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

Zuly Yuranny Davila Paredes

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Dedicatoria

Dedico este trabajo a **mi mamá**, por ser mi mayor ejemplo de esfuerzo, fortaleza y amor incondicional. Gracias por acompañarme en cada etapa de mi vida, creer en mí y enseñarme que la constancia y la dedicación siempre tienen recompensa.

A mis sobrinos y hermanos, quienes con su cariño, apoyo y compañía han sido una motivación constante para continuar creciendo personal y profesionalmente.

A **Angie y Juan**, mis mejores amigos, por estar presentes en los momentos más difíciles, brindarme su apoyo incondicional y recordarme siempre mis capacidades para superar cada desafío, gracias por ser mi fortaleza.

A mis amigos, en especial a mi compañero de carrera y luchas **Edison**, sé que fue difícil el camino, pero lo logramos juntos. Y a todas las personas que hicieron parte de este camino, por sus palabras de ánimo, consejos y apoyo durante este proceso académico y personal.

Agradecimientos

En primer lugar, agradezco a **Dios** por darme la fortaleza, la sabiduría y la perseverancia necesarias para superar cada reto presentado durante este proceso académico y personal. Gracias por acompañarme en cada paso, iluminar mi camino y permitirme alcanzar una meta más en mi vida.

Expreso un agradecimiento muy especial a mis mentores **Delis y Jhon**, quienes a lo largo de este camino compartieron conmigo sus conocimientos, experiencias y consejos. Gracias por creer en mis capacidades, por motivarme constantemente y por aportar significativamente a mi formación profesional y humana. Sus enseñanzas y apoyo fueron fundamentales para mi crecimiento.

Asimismo, agradezco profundamente a la Universidad Nacional Abierta y a Distancia (UNAD), institución que no solo me permitió formarme académicamente, sino también vivir experiencias que marcaron mi vida profesional y personal. Gracias por brindarme oportunidades laborales, espacios de aprendizaje y la posibilidad de contribuir activamente a este gran proyecto educativo que transforma vidas a través del conocimiento. Ser parte de esta universidad ha representado una experiencia enriquecedora y de gran valor para mi futuro.

De igual manera, quiero agradecer a **Kathe y Angy**, personas maravillosas que conocí durante mi etapa de monitoria, una experiencia significativa que fortaleció nuestra amistad con el paso del tiempo. Gracias por acompañarme en momentos difíciles, por brindarme ánimo cuando más lo necesitaba y por estar presentes en mi transición hacia la vida profesional. Su apoyo, confianza y amistad han significado mucho para mí.

Finalmente, agradezco a todos los docentes, compañeros, familiares, amigos y personas que hicieron parte de este proceso de formación y crecimiento. Cada enseñanza, consejo, palabra de aliento y experiencia compartida aportó de manera significativa a la culminación de esta etapa y al logro de este importante objetivo.

Resumen

La ciberseguridad se ha convertido en un elemento fundamental para la protección de la información y la continuidad operativa de las organizaciones frente al incremento de amenazas informáticas. En este trabajo se analizan las capacidades técnicas, tácticas y de respuesta de los equipos Red Team y Blue Team, abordando tanto los aspectos ofensivos como defensivos dentro de un entorno controlado de pruebas de penetración. Inicialmente, se estudia el marco normativo colombiano relacionado con delitos informáticos y protección de datos personales, destacando la importancia de actuar conforme a principios éticos y legales durante las operaciones de seguridad informática. Posteriormente, se describen las etapas del pentesting y el uso de herramientas especializadas como Nmap, OpenVAS y Metasploit para el reconocimiento, análisis y explotación de vulnerabilidades. Como componente práctico, se desarrolló un laboratorio virtualizado con sistemas Windows 7 y Parrot Security OS, donde se identificó y explotó la vulnerabilidad MS17-010 (EternalBlue) a través del servicio SMB, logrando acceso remoto controlado al sistema objetivo. A partir de este escenario, se evaluaron medidas de hardening, estrategias de contención y herramientas de monitoreo como SIEM, IDS/IPS y EDR, orientadas a fortalecer la postura de seguridad de las organizaciones y reducir el impacto de posibles incidentes. Finalmente, el trabajo resalta la importancia de integrar conocimientos técnicos, capacidades de respuesta y principios éticos para enfrentar de manera adecuada los desafíos actuales de la ciberseguridad.

Palabras clave: ciberseguridad, hardening, pentesting, SIEM, vulnerabilidades.

Abstract

Cybersecurity has become a fundamental element for protecting information and ensuring organizational operational continuity against the increasing number of cyber threats. This paper analyzes the technical, tactical, and response capabilities of Red Team and Blue Team operations, addressing both offensive and defensive aspects within a controlled penetration testing environment. Initially, the Colombian legal framework related to cybercrime and personal data protection is examined, highlighting the importance of acting according to ethical and legal principles during cybersecurity operations. Subsequently, the stages of penetration testing and the use of specialized tools such as Nmap, OpenVAS, and Metasploit for reconnaissance, vulnerability analysis, and exploitation are described. As a practical component, a virtualized laboratory environment was developed using Windows 7 and Parrot Security OS, where the MS17-010 (EternalBlue) vulnerability was identified and exploited through the SMB service, achieving controlled remote access to the target system. Based on this scenario, hardening measures, containment strategies, and monitoring tools such as SIEM, IDS/IPS, and EDR were evaluated to strengthen organizational security posture and reduce the impact of potential incidents. Finally, the paper highlights the importance of integrating technical knowledge, response capabilities, and ethical principles to adequately address current cybersecurity challenges.

Keywords: cybersecurity, hardening, pentesting, SIEM, vulnerabilities.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Lista de Apéndices

Glosario

Ataque informático:

Acción dirigida a comprometer la confidencialidad, integridad o disponibilidad de sistemas, redes o información mediante el aprovechamiento de vulnerabilidades, errores de configuración o técnicas especializadas de explotación.

Blue Team:

Equipo responsable de la defensa activa y pasiva de la infraestructura tecnológica, encargado de la detección, análisis y contención de incidentes de seguridad.

Ciberespionaje:

Actividad de adquisición clandestina de información confidencial mediante técnicas digitales, usualmente por motivos políticos, económicos o militares.

Explotación (Exploit):

Procedimiento mediante el cual se aprovecha una vulnerabilidad para ejecutar acciones no autorizadas sobre un sistema.

Firewall:

Dispositivo o software que controla y filtra el tráfico de red, bloqueando accesos no autorizados y protegiendo la infraestructura.

Hardening:

Conjunto de configuraciones y acciones destinadas a fortalecer la seguridad de sistemas, reducir vulnerabilidades y prevenir posibles ataques.

HTTPS:

Protocolo de comunicación segura en internet que cifra los datos transmitidos para garantizar la confidencialidad e integridad de la información.

IDS/IPS:

Sistemas de detección (IDS) y prevención (IPS) de intrusiones que monitorizan y controlan actividades sospechosas en la red.

Meterpreter:

Payload avanzado que permite gestionar sesiones remotas en sistemas comprometidos, facilitando tareas como escalamiento de privilegios, captura de información y control del sistema de manera interactiva.

Movimientos laterales:

Técnica de ataque que consiste en desplazarse dentro de una red comprometida para acceder a otros sistemas y recursos.

Pentesting:

Pruebas controladas de penetración realizadas para identificar vulnerabilidades en sistemas, redes o aplicaciones antes de que puedan ser explotadas por atacantes.

Pivoting:

Método empleado por un atacante para utilizar un equipo previamente comprometido como puente hacia otros sistemas dentro de la red interna.

Red Team:

Equipo encargado de simular ataques reales para evaluar la postura de seguridad de una organización mediante el uso de técnicas ofensivas controladas.

SIEM (Security Information and Event Management):

Solución de seguridad que permite recopilar, correlacionar y analizar registros de eventos provenientes de múltiples dispositivos y aplicaciones con el fin de detectar amenazas, generar alertas y facilitar la respuesta ante incidentes de seguridad.

Vulnerabilidad:

Debilidad presente en un sistema, aplicación o infraestructura que puede ser explotada por atacantes para comprometer la confidencialidad, integridad o disponibilidad de la información.

Introducción

En la actualidad, las organizaciones dependen cada vez más de las tecnologías de la información para desarrollar sus actividades operativas, administrativas y estratégicas. Esta dependencia ha incrementado la necesidad de proteger los sistemas informáticos frente a amenazas que pueden afectar la confidencialidad, integridad y disponibilidad de los datos. Según Stallings (2018), la seguridad informática debe abordarse mediante la implementación de controles técnicos, administrativos y operativos que permitan prevenir, detectar y responder de manera efectiva ante posibles incidentes.

Ante este panorama, las estrategias de ciberseguridad han evolucionado hacia modelos que combinan capacidades ofensivas y defensivas con el fin de fortalecer la protección de los activos digitales. De acuerdo con Kim y Solomon (2016), los equipos Red Team realizan ejercicios controlados de simulación de ataques para identificar vulnerabilidades y evaluar la efectividad de los controles de seguridad existentes, mientras que los equipos Blue Team centran sus esfuerzos en la vigilancia, detección y respuesta frente a actividades maliciosas dentro de la infraestructura tecnológica.

El presente trabajo analiza los principales conceptos relacionados con las operaciones Red Team y Blue Team, abordando aspectos como las fases del pentesting, el análisis de vulnerabilidades, la explotación controlada de sistemas y las estrategias de respuesta ante incidentes. Asimismo, se estudian diferentes herramientas utilizadas en entornos de ciberseguridad para comprender su aporte en los procesos de identificación, mitigación y gestión de riesgos tecnológicos.

Como complemento al componente teórico, se desarrolló un laboratorio práctico orientado a la identificación y explotación de la vulnerabilidad MS17-010 (EternalBlue) en un entorno virtualizado. Esta actividad permitió observar de manera controlada el impacto que

pueden generar las configuraciones inseguras y la falta de actualización de los sistemas, evidenciando la importancia de implementar medidas como la gestión de parches, la segmentación de redes y el monitoreo continuo para reducir la probabilidad de compromiso de la infraestructura tecnológica (Scarfone & Mell, 2007).

Justificación

La transformación digital ha incrementado la dependencia de las organizaciones respecto a sus sistemas de información, lo que ha convertido la ciberseguridad en un componente estratégico para proteger los activos tecnológicos y garantizar la continuidad de las operaciones. De acuerdo con Stallings (2018), la implementación de mecanismos de protección debe contemplar tanto medidas preventivas como controles de detección y respuesta que permitan reducir la exposición frente a amenazas cada vez más sofisticadas.

En este contexto, el estudio de los equipos Red Team y Blue Team resulta relevante debido a que ambos contribuyen al fortalecimiento de la seguridad organizacional desde perspectivas complementarias. Mientras las actividades ofensivas permiten identificar vulnerabilidades mediante la simulación de ataques controlados, las estrategias defensivas buscan detectar, contener y mitigar incidentes antes de que generen impactos significativos sobre la infraestructura tecnológica (Kim & Solomon, 2016).

Asimismo, el desarrollo del laboratorio práctico permite aplicar conocimientos relacionados con pruebas de penetración, análisis de vulnerabilidades y respuesta ante incidentes en un entorno controlado. Esta experiencia facilita la comprensión de los riesgos asociados a configuraciones inseguras, sistemas desactualizados y deficiencias en la gestión de la seguridad, aspectos que continúan siendo aprovechados por los atacantes para comprometer sistemas informáticos (Scarfone & Mell, 2007).

Finalmente, esta investigación aporta elementos técnicos y metodológicos que permiten comprender la importancia de integrar estrategias ofensivas y defensivas dentro de un programa de ciberseguridad, favoreciendo la adopción de medidas orientadas a mejorar la protección de la información y la resiliencia organizacional frente a las amenazas digitales actuales.

Objetivos

Objetivo General

Analizar la importancia de las estrategias ofensivas y defensivas en ciberseguridad mediante el estudio de las funciones de los equipos Red Team y Blue Team, con el fin de comprender su contribución en la identificación de vulnerabilidades y el fortalecimiento de la seguridad de los sistemas de información.

Objetivos Específicos

Analizar las funciones, metodologías y herramientas empleadas por los equipos Red Team y Blue Team en los procesos de evaluación y fortalecimiento de la seguridad informática.

Identificar vulnerabilidades presentes en un entorno de pruebas mediante actividades de reconocimiento y análisis de seguridad.

Ejecutar de forma controlada la explotación de la vulnerabilidad MS17-010 (EternalBlue) para evaluar su impacto sobre sistemas que no cuentan con las actualizaciones de seguridad correspondientes.

Proponer medidas de mitigación y controles de seguridad orientados a la reducción de riesgos y al fortalecimiento de las capacidades de detección y respuesta ante incidentes.

Fundamentos de Operaciones Red Team y Blue Team

La protección de los sistemas de información requiere la aplicación de enfoques que permitan anticipar amenazas, identificar debilidades y establecer controles capaces de reducir los riesgos asociados al entorno digital. De acuerdo con Stallings (2018), las organizaciones deben adoptar estrategias integrales de seguridad que combinen actividades de evaluación, monitoreo y respuesta para garantizar la protección de sus recursos tecnológicos. En este contexto, los equipos Red Team y Blue Team constituyen componentes esenciales dentro de los programas de ciberseguridad, ya que sus funciones permiten evaluar la eficacia de los controles existentes y fortalecer las capacidades de defensa frente a posibles incidentes.

Según Kim y Solomon (2016), las actividades desarrolladas por el Red Team se orientan a la identificación de vulnerabilidades mediante ejercicios controlados que replican técnicas utilizadas por actores maliciosos, mientras que el Blue Team se encarga de supervisar los sistemas, detectar comportamientos anómalos y coordinar acciones de mitigación. Por esta razón, el trabajo conjunto de ambos equipos contribuye a una comprensión más amplia de los riesgos y favorece la implementación de medidas orientadas al fortalecimiento de la seguridad organizacional.

En esta primera fase se presentan los conceptos fundamentales relacionados con las operaciones Red Team y Blue Team, abordando sus responsabilidades, metodologías y aportes dentro de los procesos de gestión de la seguridad informática. Asimismo, se analiza la relevancia de la colaboración entre ambos enfoques para mejorar la capacidad de las organizaciones frente a las amenazas que afectan los entornos tecnológicos actuales.

Legislación sobre delitos informáticos y protección de datos en Colombia

El marco jurídico colombiano relacionado con la seguridad de la información y la protección de datos personales ha sido fortalecido durante los últimos años con el propósito de responder a los riesgos derivados del uso de las tecnologías de la información. Estas disposiciones buscan proteger tanto los sistemas informáticos como los derechos de los ciudadanos frente al tratamiento de sus datos personales, estableciendo responsabilidades y sanciones para quienes incumplan la normativa vigente.

Ley 1273 de 2009: protección penal de la información y los sistemas informáticos

Con la expedición de la Ley 1273 de 2009 se incorporó al ordenamiento jurídico colombiano un conjunto de delitos orientados a proteger la información digital y los sistemas tecnológicos. Esta norma modificó el Código Penal e introdujo un nuevo bien jurídico relacionado con la protección de la información y de los datos (Congreso de Colombia, 2009). Entre las conductas sancionadas se encuentran el acceso no autorizado a sistemas informáticos, la interceptación de información, la alteración de datos y la distribución de software destinado a causar afectaciones en los sistemas. De esta manera, la ley busca preservar principios esenciales de la seguridad de la información, como la confidencialidad, la integridad y la disponibilidad.

Ley 1266 de 2008: regulación del habeas data financiero

La Ley 1266 de 2008 establece las condiciones para el tratamiento de información financiera, crediticia, comercial y de servicios. Su finalidad principal es garantizar que los ciudadanos puedan ejercer control sobre la información registrada en bases de datos relacionadas con su historial financiero. Según esta norma, los titulares tienen la facultad de consultar, actualizar y corregir los datos que reposen sobre ellos en este tipo de sistemas de información (Congreso de Colombia, 2008). Asimismo, la ley define principios y responsabilidades que

deben cumplir las entidades encargadas del manejo de dichos datos para asegurar un tratamiento adecuado y transparente.

Ley 1581 de 2012: régimen general de protección de datos personales

La Ley 1581 de 2012 constituye la principal norma colombiana en materia de protección de datos personales. Su propósito es desarrollar el derecho de las personas a conocer, actualizar y rectificar la información que haya sido recopilada sobre ellas por entidades públicas o privadas (Congreso de Colombia, 2012). Esta legislación establece principios que orientan el tratamiento de los datos, entre ellos la legalidad, la finalidad, la libertad, la transparencia, la seguridad y la confidencialidad. Además, reconoce derechos específicos para los titulares y contempla medidas especiales para la protección de información sensible y de datos relacionados con menores de edad.

Decreto 1377 de 2013: reglamentación del tratamiento de datos personales

Con el objetivo de facilitar la aplicación práctica de la Ley 1581 de 2012, el Decreto 1377 de 2013 definió lineamientos relacionados con la autorización para el tratamiento de datos personales y las obligaciones de quienes administran dicha información. La norma establece que la autorización del titular debe obtenerse de manera previa, informada y expresa antes de realizar cualquier tratamiento de los datos (Ministerio de Comercio, Industria y Turismo, 2013). Igualmente, exige la adopción de políticas internas que permitan a los ciudadanos ejercer sus derechos de consulta, actualización, corrección y supresión de la información cuando corresponda.

Constitución Política de Colombia: fundamento del derecho a la protección de datos

La base constitucional de toda la regulación colombiana en materia de protección de datos se encuentra en el artículo 15 de la Constitución Política de 1991. Esta disposición reconoce el derecho de las personas a la intimidad, al buen nombre y al control sobre la

información que se almacena acerca de ellas. Asimismo, establece la facultad de conocer, actualizar y rectificar los datos personales registrados en archivos o bases de datos públicas y privadas (Constitución Política de Colombia, 1991). A partir de este mandato constitucional se han desarrollado las diferentes normas que actualmente regulan la protección de la información personal en el país.

En el ámbito de la ciberseguridad, el conocimiento y cumplimiento de estas disposiciones resulta indispensable para garantizar que actividades como las pruebas de penetración, el análisis de vulnerabilidades y la gestión de incidentes se desarrollen de manera ética, responsable y conforme a la legislación colombiana vigente.

Relación del marco legal con las actividades de Red Team y Blue Team

Las actividades desarrolladas por los equipos Red Team y Blue Team deben ejecutarse dentro de un marco normativo que garantice la protección de la información, el respeto por la privacidad de los usuarios y el cumplimiento de las disposiciones legales vigentes. En el contexto de las pruebas de penetración y los ejercicios de seguridad ofensiva, la legislación colombiana establece límites y responsabilidades que condicionan la planeación, ejecución y documentación de este tipo de actividades (Congreso de Colombia, 2009).

En el caso de las operaciones Red Team, la Ley 1273 de 2009 adquiere especial relevancia debido a que tipifica conductas relacionadas con el acceso no autorizado a sistemas informáticos, la interceptación de datos y otras acciones que pueden afectar la seguridad de la información. Por esta razón, las pruebas de penetración deben realizarse únicamente bajo autorización expresa de la organización, dentro de un alcance previamente definido y con fines legítimos de evaluación de seguridad, evitando cualquier actuación que pueda interpretarse como una conducta delictiva (Congreso de Colombia, 2009).

De igual manera, la Ley 1581 de 2012, el Decreto 1377 de 2013 y el artículo 15 de la Constitución Política de Colombia establecen principios relacionados con la protección de datos personales y el derecho fundamental al habeas data. Durante la ejecución de actividades de seguridad informática, los profesionales pueden acceder a información sensible o confidencial, por lo que resulta necesario garantizar que el tratamiento de dichos datos se realice conforme a los principios de legalidad, finalidad, seguridad y confidencialidad establecidos por la normativa colombiana (Congreso de Colombia, 2012; Ministerio de Comercio, Industria y Turismo, 2013; Constitución Política de Colombia, 1991).

Por su parte, los equipos Blue Team tienen la responsabilidad de implementar mecanismos de monitoreo, detección y respuesta ante incidentes, asegurando que la recolección y el análisis de eventos de seguridad se desarrollen respetando los derechos de los titulares de la información. Asimismo, la elaboración de informes técnicos y el reporte de hallazgos deben realizarse bajo criterios de responsabilidad profesional, evitando la divulgación indebida de datos o vulnerabilidades que puedan comprometer la seguridad de la organización (Congreso de Colombia, 2012).

En consecuencia, el cumplimiento de las disposiciones legales no solo constituye una obligación normativa, sino también un elemento esencial para garantizar que las actividades de Red Team y Blue Team se desarrollen de manera ética, controlada y alineada con las buenas prácticas de ciberseguridad, contribuyendo al fortalecimiento de la seguridad de los sistemas de información y a la protección de los datos personales (Congreso de Colombia, 2009; Congreso de Colombia, 2012).

Si bien el cumplimiento de la normativa vigente constituye un requisito fundamental para el desarrollo de actividades relacionadas con la ciberseguridad, la actuación de los profesionales no debe limitarse únicamente al marco legal. La ejecución de pruebas de penetración, el análisis

de vulnerabilidades y la gestión de información sensible también requieren la aplicación de principios éticos que orienten la toma de decisiones y garanticen una actuación responsable frente a los riesgos asociados al uso de herramientas y técnicas de seguridad informática. En este sentido, la ética profesional complementa las disposiciones legales al promover valores como la integridad, la confidencialidad, la responsabilidad y el respeto por los derechos de las personas y las organizaciones. Por ello, resulta pertinente analizar situaciones prácticas en las que los aspectos éticos y normativos convergen, permitiendo evaluar los desafíos que enfrentan los profesionales de ciberseguridad en el ejercicio de sus funciones.

Ética Profesional y Marco Normativo en Operaciones de Ciberseguridad

El análisis de la documentación suministrada por SecureNova Labs permitió identificar diversas situaciones que generan preocupaciones tanto desde la perspectiva ética como legal. Uno de los aspectos más relevantes es la inclusión de actividades relacionadas con interceptación de datos, accesos no autorizados y otras prácticas que podrían estar asociadas con delitos informáticos. Esta situación resulta especialmente delicada debido a que dichas acciones son presentadas como parte de la información confidencial de la organización, lo que evidencia un posible conocimiento y aceptación de conductas que podrían vulnerar la normativa vigente.

Adicionalmente, el acuerdo establece restricciones relacionadas con la divulgación de información, incluso cuando esta se encuentra asociada a posibles actividades ilícitas. Este tipo de cláusulas pueden interpretarse como mecanismos orientados a limitar la denuncia de conductas irregulares ante las autoridades competentes, lo que genera conflictos con principios fundamentales de transparencia, responsabilidad y cumplimiento normativo. En este sentido, las disposiciones analizadas se alejan de los principios que orientan el ejercicio profesional de la

ciberseguridad, cuyo propósito principal debe ser la protección de la información y el fortalecimiento de la seguridad digital (Zuluaga Mateus, 2017).

Desde el ámbito jurídico, el acuerdo presenta posibles conflictos con diversas disposiciones establecidas en la Ley 1273 de 2009, norma que incorporó al ordenamiento jurídico colombiano los delitos informáticos. Entre los aspectos identificados se encuentran posibles vulneraciones relacionadas con el acceso abusivo a sistemas informáticos, la interceptación de datos informáticos y el tratamiento inadecuado de información sensible sin la debida autorización. Asimismo, algunas de las actividades descritas podrían afectar la confidencialidad, integridad y disponibilidad de la información, principios fundamentales protegidos por la legislación colombiana (Guarnizo Portela, 2024).

Bajo este contexto, aceptar una vinculación laboral bajo las condiciones planteadas por SecureNova Labs representaría un conflicto importante con los principios éticos y profesionales que deben orientar el ejercicio de la ciberseguridad. Aunque la propuesta puede resultar atractiva desde el punto de vista económico, la participación en actividades que impliquen la aceptación o el encubrimiento de conductas contrarias a la ley podría generar responsabilidades legales y afectar la integridad profesional. De acuerdo con el Código de Ética del COPNIA (2015), los profesionales tienen la obligación de actuar con responsabilidad, honestidad y respeto por la normativa vigente, priorizando siempre el bienestar de la sociedad y la protección de los derechos de terceros.

Por otra parte, el caso evidencia la importancia de establecer límites claros respecto al acceso y uso de información sensible dentro de las organizaciones dedicadas a la ciberseguridad. Aunque las auditorías y pruebas de seguridad requieren acceso a determinados recursos para identificar vulnerabilidades y riesgos, dicho acceso debe regirse por los principios de necesidad, proporcionalidad y autorización previa. No todos los profesionales deben tener acceso a toda la

información disponible, sino únicamente a aquella que resulte indispensable para el cumplimiento de sus funciones.

Asimismo, es fundamental implementar mecanismos de control que permitan supervisar el uso de la información sensible. Entre ellos se destacan los registros de actividad, la segregación de funciones, el monitoreo continuo y la definición de políticas claras sobre el tratamiento de datos. Estas medidas contribuyen a prevenir abusos, fortalecer la confianza de los clientes y garantizar que las actividades de auditoría se desarrollen dentro de los límites éticos y legales establecidos.

Finalmente, el caso de SecureNova Labs permite reflexionar sobre la responsabilidad que tienen las organizaciones de ciberseguridad frente al manejo de información crítica. La confianza depositada por clientes y usuarios exige que las actividades de protección se desarrollen bajo estrictos estándares éticos, legales y profesionales. Cuando estos principios no son respetados, los impactos trascienden el ámbito técnico y pueden afectar la reputación, la credibilidad y la sostenibilidad de la organización. Por esta razón, el ejercicio de la ciberseguridad debe fundamentarse siempre en la legalidad, la transparencia y el compromiso con la protección de la información.

El análisis de los aspectos éticos y normativos permite comprender que las actividades de ciberseguridad deben desarrollarse bajo criterios de responsabilidad profesional, respeto por la legislación vigente y protección de la información. Sin embargo, además de conocer los límites legales y éticos que regulan estas prácticas, resulta necesario comprender las metodologías técnicas utilizadas para evaluar la seguridad de los sistemas informáticos. En este contexto, las pruebas de penetración o pentesting constituyen una de las estrategias más empleadas para identificar vulnerabilidades, analizar riesgos y validar el nivel de exposición de una infraestructura tecnológica mediante procedimientos controlados y previamente autorizados. Por

esta razón, a continuación, se describen las principales etapas que conforman el proceso de pentesting y su importancia dentro de las operaciones de ciberseguridad.

Etapas del Pentesting

Las pruebas de penetración o *pentesting* constituyen un proceso estructurado que permite evaluar la seguridad de sistemas, redes y aplicaciones mediante la simulación controlada de ataques. Su finalidad es identificar vulnerabilidades, validar su impacto potencial y generar recomendaciones que contribuyan al fortalecimiento de la postura de seguridad de una organización. Para ello, el proceso se desarrolla a través de varias etapas secuenciales que permiten obtener información, analizar riesgos y documentar los resultados obtenidos (EC-Council, 2023).

La primera fase corresponde al **reconocimiento o footprinting**, cuyo propósito es recopilar la mayor cantidad posible de información sobre el objetivo. Esta actividad puede realizarse de forma pasiva, utilizando fuentes públicas de información, o de manera activa mediante una interacción limitada con el entorno evaluado. Durante esta etapa se busca identificar dominios, direcciones IP, tecnologías empleadas y posibles puntos de entrada que puedan ser utilizados en fases posteriores. Herramientas como **Maltego** facilitan este proceso al permitir la recolección y visualización de relaciones entre dominios, direcciones IP y cuentas de correo electrónico (EC-Council, 2023).

Posteriormente se desarrolla la fase de **escaneo y enumeración**, en la cual se analizan los sistemas identificados para determinar qué servicios se encuentran disponibles, cuáles son los puertos abiertos y qué versiones de software están en ejecución. Asimismo, esta etapa permite obtener información adicional sobre usuarios, recursos compartidos y configuraciones relevantes

para la evaluación de seguridad. Para estas actividades es común emplear herramientas como **Nmap**, ampliamente utilizada para el descubrimiento de hosts, la identificación de servicios y el análisis de puertos en redes informáticas (EC-Council, 2023).

Una vez recopilada esta información, se procede al **análisis de vulnerabilidades**, etapa orientada a identificar debilidades específicas que puedan comprometer la seguridad de los sistemas evaluados. Entre las vulnerabilidades más comunes se encuentran las configuraciones inseguras, el uso de software desactualizado y la presencia de fallos de seguridad previamente documentados. En este contexto, soluciones como **OpenVAS** permiten automatizar el proceso de detección y clasificación de vulnerabilidades, facilitando la identificación de riesgos potenciales que requieren atención (NIST, 2020).

La fase de **explotación** tiene como objetivo comprobar si las vulnerabilidades identificadas pueden ser aprovechadas de manera efectiva. Durante esta etapa se ejecutan pruebas controladas para validar el impacto real de las debilidades detectadas y determinar el nivel de acceso que podría obtener un atacante. Una de las herramientas más utilizadas para este propósito es **Metasploit Framework**, plataforma que proporciona múltiples módulos para la ejecución de pruebas de explotación sobre diferentes sistemas y servicios (EC-Council, 2023).

Después de lograr el acceso inicial, se desarrolla la etapa de **post-explotación**, la cual permite evaluar el alcance del compromiso alcanzado dentro de la infraestructura. En esta fase se analizan aspectos como el escalamiento de privilegios, el acceso a información sensible y la posibilidad de realizar movimientos laterales hacia otros sistemas de la red. Herramientas como **Mimikatz** son utilizadas frecuentemente para demostrar el impacto de una vulnerabilidad mediante la extracción controlada de credenciales almacenadas en sistemas comprometidos (Microsoft, 2017).

Finalmente, la fase de **reporte o reporting** consiste en documentar de manera detallada todos los hallazgos obtenidos durante la prueba de penetración. El informe resultante debe incluir las vulnerabilidades identificadas, las evidencias recopiladas, el impacto asociado a cada hallazgo y las recomendaciones necesarias para mitigar los riesgos detectados. Esta etapa constituye uno de los componentes más importantes del pentesting, ya que permite a las organizaciones tomar decisiones informadas para fortalecer sus controles de seguridad y mejorar sus capacidades de prevención, detección y respuesta ante incidentes (EC-Council, 2023).

Herramientas y servicios en ciberseguridad

Las actividades de evaluación de seguridad requieren el uso de herramientas especializadas que permitan identificar vulnerabilidades, analizar configuraciones, obtener información sobre los sistemas objetivo y validar el impacto de posibles fallos de seguridad. Dentro de los procesos de pentesting, estas herramientas apoyan las diferentes fases de reconocimiento, análisis y explotación, proporcionando información relevante para la toma de decisiones y la gestión de riesgos.

En la fase de reconocimiento y análisis de redes, una de las herramientas más utilizadas es **Nmap (Network Mapper)**. De acuerdo con el Nmap Project (s.f.), esta aplicación corresponde a una herramienta orientada al descubrimiento de dispositivos y auditoría de seguridad en redes. Su utilización permite identificar hosts activos, detectar puertos abiertos, reconocer servicios en ejecución y obtener información sobre los sistemas operativos presentes en la infraestructura evaluada. Estas capacidades convierten a Nmap en un recurso fundamental para la recopilación inicial de información durante una prueba de penetración.

Complementando las actividades de reconocimiento, los profesionales de seguridad suelen emplear herramientas de análisis de vulnerabilidades como **OpenVAS (Open Vulnerability Assessment System)**. Según Greenbone Networks (s.f.), se trata de un escáner integral de vulnerabilidades diseñado para identificar debilidades de seguridad en sistemas, aplicaciones y servicios de red. Mediante procesos automatizados de evaluación, OpenVAS facilita la detección de configuraciones inseguras, software desactualizado y vulnerabilidades conocidas, contribuyendo a la identificación temprana de riesgos dentro de la organización.

Una vez identificadas posibles vulnerabilidades, es necesario validar su impacto real mediante herramientas especializadas de explotación controlada. En este contexto, **Metasploit** constituye uno de los frameworks más reconocidos en el ámbito de las pruebas de penetración. De acuerdo con Rapid7 (s.f.), esta plataforma permite localizar, explotar y validar vulnerabilidades mediante el uso de módulos preconfigurados. Su utilización facilita la simulación de ataques reales en entornos controlados, permitiendo verificar el alcance de una vulnerabilidad y evaluar las posibles consecuencias de su explotación sobre los sistemas analizados.

Además de las herramientas de análisis y explotación, los profesionales de ciberseguridad recurren frecuentemente a servicios especializados para la consulta y clasificación de vulnerabilidades. Uno de los más relevantes es **Exploit Database (ExploitDB)**, repositorio público que almacena información técnica sobre vulnerabilidades y exploits conocidos. Según Offensive Security (s.f.), esta plataforma proporciona acceso a ejemplos documentados de explotación que permiten comprender el funcionamiento de diferentes ataques y apoyar las actividades de investigación y análisis de seguridad.

De manera complementaria, el sistema **Common Vulnerabilities and Exposures (CVE)** proporciona un mecanismo estandarizado para la identificación y clasificación de vulnerabilidades. MITRE (s.f.) señala que este sistema mantiene un listado de vulnerabilidades

públicamente conocidas, asignando a cada una un identificador único acompañado de información descriptiva y referencias técnicas. Gracias a esta estandarización, organizaciones, fabricantes y profesionales de seguridad pueden intercambiar información de manera consistente y facilitar la gestión de riesgos asociados a vulnerabilidades conocidas.

En conjunto, estas herramientas y servicios desempeñan un papel fundamental dentro de las actividades de Red Team y pentesting, ya que permiten obtener información detallada sobre los sistemas evaluados, identificar vulnerabilidades, validar su explotación y consultar información técnica que facilite la implementación de medidas de mitigación y fortalecimiento de la seguridad.

Si bien las herramientas y servicios especializados permiten identificar vulnerabilidades, analizar configuraciones y validar el impacto de posibles fallos de seguridad, su utilización debe realizarse dentro de límites técnicos, éticos y legales claramente establecidos. El acceso a sistemas, la recopilación de información y la ejecución de pruebas de penetración pueden involucrar datos sensibles e infraestructuras críticas, por lo que resulta indispensable que estas actividades se desarrollen bajo principios de responsabilidad profesional y en cumplimiento de la normativa vigente. En consecuencia, además del conocimiento técnico requerido para las operaciones de ciberseguridad, los profesionales deben comprender las obligaciones éticas y legales que regulan el ejercicio de estas actividades.

Las herramientas y servicios de ciberseguridad desempeñan un papel fundamental en la identificación de vulnerabilidades, el análisis de riesgos y la ejecución de pruebas de seguridad dentro de entornos controlados. No obstante, el uso de estas tecnologías implica responsabilidades relacionadas con la integridad de la información, la preservación de evidencias digitales y el cumplimiento de procedimientos establecidos para la gestión de incidentes. Por esta razón, además de conocer las capacidades técnicas de las herramientas empleadas durante las

actividades de seguridad informática, resulta necesario implementar mecanismos de control y supervisión que permitan garantizar un uso adecuado de los recursos tecnológicos, fortalecer los procesos de investigación y asegurar la confiabilidad de la información obtenida durante los análisis forenses. En este contexto, las estrategias de control y supervisión constituyen un componente esencial para la gestión segura y efectiva de las herramientas utilizadas en los procesos de análisis e investigación digital.

Estrategias de control y supervisión en el uso de herramientas forenses

El uso de herramientas forenses dentro de una organización requiere la implementación de mecanismos de control y supervisión que garanticen su utilización adecuada y conforme a los principios éticos y legales establecidos. No resulta suficiente confiar únicamente en el criterio individual de los empleados; por el contrario, es necesario establecer políticas y procedimientos que regulen el acceso, uso y monitoreo de estas herramientas especializadas (NIST, 2020).

Una de las medidas más importantes consiste en aplicar el principio de mínimo privilegio, mediante el cual cada usuario dispone únicamente de los permisos estrictamente necesarios para el cumplimiento de sus funciones. Esta práctica reduce significativamente el riesgo de accesos indebidos y limita las posibilidades de uso inadecuado de información sensible o de herramientas con capacidades avanzadas de análisis (NIST, 2020).

De igual manera, resulta fundamental implementar mecanismos de auditoría y trazabilidad que permitan registrar las actividades realizadas por los usuarios dentro de los sistemas. El mantenimiento de registros de actividad facilita la detección de comportamientos anómalos, el análisis de incidentes de seguridad y la identificación de posibles incumplimientos de las políticas organizacionales. Asimismo, estos controles actúan como una medida preventiva

al promover una mayor responsabilidad en el uso de los recursos tecnológicos (EC-Council, 2023).

Adicionalmente, las organizaciones deben establecer lineamientos claros respecto al uso permitido de las herramientas forenses, definiendo responsabilidades, restricciones y procedimientos de actuación. La capacitación continua y la sensibilización sobre aspectos éticos contribuyen a fortalecer la cultura de seguridad y a reducir riesgos derivados del desconocimiento o de prácticas inadecuadas. En consecuencia, la combinación de controles técnicos, supervisión permanente y responsabilidad profesional constituye un elemento esencial para garantizar un uso seguro y adecuado de las herramientas forenses (COPNIA, 2015).

Diferencias entre un equipo Blue Team y un equipo de respuesta a incidentes informáticos

El equipo Blue Team se encarga principalmente de proteger la infraestructura tecnológica de una organización mediante tareas preventivas y de monitoreo constante. Sus funciones incluyen identificar vulnerabilidades, fortalecer la seguridad de los sistemas, revisar eventos sospechosos y aplicar medidas de protección para evitar posibles ataques. Además, trabajan continuamente en mejorar la postura de seguridad de la organización y en reducir riesgos antes de que ocurra un incidente. Según Kotwani B., Sawant M. R. y Chopra D. S. (2023), los equipos Blue Team representan una defensa permanente frente a amenazas y ataques informáticos gracias al monitoreo continuo de la infraestructura tecnológica.

Por otro lado, los equipos de respuesta a incidentes informáticos actúan cuando el ataque o incidente ya ocurrió. Su trabajo se enfoca en contener el problema, analizar qué sucedió, eliminar la amenaza y recuperar los sistemas afectados para restablecer el funcionamiento normal de la organización. También se encargan de preservar evidencias digitales para apoyar investigaciones posteriores. A diferencia del Blue Team, que tiene un enfoque más preventivo, el

equipo de respuesta a incidentes trabaja de manera reactiva frente a situaciones de emergencia relacionadas con la seguridad informática. De acuerdo con Zambrano Hernández L. F., Peña Hidalgo H. J. y Cárdenas Corral J. (2024), una adecuada gestión de incidentes debe incluir procesos de identificación, contención, análisis y recuperación para disminuir el impacto de las amenazas cibernéticas.

Tabla 1

Diferencias entre el equipo Blue Team y el de respuesta a incidentes informáticos

Aspecto	Blue Team	Equipo de respuesta a incidentes
Enfoque principal	Prevención y monitoreo	Respuesta y recuperación
Momento de actuación	Antes de los incidentes	Durante y después del incidente
Objetivo	Evitar ataques y fortalecer la seguridad	Contener y solucionar incidentes
Actividades principales	Hardening, monitoreo, análisis de riesgos	Contención, análisis forense y recuperación
Tipo de trabajo	Preventivo	Reactivo
Herramientas comunes	SIEM, IDS/IPS, EDR	Forense digital, análisis de logs, contención
Resultado esperado	Reducir vulnerabilidades y riesgos	Minimizar daños y restaurar servicios

Nota. La tabla presenta las principales diferencias entre las funciones desarrolladas por un equipo Blue Team y un equipo de respuesta a incidentes dentro de una organización. Se destacan aspectos relacionados con el enfoque de trabajo, momento de actuación, objetivos, herramientas

utilizadas y actividades principales orientadas a la protección, detección, contención y recuperación frente a incidentes de ciberseguridad.

Aplicación de Controles CIS en Equipos Blue Team

Dentro de un equipo Blue Team, los controles CIS servirían como una guía para mejorar la seguridad de los sistemas y reducir posibles vulnerabilidades. Estos lineamientos ayudan a configurar de forma más segura equipos, servidores, redes y aplicaciones, evitando errores de configuración que podrían ser aprovechados por atacantes.

En el caso trabajado durante el laboratorio, aplicar controles CIS ayudaría a fortalecer la seguridad de los equipos Windows, por ejemplo, deshabilitando SMBv1, mejorando las políticas de contraseñas y limitando configuraciones inseguras dentro de la red. También serían útiles para realizar revisiones de seguridad y verificar si los sistemas cumplen con buenas prácticas de protección.

Otra ventaja de utilizar CIS es que permite organizar mejor las tareas de hardening y monitoreo dentro de la empresa. Además, ayuda a reducir riesgos relacionados con accesos no autorizados, vulnerabilidades conocidas y malas configuraciones que pueden facilitar ataques informáticos.

Aplicación de controles CIS y modelo Zero Trust

Actualmente, las organizaciones enfrentan una gran cantidad de amenazas informáticas que evolucionan constantemente y aprovechan cualquier vulnerabilidad presente dentro de la infraestructura tecnológica. Debido a esto, ya no es suficiente depender únicamente de antivirus tradicionales o firewalls básicos, sino que es necesario implementar estrategias de seguridad mucho más completas y enfocadas en la prevención, monitoreo y reducción de riesgos. Dentro

de estas estrategias, los CIS Controls y el modelo Zero Trust se han convertido en dos de los enfoques más utilizados para fortalecer la seguridad de las organizaciones y mejorar las capacidades de los equipos Blue Team encargados de la defensa y respuesta ante incidentes.

Los CIS Controls son un conjunto de buenas prácticas de seguridad desarrolladas por el Center for Internet Security (CIS), cuyo objetivo es ayudar a las organizaciones a proteger sus sistemas frente a amenazas comunes. Estos controles incluyen recomendaciones relacionadas con gestión de activos, control de accesos, monitoreo de eventos, gestión de vulnerabilidades y protección de datos. Según CIS (2024), la implementación adecuada de estos controles permite reducir significativamente la superficie de ataque y mejorar la capacidad de detección frente a incidentes de seguridad.

Uno de los aspectos más importantes de los CIS Controls es que están diseñados de forma práctica y priorizada, permitiendo que las organizaciones implementen medidas de seguridad de acuerdo con sus necesidades y capacidades. Por ejemplo, algunos controles básicos recomiendan mantener inventarios actualizados de dispositivos y software, eliminar servicios innecesarios y aplicar configuraciones seguras sobre sistemas operativos y aplicaciones. Estas medidas, aunque parecen simples, ayudan a reducir muchos de los riesgos explotados comúnmente por los atacantes.

Dentro del laboratorio desarrollado durante las pruebas de penetración, se evidenció cómo la falta de actualización y el uso de protocolos inseguros como SMBv1 facilitaron la explotación de la vulnerabilidad EternalBlue. Esto demuestra la importancia de aplicar controles relacionados con gestión de vulnerabilidades y administración de parches. La gestión de parches consiste en mantener los sistemas operativos, aplicaciones y servicios actualizados para corregir fallas de seguridad conocidas antes de que puedan ser aprovechadas por atacantes. Microsoft (2017) indicó que la vulnerabilidad MS17-010 podía mitigarse mediante actualizaciones de

seguridad liberadas previamente al ataque WannaCry, pero muchas organizaciones no aplicaron los parches correspondientes a tiempo.

Otro mecanismo importante dentro de las estrategias defensivas es la autenticación multifactor o MFA (Multi-Factor Authentication). Este mecanismo agrega una capa adicional de seguridad al proceso de autenticación, solicitando más de un método de verificación antes de permitir el acceso a un sistema. Por ejemplo, además de la contraseña, el usuario puede necesitar un código enviado al teléfono móvil o una aplicación de autenticación. Según Microsoft Security (2023), la implementación de MFA reduce considerablemente el riesgo de accesos no autorizados relacionados con robo o filtración de credenciales.

La autenticación multifactor se ha convertido en una práctica fundamental debido al incremento de ataques relacionados con robo de contraseñas, phishing y filtraciones de bases de datos. Incluso si un atacante obtiene las credenciales de un usuario, el acceso puede bloquearse si no posee el segundo factor de autenticación. Este tipo de medidas fortalece significativamente la seguridad de cuentas administrativas, accesos remotos y plataformas empresariales críticas.

Asimismo, otro enfoque que ha ganado gran relevancia en los últimos años es el modelo Zero Trust. Este modelo de seguridad se basa en el principio de “nunca confiar, siempre verificar”, lo que significa que ningún usuario o dispositivo debe considerarse confiable automáticamente, incluso si se encuentra dentro de la red interna de la organización. A diferencia de modelos tradicionales donde se asumía que todo lo que estaba dentro de la red corporativa era seguro, Zero Trust busca validar continuamente identidades, dispositivos y accesos antes de permitir interacción con recursos sensibles.

El modelo Zero Trust cobra aún más importancia en escenarios donde los atacantes logran comprometer un dispositivo interno mediante vulnerabilidades como EternalBlue. Si no existen controles adecuados, el atacante puede desplazarse lateralmente y acceder a múltiples

sistemas dentro de la red. Sin embargo, mediante Zero Trust y segmentación adecuada, es posible limitar considerablemente el alcance del ataque y reducir la propagación dentro de la infraestructura tecnológica. Según NIST (2020), Zero Trust mejora la protección de recursos críticos mediante controles de autenticación, monitoreo continuo y segmentación de acceso.

Relacionado con esto, otro principio importante es el least privilege o privilegio mínimo. Este concepto consiste en otorgar a usuarios y sistemas únicamente los permisos estrictamente necesarios para realizar sus funciones. De esta manera, si una cuenta es comprometida, el impacto del ataque será mucho menor debido a las limitaciones de acceso existentes. Muchas organizaciones presentan riesgos elevados porque los usuarios poseen permisos administrativos innecesarios o accesos excesivos sobre recursos críticos.

La segmentación de red también representa un componente clave dentro de las estrategias defensivas modernas. Consiste en dividir la infraestructura en diferentes segmentos o zonas de seguridad para limitar la comunicación directa entre sistemas. Esto ayuda a evitar movimientos laterales y dificulta que un atacante pueda expandirse rápidamente dentro de la red después de comprometer un dispositivo. Durante el laboratorio realizado, se pudo evidenciar cómo una mala segmentación podría facilitar la propagación del exploit EternalBlue hacia otros equipos vulnerables dentro del entorno corporativo.

Por otra parte, la combinación entre CIS Controls, Zero Trust, MFA y gestión de parches fortalece significativamente las capacidades de los equipos Blue Team encargados de la protección y monitoreo de los sistemas. Estas estrategias permiten detectar comportamientos anómalos, reducir superficies de ataque y responder de manera más rápida frente a incidentes de seguridad. Además, ayudan a establecer políticas más sólidas relacionadas con accesos, monitoreo y protección de información sensible.

Finalmente, la implementación de buenas prácticas de seguridad ya no debe verse como una opción adicional dentro de las organizaciones, sino como una necesidad fundamental frente al crecimiento de amenazas informáticas actuales. La correcta aplicación de controles de seguridad, autenticación robusta, segmentación y monitoreo continuo permite reducir considerablemente los riesgos asociados a vulnerabilidades críticas y fortalecer la resiliencia de las infraestructuras tecnológicas frente a posibles ataques.

Funciones y características SIEM

Un SIEM es una herramienta utilizada para recopilar y analizar información de seguridad proveniente de diferentes dispositivos y sistemas conectados a la red, como servidores, firewalls, antivirus y computadores. Su función principal es ayudar a detectar actividades sospechosas o posibles ataques desde un solo lugar, facilitando el trabajo de los equipos de seguridad.

Una de las ventajas más importantes de estas plataformas es que permiten centralizar los logs y eventos generados por diferentes dispositivos. Gracias a esto, es más fácil identificar comportamientos extraños o relacionar eventos que podrían indicar un ataque informático. Por ejemplo, el sistema puede detectar múltiples intentos fallidos de inicio de sesión o conexiones sospechosas dentro de la red y generar alertas automáticamente.

Además, un SIEM ayuda a monitorear lo que sucede en tiempo real y permite responder más rápido frente a incidentes de seguridad. En el caso del laboratorio realizado, esta herramienta habría servido para identificar conexiones sospechosas sobre el puerto 445 y actividades relacionadas con EternalBlue antes de que el ataque afectara otros equipos.

Otra característica importante es el monitoreo en tiempo real, ya que permite detectar amenazas mientras están ocurriendo y actuar rápidamente para evitar mayores daños. También puede automatizar algunas acciones de respuesta, como bloquear direcciones IP sospechosas,

aislar equipos comprometidos o generar alertas para el equipo de seguridad. En el caso del escenario trabajado, un SIEM habría ayudado a detectar actividades relacionadas con el exploit EternalBlue, como conexiones sospechosas por el puerto 445, procesos extraños ejecutándose en el sistema y posibles movimientos laterales dentro de la red.

Asimismo, los SIEM ofrecen capacidades de auditoría y análisis forense, ya que almacenan históricos de eventos que pueden utilizarse como evidencia digital en investigaciones posteriores o para cumplimiento de normativas y estándares de seguridad como ISO 27001 y NIST. Entre las características más importantes de estas plataformas se destacan la centralización de eventos, correlación inteligente de logs, monitoreo continuo, generación automática de alertas, análisis de amenazas en tiempo real, integración con herramientas de respuesta a incidentes y visualización de información mediante dashboards y reportes. Según Microsoft (2024), las soluciones SIEM ayudan a reducir considerablemente los tiempos de detección y contención de incidentes gracias a la automatización y análisis avanzado de eventos de seguridad.

Automatización y respuesta inteligente ante incidentes

En la actualidad, las organizaciones enfrentan una cantidad enorme de alertas y eventos de seguridad todos los días, lo que hace cada vez más difícil que los equipos de ciberseguridad puedan revisar manualmente cada incidente. Debido a esto, muchas empresas han comenzado a implementar tecnologías de automatización e inteligencia artificial que permiten mejorar la detección de amenazas y acelerar los procesos de respuesta frente a posibles ataques. Estas herramientas no buscan reemplazar completamente a los analistas de seguridad, sino ayudarlos a reducir tiempos de análisis, priorizar incidentes importantes y responder de manera más eficiente ante situaciones críticas.

Uno de los conceptos más importantes dentro de este tema es SOAR, sigla de Security Orchestration, Automation and Response. Este tipo de plataformas permiten integrar diferentes herramientas de seguridad dentro de un mismo entorno para automatizar tareas repetitivas relacionadas con monitoreo, análisis y respuesta a incidentes. Según Palo Alto Networks (2024), las soluciones SOAR ayudan a optimizar el trabajo de los SOC al automatizar procesos como clasificación de alertas, recopilación de evidencias y ejecución de acciones de contención frente a amenazas detectadas.

Por ejemplo, en un entorno tradicional, cuando un SIEM detecta actividad sospechosa, un analista debe revisar manualmente los registros, validar la amenaza y tomar decisiones sobre cómo responder. Sin embargo, mediante automatización SOAR, muchas de estas tareas pueden ejecutarse automáticamente, reduciendo considerablemente el tiempo de respuesta. Algunas plataformas incluso pueden aislar equipos comprometidos, bloquear direcciones IP maliciosas o generar tickets de incidentes sin necesidad de intervención inmediata del analista.

Otro tema que ha tomado bastante fuerza en los últimos años es el uso de inteligencia artificial (IA) dentro de la ciberseguridad. Actualmente, muchas herramientas modernas utilizan algoritmos capaces de identificar comportamientos anómalos y detectar patrones sospechosos que podrían pasar desapercibidos para los humanos. IBM (2024) menciona que la inteligencia artificial permite analizar grandes volúmenes de datos en menor tiempo, ayudando a identificar amenazas avanzadas y mejorar la capacidad de respuesta frente a incidentes.

La IA en ciberseguridad también se utiliza para analizar comportamientos de usuarios, tráfico de red y actividad de dispositivos con el objetivo de detectar acciones inusuales que puedan indicar un ataque. Por ejemplo, si un usuario inicia sesión desde un país diferente o accede a información fuera de su comportamiento habitual, algunos sistemas pueden generar

alertas automáticas o solicitar verificaciones adicionales. Esto ayuda a detectar accesos no autorizados y posibles compromisos de cuentas antes de que el incidente escale.

Relacionado con esto, también aparece el concepto de Machine Learning o aprendizaje automático. Aunque muchas veces se relaciona directamente con inteligencia artificial, realmente se trata de una técnica específica que permite a los sistemas aprender patrones a partir de datos históricos y mejorar sus procesos de detección con el tiempo. En ciberseguridad, el Machine Learning se utiliza para identificar malware, detectar anomalías y reconocer actividades sospechosas dentro de las redes empresariales. Según Cisco (2023), estas tecnologías ayudan a mejorar la precisión en la detección de amenazas y reducir falsos positivos dentro de los sistemas de monitoreo.

Dentro de los Centros de Operaciones de Seguridad (SOC), la automatización también juega un papel fundamental. Los SOC modernos reciben miles de alertas diariamente provenientes de firewalls, SIEM, IDS/IPS, EDR y otras herramientas de seguridad. Revisar manualmente toda esta información sería prácticamente imposible, por lo que la automatización permite filtrar eventos, priorizar amenazas críticas y agilizar procesos de investigación. Esto resulta especialmente importante frente a ataques avanzados donde cada minuto puede marcar la diferencia entre contener una amenaza o permitir que se propague dentro de la organización.

Otro aspecto importante es la correlación avanzada de eventos. Muchas herramientas actuales son capaces de relacionar información proveniente de diferentes dispositivos y sistemas para detectar patrones de ataque más complejos. Por ejemplo, una conexión sospechosa detectada por el firewall puede relacionarse con múltiples intentos fallidos de autenticación registrados en el SIEM y actividad inusual identificada por un EDR. Cuando estas alertas se analizan de manera conjunta, es mucho más fácil detectar incidentes reales y evitar que amenazas avanzadas pasen desapercibidas.

En el caso del laboratorio desarrollado durante esta práctica, se pudo evidenciar cómo herramientas defensivas como SIEM, IDS/IPS y EDR ayudan a detectar actividades relacionadas con explotación de vulnerabilidades y comportamientos sospechosos dentro de la red. Sin embargo, en entornos empresariales reales, la cantidad de eventos generados suele ser mucho mayor, razón por la cual la automatización y la inteligencia artificial se han convertido en componentes fundamentales dentro de las estrategias modernas de ciberseguridad.

A pesar de las ventajas que ofrecen estas tecnologías, también existen desafíos importantes relacionados con su implementación. Muchas soluciones requieren configuraciones adecuadas, entrenamiento constante y supervisión humana para evitar errores o falsos positivos. Además, los atacantes también han comenzado a utilizar inteligencia artificial para desarrollar amenazas más sofisticadas, automatizar ataques y evadir mecanismos tradicionales de detección. Esto demuestra que la ciberseguridad es un entorno en constante evolución donde tanto defensores como atacantes buscan aprovechar nuevas tecnologías.

Finalmente, la automatización y la respuesta inteligente ante incidentes representan una evolución importante dentro de la seguridad informática moderna. La combinación entre inteligencia artificial, Machine Learning, correlación avanzada y plataformas SOAR permite mejorar significativamente la capacidad de detección y respuesta frente a amenazas cada vez más complejas. Asimismo, fortalece el trabajo de los equipos Blue Team y contribuye a construir entornos empresariales más seguros, eficientes y preparados para enfrentar ataques modernos.

Respuesta y Contención ante Incidentes de Ciberseguridad

Cuando se detecta un ataque informático en tiempo real, lo primero que se debe hacer es revisar qué está pasando en el sistema y qué tan comprometida está la red. Para eso, es importante verificar conexiones activas, procesos sospechosos, puertos abiertos y comportamientos extraños dentro del tráfico de red. Esto ayuda a identificar si el atacante todavía tiene acceso al equipo o si continúa realizando acciones maliciosas dentro de la infraestructura. Según INCIBE (2019), una respuesta rápida ante incidentes debe enfocarse en contener el ataque y conservar evidencias para facilitar el análisis posterior.

En este caso, el ataque se realiza explotando la vulnerabilidad MS17-010 por medio del servicio SMB en el puerto 445, por lo que una de las primeras medidas sería aislar el equipo afectado de la red para evitar que el ataque se propague a otros dispositivos. Después de eso, sería necesario revisar los logs del sistema, eventos de Windows y conexiones remotas para identificar actividades sospechosas, usuarios creados sin autorización o procesos maliciosos ejecutados por el atacante.

También es importante analizar el tráfico y los registros de seguridad para encontrar indicadores de compromiso (IoC) y detectar posibles mecanismos de persistencia. Todo esto permite controlar el incidente antes de iniciar la recuperación del sistema y disminuir el impacto sobre la información y los servicios de la organización. De acuerdo con Zambrano Hernández L. F., Peña Hidalgo H. J. y Cárdenas Corral J. (2024), una buena gestión de incidentes debe incluir procesos de identificación, análisis y contención para reducir riesgos frente a ataques cibernéticos.

Herramientas de contención de ataques informáticos “hardware o software”

Las herramientas de contención son soluciones que ayudan a detener o limitar un ataque informático cuando este ya fue detectado. Su objetivo principal es evitar que la amenaza continúe propagándose dentro de la red o afecte otros equipos de la empresa. A diferencia de las herramientas de detección, que solamente identifican actividades sospechosas, las herramientas de contención permiten actuar directamente para reducir el impacto del ataque.

Estas herramientas son muy importantes dentro de los procesos de respuesta a incidentes, porque ayudan a proteger la información y mantener funcionando los servicios mientras se controla la amenaza. Algunas de las más utilizadas son los firewalls, IDS/IPS y soluciones EDR, ya que permiten bloquear conexiones sospechosas, aislar dispositivos comprometidos y detener actividades maliciosas en tiempo real.

Las organizaciones utilizan diferentes mecanismos de contención para limitar el impacto de los ataques informáticos una vez han sido detectados. Estas soluciones actúan en distintos niveles de la infraestructura tecnológica, desde el control del tráfico de red hasta la protección de los dispositivos finales. Entre las herramientas más utilizadas para este propósito se encuentran los firewalls, los sistemas IDS/IPS y las soluciones EDR, las cuales desempeñan funciones complementarias dentro de una estrategia integral de respuesta a incidentes (Cisco, 2023; Palo Alto Networks, 2024; CrowdStrike, 2024).

Firewall

Un firewall es una herramienta de seguridad encargada de controlar y filtrar el tráfico de red entrante y saliente mediante reglas previamente configuradas. Su principal función consiste en impedir conexiones no autorizadas y restringir el acceso a servicios vulnerables dentro de la infraestructura tecnológica. Los firewalls pueden implementarse tanto a nivel de hardware como

de software y constituyen una de las primeras líneas de defensa dentro de la ciberseguridad organizacional. En el escenario analizado, un firewall correctamente configurado habría permitido bloquear conexiones externas hacia el puerto 445, evitando la explotación del servicio SMB vulnerable a MS17-010. Asimismo, esta herramienta permite segmentar redes internas y limitar movimientos laterales ejecutados por un atacante después de comprometer un dispositivo. Los firewalls modernos también incorporan funcionalidades avanzadas como inspección profunda de paquetes (DPI), filtrado de aplicaciones y análisis de tráfico basado en comportamiento. Según Cisco (2023), los firewalls constituyen mecanismos esenciales para prevenir accesos no autorizados y contener amenazas dentro de entornos corporativos.

IDS/IPS (Intrusion Detection and Prevention System)

Los sistemas IDS (Intrusion Detection System) e IPS (Intrusion Prevention System) son herramientas de seguridad diseñadas para monitorear el tráfico de red y detectar actividades sospechosas o patrones relacionados con ataques informáticos. La principal diferencia entre ambos radica en que un IDS únicamente detecta eventos maliciosos y genera alertas, mientras que un IPS posee la capacidad de bloquear automáticamente el tráfico sospechoso en tiempo real. Estas herramientas son fundamentales para contener amenazas avanzadas, ya que permiten identificar intentos de explotación, malware, escaneos de red y movimientos laterales dentro de la infraestructura tecnológica. En el caso del ataque EternalBlue, un IPS habría podido detectar paquetes SMB maliciosos y bloquear la conexión antes de que el exploit lograra ejecutarse sobre el sistema Windows vulnerable.

Además, los IDS/IPS utilizan firmas de ataques conocidos y análisis de comportamiento para identificar amenazas tanto conocidas como desconocidas, generando registros detallados que facilitan procesos de análisis forense e investigación de incidentes. De acuerdo con Palo Alto

Networks (2024), los sistemas IPS son herramientas fundamentales para detener ataques en tiempo real y reducir significativamente la superficie de exposición frente a amenazas persistentes.

EDR (Endpoint Detection and Response)

Un EDR (Endpoint Detection and Response) es una solución de seguridad enfocada en la protección, monitoreo y respuesta sobre dispositivos finales como computadores, servidores y estaciones de trabajo. Su objetivo principal es detectar comportamientos anómalos, responder ante incidentes y contener amenazas directamente en los endpoints comprometidos. A diferencia de los antivirus tradicionales, los EDR poseen capacidades avanzadas de análisis de comportamiento y respuesta automatizada, permitiendo identificar actividades sospechosas incluso cuando el malware es desconocido o no posee firmas previamente registradas.

Estas herramientas permiten aislar automáticamente un equipo infectado de la red, finalizar procesos maliciosos, eliminar archivos peligrosos y recopilar evidencia digital útil para análisis forense. En el escenario trabajado, un EDR habría permitido detectar la ejecución anómala del exploit EternalBlue y aislar inmediatamente la máquina comprometida para evitar propagación hacia otros dispositivos internos. Asimismo, habría facilitado el análisis de procesos ejecutados por el atacante y la identificación de indicadores de compromiso (IoC). Según CrowdStrike (2024), las soluciones EDR fortalecen significativamente la capacidad de respuesta frente a amenazas avanzadas mediante monitoreo continuo y automatización de acciones de contención sobre dispositivos comprometidos.

Medidas de Hardening para la Mitigación de Vulnerabilidades

Teniendo en cuenta que el ataque aprovechó la vulnerabilidad MS17-010 en el servicio SMB, una de las primeras medidas de hardenización sería mantener todos los sistemas actualizados con los últimos parches de seguridad. Muchas veces los ataques ocurren porque los equipos tienen vulnerabilidades conocidas que no han sido corregidas. Según Center for Internet Security (2020), actualizar constantemente los sistemas operativos y aplicaciones ayuda a disminuir riesgos y mejorar la seguridad de la infraestructura tecnológica.

También sería importante desactivar protocolos y servicios que ya no sean necesarios o que representen un riesgo para la red. En este caso, deshabilitar SMBv1 ayudaría a evitar ataques relacionados con EternalBlue y otras vulnerabilidades similares. Además, se podrían configurar reglas de firewall para restringir el acceso al puerto 445 y permitir únicamente conexiones autorizadas dentro de la red interna.

Otra medida recomendable sería implementar segmentación de red para evitar que un atacante pueda moverse fácilmente entre diferentes equipos en caso de comprometer un dispositivo. De igual manera, sería útil utilizar herramientas de seguridad como IDS/IPS, EDR y plataformas SIEM para monitorear eventos sospechosos y detectar amenazas a tiempo. De acuerdo con Moreno P. (2015), las plataformas SIEM ayudan a centralizar y correlacionar eventos de seguridad para identificar incidentes de manera más rápida.

Finalmente, también se deberían aplicar políticas de privilegios mínimos, evitando que los usuarios tengan permisos administrativos innecesarios. Igualmente, es importante fortalecer las contraseñas y utilizar mecanismos adicionales de autenticación para reducir la posibilidad de accesos no autorizados. Todas estas medidas ayudan a disminuir la superficie de ataque y fortalecer la seguridad de la organización frente a futuros incidentes.

Acciones institucionales frente a incidentes de ciberespionaje y recuperación de la confianza

Ante la ocurrencia de un incidente de ciberespionaje cometido por una empresa contratista o proveedora de servicios de ciberseguridad (SecureNova), la respuesta institucional debe ser inmediata y proporcional a la gravedad de los hechos. Este tipo de situaciones representa una vulneración significativa de la confianza depositada por la organización y puede comprometer la confidencialidad, integridad y disponibilidad de la información (Congreso de Colombia, 2009).

Como primera medida, resulta necesario suspender o finalizar la relación contractual con la entidad involucrada mientras se desarrolla una investigación exhaustiva que permita determinar el alcance del incidente, la información comprometida y los responsables de las acciones realizadas. Paralelamente, la organización debe activar sus procedimientos de respuesta a incidentes con el fin de contener los posibles impactos y preservar las evidencias necesarias para el análisis forense correspondiente (NIST, 2020).

Asimismo, es indispensable notificar los hechos a las autoridades competentes y cumplir con las obligaciones legales y regulatorias aplicables. La denuncia oportuna contribuye a garantizar la transparencia institucional, facilita las investigaciones y permite la aplicación de las sanciones correspondientes cuando se comprueben conductas contrarias a la normativa vigente. Estas acciones fortalecen la gestión del incidente y demuestran el compromiso de la organización con la legalidad y la protección de la información (Congreso de Colombia, 2009).

Medidas para restablecer la confianza y prevenir la repetición de incidentes

La recuperación de la confianza después de un incidente de ciberespionaje requiere la adopción de medidas correctivas orientadas a fortalecer la transparencia, la supervisión y la gestión de

riesgos. En este sentido, la organización debe comunicar de manera clara las acciones implementadas para atender el incidente, así como las mejoras realizadas en sus procesos de seguridad y control interno (NIST, 2020).

De igual forma, resulta necesario reforzar los criterios de selección y evaluación de proveedores de servicios de ciberseguridad, incorporando no solo aspectos relacionados con capacidades técnicas, sino también elementos asociados al cumplimiento normativo, la ética profesional y la reputación organizacional. Este enfoque contribuye a reducir la probabilidad de establecer relaciones comerciales con entidades que representen riesgos para la seguridad de la información (COPNIA, 2015).

La realización periódica de auditorías internas y externas constituye otra medida relevante para verificar el cumplimiento de los controles implementados y detectar oportunamente posibles debilidades. Finalmente, el fortalecimiento de una cultura organizacional basada en principios éticos, responsabilidad profesional y compromiso con la seguridad de la información permite consolidar un entorno de confianza y disminuir la probabilidad de que incidentes similares vuelvan a ocurrir en el futuro (EC-Council, 2023).

La implementación de medidas correctivas y preventivas permite reducir la probabilidad de que un incidente vuelva a ocurrir y contribuye al fortalecimiento de la postura de seguridad de la organización. Sin embargo, para comprender la importancia de estas acciones, resulta necesario analizar las consecuencias que una vulnerabilidad explotada puede generar sobre los procesos, los recursos tecnológicos y la continuidad operativa de una entidad. En este sentido, los ataques dirigidos contra el protocolo SMB representan una amenaza significativa debido a su capacidad para comprometer sistemas, facilitar movimientos laterales dentro de la red y afectar la disponibilidad de los servicios. Por esta razón, a continuación, se examina el impacto

organizacional que puede producir la explotación de vulnerabilidades asociadas a este protocolo dentro de los entornos corporativos.

Impacto organizacional de un ataque SMB

Las vulnerabilidades relacionadas con el protocolo SMB representan uno de los riesgos más graves dentro de las organizaciones, especialmente cuando existen sistemas desactualizados o configuraciones inseguras dentro de la red. SMB (Server Message Block) es un protocolo utilizado principalmente para compartir archivos, impresoras y recursos entre dispositivos conectados a una red. Aunque cumple funciones importantes dentro de entornos corporativos, también ha sido uno de los principales objetivos de múltiples ataques informáticos debido a las fallas de seguridad identificadas en algunas de sus versiones, especialmente SMBv1. Según Microsoft (2017), la vulnerabilidad MS17-010 permitió la ejecución remota de código sobre sistemas Windows vulnerables, facilitando ataques masivos a nivel mundial.

Uno de los principales impactos de un ataque SMB es el daño financiero que puede generar dentro de una organización. Cuando un atacante logra comprometer sistemas críticos, las empresas pueden enfrentar pérdidas económicas relacionadas con interrupciones operativas, recuperación de infraestructura, pago de servicios de respuesta a incidentes y afectaciones sobre la productividad. Además, en algunos casos las organizaciones deben invertir grandes cantidades de dinero en recuperación de respaldos, fortalecimiento de seguridad y contratación de especialistas para contener el incidente. IBM (2024) señala que los costos promedio asociados a incidentes de ciberseguridad continúan aumentando cada año debido al crecimiento de ataques dirigidos y ransomware.

Otro aspecto importante es el impacto operativo que produce este tipo de ataques. Muchas organizaciones dependen completamente de sus sistemas tecnológicos para desarrollar procesos administrativos, financieros y operacionales. Cuando ocurre una explotación de vulnerabilidades SMB, los atacantes pueden bloquear sistemas, cifrar información o interrumpir servicios internos, afectando directamente el funcionamiento normal de la empresa. En ataques avanzados, incluso un solo equipo comprometido puede permitir movimientos laterales hacia otros dispositivos dentro de la red, aumentando considerablemente el alcance del incidente.

Un ejemplo claro de esto fue el caso de WannaCry en 2017, considerado uno de los ataques de ransomware más importantes de los últimos años. Este malware aprovechó la vulnerabilidad EternalBlue (MS17-010) para propagarse automáticamente entre equipos Windows vulnerables mediante el protocolo SMBv1. El ataque afectó hospitales, empresas, universidades y entidades gubernamentales en diferentes países, causando interrupciones masivas y pérdidas económicas millonarias. Según Europol (2017), WannaCry impactó más de 150 países y comprometió cientos de miles de dispositivos en pocas horas, demostrando el peligro que representan las vulnerabilidades sin corregir dentro de las organizaciones.

Además del impacto financiero y operativo, los ataques SMB también generan riesgos reputacionales importantes. Actualmente, las empresas manejan grandes cantidades de información relacionada con clientes, empleados y procesos internos, por lo que cualquier incidente de seguridad puede afectar seriamente la confianza de usuarios y socios comerciales. Cuando una organización sufre una filtración de información o interrupciones prolongadas de servicios, su imagen pública puede verse afectada, generando pérdida de credibilidad y disminución de confianza por parte de clientes y proveedores. En algunos casos, este daño

reputacional puede tener consecuencias más graves y duraderas que las pérdidas económicas inmediatas.

El robo de información es otro de los riesgos más comunes asociados a este tipo de ataques. Una vez que los atacantes obtienen acceso a un sistema vulnerable, pueden capturar credenciales, documentos internos, bases de datos y archivos confidenciales. Dependiendo de la información comprometida, las consecuencias pueden incluir fraudes, espionaje corporativo, filtraciones de datos personales o venta de información en mercados ilegales. MITRE (2024) menciona que muchas campañas de ataque modernas utilizan vulnerabilidades de red como SMB para facilitar movimientos laterales y ampliar el acceso dentro de las infraestructuras comprometidas.

Asimismo, las organizaciones también enfrentan riesgos legales derivados de incidentes de ciberseguridad. En muchos países existen normativas relacionadas con protección de datos personales y seguridad de la información, por lo que una empresa que no implemente controles adecuados podría recibir sanciones económicas o enfrentar procesos legales después de una filtración de información. En Colombia, por ejemplo, la Ley 1581 de 2012 establece obligaciones relacionadas con la protección de datos personales y el manejo responsable de información sensible. Esto significa que una falla de seguridad no solo afecta técnicamente a la organización, sino también desde el punto de vista legal y regulatorio.

Otro caso relevante relacionado con el impacto organizacional de ataques cibernéticos fue el incidente de Colonial Pipeline en 2021. Aunque el ataque estuvo relacionado principalmente con ransomware, el caso evidenció cómo una afectación sobre sistemas tecnológicos puede interrumpir operaciones críticas y generar consecuencias económicas y sociales significativas. El ataque obligó a detener temporalmente operaciones de distribución de combustible en Estados Unidos, demostrando el nivel de impacto que pueden alcanzar los incidentes de seguridad sobre

infraestructuras críticas. Según CISA (2021), este tipo de eventos refleja la necesidad de fortalecer continuamente las estrategias de protección y monitoreo dentro de las organizaciones.

Finalmente, los ataques relacionados con SMB y otras vulnerabilidades de red demuestran que las organizaciones deben mantener controles de seguridad actualizados y adoptar estrategias preventivas que reduzcan el riesgo de explotación. La gestión de parches, segmentación de red, monitoreo constante y eliminación de protocolos inseguros como SMBv1 son medidas fundamentales para disminuir la superficie de ataque y fortalecer la seguridad de las infraestructuras tecnológicas modernas.

Los resultados obtenidos durante el componente práctico permiten identificar la necesidad de contar con mecanismos efectivos de detección, respuesta y recuperación frente a incidentes de seguridad. En este sentido, la última fase se enfoca en las estrategias, herramientas y procedimientos utilizados por los equipos de ciberseguridad para contener amenazas, minimizar el impacto de los ataques y garantizar la continuidad de las operaciones. Además, se analizan diferentes enfoques de defensa que contribuyen al fortalecimiento de la resiliencia organizacional frente a un panorama de amenazas cada vez más complejo.

Desarrollo de un Laboratorio de Pentesting para la Evaluación de la Vulnerabilidad MS17-010 (EternalBlue)

Herramientas utilizadas

Para el desarrollo del escenario práctico de Red Team se emplearon diversas herramientas especializadas, organizadas de acuerdo con las diferentes fases del proceso de pentesting. Esta metodología permitió llevar a cabo un procedimiento estructurado para la identificación, análisis y explotación controlada de vulnerabilidades presentes en el entorno de pruebas.

Con el propósito de garantizar un ambiente seguro para la ejecución de las actividades, se configuró un laboratorio virtual mediante tecnologías de virtualización. Dicho laboratorio estuvo compuesto por una máquina atacante basada en **Parrot OS Security Edition**, utilizada para las tareas de reconocimiento, análisis y explotación, y una máquina víctima correspondiente a **Windows 7 Professional Service Pack 1 (SP1)**, seleccionada debido a la presencia de la vulnerabilidad **MS17-010 (EternalBlue)**. Asimismo, ambas máquinas fueron conectadas mediante una red compartida, lo que permitió establecer la comunicación necesaria para la realización de las pruebas y la validación de los resultados obtenidos durante el ejercicio de seguridad ofensiva.

Arquitectura del entorno virtualizado

Para el desarrollo de las pruebas de penetración y análisis de vulnerabilidades se implementó un entorno virtualizado controlado, el cual permitió ejecutar actividades ofensivas y defensivas de manera segura, evitando afectar equipos reales o redes externas. La virtualización es una tecnología ampliamente utilizada en ciberseguridad debido a que facilita la creación de laboratorios de práctica donde es posible simular ataques, detectar vulnerabilidades y evaluar mecanismos de protección sin comprometer la infraestructura física de una organización.

En este caso, el laboratorio fue configurado utilizando herramientas de virtualización como VirtualBox y VMware, plataformas que permiten crear máquinas virtuales capaces de ejecutar distintos sistemas operativos dentro de un mismo equipo físico. Gracias a estas herramientas, fue posible configurar un entorno compuesto por una máquina atacante basada en Parrot OS y una máquina víctima con Windows 7 vulnerable al exploit EternalBlue (MS17-010). Este tipo de entornos resulta fundamental en procesos de aprendizaje y pruebas de seguridad, ya que ofrecen flexibilidad, aislamiento y facilidad de restauración ante posibles fallos durante las pruebas.

Dentro de la arquitectura implementada, la máquina Parrot OS fue utilizada como sistema atacante debido a que incorpora múltiples herramientas orientadas al pentesting, análisis forense y auditorías de seguridad. Entre las herramientas utilizadas se encuentran Nmap para reconocimiento de red y Metasploit Framework para la explotación de vulnerabilidades. Por otra parte, Windows 7 fue seleccionado como máquina víctima debido a que presenta vulnerabilidades conocidas en el protocolo SMBv1, lo que permitió desarrollar las pruebas relacionadas con EternalBlue en un entorno controlado.

La comunicación entre ambas máquinas virtuales se realizó mediante una configuración de red Host-Only. Este tipo de red permite que las máquinas virtuales se comuniquen entre sí y con el equipo anfitrión, pero sin acceso directo a Internet o a redes externas. Gracias a esto, se logró mantener el laboratorio completamente aislado, reduciendo riesgos de propagación accidental del exploit o de afectar otros dispositivos fuera del entorno de pruebas. La configuración Host-Only es ampliamente utilizada en laboratorios de ciberseguridad debido a que proporciona un entorno seguro para realizar simulaciones de ataques y análisis de vulnerabilidades.

Adicionalmente, también se utilizaron configuraciones de red NAT (Network Address Translation), las cuales permiten que una máquina virtual tenga acceso a Internet a través del sistema anfitrión sin exponer directamente la dirección IP real de la máquina virtual dentro de la red externa. Este tipo de configuración resulta útil para descargar herramientas, actualizaciones o paquetes necesarios durante el desarrollo del laboratorio, manteniendo cierto nivel de aislamiento y control sobre las conexiones realizadas.

Otro aspecto importante dentro de la arquitectura virtualizada es la segmentación de red virtual. La segmentación permite separar distintos entornos o servicios dentro del laboratorio, evitando que todos los dispositivos tengan comunicación directa entre sí. En entornos empresariales reales, este principio es utilizado para limitar movimientos laterales de los atacantes y reducir el impacto de posibles incidentes de seguridad. Implementar este tipo de prácticas dentro de laboratorios académicos también ayuda a comprender cómo funcionan las estrategias de contención y protección utilizadas actualmente en organizaciones y centros de datos.

Asimismo, el uso de laboratorios aislados resulta fundamental dentro de la ciberseguridad moderna, especialmente cuando se realizan pruebas ofensivas o explotación de vulnerabilidades críticas. Ejecutar exploits o malware en redes reales podría ocasionar daños graves, pérdida de información o interrupciones de servicios. Por esta razón, los entornos virtualizados ofrecen una alternativa segura y controlada para practicar técnicas de hacking ético, desarrollar habilidades técnicas y comprender el funcionamiento de distintas amenazas informáticas sin poner en riesgo sistemas productivos.

La siguiente tabla resume los principales componentes utilizados dentro del entorno virtualizado implementado para el desarrollo de las pruebas:

Tabla 2

Componentes y funciones de la VM

Componente	Función
Parrot OS	Máquina atacante utilizada para reconocimiento y explotación
Windows 7	Máquina víctima vulnerable al exploit EternalBlue
VirtualBox/VMware	Plataforma de virtualización utilizada para crear el laboratorio
Host-Only	Comunicación interna aislada entre máquinas virtuales
NAT	Acceso controlado a Internet mediante el host
Metasploit Framework	Herramienta utilizada para la explotación de vulnerabilidades
Nmap	Herramienta utilizada para reconocimiento y escaneo de red

Nota. La tabla presenta los principales componentes implementados dentro del entorno virtualizado, así como la función que desempeñó cada uno durante el desarrollo de las pruebas de penetración y análisis de vulnerabilidades.

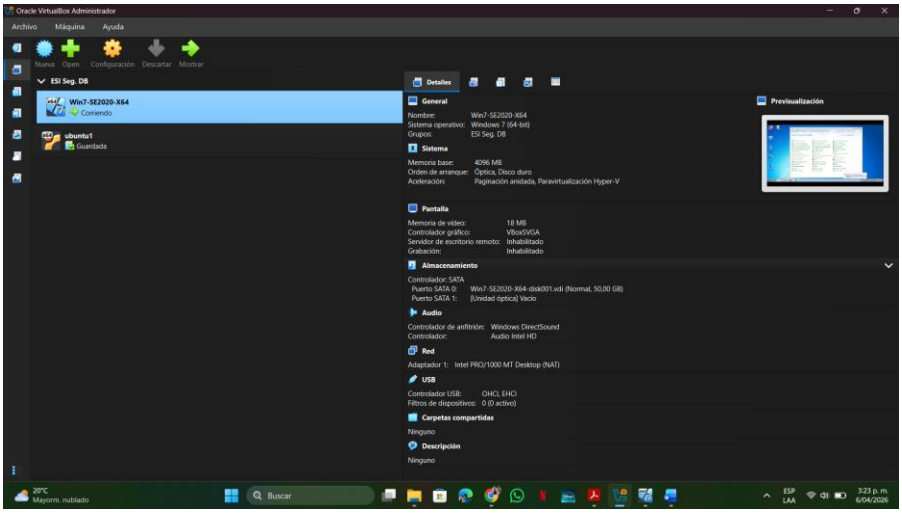
Preparación y validación del entorno de laboratorio

Como parte de la fase inicial del laboratorio, se realizó la configuración y validación del entorno virtualizado utilizado para el desarrollo de las actividades de análisis de vulnerabilidades y pruebas de penetración. Esta etapa incluyó la implementación de una máquina atacante basada en Parrot Security OS y una máquina objetivo con Windows 7 Professional SP1, así como la verificación de la conectividad entre ambos sistemas mediante una red Host-Only. Asimismo, se comprobó el correcto funcionamiento de los sistemas operativos, la disponibilidad de las

herramientas de seguridad y la configuración de los parámetros de red necesarios para garantizar un entorno controlado y seguro para la ejecución del ejercicio práctico.

Figura 1

Montaje VM Windows 7



Nota. Representación del entorno virtualizado utilizado durante el laboratorio, compuesto por una máquina atacante Parrot OS y una máquina víctima Windows 7 conectadas mediante una red Host-Only. Elaboración propia.

Una vez implementada la máquina virtual Windows 7 Professional SP1, se verificó el correcto arranque del sistema operativo y el acceso al entorno de trabajo con el fin de garantizar la disponibilidad de la plataforma objetivo para el desarrollo del laboratorio. Posteriormente, se revisaron diferentes componentes administrativos y configuraciones básicas del sistema, incluyendo parámetros de red, gestión de usuarios y mecanismos de seguridad integrados. Estas actividades permitieron validar el funcionamiento adecuado del entorno y establecer una línea base para las fases posteriores de reconocimiento, análisis de vulnerabilidades y evaluación de seguridad.

Parrot Security OS

Una vez validado el funcionamiento del sistema objetivo, se procedió a verificar la configuración y disponibilidad de la máquina virtual Parrot Security OS, la cual fue utilizada como plataforma principal para las actividades de reconocimiento, análisis de vulnerabilidades y pruebas de penetración. Esta etapa permitió confirmar que el entorno atacante contaba con las herramientas necesarias para ejecutar las diferentes fases del ejercicio práctico de ciberseguridad.

Figura 2

Configuración de la máquina virtual Parrot Security OS

Nota. Interfaz de Parrot Security OS utilizada como plataforma de trabajo para la ejecución de herramientas de reconocimiento, análisis de vulnerabilidades y pruebas de seguridad dentro del entorno virtualizado. Elaboración propia.

Una vez completada la configuración de la máquina virtual Parrot Security OS, se verificó el acceso al entorno de trabajo y la disponibilidad de los recursos necesarios para el desarrollo del laboratorio. Esta validación permitió confirmar que la plataforma atacante se encontraba preparada para ejecutar actividades de reconocimiento, análisis de vulnerabilidades y pruebas de penetración dentro de un entorno controlado.

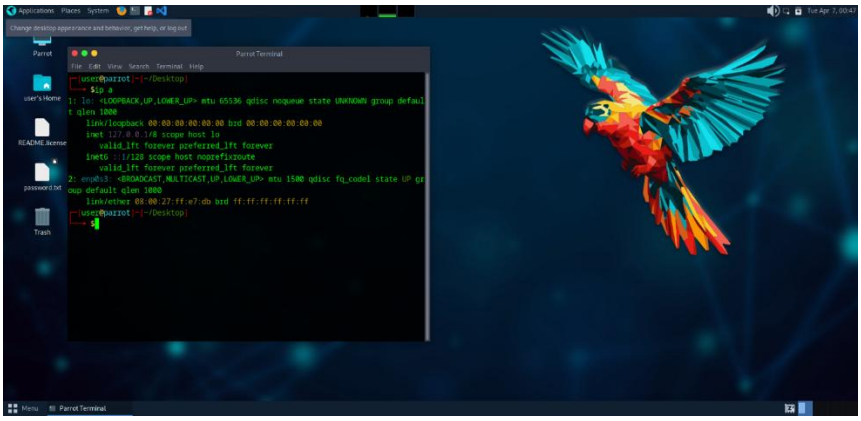
Posteriormente, se realizó una revisión de los componentes técnicos y de las herramientas integradas en el sistema operativo con el fin de identificar las capacidades disponibles para el ejercicio práctico. Este análisis permitió reconocer aplicaciones especializadas para el descubrimiento de servicios, la evaluación de vulnerabilidades y la explotación controlada de sistemas, las cuales serían utilizadas en las fases posteriores del laboratorio.

Adicionalmente, se revisó la organización básica del sistema y la ubicación de recursos relevantes para la administración del entorno de trabajo. Esta actividad facilitó la familiarización con la plataforma y permitió garantizar el acceso eficiente a las herramientas requeridas durante el desarrollo de las pruebas de seguridad.

Finalizada la validación de la máquina atacante, se procedió a revisar la configuración del entorno virtualizado implementado en VirtualBox. Para ello, se verificaron aspectos relacionados con la asignación de recursos de hardware y la configuración de red de las máquinas virtuales. Durante esta etapa fue necesario corregir inconvenientes asociados al arranque de los sistemas y a la comunicación entre los equipos, realizando ajustes que permitieron establecer una conectividad adecuada dentro del laboratorio. Una vez solucionados estos aspectos, se procedió a validar la dirección IP asignada a Parrot Security OS como paso previo a las actividades de reconocimiento y análisis de red.

Figura 3

Verificación de la dirección IP de Parrot Security OS



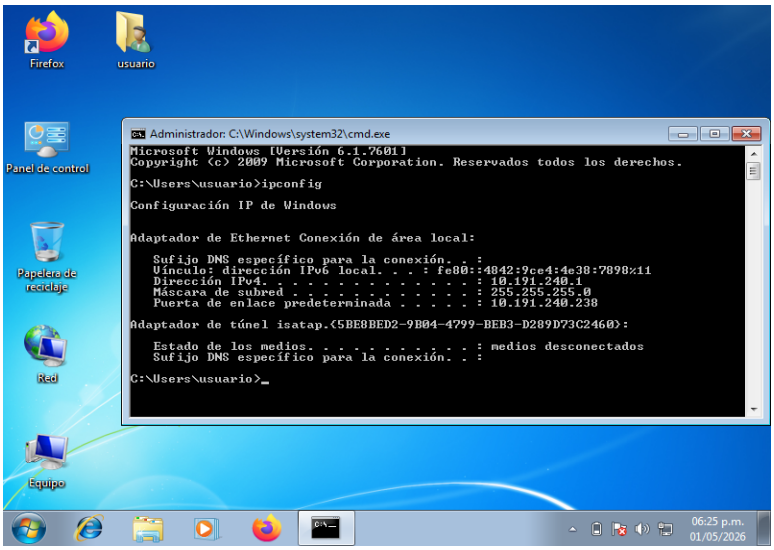
Nota. Resultado de la consulta de la configuración de red en Parrot Security OS, utilizada para verificar la dirección IP asignada y la correcta conectividad dentro del entorno virtualizado de laboratorio. Elaboración propia.

Una vez corregidos los inconvenientes iniciales de conectividad, se realizaron ajustes adicionales sobre la configuración de red de las máquinas virtuales. Para ello, se implementó el modo Adaptador Host-Only, permitiendo que ambos sistemas compartieran un mismo segmento de red y pudieran comunicarse directamente. Asimismo, se verificó el estado de los adaptadores virtuales y la correcta conexión de estos para garantizar la asignación adecuada de direcciones IP. Durante esta etapa también se identificó que la interfaz de red de Parrot Security OS se encontraba inactiva, situación que fue solucionada mediante la habilitación de la interfaz y la renovación de la configuración de red. Finalmente, se comprobó la comunicación entre las máquinas virtuales mediante pruebas de conectividad, confirmando el correcto funcionamiento del entorno de laboratorio y dejando preparada la infraestructura para las fases posteriores de reconocimiento y análisis de seguridad.

Se identificó la dirección IP de la máquina objetivo mediante el comando:

Figura 4

Verificación de la configuración IP en Windows 7

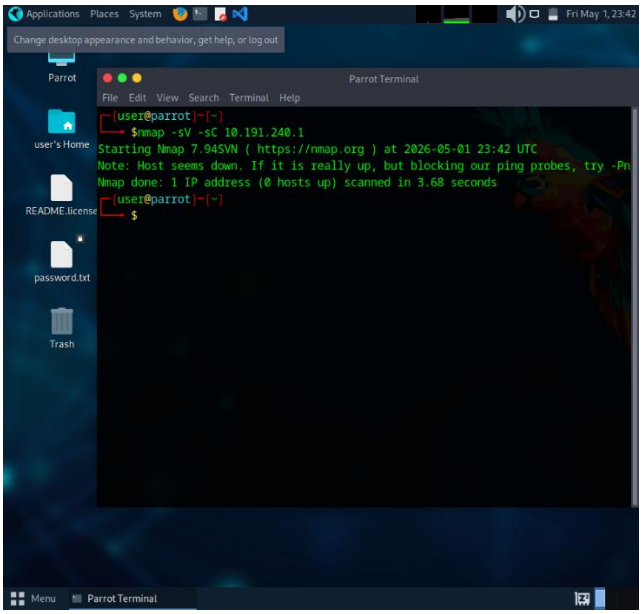


Nota. Resultado obtenido mediante el comando *ipconfig* en Windows 7 para identificar la dirección IP asignada al sistema objetivo dentro del entorno virtualizado. Elaboración propia.

Una vez identificada la dirección IP del sistema objetivo, se inició la fase de reconocimiento activo mediante el uso de herramientas de escaneo de red. Durante este proceso se ejecutaron pruebas para identificar puertos abiertos y servicios disponibles en el equipo objetivo. Inicialmente no se obtuvieron resultados debido a las restricciones impuestas por el firewall del sistema Windows, lo que impedía la detección de puertos desde la máquina atacante. Tras realizar los ajustes necesarios sobre la configuración de seguridad del sistema, fue posible repetir el procedimiento y obtener información relevante sobre los servicios expuestos en la red.

Figura 5

Escaneo de red con Nmap desde Parrot Security OS



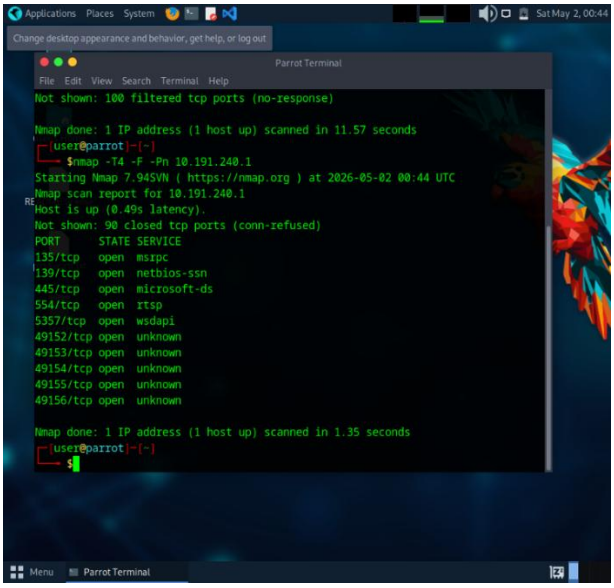
Nota. Resultado del escaneo realizado con Nmap para identificar puertos abiertos y servicios accesibles en el sistema objetivo dentro del entorno de laboratorio. Elaboración propia.

Los resultados obtenidos durante la fase de reconocimiento permitieron identificar los servicios expuestos en el sistema objetivo y determinar posibles vectores de ataque. Entre los hallazgos más relevantes se encontró el servicio SMB (Server Message Block) ejecutándose sobre el puerto 445/TCP, protocolo ampliamente utilizado en entornos Windows para compartir recursos y servicios de red. Debido a que diversas vulnerabilidades críticas han estado asociadas históricamente a este servicio, la información obtenida durante el escaneo constituyó un insumo fundamental para la fase de explotación. A partir de estos resultados se seleccionaron las herramientas y módulos necesarios para validar la existencia de vulnerabilidades y evaluar el nivel de exposición del sistema objetivo.

Se utilizó la herramienta **Metasploit Framework** para explotar la vulnerabilidad:

Figura 6

Resultados del escaneo de puertos y servicios con Nmap



Nota. Resultados obtenidos mediante Nmap que evidencian los puertos abiertos y servicios activos en el sistema objetivo, incluyendo el servicio SMB asociado al puerto 445/TCP. Elaboración propia.

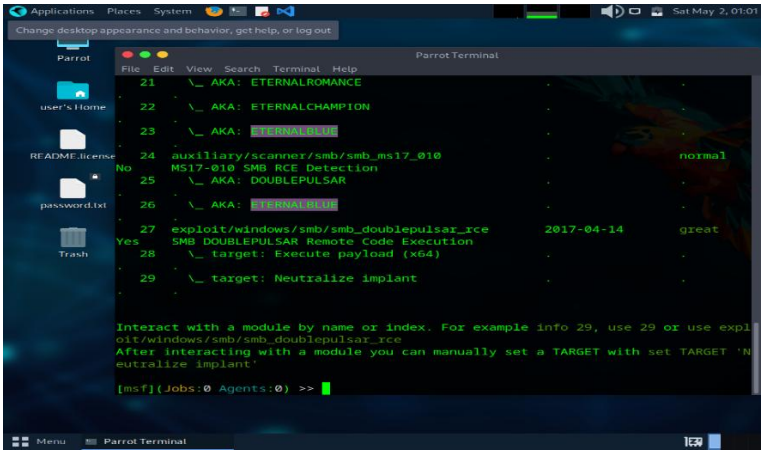
Identificación de la vulnerabilidad MS17-010 (EternalBlue)

Tras identificar la presencia del servicio SMB en el sistema objetivo, se procedió a utilizar Metasploit Framework para buscar módulos de explotación relacionados con vulnerabilidades conocidas de este protocolo. Esta actividad permitió identificar diferentes opciones disponibles dentro de la plataforma, facilitando la selección de herramientas específicas para validar la existencia de fallas de seguridad y evaluar el nivel de exposición del equipo analizado. La búsqueda de módulos constituye una etapa importante dentro del proceso de

explotación, ya que permite asociar los servicios detectados con vulnerabilidades documentadas y posibles vectores de ataque.

Figura 7

Búsqueda de exploits SMB en Metasploit Framework

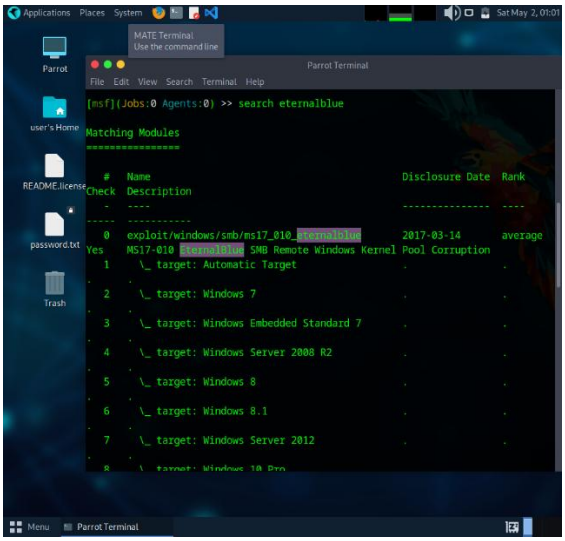


Nota. Resultado de la búsqueda de módulos de explotación relacionados con vulnerabilidades del protocolo SMB dentro de Metasploit Framework, incluyendo variantes asociadas a EternalBlue, EternalChampion y EternalRomance. Elaboración propia.

Una vez identificado el servicio SMB y seleccionados los módulos de explotación disponibles en Metasploit Framework, se procedió a configurar el exploit asociado a la vulnerabilidad MS17-010 (EternalBlue). Para ello, se establecieron los parámetros correspondientes al sistema objetivo y al equipo atacante dentro del entorno controlado de laboratorio. La ejecución del módulo permitió validar la existencia de la vulnerabilidad y demostrar el impacto que puede generar la falta de actualizaciones de seguridad en sistemas Windows. Como resultado, se obtuvo acceso al equipo objetivo mediante una sesión Meterpreter, evidenciando el compromiso exitoso del sistema dentro del escenario de pruebas autorizado.

Figura 8

Explotación Exitosa de MS17-010 (EternalBlue) mediante Metasploit

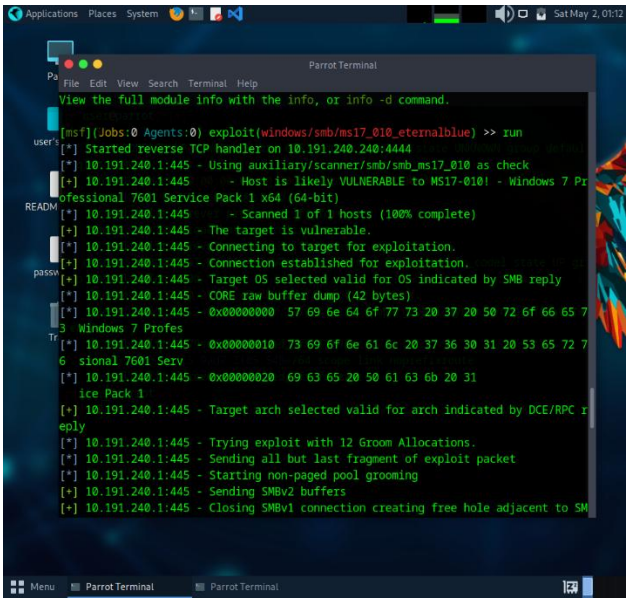


Nota. Sesión Meterpreter establecida tras la ejecución exitosa del módulo de explotación MS17-010 sobre el sistema objetivo dentro del entorno controlado de laboratorio. Elaboración propia.

Una vez configurado el módulo de explotación y verificada la accesibilidad del servicio SMB, se ejecutó el exploit EternalBlue con el objetivo de validar la vulnerabilidad MS17-010 identificada durante las fases previas de reconocimiento y enumeración. La ejecución del ataque permitió comprobar que el sistema Windows 7 SP1 carecía de las actualizaciones de seguridad necesarias para mitigar esta vulnerabilidad. Durante el proceso se estableció un canal de comunicación entre el equipo atacante y el sistema objetivo, evidenciando el impacto que puede generar la explotación de servicios expuestos y desactualizados dentro de una infraestructura tecnológica. Los resultados obtenidos confirmaron la efectividad del ataque en un entorno controlado y demostraron los riesgos asociados a la falta de gestión de parches de seguridad.

Figura 9

Ejecución del exploit EternalBlue contra Windows 7 SP1

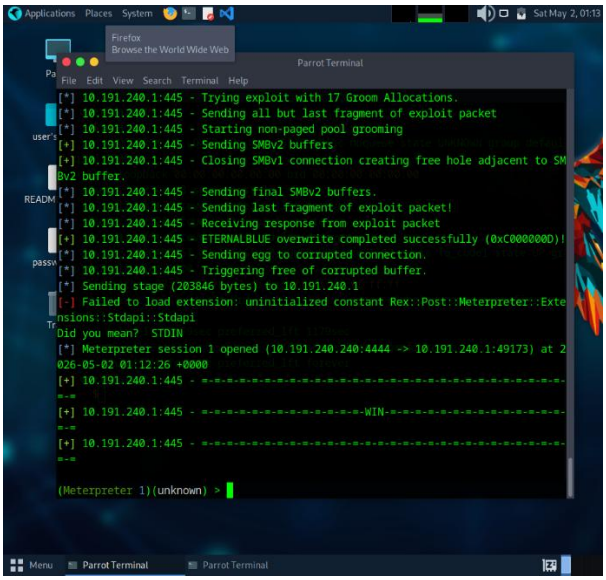


Nota. Ejecución del módulo de explotación MS17-010 (EternalBlue) mediante Metasploit Framework, confirmando la vulnerabilidad del sistema objetivo y el establecimiento de una sesión remota dentro del entorno de laboratorio. Elaboración propia.

La explotación exitosa de la vulnerabilidad MS17-010 permitió obtener acceso remoto al sistema objetivo, demostrando las consecuencias que puede generar la presencia de servicios vulnerables en una infraestructura tecnológica. Una vez establecida la sesión remota, fue posible interactuar con el equipo comprometido desde la máquina atacante, evidenciando el nivel de exposición que puede alcanzar una organización cuando no se implementan mecanismos adecuados de actualización, monitoreo y gestión de vulnerabilidades. Este resultado confirma la importancia de aplicar controles preventivos que reduzcan la superficie de ataque y mitiguen riesgos asociados a vulnerabilidades conocidas.

Figura 10

Explotación exitosa del puerto 445 en el sistema objetivo



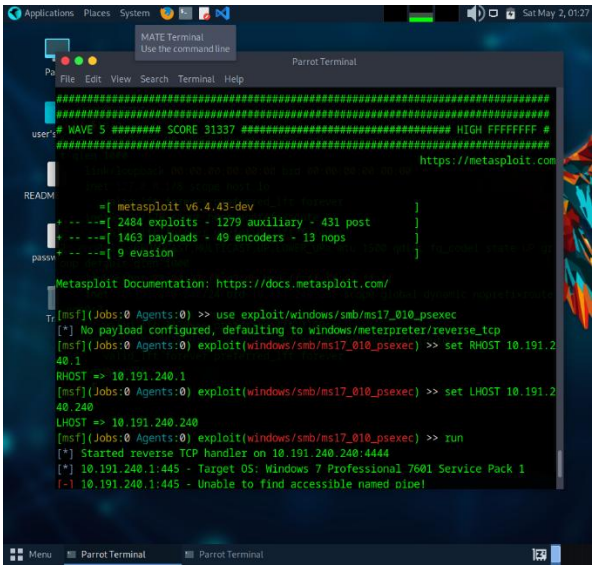
Nota. Establecimiento exitoso de una sesión remota sobre el sistema objetivo tras la explotación de la vulnerabilidad MS17-010 (EternalBlue) asociada al servicio SMB en el puerto 445/TCP. Elaboración propia.

Durante la fase de post-explotación se presentaron inconvenientes relacionados con la estabilidad de la sesión obtenida inicialmente mediante EternalBlue. Ante esta situación, fue necesario recurrir a un método alternativo de explotación que permitiera restablecer el acceso al sistema comprometido y continuar con las actividades de validación. Para ello, se utilizó un módulo adicional disponible en Metasploit Framework, aprovechando las capacidades del protocolo SMB para mantener la interacción con el sistema objetivo dentro del entorno controlado de laboratorio. Esta etapa permitió evidenciar la importancia de contar con diferentes mecanismos de acceso durante una evaluación de seguridad, especialmente cuando se presentan limitaciones técnicas o interrupciones en las sesiones activas.

Debido a inestabilidad en la sesión inicial, se empleó un segundo método:

Figura 11

Implementación del método alternativo MS17-010 psexec

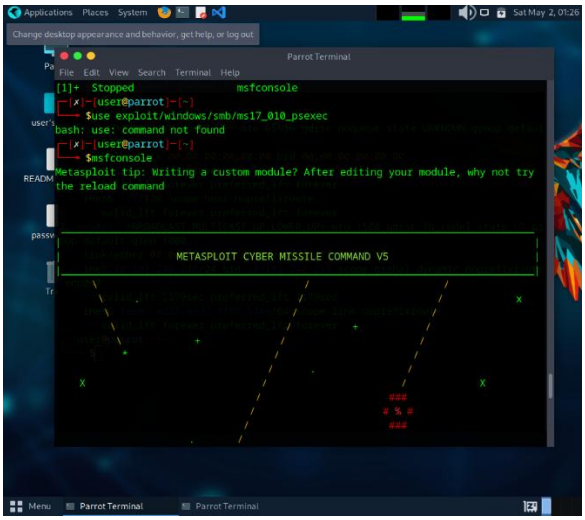


Nota. Carga y preparación de Metasploit Framework para la ejecución de un método alternativo de explotación basado en MS17-010, utilizado para restablecer el acceso al sistema objetivo tras la inestabilidad de la sesión inicial. Elaboración propia.

Con el propósito de recuperar la estabilidad del acceso al sistema comprometido, se configuró un método alternativo basado en el módulo MS17-010 psexec disponible en Metasploit Framework. Durante esta etapa se ajustaron nuevamente los parámetros de comunicación entre la máquina atacante y el sistema objetivo, validando la conectividad y los servicios necesarios para la ejecución del módulo. Aunque se presentaron algunas limitaciones durante el proceso de conexión, esta actividad permitió evidenciar los desafíos que pueden surgir durante la fase de post-explotación, especialmente cuando se busca mantener el acceso a un sistema comprometido o recuperar una sesión previamente perdida.

Figura 12

Reinicio de Metasploit Framework y configuración del módulo MS17-010 psexec

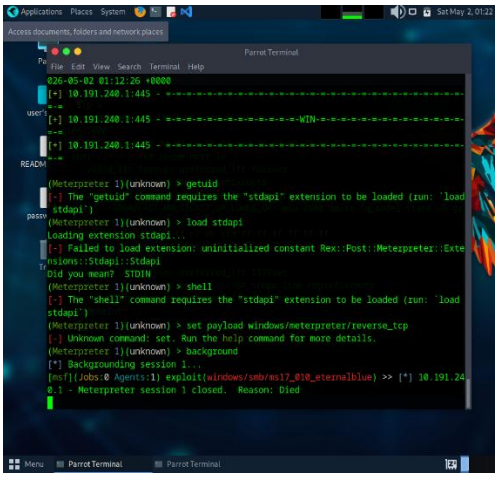


Nota. Configuración y preparación del módulo MS17-010 psexec en Metasploit Framework para restablecer el acceso al sistema objetivo durante la fase de post-explotación. Elaboración propia.

Aunque la explotación de la vulnerabilidad permitió obtener acceso al sistema objetivo, durante las actividades posteriores se identificaron problemas relacionados con la estabilidad de la sesión establecida. Este tipo de situaciones son comunes en escenarios de pruebas de penetración, especialmente cuando la explotación depende de vulnerabilidades que afectan componentes críticos del sistema operativo. Por esta razón, se realizaron diferentes verificaciones sobre el estado de la sesión y las funcionalidades disponibles dentro del entorno comprometido. Los resultados obtenidos permitieron identificar limitaciones operativas que afectaban la interacción con el sistema, evidenciando la necesidad de implementar mecanismos alternativos para mantener el acceso y continuar con el proceso de validación de seguridad.

Figura 13

Diagnóstico de Errores en la consola Meterpreter



Nota. Verificación del estado de la sesión Meterpreter tras la explotación del sistema objetivo, evidenciando errores operativos que afectaron la estabilidad y continuidad del acceso remoto obtenido. Elaboración propia.

Datos del escenario que ayudaron a identificar el fallo

Del Anexo 4 – Escenario 3 se identificaron varios elementos clave que permitieron determinar la vulnerabilidad en la máquina Windows (Host-A). En primer lugar, se menciona que existía una “aplicación vulnerable” en ejecución, lo cual indicaba la presencia de un servicio expuesto. Asimismo, se hace referencia a la obtención de acceso tipo shell y al escalamiento de privilegios, lo que sugiere una vulnerabilidad crítica que permite ejecución remota de código. Adicionalmente, la creación no autorizada de un usuario administrador indica que el atacante logró control total del sistema. Finalmente, el hecho de que se hayan presentado movimientos laterales hacia otra máquina (Host-B) confirma que la vulnerabilidad permitió comprometer la red interna. Estos elementos orientaron el análisis hacia servicios comúnmente vulnerables en Windows, como SMB, permitiendo identificar la falla MS17-010 como el punto de ataque principal.

Herramienta utilizada y puerto identificado

La herramienta utilizada para identificar los fallos de seguridad en la máquina Windows fue **Nmap**, la cual permitió realizar un escaneo de puertos y detectar los servicios activos en el sistema. Gracias a este análisis, se identificó el puerto **445/tcp**, correspondiente al servicio SMB (microsoft-ds), el cual es ampliamente conocido por presentar vulnerabilidades críticas en sistemas Windows, como la MS17-010. Posteriormente, esta información fue validada mediante el uso de Metasploit, confirmando que dicho servicio era vulnerable y podía ser explotado para obtener acceso remoto al sistema.

Análisis gráfico de las fases del ataque EternalBlue

El ataque realizado afecta a las máquinas Windows de la red aprovechando una vulnerabilidad en el servicio SMB (puerto 445), la cual permite que un atacante ejecute código de forma remota sin necesidad de autenticarse. En este caso, el atacante (Parrot OS) primero identifica que la máquina Windows tiene abierto dicho puerto y posteriormente utiliza un exploit (EternalBlue) para enviar paquetes maliciosos que aprovechan un fallo en la gestión de memoria del sistema. Como resultado, logra obtener acceso al sistema, lo que le permite ejecutar comandos, manipular archivos, crear usuarios con privilegios administrativos y tomar el control total del equipo.

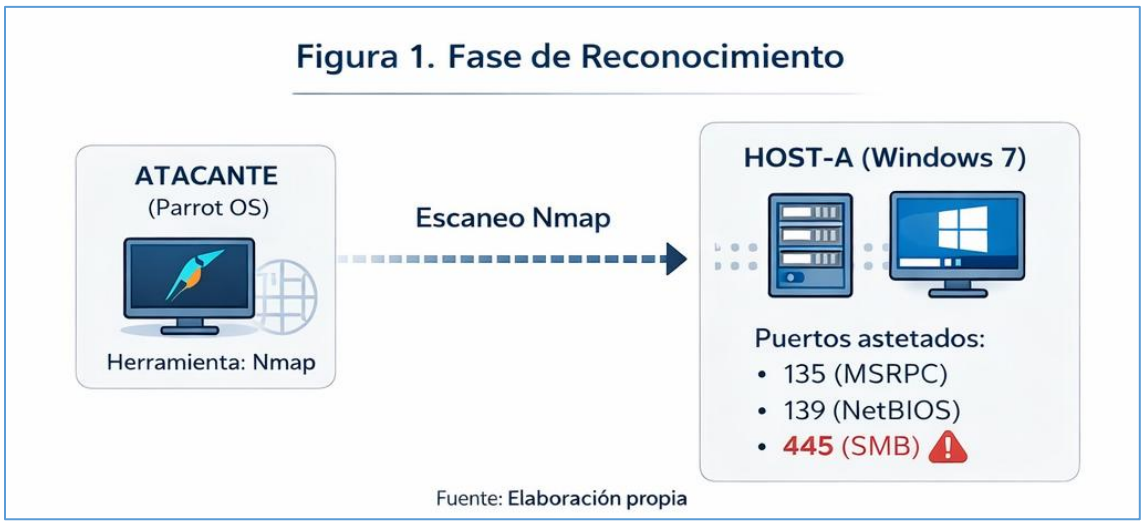
Una vez comprometida la máquina (Host-A), esta deja de ser un equipo seguro y pasa a convertirse en un punto de entrada dentro de la red. Esto significa que el atacante puede usarla como puente para explorar otros dispositivos conectados (Host-B), realizar movimientos laterales (pivoting) y acceder a información sensible almacenada en servidores o bases de datos. En términos de impacto, el ataque compromete la confidencialidad, integridad y disponibilidad de la información, ya que el atacante puede robar datos, modificarlos o incluso bloquear el sistema. Para esto se describen de forma detallada las fases desarrolladas a continuación:

Fase 1: Reconocimiento

La fase de reconocimiento constituye el punto de partida de cualquier ejercicio de seguridad ofensiva, ya que permite recopilar información relevante sobre el sistema objetivo antes de intentar explotar una vulnerabilidad. Durante esta etapa se emplean herramientas de análisis de red para identificar equipos activos, servicios expuestos, puertos abiertos y posibles vectores de ataque. La información obtenida facilita la comprensión de la superficie de exposición del sistema y sirve como base para las fases posteriores de identificación de vulnerabilidades y explotación.

Figura 14

Fase de reconocimiento del sistema objetivo



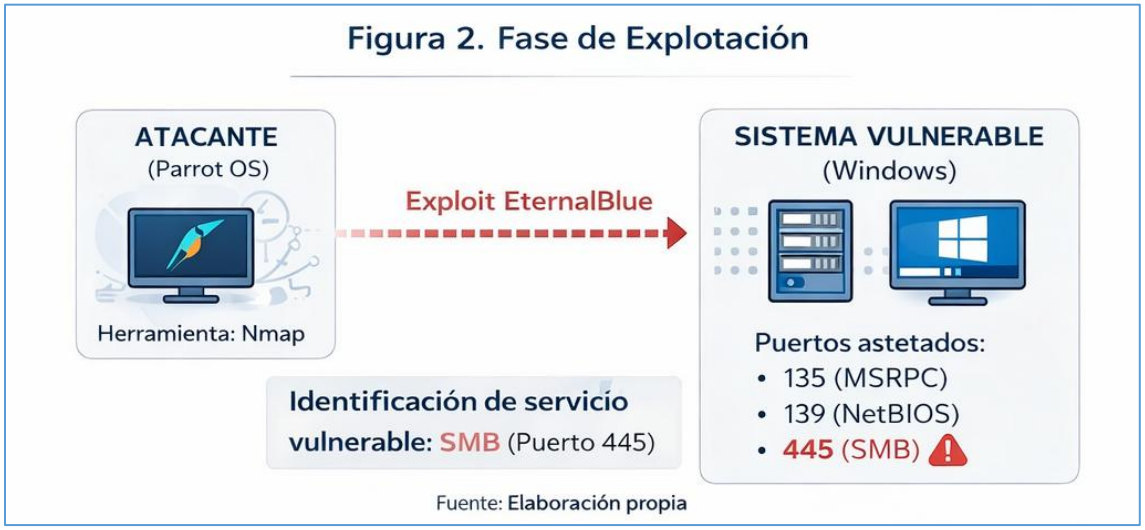
Nota. Representación del proceso de reconocimiento realizado sobre el sistema objetivo mediante herramientas de análisis de red, permitiendo identificar servicios activos, puertos abiertos y posibles vectores de ataque. Elaboración propia.

Fase 2: Explotación

Una vez identificadas las vulnerabilidades presentes en el sistema objetivo, se procede a la fase de explotación, cuyo propósito es validar el impacto real de las debilidades detectadas. Durante esta etapa se emplean herramientas especializadas que permiten aprovechar vulnerabilidades conocidas para obtener acceso no autorizado al sistema. Los resultados obtenidos permiten evaluar el nivel de riesgo al que se encuentra expuesta la infraestructura y comprender las posibles consecuencias que tendría un ataque exitoso en un entorno real.

Figura 15

Fase de explotación de la vulnerabilidad identificada



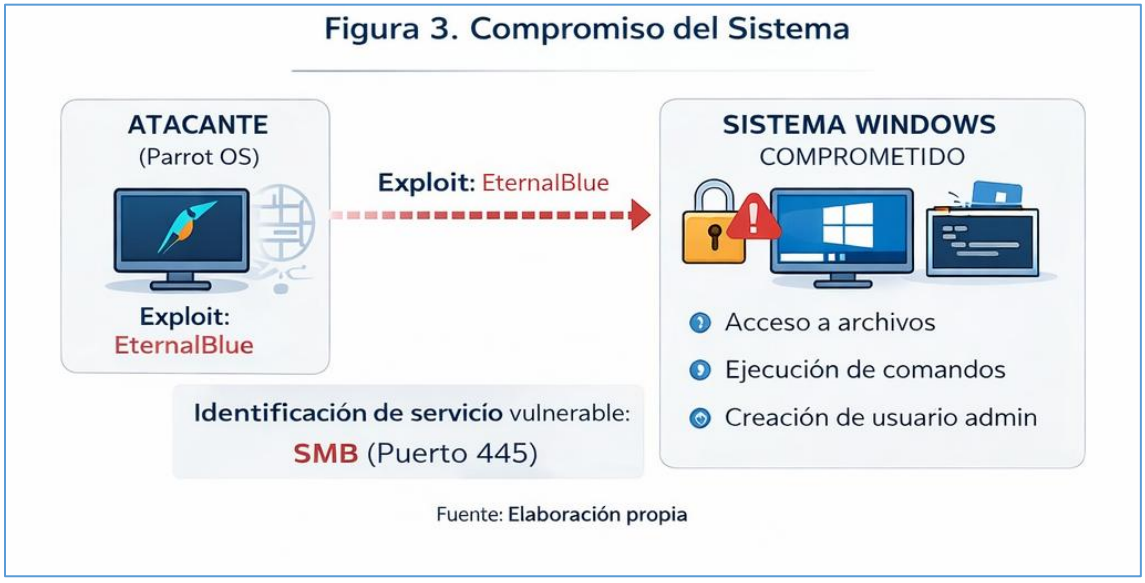
Nota. Representación del proceso de explotación realizado sobre el sistema objetivo mediante el aprovechamiento de una vulnerabilidad identificada durante la fase de reconocimiento. Elaboración propia.

Fase 3: Compromiso del sistema

Tras la explotación exitosa de la vulnerabilidad identificada, se alcanza la fase de compromiso del sistema, en la cual el atacante obtiene acceso a recursos internos y capacidades que no deberían estar disponibles para usuarios no autorizados. Esta etapa permite dimensionar el impacto real que una vulnerabilidad puede tener sobre la confidencialidad, integridad y disponibilidad de la información. Asimismo, evidencia la importancia de implementar controles de seguridad que reduzcan la probabilidad de accesos indebidos y minimicen las consecuencias de un incidente de ciberseguridad.

Figura 16

Compromiso del sistema objetivo



Nota. Representación de la fase de compromiso del sistema, en la que una vulnerabilidad explotada permite obtener acceso no autorizado a recursos y funcionalidades del equipo objetivo. Elaboración propia.

Análisis de los resultados obtenidos

Los resultados del proceso de reconocimiento evidenciaron que el sistema Windows 7 mantenía habilitado el servicio SMB a través del puerto 445/TCP. Este hallazgo resulta especialmente relevante debido a que dicho protocolo ha sido históricamente uno de los principales vectores de ataque en entornos Windows cuando no se encuentra adecuadamente actualizado o protegido. La presencia de este servicio permitió identificar la exposición a la vulnerabilidad MS17-010 (EternalBlue), una falla crítica que afecta la implementación de SMBv1 y que posibilita la ejecución remota de código sin necesidad de autenticación previa por parte del atacante.

La explotación exitosa de esta vulnerabilidad fue posible debido a la combinación de varios factores, entre ellos la utilización de un sistema operativo sin las actualizaciones de seguridad correspondientes, la disponibilidad del servicio SMB accesible desde la red y la ausencia de mecanismos adicionales de protección capaces de bloquear o detectar la ejecución del exploit. Estas condiciones generaron un escenario favorable para comprometer el sistema objetivo mediante técnicas ampliamente conocidas dentro del ámbito de la ciberseguridad ofensiva.

Como evidencia del nivel de acceso obtenido, se logró establecer una sesión remota sobre el sistema comprometido mediante Meterpreter, permitiendo la ejecución de comandos, la consulta de información del sistema y la interacción con recursos internos del equipo objetivo. Este resultado demuestra el impacto que puede generar una vulnerabilidad crítica cuando no se implementan medidas adecuadas de actualización, monitoreo y control de acceso sobre los servicios expuestos en la red.

Relación entre los hallazgos del Red Team y las medidas de mitigación

Las medidas defensivas propuestas se encuentran directamente relacionadas con las debilidades identificadas durante las actividades de Red Team. La detección del puerto 445 expuesto y la presencia de la vulnerabilidad MS17-010 evidenciaron la necesidad de implementar procesos de gestión de parches, segmentación de red y restricciones de acceso a servicios críticos. Asimismo, la obtención de acceso remoto al sistema demostró la importancia de contar con mecanismos de monitoreo continuo capaces de detectar comportamientos anómalos y responder oportunamente ante intentos de explotación.

En este contexto, herramientas como los firewalls contribuyen a limitar la exposición de servicios SMB, mientras que los sistemas IDS/IPS permiten identificar y bloquear patrones asociados a intentos de explotación. De igual manera, las soluciones EDR fortalecen la capacidad de detección y contención sobre los equipos comprometidos, reduciendo el riesgo de movimientos laterales y propagación de amenazas dentro de la infraestructura tecnológica. Estas medidas, complementadas con estrategias de hardening y modelos de seguridad como Zero Trust, permiten disminuir significativamente la superficie de ataque y fortalecer la postura de seguridad de la organización.

Discusión de resultados

Durante el desarrollo de las diferentes fases planteadas por SecureNova Labs dentro del proceso de evaluación técnica para equipos Red Team y Blue Team, fue posible analizar de manera práctica distintos escenarios relacionados con identificación de vulnerabilidades, explotación controlada, análisis defensivo y aplicación de estrategias de contención frente a amenazas informáticas. Las actividades realizadas permitieron demostrar conocimientos técnicos y metodológicos relacionados con pruebas de penetración, hardening, monitoreo y respuesta ante incidentes dentro de un entorno controlado.

Uno de los aspectos más importantes observados durante el desarrollo del laboratorio fue el nivel de criticidad que representa la vulnerabilidad EternalBlue (MS17-010) sobre sistemas Windows vulnerables. A través de las pruebas realizadas se evidenció que un sistema desactualizado y con el protocolo SMBv1 habilitado puede ser comprometido de manera relativamente rápida utilizando herramientas ampliamente conocidas dentro del ámbito ofensivo, como Nmap y Metasploit Framework. Esto permitió comprender cómo los atacantes aprovechan vulnerabilidades conocidas para obtener acceso inicial a sistemas empresariales y posteriormente expandirse dentro de la infraestructura comprometida.

Los resultados obtenidos durante la fase Red Team demostraron que la explotación de vulnerabilidades relacionadas con SMB puede facilitar la ejecución remota de código, comprometer credenciales y permitir actividades posteriores como persistencia y escalamiento de privilegios. Según Microsoft (2017), la vulnerabilidad MS17-010 fue una de las principales causas de propagación del ransomware WannaCry debido a la facilidad con la que permitía comprometer sistemas Windows sin autenticación previa. Esto confirma la importancia de

mantener políticas adecuadas de actualización y gestión de vulnerabilidades dentro de las organizaciones.

Asimismo, el laboratorio permitió evidenciar cómo una vulnerabilidad aparentemente simple puede representar un riesgo organizacional bastante alto cuando no existen controles de seguridad adecuados. Dentro de un entorno empresarial real, un atacante podría utilizar este tipo de fallos para desplazarse lateralmente, comprometer servidores críticos, acceder a información confidencial o afectar procesos operativos importantes. Esto demuestra que las organizaciones no solo deben enfocarse en mecanismos preventivos, sino también en fortalecer capacidades de monitoreo, detección y respuesta ante incidentes.

Por otra parte, durante el desarrollo de las actividades también se identificaron algunas limitaciones relacionadas con el entorno de pruebas utilizado. Aunque el laboratorio virtualizado permitió ejecutar las diferentes fases del proceso de explotación de manera segura y controlada, el escenario no representa completamente la complejidad de una infraestructura corporativa real. En ambientes empresariales modernos suelen existir mecanismos adicionales de protección como segmentación avanzada, autenticación multifactor, monitoreo SIEM, herramientas EDR y políticas Zero Trust que dificultan considerablemente la explotación de vulnerabilidades.

Sin embargo, a pesar de estas limitaciones, el escenario implementado sí resulta bastante útil desde el punto de vista académico y profesional, ya que permitió comprender las diferentes etapas involucradas dentro de un ataque controlado y analizar posteriormente las estrategias defensivas necesarias para mitigar este tipo de amenazas. Además, el laboratorio permitió fortalecer habilidades relacionadas con reconocimiento, enumeración, explotación y análisis defensivo, competencias fundamentales dentro de equipos especializados de ciberseguridad.

Otro aspecto importante observado durante el desarrollo del caso fue la relevancia de los equipos Blue Team dentro de la protección organizacional. Aunque gran parte del ejercicio estuvo orientado a las capacidades ofensivas del Red Team, también se evidenció la necesidad de implementar mecanismos de defensa capaces de detectar actividades sospechosas, reducir la superficie de ataque y responder rápidamente frente a incidentes de seguridad. Herramientas como IDS/IPS, SIEM, EDR y controles CIS permiten fortalecer significativamente la postura de seguridad de las organizaciones y mejorar la capacidad de respuesta frente a amenazas modernas.

Además, el ejercicio permitió comprender que la seguridad informática no depende únicamente del uso de herramientas tecnológicas, sino también de procesos organizacionales, monitoreo continuo y buenas prácticas de administración. Durante las pruebas realizadas se evidenció que factores como la falta de actualizaciones, configuraciones inseguras o ausencia de segmentación pueden facilitar considerablemente el trabajo de un atacante. Esto demuestra la importancia de implementar políticas de hardening, gestión de parches y control de accesos dentro de los entornos corporativos.

También se identificó que la automatización y las estrategias modernas de ciberseguridad juegan un papel cada vez más importante dentro de los procesos defensivos. Tecnologías relacionadas con inteligencia artificial, Machine Learning y automatización SOC permiten optimizar la detección y análisis de eventos sospechosos, ayudando a los equipos Blue Team a responder de manera más eficiente frente a incidentes de seguridad. Este tipo de capacidades resultan fundamentales debido al crecimiento constante de amenazas dirigidas y ataques automatizados.

Durante el desarrollo del laboratorio también surgieron algunas dificultades técnicas relacionadas con configuración de red, comunicación entre máquinas virtuales y compatibilidad de herramientas ofensivas. Aspectos como la correcta configuración de redes Host-Only, asignación

de direcciones IP y sincronización entre sistemas operativos fueron fundamentales para lograr el funcionamiento adecuado del entorno virtualizado. Aunque estas dificultades hicieron parte del proceso práctico, también permitieron fortalecer habilidades relacionadas con administración de entornos de prueba y resolución de problemas técnicos.

Finalmente, los resultados obtenidos durante las diferentes fases desarrolladas para SecureNova Labs permitieron demostrar conocimientos técnicos tanto ofensivos como defensivos relacionados con pruebas de penetración, explotación controlada, análisis de vulnerabilidades y respuesta ante incidentes. Asimismo, el ejercicio permitió comprender la importancia de integrar estrategias Red Team y Blue Team dentro de las organizaciones para fortalecer la protección de infraestructuras críticas y reducir riesgos asociados a amenazas cibernéticas modernas.

Evidencias de Sustentación

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

Video de sustentación del informe final: https://youtu.be/D9_2QKzDumg

Conclusiones

El desarrollo de la actividad permitió analizar el funcionamiento y la utilidad de diferentes herramientas empleadas en pruebas de penetración y análisis de vulnerabilidades. Herramientas como Nmap, OpenVAS y Metasploit facilitaron la identificación de servicios expuestos, la detección de vulnerabilidades conocidas y la validación práctica de riesgos de seguridad en un entorno controlado. Este proceso evidenció la importancia de combinar herramientas de reconocimiento, análisis y explotación para obtener una visión integral del nivel de exposición de un sistema informático.

A partir del reconocimiento realizado sobre el sistema objetivo, fue posible identificar el puerto 445/TCP asociado al servicio SMB (Server Message Block), el cual se encontraba expuesto y representaba un posible vector de ataque. La información obtenida mediante Nmap permitió orientar el proceso de análisis hacia vulnerabilidades históricamente relacionadas con este servicio, demostrando la importancia de la fase de reconocimiento dentro de una metodología de pentesting.

La explotación controlada de la vulnerabilidad MS17-010 (EternalBlue) mediante Metasploit Framework permitió validar el impacto real que puede generar la ausencia de actualizaciones de seguridad en sistemas Windows. Los resultados obtenidos confirmaron que el equipo Windows 7 SP1 evaluado era vulnerable a la ejecución remota de código, permitiendo el establecimiento de una sesión Meterpreter y la obtención de acceso remoto al sistema. Este hallazgo evidenció cómo una vulnerabilidad conocida puede comprometer la confidencialidad, integridad y disponibilidad de la información cuando no se aplican oportunamente los parches de seguridad correspondientes.

Asimismo, durante la fase de post-explotación se identificaron limitaciones relacionadas con la estabilidad de la sesión obtenida inicialmente, lo que hizo necesario utilizar mecanismos alternativos de acceso mediante módulos complementarios de Metasploit. Esta situación permitió comprender que los procesos de explotación y mantenimiento del acceso pueden presentar dificultades técnicas que requieren la aplicación de diferentes estrategias de validación dentro de un ejercicio de seguridad ofensiva.

Finalmente, el análisis realizado permitió proponer controles defensivos orientados a la mitigación de vulnerabilidades similares en entornos organizacionales. Entre las medidas más relevantes se destacan la gestión continua de parches de seguridad, la desactivación de protocolos obsoletos como SMBv1, la implementación de soluciones EDR y SIEM para monitoreo de eventos, la segmentación de redes y la aplicación de controles de acceso basados en el principio de mínimo privilegio. Estas acciones contribuyen significativamente a reducir la superficie de ataque y fortalecer la postura de ciberseguridad de las organizaciones.

De acuerdo con Scarfone et al. (2008), las evaluaciones de seguridad constituyen un mecanismo fundamental para identificar vulnerabilidades, validar riesgos y generar recomendaciones orientadas al fortalecimiento de los controles de protección de la información. En este sentido, los resultados obtenidos durante el laboratorio evidencian la importancia de realizar evaluaciones periódicas de seguridad como mecanismo para la identificación temprana y mitigación de amenazas en infraestructuras tecnológicas.

Recomendaciones

A partir de los resultados obtenidos durante el laboratorio, se identificó que la exposición del servicio SMB a través del puerto 445/TCP y la ausencia de actualizaciones de seguridad permitieron la explotación exitosa de la vulnerabilidad MS17-010 (EternalBlue). En consecuencia, se proponen las siguientes recomendaciones orientadas a fortalecer la postura de seguridad y reducir el riesgo de incidentes similares en entornos organizacionales.

Acciones inmediatas

Como primera medida, se recomienda implementar un proceso de gestión de parches que garantice la instalación oportuna de las actualizaciones de seguridad publicadas por los fabricantes de software. La explotación realizada durante el laboratorio demostró que la falta de actualización de Windows 7 SP1 permitió la ejecución remota de código mediante EternalBlue. La aplicación periódica de parches constituye uno de los controles más efectivos para reducir la exposición a vulnerabilidades conocidas (Microsoft, 2017).

Asimismo, se recomienda deshabilitar SMBv1 en todos los sistemas donde aún se encuentre habilitado. Diversas vulnerabilidades críticas han estado asociadas a esta versión del protocolo, incluyendo MS17-010, utilizada en ataques masivos como WannaCry. La eliminación de protocolos obsoletos reduce significativamente la superficie de ataque disponible para los actores maliciosos (CISA, 2024).

De igual manera, es necesario fortalecer las reglas de firewall para restringir el acceso al puerto 445/TCP únicamente a los equipos y servicios que realmente lo requieran. Esta medida disminuye la probabilidad de que servicios vulnerables sean identificados y explotados por atacantes externos o internos.

Acciones de mediano plazo

Se recomienda implementar soluciones de detección y respuesta en endpoints (EDR) que permitan identificar comportamientos sospechosos asociados a explotación de vulnerabilidades, movimientos laterales y ejecución no autorizada de procesos. Durante el laboratorio se evidenció que, una vez comprometido el sistema, era posible obtener acceso remoto y ejecutar acciones sobre el equipo objetivo, situación que podría ser detectada tempranamente mediante herramientas especializadas de monitoreo y respuesta.

Adicionalmente, resulta conveniente implementar mecanismos de segmentación de red para limitar la propagación de amenazas entre diferentes segmentos de la infraestructura tecnológica. Esta práctica dificulta los movimientos laterales y reduce el impacto potencial de un incidente de seguridad, especialmente cuando un atacante logra comprometer un equipo dentro de la organización (NIST, 2020).

También se recomienda realizar evaluaciones periódicas de vulnerabilidades utilizando herramientas especializadas como OpenVAS o soluciones equivalentes. Estas actividades permiten identificar debilidades antes de que sean aprovechadas por actores maliciosos y facilitan la priorización de actividades de remediación.

Acciones permanentes

Como estrategia de mejora continua, se recomienda implementar una plataforma de gestión de eventos e información de seguridad (SIEM) que permita centralizar registros, correlacionar eventos y generar alertas tempranas frente a posibles incidentes de ciberseguridad. El monitoreo continuo facilita la detección oportuna de actividades anómalas y fortalece la capacidad de respuesta de la organización.

Asimismo, se recomienda desarrollar programas permanentes de concientización y capacitación en ciberseguridad para personal técnico y administrativo. La formación continua

contribuye a fortalecer la cultura organizacional de seguridad y mejora la capacidad institucional para prevenir, identificar y responder ante amenazas emergentes.

Finalmente, se recomienda realizar ejercicios periódicos de Red Team y Blue Team con el propósito de evaluar la efectividad de los controles implementados, validar la capacidad de detección y respuesta ante incidentes, e identificar oportunidades de mejora en los procesos de seguridad. Este tipo de ejercicios permite mantener una evaluación continua del nivel de madurez de ciberseguridad de la organización y fortalecer sus capacidades defensivas frente a amenazas reales (Scarfone & Mell, 2007).

Referencias Bibliográficas

Center for Internet Security. (2024). *CIS Controls Version 8*. https://www.cisecurity.org/controls

Cisco. (2023). *What is network security?* Cisco. https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

Congreso de la República de Colombia. (2008). *Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial y de servicios y la proveniente de terceros países y se dictan otras disposiciones*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

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

CrowdStrike. (2024). *What is endpoint detection and response (EDR)?* https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr

Cybersecurity and Infrastructure Security Agency (CISA). (2021). *Reducing the significant risk of known exploited vulnerabilities*. https://www.cisa.gov

EC-Council. (2023). *Certified Ethical Hacker (CEH) program*. https://www.eccouncil.org

Europol. (2017). *Internet Organised Crime Threat Assessment (IOCTA) 2017*. https://www.europol.europa.eu

Greenbone Networks. (2024). *OpenVAS vulnerability management*. https://www.greenbone.net

IBM Security. (2024). *Artificial intelligence in cybersecurity*. IBM. https://www.ibm.com/topics/artificial-intelligence-cybersecurity

IBM Security. (2024). *Cost of a Data Breach Report 2024*. IBM. https://www.ibm.com/reports/data-breach

Kim, D., & Solomon, M. G. (2016). *Fundamentals of information systems security* (3.ª ed.). Jones & Bartlett Learning.

Microsoft. (2017). *Microsoft Security Bulletin MS17-010: Security update for Microsoft Windows SMB Server*. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010

Microsoft Security. (2023). *Microsoft Digital Defense Report 2023*. Microsoft. https://www.microsoft.com/security/business/microsoft-digital-defense-report

Ministerio de Comercio, Industria y Turismo. (2013). *Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012*. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

MITRE. (2024). *Common Vulnerabilities and Exposures (CVE).* https://www.cve.org

MITRE. (2024). *MITRE ATT&CK Framework*. https://attack.mitre.org

National Institute of Standards and Technology. (2020). *Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5)*. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Nmap Project. (2024). *Nmap Reference Guide*. https://nmap.org

Palo Alto Networks. (2024). *What is Zero Trust? Definition, principles, and strategy*. Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-zero-trust

Rapid7. (2024). *Metasploit Framework Documentation*. https://docs.rapid7.com/metasploit/

República de Colombia. (1991). *Constitución Política de Colombia*. https://www.constitucioncolombia.com

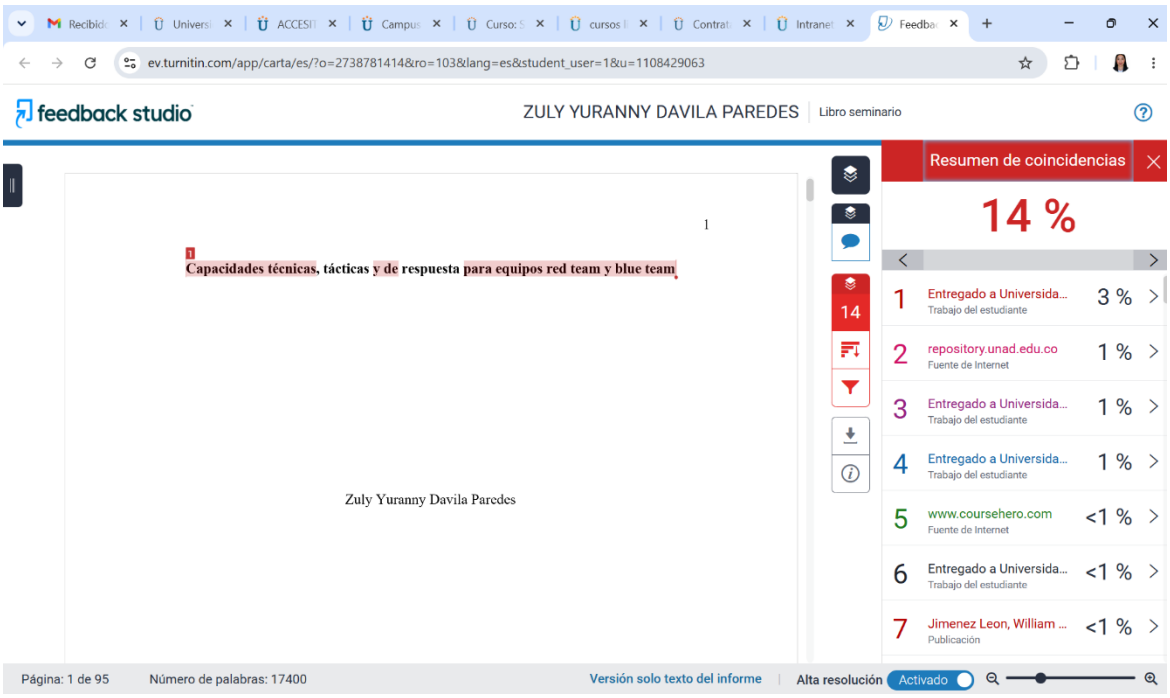
Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical Guide to Information Security Testing and Assessment (Special Publication 800-115).* National Institute of Standards and Technology. https://csrc.nist.gov/pubs/sp/800/115/final

Stallings, W. (2018). *Effective cybersecurity: A guide to using best practices and standards*. Addison-Wesley Professional. https://www.pearson.com/en-us/subject-catalog/p/effective-cybersecurity-a-guide-to-using-best-practices-and-standards/P200000003227

Apéndices

Apéndice A

Resultado de revisión en Turnitin



Nota. En esta imagen se muestran los resultados del reporte de turnitin del presente documento.