Capacidades Técnicas, Legales y de Gestión para Equipos Blue Team y Red Team

Eduar Manquillo Solarte

Asesor

Eduvin Trigos Sánchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización En Seguridad Informática

Cali

Mayo 2025

Resumen

Informe técnico y académico sobre herramientas, capacidades legales, éticas y de gestión propias de equipos blue team y red team, realizadas a partir de un caso de estudio y un entorno simulado y controlado, con el fin de explorar las diferentes aspectos y métodos que deben ser aplicados en un pentesting real, y así mismo conocer el contesto ético y legal que se debe tener en cuenta en un este proceso.

En el caso de estudio se presenta un escenario con un Windows 7 como sistema víctima y un Kali Linux como suite de herramienta de Hacking Ético, donde se ejecuta paso a paso las recomendaciones o pasos a seguir para en un pentesting, documentado resultados como el escalado de privilegios, donde a partir de la explotación de una vulnerabilidad se puede generar una Reverse Shell permitiendo el control total de la maquina victima a través de la generación de un usuario administrador , de igual manera generando recomendaciones o acciones a realizar como el Hardenig, la actualización del sistema operativo entre otras recomendaciones que permitan mitigar este tipo de ataques.

Palabras clave: Análisis, Defensa, Explotación, Monitoreo, Reconocimiento.

Abstract

This is a technical and academic report on the tools, legal, ethical, and management capabilities of blue and red teams. This report is based on a case study and a simulated and controlled environment. The report explores the different aspects and methods that must be applied in real-life pentesting, as well as the ethical and legal requirements that must be taken into account in this process.

This case study presents a scenario with Windows 7 as the victim system and Kali Linux as the Ethical Hacking tool suite. The recommendations or steps to follow for pentesting are executed step by step. The results are documented, such as privilege escalation. The exploitation of a vulnerability can generate a reverse shell, allowing full control of the victim machine through the creation of an administrator user. It also generates recommendations or actions to be taken, such as hardening and updating the operating system, among others, to mitigate these types of attacks.

Keywords: *Analysis*, Defense, Exploitation, Monitoring, Reconnaissance.

Contenido

Glosario

Análisis de Vulnerabilidades: Verificación de sistemas y redes para identificar debilidades que pueden ser explotadas por atacantes, permitiendo priorizar acciones de mitigación.

Auditoría de Seguridad: Revisión de políticas, procedimientos y controles de seguridad en una organización para identificar áreas de mejora asegurando el cumplimiento normativo.

Blue Team: Equipo de ciberseguridad que es responsable de la defensa activa de los sistemas y activos de una organización, mediante la identificación, mitigación y prevención de amenazas.

Capacidades Legales y Éticas: Normativas y principios éticos que regulan la actuación de los equipos Red y Blue Team, asegurandose que las pruebas se realicen dentro del marco legal.

Colaboración Blue Team - Red Team: Interacción entre ambos equipos para compartir hallazgos, lecciones aprendidas y recomendaciones, y así fortalecer la postura de seguridad mediante ejercicios conjuntos.

Entorno Simulado y Controlado: Laboratorio donde se recrean o simulan escenarios de ataque y defensa para pruebas de pentesting.

Escalado de Privilegios: Proceso en el que se obtiene mayores permisos dentro de un sistema tras explotar una vulnerabilidad, permitiendo acceso a recursos restringidos.

Hardening: Procesos y acciones que permiten reforzar la seguridad de sistemas y aplicaciones, minimizando la superficie de ataque y mitigando vulnerabilidades.

Pentesting (Pruebas de Penetración): Simulación controlada de ataques sobre sistemas informáticos para identificar y explotar vulnerabilidades, documentando resultados y proponiendo acciones correctivas.

Red Team: Equipo especializado en simular ataques reales para evaluar la seguridad de una organización, identificando brechas y probando la efectividad de las defensas.

Respuesta a Incidentes: Procedimientos que permiten detectar, contener, erradicar y recuperar sistemas de información ante incidentes de seguridad, asegurando la continuidad de las operaciones.

Reverse Shell: Proceso utilizado para obtener acceso remoto y control total de una máquina víctima, normalmente tras explotar una vulnerabilidad y escalar privilegios.

Lista de Tablas

Lista de Figuras

Introducción

En la actualidad el tema de la ciberseguridad ha trascendido siendo de gran interés para las organizaciones y personas, es por esta razón que, en Colombia, el marco legal sobre delitos informáticos y protección de datos personales ha evolucionado significativamente para adaptarse a los retos del entorno digital. A razón de esto, también se han establecido pruebas o procesos estructurados que permiten evaluar la seguridad de los sistemas de información, ya que son ejecutados con el fin de identificar vulnerabilidades antes de que puedan ser explotadas por ciberdelincuentes.

Sin embargo, la efectividad de estas acciones no solo depende de sus capacidades técnicas, sino también del cumplimiento de principios éticos y legales que rigen la ciberseguridad. La realización de pruebas de penetración, simulaciones de ataques y la gestión de incidentes deben llevarse a cabo bajo estrictos marcos normativos y códigos de conducta profesional, para evitar consecuencias legales, daños reputacionales y violaciones a la privacidad.

Objetivos

Objetivo General

Evaluar las acciones de los equipos Red Team & Blue Team de una organización bajo los criterios éticos y legales que apliquen, mediante un caso de estudio y un entorno simulado y controlado.

Objetivos Específicos

Determinar los riesgos legales y éticos asociados a las acciones de los equipos Red Team y Blue Team en el entorno organizacional.

Identificar vulnerabilidades en un sistema informático mediante el uso de metodologías y técnicas de pruebas de penetración.

Generar recomendaciones y estrategias que endurezcan los aspectos de seguridad informática en las organizaciones.

Desarrollo del Informe

Aspectos Legales y Proceso de un Pentesting

Ley 1273 de 2009 – Delitos Informáticos

Esta ley modificó el Código Penal Colombiano, creando un nuevo “bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. Tiene como objetivo castigar penalmente los atentados que afecten la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos (Ley 1273 de 2009 - Gestor Normativo, 2009).

Ley 1581 de 2012 – Protección de Datos Personales

Ley que protege los datos personales en Colombia. Esta reconoce el derecho fundamental al habeas data, es decir, el derecho que tienen las personas a conocer, actualizar y rectificar la información que se hayan recogido sobre ellas en bases de datos (Ley 1581 de 2012 - Gestor Normativo, 2012).

Decreto 1377 de 2013

Este decreto reglamenta parcialmente la Ley 1581 de 2012. Se centra en cómo obtener el consentimiento de los titulares de los datos recolectados antes de la entrada en vigor la ley. (Decreto 1377 de 2013 - Gestor Normativo, 2013).

Ley 1621 de 2013 – Ley de Inteligencia y Contrainteligencia

Aunque está orientada a los organismos de seguridad del Estado, también tiene implicaciones en el manejo de información personal y protección de datos (Ley 1621 de 2013 - Gestor Normativo, 2013).

Etapas del Pentesting

Las pruebas de penetración o pentesting son procesos estructurados que permiten evaluar la seguridad de sistemas, redes o aplicaciones, simulando ataques reales que podrían

ser ejecutados por ciberdelincuentes. El objetivo es identificar vulnerabilidades antes de que puedan ser explotadas por actores maliciosos.

Reconocimiento.

Esta es la fase inicial donde se recolecta toda la información posible sobre un objetivo, en esta fase se identifica direcciones IP, nombres de dominio, servidores, tecnología utilizada, mails de los usuarios, entre muchas otras opciones, esto dependiendo de los objetivos planteados.

Escaneo y Enumeración

En esta fase se realiza un escaneo activo del objetivo para descubrir los servicios, puertos abiertos, sistemas operativos y posibles puntos de entrada.

Explotación.

Es en esta fase donde se pone a prueba las vulnerabilidades encontradas, con el fin de ser explotadas y obtener acceso no autorizado, elevar privilegios o ejecutar acciones maliciosas sobre el sistema objetivo. Es aquí donde se evidencia la gravedad real de una vulnerabilidad.

Post-Explotación

En esta fase se establecen métodos que permitan mantener el acceso a los sistemas comprometidos, ejemplo de esto es la instalación de puertas traseras (backdoors) o la creación de usuarios ocultos. Esta etapa permite simular ataques persistentes avanzados.

Análisis y Reporte, También de Mitigación

En esta fase se genera un informe técnico y ejecutivo con todos los hallazgos, incluyendo las vulnerabilidades explotadas, el impacto potencial, y las recomendaciones de mitigación o las acciones de mitigación implementadas. Es aquí donde se comunica los resultados al cliente o a la organización.

Herramientas:

Las herramientas de ciberseguridad son de vital importancia, además que existe una gran cantidad de posibles herramientas y software especializado. Entre ellas se encuentran las siguientes:

Metasploit. Framework de código abierto utilizado principalmente para realizar pruebas de penetración (pentesting) y desarrollar y ejecutar exploits sobre sistemas vulnerables.(Sivamanikanta et al., 2024)

Nmap. Nmap (Network Mapper) es una herramienta de código abierto utilizada para escaneo de redes y auditoría de seguridad. (Ireneo & Colque, 2021)

OpenVas. (Open Vulnerability Assessment System) es un escáner de vulnerabilidades de código abierto que permite identificar debilidades en sistemas, redes y aplicaciones.(En & De Información, 2022)

Herramientas en línea:

ExploitDB. Base de datos pública en línea que recopila exploits conocidos y proof of concepts (pruebas de concepto) sobre vulnerabilidades en software, sistemas y aplicaciones.(Profesional Autor et al., 2021)

CVE. un sistema de identificación pública y estandarizada de vulnerabilidades de seguridad en software y hardware. Cada vulnerabilidad recibe un código único (por ejemplo, CVE-2023-12345). (Briones Ronquillo, 2024)

Actuación Ética y Legal

Procesos Ilegales y no Éticos en el Acuerdo del Anexo 3

Cláusula Primera

"La parte receptora se obliga a no divulgar ... sobre procesos ilegales dentro de CyberFort Technologies..."

Esta cláusula está impidiendo que la persona empleada denuncie actividades ilegales. Lo que desde el punto de vista legal y ético es inaceptable, ya que esto sería proteger prácticas delictivas, lo que lo hace responsable de impedir el delito en lugar de promover la transparencia, y puede ser catalogado como cómplice e incluso a tener responsabilidades penales.

Cláusula Cuarta

Punto 3 "No denunciar ante las autoridades actividades sospechosas de espionaje"

Punto 4 "Abstenerse de denunciar y publicar la información confidencial e ilegal"

Las anteriores afirmaciones están comprometiendo al firmante o contratado a encubrir posibles delitos, lo que viola en gran manera los principios fundamentales de legalidad, ética profesional y derechos ciudadanos.

Cláusula Octava

"En caso de que la información ilegal o confidencial sea encontrada en manos del receptor este deberá acudir a un abogado privado y dejar exenta de cualquier responsabilidad legal y penal a CyberFort Technologies."

Esto busca que la empresa quede exenta de toda responsabilidad ilegal o en caso de delitos ilegales, delegando completamente al trabajador, lo que lo hace inaceptable ética y moralmente, así como profesionalmente.

Artículos de la Ley 1273 que se Podrían Vulnerar

La Ley 1273 de 2009 en Colombia es la encargada de proteger la información y los datos contenidos en los sistemas informáticos. Por lo que en el anexo 3 – acuerdo Se vulnerarían especialmente los siguientes artículos:

Artículo 269A – Acceso abusivo a un sistema informático: Si el empleado tiene acceso a sistemas sin consentimiento, aunque sea en nombre de la empresa, se incurre en delito si ese acceso no tiene respaldo legal o es utilizado con fines indebidos.

Artículo 269F – Violación de datos personales: Cualquier tratamiento, acceso o revelación no autorizada de datos personales del cliente (como en el caso del ciber espionaje) vulnera este artículo.

Artículo 269H – Uso de software malicioso: Si la empresa permite la manipulación o extracción de datos mediante herramientas forenses o malware sin consentimiento, también se estaría incurriendo en delito.

¿Aplicaría al trabajo en CyberFort Technologies?

Dado el caso de estudio donde se expone un salario mensual ($150.000 COP) y un contrato vitalicio, son atractivos, pero no aplicaría para el cargo. La razón principal de que no podría aceptar este trabajo sería que dicho acuerdo tiene cláusulas ilegales y antiéticas que fuerzan a encubrir delitos y vulnerar mis valores profesionales.

Además, según el Código de Ética del COPNIA para ingenieros o profesional en ciberseguridad, se debe:

- Actuar de conformidad y con responsabilidad social.
- Denunciar cualquier actividad ilícita o contraria a los intereses públicos o privados.
- Repudiar cualquier práctica que ofenda la dignidad de la profesión.

Por lo tanto, aceptar este trabajo sería ir en contra de estos principios éticos y morales.

Análisis del caso “Ciber espionaje y Ética en CyberFort Technologies”

El caso evidencia una grave violación a la ética profesional. Aunque los empleados de CyberFort estaban autorizados para realizar auditorías, su decisión de utilizar el acceso privilegiado para recopilar y vender información sensible es totalmente inaceptable.

Interrogantes

¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes?

Las empresas pueden acceder de forma estrictamente necesaria a la información requerida para llevar a cabo su deber de auditoría; pero además con el consentimiento explícito del cliente. Debe ser temporal, supervisada y documentada.

¿Qué mecanismos de supervisión y control deberían implementarse?

- Políticas claras de acceso y uso de información.
- Obligar legalmente a proteger la información y establecer consecuencias en caso de filtración o mal uso.
- Especificar exactamente a qué datos pueden acceder, bajo qué circunstancias y durante cuánto tiempo.
- Supervisión externa durante auditorías críticas.
- Trazabilidad y bitácoras de todas las acciones técnicas.
- Código de conducta firmado por cada analista.
- Controles automatizados que alerten sobre actividades sospechosas.

¿Cómo deberían responder los gobiernos y organizaciones ante actos de ciber espionaje por parte de una empresa contratada?

Identificación y Contención

Identificación de la magnitud del espionaje: cuántos datos, cómo y por qué ocurrió y por cuanto tiempo.

Aislar los sistemas comprometidos para evitar un amplio alcance o extirpación de más información.

Investigación extensiva

Auditoría forense digital: revisión del funcionamiento de los sistemas obteniendo evidencias necesarias y entendiendo la lógica empleada.

Participación en línea con expertos en ciberseguridad y, en caso deliberativo, con agencias de inteligencia.

Notificación y transparencia

Notificar por ley a las partes afectadas (usuarios, empleados, socios comerciales) según las leyes de protecciones de datos.

Notificar la situación a autoridades competentes (policía cibernética, presencia local de espionaje, etc.).

Legalización

Demandar legalmente a la empresa contratada si se demuestra responsabilidad por mecanizado

Cancelar contratos y disciplinar conforme las cláusulas del contrato de servicio.

Pedir ayuda internacional si el ataque es multilateral.

Diplomacia

Protesta al gobierno del país en que opera la empresa.

Sanción diplomática o económica tras confirmar la complicidad del estado.

Fortalecimiento de Priorización y Comprensión

Revisar y editar esquemas empresariales de contrataciones y regulaciones sobre proveedores.

Promocionar la capacitación continua sobre ciberseguridad con empleados y el alta directivo.

Implementar mayor control en las áreas de acceso y monitoreo de sistemas crítico.

Ejecución Pruebas de Intrusión

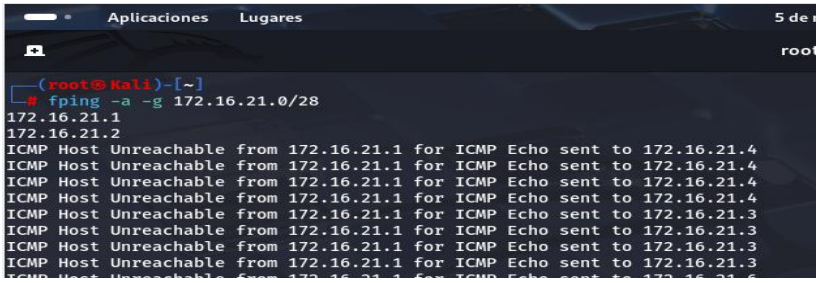
Kali Linux: Como herramienta principal y de manera general para la actividad se utiliza la distribución de Linux Kali Linux la cual está orientada al pentesting como lo expone Zapata, Kali Linux es una distribución de Linux basada en Debian destinada a pruebas avanzadas de penetración y auditoria de seguridad, contiene varios cientos de herramientas orientadas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa. (Linux & Zapata, 2022)

Fase de Reconocimiento

FPING: Herramienta de línea de comandos que permite enviar solicitudes de eco ICMP a una red para identificar host que responden a dicha solicitud.

Figura 1

Herramienta fping



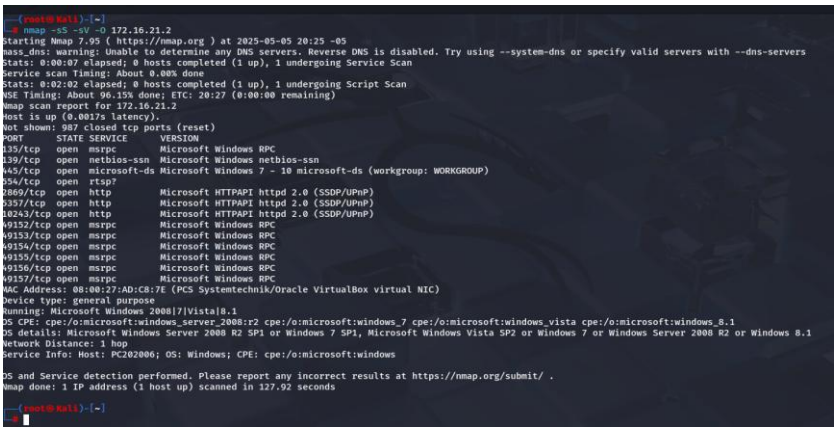
Autor: Autoría Propia

En la Figura 1 se hace uso de la herramienta fping para la identificación de host que responden a solicitudes ICMP.

NMAP: Herramienta de código abierto que es utilizada para analizar redes y realizar auditorías de seguridad.(Buenning Makenzie, 2025)

Figura 2

Herramienta nmap



Autor: Autoría Propia

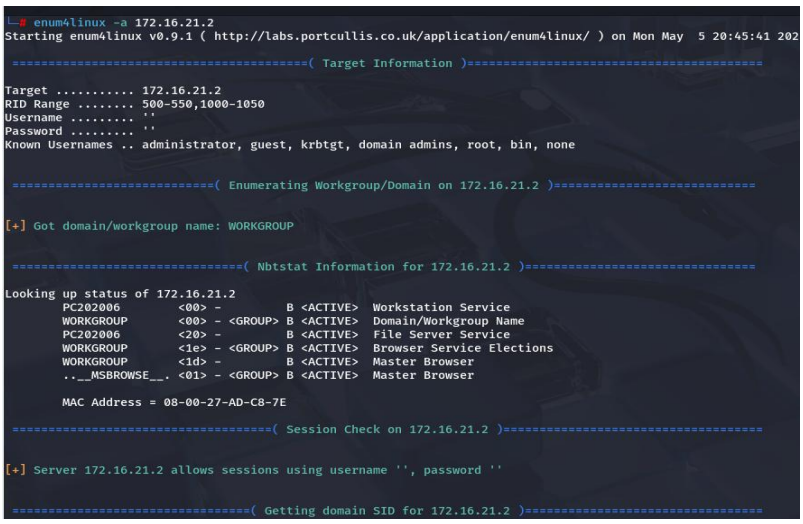
En la Figura 2 se utiliza NMAP para identificar sistema operativo y servicios que se encuentran corriendo en la maquina a reconocer.

Fase de Escaneo y Enumeración

ENUM4LINUX: Herramienta para enumerar información de sistemas Windows y Samba.

Figura 3

Herramienta enum4linux



Autor: Autoría Propia

En la Figura 3 se ejecuta enum4linux donde se validan nombres de grupos entre otros.

NMAP: Herramienta de código abierto que es utilizada para analizar redes y realizar auditorías de seguridad.(Buenning Makenzie, 2025)

Figura 4

Herramienta nmap

Autor: Autoría Propia

En la Figura 4 se ejecuta NMAP con script que permitan enumerar servicios compartidos.

NBTSCAN: herramienta de línea de comandos que busca servidores de nombres NETBIOS abiertos en una red TCP/IP local o remota, y este es un primer paso para encontrar Acciones abiertas.

Figura 5

Herramienta nbtscan

Autor: Autoría Propia

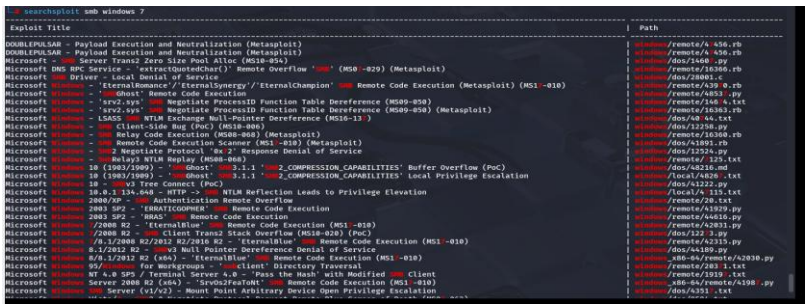
En la Figura 5 se ejecuta nbtscan pata identificar nombre y MAC asociados a la dirección IP.

Fase de Explotación

SEARCHSPLOIT: Herramienta de línea de comandos que permite buscar exploits disponibles en su base de datos.

Figura 6

Herramienta searchsploit



Autor: Autoría Propia

En la Figura 6 se ejecuta el comando searchsploit para identificar exploits disponibles para smb en Windows 7.

NMAP –script

Figura 7

Herramienta nmap --scripts

Autor: Autoría Propia

En la Figura 7, con NMAP identificamos la vulnerabilidad la cual se explotará con la herramienta metasploit.

Metasploit: Herramienta de software libre, la cual es desarrollada con el fin de realizar auditorías de seguridad, que provee de una gran cantidad de exploits que se pueden ejecutar hacia maquinas, dispositivos o servicios que presenten vulnerabilidades para las que los explots hayan sido desarrollados, además cuenta con herramientas como Shell codes que permiten generar una reverse Shell.(Vicente et al., 2022)

Figura 8

Herramienta metasploit

Autor: Autoría Propia

En la Figura de 8 se muestra el inicio de la herramienta metasploit.

Figura 9

Exploit

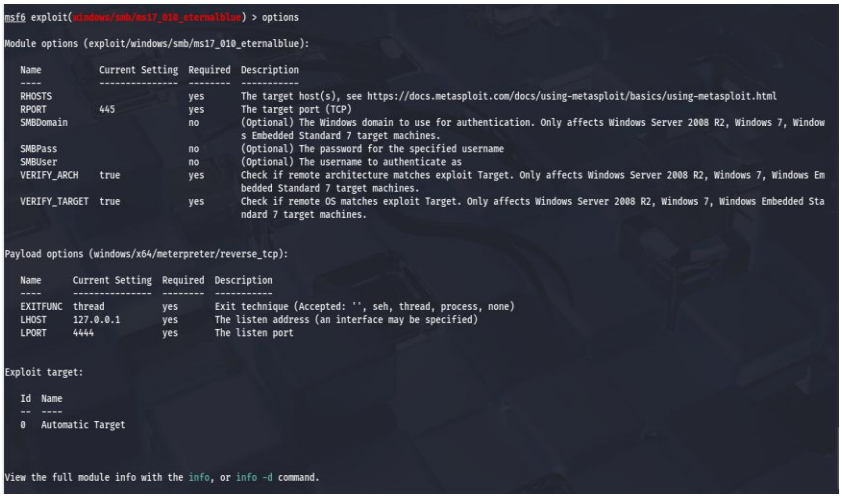
Autor: Autoría Propia

En la Figura 9 se procede a utilizar el exploit identificado en la vulnerabilidad.

El exploit EternalBlue funciona aprovechando las vulnerabilidades de SMBv1 presentes en versiones antiguas de los sistemas operativos de Microsoft.

Figura 10

Opciones de exploit



Autor: Autoría Propia

En la Figura 10 validamos las opciones con las que cuenta el exploit.

Figura 11

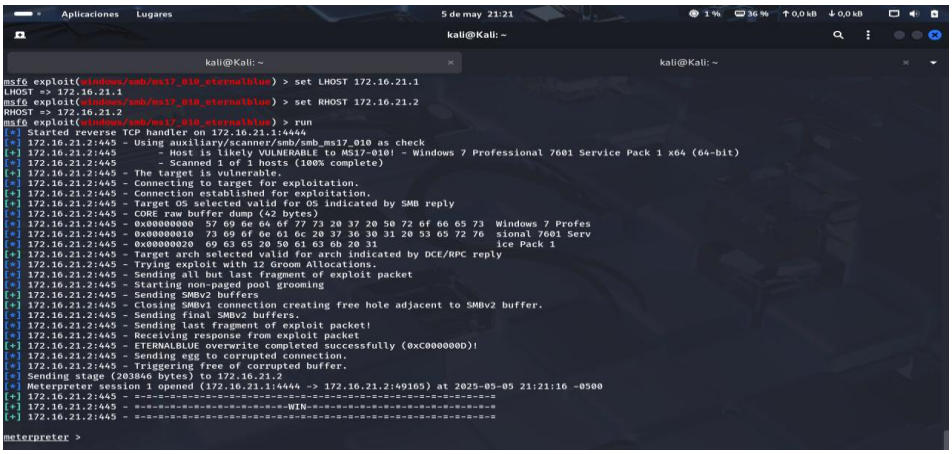
Payload

Autor: Autoría Propia

En la Figura 11 cargamos el PAYLOAD de Shell reverse y proceder a la configuración.

Figura 12

Configuración - meterpreter



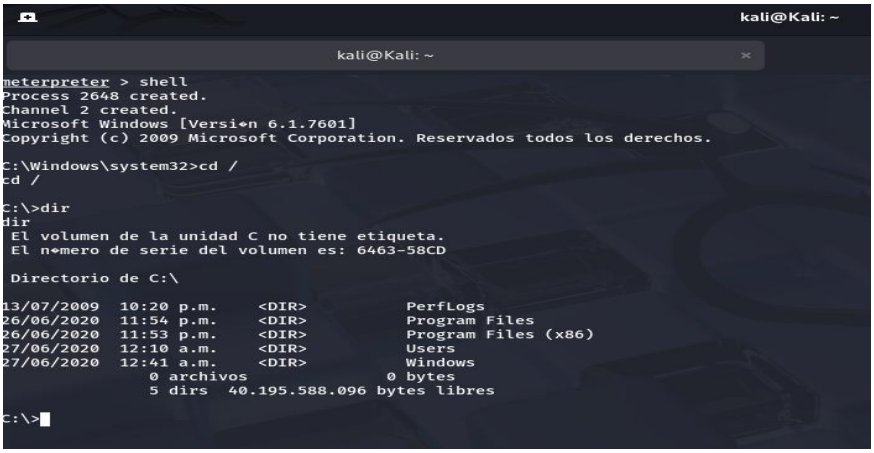
Autor: Autoría Propia

En la Figura 12 se configura el exploit y se procede a ejecutar para obtener una Shell meterpreter y posteriormente escalar privilegios.

Fase de Post- Explotación

Figura 13

Shell Windows



Autor: Autoría Propia

En la Figura 13 se evidencia la generación de la Shell que nos permitirá ejecutar tareas sobre el sistema o la maquina atacada y elevar privilegios como se muestra en las siguientes ilustraciones.

Figura 14

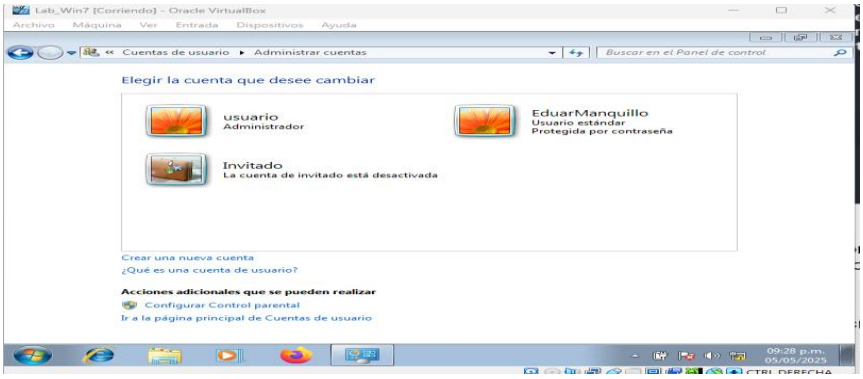
Shell Windows

Autor: Autoría Propia

Generación de un usuario con privilegios de administrador, proceso que se mostrará en las siguientes imágenes.

Figura 15

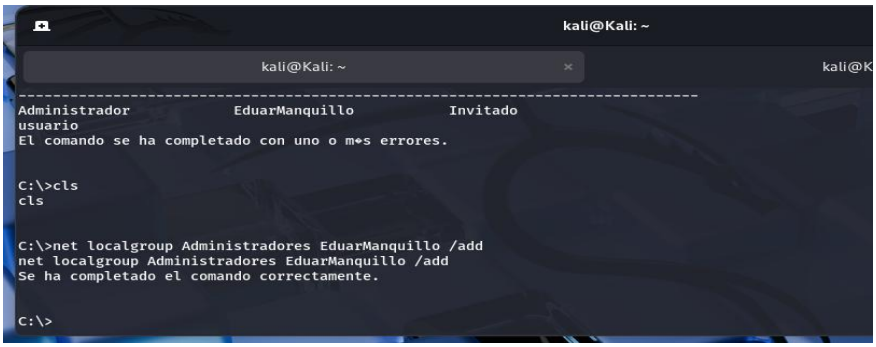
Usuarios Windows



Autor: Autoría Propia

Figura 16

Shell Windows usuario con privilegios



Autor: Autoría Propia

Figura 17

Usuarios Windows

Autor: Autoría Propia

Como se pudo observar, se logra generar un usuario con privilegios de administrador, lo que permitirá ejecutar cualquier tarea o proceso sobre la maquina víctima.

1. A continuación, liste y describa los datos e información del anexo 4 – escenario 3 que le fueron de ayuda para identificar el fallo de seguridad específico el cual ataca a la máquina Windows.

Máquina con aplicación vulnerable bajo el sistema operativo Windows. No se trata solo de vulnerabilidades del sistema operativo base, sino de una aplicación específica instalada. Por lo

tanto, el escaneo de puertos y vulnerabilidades de versiones es fundamental para encontrar esta aplicación y su vulnerabilidad.

Se confirma la existencia de posibles exploits, por lo tanto, es un muy buen punto de partida buscar activamente exploits conocidos para la aplicación y versión que se identifique. En este caso, herramientas como searchsploit o la búsqueda en Metasploit son necesarias.

El exploit puede terminar en un acceso a través de Shell, escalación de privilegios u otro tipo de ataque, por lo que indica la naturaleza del fallo a buscar: uno que permita ejecución remota de código (RCE) o acceso similar. También adelanta el siguiente paso: la escalada de privilegios.

“Investiga un escalamiento de privilegios por medio de la creación de un usuario tipo administrador": Aquí se define claramente el objetivo final de la PoC una vez se obtenga acceso inicial.

Herramientas que se utilizaron para poder identificar los fallos de seguridad de la “máquina Windows”.

Se utilizó Nmap con scripts NSE (--script vuln y smb-vuln-ms17-010) para detectar fallas de seguridad.

También se usó Metasploit con el módulo auxiliary/scanner/smb/smb_ms17_010 para confirmar la vulnerabilidad EternalBlue (MS17-010).

El puerto utilizado por la aplicación vulnerable es el 445 (SMB), ampliamente utilizado para compartir archivos en redes Windows.

2. Explique con sus palabras y de manera específica cómo afecta el ataque a la máquina (Windows), haga uso de gráficos para explicar el ataque.

Si el ataque tiene éxito, esto va a comprometer gravemente la seguridad de la máquina Windows y de la red como tal.

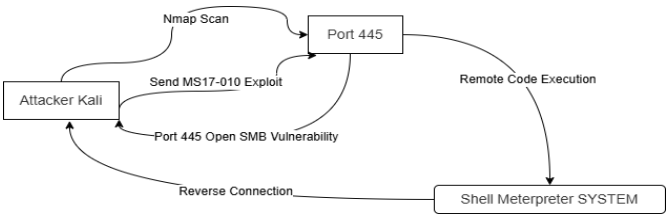
Cómo Afecta:

Acceso Inicial: El exploit de la aplicación vulnerable permite al atacante ejecutar comandos en la máquina víctima, usualmente con los privilegios del servicio de la aplicación vulnerable que pueden ser estándar, esto inicialmente.

Fuga de Información: Desde este punto de acceso, el atacante puede buscar, leer y copiar archivos sensibles.

Figura 18

Diagrama Explotación inicial



Autor: Autoría Propia

Explicación: se escanea desde Kali Linux, encontrando la aplicación vulnerable en el Puerto 445, por lo que se procede a enviar un exploit a ese puerto, este permite ejecutar código y obtiene una conexión de vuelta (Shell/Meterpreter).

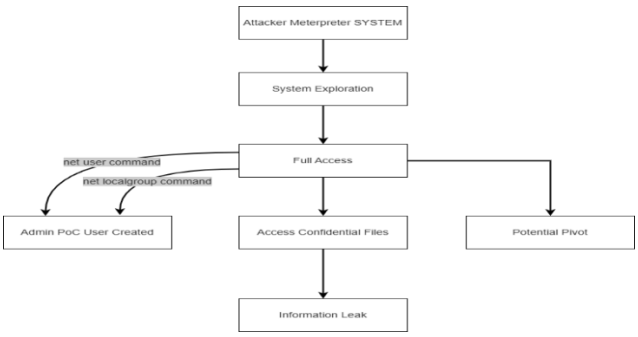
Escalada de Privilegios: Si un atacante logra escalar privilegios ya sea mediante un exploit o de configuraciones débiles para convertirse en Administrador, se obtendrá control total sobre la máquina.

Control Total: Como administrador, el atacante puede realizar todo proceso o tarea, como la instalación de software malicioso, modificar o borrar datos críticos, crear/modificar/eliminar cuentas de usuario como lo indica el PoC, desactivar software de seguridad, y hasta utilizar la máquina comprometida como punto de pivote para atacar otras máquinas en la red interna, también le permitirá establecer persistencia, asegurándose que ante reinicios las acciones realizadas continúen y continue el acceso.

Diagrama 1 Post-Explotación y Escalada de privilegios

Figura 19

Diagrama Post-Explotación y Escalada de privilegios



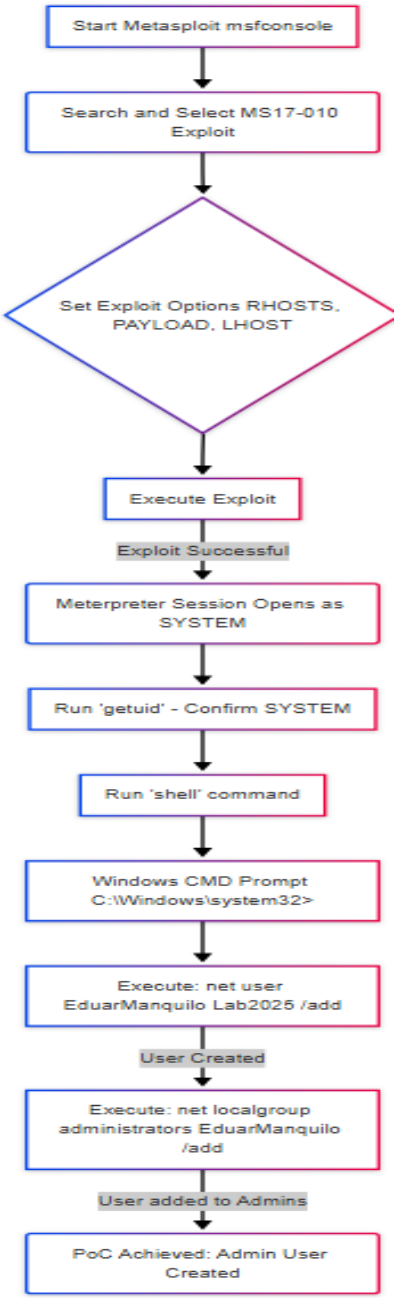
Autor: Autoría Propia

Explicación: Con acceso inicial, el atacante explora, encuentra cómo escalar privilegios, se convierte en administrador, crea el usuario PoC, y ahora tiene capacidad para robar información o atacar más sistemas.

3. Documente cada uno de los pasos que ejecutó y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7.

Tabla 1

Pasos de ejecución de la actividad.



1. Se inicia metasploit.
2. Se procede a buscar el metasploit y se selecciona. MS17-010 Exploit: módulo exploit/windows/smb/ms17_010_eternalblue.
3. Se configura el exploit: Set Exploit Options RHOSTS, PAYLOAD, LHOST, parámetros necesarios para el ataque. (IP víctima, tipo de conexión de vuelta, IP atacante).
4. Execute Exploit: Se ejecuta el exploit.
5. Meterpreter Session Opens as SYSTEM: El exploit tiene éxito, se obtiene una sesión de Meterpreter con los máximos privilegios.
6. Run 'getuid' - Confirm SYSTEM: Verificación de que se tienen privilegios de NT AUTHORITY\SYSTEM.
7. Run 'shell' command: Obtención de una consola de comandos de Windows desde Meterpreter.
8. Windows CMD Prompt C:\Windows\system32>: Acceso a la línea de comandos de la máquina víctima.
9. Execute: net user EduarManquillo Lab2025 /add: Creación del nuevo usuario.
10. Execute: net localgroup Administrador EduarManquillo /add: Adición del nuevo usuario al grupo de administradores locales.
11. PoC logrado: Usuario administrador creado: Se cumple el objetivo de la prueba de concepto.

Este diagrama resume el flujo de acciones realizadas en la actividad, evidencias realizadas en el punto 1.

Autor: Autoría Propia

Contención de Ataques Informáticos

¿Qué sería lo primero que indagaría y haría si llegara a encontrarse un ataque en tiempo real? Especifique su respuesta con argumentos técnicos.

Ante la detección de un ataque en tiempo real, procedería a realizar las siguientes acciones inmediatas y fundamentales:

Aislar el sistema afectado: La primera acción seria aislar el dispositivo o la máquina comprometida de la red para evitar la propagación del ataque y proteger otros sistemas críticos. Según Jim Holdsworth, esta contención inicial es clave para limitar daños, es una práctica recomendada por los marcos internacionales de respuesta a incidentes, como los del NIST y SANS.(Jim Holdsworth, 2024)

Verificar y analizar la alerta: Confirmar que la alerta corresponde a un incidente real y no a un falso positivo. Esto implica la revisión de los logs o registros de eventos del sistema operativo, firewall y herramientas de correlación de eventos SIEM, buscando patrones anómalos como accesos fuera de horario o procesos inusuales.(Jim Holdsworth, 2024)

Monitorear el tráfico de red: Haciendo uso de herramientas de detección y prevención de intrusiones (IDS/IPS) como Snort, que permiten analizar el tráfico en tiempo real, identificar patrones de ataque conocidos y generar alertas o bloquear tráfico malicioso automáticamente.(Janampa Patilla et al., 2021)

Analizar los procesos y servicios que se encuentren activos: Realizar revisión de los procesos que se encuentran en ejecución para identificar software malicioso o procesos no autorizados, esto ayuda a la detección del ataque.

Preservar evidencia: Documentar todas las acciones y recolectar evidencia digital para análisis forense posterior, siguiendo buenas prácticas legales y técnicas recomendadas.(Jim Holdsworth, 2024)

Notificar y escalar: Informar al equipo de respuesta a incidentes (CSIRT) y coordinar la respuesta para mitigar el impacto del ataque.(Van der Kleij et al., 2017)

Teniendo en cuenta lo anterior, son las acciones que realizaría al tener un incidente en tiempo real, son acciones respaldadas por marcos donde se enfatiza la importancia de una reacción rápida, estructurada y basada en procedimientos formales para minimizar el impacto de un incidente de seguridad

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red team, qué medidas de hardenización propondría para que el ataque no se repita?

El hardening o endurecimiento de sistemas es fundamental para reducir la superficie de ataque y prevenir futuros incidentes. Las medidas que tomaría según el ejercicio de Red team, seria las siguientes:

Actualizar y parchear de manera constante: Mantener el sistema operativo y las aplicaciones actualizadas con los últimos parches de seguridad, cierra vulnerabilidades conocidas y es una de las defensas más efectivas.(Fache Montaña, 2017)

Deshabilitar servicios y puertos innecesarios: Solo dejar activos los servicios esenciales. Desactivar RDP, SMBv1 u otros servicios no requeridos y bloquear puertos no utilizados en el firewall.(Fache Montaña, 2017)

Principio de mínimo privilegio: Limitar los permisos de usuarios y aplicaciones, eliminando cuentas innecesarias y aplicando controles de acceso estrictos, esto reduce el riesgo de escalamiento de privilegios en caso de compromiso.

Implementar autenticación multifactor (MFA): Añadir una segunda capa de autenticación, especialmente en accesos remotos y servicios críticos, esto dificulta el acceso no autorizado incluso si se comprometen las credenciales.

Segmentar la red: Dividir la red en segmentos lógicos para limitar el movimiento lateral del atacante, separando la red de usuarios de la de servidores críticos.

Auditoría y monitoreo continuo: Configurar registros detallados de acceso y actividad, y revisarlos regularmente usando un correlacionador de eventos para detectar patrones sospechosos. (González-Granadillo et al., 2021)

Aplicación de CIS Benchmarks: Seguir las recomendaciones del Center for Internet Security (CIS) para la configuración segura de sistemas y aplicaciones, lo que proporciona un marco probado y actualizado para el hardening.

Estas medidas, reduciría significativamente el riesgo de ataques exitosos y mejoraría la resiliencia de la organización.

¿Describa con sus palabras las diferencias entre un equipo Blue team y un equipo de respuesta a incidentes informáticos?

Tabla 2

Diferencias principales Blue Team vs CSIRT

Factores principales	Blue Team	CSIRT (Equipo de Respuesta a Incidentes)
Enfoque	Proactivo y defensivo: prevención, monitoreo, detección y mejora continua	Reactivo y estratégico: contención, análisis y recuperación
Momento de acción	Antes y durante el incidente	Durante y después de un incidente concreto
Rol principal	Fortalecer la seguridad, anticipar amenazas, monitorear y responder	Gestionar incidentes, contener, erradicar y restaurar
Duración del trabajo	Continuo y permanente	Temporal, basado en incidentes
Ejemplo de acciones a realizar	Configurar firewalls, SIEM, auditorías, simulacros de ataque	Contener ransomware, investigar intrusiones, recuperación

En la tabla 2 se especifica que el Blue Team se encarga de la defensa permanente y preventiva de la infraestructura, implementando medidas de seguridad, monitoreo continuo y análisis de vulnerabilidades. Por otro lado, el CSIRT actúa de manera reactiva y puntual cuando ocurre un incidente, enfocándose en contener, analizar y restaurar la normalidad, además de aprender del evento para mejorar la defensa futura. (Domínguez Álvarez & Rodríguez Sánchez, 2025)

Si dentro de un equipo Blue team le indican que debe trabajar con CIS “Center For Internet Security”, ¿usted lo utilizaría, para qué fin?

El Center for Internet Security (CIS) proporciona Benchmarks y Controles reconocidos internacionalmente para la configuración segura de sistemas, aplicaciones y redes. Un Blue Team puede utilizar el CIS para:

Implementar configuraciones seguras: Los CIS Benchmarks ofrecen guías detalladas y prescriptivas para el hardening de sistemas operativos, bases de datos, aplicaciones y dispositivos de red, reduciendo la superficie de ataque.

Alinear la seguridad con normativas internacionales: Seguir los CIS Benchmarks ayuda a cumplir con normativas como PCI DSS, NIST, ISO 27001, facilitando auditorías y cumplimiento regulatorio.

Automatizar evaluaciones y auditorías de seguridad: Herramientas como CIS-CAT permiten evaluar automáticamente el cumplimiento de los controles, generando reportes y facilitando la corrección de desviaciones.

Mejora continua: Los controles CIS se actualizan regularmente para reflejar nuevas amenazas y tecnologías, permitiendo mantener una postura de seguridad robusta y actualizada.

En resumen, el CIS es fundamental para establecer una base sólida de seguridad, priorizar recursos y mantener las mejores prácticas en la protección de la infraestructura digital. (Marchand-Niño et al., 2020)

Explique y redacte las funciones y características principales de lo que es un SIEM.

Un SIEM (Security Information and Event Management) es una plataforma centralizada que recopila, correlaciona y analiza registros de eventos de múltiples fuentes, permitiendo detectar amenazas y facilitando la respuesta a incidentes. (López Soto et al., 2024)

Entre sus funciones y características principales estarían las siguientes:

Centralización de logs: Recopila registros de sistemas, dispositivos de red, aplicaciones y herramientas de seguridad en una única plataforma, facilitando el análisis y la auditoría.

Correlación y análisis de eventos: Utiliza reglas y algoritmos (incluyendo machine learning en sistemas avanzados) para identificar patrones de ataque, anomalías y amenazas avanzadas, diferenciando entre incidentes reales y falsos positivos.

Alertas y notificaciones automatizadas: Genera alertas en tiempo real ante comportamientos sospechosos, permitiendo una respuesta rápida y coordinada.

Cumplimiento normativo: Facilita la generación de informes y documentación para cumplir con regulaciones y auditorías de seguridad (ej. GDPR, PCI DSS, HIPAA) (Farrel et al., 2024)

Soporte a la respuesta a incidentes: Proporciona información contextual y detallada sobre los incidentes, ayudando a los equipos de seguridad a tomar decisiones informadas y documentar el proceso de resolución.

Escalabilidad y flexibilidad: Puede integrarse con múltiples fuentes de datos y adaptarse a entornos locales y en la nube.

Defina por lo menos 3 herramientas de contención de ataques informáticos “hardware o software”, recuerde que las herramientas de contención son diferentes a las herramientas de detección.

Herramientas de Contención de Ataques

Las herramientas de contención permiten detener o limitar el impacto de un ataque en curso. Según lo requerido se define las siguientes herramientas:

Snort Sistema de Prevención de Intrusiones

Snort sistema que detecta y previene que intrusos ingresen a la red, libre y gratuito, que implementa un motor de detección de ataques y barrido de puertos. Permitiendo registrar, alertar y responder ante cualquier anomalía en tiempo real, combinando inspección basada en firmas y anomalías. Snort puede filtrar eventos y vulnerabilidades, alertando sobre intentos de

ataques como denegación de servicios, accesos no autorizados y escaneo de puertos. Su motor de reglas permite bloquear tráfico malicioso y aislar segmentos comprometidos. (Janampa Patilla et al., 2021)

pfSense Firewall de Código Abierto

pfSense es una solución de firewall y router de código abierto que permite implementar reglas para bloquear tráfico malicioso, segmentar la red y restringir el acceso a recursos críticos. Se utiliza para aislar segmentos comprometidos y evitar la propagación de amenazas dentro de la red, siendo especialmente útil en entornos empresariales por su flexibilidad y facilidad de integración con otras herramientas de seguridad. (Fabrizzio & Peche, 2022)

Fail2Ban

Fail2Ban monitorea los registros de servicios (como SSH, FTP, web) y bloquea automáticamente las direcciones IP que muestran patrones de ataque, como múltiples intentos fallidos de autenticación. Es ideal para proteger servicios expuestos a Internet y reducir el riesgo de ataques de fuerza bruta o escaneo de credenciales. (Álvarez Enríquez et al., 2024)

Estas herramientas, de licencia GPL, son ampliamente recomendadas siendo eficientes en sus tareas, flexibilidad y bajo costo, permitiendo a los equipos Blue Team contener amenazas de manera efectiva sin depender de soluciones propietarias.

Conclusiones

Se destacan varios puntos a lo largo de este trabajo, en el análisis de cómo proteger los datos digitales de una organización de manera ética, moral y profesional, que permitan fortalecer las capacidades defensivas, lo cual es clave en el logro de una postura de ciberseguridad sólida.

Del mismo modo, se ha confirmado que la eficacia de estas acciones no es solo un factor de los conocimientos técnicos y la capacidad de respuesta en situaciones de amenaza, sino también otros marcados por fuentes éticas y legales que se refieren a la misma actividad dentro de la ciberseguridad. Las pruebas de penetración, las simulaciones de ataque, la administración de incidentes, etc., siempre deben estar sujetas a autorizaciones formales y políticas internas ajustadas, para garantizar el respeto de la privacidad y los derechos personales de los usuarios y miembros.

Por lo tanto, es de mencionar que los procesos realizados por los equipos Red Team y Blue Team son esenciales en la protección de la información en las organizaciones, a razón de esto es necesario que la parte técnica se alineé con la parte ética y legal estableciendo canales eficaces de supervisión y control, como las auditorías periódicas, registros de las actividades en detalle, programas de formación en ética y legislación aplicable y continua, para así evitar sanciones legales o daños a la reputación.

Recomendaciones

Implementar defensa en profundidad utilizando múltiples capas de seguridad de firewalls o sistemas como IDS/IPS, segmentación de red y la actualización de los sistemas de información en cuanto a parches de seguridad, esto permitirá minimizar riesgos.(Fabrizzio & Peche, 2022)

Monitoreo y análisis continuo de logs y registros generados por los diferentes sistemas de información, se puede incluir herramientas SIEM para la recolección, correlación y análisis de los eventos de seguridad en tiempo real.(López Soto et al., 2024)

Desarrollar pruebas y planes de respuesta a incidentes, donde se incluya roles y responsabilidades para la contención y recuperación de desastres.(Jim Holdsworth, 2024)

Aprendizaje continuo a través de la lecciones aprendidas y actualizaciones de los procedimientos de seguridad de acuerdo con los diferentes hallazgos realizados.

Simular de manera real ataques con metodologías reconocidas como el MITRE ATT&CK y técnicas avanzadas que incluyan explotación de vulnerabilidades y movimiento lateral.

Informes detallados de cada proceso realizado y colaboración entre equipos y así fortalecer la postura de ciberseguridad en la organización.

Referencias Bibliográficas

Álvarez Enríquez, M., Marcial, J. P., Del Carmen, M., Díaz, S., Trinidad, G., Linares, R., Claudia, A., & Vázquez, Z. (2024). Analysis of services and applications in Linux systems with logs monitoring [Análisis de servicios y aplicaciones en sistemas Linux con monitoreo de logs]. *Revista Electrónica de la Facultad de Matemáticas*, *47(1),* 23–32. https://www.abstractionandapplication.com/index.php/ojs/article/view/21

Briones Ronquillo, R. J. (2024). Enfoque Analítico en la Clasificación de Vulnerabilidades CVE y la Identificación de Amenazas a través del Registro Malicioso en DNS. *DSpace de la Universidad Técnica de Babahoyo.* http://dspace.utb.edu.ec/handle/49000/15657

Buenning Makenzie. (2025, April 21). Cómo usar Nmap en 2023: guía completa con ejemplos. *Ninjaone*. https://www.ninjaone.com/es/blog/utilizar-nmap-guia-completa/

Ciampa, M. D. . (2022). *CompTIA Security+ : guide to network security fundamentals* (7 ed). Cengage.23-50 https://unidel.edu.ng/focelibrary/books/A%202022%20Comptia%20Security+%20Guide%20to%20Network%20Security%20Fundamentals%20by%20Mark%20Ciampa%20(z-lib.org).pdf

Diogenes, Y. Ozkaya, E. (2018). *Cybersecurity - Attack and Defense Strategies*: [Ciberseguridad - Estrategias de ataque y defensa]. https://books.google.com.co/books?hl=es&lr=&id=pyZKDwAAQBAJ&oi=fnd&pg=PP1&dq=red+team+cyber+security&ots=VtFqHTxx02&sig=c0HXUgfEUByEh2vYePWE-b8qXXg&redir_esc=y#v=onepage&q=red%20team%20cyber%20security&f=false

Domínguez Álvarez, J. L., & Rodríguez Sánchez, A. (2025). *La importancia de los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT)*. (Recursos didácticos. Grado en Seguridad, Universidad de Salamanca). Repositorio Documental CREDOS Universidad de Salamanca https://gredos.usal.es/handle/10366/165020

En, I., & De Información, S. (2022). Análisis de las vulnerabilidades de la red informática mediante la Herramienta Openvas del GAD de Vinces. *DSpace de la Universidad Técnica de Babahoyo*. http://dspace.utb.edu.ec/handle/49000/12672

Engebretson, P. (2013). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*. Elsevier Inc

Fabrizzio, B. M., & Peche, E. (2022). *Mitigación de vulnerabilidades informáticas utilizando un firewall de software libre con PFSENSE en las empresas de revisiones técnicas de la ciudad de Tacna en el año 2021*. [Tesis de ingeniero electrónico, Universidad de Privada de Tacna]. Repositorio Universidad Privada de Tacna. http://repositorio.upt.edu.pe/handle/20.500.12969/2575

Fache Montaña, J. D. (2017, April 17). *Estudio sobre la aplicación de Hardening para mejorar la seguridad informática en el Centro Técnico Laboral de Tunja – Cotel*. [Trabajo de grado de especialista, Universidad Nacional Abierta y a Distancia]. Archivo Digital Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/handle/10596/11908

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021, julio). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. [Gestión de Eventos e Información de Seguridad (SIEM): Análisis, Tendencias y Uso en Infraestructuras Críticas]. *Revista Sensors, 21(14*), 4759. https://doi.org/10.3390/S21144759

Ireneo, S., & Colque, J. (2021). NMAP Como una Herramienta para la Seguridad de Redes. *Revista Científica: Ciencia y Tecnología Informática, 2(2),* 22–25. https://rcti.informatica-unsxx.net/index.php/RCYTI/article/view/60

Ismail, Kurnia, R., Widyatama, F., Wibawa, I. M., Brata, Z. A., Ukasyah, Nelistiani, G. A., & Kim, H. (2025). Enhancing Security Operations Center: Wazuh Security Event Response with Retrieval-Augmented-Generation-Driven Copilot. [Mejora del Centro de Operaciones de

Seguridad: Respuesta a Eventos de Seguridad de Wazuh con Copiloto Impulsado por Generación Aumentada y Recuperación]. *Revista Sensors 25(3), 870*. https://doi.org/10.3390/S25030870

Janampa Patilla, H., Huamani Santiago, H. L., Meneses Conislla, Y., Janampa Patilla, H., Huamani Santiago, H. L., & Meneses Conislla, Y. (2021). Snort Open Source como detección de intrusos para la seguridad de la infraestructura de red*. Revista Cubana de Ciencias Informáticas, 15(3)*, 55–73. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992021000300055&lng=es&nrm=iso&tlng=es

Jim Holdsworth, M. K. (2024, agosto 20). *¿Qué es la respuesta a incidentes?*. IBM. Recuperado el 9 de junio de 2025. https://www.ibm.com/es-es/topics/incident-response

Kim, D., & Solomon, M. G. (2023). *Malicious Software and Attack Vectors. Fundamentals of Information Systems*. [Software malicioso y vectores de ataque. Fundamentos de los sistemas de información]. Jones & Bartlett Learning, LLC, 255–296. https://www.jblearning.com/catalog

Kim, D., & Solomon, M. G. (2023*). Fundamentals of information systems security*. [Fundamentos de la seguridad de los sistemas de información]. Jones & Bartlett Learning, LLC. https://books.google.com.co/books?hl=es&lr=&id=Yb4eDQAAQBAJ&oi=fnd&pg=PP1&dq=Kim,+D.,+%26+Solomon,+M.+G.+(2023b).+Title:+Fundamentals+of+information+systems+security&ots=CYHuv8fx5R&sig=3SIA8cuniV8O2JxdjM4eHC3uGiM#v=onepage&q&f=false

Linux, K., & Zapata, J. (2022). Kali Linux. *Revista Científica Creando Ingenios, 2(2),* 43–55. https://creandoingenios.net/index.php/revista/article/view/15/28

López Soto, J. C., Marulanda Hernández, A. F. (2024). *Implementación de un SIEM (Security Information and Event Management) para la infraestructura de la empresa Agofer S.A.S Dith Group en la sede Bogotá*. [Trabajo de grado de especialización, Universidad Piloto

de Colombia]. Repositorio Institucional Universidad Piloto de Colombia. http://repository.unipiloto.edu.co/handle/20.500.12277/13683

Marchand-Niño, W.-R., Vega Ventocilla, E. J. (2020, diciembre). Modelo Balanced Scorecard para los controles críticos de seguridad informática según el Center for Internet Security (CIS). *Revista Interfases, 13(013)*, 57–76. https://doi.org/10.26439/INTERFASES2020.N013.4876

Peltier, T. R. (2016*). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. [Políticas, procedimientos y estándares de seguridad de la información: directrices para una gestión eficaz de la seguridad de la información.]. Taylor & Francis Group, LLC. https://doi.org/10.1201/9780849390326

Núñez Alcalá, C. (2021). *Penetration testing: auditoría profesional*. [Trabajo de grado de ingeniería, Universidad Oberta de Catalunya]. Repositorio Institucional Universidad Oberta de Catalunya. https://openaccess.uoc.edu/handle/10609/132609

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008, septiembre). Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology. [Guía técnica para pruebas y evaluación de seguridad de la información Recomendaciones del Instituto Nacional de Estándares y Tecnología]. *National Institute of Standards and Technology, (800-115),*. https://doi.org/10.6028/NIST.SP.800-115

Sivamanikanta, M., Abbas, M. A. M., & Das, P. (2024). Exploring the Capabilities of the Metasploit Framework for Effective Penetration Testing. [Explorando las capacidades del marco Metasploit para pruebas de penetración efectivas]. *Lecture Notes in Networks and Systems, (791).* 457–471. https://doi.org/10.1007/978-981-99-6755-1_35

Van der Kleij, R., Kleinhuis, G., & Young, H. (2017, diciembre). Computer security incident response team effectiveness: A needs assessment. [Eficacia del equipo de respuesta a

incidentes de seguridad informática: Evaluación de necesidades]. *Frontiers in Psychology, (8)* Articulo 2179.. https://doi.org/10.3389/fpsyg.2017.02179

Acosta Santana, J. J. (2022). *Pentesting en entornos controlados*. [Trabajo de grado de ingeniería, Universidad de la Laguna]. Repositorio institucional Universidad de la Laguna. https://riull.ull.es/xmlui/handle/915/28744

Witman, M. E., & Mattord, H. J. (2022). *Principles of Information Security Seventh Edition*. [Principios de Seguridad de la Información]. Cengage Learning, Inc.

Anexos.

Enlace video de sustentación: [Sustentación.mp4]

Resultado de Turnitin