Capacidades técnicas, tácticas y de respuesta para equipos red Team y Blue Tam

Miguel Ángel Ortiz Carreño

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2025

Resumen

El presente trabajo es el resultado de un análisis a los procesos de ciberdefensa realizados por Red Team y Blue Team en SecureNova Labs, empresa que ha sido afectada con irregularidades en contratos y atacada desde un Host-A (Windows 7 con HFS 2.3 vulnerable) hacia Host-B vía pivoting y EternalBlue (MS17-010), proceso que derivó a la creación de un usuario administrativo no autorizado y la fuga de datos sensibles de la empresa. A través del laboratorio creado por Red Team, se aplicaron fases de reconocimiento (Nmap, ARP), explotación (Metasploit), post-explotación y pivoting (autoroute, portproxy). Por otro lado, Blue Team propone responder al ataque en tiempo real a partir del uso de herramientas nativas como netstat, tasklist, para la contención: firewall, VLAN, para el hardening: parches, la CIS Controls, y SIEM (Security Information and Event Management) para la activación de eventos. A partir de los procedimientos mencionados anteriormente, los hallazgos sugieren la segmentación de la red, auditorías internas, pruebas recurrentes para mitigar recurrencias en los ataques y puntos vulnerables que propaguen demás accesos no autorizados con el propósito de contribuir a la madurez defensiva de la organización. Además, de que se recomienda la incorporación de las estrategias usadas para mitigar los ataques como una manera de promover y mejorar la ciberdefensa de la empresa tanto para el cuidado de los datos internos como para proteger sus equipos y servidores.

Palabras clave: Ataque, Blue Team, Laboratorio, Red Team, Vulnerabilidades

Abstract

This paper is the result of an analysis of the cyber defence processes carried out by Red Team and Blue Team at SecureNova Labs, a company that has been affected by contract irregularities and attacked from Host-A (Windows 7 with vulnerable HFS 2.3) to Host-B via pivoting and EternalBlue (MS17-010), a process that led to the creation of an unauthorised administrative user and the leakage of sensitive company data. Through the laboratory created by Red Team, phases of reconnaissance (Nmap, ARP), exploitation (Metasploit), post-exploitation and pivoting (autoroute, portproxy) were applied. On the other hand, Blue Team proposes responding to the attack in real time using native tools such as netstat and tasklist for containment; firewall and VLAN for hardening; patches, CIS Controls, and SIEM (Security Information and Event Management) for event activation. The findings suggest that the network segmentation, internal audits, and recurring tests to mitigate attack recurrences and vulnerabilities that propagate further unauthorised access, with the aim of contributing to the organisation's defensive maturity. In addition, it is recommended that strategies to mitigate attacks be incorporated to promote and improve the company's cyber defence, for the protection of internal data and to safeguard its equipment and servers.

Keywords: Attack, Blue Team, Laboratory, Red Team, Vulnerabilities

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Glosario

Análisis Forense

Proceso técnico que busca preservar, identificar, extraer y documentar evidencia de manera digital en sistemas que se ven comprometidos, para realizar una reconstrucción de eventos como accesos no autorizados y actividad realizada por terceros a partir de movimientos laterales.

ARP Scanner

Herramienta para escanear, hace uso de protocolos ARP con los cuales se puede descubrir el uso de hosts activos en una red interna. Así, se pueden identificar dispositivos como el Host-B desde un pivote que compromete el Host-A.

Ataque Lateral (Lateral Movement)

Técnica utilizada por un atacante con el propósito de comprometer un equipo inicial, para desplazarse a través de la red interna para tener información y acceso a otros sistemas y recursos.

Autoroute

Módulo de Metasploit, configura rutas automáticas a través de un host comprometido. Así, logra habilitar el pivoting desde Host-A hacia redes internas como 10.0.2.0/24.

Blue Team

Equipo defensivo de ciberdefensa responsable del monitoreo continuo de la seguridad a través de tareas como la detección, análisis y contención de incidentes que puedan perjudicar a SecureNova Labs, hace uso de herramientas como SIEM y controles CIS para mitigar ataques en tiempo real.

CIS Controls

Conjunto de controles de seguridad que son prioritarios en el Center for Internet Security, aplicados por Blue Team para el hardening de sistemas Windows, segmentación de red y gestión de vulnerabilidades como MS17-010.

EDR (Endpoint Detection and Response)

Software diseñado para solucionar problemas en equipos a través de procesos como el aislamiento automático de dispositivos comprometidos,

bloqueo de procesos maliciosos y contención de movimientos laterales en ataques como el de Host-A.

EternalBlue

Exploit que aprovecha una vulnerabilidad, que es usada por el atacante para realizar infiltraciones ilegales a través de la ejecución de código de forma remota como en este caso se hizo con el equipo Windows.

Exploit (explotación)

Código o procedimiento que busca aprovecharse de una vulnerabilidad en concreto como CVE-2014-6287 en HFS 2.3 de Host-A o MS17-010 en Host-B, para lograr obtener un acceso no autorizado y por ende, privilegios elevados.

Hardening

Proceso en el que se brinda un fortalecimiento de sistemas mediante parches, deshabilitación de servicios innecesarios, segmentación de red y principio de mínimo privilegio con el fin de prevenir incidencias del ataque en SecureNova Labs.

HFS 2.3

HttpFileServer versión 2.3, servicio web vulnerable en puerto 80 de Host-A (192.168.1.83), el cual es explotado por vía Rejetto HFS para shell remota y pivoting inicial. **Host-A.** Equipo Windows 7, el cual es el equipo comprometido inicialmente en el ataque porque estaba vulnerable, a través de este, se dio la fuga de datos hacia Host-B mediante pivoting y EternalBlue.

Host-B

Es el servidor interno en red 10.0.2.0/24 vulnerable a MS17-010, que fue accesible por vía pivoting desde el Host-A, en el que se creó un usuario administrativo no autorizado por parte del atacante, mediante el que se transfirieron datos internos de SecureNova Labs.

Meterpreter

Payload avanzado de Metasploit que proporciona shell interactiva post- explotación, el cual es usado para sysinfo, getuid, ipconfig, además de la creación de usuarios en Host-A y Host-B.

MS17-010

Vulnerabilidad crítica que se presenta en el protocolo SMB de Windows (EternalBlue), la cual fue detectada en Host-B vía Nmap, para explotar privilegios elevados mediante la persistencia administrativa.

Pivoting

Técnica ofensiva en el que un host comprometido como Host-A, usado como un puente para atacar redes internas a través de la configuración de autoroute y portproxy hacia Host- B.

Portproxy

Mecanismo para redireccionar puertos en Metasploit, aplicado para forwardear tráfico SMB (puerto 445) desde Kali hacia Host-B mediante Host-A.

Red Team

Equipo que simula ataques cibernéticos reales en laboratorios aislados para recrear compromiso de Host-A vía HFS 2.3 y pivoting a Host-B para identificar vectores en SecureNova Labs, con el objetivo de evaluar la seguridad proporcionada a la organización.

SIEM (Security Information and Event Management)

Sistema especializado para centralización, correlación de logs y alertas en tiempo real, esencial para Blue Team en cuanto a la detección de anomalías como en Host-A.

Timeline Forense (Línea de Tiempo Forense)

Cronograma secuencial de eventos de seguridad reconstruido desde logs y artefactos, usado para lograr mapear explotación en Host-A, pivoting y la creación de usuario en Host-B.

Introducción

Este documento tiene como propósito presentar un análisis detallado que se ha desarrollado a lo largo de las etapas del seminario especializado, en las cuales, se han realizado reportes técnicos realizados por parte de Red Team y Blue Team, equipos que fueron contratados por la empresa SecureNova Labs. Teniendo en cuenta que la infraestructura ha presentado vulnerabilidades que fueron explotadas desde el momento de su contratación, tanto en los contratos emitidos inicialmente que contenían irregularidades como en divulgaciones no autorizadas de datos desde Host-A hacia Host-B, privilegios elevados, traspaso de archivos, datos e información.

Por lo tanto, este trabajo se centra en realizar un reporte de estas problemáticas enfrentadas por Red Team y Blue Team para identificar, examinar y esclarecer las problemáticas que se presentaron en cuanto al acceso no autorizado a la información interna de la empresa. De manera que este análisis contiene los laboratorios realizados con los cuales, se encontraron las irregularidades y se indicaron las posibles soluciones que pueden impedir futuros ataques. Así, el enfoque de este trabajo se basa en el análisis de las problemáticas para ayudar a dimensionar los laboratorios aislados que ayudaron a interpretar lo sucedido.

Igualmente, se ha procurado tener una visión reflexiva para evaluar y cuestionar las dinámicas halladas. A lo largo del documento, se desarrollan las principales problemáticas presentadas para Red Team y Blue Team en cuanto a las vulneraciones en sus sistemas de seguridad, además del timeline y el análisis forense realizado para poder brindar soluciones al respecto teniendo en cuenta la naturaleza del ataque.

Finalmente, se presentan recomendaciones y conclusiones que buscan aportar al campo profesional, con el propósito de brindar soluciones de acuerdo con las problemáticas presentadas.

También, se busca que este estudio pueda contribuir al campo académico a partir del análisis de la selección de las herramientas y los procesos realizados con estas, los cuales, ayudaron a mitigar el ataque. De esta manera, se espera realizar un aporte a la comprensión de este tipo de fenómenos.

Justificación

La elección de este tema para el desarrollo del presente trabajo corresponde a la necesidad de impactar de manera significativa en los distintos ámbitos de la sociedad. En este caso, se busca brindar soluciones a una parte de las problemáticas que se desprenden del sector tecnológico, tal como lo son los ataques a la ciberseguridad de las empresas. Así, este trabajo reporta y comunica el análisis realizado de los casos presentados en Red Team y Blue Team, que sirvieron como base para identificar, examinar y esclarecer los ataques sufridos. Consecuentemente, se establecieron una serie de soluciones a este tipo de problemáticas con el objetivo de proteger los equipos para mitigar ataques futuros.

En este orden de ideas, también se busca impactar de manera positiva a la comunidad, empresas e instituciones, dado que la naturaleza de este reporte es contribuir el abordaje de problemáticas en el mundo tecnológico como se ha hecho a lo largo de las etapas 1, 2, 3 y 4, las cuales se integran y sintetizan a lo largo de este trabajo como el resultado de los aprendizajes adquiridos a lo largo del seminario.

Se establece una relación entre la demostración de las vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión, la formulación de estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI y la evaluación de las acciones de los equipos Red Team y Blue Team de una organización en el marco de los criterios éticos y legales, a través de diversas propuestas y procesos que favorezcan la comprensión y el tratamiento adecuado de estos.

Igualmente, se tuvieron en cuenta las particularidades de los ataques sufridos, se busca formular estrategias de protección para suplir los vacíos que puedan existir alrededor de este tema específico. Por lo tanto, esta investigación busca realizar un aporte al conocimiento desde la

evidencia empírica y la reflexión crítica para fomentar los procesos conscientes e informados en la protección de datos en la ciberseguridad.

De este modo, la justificación del presente trabajo radica en su potencial para un impacto positivo tanto para el campo académico como el profesional, puesto que los hallazgos, resultados, recomendaciones y conclusiones, pueden ser utilizados tanto como base para la creación de programas y diseño de demás líneas de estudio en ciberseguridad como para la resolución de problemáticas similares en el entorno laboral que exijan intervenciones similares como las realizadas a lo largo de esta investigación

Objetivos

Objetivo General

Analizar el impacto de los ataques cibernéticos de Red Team y Blue Team, quiénes prestan sus servicios de protección a SecureNova Labs, con el fin de comprender sus principales causas, efectos y posibles soluciones.

Objetivos Específicos

Identificar los factores que contribuyen al desarrollo de los ataques cibernéticos en SecureNova Labs, a través de Red Team y Blue Team mediante la recopilación de información teórica y empírica de laboratorios.

Examinar los factores que contribuyen al desarrollo de los ataques cibernéticos en SecureNova Labs, mediante la recopilación y análisis de contratos irregulares y análisis forense de los movimientos del atacante.

Esclarecer los factores que contribuyen al desarrollo de los ataques cibernéticos en SecureNova Labs, mediante la recopilación y análisis de información teórica y empírica de timelines y mitigaciones.

Relación entre Aspectos Legales y Éticos

Contratos Irregulares

Respecto a los inconvenientes presentados con el contrato de confidencialidad que SecureNova Labs le presenta a Red Team y Blue Team, en el cual se exponen las obligaciones que estas empresas deben seguir para garantizar un buen servicio y evitar inconvenientes legales. No obstante, al revisar el contrato, se encuentran diversas ambigüedades, cláusulas no éticas que infringen las políticas colombianas sobre la protección de datos personales.

Además, de que afectan la buena imagen y el profesionalismo de SecureNova Labs, dado que no se cumplen con los objetivos elementales de la ciberseguridad ni la revisión de los contratos con terceros. Esto también presenta un riesgo tanto para la empresa como para los ingenieros que trabajan con ella, puesto que, según el (Copnia 2015) estos pueden ser inhabilitados por la violación a su código ético.

Consecuentemente, se infringen las Políticas de Privacidad y Condiciones de Uso estipuladas por (MINTIC 2022), las cuales exigen que haya estrategias de seguridad digital con las que se pueda brindar y garantizar los derechos a la privacidad de los ciudadanos.

Por lo tanto, debe existir un manual, formato, etc en el que se integren lineamientos para el manejo de la seguridad. Teniendo en cuenta el caso de SecureNova Labs, se puede intuir que tampoco existen lineamientos de protección, dado que los contratos poseen cláusulas ilícitas que atentan contra el profesionalismo de la empresa y de sus empleados.

Mitigar Irregularidades y Vacíos Legales

En primera instancia, la empresa SecureNova Labs, debió realizar una revisión de los contratos debido a los inconvenientes presentados con el abogado que los diligenció porque esto podría indicar irregularidades también dentro de la elaboración de los contratos. Debido a lo

anterior, se presentan rupturas que infringen la (Copnia 2015) como realizar actividades ilícitas con la información personal. En este sentido, el contrato prohíbe realizar denuncias respecto al uso indebido de los datos. A pesar de contar con distintos ítems que cumplen a cabalidad los requerimientos de las leyes como la devolución de la información y sus copias una vez se haya acabado su relación con las empresas, no significa que la empresa haya realizado un contrato ético.

Sin embargo, esto puede deberse a una falta de claridad. Teniendo en cuenta las normativas y leyes colombianas, este tipo de irregularidades en procesos de contratación pueden ser comunes debido a la falta de capacitación sobre las políticas encargadas de la protección de datos y ciberseguridad en el país. De modo que, el desconocimiento y la poca aplicación de este tipo de normativas puede perjudicar la seguridad tanto de las empresas como de los individuos como lo manifiestan Enríquez y López (2023) “El marco normativo actual en Colombia, aunque ha avanzado en la regulación de la ciberseguridad y la seguridad de la información, aún presenta desafíos en términos de claridad, consistencia, aplicación y coordinación interinstitucional” (p, 29).

Igualmente, se presentan ítems como el segundo del contrato en el que se habla de la “Definición de información confidencial”, en la cual se mencionan las chuzadas, interceptaciones y demás maneras de obtener información confidencial y privada de forma no legal. De esta manera, se vulneran las normativas colombianas como la ley 1581 del 2012, específicamente, se vulnera el artículo 269A en el cual se establece que se debe pedir la información al ciudadano o a la empresa de manera directa, además de notificar para qué será usada.

También se presentan ítems como en la cuarta parte del contrato, denominada "Obligaciones de la parte receptora", en el que el tercer ítem, el cual es no legal y no ético, estipula que la empresa no se hace responsable de la información de los usuarios una vez hayan pasado a manos de terceros, así sea que esta sea usada de manera indebida. En este sentido, se vulnera el artículo 269F que protege los datos personales, específicamente aquellos datos que son vulnerables como direcciones, correos, contraseñas, etc.

De manera complementaria, también se presenta el cuarto ítem del contrato que sostiene que tampoco se puede realizar alguna denuncia o acción legal si los terceros usan la información personal para actividades sospechosas. Esto representa peligro y vulneración al derecho de la privacidad de las personas. Además, de que esto afecta la ética profesional de los trabajadores, dado que se busca que no actúen cuando haya delitos cibernéticos, lo cual afecta la honestidad y transparencia de la empresa. Por estas razones, se atenta contra la certificación de la autorización y el consentimiento para el uso de los datos personales. A partir de este aspecto es que se presenta vía libre para divulgar la información de manera indirecta a través de terceros.

Por lo tanto, este incumplimiento representa una violación a las leyes y normativas colombianas como a la Ley 1581 de 2012, en la cual se centra el principio de finalidad que consiste en que la información personal sea usada para el propósito del cual el titular tiene conocimiento, es decir, no debe usarse por demás razones. También se incumple con el principio de libertad, puesto que el tratamiento de los datos por parte de terceros se puede realizar cuando haya un consentimiento del titular para el uso de su información y simultáneamente se incumple con el principio de confidencialidad porque no se garantiza la reserva ni la garantía del cuidado de la información.

De lo contrario, se atenta contra el artículo 269H de la Ley 1851 de 2012, especialmente en su quinto ítem que manifiesta “5. Obteniendo provecho para sí o para un tercero” (p, 2), puesto que no se establece una relación directa de trabajo con terceros y tampoco se específica el porqué del uso de información y que datos personales se usarían en caso de que los clientes accedan a que otra empresa, entidad o persona acceda a su información.

Por otro lado, también se señala la octava cláusula del contrato como irregular, dado que en ella se expresa que en caso de que se obtenga información ilegal, el proceso legal se realizará bajo circunstancias privadas en las que la empresa no será involucrada. Esto hace que el caso se concentre en una de las partes y que SecureNova Labs sea exonerada de sus responsabilidades judiciales y que no se castiguen a los culpables.

Además, de que nuevamente se incumple el artículo 269D, llamado “Daño informático” de la ley 1273 de 2009, el cual estipula un castigo penitenciario o multa por un mal uso del manejo de datos informáticos. Por lo tanto, la ley establece que al incumplir las normativas y causar un daño informático, quién lo haya cometido debe ser sometido a la justicia por el uso indebido de los datos de las personas para iniciar el debido proceso.

En este sentido, al no cumplir con los principios para la protección de los datos personales, las empresas deben responder ante la justicia, dado que se vulnera el derecho de privacidad, el cual se encuentra estipulado dentro del artículo 15 de la Constitución Política de Colombia, “En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.”(p, 7), puesto que este establece que los ciudadanos tienen derecho al buen nombre y que el estado debe hacer respetar esto, además de que se tiene el derecho a conocer la información personal usada tanto por entidades públicas como privadas.

Además, el artículo 269F de la Ley 1581 del 2012 contempla la divulgación de información sin consentimiento como un delito de robo y uso ilícito de datos personales, dado que se puede hacer suplantación, fraude y violación a la intimidad a partir de estos incumplimientos de los principios de esta misma ley. Por esta razón, las normativas han optado por garantizar el tratamiento de los datos personales bajo medidas de seguridad como las que El Parlamento Europeo y El Consejo De La Unión Europea (2016) han estipulado a través del Reglamento General de Protección de Datos de la Unión Europea, dado que son normativas internacionales que contemplan diversas situaciones y diferentes tipos de información que pueden llegar a afectar la protección de los derechos de las personas.

Por lo tanto, la ley colombiana establece obligaciones que deben ser cumplidas por las entidades para poder cumplir con las leyes y normativas colombianas al respecto como informar sobre la información usada, garantizar el buen uso de los datos personales y en caso de que esta haya sido usada de manera indebida, la entidad debe responder por este incumplimiento, ya sea como lo estipula la ley 1273 del 2009 a través de artículos como el 269F y 269G, los cuales contemplan multas económicas y cárcel entre los 48 y 96 meses.

Teniendo en cuenta lo expuesto anteriormente, los vacíos legales e irregularidades presentan diversas situaciones no éticas y no legales, las cuales, atentan de manera directa contra los derechos básicos de los ciudadanos como la garantía del buen uso de su información. Igualmente, al encubrir este tipo de delitos informáticos a través de un contrato laboral corporativo demuestra falta de profesionalismo, dado que no se conocen las normativas colombianas, además de que estas acciones carecen de ética porque el contrato es una manera de validar el quebramiento de la ley.

Finalmente, la empresa SecureNova Labs, para evitar los inconvenientes legales producto de las cláusulas ilegales y ambiguas elaboradas por su antiguo abogado, debe realizar una revisión del contrato en la cual se modifiquen aquellos parámetros y requisitos que incumplan las leyes colombianas para la protección de datos y privacidad de los ciudadanos. No obstante, esta revisión no se debe realizar exclusivamente por evitar inconvenientes legales, sino por fortalecer su ética profesional, la cual significa confiabilidad, puesto que se debe delimitar el acceso a la información personal sensible de los clientes porque se debe garantizar el uso adecuado de esta sin que se vulneren las leyes.

Implicaciones Éticas

En cuanto a la visión particular e individual de este caso, a pesar de que este tipo de contrato represente un alto beneficio económico como un salario de $15.000.000 de pesos, además de la estabilidad financiera y laboral que puede representar, es poco ético laborar bajo estas condiciones, dado que se vulneran y violan diversas normativas colombianas como las mencionadas anteriormente que buscan proteger la privacidad de los ciudadanos.

Además, de que aceptar un trabajo como este representa poco profesionalismo y una ética nula, porque tampoco se tiene presente el (Copnia 2015), el código ético de los ingenieros. En resumen, aceptar un trabajo laboral bajo estas condiciones representa la muerte ética y moral del ingeniero, dado que se le da más prioridad al beneficio personal que al cumplimiento adecuado de la ley.

Al respecto de la ética laboral de los ingenieros, la empresa debe también prevenir la vulneración a la información interna a través de distintos mecanismos como auditorías internas en las que se usen estaciones forenses también ayuda a complementar la tarea de la auditoría, dado que con esta herramienta se puede realizar una revisión profunda.

Igualmente, las auditorías externas, pueden ayudar a que haya una revisión exhaustiva en la que se pueda realizar una verificación de los datos de la empresa. De manera que, bajo la premisa de la ética laboral de los ingenieros y los hallazgos encontrados con el desarrollo del laboratorio, es fundamental lograr la integración de los resultados dentro de las estrategias de la empresa. De esta manera, se puede promover la proactividad en la protección de los activos digitales mientras que se dinamizan las dinámicas de cuidado de la empresa y se trabaja por contrarrestar la hostilidad que pueden generar las vulnerabilidades (Mizrak, 2023).

También se deben tener en cuenta la creación de políticas internas en las que se estipule de manera clara y explícita los riesgos que tienen las herramientas avanzadas de análisis forense sin autorización. Además, de capacitaciones constantes al respecto para asegurar el tratamiento adecuado de los datos de la empresa.

Posición Ética

Respecto a las condiciones que se gozarían al ser empleado de SecureNova Labs como disponer de un salario alto y de un contrato vitalicio, estas características no deberían ser pretexto para aceptar trabajar bajo cláusulas poco éticas que atentan contra los principios de la profesión y no legales que contradicen la legislación vigente. A pesar de la búsqueda de normalizar conductas ilícitas a través del contrato como lo es la interceptación de comunicaciones, el acceso abusivo a sistemas informáticos y la omisión deliberada de denuncias ante autoridades, aceptar ese tipo de contrato implicaría asumir riesgos penales directos por violación a las leyes colombianas, que sancionan el acceso no autorizado, la violación de datos personales y la participación en actos agravados cometidos bajo posición de confianza.

Desde el punto de vista del Código de Ética Profesional del COPNIA, se establece que el ingeniero debe actuar siempre conforme a la ley, preservar el interés público, y abstenerse de

ejecutar trabajos que vayan en contra de los valores sociales o morales. La aceptación de un contrato que pretende silenciar posibles delitos informáticos sería equivalente a renunciar a los principios de honestidad, transparencia y responsabilidad social que caracterizan el ejercicio de la ingeniería.

Desde la percepción personal como experto en ciberseguridad, se entiende que el valor del trabajo no se mide solo por el salario, sino por la credibilidad profesional y la confianza social que se construyen a lo largo de los años. Aceptar un contrato ilegal comprometería la reputación y la integridad de los sistemas que, como empleado, se deben proteger.

Por lo tanto, la decisión personal sería la de rechazar la oferta laboral en los términos propuestos y solicitar la revisión o modificación del acuerdo, asegurando que se excluyan las prácticas ilícitas, se garantice la transparencia, y se ajusten las cláusulas al marco legal colombiano y a los principios éticos del COPNIA.

Mecanismos de Supervisión para la Ética en el Equipo de Trabajo

Los mecanismos de supervisión se pueden ver reflejados en la gobernanza de la seguridad robusta: Matrices RACI claras sobre quién autoriza, ejecuta y supervisa. Además de la segregación de funciones entre equipos Red Team, Blue Team y Forense. Igualmente, las auditorías internas y externas periódicas y el uso de estaciones forenses bastionadas, bitácoras cifradas acompañadas de monitoreo mediante SIEM y UEBA, ayudan a establecer puntos de referencia para el control interno de la empresa.

Estas políticas disciplinarias acompañadas de la capacitación ética continua contribuyen a promover estrategias para el cuidado. Además, el MSPI del MinTIC (2023) refuerza estos controles al exigir trazabilidad completa de accesos y medidas de privacidad alineadas con ISO/IEC 27001.

Confianza y Respuestas en Caso de Ciberespionaje

En caso de que se vea infringida la ciberdefensa de las organizaciones deben activar inmediatamente su plan de respuesta a incidentes, aislar el acceso comprometido, preservar evidencias digitales y notificar a las autoridades competentes (Fiscalía, MinTIC o CCIC).

El gobierno, por su parte, debe aplicar la Ley 1273, abrir investigaciones penales y sancionar tanto a las empresas como a los profesionales implicados.

Además, debe fortalecer los mecanismos de certificación ética y de auditoría para las compañías de ciberseguridad, garantizando que quienes prestan servicios críticos cumplan con estándares técnicos y morales. Solo mediante una respuesta coordinada legal, técnica y ética se preserva la confianza en el ecosistema digital y se reafirma que la ciberseguridad debe servir para proteger, no para espiar.

Tabla 1

Tareas de las Organizaciones y del Gobierno

Actor	Responsabilidades a Cargo
Organizaciones	Realizar la activación del plan de respuesta a incidentes. Aislar accesos comprometidos, preservar evidencias digitales para realizar la respectiva notificación en las autoridades competentes como la Fiscalía, MinTIC o CCIC.
Gobierno	Aplicar de manera eficiente las normativas como la Ley 1273. Realizar investigaciones, sancionar tanto a empresas como profesionales implicados en delitos cibernéticos. Fortalecer la educación ética. Realizar auditorías de manera periódica.

Nota. En la tabla anterior se presentan de manera concisa los actores que intervienen en la confianza y las respuestas al ciberespionaje con sus respectivas tareas.

Estrategias de Red Team

Las estrategias empleadas por el equipo Red Team se centran en aplicar una metodología de pentesting, la cual es definida por Incibe (2019) en "¿Qué es el pentesting?" como "[…] un conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas". (párr, 9). De modo que esta estrategia se realizó dentro de un laboratorio aislado con Kali Linux con el propósito de recrear el ciberataque sufrido en SecureNova Labs desde el Host-A (192.168.1.83, HFS 2.3 puerto 80) hacia el Host-B (10.0.2.0/24) para realizar un seguimiento a lo hecho por el atacante.

Igualmente, (Chindrus y Caruntu, 2023) presentaron un enfoque en el cual usaban los equipos Red Team para simular un ciberataque, de manera que Blue Team realizaba un proceso de ciberdefensa. Así, los autores presentaron un método práctico, en el que los mismos equipos aliados podían trabajar en el mejoramiento de sus estrategias defensivas, táctica que también es implementada a lo largo de este apartado para tratar un problema específico, el cual, puede ser visto como una guía o formato para tratar ataques similares de acceso no autorizado con el propósito de mitigar vulnerabilidades y mejorar la seguridad.

Para realizar este enfoque de estrategias, se incluyen los siguientes procesos para hallar los pasos del ataque como el reconocimiento (arp-scan, ping), el escaneo Nmap intensivo (-p- -sS -sC -sV), la enumeración (searchsploit CVE-2014-6287), la explotación Metasploit (rejetto_hfs_exec para Meterpreter), el post-explotación (ipconfig, ls fuga datos), el pivoting (autoroute, ARP scanner, portproxy 445→4443), la validación MS17- 010 y, por último, la creación administrativa usuario efímero.

Sin embargo, podría decirse que la intención del laboratorio realizado se centra más en saber y entender cómo el atacante logró tener acceso no autorizado al equipo Windows que en saber qué información interna usó. De esta manera, Cubillos y López (2022), señalan que para las empresas la información no es lo único fundamental para el cuidado de los datos de la empresa, también lo son sus canales de transmisión:

> Actualmente las entidades no solo consideran la información como el único activo de valor, también están teniendo en cuenta los diversos canales de transmisión, en el sentido que por medio de ellos viaja un gran flujo de datos y pueden correr el riesgo de ser vulnerados si no se tienen los parámetros de seguridad aceptables (p. 9).

A través del laboratorio aislado se pudo recrear el escenario por el cual el atacante ahondó y logró obtener información interna de la empresa a través de la creación de un nuevo usuario con acceso no autorizado, interceptando el equipo Windows de SecureNova Labs. Posteriormente, se presentan las fases llevadas a cabo durante el laboratorio para identificar los factores que contribuyeron al desarrollo de los ataques cibernéticos en SecureNova Labs, a través de Red Team y Blue Team mediante la recopilación de información teórica y empírica de laboratorios. Además de examinar los factores que contribuyen al desarrollo de ataques cibernéticos, mediante la recopilación y análisis contratos irregulares y análisis forense de los movimientos del atacante.

A continuación, se presentan las fases desarrolladas a lo largo del laboratorio aislado, con el cual, se desglosó el análisis técnico de las etapas:

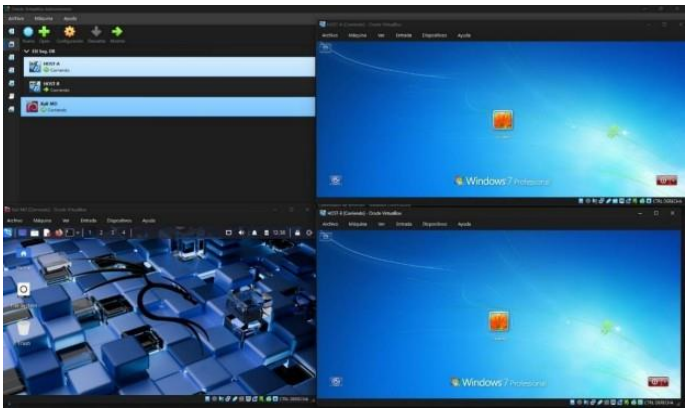
Fases del Laboratorio: Preparación del Entorno – Kali Linux

Se implementó un entorno de virtualización utilizando Oracle VirtualBox, en el cual se desplegaron dos máquinas virtuales con sistema operativo Windows 7 a partir de archivos OVA, así como una máquina virtual con Kali Linux. Este entorno fue preparado con el objetivo de

establecer un laboratorio controlado para el desarrollo de pruebas y ejercicios prácticos, garantizando el aislamiento y la seguridad de las actividades realizadas.

Figura 1

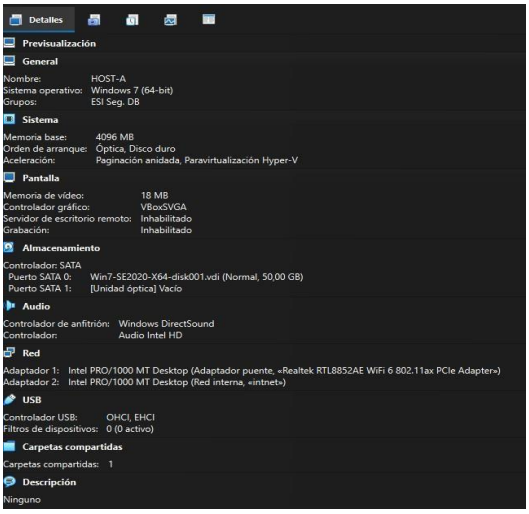
Entorno Virtual



Nota. Entorno virtualizado utilizado en el laboratorio, 1 maquina Kali Linux y 2 máquinas Windows.

Figura 2

Configuración de Máquina 1 (Host A)

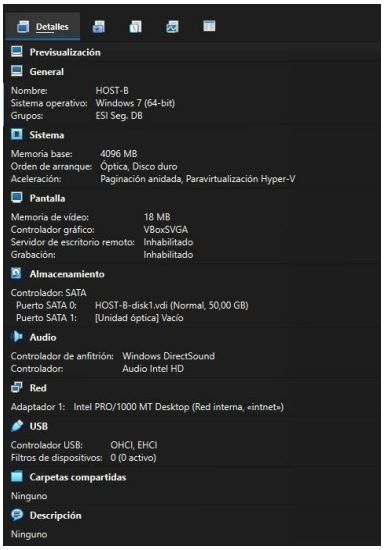


Nota. Representación visual de la configuración de la Maquina 1 (Host A) con 2 tarjetas de Red

(Externa/Interna).

Figura 3

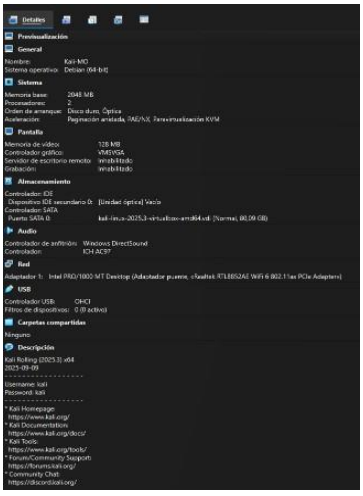
Configuración de Máquina 2 (Host B)



Nota. Representación visual de la configuración de la Maquina 2 (Host B) con 1 tarjeta de Red (Interna).

Figura 4

Configuración de Máquina 3 (Kali Linux)



Nota. Representación visual de la configuración de la Maquina Kali Linux con 1 tarjeta de Red (Externa).

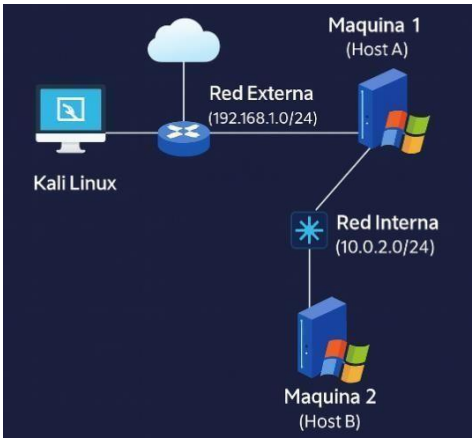
La distribución de red implementada para el laboratorio y la interacción entre los distintos componentes del entorno virtualizado es la siguiente:

Red externa: 192.168.1.0/24

Red interna: 10.0.2.0/24

Figura 5

Diagrama de Red de Laboratorio



Nota. El diagrama representa la arquitectura de red del laboratorio, mostrando la conexión del equipo Kali Linux hacia la *Red Externa* (192.168.1.0/24), la cual enlaza con la Máquina 1 (Host A).

Validación de Red

Desde la terminal de Kali se ejecutó ifconfig, confirmando que la interfaz eth0 tenía:

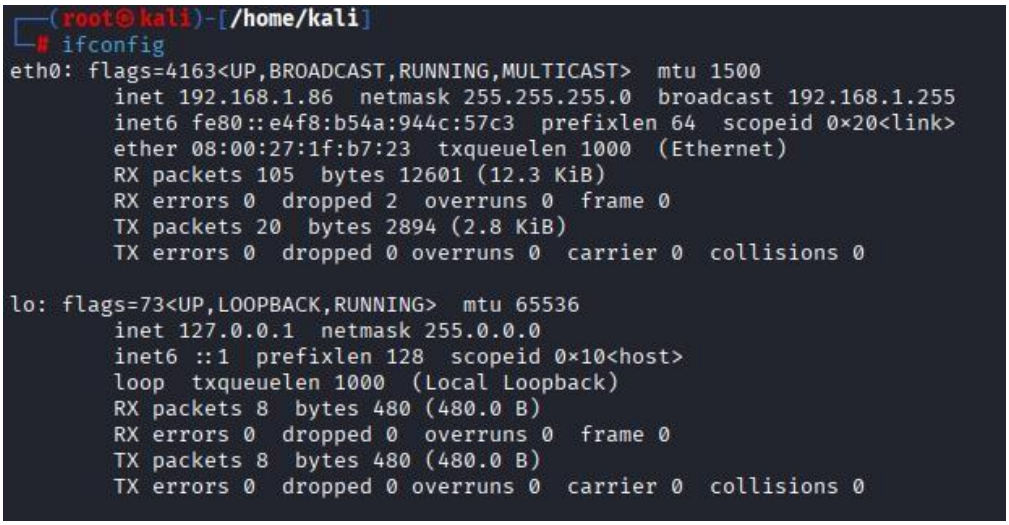
Dirección IP: 192.168.1.86

Máscara: 255.255.255.0

Gateway dentro de la red 192.168.1.0/24

Figura 6

Configuración de Red en Kali Linux – Ifconfig



Nota. Salida detallada del comando ifconfig evidenciando interfaces activas, dirección IPv4 asignada, máscara, MTU y parámetros de red esenciales para el reconocimiento.

Se verificó el estado general de paquetes con apt para asegurar que las herramientas como Nmap, Metasploit, arp-scan y otras estuvieran disponibles y actualizadas.

Fase de Reconocimiento

Descubrimiento de Hosts en la Red 192.168.1.0/24

Mediante un escaneo ARP sobre el segmento 192.168.1.0/24 se identificaron varios dispositivos. Entre ellos, se destacó la dirección 192.168.1.83, la cual se asumió como Host A.

Figura 7

Descubrimiento de Red – Identificación de Host A (192.168.1.83)

Nota. Trama ARP descubierta mediante arp-scan, confirmando presencia activa de un host con respuesta ARP sin requerir ICMP, característica relevante en redes con filtrado.

Se intentó un ping tradicional (ping -c 3 192.168.1.83), sin obtener respuesta ICMP, aunque el host sí respondió a nivel de ARP, confirmando que estaba encendido y conectado a la red.

Fase de Escaneo y Enumeración – Host A

Escaneo de Puertos con Nmap

Se ejecutó un escaneo intensivo con Nmap:

Todos los puertos (-p-)

Escaneo SYN (-sS)

Scripts básicos (-sC)

Detección de versión (-sV)

Sin resolución DNS (-n)

Modo sigiloso moderado

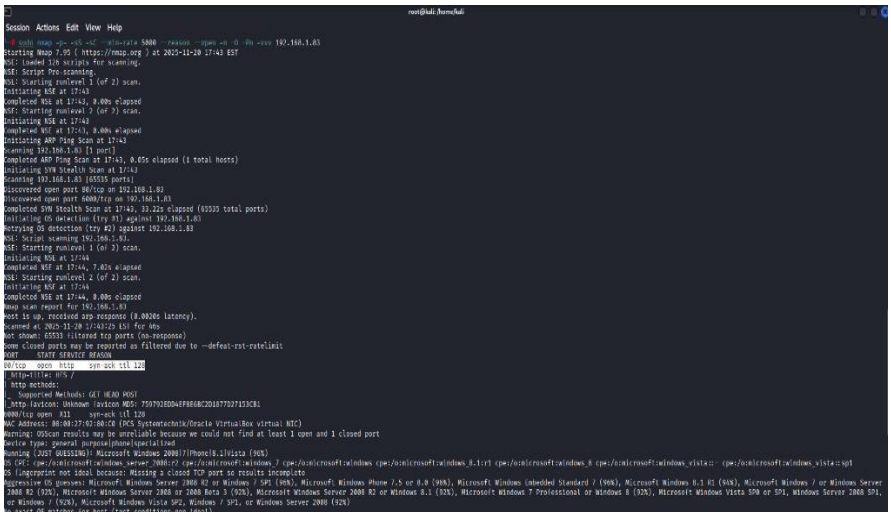
El resultado mostró un único puerto abierto:

80/tcp → Servicio HttpFileServer (HFS) 2.3

El escaneo con Nmap queda en evidencia en la siguiente captura:

Figura 8

Escaneo Nmap a Host A – Puerto 80 Abierto con HFS 2.3



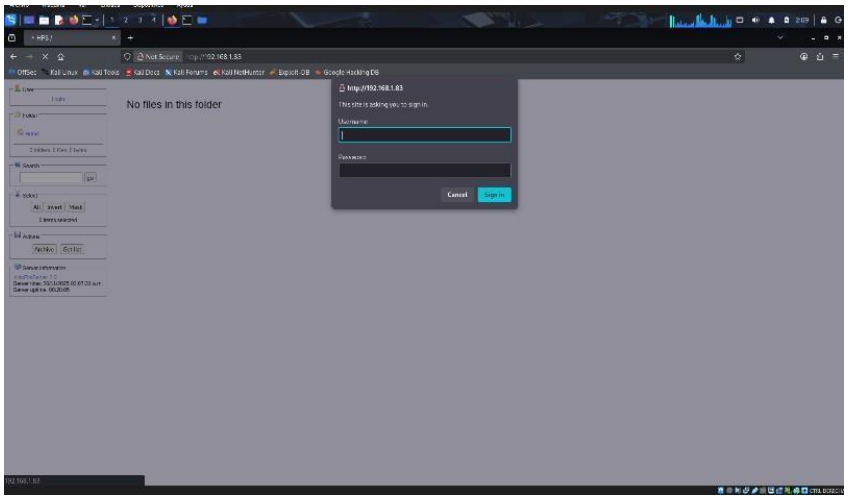
Nota. Resultado escaneo Nmap, se identifica SYN stealth (-sS) enumerando el puerto 80/tcp ejecutando HttpFileServer 2.3; correlación directa con vector de explotación CVE-2014-6287.

Enumeración de Servicio HFS 2.3

A partir del uso del navegador de Kali se accedió a http://192.168.1.83/, validando que se trataba de HFS 2.3. Posteriormente se utilizó searchsploit hfs 2.3 para identificar exploits conocidos, encontrando referencias a CVE-2014-6287, vulnerabilidad crítica de ejecución remota de código, (Fortra.com, 2022) señala la importancia de establecer escaneos periódicos para prevenir explotación de riesgos por parte de terceros no autorizados.

Figura 9

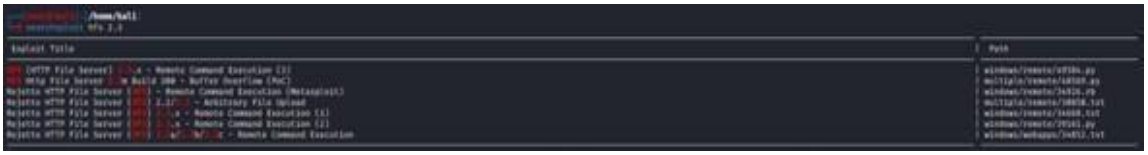
Interfaz Web de HFS 2.3 en Host A



Nota. Interfaz HTTP de HFS 2.3 revelando el árbol de directorios y confirmando versión vulnerable asociada a ejecución remota de comandos.

Figura 10

Resultados de Searchsploit para HFS 2.3



Nota. Matriz de exploits asociados a HFS 2.3 recuperados vía Searchsploit, permitiendo mapear payloads compatibles con Metasploit.

Este análisis permitió concluir que el servicio web constituía el principal vector de ataque contra Host A.

Fase de Explotación – Compromiso de Host A

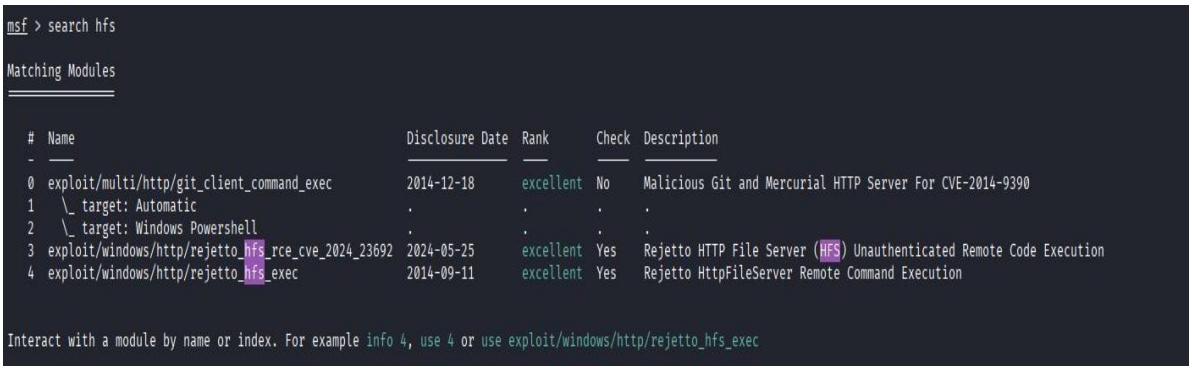
Desde Kali Linux se inició Metasploit (msfconsole) y se buscó el módulo relacionado con HFS:

Search hfs

Selección de exploit/windows/http/rejetto_hfs_exec

Figura 11

Búsqueda y Selección del Módulo Rejetto HFS en Metasploit



Nota. Resultado de la búsqueda del módulo Rejetto HFS.

Se configuraron los parámetros clave:

RHOSTS → 192.168.1.83

RPORT → 80

Opciones del payload para obtener una sesión Meterpreter reversa desde Host A. Tras ejecutar el exploit, se obtuvo una sesión Meterpreter activa sobre Host A.

Figura 12

Ejecución del Exploit y Apertura de Sesión Meterpreter en Host A

Nota. Ejecución exitosa del payload reverse TCP con establecimiento de canal Meterpreter cifrado mediante pipeline TCP.

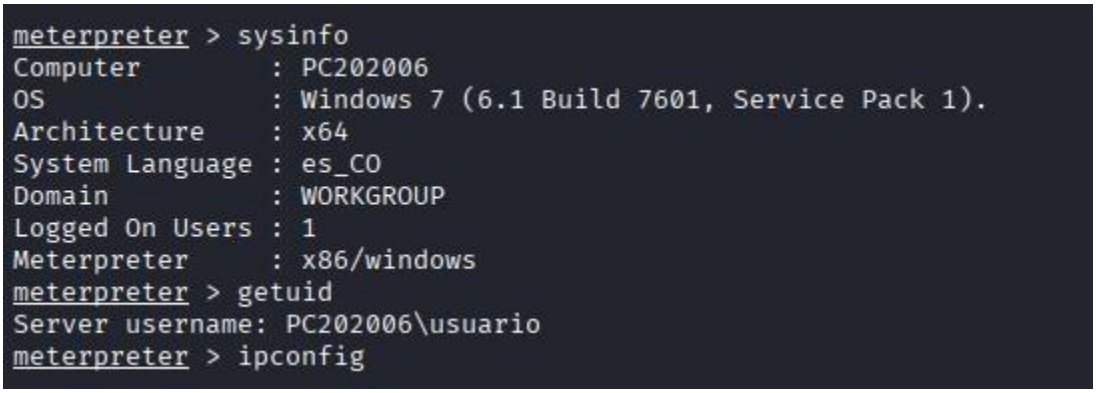
Mediante sysinfo y getuid se verificó:

Sistema operativo: Windows 7

Hostname: PC202006

Figura 13

Información de Sistema en Host A – Sysinfo / Getuid



Nota. Enumeración del entorno comprometido: arquitectura NT, build version, usuario en contexto, y privilegios disponibles para post-explotación.

Fase de Post-Explotación – Host A

Con la sesión activa en Host A, se ejecutó ipconfig para conocer las interfaces de red. Por lo tanto, se observó lo siguiente:

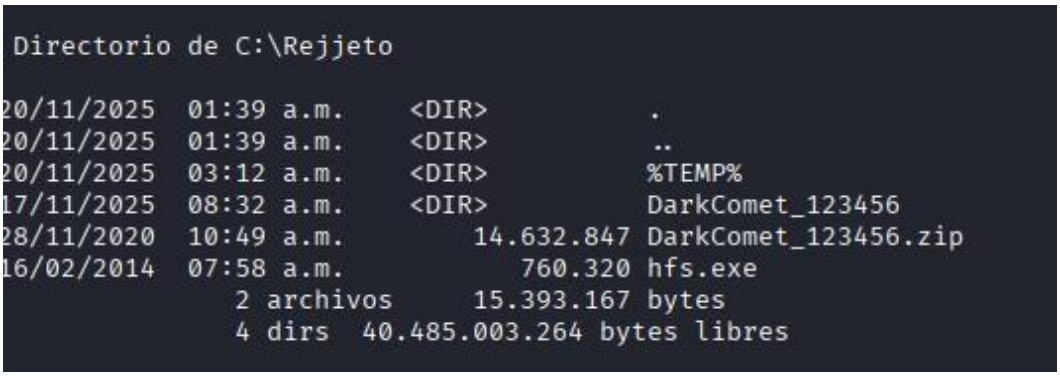
Una interfaz en la red 192.168.1.0/24.

Una segunda interfaz en la red 10.0.2.0/24, indican que Host A tenía conectividad hacia otra red interna.

Adicionalmente, se listaron directorios y archivos para fuga de información desde la estación de trabajo comprometida, guardando evidencia de directorios accesibles desde la sesión Meterpreter.

Figura 14

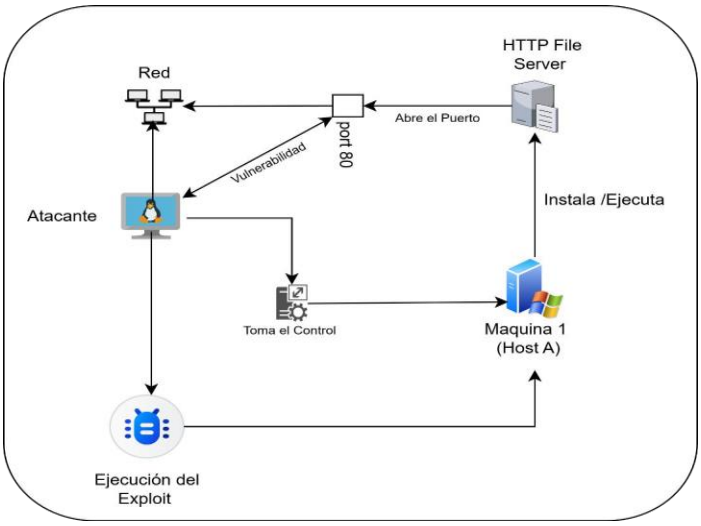
Listado de Archivos en Host A a Modo de Fuga de Información Simulada



Nota. Exfiltración simulada listando directorios críticos accesibles desde el contexto del exploit.

Figura 15

Diagrama Explicación del Ataque Rejetto 2.3

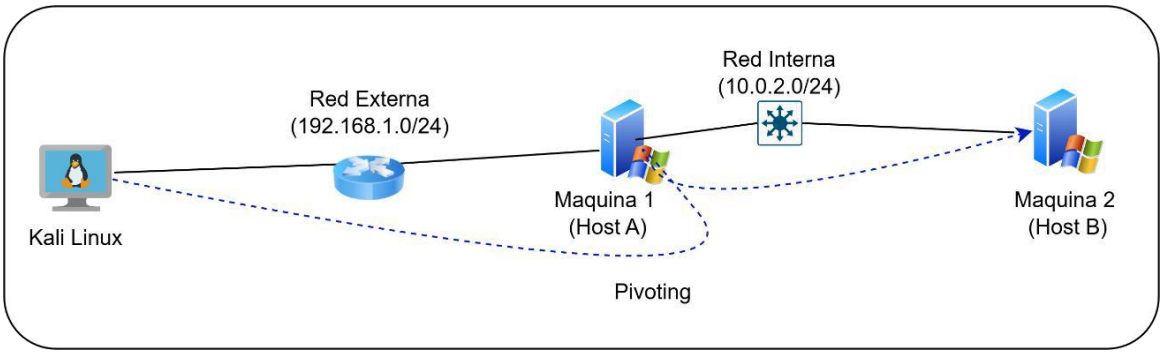


Nota. La secuencia refleja la cadena de explotación, desde el descubrimiento de la superficie expuesta hasta la ejecución del código malicioso y el control del host comprometido.

Fase de Pivoting – Acceso a la Red Interna 10.0.2.0/24

Figura 16

Diagrama Pivoting



Nota. La representación evidencia la creación de un túnel lógico que permite alcanzar Host B, expandiendo la superficie de ataque mediante técnicas de enrutamiento dinámico y redireccionamiento.

Configuración de Rutas con Autoroute

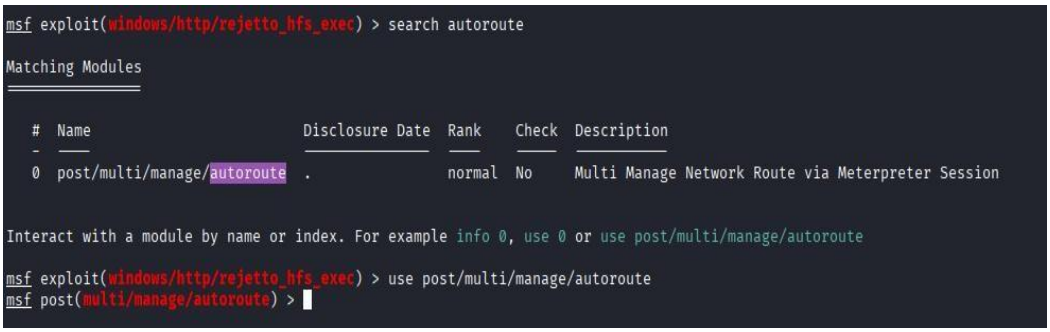
Para utilizar Host A como pivote, se dejó la sesión en segundo plano y se utilizó el módulo:

Post/multi/manage/autoroute

Se configuró la sesión correspondiente (por ejemplo, SESSION 1) y al ejecutarse, el módulo añadió automáticamente rutas hacia la red 10.0.2.0/24 a través de la sesión de Host A.

Figura 17

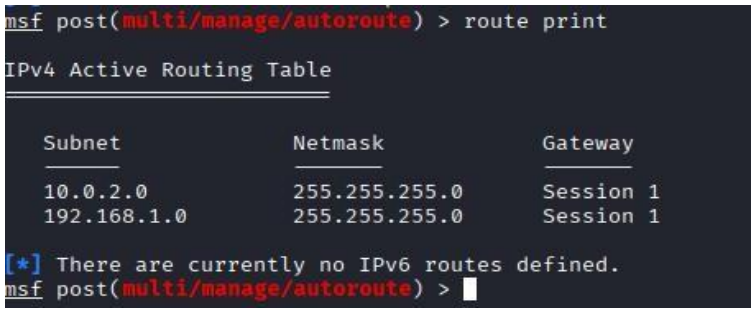
Configuración de Autoroute Metasploit



Nota. Inyección de rutas dinámicas mediante autoroute, permitiendo encaminamiento persistente hacia redes no directamente accesibles.

Figura 18

Salida de Route Print mostrando la Ruta hacia 10.0.2.0/24



Nota. Confirmación de tabla de enrutamiento creada por Metasploit, con rutas activas hacia la red interna 10.0.2.0/24.

Descubrimiento de Hosts Internos (ARP Scanner)

A continuación, se utilizó:

Post/windows/gather/arp_scanner

Lo cual configuró:

RHOSTS → 10.0.2.0/24

SESSION → sesión activa en Host A

El resultado permitió identificar el Host B dentro de la red interna.

Figura 19

ARP Scanner Interno desde Host A – Identificación de Host B

Nota. Mapeo ARP interno que identifica dispositivos activos mediante peticiones ARP retransmitidas a través del túnel Meterpreter.

Escaneo de Puertos en Host B

Conocida la IP de Host B (por ejemplo 10.0.2.3), se utilizó el módulo:

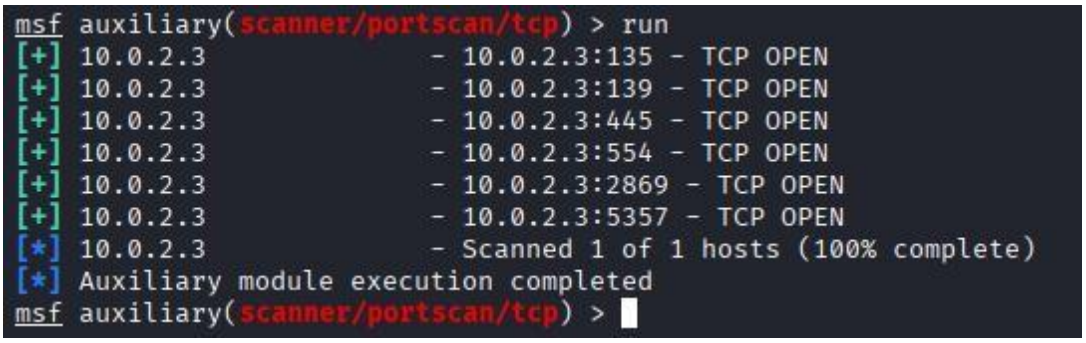
Auxiliary/scanner/portscan/tcp

De tal manera, se identificaron puertos abiertos, observando:

135/tcp, 139/tcp, 445/tcp, 554/tcp, 2869/tcp, 5357/tcp, entre otros.

Figura 20

Portscan TCP Interno sobre Host B



Nota. Enumeración de puertos: servicios RPC, SMB, HTTP y WS-Discovery, clave para evaluar superficie de ataque lateral.

Portproxy / Port Forwarding hacia Host B

Para facilitar la explotación desde Kali, se aplicó el módulo de portproxy, configurando:

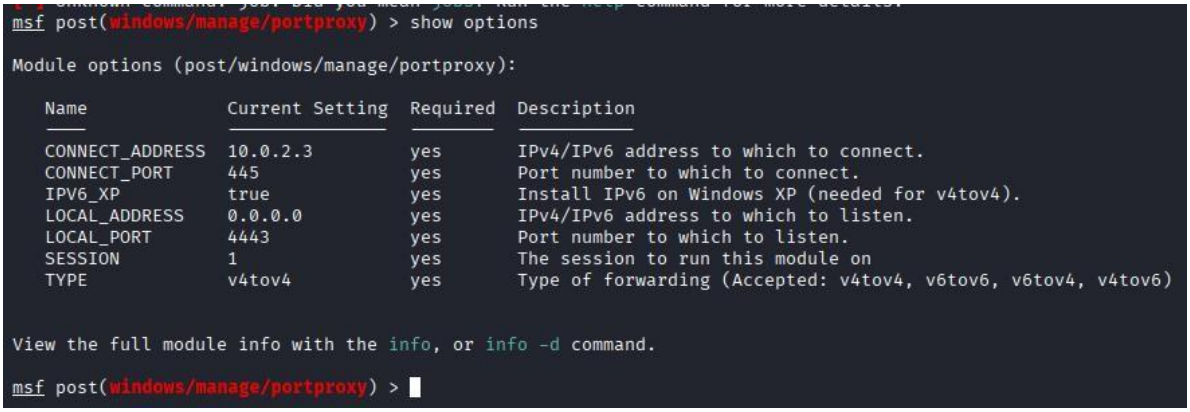
Dirección interna de Host B: 10.0.2.3

Puerto remoto: 445
Puerto local: 4443

De esta forma, el tráfico SMB enviado al puerto 445 del atacante era redirigido, a través de Host A, hacia Host B.

Figura 21

Configuración de Portproxy hacia el Puerto 445 de Host B



Nota. Configuración del portproxy.

Validación de MS17-010 (Eternalblue) en Host B

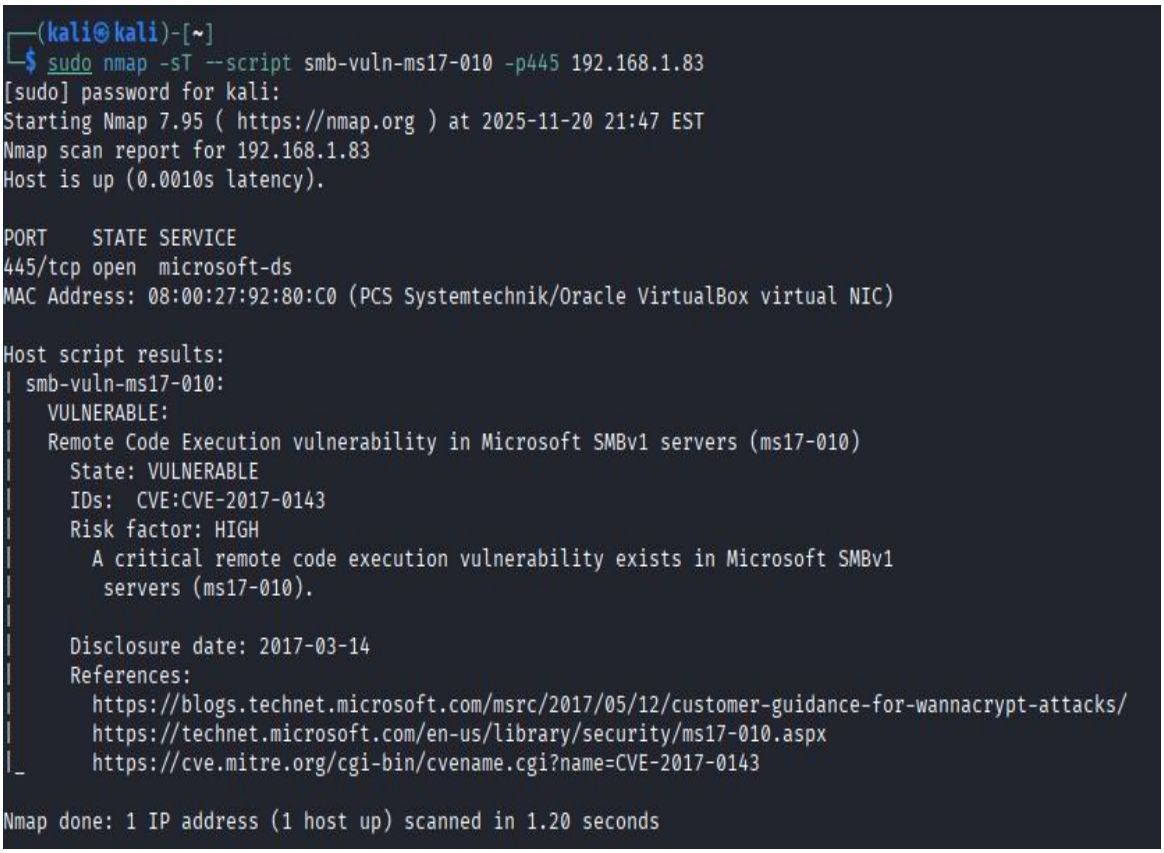
Teniendo disponible el puerto 445 de Host B, se utilizaron scripts de Nmap relacionados con SMB para validar la presencia de la vulnerabilidad MS17-010 (smb-vuln- ms17-010). El resultado indicó que:

Host B ejecutaba Windows 7 Professional Service Pack 1.

El sistema era probablemente vulnerable a MS17-010.

Figura 22

Nmap – Detección de Vulnerabilidad MS17-010 en Host B



Nota. Confirmación técnica de la vulnerabilidad MS17-010 mediante scripts smb-vuln- ms17-010 y fingerprinting del stack SMB.

Explotación Controlada de Eternalblue en Host B

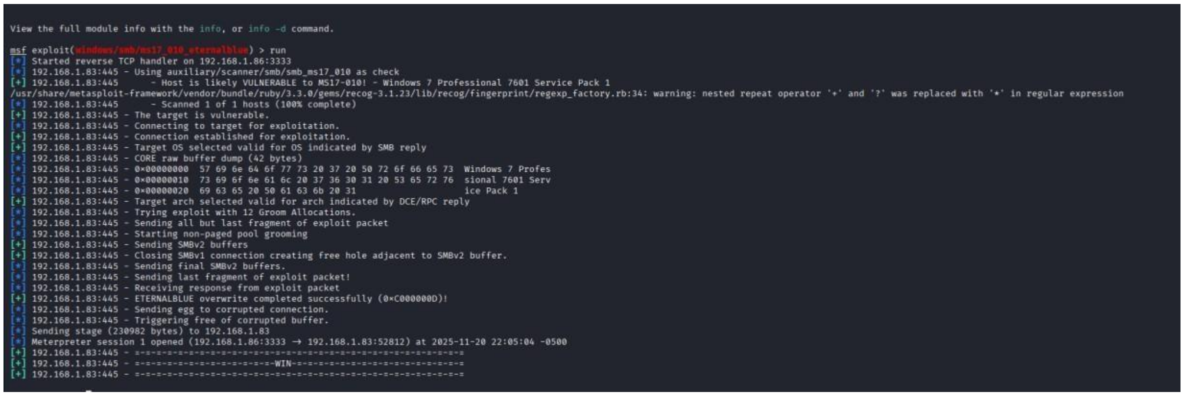
Desde Metasploit se eligió:

Exploit/windows/smb/ms17_010_eternalblue

Se configuraron los parámetros del objetivo y, tras ejecutar el exploit dentro del laboratorio, se obtuvo una nueva sesión Meterpreter en Host B.

Figura 23

Ejecución de Exploit EternalBlue y Apertura de Sesión en Host B

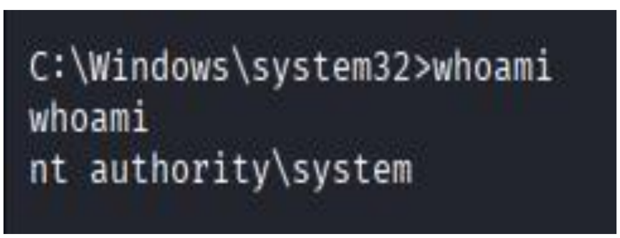


Nota. Ejecución del exploit EternalBlue aprovechando la corrupción de memoria en transacciones SMB, generando ejecución arbitraria de código.

Se confirmó con sysinfo que se trataba de un Windows 7 SP1 y con getuid que la sesión poseía altos privilegios.

Figura 24

Validación de Sistema y Privilegios en Host B



Nota. Verificación post-explotación revelando privilegios SYSTEM y arquitectura del host comprometido.

Creación de Usuario Administrativo Efímero en Host B

Siguiendo las instrucciones del escenario, se procedió a:

Crear un usuario con el formato indicado (primerNombre+primerApellido).

Verificar la creación del usuario.

Agregarlo al grupo de administradores locales del Host B.

Todo esto se realizó como prueba de concepto controlada, registrando:

Comando de creación de usuario.

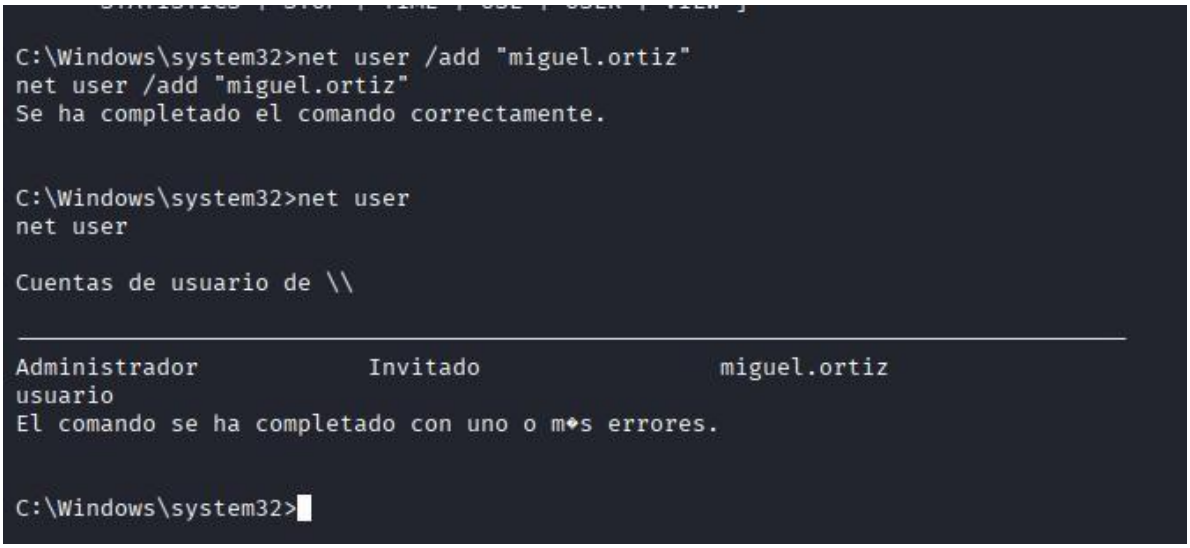
Listado de usuarios después de la creación.

Listado de grupos para identificar “Administradores”.

Comando de incorporación del usuario al grupo de administradores.

Figura 25

Creación del Usuario en Host B



Nota. Creación de usuario persistente mediante comando net user ejecutado en contexto elevado.

Posteriormente a la verificación y validación de los privilegios elevados del Host B, se realizó la creación del Host B, es decir, del usuario no autorizado.

Figura 26

Usuario Agregado al Grupo Administradores de Host B

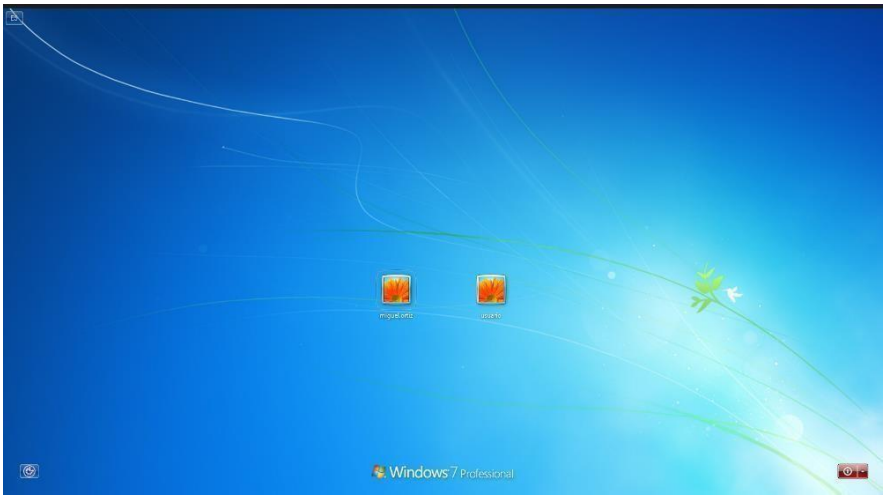
```
meterpreter > add_localgroup_user Administradores miguel.ortiz
[*] Attempting to add user miguel.ortiz to localgroup Administradores on host 127.0.0.1
[+] Successfully added user to local group
```

Nota. Modificación del grupo Administradores del sistema mediante privilegios escalados obtenidos por el exploit.

Finalmente, se crea de manera oficial el usuario no autorizado, del cual se puede verificar y comprobar su existencia en el grupo de administradores de Host B.

Figura 27

Interfaz de Inicio de Windows de Host B



Nota. Interfaz de Windows que muestra los usuarios disponibles para inicio de sesión.

Estrategias Blue Team

Detección: Procesos para Identificar un Ataque en Tiempo Real como Empleado de Blue Team

En cuanto a las estrategias desarrolladas por el equipo Blue Team entorno a la actuación que se llevaría a cabo ante la presencia de un ataque en tiempo real como primera medida, se debe tener en cuenta que es imperativo confirmar la veracidad del incidente.

Posteriormente, se debe identificar este de dónde viene, que afectó, qué está afectando y si este continúa activo. Para esto es conveniente realizar una revisión inmediata tanto del comportamiento en red como del estado del sistema operativo, validando así: conexiones, procesos, sesiones, registros y cualquier actividad que denote un funcionamiento anormal del equipo o del servicio comprometido.

Igualmente, este punto de vista también es contemplado por el Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD (2024), dado que resalta la valoración de los riesgos en activos de información con el propósito de identificar vulnerabilidades y así, poder priorizar controles que establezcan el cuidado de la seguridad de la empresa al momento en el que se presente un incidente.

De este modo, el enfoque que se plantea orientar para este caso es verificar que sucede con el equipo, para así, continuar con la aplicación de acción de contención que no afecten la evidencia que se tiene en cuenta y que se necesitará posteriormente para el desarrollo de la fase de análisis. Consecuentemente, en el caso de que SecureNova Labs se encuentre experimentado un ataque en tiempo real, el enfoque que se usaría sería el siguiente:

Validar con evidencia técnica que el ataque está activo.

Revisar red, procesos, servicios, sesiones y registros.

Identificar el vector inicial y determinar el alcance.

Aplicar contención sin interrumpir o borrar evidencia.

Preservar artefactos para análisis detallado.

Documentar todo lo realizado para asegurar trazabilidad.

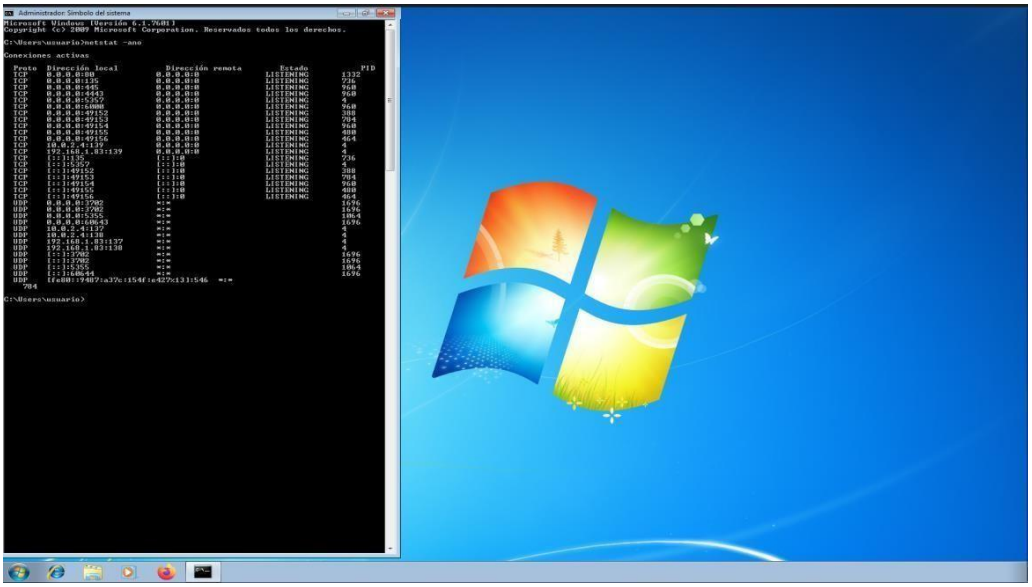
Así, se trabaja bajo la lógica que plantea CNN Cert (2018), puesto que buscan brindar seguridad se debe adoptar una serie de mecanismos apropiados que permitan identificar las vulnerabilidades del sistema para prevenir ataques. Teniendo en cuenta los pasos anteriores, mi prioridad es detener el avance del ataque para mantener la operación estable y, por ende, garantizar que toda la información necesaria para el análisis posterior se encuentre preservada sin ninguna alteración.

Primeramente, es fundamental realizar una revisión para saber si existen conexiones o patrones de tráfico que indiquen actividad maliciosa en el equipo Windows, a través de herramientas nativas como las siguientes:

Netstat-ano, el uso de esta herramienta me permite identificar si existen conexiones activas, puertos abiertos, direcciones sospechosas y el PID del proceso asociado. En caso de que se encuentren sesiones establecidas con IPs desconocidas o puertos que no deberían estar siendo utilizados, esta herramienta me confirma la actividad anómala.

Figura 28

Comando Netstat –Ano



Nota. Esta información permite identificar servicios expuestos, conexiones activas posiblemente originadas tras la explotación y procesos que mantienen comunicación con otros hosts.

Arp-a: con esta herramienta, se puede ver dispositivos con los que el equipo ha interactuado de manera recientemente. De esta manera, se identifica el escaneo interno o reconocimiento inicial de la red.

Registros del Firewall de Windows: a partir de los registros del Firewall de Windows, se puede ver los intentos de conexión entrante y saliente, bloqueos, repeticiones y tráfico hacia destinos no autorizados.

Luego, con el propósito de confirmar la alerta y el alcance inicial, se correlacionan las alertas del SIEM con los registros del firewall perimetral, IDS/IPS y logs del servidor web para poder realizar un análisis de lo que ha ocurrido con el ataque en tiempo real.

Moreno (2015) establece que los sistemas SIEM tienen una tarea fundamental para la detección temprana de ataques, a partir de la correlación de eventos que manifiestan actividades sospechosas que pudieron darse a partir de vulnerabilidades de los equipos.

Posteriormente, se verifica en el firewall las conexiones entrantes hacia el puerto 80 del Host A y patrones de tráfico inusual en el equipo como pueden ser los picos de solicitudes, payloads extraños y usuarios no autorizados. Igualmente, también se plantea la revisión rápida de otros hosts que presenten alertas similares a través de la contención táctica en la red, lo cual permite aplicar reglas temporales en el firewall para bloquear el tráfico sospechoso del ataque hacia el puerto o hacia la URL que se encuentra afectada. De esta manera se puede realizar un bloqueo al acceso externo a HFS 2.3.

Si se logra identificar que el Host A ha sido infectado, este se puede aislar lógicamente de la red crítica, para impedir que el ataque continúe. Esto se puede realizar a partir de que este Host se mueva a una VLAN, para que esté en cuarentena, también se puede bloquear la comunicación de este con la red 10.0.2.0/24 o si se requiere, se le pueden aplicar reglas específicas de bloqueo SMB.

Consecuentemente, para verificar el sistema operativo y los procesos activos es necesario conectarse al Host A con credenciales administrativas seguras o a través de una consola de gestión externa. Por lo tanto, se deben revisar los procesos que se han ejecutado con el uso de herramientas como el Administrador de Tareas o el Process Explorer, dado que estas realizan un rastreo de cualquier actividad inusual que se presente en el equipo y que pueda afectar a las empresas, tal como lo son los procesos en directorios temporales o asociados a shells remotas. También, es necesario realizar un análisis de las conexiones de red activa con comandos tales como netstat -ano o Get-NetTCPConnection, para detectar conexiones establecidas con direcciones IP extrañas.

Respecto a la revisión de cuentas y sesiones de usuario, deben ser comprobadas para identificar si estas se han creado recientemente con el uso de las herramientas como net user,

PowerShell o revisiones en Active Directory. Igualmente, se deben evaluar las sesiones activas y la actividad de inicio de sesión a través de la inspección de eventos específicos (por ejemplo, 4624, 4625, 4720, 4728, 4732), verificando si existen accesos fuera de horario, desde IPs inusuales o con aumento de privilegios.

Por otro lado, para un mayor detalle del tráfico se deben utilizar herramientas GPL. Entre ellas se encuentran las siguientes:

Wireshark: la cual me permite ver en tiempo real cualquier paquete malformado, patrones de escaneo, intentos de explotación o actividad fuera del comportamiento habitual.

TCPDump: para en caso de que se esté en un sensor Linux o en un entorno donde requiera capturas rápidas desde terminal.

Luego de la confirmación de los indicios en la red, reviso el estado interno del equipo afectado. Para lo cual, se hace uso de:

Tasklist/v: el cual ayuda a identificar procesos que no deberían darse como aquellos que involucren el no uso de un usuario interactivo o comandos que se lanzan de forma automática sin justificación.

Scquery: esta herramienta permite validar servicios iniciados recientemente o servicios que fallaron, lo cual también puede indicar manipulación o carga de código malicioso.

Process Explorer (Sysinternals – Free): el cual es esencial para visualizar el árbol de procesos, tener un panorama sobre qué ejecutó para poder confirmar si existen procesos hijos que no corresponden a la operación normal del sistema.

Process Hacker (GPL): esta se usa para cuando se necesite ver memoria, hilos o conexiones asociadas a un proceso en concreto.

Análisis para la Verificación del Ataque

Consecuentemente, una de las primeras prioridades es determinar si hubo compromiso de credenciales o escalamiento de privilegios. De este modo, se hace uso de las siguientes herramientas para continuar con el proceso:

Net user: usada con el propósito de validar la existencia de usuarios nuevos o cambios inesperados.

Net localgroup administrators: para confirmar si se agregaron cuentas con privilegios sin autorización.

Query user: usada para revisar sesiones activas que no corresponden a usuarios legítimos.

En caso de que se detecten sesiones remotas o cuentas creadas recientemente que han logrado interceptar el equipo a través de las herramientas y los pasos mencionados anteriormente, se tiene conocimiento de que el atacante está dentro del sistema y, por lo tanto, se debe actuar con mayor rapidez para impedir que se siga propagando el ataque. De este modo, el análisis del registro es trascendental para poder encontrar qué ocurrió y cuándo. Para lo cual, se busca en el sistema registros de seguridad distintos registros que permiten hallar los procesos realizados como lo son:

Inicios de sesión exitosos y fallidos (4624 / 4625)

Privilegios especiales asignados (4672)

Creación de usuarios (4720)

Modificaciones en grupos administrativos (4732)

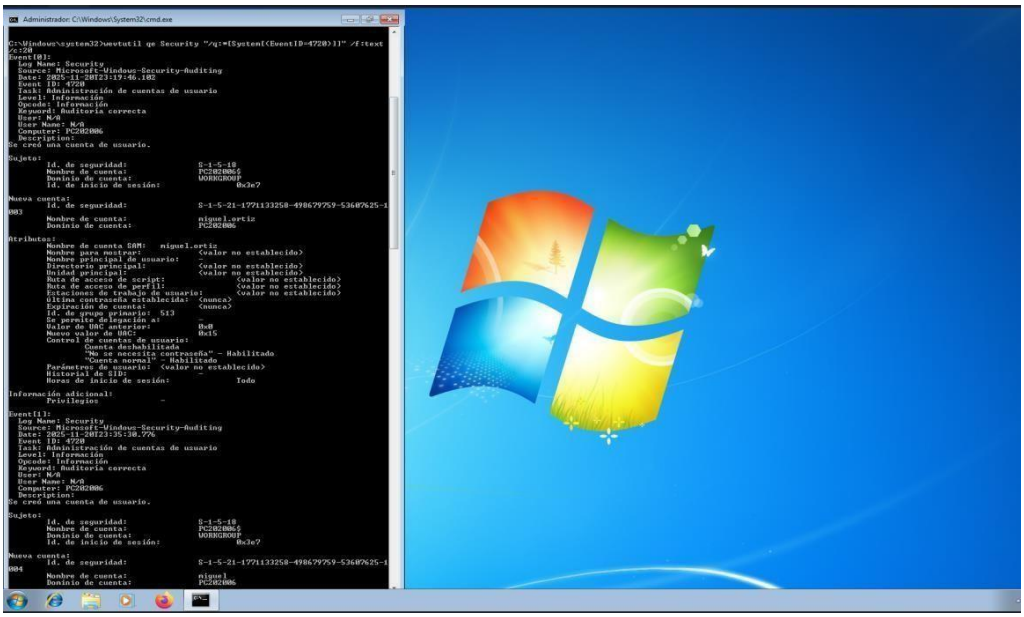
Para acelerar esta revisión se hace uso de:

Event Viewer

Wevtutil para exportar logs sin modificarlos

Figura 29

Comando Wevtutil



Nota. Se muestran atributos de la cuenta, SID asociado y acciones administrativas registradas por el subsistema de auditoría de Windows Security-Auditing, lo cual permite validar la actividad post-explotación y la persistencia generada en el host.

Event Log Explorer para filtrar rápidamente eventos por IP, usuario o fecha.

Posteriormente a la validación del ataque, se aplica la contención puntual y controlada de la siguiente manera:

Uso el Firewall de Windows con:

netsh advfirewall firewall add rule name="Block_Attack" dir=in action=block remoteip=<IP_sospechosa>

Consecuentemente, se realiza un bloqueo de tráfico hacia otros segmentos a partir del uso de:

Reglas del firewall local

ACLs del router

VLANs temporales si están disponibles

De esta manera, se cumple con el objetivo de evitar que el ataque se propague sin que haya una interrupción en el sistema en línea para análisis. Por lo tanto, antes de continuar con el proceso y las acciones profundas, guardo toda la información relevante del estado del sistema:

tasklist /v > C:\Evidencia\procesos.txt netstat -ano > C:\Evidencia\conexiones.txt ipconfig /all > C:\Evidencia\ip.txt

wevtutil epl Security C:\Evidencia\Security.evtx

Además, de que, si se requiere analizar la memoria, se hace uso de las siguientes herramientas:

Magnet RAM Capture

DumpIt

Autopsy o Sleuth Kit (GPL)

Por otro lado, (Palomo et. al., 2024) sostienen que este tipo de procesos para la identificación de ataques pueden acarrear desventajas, tal como lo es “la pérdida de tiempo” que involucra la creación del laboratorio aislado, la recolección de datos, la evaluación de amenazas, la identificación de vulnerabilidades, la ejecución de explotación la persistencia y los movimientos laterales. Los autores señalan que realizar este tipo de procesos pueden ralentizar las dinámicas de la empresa, además de que se requiera de un personal calificado para llevar a cabo estas tareas.

No obstante, esto no debe ser visto como una desventaja, dado que la creación de laboratorios aislados para la identificación de vulnerabilidades es una estrategia práctica que

contribuye con el tratamiento adecuado para mejorar la ciberdefensa de una empresa. En este sentido, esto debe ser visto como una oportunidad para promover auditorias y demás procesos de cuidado tanto para la información interna como para los equipos.

Además, de que requerir de personal capacitado no es precisamente un aspecto negativo, esto significa que los empleados deben mantenerse en constante actualización para poder brindar un buen desempeño dentro de sus cargos.

En contraposición, (Kristian et. al., 2024), resaltan la importancia de la creación constante de estrategias para la prevención, detección y respuesta a los ataques cibernéticos y cómo la capacitación constante del personal, además de las políticas internas de inversión en la seguridad de la empresa como aspectos fundamentales para el cuidado de las empresas y, por ende, de las estrategias y normativas en la gestión de riesgos.

También, se debe recalcar que la inversión de tiempo puede asegurar la mitigación de demás ataques a los equipos, porque el propósito de los laboratorios y los procesos que se desarrollan durante su ejecución es el de hallar fallas, vulnerabilidades y demás aspectos que puedan propiciar la fuga de información en el futuro y el acceso a los equipos. Por lo tanto, este tipo de estrategias puede ahorrar la presencia de demás inconvenientes que afectan la estabilidad de la empresa.

Medidas de Hardenización para Evitar Ataques Similares

Respecto a lo ocurrido durante la actividad Red Team, las medidas de hardenización que se propondrían tienen como objetivo cerrar los puntos débiles que permitieron el acceso inicial, el movimiento lateral y el aumento de privilegios al usuario desconocido que ingresó al equipo, además de dejar la infraestructura cuidada, para que, en caso de un nuevo ataque, esta no permita el avance del usuario desconocido y el equipo tenga más barreras técnicas para avanzar.

A continuación, se detalla de forma organizada, las principales acciones que implementaría para cumplir con lo propuesto. Primeramente, realizaría una revisión en el estado de los sistemas operativos y del software instalado, dado que el ataque pudo proseguir debido a vulnerabilidades conocidas y en aplicaciones desactualizadas. Por lo tanto, se seguirían una serie de pasos para prevenir futuros ataques:

Parches y Actualizaciones

Implementación de un proceso formal para la gestión de parches, el cual consistiría en revisiones periódicas, para garantizar que los equipos tengan instaladas las actualizaciones de seguridad críticas.

Priorización a las vulnerabilidades de ejecución remota de código (RCE), específicamente a aquellas que afectan servicios expuestos o protocolos de red como SMB.

Mantenimiento del inventariado, para identificar qué sistemas están fuera de soporte para planear su adecuada sustitución.

Eliminación de Software Obsoleto o no Soportado

Revisión de las aplicaciones que realmente son necesarias para la empresa y la eliminación de las que se encuentren obsoletas, sin soporte o que no aporten valor.

Sustitución del servicio de publicación de archivos y contenidos para solucionar las problemáticas actuales, a partir de un soporte del fabricante y capacidades de registro y autenticación adecuadas.

Configuración Segura del Sistema

Fortalecimiento de la configuración del sistema operativo a partir del uso de plantillas de seguridad o GPO, mientras que se deshabilitan servicios innecesarios, los cuales impliquen

características que no se utilizan o no son necesarias. Además, de impulsar el componente que incremente la superficie de ataque.

Revisión de permisos de archivos, carpetas y servicios críticos para poder brindar un aseguramiento que solo las cuentas necesarias tienen acceso.

No obstante, otra lección clave del ejercicio es que la red permitía demasiado "libre tránsito" entre equipos y servicios, lo cual, pudo haber sido una de las causantes para el desarrollo del ataque.

Revisión de Servicios Publicados

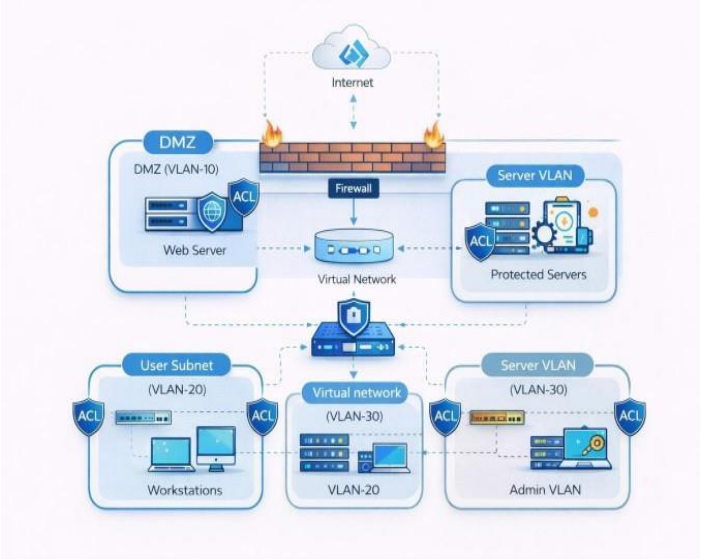
Revisión y verificación de los servicios que necesitan realmente acceso desde Internet y a partir de los resultados, retirar o restringir el resto.

Organizar los dispositivos perimetrales adecuados como (firewall, reverse proxy, WAF, según la necesidad) para que los servicios que deban estar publicados.

Segmentación de Red

Figura 30

Arquitectura de Red Segmentada con Enfoque en Seguridad Perimetral y Control de Acceso



Nota. La figura representa un diseño de red basado en buenas prácticas de seguridad, que integra un firewall perimetral, una zona DMZ para servicios expuestos, segmentación mediante VLAN y subredes internas, así como controles de acceso (ACL) para limitar la comunicación entre segmentos. Este enfoque reduce la superficie de ataque y mitiga movimientos laterales no autorizados dentro de la infraestructura.

Separación la red en segmentos o VLAN con diferentes jerarquías de confianza como pueden ser (usuarios, servidores internos, servicios expuestos, administración, etc.).

Limitación del tráfico entre segmentos, para utilizar listas de control de acceso (ACL) y reglas de firewall internas.

Las VLAN (Virtual Local Area Network), al tener la capacidad de segmentar y subdividir redes dentro de una misma una red a partir de funciones específicas. Esta habilidad permite que los Hosts puedan mantener una comunicación directa entre sí como si estuviesen conectados a un switch único para este grupo sin importar la ubicación que estos tengan. Es decir, el tráfico de la

red dentro de una VLAN hace que se mantenga aislado el tráfico de otras VLAN. Por lo tanto, la seguridad de los equipos que están conectados a una misma red no se ve afectada por otras conexiones ajenas. De esta manera, se promueve la seguridad y la eficiencia en el tratamiento de los equipos, además de que la difusión de información se encuentra controlada.

Sin embargo, la comunicación entre los hosts a través de VLAN no ocurre de manera automática, dado que se requiere que haya una autorización por parte del administrador de la red. Para realizar este proceso es común hacer uso de la técnica de VLAN Trunking, la cual habilita la comunicación entre equipos a partir de la configuración de troncales que permiten que varias VLAN puedan traficarse de manera sincrónica. A través del switch y sus puertos, se configura el acceso que permite que la conexión con la troncal y los hosts directamente relacionados.

Control del Tráfico Lateral

Restricción del uso de SMB y demás protocolos de comunicación sensible entre equipos cuando no es necesario

Revisión y ajustes para cerrar puertos abiertos en servidores y estaciones de trabajo, en los cuales estas funciones no sean necesarias.

Posteriormente, al control del impacto, la empresa Blue Team debe ahondar en el análisis técnico para entender el vector de entrada, el alcance del compromiso y movimiento lateral, lo cual, se puede lograr a partir del análisis de malware, scripts descargados a través de HFS 2.3. Igualmente, el proceso de verificación del uso de las vulnerabilidades como MS17-010 en los equipos de la empresa. Asimismo, una reconstrucción de la línea de tiempo del incidente, en el cual se pueda evidenciar un mapeo de las acciones realizadas por el atacante en los hosts A y B, permiten identificar los procesos que este tercero ejecutó y cuales vulnerabilidades de la empresa aprovechó para realizar la infiltración en el equipo Windows.

En este sentido, las medidas mencionadas anteriormente, ayudarán a que la información obtenida sea usada paras alimentar las medidas de hardenización y así, poder plantear las mejoras en los controles defensivos. A partir del ataque, se evidenció que el agente externo pudo llegar a determinadas cuentas a partir de diferentes privilegios.

Principio de Mínimo Privilegio

Revisión de las cuentas que poseen privilegios administrativos.

Reducción de los privilegios de las cuentas a un mínimo.

Separación de las cuentas de uso diario de las cuentas de administración, para evitar así que un mismo usuario haga uso constante de las credenciales que permiten el acceso a la información alto privilegio de la empresa.

La (CIS Security, 2020) resalta la implementación de los controles de seguridad como el mínimo privilegio como una gestión que contribuye a reducir de manera significativa la elevación de los privilegios, de manera que se puedan mitigar posibles amenazas a partir de vulnerabilidades que se pueden hallar a partir de privilegios amplios que podrían afectar de manera negativa los equipos.

Gestión de Cuentas Locales

Deshabilitación de las cuentas locales que no se usen.

Establecer la creación de contraseñas.

Implementación de controles y alertas para las nuevas cuentas de la empresa.

Reforzar Autenticación Remota

Restringir el acceso remoto para que solo se pueda acceder a equipos, usuarios y horarios autorizados por la empresa.

Añadir factores y procesos adicionales para la autentificación de los accesos administrativos que se presenten desde redes externas.

No obstante, hay otro aspecto importante que no debe ser dejado de lado y es la detección de las acciones del agente externo a partir de determinados registros que se pueden llegar a identificar a partir de la correlación que el capital humano realiza de estos pasos. Por lo tanto, es determinante implementar los siguientes procesos:

Ampliar y Estandarizar el Registro de Eventos

Habilitar auditorías en los sistemas críticos, en cuanto a los inicios de sesión, cambios de privilegios, creación de cuentas, acceso a recursos sensibles y ejecución de procesos, con el fin de realizar rastreos

Asegurar el envío de los registros a un repositorio central para monitorearlos, con el fin de que no dependan únicamente del equipo afectado.

Respecto a la implementación de las auditorías, (Zambrano Hernández et. al., 2024), manifiestan que la detección de actividades anormales puede prevenir incidentes de interceptación de los equipos.

Definir Alertas Específicas

Configurar alertas para los eventos clave como lo pueden ser:

Creación de nuevas cuentas.

Inclusión de usuarios en grupos administrativos.

Actividad inusual desde direcciones IP externas o no habituales.

Ejecución de procesos desde rutas poco comunes o temporales.

Estas alertas podrían permitir llegar al equipo de seguridad a través de los canales definidos (correo, consola de monitoreo, ticketing, etc.) para así, realizar una revisión. Por otro

lado, también haría un refuerzo de los aspectos generales que ayudan a evitar que un ataque inicial prospere y se convierta en un compromiso mayor que tenga mayor afectación para la empresa.

Reducción de Software y Herramientas Innecesarias

Mantener un catálogo conciso tanto para softwares autorizados y prohibidos.

Justificación para cada herramienta adicional hallada en los equipos de la empresa.

Controles sobre Scripts y Herramientas de Administración

Uso restringido de PowerShell y demás consolas de administración, bajo políticas internas que limiten su ejecución a usuarios.

Evaluación del uso de mecanismos como AppLocker o controles de ejecución de aplicaciones para impedir que binarios no autorizados se ejecuten en los equipos.

Pruebas Recurrentes y Estrategias

Programación de evaluaciones de manera periódica, para brindar seguridad. Estas evaluaciones harían uso de procesos como escaneos de vulnerabilidades, revisiones de configuración y pruebas de intrusión controladas, para así, poder confirmar y comprobar que las medidas de hardenización aplicadas siguen vigentes y se manejan de forma efectiva.

En cuanto a las estrategias para brindar mayor seguridad a los equipos de la empresa, (Cheng y Wang, 2022) contemplan distintas estrategias que integran distintas aristas que van de lo general a lo particular como es el fortalecimiento de la gobernanza institucional, la revisión de los equipos de la empresa, la explicación de las políticas de ciberseguridad a los empleados y campañas de formación y concienciación sobre ciberdefensa.

De esta manera, la atención no está únicamente focalizada a la creación y apropiación de estrategias y ejercicios realizados. También se presenta un enfoque que busca focalizar la

competitividad a partir de la formación de los trabajadores, dado que así, se puede capacitar al personal para que la información hallada a lo largo de experiencias como los laboratorios, sea de acceso a todo el personal, lo cual les permite mantenerse al día con las estrategias desarrolladas por la empresa. Por lo tanto, los empleados pueden conocer y saber cómo podrían identificar, examinar y esclarecer vulnerabilidades o actividades sospechas en caso de que se presenten ataques similares

Contención: Blue Team como Protector de Securenova Labs

El equipo de Blue Team es el equipo defensivo de SecureNova Labs, el cual debe proteger la infraestructura de TI de la organización, las cuales, debe cumplir las siguientes funciones:

Monitoreo continuo de la seguridad (SIEM, EDR, IDS/IPS, firewalls).

Implementación y mantenimiento de controles técnicos (parches, hardenización, segmentación, reglas de firewall).

Gestión de vulnerabilidades y análisis de riesgos.

Elaboración de políticas de seguridad, procedimientos y mejoras continúas basadas en lecciones aprendidas.

Coordinación con el Red Team para ejercicios de simulación y validación de la postura defensiva.

Siendo esta última una herramienta fundamental para la creación de simulaciones y laboratorios que contribuyan con la creación de espacios para fortalecer las estrategias de seguridad. Del mismo modo, Rajendran, Jyothi y Karri (2011) plantean que “Un enfoque de equipo rojo y equipo azul imita escenarios de ataque dinámicos y, por tanto, puede utilizarse para

validar dichas técnicas determinando la efectividad de una defensa e identificando vulnerabilidades en ella" (p, 1).

Bajo esta premisa, el desarrollo de laboratorio aislados corrobora con el mejoramiento al funcionamiento de una empresa, específicamente, contribuye a su practicidad en el campo de la ciberdefensa para hallar e identificar vulnerabilidades que pueden ser explotadas por terceros. Igualmente, la ejecución de pruebas de ataque pone en un entorno más real la práctica, dado que así, se puede realizar un mapeo de procesos que pueden ser llevados a cabo para obtener privilegios, además, de que este tipo de pruebas ayudan a verificar si los procesos de ciberdefensa empleados cumplen a cabalidad con sus funciones.

Posteriormente a esto, (Ijiga, et al., 2024), manifiestan que el aprendizaje autónomo a partir de experiencias similares como las que pueden brindar los laboratorios puede ser automatizadas para incorporar normativas de ciberseguridad. De manera que se puedan brindar procesos como la detección, el análisis y la respuesta eficaz a posibles ataques, con el propósito de que a través de este tipo de experiencias se puedan incorporar las amenazas como puntos de identificación de ataques similares.

Finalmente, el fortalecimiento de las capacidades tanto de los equipos como del personal de la empresa se logra a partir de la investigación, formulación y creación de políticas internas y por supuesto, del desarrollo de proyectos y estrategias que incentiven a mantenerse en la vanguardia del mundo tecnológico para continuar brindando competitividad dentro del mercado.

Blue Team Vs. Equipo de Respuestas a Incidentes Informáticos

No obstante, hay diferencias entre ambas empresas que colaboran:

Enfoque: el Blue Team se centra en la defensa operacional continua; el CSIRT/CERT se enfoca en la gestión estructurada de incidentes.

Alcance: el Blue Team trabaja día a día en la infraestructura interna; el CSIRT puede actuar a nivel organizacional, nacional o sectorial, con un marco formal de gestión de incidentes.

Momento de intervención: el Blue Team está activo antes, durante y después del ataque; el CSIRT se activa principalmente cuando hay incidentes significativos que requieren coordinación formal.

En este sentido, Blue Team es la primera empresa que hace frente respecto a las amenazas de seguridad que se presentan para la empresa SecureNova Labs, dado que esta es la encargada de detectar anomalías y ejecuciones de acciones iniciales, puesto que Blue Team, fue contactada por SecureNova Labs para reforzar la seguridad de la empresa, por lo tanto, Blue Team es la primera barrera que debe enfrentar los ataques cibernéticos, mientras que el CSIRT coordina la respuesta global, asegura la trazabilidad de la evidencia y reporta a la dirección.

En este orden de ideas, la empresa Blue Team debe realizar un monitoreo constante de la información de la empresa, además, de responder por los ataques que esta sufra, mientras que el CSIRT/CERT responde de manera especializada cuando el incidente ya está en curso. De esta manera, ambos se complementan, pero sus responsabilidades y momentos de intervención son distintos.

El Uso de Center for Internet Security

Teniendo en cuenta que si tuviera un rol dentro del Blue Team debo trabajar con los controles y guías del CIS, los usaría como una referencia formal para estandarizar la seguridad de los sistemas, para asegurar que la infraestructura cumpla con configuraciones mínimas y buenas prácticas reconocidas internacionalmente. Estos procesos me permiten establecer una línea base de hardening, que me permite priorizar los controles más críticos, que busquen disminuir el área de ataque y definir ajustes que sean uniformes en todos los dispositivos.

Asimismo, también realizaría una implementación de los CIS Controls para poder determinar brechas, examinar el nivel de madurez de la compañía y dirigir las acciones de protección hacia los aspectos más frágiles. Del mismo modo, los utilizaría para optimizar los procedimientos de auditoría, registro y monitoreo, con el fin de potenciar la capacidad del Blue Team de detectar y responder.

Finalmente, estos controles son útiles como respaldo en auditorías y como orientación objetiva para fundamentar decisiones técnicas vinculadas con la seguridad, porque permiten establecer una línea base para poder realizar una configuración segura a partir de la cual se pueda realizar una implementación de CIS Benchmarks concretos para Windows 7/Windows Server, garantizando que los ajustes de seguridad del sistema operativo se hallen fortalecidos.

Además, de que se pueda realizar una definición de configuraciones estándar para servicios como SMB, inhabilitando las versiones que no son seguras y fortaleciendo la autenticación, que permiten priorizar la implementación de controles, las evaluaciones de nivel de madurez y brechas de seguridad. Para así, fortalecer la detección de ataques y las respuestas de hacia estos inconvenientes.

SIEM: Características y Funciones Principales

Un SIEM es una herramienta clave porque permite centralizar, correlacionar y analizar los eventos de seguridad generados en toda la infraestructura. Sus funciones principales son:

Recopilación y centralización de registros: unifica en un solo lugar los eventos de servidores, sistemas, dispositivos de red, firewalls y aplicaciones para que el entorno sea completamente visible.

Correlación de sucesos: establece conexiones entre acciones que, tomadas individualmente, parecen normales. Sin embargo, juntas pueden señalar un ataque, tal como los intentos no exitosos de autenticación, uso de privilegios o conexiones poco habituales.

Generación de alertas: informa al equipo cuando advierte conductas sospechosas o infracciones a las políticas de seguridad.

Supervisión en tiempo real: brinda paneles de control y visualizaciones operativas para detectar anomalías de forma instantánea.

Apoyo para la investigación forense: posibilita el examen de sucesos históricos, la reconstrucción de la secuencia temporal de un incidente y la obtención de pruebas fiables.

Cumplimiento normativo: para acatar estándares de auditoría y retención de registros.

Figura 31

Arquitectura Conceptual de un Sistema SIEM

Nota. La figura representa un sistema SIEM como núcleo central que recopila y analiza eventos de seguridad provenientes de la red corporativa y servicios en la nube para apoyar la detección de amenazas y la gestión de la seguridad.

En resumen, un SIEM proporciona la visibilidad, correlación y alertamiento necesarios para detectar y responder a incidentes de forma oportuna. De esta manera, presenta un mejoramiento de la eficacia del Blue Team para fortalecer la postura de seguridad de la organización.

Herramientas de Contención de Ataques Informáticos

Las soluciones EDR como Microsoft Defender for Endpoint, CrowdStrike o SentinelOne son una de las herramientas más efectivas para detener un ataque en curso. Desde la consola se puede aislar inmediatamente el dispositivo comprometido, bloquear procesos sospechosos, cortar conexiones hacia servidores externos y evitar que el atacante siga ejecutando comandos o moviéndose por la red. Asimismo, se posibilita el control de la ejecución de binarios y scripts no autorizados, lo que afecta la habilidad del atacante para seguir su actividad después de ser detectado.

De esta manera, Wazuh brinda acciones de contención mediante su función Active Response, además de actuar como SIEM/EDR. Esto permite que haya una interrupción de procesos en cuanto a s funcionamiento, aplicación automática de reglas de firewall y bloqueo de direcciones IP maliciosas. También, de que se puede aislar provisionalmente un dispositivo para impedir el movimiento lateral. De este modo, es una herramienta de código abierto, que es eficaz a pesar de la falta de presupuesto.

Así, las plataformas SOAR hacen posible la automatización de la contención a través de playbooks que llevan a cabo acciones inmediatamente cuando se identifica un incidente. Dentro de las cuales se encuentran: el aislamiento de un endpoint a partir del EDR, la deshabilitación de una cuenta comprometida, el bloqueo de una IP en todos los firewalls, cerrar sesiones activas o revocar credenciales. La ventaja principal es que centraliza la respuesta, reduce el tiempo de

reacción y asegura que las acciones críticas se ejecuten de manera consistente en toda la infraestructura.

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://www.youtube.com/watch?v=aPX_3L-DK6o

Conclusiones

Aspectos Críticos

El análisis realizado permitió identificar, examinar y esclarecer la complejidad del tema abordado, al igual que la necesidad de continuar con la profundización del laboratorio para ahondar en vulnerabilidades y demás dimensiones como las estrategias de la empresa y aportes que este tipo de ejercicios pueden generar. Los hallazgos obtenidos sostienen la relevancia del estudio realizada, además de abrir nuevos caminos de reflexión para el campo laboral y académico.

En cuanto a las estrategias implementadas por el equipo Red Team a través del desarrollo del laboratorio aislado, se puede decir que la recreación que este ejercicio permitió recrear las condiciones de vulnerabilidad con las cuales se dieron el ataque. A partir de esto, se pudo establecer el recorrido que hizo el atacante y continuar el proceso hasta la creación del usuario no autorizado en el equipo Windows.

La recreación del recorrido permitió demostrar que un servicio vulnerable no parcheado como el (HFS 2.3) en Host A facilitó la obtención de shell remota. Esto, sumado a la falta de segmentación interna posibilitó el uso de Host A como pivote hacia Host B, un servidor con SMB vulnerable a MS17-010.

Así, desde Host B, un atacante podría acceder a archivos o bases de datos sensibles como crear cuentas administrativas no autorizadas, consolidando la fuga de información descrita en el escenario original para elevar privilegios. Este proceso dio cuenta de que hubo varias debilidades dentro del sistema interno de la empresa como en la segmentación de la red y la gestión de los accesos administrativos.

De este modo, se pudo realizar una revisión profunda, la cual, tiene como propósito evitar ataques similares, además, de ser un ejemplo para implementar estrategias similares para mitigar los ataques cibernéticos y hallar los procedimientos realizados por el atacante, para que, de esa manera, halla más facilidad al identificar, examinar y esclarecer vulnerabilidad y por supuesto, de eliminarlas.

Por otro parte, las estrategias empleadas por Blue Team, demuestran que el ataque no se produjo específicamente por una vulnerabilidad en específico, sino que el atacante comprometió diversos sistemas con el propósito de crear usuarios administrativos no autorizados a partir del uso del software obsoleto (HFS 2.3), diversas vulnerabilidades críticas sin parches (MS17-010), la ausencia de segmentación de red y las debilidades en el manejo de cuentas privilegiadas. Estos puntos permitieron que el atacante ingresara al equipo Windows.

No obstante, Blue Team también demostró que a partir del uso de distintas herramientas nativas como netstat, tasklist y arp-a, se podía examinar diversos comportamientos anormales, al igual que demás conexiones extrañas. Así fue como se pudo identificar el ataque en tiempo real a partir de reglas de reglas en firewall y segmentación de red con VLAN. Esto permitió que se tomaran medidas como la aplicación de parches, eliminación de software obsoleto, segmentación del tráfico lateral y configuración de servicios.

A partir de estas medidas de prevención se estableció un enfoque protector. Además, de que la explotación de CIS Controls y el uso de sistemas SIEM brindaron establecer una perspectiva holística que tener en cuenta la recreación del laboratorio para tener en cuenta en futuras ocasiones. De este modo se fortaleció la posición defensiva para mitigar ataques similares y prevenir demás eventualidades.

En cuanto a los aspectos legales, el análisis de las normativas dejó en evidencia que los contratos realizados para vincular a Blue Team y Red Team como equipos de SecureNova Labs para la protección de información, poseían diversas cláusulas ambiguas que atentaban contra las leyes. A partir de los vacíos legales que se identificaron, tanto los empleados como los equipos pudieron haber recibido sanciones de cárcel.

Además, de que no solo se corría un riesgo legal en caso de que estos contratos se hubiesen firmado como estaban, esto también presentaba una falla ética, dado que el Código de Ética de la Ingeniería en Colombia (Copnia 2015), establece diversos parámetros para que los ingenieros puedan realizar un trabajo con el cual garanticen tanto la seguridad de la empresa como la protección de los clientes.

Por lo tanto, este análisis deja en evidencia que la ética profesional es uno de los pilares más importantes al momento de ejercer laboralmente, dado que, al romperse los lineamientos morales de los profesionales, también se quiebra la transparencia, responsabilidad y las leyes. Igualmente, se muestra la pasividad como una manera de negligencia, tanto en la no revisión del contrato al saberse que quién lo elaboró fue despedido por irregularidades en su desempeño y la empresa SecureNova Labs, no realizó veeduría o revisión de los contratos que se entregarían a una nueva empresa.

En conclusión, se refuerza la idea de que la empresa SecureNova Labs debe continuar con la tarea de buscar nuevas empresas y empleados que se ciñan a las normativas colombianas y tengan presente su código ético para brindar un servicio de calidad, el cual pueda incrementar la buena imagen de la empresa a través de la legalidad y transparencia de su trabajo, sin vulnerar o violar derechos de los ciudadanos.

Aspectos Secundarios

También se destaca la importancia de adoptar un enfoque holístico que tenga en cuenta las condiciones del contexto como se vio con la recreación del laboratorio. Este ejercicio permitió contemplar de manera práctica las vulnerabilidades del sistema de la empresa que fueron aprovechadas por el atacante. Este acercamiento hizo posible la comprensión del impacto de factores críticos que brindaron una posibilidad para fortalecer los equipos y construir una base sólida para mitigar ataques futuros.

Además de fortalecer los procedimientos, controles, restricciones, políticas internas y auditorías, también es fundamental que el capital humano pueda capacitarse de manera constante para mantenerse a la vanguardia de la tecnología y sus avances. En este orden de ideas, la actualización tiene un papel importante en diversas áreas como las de hallar nuevas vulnerabilidades que sean más sofisticadas para usar distintas herramientas que permitan abarcar los problemas de manera más integral y demás.

Finalmente, es necesario resaltar que, para lograr llegar a una resolución de los problemas identificados, se debe contar con un equipo que colabore en la recreación de un laboratorio para que se contemplen todas las aristas dentro de un ataque en tiempo real y se pueda realizar una revisión total del equipo atacado. De esta manera, el trabajo en equipo es una pieza clave para construir conocimiento desde el campo profesional con el fin de brindar soluciones al mundo actual.

Recomendaciones

A continuación, se desglosan una serie de recomendaciones las cuales se obtuvieron como resultado de los hallazgos y conclusiones:

Prioridad Crítica y Horizonte de Implementación a Corto Plazo

Uno de los puntos más importantes para tener en cuenta es la recomendación de parchear vulnerabilidades detectadas en servicios críticos de manera inmediata como fue el caso de HttpFileServer (HFS 2.3) en Host A y SMB en Host B. De este modo se eliminan vectores de ataque y se actúa de manera eficaz en la prevención de ataques. También se resalta a manera de recomendación la implementación de una segmentación estricta de la red interna para mitigar y evitar movimientos laterales no autorizados entre los equipos.

Para que así, se limite el acceso entre Host A y Host B y hacia otros recursos, equipos o datos sensibles.

Otro aspecto para tener en cuenta es el fortalecimiento de la gestión de cuentas administrativas, las cuales deben tener controles como la restricción a la creación y el uso de cuentas con privilegios elevados, dado que esto puede ser aprovechado por un atacante para infiltrarse en los equipos. Igualmente, también se propone aplicar nuevas políticas de auditoría para realizar un monitoreo continuo con el fin de detectar cuentas no autorizadas y actividades sospechosas que pueden indicar que los equipos pueden ser vulnerados. Bajo la misma línea de los privilegios, se recomienda restringir algunos para que se minimicen los intentos a accesos de manera remota. De esta manera, la empresa puede actuar de manera inmediata para prevenir nuevos episodios de ataques.

Prioridad Alta y Horizonte de Implementación a Medio Plazo

Teniendo en cuenta que se apliquen nuevas políticas, dentro de estas entraría la configuración y el mantenimiento de los sistemas de detección y prevención de intrusiones (IDS/IPS) para identificar y bloquear de manera inmediata intentos de explotación y movimientos laterales no autorizados. Igualmente, también se recomienda la adopción de una autenticación para sistemas críticos, además de establecer controles de acceso de acuerdo con los cargos o roles que se desempeñen en la empresa con el propósito de mitigar riesgos de robo de credenciales. Acompañado de lo anterior, se recomienda la revisión de software para bloquear herramientas de administración no reguladas, además de restringir el uso de PowerShell y otras consolas de comandos.

Consecuentemente, también se propone la realización de actividades periódicas como la caza de amenazas (threat hunting) para identificar comportamientos anómalos, archivos sospechosos, y patrones de movimiento lateral o persistencia dentro de la red. Además, de que esta estrategia también puede servir para actualizar de manera inmediata sistemas o equipos que lo requieran para evitar que se vuelvan vulnerables. Del mismo modo, el despliegue de sistemas para detener y responder en endpoints (EDR) es vital para poder poner los dispositivos comprometidos en cuarentena de manera automática, para que el sistema SIEM evalúe y analice los eventos en tiempo real.

Prioridad Media y Horizonte de Implementación a Largo Plazo

Respecto a la temática legal, se recomienda realizar una revisión de contratos como por ejemplo los de Red Team y Blue Team, para eliminar cláusulas ambiguas, asegurar el cumplimiento de las leyes al respecto del manejo de información y de informática, lo cual hará que la empresa tenga un mejor manejo de responsabilidad con sus equipos aliados.

También, se recomienda establecer auditorías periódicas tanto para contratos con agentes externos como para realizar seguimiento al cumplimiento de las normativas y asegurar que la empresa esté cumpliendo a cabalidad lo que indica la ley.

Por último, en cuento a lo ético, se recomienda que se capacite al personal en cuanto a la ética profesional como lo estipula Copnia, con el propósito de realizar una revisión a las normativas que son resaltadas por este manual para tener en cuenta y evitar vulneraciones tanto a las leyes como al profesionalismo de cada empleado. Del mismo modo, se recomienda también realizar actividades y talleres para mantener actualizados a los trabajadores respecto a nuevas vulnerabilidades, procesos y ejercicios novedosos para mitigar ataques.

Referencias Bibliográficas

Alonso-Cubillos, D & Antolinez-López, L. (2022). Análisis de vulnerabilidades a un segmento de la red privada del área de TI de una empresa del sector industrial basado en la metodología PTES. Universidad Católica de Colombia. Disponible en: https://hdl.handle.net/10983/30285

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10–29). https://www.ccncert.cni.es/pdf/guias/series-ccn-stic/guias deacceso-publico-ccnstic/1617-ccn-stic-495-seguridad-en ipv6/file.html

Centro de Respuestas a Incidentes Informáticos – CSIRT Académico UNAD. (2024). Guía para la valoración y evaluación de riesgos de ciberseguridad de los activos de información UNADISTAS. Universidad Nacional Abierta y a Distancia – UNAD (Versión 1.0, pp. 5 31). https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Guia_para_la_valoración_y_evaluación_de_riesgos_de_ciberseguridad Pag_publicado.pdf

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(4), 192. https://doi.org/10.3390/info13040192

Chindrus, C., & Caruntu, C. F. (2023). Securing the network: a red and blue cybersecurity competition case study. *Information*, *14*(11), 587. https://doi.org/10.3390/info14110587

CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

Congreso de la República de Colombia. (2009, 05 de enero). Ley 1273 de 2009 (enero 05) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan

integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial, 2009, No. 47256, 1–3.

Congreso de la República de Colombia. (2012, 17 de octubre). Ley 1581 de 2012 (octubre 17). Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada Parcialmente por el Decreto 1081 de 2015. Ver sentencia C-748 de 2011. Ver Decreto 255 de 2022. Diario Oficial 48587 de octubre 18 de 2012. [Diario Oficial de Colombia 48587], 1-9.

Constitución Política de Colombia, 1991. (1991, 7 de julio). Art. 15. 7 de julio de 1991.

Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia (pp. 3–26). https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

Fortra.com. (2022). Qué es el escaneo de vulnerabilidades y cómo funciona. Obtenido de https://www.fortra.com/es/blog/escaneo-vulnerabilidades

Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI- driven strategies in cybersecurity risk assessment and fraud prevention. *J. Sci.Technol*, *11*, 001-024. https://doi.org/10.53022/oarjst.2024.11.1.0060

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protegetuempresa/blog/elpentestingauditandoseguridadtus- sistemas

Kristian, A., Az-Zahra, A. R., Hidayat, F., Fauzi, A. Y., & Kallas, E. (2024). Enhancing Cybersecurity Risk Management Strategies in Financial Institutions: A Comprehensive Analysis of Threats and Mitigation Approaches. *Journal of Computer Science and Technology Application*, *1*(2), 96-103. https://doi.org/10.33050/corisinta.v1i2.31

MINTIC. (2022). Políticas de Privacidad y Condiciones de Uso. https://www.mintic.gov.co/portal/inicio/Secciones-auxiliares/Politicas/2627:Politicas- de-Privacidad-y-Condiciones-de-Uso

Mızrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), 98-108. https://doi.org/10.17261/Pressacademia.2023.1807

Moreno, P. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management). USFQ (pp. 31– 63). http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/1208 01.pdf

Palomo Luna, D. F., Zambrano Hernández, L. F., Moreno Molano, S. X., & Peña Hidalgo, H. J. (2024, octubre). Una mirada a metodologías para pruebas de penetración en ciberseguridad. Boletín Informativo CSIRT Académico UNAD, (28). https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Boletin/Octubre_2024.pdf

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. 2011 IEEE 29th International Conference on Computer Design (ICCD), 285–288. https://doi.org/10.1109/ICCD.2011.6081410

Reglamento (Unión Europea). (2016/679). (Reglamento General de Protección de Datos). Diario Oficial de la Unión Europea L 119, de 4 de mayo de 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Zambrano Hernández, Peña Hidalgo, H. J., & Cárdenas Corral. (2024). Guía para la Gestión y Clasificación de Incidentes de Ciberseguridad. Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

Apéndices

Apéndice A

Resultado de Revisión en Turnitin

Título	Fecha de inicio	Fecha Esperada	Fecha de publicación	Puntos disponibles
ECBTI - Draftbank 1 - Sección 2	7 ene 2026 - 08:19	31 dic 2026 - 08:19	31 dic 2026 - 08:19	0

Refrescar Envíos

	Título del Envío	Identificador del trabajo de Turnitin	Enviado	Similitud	Calificación	Calificación General	
Ver Recibo Digital	Capacidades técnicas, tácticas y de respuesta para equipos red team y blue team	2866024986	28/01/2026 22:17	6%	N/A	--	Entregar Trabajo

Nota. La captura anexada es el resultado de la revisión realizada por Turnitin, la cual indica el nivel de plagio hallado en este trabajo.