass.exe o svchost.exe habrían generado una alerta casi inmediata.

En conjunto, el SIEM no solo habría detectado cada etapa, sino que habría permitido reconstruir la línea temporal del ataque, facilitando la respuesta del Blue Team.

Definir al menos 3 herramientas de contención de ataques informáticos "hardware o software".

Firewalls de Próxima Generación (NGFW) → Hardware/Software

Son dispositivos que permiten bloquear tráfico, aislar redes y aplicar reglas estrictas durante un ataque (CISCO, 2018).

Ejemplos:

- Palo Alto NGFW
- Fortinet Fortigate
- Cisco Firepower
- pfSense (software libre)
- OPNsense (software libre)

Función de contención: cortar comunicación maliciosa, bloquear IPs, cerrar puertos y limitar el avance de un atacante.

Sistemas de Control de Acceso NAC → Hardware/Software

Estos sistemas permiten desconectar, aislar o aplicar cuarentena a dispositivos comprometidos (CISCO, s.f.).

Ejemplos:

- FortiNAC de Fortinet
- Aruba ClearPass
- PacketFence (software libre)

Función de contención: aislar equipos infectados en VLANs de cuarentena.

EDR/XDR con capacidades de aislamiento → Software

Aunque los EDR detectan, su función de aislar el host es oficialmente una acción de contención.

Ejemplos:

- CrowdStrike Falcon
- Microsoft Defender for Endpoint
- SentinelOne
- Sophos Intercept X
- Velociraptor (software libre)

Función de contención: desconectar el equipo de la red, bloquear procesos maliciosos, impedir movimientos laterales. (CrowdStrike, 2025)

Relación técnica entre la Etapa 3 y la Etapa 4 (Red Team → Blue Team)

En la Etapa 3 se reconstruyó todo el ciclo del ataque ejecutado por el Red Team, el cual inició con la explotación de Rejetto HFS 2.3 en el Host A. Esta vulnerabilidad permitió obtener una sesión Meterpreter, realizar escalada de privilegios y posteriormente ejecutar un proceso de

pivoting, aprovechando que el Host A tenía acceso simultáneo a la red 192.168.20.0/24 y 10.0.2.0/29. Desde allí, el atacante alcanzó el Host B y explotó la vulnerabilidad EternalBlue (MS17-010). Finalmente, creó un usuario administrativo en Host B para consolidar control antes de ejecutar la fase de limpieza.

La Etapa 4 toma ese mismo recorrido ofensivo y lo traduce en acciones concretas que el Blue Team debería ejecutar para detectar, contener y mitigar el incidente. Cada vulnerabilidad explotada durante el ataque tiene su contramedida correspondiente dentro de la respuesta defensiva:

Explotación inicial de Rejetto HFS 2.3 en Host A

Acción del atacante (Etapa 3)

El atacante explotó la vulnerabilidad RCE de Rejetto HFS 2.3, lo que permitió ejecutar código remoto y obtener una sesión Meterpreter en Host A.

Cómo se habría detectado (Etapa 4)

- Alertas del SIEM por actividad irregular del servicio HFS (creación de procesos hijos no habituales).
- Registros de Windows mostrando ejecución inesperada de powershell.exe.
- Conexiones entrantes o reverse shells dirigidos hacia IPs externas no autorizadas.
- Eventos de red relacionados con solicitudes HTTP modificadas que incluyen cargas maliciosas.

Medidas de hardenización directamente relacionadas

Estas medidas detienen exactamente este tipo de explotación:

1. Eliminar o reemplazar Rejetto HFS 2.3, ya que es software vulnerable y obsoleto.
2. Actualizar el sistema operativo para reducir vectores de ejecución remota.

3. Configurar firewall para bloquear el puerto del servicio si no es imprescindible.
4. Segmentar el servicio en una red aislada (si debiera existir).
5. Aplicar CIS Benchmarks (“Application Software Security” y “Service Hardening”).

Estas acciones apuntan a la vulnerabilidad específica explotada.

Enumeración de redes desde Host A

Acción del atacante (Etapa 3)

Con la sesión Meterpreter activa, se ejecutó route print para identificar si el Host A estaba conectado a múltiples redes.

Cómo se habría detectado (Etapa 4)

- Alertas por comandos ejecutados con privilegios anómalos.
- Evidencia en logs de Windows por acceso a rutas y adaptadores de red.
- Actividad inusual en consultas ARP o tráfico exploratorio (“host discovery”).

Medidas de hardenización asociadas

1. Segmentación de red estricta para que un host en la DMZ no tenga acceso a redes internas.
2. Deshabilitar adaptadores innecesarios en máquinas expuestas.
3. Aplicación de ACL internas para limitar quién puede alcanzar la red 10.0.2.x.
4. Principio de privilegios mínimos: impedir que un proceso comprometido consulte rutas internas.

Pivoting desde Host A hacia HOST B

Acción del atacante (Etapa 3)

El atacante configuró autoroute en Meterpreter y estableció un portproxy, permitiendo que Host A actuara como puente hacia la red interna donde estaba Host B.

Cómo se habría detectado (Etapa 4)

- Tráfico inusual saliendo de Host A hacia una red que normalmente no debería alcanzar.
- Incremento en conexiones SMB desde un host que no debería operar servicios de archivos.
- Cambios en las reglas de red o apariciones de proxys inesperados.
- Alertas por uso de túneles o patrones de pivoting detectables (flujo anómalo entre VLANs).

Medidas de hardenización asociadas

1. Segmentación interna correcta → Host A nunca debería acceder a Host B.
2. Firewall interno restringiendo SMB solo entre equipos autorizados.
3. Bloqueo de creación de reglas portproxy mediante políticas GPO.
4. Network Access Control (NAC) para bloquear tráfico inesperado entre redes.

Sin estas medidas, el pivoting siempre será posible.

Explotación de EternalBlue en Host B

Acción del atacante (Etapa 3)

Tras pivotar, el atacante aprovechó MS17-010 mediante EternalBlue para ejecutar código remoto en Host B.

Cómo se habría detectado (Etapa 4)

- Eventos SMB anómalos detectados por SIEM o IDS.
- Bloques repetitivos de paquetes “trans2” característicos del exploit EternalBlue.
- Logs de Windows mostrando reinicios inesperados de servicios asociados a SMB.
- Alertas por carga de ejecutables no firmados o uso de “service creation”.

Medidas de hardenización asociadas

1. Aplicar parche MS17-010 (mitigación directa del exploit).
2. Deshabilitar SMBv1, protocolo inseguro explotado por EternalBlue.
3. Configurar firewall para permitir SMB solo entre equipos que realmente lo necesitan.
4. Usar EDR con reglas de comportamiento para detener ejecución remota sospechosa.
5. Mantener Windows 7 actualizado o reemplazarlo (fin de soporte desde 2020).

creación de usuario administrativo en HOST B

Acción del atacante (Etapa 3)

El atacante creó un usuario administrador en Host B para garantizar control persistente.

Cómo se habría detectado (Etapa 4)

- Logs de Windows → ID 4720 (creación de usuario).
- Alertas del SIEM ante creación de cuentas privilegiadas.
- Cambios en privilegios de grupos como “Administradores”.

Medidas de hardenización asociadas

1. Habilitar auditoría avanzada de cuentas.
2. Políticas GPO que bloquean creación de usuarios locales.
3. EDR con detección de escalada de privilegios.
4. Revisión diaria de cuentas activas y grupos críticos.

Limpieza / eliminación de rastros

Acción del atacante (Etapa 3)

Tras completar el ataque, se eliminó el usuario para borrar evidencia.

Cómo se habría detectado (Etapa 4)

- Logs: ID 4726 (eliminación de usuario).

- Comparación de eventos antes/después del incidente.
- Incongruencias en auditorías de seguridad.

Medidas de hardenización asociadas

1. SIEM con retención de logs a largo plazo (evita ocultamiento).
2. HIDS para detectar manipulación de cuentas y archivos sensibles.
3. Backups de seguridad del registro de eventos.

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/EVncxv9nuwE

Conclusiones

El ejercicio evidenció que un sistema desactualizado y sin controles adecuados, como Windows 7, puede ser comprometido con relativa facilidad mediante vulnerabilidades públicas ampliamente documentadas.

La explotación de Rejetto HFS y EternalBlue demostró cómo un atacante puede obtener control total del sistema y emplearlo como punto de pivote hacia otros equipos de la red.

El análisis defensivo permitió reconstruir el flujo completo del ataque, confirmando que las buenas prácticas de monitoreo y registro son fundamentales para detectar actividades anómalas.

La ejecución de pruebas ofensivas y defensivas en entornos controlados refuerza significativamente la capacidad de respuesta ante incidentes reales.

La integración entre Red Team y Blue Team facilita una comprensión más profunda del ciclo completo de un ataque y permite desarrollar estrategias de protección más sólidas.

Recomendaciones

Deshabilitar y eliminar servicios obsoletos como SMBv1 y aplicaciones sin soporte como Rejetto HFS.

Implementar un ciclo de actualización y parcheo regular que incluya sistemas operativos, aplicaciones y servicios expuestos.

Adoptar herramientas de monitoreo continuo e integrar los logs en un SIEM para detectar comportamientos anómalos.

Establecer segmentación de red adecuada para evitar movimientos laterales y limitar el alcance de una intrusión.

Fortalecer políticas de acceso, contraseñas y privilegios mínimos para reducir el riesgo de escalamiento interno.

Realizar simulaciones periódicas de Red Team/Blue Team para evaluar la seguridad y mejorar la capacidad de respuesta.

Referencias Bibliograficas

Afif Saktiansyah, M. M. (17 de 01 de 2022). Obtenido de https://journal.universitasbumigora.ac.id/IJECSA/article/view/3297/1445

Center for Internet Security. (2021). Obtenido de The 18 CIS Critical Security Controls: https://www.cisecurity.org/controls/cis-controls-list

CIS - Center for Internet Security. (s.f.). Obtenido de https://www.cisecurity.org/controls

CISCO. (s.f.). Obtenido de What is network access control: https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-access-control-nac.html

CISCO. (08 de 11 de 2018). Obtenido de ¿Qué es un firewall de próxima generación?: https://www.cisco.com/c/en_au/products/security/firewalls/what-is-a-next-generation-firewall.html

Copnia. (2003). *Código de ética*. Obtenido de https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

CrowdStrike. (07 de 01 de 2025). Obtenido de What is Endpoint Detection and Response (EDR): https://www.crowdstrike.com/en-us/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/

Eternalblue. (s.f.). Obtenido de EternalBlue – Everything There Is To Know: https://research.checkpoint.com/2017/eternalblue-everything-know/

Función Pública. (05 de enero de 2009). Obtenido de Ley 1273 de 2009: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Función Pública. (17 de 10 de 2012). Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Función Pública. (27 de 06 de 2013). Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Garg & Bansal. (2021). Obtenido de A Systematic Review on Penetration Testing. In 2021 2nd Global Conference for Advancement in Technology (GCAT) (pp. 1-4). IEEE: https://ieeexplore.ieee.org/abstract/document/9587771

Incibe. (2014). Vulnerabilidad en la función findMacroMarker en Rejetto HFS (CVE-2014-6287). https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-6287

Machap et al. (08 de 2024). Obtenido de A survey of Nmap command builder for learning penetration testing. In AIP Conference Proceedings (Vol. 3161, NMo 1, p.020171). AIP Piblishing LLC: https://pubs.aip.org/aip/acp/article-abstract/3161/1/020171/3310512/A-survey-of-Nmap-command-builder-for-learning

MICROSOFT - ¿Qué es SIEM? (s.f.). Obtenido de https://www.microsoft.com/es-co/security/business/security-101/what-is-siem

Microsoft. (2025). Obtenido de Detectar, habilitar y deshabilitar SMBv1, SMBv2 y SMBv3 en Windows: https://learn.microsoft.com/es-es/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server

Sarker, K. (30 de 04 de 2023). *MPDI*. Obtenido de Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods: https://www.mdpi.com/2071-1050/15/13/10471

Sistema Único de Información Normativa. (2018). Obtenido de https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/30035501

SMB. (2025). Obtenido de Detectar, habilitar y deshabilitar SMBv1, SMBv2 y SMBv3 en Windows: https://learn.microsoft.com/es-es/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server

Apéndices

Apéndice 1

Calificación en Turnitin