Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Carlos Eduardo Agudelo Velasco

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en seguridad informática

2025

Capacidades técnicas, legales y de gestión para equipos Blue Team y Red Team

Carlos Eduardo Agudelo Velasco

Asesor

Eduvin Trigos Sanchez

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Especialización en seguridad informática

2025

Resumen

El documento presenta la evaluación de las vulnerabilidades identificadas en la infraestructura tecnológica de la organización CyberFort Technologies, se ejecutan múltiples procesos que correspondes a las funciones que desempeñan los equipo de del Red Team, Blue Team y se mencionan aspectos legales que van relacionan con la ciberseguridad. En el análisis realiza se logran identificar y explotar algunas vulnerabilidades.

Posterior a el análisis realizado y con los resultados finales se presentan algunas estrategias que van a permitir mitigar, detectar y contener diferentes incidentes de seguridad

Palabras clave: Ciberseguridad, CIS, Contención de amenazas, Escalamiento de privilegios, Explotación, Hardening, Red Team, Seguridad de la información, SIEM, SOAR, Vulnerabilidades, WAF.

Abstract

The document presents an assessment of the vulnerabilities identified in CyberFort Technologies' technological infrastructure. Multiple processes are executed that correspond to the roles performed by the Red Team and Blue Team teams, and legal aspects related to cybersecurity are mentioned. The analysis identifies and exploits several vulnerabilities.

Following the analysis and the final results, several strategies are presented to mitigate, detect, and contain various security incidents.

Keywords: Cybersecurity, CIS, Threat Containment, Privilege Escalation, Exploitation, Hardening, Red Team, Information Security, SIEM, SOAR, Vulnerabilities, WAF.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Glosario

Blue Team. Profesionales encargados de proteger y defender los activos tecnológicos y seguridad de los sistemas de una organización.

Exploit. Código malicioso diseñado para explotar vulnerabilidades y comprometer un sistema de información.

Pentesting. Simulación autorizada que permite realizar una intrusión o analizar las vulnerabilidades de un sistema.

SMBv1. Protocolo utilizado para compartir archivos en los sistemas operativo Windows.

SIEM. Herramienta que gestiona eventos de seguridad, monitorea, analiza y ejecuta respuestas autorizadas para mitigar eventos de seguridad o amenazas.

SOAR. Aplicación que en la que se automatizan tareas que dan respuestas a eventos o incidentes de seguridad.

WAF. Herramineta que prtmite generar una capa de protección a entornos o sitios web.

EDR. Sistema que permite detectar y dar respuesta a dispositivos finales.

CIS Controls. Estandar de buenas prácticas que permiten ser utilizada y aplicadas para mejorar los entornos de ciberseguridad.

Escalamiento de privilegios. Metodo utilizado por un atacante para asignar privilegios de administrador a un usuario.

Introducción

El objetivo del trabajo es analizar el caso propuesto de la organización CyberFort Technologies, se busca detectar y contener un ataque informático, a través de un enfoque técnico y el uso de herramientas de seguridad que facilitan la mitigación de este tipo de incidentes.

Se resalta el rol tan importante que desempeñan los equipos de respuesta de defensa y ofensiva, quienes deben responder de manera ágil y efectiva frente a incidentes de ciberseguridad. En este contexto, el Ministerio TIC (2021) establece lineamientos claros para la gestión de la ciberseguridad en Colombia, proporcionando una base normativa para enfrentar estas situaciones.

Asimismo, se aborda la importancia del estándar del Center for Internet Security (CIS) para el fortalecimiento de la postura de seguridad de las organizaciones, mediante la implementación de controles técnicos y buenas prácticas orientadas a prevenir amenazas futuras.

Dado que la empresa CyberFort Technologies ha experimentado incidentes relacionados con fugas de información, surge la necesidad de realizar un análisis técnico que permita detectar vulnerabilidades existentes y, a partir de sus resultados, establecer estrategias efectivas de seguridad que eviten futuros incidentes y reduzcan el riesgo de comprometer los principios fundamentales de la seguridad informática.

Como lo señala Andress (2014), “la aplicación de principios como la confidencialidad, integridad y disponibilidad es fundamental en la gestión de incidentes”, principios que deben guiar toda respuesta ante amenazas en los sistemas de información.

Objetivos

Objetivo General

Ejecutar un análisis que permita identificar, explotar y mitigar algún tipo de vulnerabilidad, aplicando cada fase del proceso de pentesting, para así identificar y explotar las fallas de seguridad encontradas.

Objetivos Específicos

Identificar los puertos y servicios que se encuentran expuestos en lamáquina objetivo utilizando herramientas de reconocimiento.

Analizar la información recolectada para detectar posibles vulnerabilidades explotables.

Utilizar herramientas de explotación para evidencias la ejecución de código que demuestre el acceso remoto al equipo comprometido.

Evaluar el impacto del ataque realizado sobre el equipo objetivo y cuáles serían las medidas que se deben de tomar para mitigar la vulnerabilidad.

Informe técnico

Análisis Red Team

"El equipo Red Team ejecuta ataques controlados para evaluar la resistencia de los sistemas de seguridad (Fortra, s. f.)."

Para llevar ejecutar la inspección de la red e identificación de la infraestructura tecnológica que incluye los activos tecnológicos pertenecientes a la organización **CyberFort Technologies** se emplearon diversas herramientas que se enfocan en la inspección y evaluación de las vulnerabilidades:

- NMAP: Herramienta utilizada para examinar la red, identificar los dispositivos conectados y detectar posibles puntos débiles en el sistema objetivo. "Nmap facilita la detección de puertos abiertos y servicios expuestos en los dispositivos conectados a la red" (CVE - CVE-2017-0143, s. f.).

"Nmap también es utilizado como base en auditorías internas conforme a estándares como el NIST SP 800-94, dado que permite evaluar el estado de los servicios expuestos y su configuración." (Scarfone & Mell, 2007).

- Metasploit: Herramienta que permite a un analista de seguridad realizar pruebas de penetración con el fin de encontrar y explotar las debilidades en sistemas y redes, con el propósito de ayudar a evaluar la seguridad de aplicaciones y plataformas. Su objetivo es facilitar la evaluación de la seguridad de las aplicaciones y los sistemas. "Metasploit es una plataforma para realizar pruebas de penetración automatizadas y ejecutar exploits conocidos" (Ediciones ENI, s. f.).
- Meterpreter: Herramienta utilizada para realizar escalamiento de permisos después de haber comprometido un sistema.

"Metasploit es una plataforma para realizar pruebas de penetración automatizadas y ejecutar exploits conocidos" (Ediciones ENI, s. f.).

1. Fases del Pentesting

1.1 Reconocimiento

Para iniciar la fase de reconocimiento, identificamos el segmento de red para posterior a ello hacer la inspección o análisis de la red, el cual se ejecutará con el sistema operativo Kali Linux instalada en una máquina virtual. Empezamos identificando la IP de la maquina con SO Kali Linux ejecutando el comando **ifconfig**.

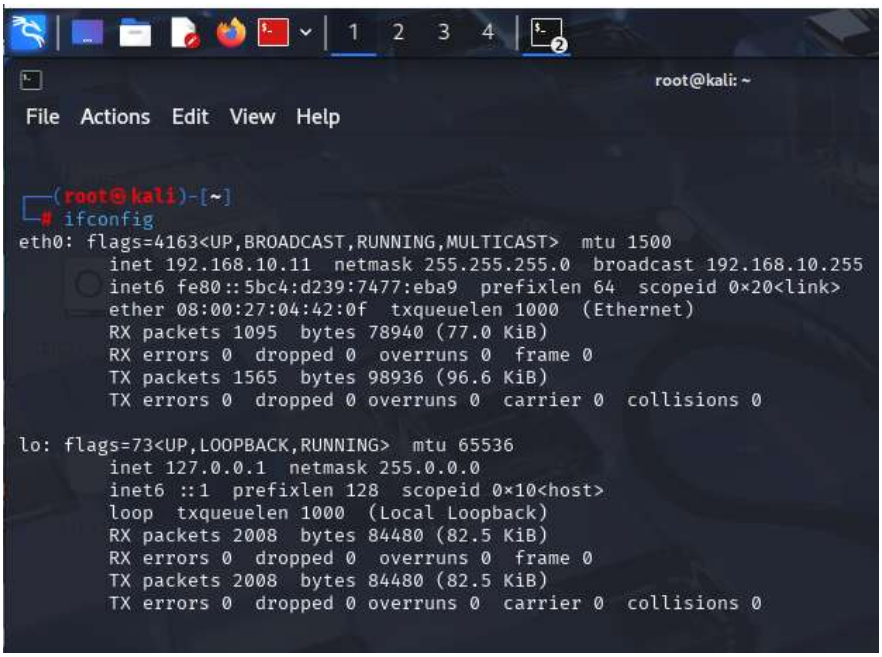
IP Maquina con SO Kali Linux: 192.168.10.11.

Mascara: 24 o 255.255.255.0

Rango de IP local: 192.168.10.xxx

Figura 1

Reconocimiento



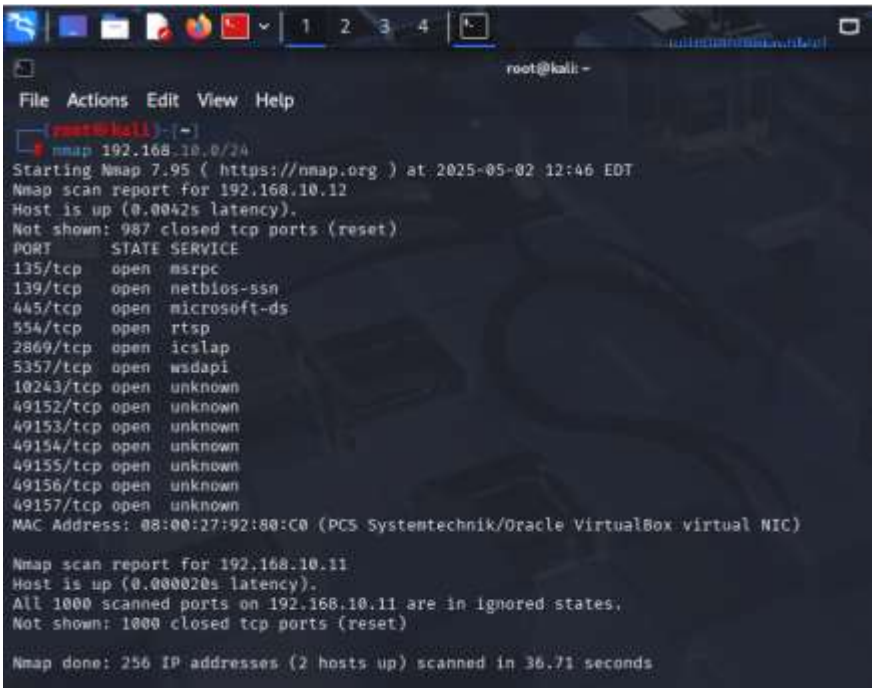
Fuente: Elaboración Propia

1.2 Escaneo

Analizamos la red ejecutando el comando **nmap 192.168.10.0/24** para inspecciona la red y así identificar los dispositivos enlazados, puertos accesibles y los servicios vinculados.

Figura 2

Análisis de red



Fuente: Elaboración Propia

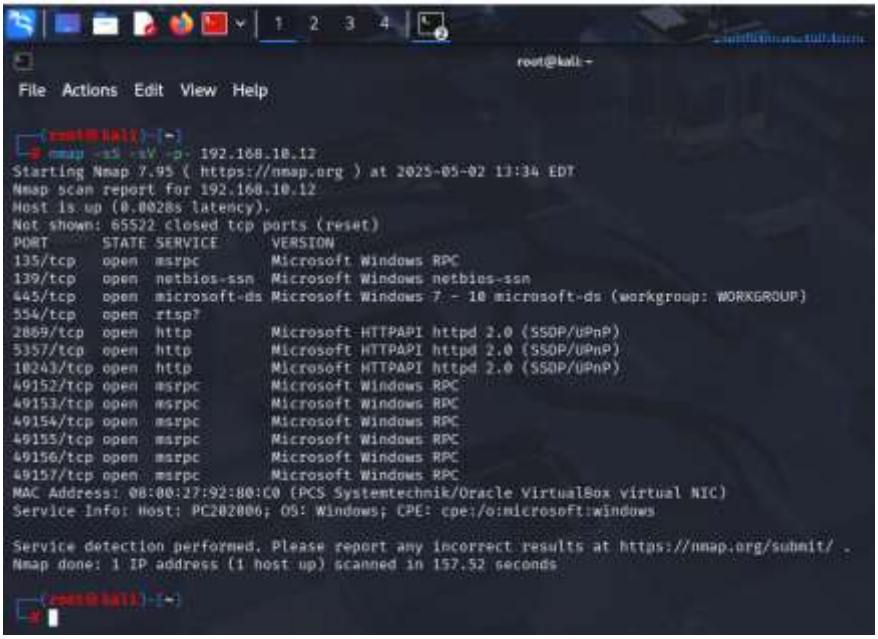
Se detecta un equipo que se tomara como blanco del analisi, esta máquina tiene asignada la IP **192.168.10.12**, al igual que la **MAC 08:00:27:92:80:C0** de la tarjeta de red

Ahora, inspeccionamos puertos expuestos ejecutando el comando **nmap -sS -sV -p- 192.168.10.12** que analiza su versionamiento y de qué forma están expuestos.

“Nmap facilita la detección de puertos abiertos y servicios expuestos en los dispositivos conectados a la red” (CVE - CVE-2017-0143, s. f.).

Figura 3

Análisis de puertos, software y versión correspondiente.



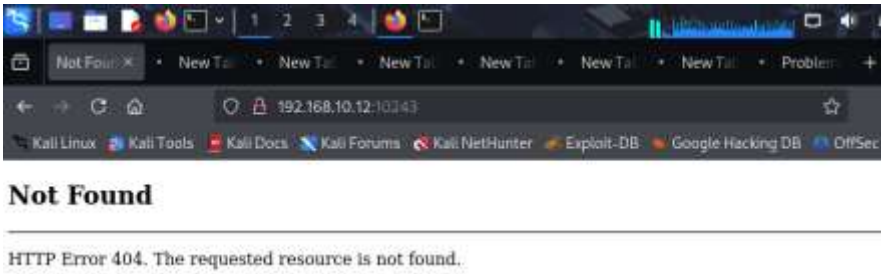
Fuente: Elaboración Propia

Se observa que el equipo cuenta con 13 puertos abiertos, los cuales se emplean para servicios dedicados al intercambio de archivos, transmisión de audio y servicios HTTP.

Al realizar pruebas mediante el navegador web, se detecta que el equipo objetivo dispone de un servicio web activo, pero no está configurado. URL http://192.168.10.12:10243/

Figura 4

Pruebas del servicio http apuntando al puerto 10243



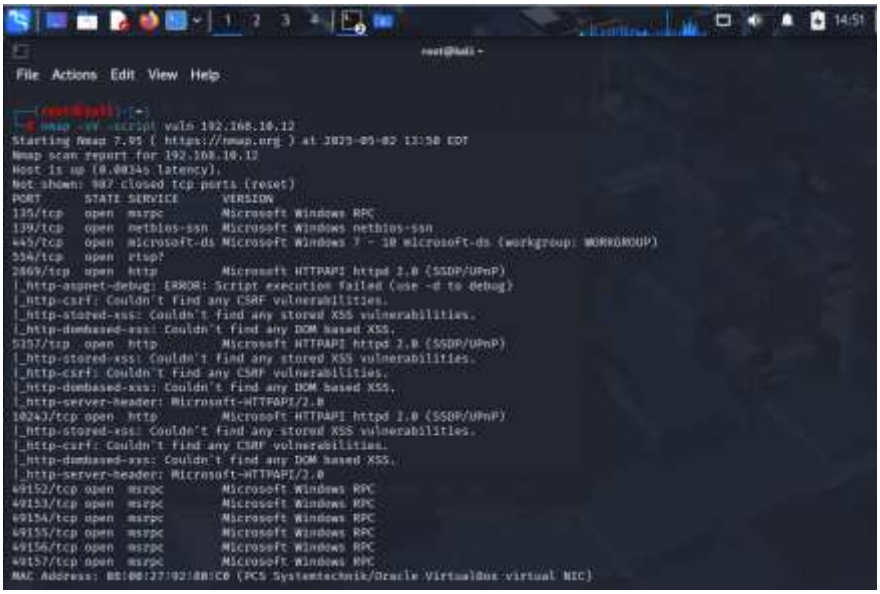
Fuente: Elaboración Propia

1.3 Explotación

Después de identificar los puertos abiertos, las versiones de los servicios y las aplicaciones en ejecución, se utiliza el comando **nmap -sV --script vuln 192.168.10.12** para profundizar en la detección de fallos de seguridad. Esta instrucción permite escanear el sistema en busca de vulnerabilidades conocidas relacionadas con los servicios detectados.

Figura 5

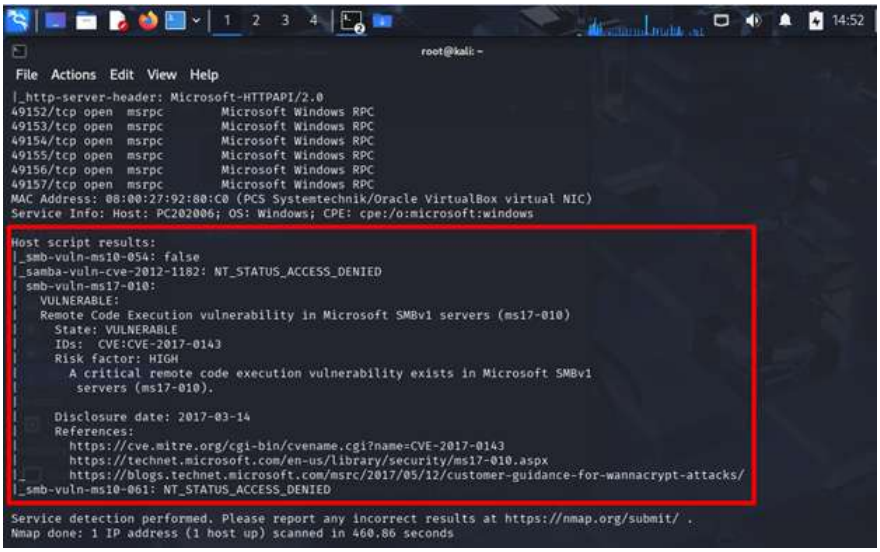
Parte1 Vulnerabilidades



Fuente: Elaboración Propia

Figura 6

Parte 2 Identificación de vulnerabilidades



Fuente: Elaboración Propia

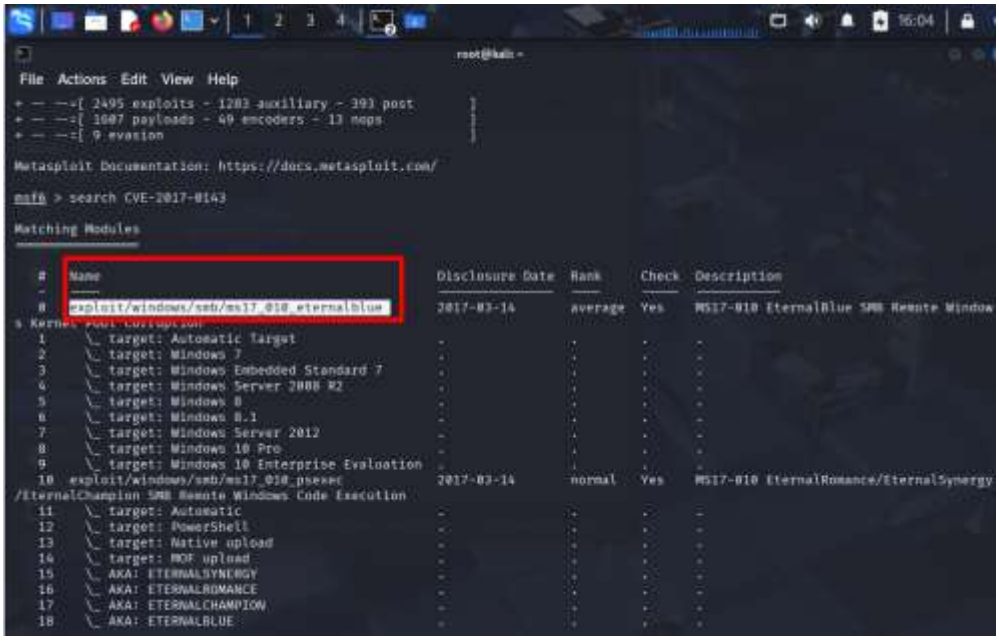
Tras el análisis realizado, se identificaron vulnerabilidades, entre ellas una registrada como CVE-2017-0143, en su documentación reporta que permite la ejecución de código malicioso aprovechando una vulnerabilidad en el servicio SMBv1. La vulnerabilidad impacta a equipos con sistema operativo Windows, incluyendo Microsoft Vista SP2, 7 SP1, 8.1 y Server 2012 R2.

"La vulnerabilidad CVE-2017-0143 permite la ejecución remota de código a través de SMBv1" (INCIBE, s. f.).

Una vez identificada la vulnerabilidad, se procederá a su explotación empleando la herramienta Metasploit, aprovechando la falla en el servicio SMBv1. Para ello, se realiza una búsqueda del exploit dentro del framework Metasploit utilizando el comando search CVE-2017-01, el cual localiza el exploit y confirmado, la vulnerabilidad MS17-010 (EternalBlue) se encuentra en Metasploit bajo la ruta: exploit/windows/smb/ms17_010_eternalblue

Figura 7

Búsqueda exploit

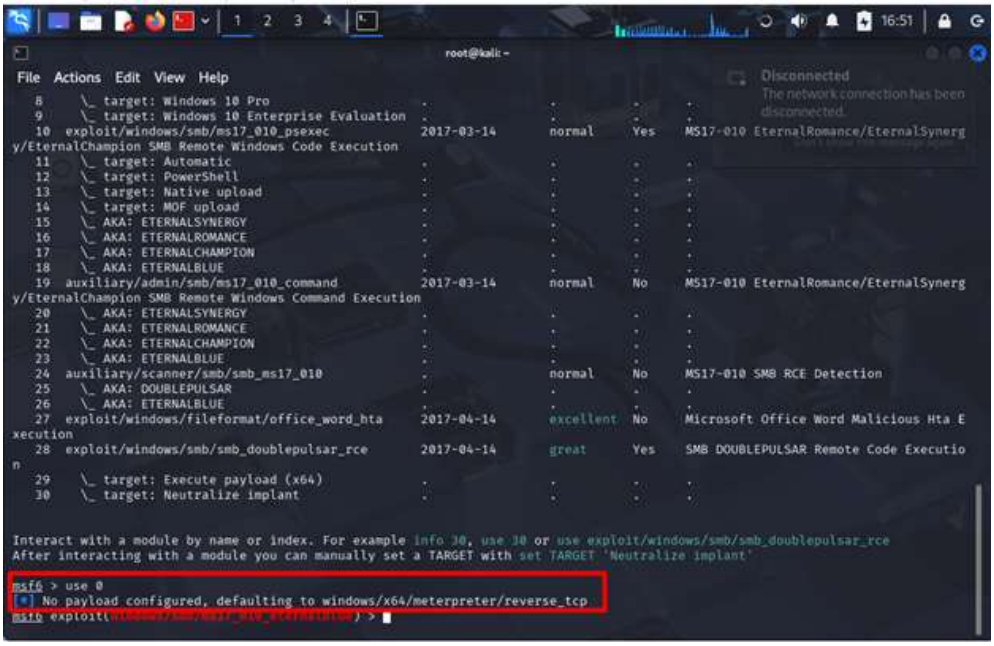


Fuente: Elaboración Propia

Como ya ubicamos el exploit lo escogemos utilizando el comando use **0** en el en la herramienta metasploit, le asignamos parámetros para posterior a ello explotar la explotación de la vulnerabilidad.

Figura 8

Selección exploit

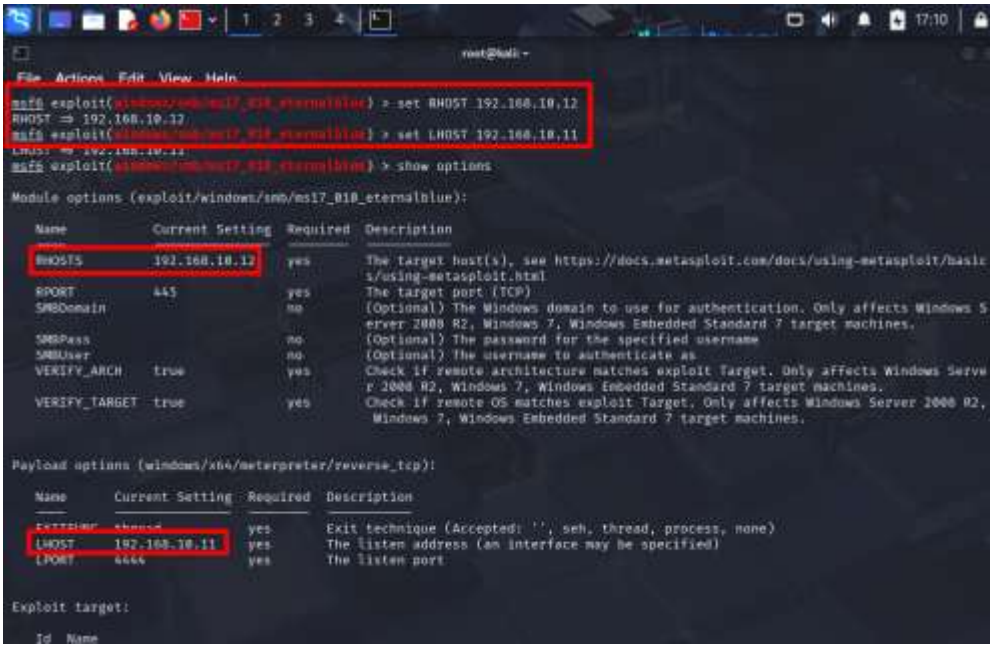


Fuente: Elaboración Propia

Se configuran los valores correspondientes, que incluyen la IP de la máquina que presenta la vulnerabilidad y la IP del equipo atacante. Esto se hace mediante la ejecución de los comandos set RHOST: 192.168.10.12, y set LHOST: 192.168.10.11.

Figura 9

Configuración el exploit



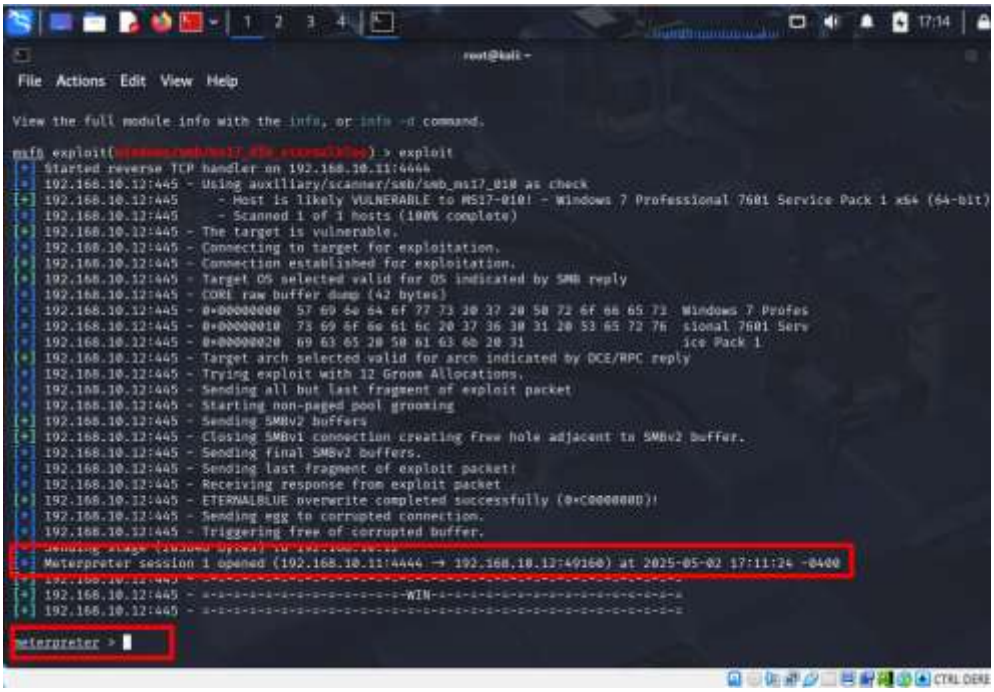
Fuente: Elaboración Propia

1.4 Post-Explotación

Se lanza el exploit contra la máquina objetivo para aprovechar la vulnerabilidad previamente descrita. Confirmamos que la explotación fue exitosa y que hemos obtenido acceso al sistema de la máquina objetivo.

Figura 10

Ejecución de exploit

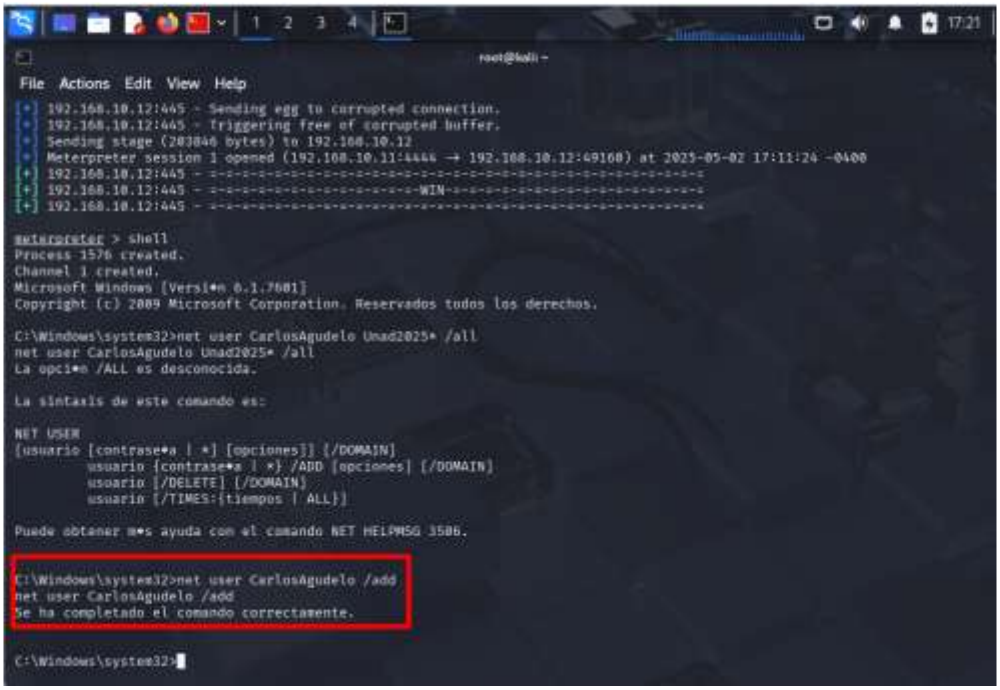


Fuente: Elaboración Propia

Ahora se confirma que la conexión con la máquina objetivo fue exitosa. Con el fin de realizar el escalamiento de privilegios, se accede a la consola del sistema operativo Windows desde la sesión de Meterpreter mediante el comando shell. Una vez dentro, se procede a crear un nuevo usuario en el sistema comprometido ejecutando el comando **net user CarlosAgudelo /add.**

Figura 11

Creamos el usuario local

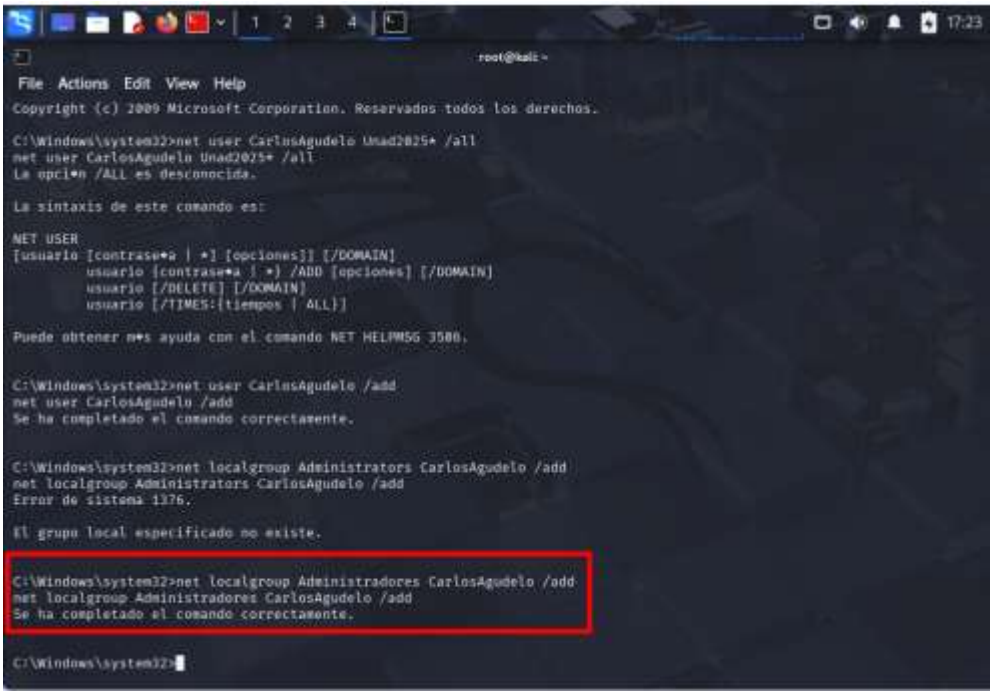


Fuente: Elaboración Propia

Después de crear el usuario local, procedemos a otorgarle privilegios administrativos en la máquina Windows. Para ello, ejecutamos el comando que añade al usuario **CarlosAgudelo** al grupo de administradores locales, garantizando así que tenga permisos completos para administrar el sistema.

Figura 12

Asignación de permisos

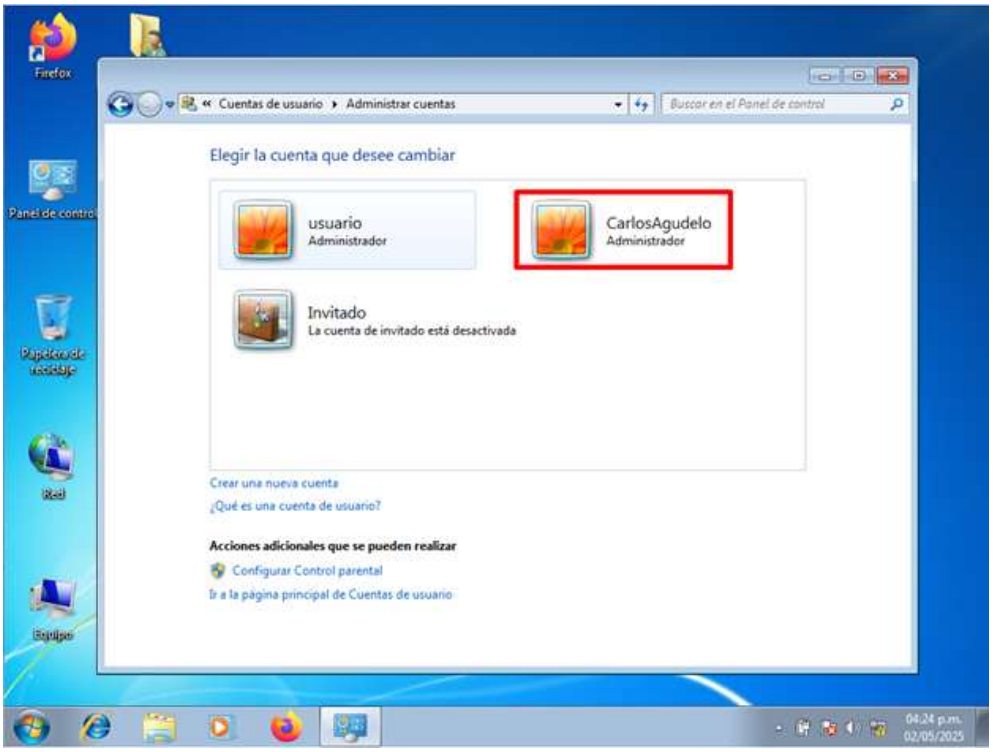


Fuente: Elaboración Propia

Por último, se ingresa al sistema comprometido para verificar que el usuario **CarlosAgudelo** ha sido creado exitosamente y que posee permisos de administrador.

Figura 13

Administrador del equipo objetivo



Fuente: Elaboración Propia

2. Detalles técnicos que ayudaron la identificación del incidente

En el anexo se presenta información relevante que ofrece pistas sobre el objetivo al que se enfrentará:

- La máquina comprometida utiliza un sistema operativo Windows.
- Este sistema operativo analizado presenta una vulnerabilidad que posibilita la ejecución remota de comandos a través de PowerShell.
- Cuenta con una aplicación que presenta fallas de seguridad.
- Existe una vulnerabilidad que facilita la ejecución remota de un exploit mediante PowerShell, lo cual posibilita el escalamiento de privilegios.

3. Aplicaciones que se utilizaron para diagnosticar las vulnerabilidades

Se empleó la herramienta NMAP para llevar a cabo el escaneo de la máquina objetivo, lo que permitió detectar la presencia de la vulnerabilidad CVE-2017-0143. Esta falla de seguridad facilita la ejecución remota de comandos mediante el servicio SMB, específicamente a través del puerto 445/TCP.

4. Consecuencias derivadas del incidente en el sistema Windows

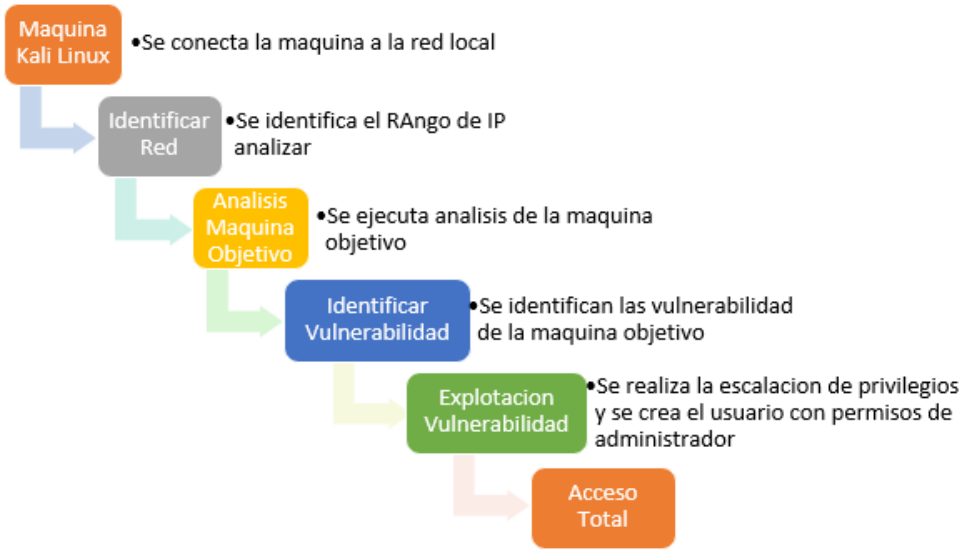
Este tipo de incidentes representa una amenaza significativa para la seguridad de la información, ya que compromete directamente los principios fundamentales que la sustentan. Al producirse una filtración de datos, se ve afectada la confidencialidad, pues la información puede quedar expuesta a personas no autorizadas. Asimismo, la integridad se ve en riesgo si los datos son modificados o manipulados. Incluso la disponibilidad podría verse comprometida si el acceso legítimo a la información se ve interrumpido. En muchos casos, los datos sustraídos pueden ser utilizados, intercambiados o comercializados por terceros con fines delictivos, como fraudes o suplantación de identidad.

4.2 ¿Cuál fue el procedimiento utilizado para explotar la falla de seguridad CVE-2017-0143 durante el ataque?

En esta sección incluye una representación gráfica que ilustra el desarrollo del ataque, detallando cada una de sus fases y señalando el punto exacto en el que se aprovechó la vulnerabilidad detectada.

Figura 14

Paso a paso del ataque



Fuente: Elaboración Propia

5. Estrategias de Contención

"Según XM Cyber (s. f.), el equipo Blue Team tiene como misión mantener la seguridad de la infraestructura mediante monitoreo y defensa activa."

Como analista de seguridad e integrante del grupo Blue Team, la primera acción que ejecutaría es aislar la máquina afectada en el incidente de seguridad, ya sea inactivando su tarjeta de red o desconectando el cable de red, para evitar la propagación del ataque, fuga de información y a su vez contener el ataque. Posterior a ello iniciar una investigación con el usuario y de la máquina afectada, al igual que generar una imagen forense. El procedimiento sería:

- Identificar si hay más máquinas comprometidas.
- Interrogar al usuario para conocer las actividades realizadas en el equipo antes del ataque y determinar si hubo algún error humano que haya contribuido al incidente.
- Revisar los procesos activos en la máquina mediante el Administrador de tareas.
- Analizar el uso de memoria RAM y espacio en disco.

- Implementar una política de grupo (GPO) a través del Active Directory para desactivar el servicio SMBv1 en los equipos de la compañía. Si no hay un Active Directory, desactivar manualmente el servicio en cada máquina.
- Analizar el equipo con el antivirus y, de forma manual, inspeccionar carpetas y subcarpetas ocultas del sistema operativo para detectar archivos sospechosos o no autorizados.
- Comprobar si hay usuarios administradores desconocidos y eliminarlos.
- Revisar y analizar el visor de sucesos del sistema operativo para identificar indicios del ataque.

En la siguiente tabla vamos a evidenciar las herramientas empleadas por los equipos de seguridad, están clasifican de acuerdo con su fase y funcionalidad.

Tabla 1

Herramientas empleadas por Red Team y Blue Team

Fase	Herramienta	Funcionalidad	Equipo
Reconocimiento	Nmap	Escaneo de puertos y detección de servicios	Red Team
Explotación	Metasploit	Ejecución de exploits	Red Team
Análisis	SIEM	Correlación de eventos y alertas	Blue Team
Respuesta automática	SOAR	Automatización de respuesta a un incidente	Blue Team
Protección Endpoints	EDR	Detección y aislamiento	Blue Team
Protección de aplicación WAF	WAF	Mitigación de ataques	Blue Team

Nota. La tabla presenta herramientas empleadas por los equipos Red Team y Blue Team, clasificadas por su funcionalidad y fase del proceso de seguridad.

Fuente: Elaboración Propia

5.1 Medidas de contención Blue Team

Para fortalecer los sistemas de información y reducir la probabilidad de futuros ataques informáticos en la organización, es fundamental aplicar las siguientes acciones de endurecimiento:

- Capacitación continua al personal en aspectos clave de ciberseguridad, abordando temas como:
  - Concienciación sobre los riesgos digitales y cómo reconocerlos.
  - Identificación de ciberataques, sus fases y la respuesta adecuada ante estos eventos.
- Implementación de soluciones anti-malware, configuradas para realizar análisis automáticos y diarios, con el fin de detectar y eliminar amenazas de forma oportuna.
- Mantener activado el firewall local en todos los equipos para bloquear accesos no autorizados.
- Aplicar controles de seguridad en la infraestructura tecnológica, tanto a nivel de red como en los dispositivos de cómputo.
- Establecer un firewall perimetral con controles de navegación para inspeccionar, supervisar y controlar el tráfico entrante y saliente de la red.
- Restringir el uso de puertos USB en los equipos para evitar la introducción de malware por dispositivos externos.
- Asignar cuentas de usuario con privilegios limitados, impidiendo que realicen cambios críticos en los sistemas sin autorización.

Definir e implementar políticas de seguridad internas, orientadas a regular el uso adecuado de los recursos tecnológicos y la protección de la información.De acuerdo con los lineamientos metodológicos de la UNAD (2023), la defensa activa debe estar acompañada de monitoreo constante y respuesta.

5.2 Herramientas de contención y defensa

Las herramientas SIEM representan un papel clave para la detección y respuesta de incidentes de seguridad, ya que recopilar, correlacionan y analizan todos los eventos generados en los dispositivos y sistemas configurados dentro de una infraestructura tecnológica.

A través de políticas previamente definidas, un SIEM ayuda a identificar comportamientos anómalos, generar alertas en tiempo real y dar una respuesta oportuna a posibles amenazas. Su principal objetivo es reducir los riesgos asociados a la seguridad de la información mediante la detección temprana de ataques o vulnerabilidades, lo cual mejora significativamente los tiempos de reacción y la efectividad de las acciones de contención. El SIEM permite centralizar eventos de seguridad, analizar patrones de amenazas y automatizar respuestas ante incidentes (Kim & Solomon, 2016).

Funcionalidades claves de un SIEM, son sistemas que cumple diversas funciones que permiten fortalecer la seguridad de una organización mediante la centralización y análisis inteligente de eventos. Sus principales capacidades son:

- **Recopilación de datos:** En esta etapa, el SIEM recolecta registros (logs) generados por servidores, firewalls, dispositivos de red y otros sistemas previamente configurados, con el objetivo de disponer de una fuente integral de información para análisis posteriores.
- **Correlación y análisis:** El sistema analiza los eventos registrados, buscando patrones de comportamiento anómalos o indicadores de compromiso. Esto se logra mediante reglas de correlación que permiten detectar relaciones entre diferentes eventos de seguridad.
- **Detección de amenazas:** Gracias a la configuración de reglas específicas, el SIEM puede identificar comportamientos sospechosos o actividades que representen una amenaza potencial, permitiendo una detección proactiva.
- **Respuesta automatizada y notificación:** Una vez detectada una posible amenaza, el sistema puede activar respuestas automáticas para contener el incidente y minimizar su impacto. Además, genera alertas que son enviadas al equipo de ciberseguridad para su atención inmediata.

- **Firewall de Aplicaciones Web (WAF)**

Los WAF son herramientas que generan una capa especializada de seguridad diseñada para proteger aplicaciones web frente a ataques dirigidos por ciberdelincuentes. Su propósito es prevenir accesos maliciosos que intenten alterar, extraer o eliminar información sensible alojada en plataformas web.

Este tipo de firewall actúa inspeccionando el tráfico HTTP y HTTPS que entra y sale de la aplicación, y es capaz de bloquear amenazas comunes como:

- Inyecciones de código SQL (SQLi)
- Cross-Site Scripting (XSS)
- Manipulación de parámetros
- Otros ataques dirigidos a vulnerabilidades en la capa de aplicación

Gracias a esta capa de protección, se reduce significativamente el riesgo de explotación de vulnerabilidades en entornos web críticos para la organización. “El WAF protege las aplicaciones web de ataques como inyección SQL o XSS, inspeccionando el tráfico entrante” (Check Point Software, s. f.).

Estas herramientas se interponen entre el cliente y la aplicación web, filtrando y deteniendo intentos de ataque como denegaciones de servicio, inyecciones de SQL malicioso, scripts entre sitios (XSS), entre otros. “De acuerdo con Oracle (s. f.), un WAF puede implementarse tanto en hardware como en la nube para proteger aplicaciones web críticas.”

Hay una variedad de fabricantes que desarrollan estas herramientas como: **AWS, Fortinet, Cloudflare, SiteLock, ModSecurity entre otros.**

- **SOAR**

Es una herramienta de seguridad utiliza por analistas de seguridad para responder a un ataque informática de forma rápida y eficaz. SOAR automatiza tareas de respuesta y permite una reacción rápida ante incidentes de seguridad (Northcutt & Shenk, 2006). Esta herramienta permite la ejecución de tareas automáticas, que gestionan el riesgo y dan respuesta a cualquier incidente de seguridad que se pueda presentar. “Pure Storage (s. f.) resalta que SOAR ayuda a reducir el tiempo de respuesta y mejora la eficiencia operativa en seguridad.”

El uso de herramientas como el SIEM permite automatizar tareas repetitivas y estandarizar los procesos de respuesta ante incidentes, lo que se traduce en una mejora significativa en los tiempos de reacción frente a amenazas. Al integrarse con soluciones de seguridad como firewalls, sistemas EDR, IPS/IDS, entre otros, la gestión de un ataque es más ligera, precisa y eficaz, reduciendo las consecuencias de los ataques cibernéticos.

Al automatizar tareas los analistas de seguridad pueden enfocar sus esfuerzos en las actividades estratégicas, como el diseño y la implementación de controles preventivos más robustos. Además, al analizar patrones de comportamiento y evolución de las amenazas, el SIEM contribuye a ajustar las políticas de defensa de forma proactiva, fortaleciendo de manera integral la postura de seguridad de la organización. “Microsoft (s. f.) destaca que SOAR es una solución integral para responder de forma automatizada a incidentes de seguridad complejos.”

- **EDR – Endpoint Detection and Response**

El EDR es una herramienta que detecta, investiga y responde a acciones maliciosas. “Zeltser (2019) sostiene que el EDR es esencial para detectar ataques en tiempo real mediante técnicas de análisis de comportamiento.” Tienen como objetivo salvaguardar los dispositivos como equipos de cómputo y servidores, por medio de un monitoreo continuo y la respuesta oportuna que se pueda presentar en la infraestructura tecnológica. Las herramientas EDR permiten monitorear y aislar endpoints comprometidos (Grimes, 2017).

A diferencia de los antivirus convencionales que se basan principalmente en firmas actualizadas, estas herramientas emplean métodos como el análisis del comportamiento y técnicas heurísticas para detectar amenazas de forma rápida, incluso aquellas desconocidas o de tipo zero-day.

Su trabajo se compone de las siguientes capacidades:

- Supervisión constante de los dispositivos.
- Documentación minuciosa de los eventos que ocurren en el sistema operativo, en la red y en los procesos en ejecución.
- Emisión de eventos ante actividades sospechosas y patrones anómalos.
- Aislamiento inmediato de las maquinas comprometidos para evitar la propagación de posibles infecciones.
- Recolección de evidencia para facilitar un análisis forense posterior.

Es una herramienta actúa protegiendo los dispositivos, también previene algún tipo de escalada y propagación de ataques dentro del entorno corporativo. Es fundamental integrarla con plataformas SOAR y SIEM, ya que esta combinación optimiza los tiempos de respuesta y mejora la capacidad de actuación ante cualquier incidente de ciberseguridad.

6. Contexto legal y Regulaciones

6.1 Regulación legal vigente en Colombia

Dentro del marco legal colombiano, la Ley 1273 de 2009 "La Ley 1273 de 2009 protege la confidencialidad, integridad y disponibilidad de los datos y sistemas de información" (Función Pública, s. f.). Se creó un marco legal puntual orientado a los crímenes informáticos, penalizando acciones como el ingreso indebido a sistemas computacionales, la interceptación no autorizada de información, la utilización o difusión de programas maliciosos, y la transmisión de datos sin aprobación previa

Entre los artículos más relevantes de esta normativa se encuentran:

Artículo 269A: Sanciona el acceso abusivo a sistemas de información.

Artículo 269C: Penaliza la interceptación de datos informáticos.

Artículo 269E: Condena la creación y uso de software malicioso.

Artículo 269F: Castiga la violación de datos personales.

Artículo 269J: Sanciona la transferencia no autorizada de activos digitales.

Estos artículos resultaron clave para evaluar legalmente los contratos ofrecidos por la empresa contratante, porque incluyen disposiciones que podrían violar esas normativas.

6.2 Análisis del contrato de CyberFort Technologies

Se evidenció que, en el proceso de selección, el acuerdo de confidencialidad contenía estipulaciones incompatibles con las leyes colombianas, específicamente al marco jurídico de los delitos informáticos establecido en la Ley 1273 de 2009. Entre las disposiciones cuestionables se encontraban:

- **Cláusula 1:** N permitía reportar actividades ilegales dentro de la empresa, lo cual vulnerando la denuncia de actos delictivos. Infringe el Artículo 269A del Código Penal Colombiano.
- **Cláusula 2, literal 2:** Consideraba como "información protegida" prácticas como interceptaciones ilegales ("chuzadas") y acceso no autorizado a datos, lo que representa una apología de actos ilícitos. Infringe los Artículos 269A y 269C.
- **Cláusulas 3 y 4:** Exigían no reportar actividades ilícitas, como la investigación o almacenamiento de información, lo que dificultaba la colaboración con las autoridades correspondientes. Esto va en contra de los Artículos 269C y 269H.
- **Cláusula Octava:** Buscaba liberar a la empresa de cualquier responsabilidad penal, transfiriendo la totalidad de las consecuencias al trabajador, lo cual infringe el Artículo 269F.

6.3 Postura ética

Desde un enfoque ético y profesional, como especialista en ciberseguridad no aceptaría ni desempeñaría funciones bajo un contrato que apoye o permita prácticas ilegales. Dicho acuerdo viola principios fundamentales de la ciberseguridad, incluyendo la integridad, la legalidad y la protección de los datos.

Asimismo, este tipo de cláusulas vulnera disposiciones del Código de Ética Profesional del COPNIA, en particular:

Literal 1.3 (Responsabilidad), que establece el deber de actuar conforme a la legislación vigente.

Literal 2.5 (Respeto por la privacidad y confidencialidad), que promueve el uso ético y legal de la información, garantizando la protección de datos personales y corporativos.

Según lo dispuesto en el Código de Ética Profesional del COPNIA (2019), todo ingeniero debe actuar con rectitud, legalidad y responsabilidad social. Aceptar un acuerdo de este tipo implicaría poner en riesgo la integridad profesional, exponerse a sanciones legales y comprometer la confianza depositada en el rol de protección que debe cumplir un profesional de ciberseguridad.

Este caso refuerza la importancia de actuar con independencia, criterio ético y pleno respeto por el marco normativo, valores esenciales para el ejercicio responsable de la profesión.

Conclusiones

Se ejecutaron pruebas de intrusión utilizando herramientas de análisis y explotación como Nmap, Metasploit y funcionalidades Menterpreter, lo cual permitido validar la existencia de brechas de seguridad. Identificando y explotando la vulnerabilidad **CVE-2017-0143,** que posibilita la ejecución de código remoto usando el servicio SMBv1 en sistemas operativos Windows 7. El ejercicio cubrió las etapas del pentesting: reconocimiento, escaneo, explotación y post-explotación, lo que facilitó un análisis detallado del banco de trabajo. Este procedimiento resaltó la necesidad de mantener los sistemas operativos actualizados, demostrando por qué este proceso es esencial para corregir vulnerabilidades existentes. Para concluir, se destaca la relevancia de implementar políticas de hardening y mantener un monitoreo constante, como acciones clave para fortalecer la seguridad organizacional.

Recomendaciones

Para fortalecer la cultura de seguridad, es crucial implementar campañas de concientización y capacitación continua en ciberseguridad para todo el personal de la organización. Esto debe incluir simulacros de phishing, buenas prácticas para el uso seguro del correo electrónico y formación para reconocer posibles amenazas. La educación juega un papel clave en la reducción del error humano, uno de los principales vectores de los ciberataques.

Se recomienda realizar evaluaciones periódicas de seguridad mediante pruebas de intrusión, como ejercicios planificados de Red Team y pentesting, que permiten validar las defensas de manera controlada y descubrir vulnerabilidades antes de que puedan ser aprovechadas por atacantes. Además, es fundamental asignar roles formales para los equipos Red Team y Blue Team, integrando profesionales con perfiles técnicos y éticos, asegurando su independencia y especialización. Esto fortalece la capacidad de detección, respuesta y prevención frente a amenazas en tiempo real.Además, debe implementarse un conjunto de herramientas integradas, como SIEM, EDR y SOAR, asegurando su correcta configuración:

- El SIEM va a realizar el monitoreo de los eventos.
- El EDR nos permitirá ejecutar o dar una respuesta en los endpoints ante un posible ataque o acciones inaducuadas,
    - SOAR tendrá tareas automatizadas para enviar alertas.

Actualizar los sistemas y aplicar procesos de hardening resulta fundamental. Mantener el software siempre actualizado con los últimos parches de seguridad, desactivar servicios que no son necesarios como SMBv1, y seguir las directrices de hardening contribuye a disminuir la superficie de ataque.

La segmentación de la red y el control de accesos son igualmente esenciales, lográndose a través de VLANs y firewalls internos que limitan el desplazamiento lateral en caso de una intrusión. Además, es necesario implementar políticas de gestión de accesos basadas en el principio de mínimos privilegios, utilizar autenticación multifactor (MFA) y monitorear las cuentas con privilegios elevados.

Contar con un plan formal de respuesta a incidentes, bien definido y probado, que contemple roles, fases, responsables y procedimientos es indispensable. Este plan debe ser revisado y ensayado periódicamente mediante simulacros para asegurar su efectividad.

Finalmente, se deben implementar backups cifrados, almacenados en distintas locaciones o datancerter, ejecutar pruebas de restauración semestrales o anuales, para asegurar la recuperación en caso de que se presente un incidente de seguridad con un ransomware u otras amenazas destructivas. Finalmente, todas las implementaciones alinearlas con estandares o frameworks como la ISO 27001, NIST, CIS, al igual que las estrategias de seguridad.

Referencias Bibliográficas

Allen, J. (2020). *Advanced penetration testing: Hacking the world's most secure networks* (2nd ed.). Wiley. https://www.wiley.com/en-us/Advanced+Penetration+Testing%3A+Hacking+the+World%27s+Most+Secure+Networks%2C+2nd+Edition-p-9781119561453

Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (2nd ed.). Syngress. https://www.elsevier.com/books/the-basics-of-information-security/andress/978-0-12-800744-0

Check Point Software. (s. f.). *Equipo rojo contra equipo azul: ¿Cuál es la diferencia?* https://www.checkpoint.com/es/cyber-hub/cyber-security/red-team-vs-blue-team/}

Ediciones ENI. (s. f.). *Metasploit—La posexplotación con Meterpreter.* https://www.ediciones-eni.com/libro/metasploit-verifique-la-seguridad-de-sus-infraestructuras-9782409040221/la-posexplotacion-con-meterpreter

Fortra. (s. f.). *Red Team | Fortra.* https://www.fortra.com/es/soluciones/ciberseguridad/red-team

Función Pública. (s. f.). *Ley 1266 de 2008—Gestor Normativo.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Función Pública. (s. f.). *Ley 1273 de 2009—Gestor Normativo.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Función Pública. (s. f.). *Ley 1581 de 2012—Gestor Normativo.* https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Grimes, R. A. (2017). *Hacking the hacker: Learn from the experts who take down hackers.* Wiley. https://www.wiley.com/en-us/Hacking+the+Hacker%3A+Learn+from+the+Experts+Who+Take+Down+Hackers-p-9781119396215

INCIBE. (s. f.). *¿Qué es el Red Teaming y por qué es importante para tu organización?* https://www.incibe.es/protege-tu-empresa/blog/red-teaming

INCIBE-CERT. (s. f.). *CVE-2017-0143.* https://www.incibe.es/en/incibe-cert/early-warning/vulnerabilities/cve-2017-0143

Kim, D., & Solomon, M. G. (2016). *Fundamentals of information systems security* (3rd ed.). Jones & Bartlett Learning. https://www.jblearning.com/catalog/productdetails/9781284116458

Microsoft. (s. f.). *¿Qué es SOAR?* https://www.microsoft.com/es-co/security/business/security-101/what-is-soar

Mitre Corporation. (s. f.). *CVE - CVE-2017-0143.* https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Northcutt, S., & Shenk, E. (2006). *Blue Team Handbook: Incident Response Edition.* NSA Red/Blue Team Training Series. https://www.sans.org/white-papers/blue-team-handbook-incident-response-edition/

Oracle. (s. f.). *¿Qué es un firewall de aplicaciones web (WAF)?* https://www.oracle.com/co/security/cloud-security/what-is-waf/

Pure Storage. (s. f.). *¿Qué es SOAR?* https://www.purestorage.com/es/knowledge/what-is-soar.html

The Bridge. (s. f.). *¿Qué es un Red Team?* https://thebridge.tech/blog/que-es-un-red-team/

XM Cyber. (s. f.). *¿Qué es un equipo Blue Team?* https://xmcyber.com/glossary/what-is-a-blue-team/

Zeltser, L. (2019). *Understanding endpoint detection and response (EDR) solutions.* SANS Institute. https://www.sans.org/white-papers/understanding-endpoint-detection-and-response-edr-solutions/

Anexos

Enlace video sustentación

https://youtu.be/0RwYDZuhQXA