Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam

Fabian Alberto Ayala Lozano

Asesor

Luis Fernando Zambrano Hernandez

Escuela de Ciencias Básicas, Tecnologías e Ingenierías ECBTI

Especialización en Seguridad informática

2025

Resumen

Para este trabajo, se realizó un análisis integral de la estrategias técnicas y éticas implementadas por los equipos RedTeam y BlueTeam, en un entorno simulado de ciberseguridad. Se abordaron metodologías pruebas de penetración, explotación de vulnerabilidades, normativas legales colombianas en delitos informáticos y mecanismos de contención de hardening. A través de la ejecución practica de ataques simulados y respuestas defensivas, se evidenciaron riesgos reales que enfrentan las organizaciones y se proponen estrategias para mitigar dichos riesgos. El trabajo final, destaca la importancia de la actuación ética, el cumplimento legal y la colaboración entre equipos, para fortalecer la estrategia de seguridad de la información de las empresas.

***Palabras clave*:** Ciberseguridad, Redteam, Blueteam, pentesting, hardening

Abstract

For this project, a comprehensive analysis was conducted on the technical and ethical strategies implemented by RedTeam and BlueTeam, within a simulated cybersecurity environment. penetration testing methodologies, vulnerability exploitation, Colombian legal regulations on cybercrime, and hardening containment mechanisms were addressed. Through the practical execution of simulated attacks and defensive responses, real risks faced by organizations were identified, and strategies were proposed to mitigate those risks. This final work highlights the importance of ethical conduct, legal compliance, and team collaboration to strengthen the information security posture of companies.

***Keywords*:** Cybersecurity, RedTeam, BlueTeam, pentesting, hardening

Tabla de contenido

Lista de ilustraciones

Glosario

Ciberseguridad: Conjunto de prácticas, tecnologías y procesos diseñados para proteger sistemas de informáticos, redes y datos contra ataques, daños o accesos no autorizados.

RedTeam: Equipo especializado en realizar simulaciones ofensivas de ciberataques para identificar vulnerabilidades en los sistemas de una empresa u organización, actuando como un atacante ético.

BlueTeam: Equipo defensor encargado de detectar, mitigar y responder a los ciberataques, garantizando la protección continua de los activos de información de una empresa u organización.

Hardening: Proceso de fortalecer la seguridad de sistemas informáticos mediante la reducción de vulnerabilidades, desactivando servicios innecesarios y aplicando configuraciones seguras.

CVE (Common Vulnerabilities and Exposures): Identificador único y estandarizado para registrar vulnerabilidades de seguridad conocidas en software y hardware.

Metasploit: Herramienta de código abierto utilizada para desarrollar, probar y ejecutar exploits contra sistemas vulnerables.

SIEM (Security Information and Event Management): Sistema que recopila, analiza y correlaciona eventos de seguridad de diversos dispositivos para detectar amenazas y facilitar la respuesta a incidente.

Purple Team: Modelo de colaboración entre los equipos Red Team y Blue Team, cuyo objetivo es mejorar las defensas mediante ejercicios conjuntos y retroalimentación mutua

Introducción

El entorno digital de las empresas y organizaciones modernas es cada vez más complejo y expuesto a múltiples amenas cibernéticas. La necesidad de utilizar sistemas informáticos y redes ha convertido la ciberseguridad en un componente esencial para la continuidad operativa de las organizaciones, además, de la obligación del cumplimiento normativo y de la protección de datos. Por este motivo, los equipos RedTeam y BlueTeam, desempeñan un papel estratégico en la identificación de vulnerabilidades, la simulación de ataques y la implementación de defensas efectivas.

Planteado lo anterior, este trabajo presenta un análisis integral de la dinámica ofensiva y defensiva de la ciberseguridad, mediante la aplicación de metodologías propias de los equipos RedTeam y BlueTeam, en un entorno controlado. Para esto, se realizan pruebas de penetración, explotación de vulnerabilidades y respuesta ante incidentes, se busca demostrar la importancia de una postura de seguridad proactiva y resiliente.

Además del enfoque técnico, el documento incorpora un análisis del marco legal colombiano, relacionado con los delitos informáticos y protección de datos personales, resaltando la necesidad de actuar acorde a principios éticos y normativos, en cualquier ejercicio de auditoría o intervención digital. Finalmente, se propone estrategias de hardening y recomendaciones orientadas al fortalecimiento de la infraestructura tecnológica en las empresas u organizaciones, contribuyendo así a una cultura de seguridad muy sólida.

Justificación

El crecimiento de las amenazas cibernéticas y la acelerada evolución de las técnicas de ataque, representan un desafío para las empresas u organizaciones públicas y privadas. Dada esta realidad, se hace necesario contar con profesionales capaces de comprender, simular y defenderse a dichas empresas u organizaciones, frente a escenarios complejos de ciberseguridad. En este sentido, el trabajo se justifica por su aporte académico y practico al desarrollo de competencias técnicas, éticas y legales en el ámbito de la seguridad informática.

Los ejercicios controlados mediante equipos RedTeam y BlueTeam, permite simular situaciones reales de intrusión y respuesta, lo que facilita una comprensión profunda de las vulnerabilidades que pueden ser explotadas en contra de las empresas, así como las tácticas más efectivas para mitigarlas. Estas simulaciones, al ser desarrolladas en entornos virtuales seguros, proporcionan una experiencia formativa para el análisis y mejora continua de la postura de seguridad en las empresas u organizaciones.

Además este documento integra, el análisis del marco normativo colombiano en relación con los delitos informáticos y la protección de datos personales, reforzando la importancia de una actuación profesional ética y legal. Así el trabajo no solo fortalece habilidades técnicas, sino que también fomenta una visión general que vincula la tecnología con la responsabilidad social y jurídica.

Objetivos

Objetivo General

Diseñar estrategias técnicas y éticas basadas en las funciones de los equipos RedTeam y BlueTeam, en un entorno controlado, mediante identificación de vulnerabilidades y la ejecución de pruebas con el fin formular mecanismos de defensa y contención que fortalezcas la postura de seguridad en empresas u organizaciones.

Objetivos Específicos

Identificar metodologías de pruebas de penetración para evaluar la seguridad de un sistema simulado, teniendo en cuenta las fases del proceso.

Analizar el marco legal y ético colombiano, relacionado con delitos informáticos y protección de datos personales, aplicando sus lineamientos a casos reales y simulados en contexto de ciberseguridad.

Proponer medidas de contención y estrategias de hardening fundamentadas en las mejores prácticas del BlueTeam, con el fin lograr mitigar ataques similares a los ejecutados durante la simulación.

Capacidades técnicas, legales y de gestión para equipos BlueTeam y RedTeam

Etapa 1 conceptos equipos de Seguridad

Marco legal en Colombia sobre delitos informáticos y protección de datos personal

Ley 1273 del 2009

Esta normativa fue creada en Colombia para la protección de la información y los datos de sistemas informáticos, redes, medios electrónicos y afines, con esta normativa se pretende combatir los delitos informáticos y reconoce en Colombia, como un derecho, la seguridad de los datos personales y corporativo, sus principales delitos tipificados fueron:

Acceso abusivo a un sistema informático, con una pena de 48 a 96 meses de prisión y multas de 10 a 1000 salarios mínimos.

Obstaculización ilegitima de sistemas informáticos o red, dado que se protege el uso continuo y seguro de los sistemas informáticos.

Interceptación de datos informáticos, en esta protege la captura, interferencia en la transmisión de datos digitales sin consentimiento.

Daño informático. protege de la modificación, borrar o dañar datos o software sin autorización.

Uso de Software malicioso, describe sobre la creación, distribución o utilización de programas con la intención de dañar o afectar sistemas.

Violación de datos personales, toca temas relacionados con la protección de la intimidad y privacidad de la información personal sin consentimiento.

suplantación de sitios web, en él se prohíbe la creación de páginas falsas para obtener datos personales. (Ministerio del Interior, 2009)

Ley 1581 de 2012

Mas conocida la como la ley de protección de datos personales, es el marco legal para el tratamiento de estos datos y su principal objetivo es proteger el derecho fundamental de la protección de datos personales que tiene toda persona. Sus puntos claves son:

Principios rectores: define la guía de cómo se deben tratara los datos personales, como su finalidad, la libertad, la transparencia, la seguridad, la confiabilidad, la veracidad o calidad del dato, la necesidad del dato, y el acceso y circulación restringida.

Derechos del titular: reconoce los derechos a las personas sobre sus datos personales.

Obligaciones y los derechos y encargados del tratamiento: este impone una seria de obligaciones a quienes recolectan y tratan datos personales.

Autorización: da las reglas para la obtención del consentimiento del titular para el tratamiento de datos personales, dado que este consentimiento debe ser previo expreso e informado.

Trasferencia y transmisión internacional de datos: este regula las condiciones bajo las cuales se pueden enviar datos personales a otros países y la exigencia del nivel adecuado protección del país receptor.

Superintendencia de industria y comercio (SIC): designa como autoridad al SIC. encargada de controlar y velar por el cumplimento de esta ley, como sus investigaciones y las sanciones. (Presidencia de la Republica Colombiana, 2012).

Decreto 1377 de 2013

Este decreto establece las condiciones y procedimientos para implementar la le 1581 del 2012 y aplica a todas las personas naturales o jurídicas públicos privadas que manejen bases de datos personales en Colombia.

Los aspectos claves del decreto son la autorización del titular, los avisos de privacidad, la política de tratamiento de la información, los canales de consultas y reclamos, las medidas de seguridad que las entidades deben implementar para la protección de datos personales. (Republica de Colombia , 2013)

Decreto 338 de 2022

Establece los lineamientos de la gobernanza de la seguridad digital en Colombia, sus objetivos principales, son fortalecer la gobernanza de la seguridad digital, identificar infraestructuras críticas y servicios esenciales, gestionar riesgos y responder a incidentes de seguridad digital. (Republica de Colombia, 2022).

Resolución 500 de 2021

Establece los lineamientos y estándares para la estrategia de seguridad digital y adopta el modelo de seguridad digital y privacidad de la información (MSPI), para que las entidades públicas implementen medidas técnicas, administrativas y de talento humano que garanticen la seguridad digital. Como sus aspectos claves están la implementación del MSPI, las estrategias de seguridad digital que cada entidad debe desarrollar, la gestión de riesgos e incidentes, y la cultura de seguridad digital. (MinTIC, 2021)

Pruebas de penetración o pentesting

las pruebas de penetración se entienden como la simulación contralada de ataques para la identificación de vulnerabilidad informáticas en sistemas, redes o aplicaciones. Estas pruebas de penetración tienen varias etapas de son la siguientes:

Reconocimiento o recolección de información:

En esta etapa se busca y recopila la mayor cantidad de información sobre el objetivo, sin interactuar directamente con él, una herramienta muy conocida es Maltego, esta es una herramienta de fuentes abiertas y forense, la cual permite la búsqueda de información de diversas fuentes, como perfiles y publicaciones, la herramienta permite cruzar datos para identificar conexiones y relaciones

Escaneo:

Se identifica las versiones del software del objetivo, puertos abiertos o los servicios activos, para comprender la distribución y posibles putos de entrada. Un ejemplo de este tipo de herramientas es Nmap, la cual es de código abierto, se utiliza para el descubrimiento de redes o auditorias de seguridad.

Enumeración y análisis de vulnerabilidades:

Se utiliza para identificar posibles fallos de seguridad, para comparar la información recopilada con bases de datos de vulnerabilidad, analizar la configuración de sistemas y evaluar la seguridad de las aplicaciones web. Un ejemplo es Nessus, esta es una herramienta que ayuda es expertos en seguridad a realizar escaneo de vulnerabilidad y reducir la superficie de ataques en las organizaciones.

Explotación:

En esta etapa, se busca demostrar el impacto real de las vulnerabilidades y evaluar la efectividad de los sistemas de seguridad, evitando posibles daños a los sistemas de los clientes. Un ejemplo, es un framework de pruebas de penetración de código abierto, el cual proporciona información sobre las vulnerabilidades, ayudando a identificar y mitigar riesgos de seguridad.

Post-explotación:

En esta etapa, después de obtener acceso, se analiza la información que se logró obtener, si se puede mantener el acceso y hasta donde se compromete el sistema o la red. Un ejemplo es Meterpreter esta herramienta se utiliza para el control remoto y explotación de sistemas comprometidos, esta facilita la administración y control por parte del atacante.

Limpieza:

En esta etapa se elimina rastros de las actividades realizadas. Un ejemplo es Clearev, esta herramienta permite el borrado de registros en sistemas operativos como Windows.

Reporte:

Esta es la etapa final del pentesting, es esta etapa se documenta detalladamente los hallazgos en el proceso y las vulnerabilidades encontradas, con recomendaciones para corregir las situaciones detectadas. Un ejemplo es Dradis, esta herramienta permite el intercambio de información recopilada durante las pruebas, lo cual facilita la colaboración y obtención de resultados. (Castillo, 2018)

Herramientas de ciberseguridad

Metasploit:

Es un entorno de desarrollo de código abierto, con el cual un profesional en seguridad prueba, ejecuta y desarrolla “exploits” en sistemas vulnerable. Con esta herramienta se puede

imitar ataques reales, probar la efectividad de las medidas de seguridad en las empresas, demostrar el impacto que podría tener la brecha de seguridad, desarrollas nuevos exploits y modelos de ataques personalizados.

Para su uso lo más normal es identificar los sistemas vulnerables, luego se selecciona un exploit apropiado, se configura el exploit objetivo con la IP y otros parámetros, se ejecuta el exploit y se accede al sistema comprometido y realiza las acciones post explotación. (metasploit, 2025).

Nmap:

Es una herramienta de código abierto para escaneo y descubrimiento de redes, muy utilizada por administradores de res y profesionales en ciberseguridad. Con ella se puede descubrir dispositivos en una red, identificar puestos abiertos en máquinas remotas, detectar servicios y versiones de ellos que estén corriendo, descubrir vulnerabilidades básicas y auditar la seguridad de una red.

Con esta herramienta de puede detectar puertos innecesariamente abiertos, validar si los servicios están funcionando correctamente, identificar software obsoleto o mal configurado y automatizar Auditorias de red. (Nmap, 2025)

OpenVas:

Herramienta de escañero de vulnerabilidades de código abierto, diseñada para detectar fallos de seguridad en sistemas, redes y aplicaciones, sirve para buscar vulnerabilidades, auditar la seguridad de redes y servidores, generar reportes y cumplir con normativas y estándares de seguridad, su funcionamiento se soporta en bases de datos de vulnerabilidades (FeeD), escaneo de objetivos, resultados y reportes.

Con ella, se puede detectar servicios desactualizados o inseguros, encontrar configuraciones erróneas, evaluar la exposición de una red ante ataques externos, monitorear la

seguridad de los activos y proteger servidores, bases de datos, aplicaciones y dispositivos IoT. (Greenbone Vulnerability Management, 2025)

ExploitDB:

Se entiende como una base de datos publica y gratis que contiene exploits, herramienta de prueba de seguridad y vulnerabilidades. Su utilidad es investigar vulnerabilidades conocidas en software, sistemas operativos y aplicaciones web, mantener exploits púbicos para pruebas de penetración, aprender técnicas de explotación reales en entornos de laboratorio y desarrollar defensas al saber cómo funcionan los ataques.

Con ExploitDb, se puede consultar si un software tiene vulnerabilidades conocidas, de ellos también se puede descargar y probar exploits en entornos controlados, investigar exploits para escribir scripts personalizados y comparar versiones vulnerables vs versiones parchadas. (EXPLOIT DATABASE, 2025)

CVE

Vulnerabilidades y exposiciones comunes (CVE) es un sistema de identificación estandarizado para las vulnerabilidades de seguridad conocidas en software y hardware. Con esta codificación, se identifican vulnerabilidades de forma universal, esto facilita la comunicación entre expertos en seguridad, se gestionan los parches y actualizaciones en función de los riesgos detectados y evaluar riesgos.

El código CVE funciona de la siguiente manera, primero una empresa o investigador en hacker ético detecta una falla de seguridad, esta vulnerabilidad es reportada en (CVE Nombering Authority) CNA alguna organización que gestiona CVE, la información se verifica y se le asigna un numero CVE y la vulnerabilidad en publicada en alguna organización o base de datos con análisis de impacto. (MITRE Corporation, 2025)

Banco de trabajo

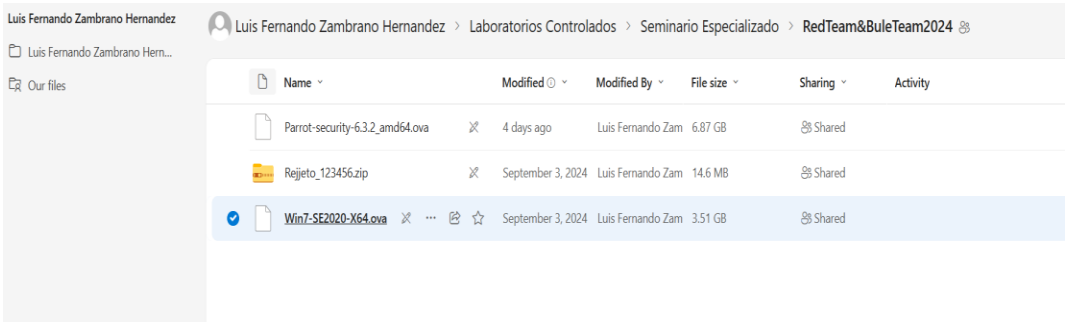
Se descargó la última versión de Oracle VirtualBox

Ilustración 1 Ultima versión de Oracle virtual Box

Fuente: Autor

Se ingresó al foro donde se encuentran las herramientas de trabajo

Ilustración 2 Foro de herramientas de trabajo

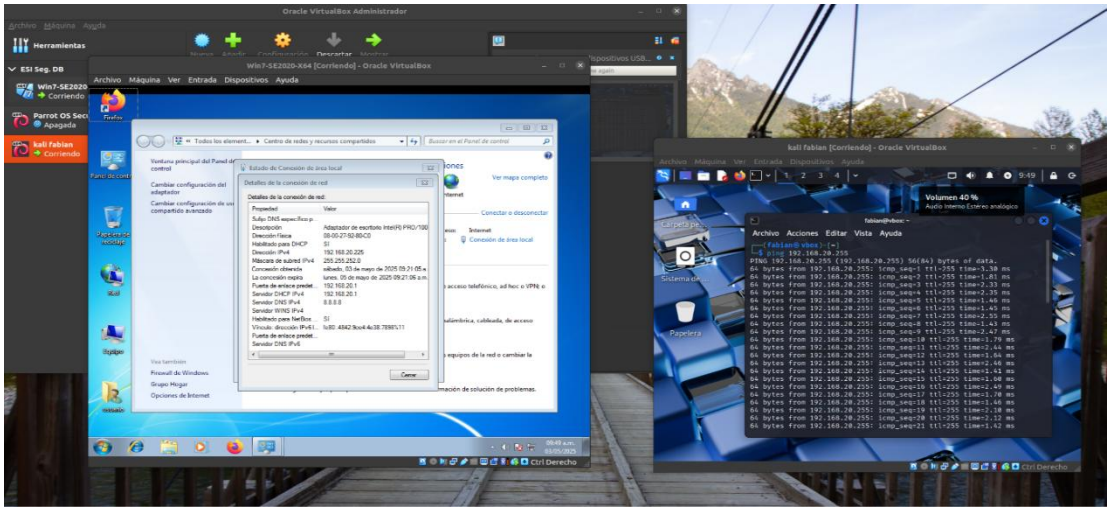


Fuente: Autor

Se realizó la importación de las dos máquinas virtuales de Windows y Kali Linux

Lo primero que se realizo fue la búsqueda del equipo el cual se va a realizar el ataque

Ilustración 3 imagen de la búsqueda del equipo a atacar



Fuente: autor

Se realizó la búsqueda desde Kali Linux y todo desde una máquina virtual instalada.

Después se realizó la instalación del software Nessus, con el cual se creó un scan y se realizó escaneo del computador con sistema operativo Windows 7 como se muestra en la ilustración 2, el cual tenía IP 192.168.20.255

Etapa 2 Actuación ética y legal

Análisis sobre el acuerdo legal CyberFort Technologieses

Revisando el contrato, no se está de acuerdo con varias cláusulas del contrato, dado que una de ella habla sobre confidencialidad sobre procesos ilegales dentro de CyberFort Technologies. Este apartado es abiertamente ilegal y poco ético, pues se está obligando al empleado a ocultar actividades ilegales, esto es penado por ley, más si la organización incurre en accesos abusivos a sistemas informáticos.

Por otra parte, en la cláusula segunda, se habla de información confidencial, en esta reconoce que existen actividades delictivas como chuzadas, lo cual, en el contexto legal del país es una acción gravísima. Por tanto, que este explicito en un contrato es abiertamente ilegal y tratar de protegerla mediante el argumento de confidencialidad, tipifica una obstrucción a la justicia.

En este mismo sentido, en la cláusula tercera ítem 3, fortalecen la idea de silenciar a la parte receptora, así sea en delitos como espionaje o apropiación de información, esto vulnera los derechos y deberes como ciudadano, pues impide la denuncia de delitos.

Por último, en la cláusula octava, la cual habla sobre solución de controversias, se pretende trasladar toda la responsabilidad penal a la persona receptora de la información, aun cuando estas actividades ilegales provienen de la empresa, se considera que esto no solo es totalmente ilegal, sino que además vulnera el derecho fundamental del firmante y lo pone en una situación de riesgo jurídico, sin ningún respaldo legal.

Análisis según artículos de la ley 1273.

De acuerdo con la lectura el anexo 3 incurre en la violación de los siguientes artículos de la ley 1273 del 2009.

El artículo 269A, castiga el acceso abusivo a un sistema informático y este acuerdo no solo admite este delito si no que lo blinda contractualmente. (Ministerio del Interior, 2009).

El articulo 269B, obstaculización ilegítima de sistema informático o red de telecomunicación esta vulnerado, dado que al inferir en sistemas de terceros para obtener datos por espionaje y chuzadas, podría estar entorpeciendo de manera ilegal su funcionamiento y esto es penalizado por este artículo. (Ministerio del Interior, 2009).

El articulo 269C, interceptación de datos informáticos, el acuerdo normaliza y cubre la interceptación de datos, lo que constituye un delito penado por este articulo y esto en Colombia solo se puede realizar mediante orden judicial, esto lo contempla este acuerdo. (Ministerio del Interior, 2009).

El articulo 269D, daño Informático, puede ser que en el acuerdo no aparezca explicitamente la manipulación o modificación de datos obtenidos mediante acceso abusivo, pero si la

información obtenida por CyberFort es alterada o dañada, esto constituiría una conducta tipificada como daño informático. (Ministerio del Interior, 2009).

El articulo 269F, el uso de software malicioso tampoco esta mencionado en el acuerdo, pero se puede interpretar que el espionaje o acceso abusivo se estaría utilizado software especializado para atacar sistemas informáticos. (Ministerio del Interior, 2009).

El articulo 269H, violación de datos personales, dado que la empresa recolecta datos personales sin consentimiento y además prohíbe la denuncia, se estaría violando el derecho a la intimidad y la ley de protección de datos personales. (Ministerio del Interior, 2009).

Procesos poco éticos CyberFort Technologies

No aceptaría el trabajo, dado que la oferta económica no me parece buena, aunque la estabilidad laboral es atractiva, no creo que sea conveniente aceptar el trabajo, dado que implica riesgos jurídicos severos, que podrían afectar mi libertad personal, reputación y fututo laboral, el contrato vitalicio no compensa el riesgo de ser procesado. Además, el acuerdo invalida la posibilidad, de cumplir con los deberes y la ética, esto genera un conflicto directo con las leyes colombianas y los lineamientos éticos planteados por el COPNIA (COPNIA, 2003). Se considera, que la ingeniería se debe ejercer con responsabilidad social y legal, tal como lo definen os lineamiento del COPNIA.

Punto de vista Ciberespionaje y Ética en CyberFort Technologies

¿Hasta qué punto las empresas de ciberseguridad deben tener acceso a información sensible de sus clientes durante una auditoría de seguridad, y cómo se puede garantizar que este acceso no sea explotado de manera indebida?

Como empresa de ciberseguridad, se debe tener acceso limitado y controlado a información sensible, para lograr identificar vulnerabilidades y riesgos, pero esto debe estar claramente

delimitado, supervisado y regulado. Para evitar lo que sucedió en este caso, el contrato establecido, debe tener alcances y límites claros, un consentimiento de auditabilidad, dado que el cliente debe aprobar previamente los procedimientos e informes claros de cada paso para esto utilizar bitácoras y herramientas de monitoreo, todo el personal debe firmar acuerdos de conductas éticas y confidenciales, con sanciones en caso de mal uso de los datos. Ya que los empleados que excedan su autorización deben ser procesador penalmente,

En la ciberseguridad la confianza es tan importante como el conocimiento técnico, para esto las empresas deben establecer marcos solios y actuación ética legal y técnica para lograr que el acceso a sistemas críticos no se convierta en una herramienta de abuso.

¿Qué mecanismos de supervisión y control deberían implementarse en las empresas de ciberseguridad para evitar que sus empleados utilicen herramientas avanzadas de análisis forense con fines no autorizados o éticamente cuestionables?

Los mejores mecanismos de supervisión y control pueden ser los siguientes

- Políticas claras de uso y acceso a herramientas: para esto es importante crear e implementar manuales internos de uso ético y técnico.
- Control de accesos basado en roles (RBAC): los accesos a herramientas forenses se beben configurar bajo principios de mínimos privilegios, dado que solo personal autorizado, bajo objetivos justificados y concretos.
- Auditorías internas y externas: se deben realizar auditorías de seguridad regulares (técnicas y éticas), en estas se deben incluir la verificación de que los accesos fueron registrados, legítimos y justificados.

- Registros y monitoreo de actividades: el uso de herramientas se debe registrar fecha y hora usuario responsable con su caso asignado y su respectiva descripción de lo realizado.
- Capacitación en ética profesional y leyes.
- Canales de denuncia seguros y anónimos: establecer canales internos para que cualquiera pueda reportar actividades sospechosas o violaciones éticas sin represalias, esto acompañado de mecanismos legales y confidenciales.
- Cláusulas contractuales de ética y sanciones
- Segregación de funciones: se debe evitar que una persona tenga control total sobre las operaciones.

¿Cómo deberían responder los gobiernos y organizaciones cuando descubren que una empresa de ciberseguridad contratada ha cometido actos de ciberespionaje? ¿Cuáles serían las medidas adecuadas para restaurar la confianza y asegurar que no ocurra nuevamente

Las medidas a tomar por parte de gobiernos y organizaciones podrían ser

Respuesta inmediata

Aislamiento y contención del incidente: para esto se debe revocar el acceso a las empresas involucradas a los sistemas, también aislar los dispositivos afectados y analizar cada uno de ellos, además activar planes de contingencia y protocolos de respuesta. Notificar a todos los interesados incluyendo autoridades judiciales, auditores externos y usuarios afectados

Acciones legales y de responsabilidad

Iniciar procesos penales y civiles contra la empresa y empleados implicados

Hacer efectivas las cláusulas contractuales para resarcimiento económico, sanciones por incumplimiento o nulidad del contrato

Auditorias y revisiones internas

Revisar que datos fueron accedidos, como se produjo el fallo de control y que vulnerabilidades fueron explotadas.

Restaurar la confianza y prevenciones futuras

Reformular políticas de contratación para esto implantar algo más estricto de verificación de antecedentes técnicos, legales y éticos.

Fortalecer la gobernanza TI mediante comités de ética y seguridad

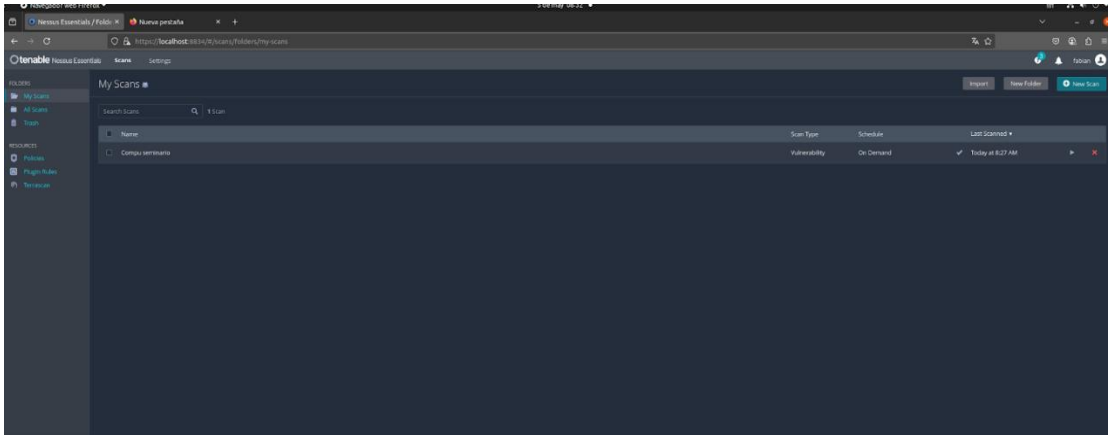
Transparencia y comunicación para esto publicar de forma responsable y transparente los hechos descubiertos y mostrar las acciones legales tomadas con sus medidas implementadas.

Etapa 3 ejecución pruebas de intrusión

Continuando con el banco de trabajo ya puesta en marca en capítulos anteriores se realizó lo siguiente:

Después se realizó la instalación del software nessus con el cual se creó un scan y se realizó escaneo del computador con sistema operativo Windows 7 como se muestra en la ilustración 2 el cual tenía ip 192.168.20.255

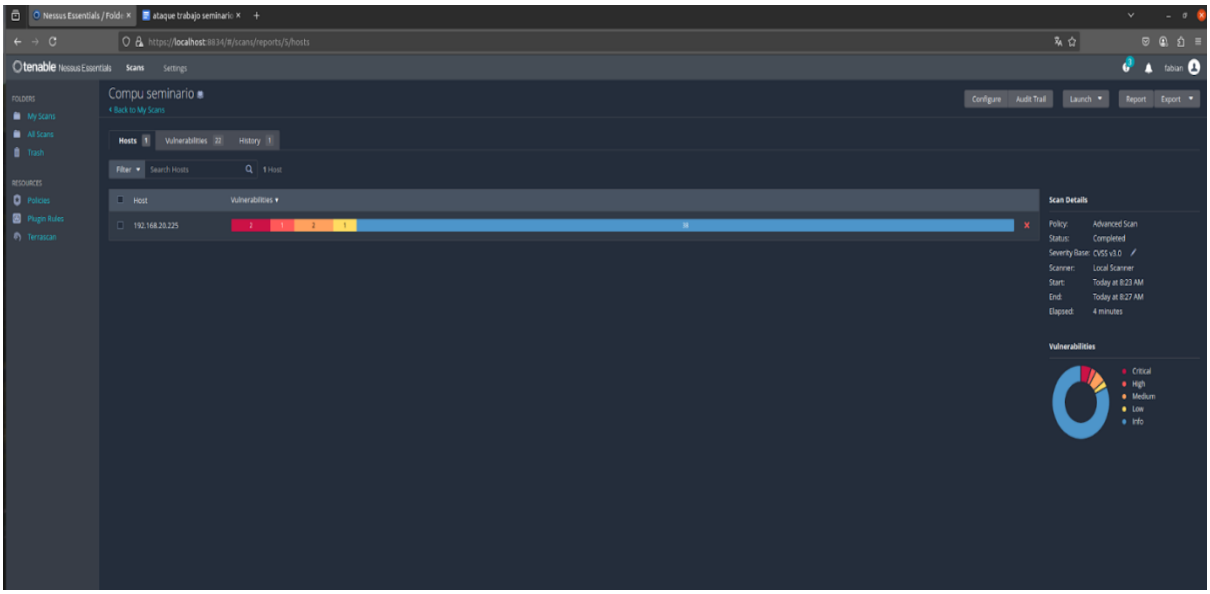
Ilustración 4 creación de scan



Fuente: Autor

Después de realizado el escaneo que evidencio las vulnerabilidades encontradas en el sistema operativo como se evidencia en la ilustración 3 en la cual de muestran 22 vulnerabilidades

Ilustración 5 vulnerabilidades encontradas

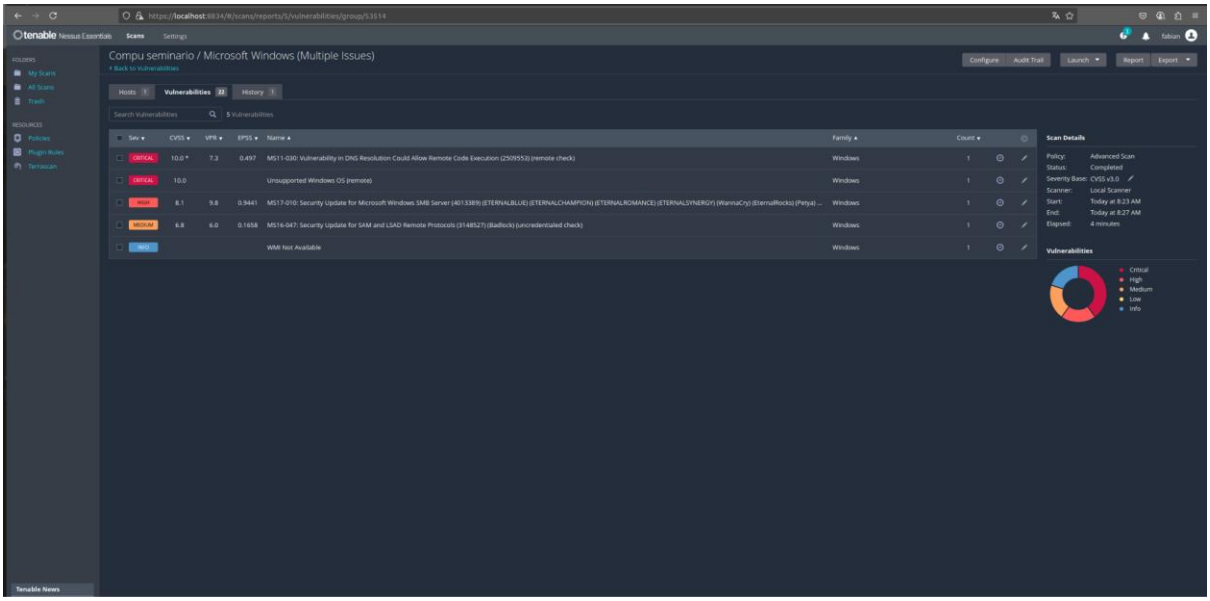


Fuente: Autor

Ilustración 6 muestra de todas las vulnerabilidades encontradas

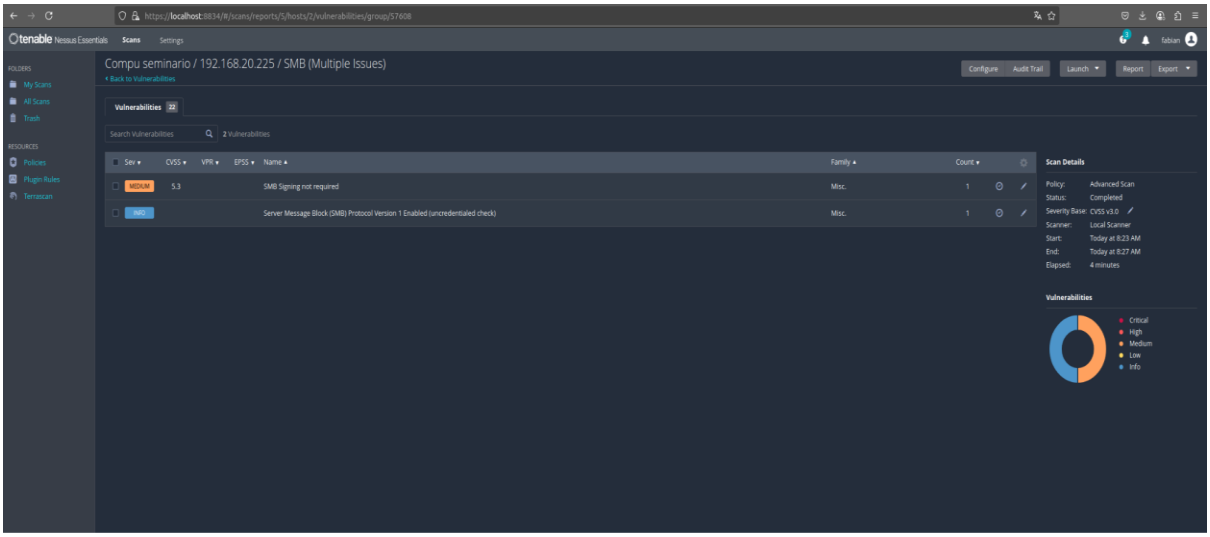
Fuente: Autor

Ilustración 7 vulnerabilidades más importantes



Fuente: Autor

Ilustración 8 vulnerabilidades nivel medio

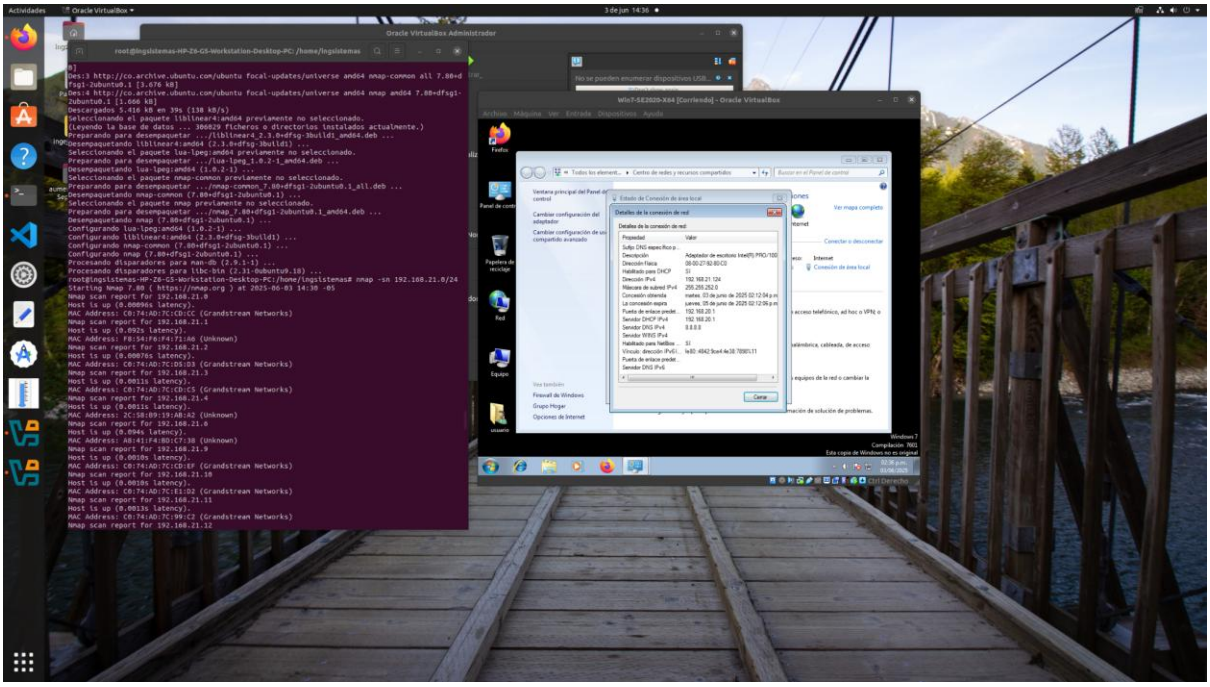


Fuente: Autor

Con la herramienta Nessus se encontraron 22 vulnerabilidades de las más importantes se evidencia las siguientes

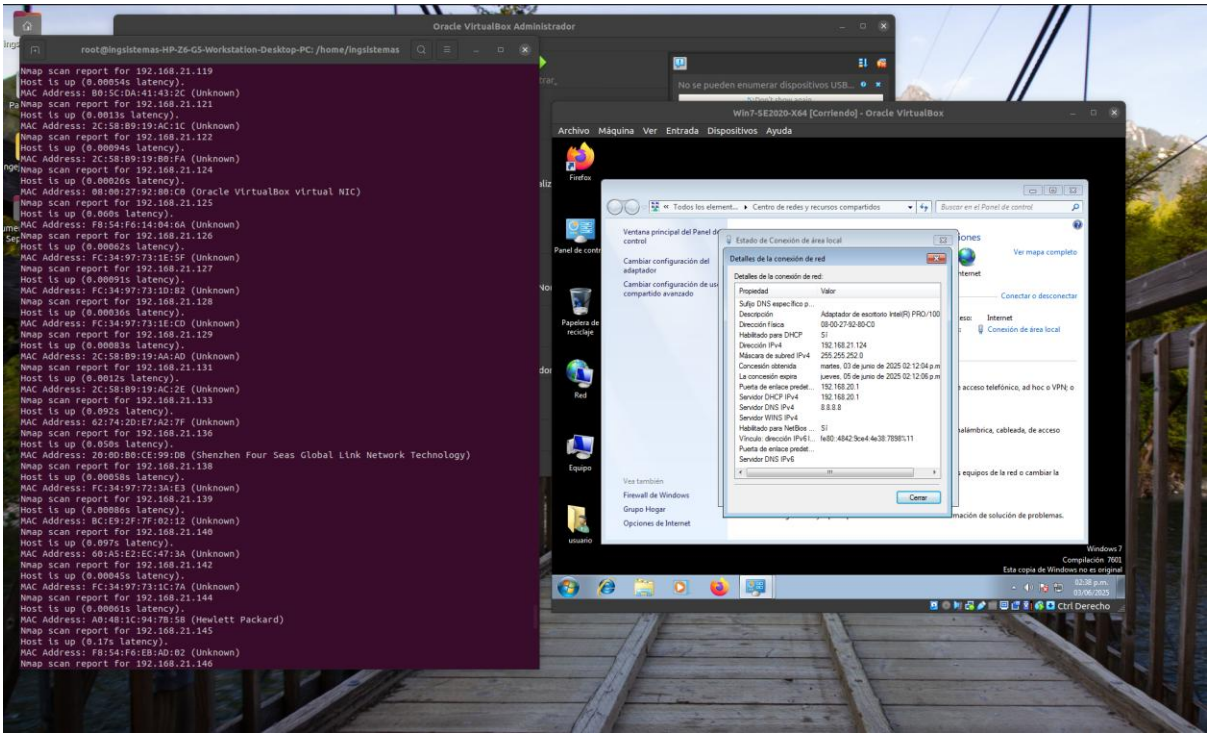
Aquí busco lo maqui con Nmap

Ilustración 9 Buscando maquina con Nmap



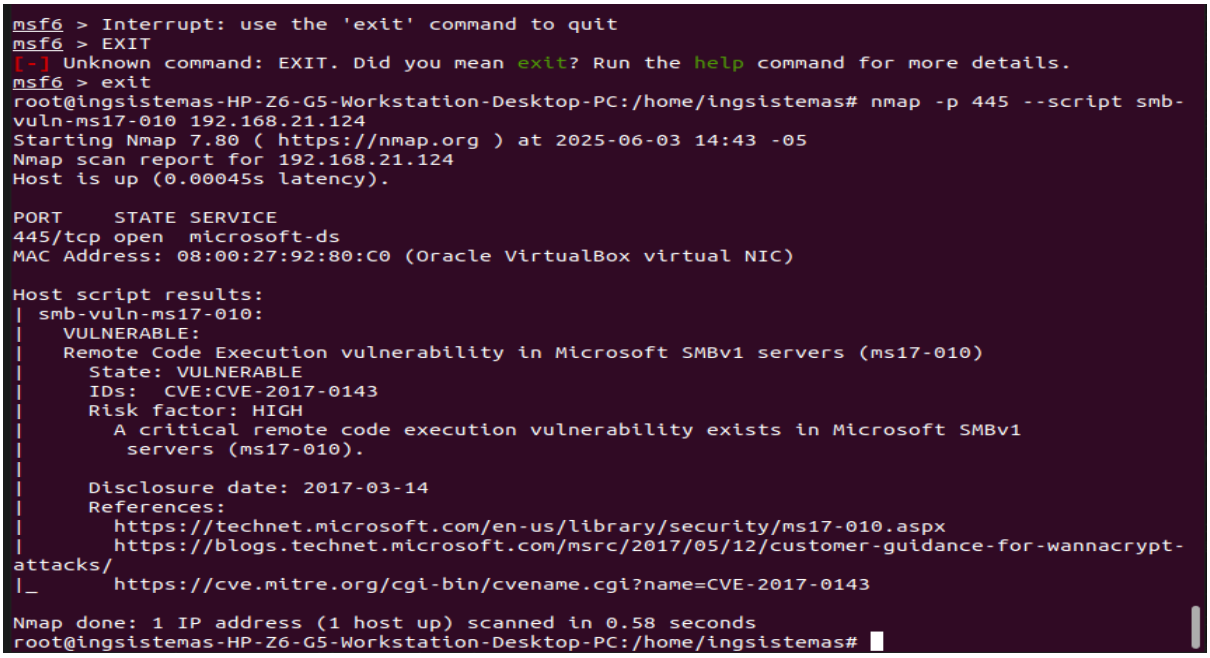
Fuente: Autor

Ilustración 10 maquina encontrada con IP 192.168.21.124



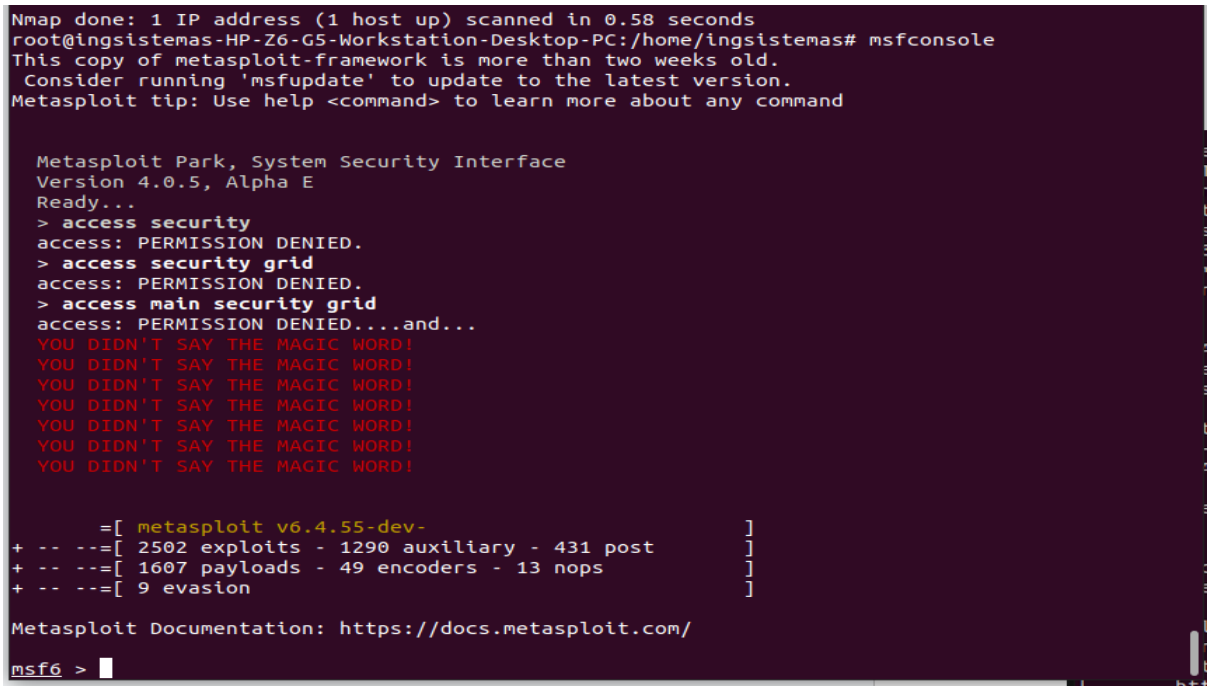
Fuente: Autor

Ilustración 11 vulnerabilidad encontrada



Fuente: Autor

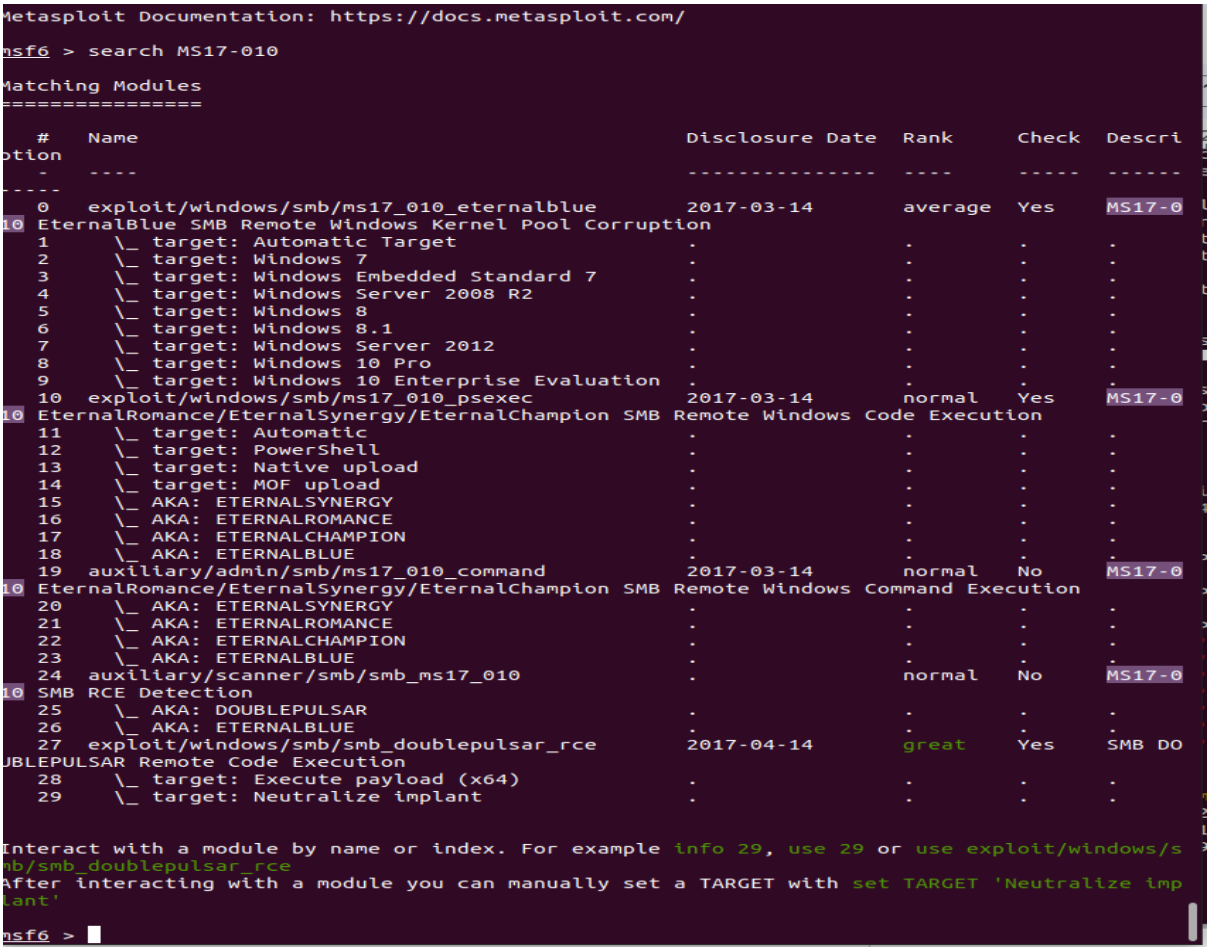
Ilustración 12 ingresando a la consola



Fuente: Autor

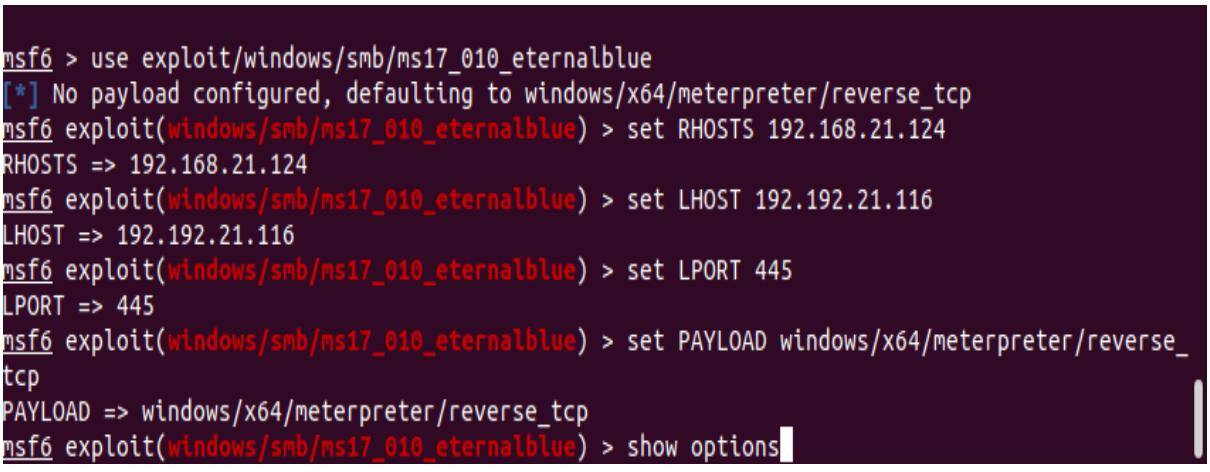
Mas vulnerabilidades visibles

Ilustración 13 MS17-010



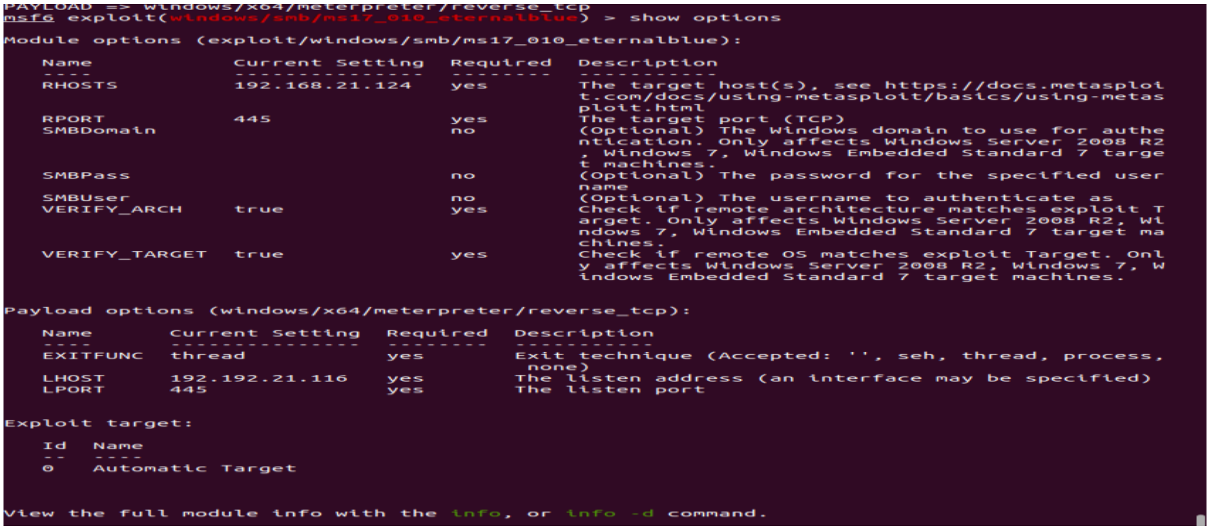
Fuente: Autor

Ilustración 14 Tomando el control



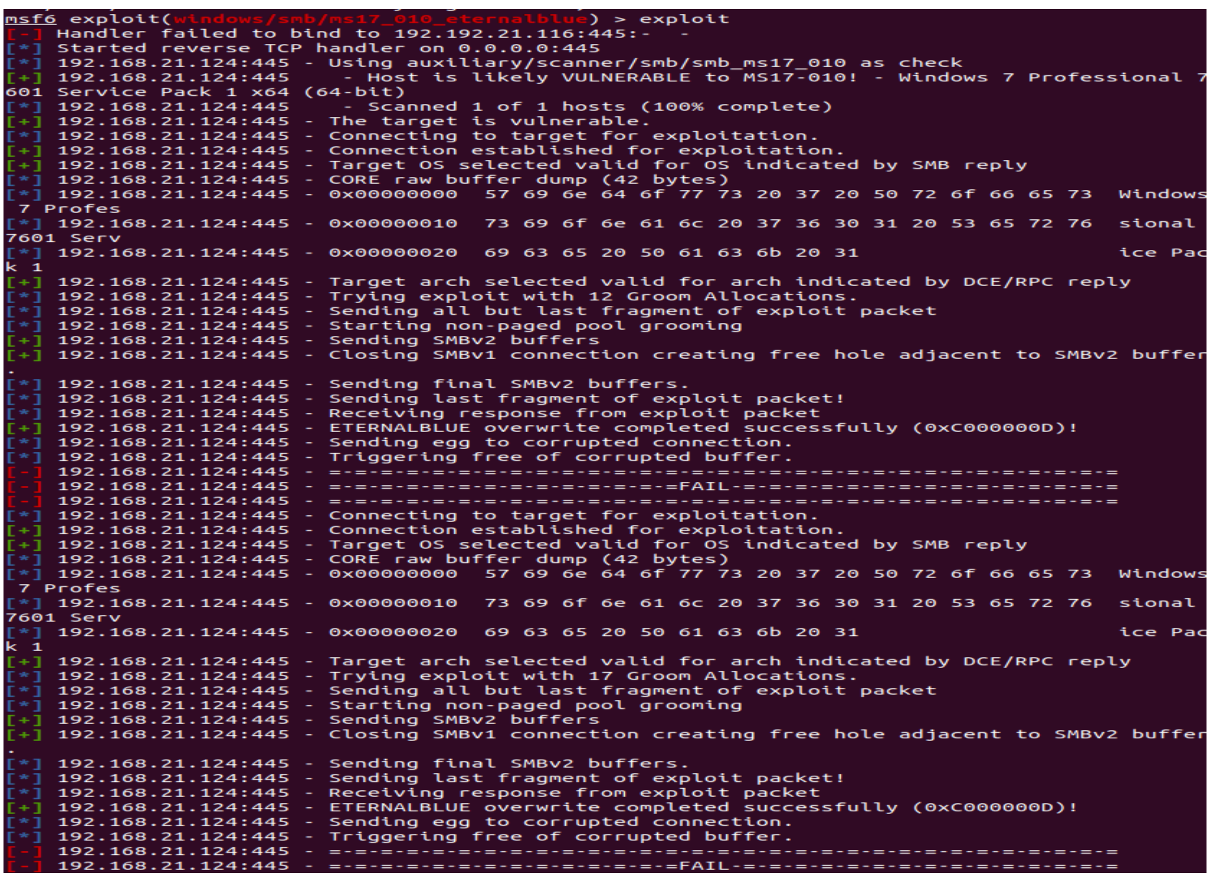
Fuente: Autor

Ilustración 15 ingresando a la maquina



Fuente: Autor

Ilustración 16 realizando el exploit



Fuente: Autor

CVE-2016-0128

“se refiere a una falla de seguridad en Microsoft Windows, específicamente en el componente Win32k.sys, que es parte del kernel del sistema operativo.

La vulnerabilidad permite a un atacante ejecutar código arbitrario en modo kernel. Un atacante que logre explotar esta vulnerabilidad podría instalar programas, ver, cambiar o eliminar datos, o crear nuevas cuentas con todos los privilegios

Tipo de vulnerabilidad: Escalada de privilegios (Privilege Escalation), Requiere que un atacante ejecute una aplicación especialmente diseñada en el sistema vulnerable.” (NVD, 2025)

CVE-2017-0143

“es una falla crítica en Microsoft Windows, relacionada con el protocolo SMBv1 (Server Message Block version 1). Es una de las vulnerabilidades más peligrosas de la última década debido a su uso en ataques globales como WannaCry.

Tipo: Ejecución remota de código (Remote Code Execution, RCE).

Componente afectado: SMBv1 (protocolo de red para compartir archivos e impresoras).

Descripción: Permite a un atacante remoto ejecutar código malicioso sin autenticación, simplemente enviando paquetes SMB especialmente diseñados a un sistema vulnerable.

Apodo del exploit: EternalBlue, desarrollado originalmente por la NSA y filtrado por el grupo Shadow Brokers.

Impacto: Control total del sistema afectado.” (NVD, 2025)

CVE-2017-0144

“también es parte del conjunto de fallos explotados por el famoso EternalBlue, igual que CVE-2017-0143, y es una de las más críticas de la historia reciente por su impacto masivo.

Tipo: Ejecución remota de código (Remote Code Execution - RCE).

Componente afectado: Microsoft SMBv1 server.

Vector de ataque: El atacante envía paquetes especialmente manipulados a través del puerto TCP 445.

Explotación pública: Sí, usada en ataques reales

Impacto: Permite a un atacante ejecutar código con privilegios del sistema, No requiere autenticación

Un atacante puede aprovechar esta falla para ejecutar código arbitrario en la máquina objetivo, lo que permite:

Propagación automática entre equipos vulnerables.

Instalación de ransomware o malware sin interacción del usuario.” (NVD, 2025)

CVE-2017-0145

“es otra de las fallas incluidas en el famoso boletín MS17-010 de Microsoft, que corrige múltiples vulnerabilidades críticas en el protocolo SMBv1 (Server Message Block versión 1). Esta en particular también está relacionada con el conjunto de herramientas de la NSA filtradas por Shadow Brokers.

Tipo: Ejecución remota de código (RCE).

Componente afectado: Microsoft Windows SMBv1 Server.

Vector de ataque: A través del puerto TCP 445, utilizando paquetes SMB malformados.

Severidad: Crítica No requiere autenticación para ser explotada.

Un atacante remoto podría: Ejecutar código arbitrario con privilegios de sistema.

Instalar programas, robar datos o controlar completamente el equipo afectado.

Propagarse lateralmente a otras máquinas en la red.” (NVD, 2025)

CVE-2017-0146

"es parte del mismo conjunto de fallos descritos en el boletín de seguridad MS17-010, que corrigió múltiples vulnerabilidades críticas en el protocolo SMBv1 (Server Message Block versión 1) de Microsoft Windows. Aunque menos conocida que CVE-2017-0143 o 0144, también es peligrosa.

Tipo: Divulgación de información (Information Disclosure).

Vector de ataque: Remoto, a través de paquetes SMB especialmente diseñados.

Severidad: Importante, aunque no tan crítica como las de ejecución de código. No requiere autenticación para explotarse.

Esta vulnerabilidad permite a un atacante remoto obtener información del sistema afectado, como: Fragmentos de la memoria del kernel, Datos internos del sistema que pueden ayudar a desarrollar exploits más peligrosos (por ejemplo, para escalada de privilegios o RCE), Detalles que pueden ayudar a evadir protecciones (como ASLR)." (NVD, 2025)

CVE-2017-0147

"es otra de las siete fallas incluidas en el boletín MS17-010 de Microsoft, todas relacionadas con el protocolo SMBv1 (Server Message Block versión 1). Aunque no es tan ampliamente conocida como CVE-2017-0143 (EternalBlue), sigue siendo significativa.

Tipo: Remote Code Execution (RCE) — Ejecución remota de código.

Vector de ataque: Remoto, a través de paquetes SMB manipulados.

Severidad: Crítica.

Requiere autenticación: No.

Puerto implicado: TCP 445.

Un atacante remoto sin necesidad de credenciales puede: Ejecutar código arbitrario en el sistema afectado, obtener control total del dispositivo y usar el sistema como punto de entrada para comprometer toda la red.” (NVD, 2025)

CVE-2017-0148

“es la última del conjunto de siete vulnerabilidades corregidas por Microsoft en el boletín de seguridad MS17-010, todas relacionadas con el protocolo SMBv1 de Windows. A diferencia de otras como EternalBlue (CVE-2017-0143), esta vulnerabilidad se clasifica como una falla de validación de entrada que puede llevar a ejecución remota de código.

Tipo: Ejecución remota de código (Remote Code Execution - RCE).

Severidad: Crítica.

Vector de ataque: Un atacante remoto puede enviar paquetes SMB manipulados al servidor vulnerable.

Requiere autenticación: No.

Un atacante remoto puede: Ejecutar código arbitrario con los privilegios del sistema, tomar control completo del equipo afectado y usar el sistema comprometido como punto de entrada para ataques en la red interna.” (NVD, 2025)

CVE-2011-0657

“afecta a Microsoft Internet Explorer y fue publicada en 2011. A continuación, te detallo los aspectos clave:

Tipo: Corrupción de memoria (Memory Corruption) puede derivar en Ejecución remota de código (RCE).

Severidad: Crítica

Descripción: La vulnerabilidad se encuentra en la forma en que IE procesa contenido web (por ejemplo, al renderizar ciertos elementos HTML o JavaScript).

Un atacante puede diseñar una página web maliciosa que, al ser visitada por la víctima, provoque corrupción de memoria lo cual puede permitir la ejecución de código arbitrario con los privilegios del usuario que ejecuta el navegador". (NVD, 2025)

CVE-1999-0524

"es una de las entradas más antiguas del catálogo CVE y describe una configuración insegura en servicios de red. No se refiere a un error de software específico, sino a una mala configuración de seguridad.

Tipo: Weak Security Configuration / Misconfiguration

Componente afectado: SNMP (Simple Network Management Protocol)

Severidad: Media a alta, dependiendo del entorno.

Descripción:

El sistema tiene habilitado el protocolo SNMP y utiliza una cadena de comunidad (community string) predeterminada o conocida, como:

"public" (solo lectura)

"private" (lectura/escritura)

SNMP se usa para administrar y monitorear dispositivos de red (switches, routers, servidores).

Si se dejan las credenciales por defecto (como "public"), un atacante puede: Ver información sensible del sistema (IP, usuarios, procesos, etc.), en algunos casos, modificar configuraciones si tiene acceso de escritura ("private"), Usar esta información para lanzar ataques más avanzados (por ejemplo, escalada o movimientos laterales en la red)" (NVD, 2025)

Etapa 4 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.

Al evidenciar un ataque en tiempo real sobre el equipo Windows analizado en el anterior informe por tal motivo los pasos a seguir serían los siguientes:

Aislar el sistema comprometido:

Esta acción de desconectar el computador de la red física o deshabilitar su red desde el administrador del sistema, esto lo realizaría dado que en el informe de vulnerabilidades dos de ellos CVE-2017-0143 y CVE-2017-0144, da vulnerabilidad a múltiples ataques remotos ya que este permite ejecución remota de código sin autenticación, esto implicaría que podrían controlar el sistema completamente y replicar al ataque a otros equipos si no se contiene de manera inmediata. (NVD, 2025)

Recolectar evidencia:

Recolectar información crítica como conexiones de red activas, sesiones abiertas y procesos de ejecución antes de reiniciar o apagar el computador para esto utilizaría comandos como netstat -ano (estadísticas de red) ya que este código me permite visualizar las conexiones activas, entrantes como salientes, los estados de los puertos y las interfaces de red. (IBM, 2025)

Ya que los ataques como EternalBlue (explotación SMB) implica cargas útiles cargadas a memoria podría capturar evidencia volátil, procesos sospechosos y posibles indicadores de compromiso. (Burdova, 2020)

Análisis de log del sistema:

Revisar los eventos recientes en el visor de eventos de Windows, directamente en los registros de seguridad, sistemas y aplicaciones. Dado que las vulnerabilidades detectadas podrían

haber sido explotadas sin interacción del usuario. El análisis de los eventos podría revelar intentos de accesos remoto, instalación de servicios maliciosos o modificaciones en la configuración del sistema

Verificar la integridad del sistema:

Realizar una comparación del estado actual del sistema como una línea base confiable y ejecutar herramientas de detección de rootkits o malware. Dado que el informe anterior señala vulnerabilidades que permiten al atacante instalar programas, eliminar datos o crear cuentas (CVE-2016-0128) esto hace necesario verificar si se han introducidos cambios en archivos críticos del sistema. (NVD, 2025)

Evaluaciones de vulnerabilidades explotadas:

Realizar identificación de las vulnerabilidades conocidas que fueron utilizadas. Dado que en el informe anterior las múltiples vulnerabilidades críticas, conocer cuales fueron explotadas permite priorizar acciones correctivas específicas.

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

Dado que CyberFort Technologies con su equipo BlueTeam considera que las medidas de hardenización deberían enfocarse en cerrar brechas conocidas, eliminar configuraciones obsoletas y reducir la superficie d ataque de la siguiente manera: (ISN, 2025)

Actualización o remplazo de sistemas operativo:

Migrar de Windows 7 a una versión soportada como Windows 10 o 11 que tiene activas sus actualizaciones.

Deshabilitar el protocolo SMBv1

Eliminar el soporte SMBv1 desde las características de sistemas o mediante ´PowerShell. Este protocolo es obsoleto, inseguro y fue el vector principal del ataque.

Aplicar parches de seguridad y actualizaciones del sistema:

Es necesario establecer un sistema de actualizaciones automatizado o centralizado como por ejemplo WSUS (Windows Server Update Services).

Configurar y reforzar políticas de firewall:

Tomar medidas como bloquear puestos de red innecesario como, por ejemplo

- Puerto TCP 445 (SMB)
- Puerto UDP 137/138, TCP 139 (NetBIOS)

Dado que el ataque fue posible por el acceso libre a estos puertos, limitar el puerto reduce drásticamente las vías de entrada para ataques remotos.

Modificar configuraciones inseguras en servicios SNMP

Cambiar las configuraciones que están por defecto, aplicar listas de comunicaciones de control de acceso y si es necesario usar SNMPv3

Deshabilitar servicios y funciones innecesarias

Revisar o detener servicios como: Telnet, servicios de escritorio remoto y comparticiones innecesarias de red. Ya que estas representan una posible entrada al sistema.

Implementar control de aplicaciones y listas blancas

Implementar la utilización de herramientas como Applocker con esto se lograría que aplicaciones no autorizadas se ejecuten incluso si logran ingresar al sistema.

Monitoreo y detección de intrusos

Realizar implementaciones como Microsoft Defender for Endpoint que analice eventos de seguridad.

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

Las diferencias entre un BlueTeam y un equipo de respuestas a incidentes informáticos (IR Team) es complejo dado que los dos equipos tiene objetivos entrelazados pero no son lo mismo, las principales diferencias podrían ser, que el equipo BlueTeam se centra en la protección continua de una organización y el IR Team está más orientado a mitigar incidentes de seguridad una vez que ocurren, pero también el BlueTeam realiza tareas como configuración de IDS/IPS, firewall y parches de seguridad aparte de auditorías de vulnerabilidades y capacitación a empleados mientras en el IR Team se activa durante un incidente y sigue un proceso estructurado. El BlueTeam opera de manera continua y trabajan a largo plazo, pero el IR Team actúa de manera específica y temporal y la principal diferencia es que el IR Team entra a trabajar cuando las defensas del BlueTeam son superadas.

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

Si una de las indicaciones al BlueTeam es que se debe trabajar con CIS lo utilizaría principalmente para aplicar guías de hardenización y mejores prácticas de seguridad estandarizadas:

Endurecer la hardenización de sistemas y configuraciones

Para deducir el área de ataques en los sistemas operativos, aplicaciones y dispositivos de red

Establecer una línea base de seguridad

Esto para definir una configuración segura mínima para servidores y estaciones de trabajo

Establecer el cumplimento

Esto para verificar si los sistemas cumplen con estándares de seguridad conocidos

Facilitar la respuesta ante auditorías externas

Esto se hace para que la organización sigue estándares internacionales de seguridad

Automatizar la seguridad desde el despliegue

Integrar las recomendaciones CIS en plantillas de configuración

Todo esto se hace para implementar y mantener configuraciones seguras como guía técnica confiable. (CalCom, 2025)

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

Las funciones y características principales de SIEM cuyo propósito principal es proporcionar una visión centralizada y en tiempo real de la seguridad de una organización son:

Recolección y centralización de logs:

Recopila registros de eventos logs desde múltiples dispositivos y sistemas en tiempo real para centralizarlos en una única plataforma facilitando su gestión y análisis.

Correlación y análisis de eventos:

Utilizas reglas predefinidas, algoritmos de machine learning y análisis de comportamiento para correlacionar eventos aparentemente inconexos y detectar patrones que indique posibles amenazas.

Detección de amenazas en tiempo real:

Monitorear continuamente los eventos y generar alertas inmediatas cuando detectan actividades sospechosas para que lo equipos BlueTeam reacciones rápidamente a incidentes.

Respuesta a incidentes:

La idea es facilitar la investigación a incidentes al proporcionar herramientas para retrasar el origen, impacto y cronología de un evento de seguridad.

Gestión de cumplimiento normativo:

Generar reportes y auditorias detalladas para demostrar el cumplimiento con regulaciones y estándares de seguridad.

Análisis forense:

Lo que se espera es proporcionar capacidades para realizar investigaciones post - incidentes, permitiendo a los analistas reconstruir eventos, identificación de la causa raíz del ataque y recopilar evidencia para acciones legales.

Visualización y reportes

Creación de dashboards para mostrar el estado de las seguridad, tendencias y métricas claves (IBM, 2025)

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

pfSense

es una solución de firewall y enrutador, que se utiliza para gestionar tráfico de red y aplicar políticas de seguridad estrictas

- alistamiento de redes
- bloqueo de tráfico malicioso
- limitaciones de acceso (pfSense, 2025)

Fail2Ban

Es una herramienta diseñada para proteger servidores contra ataques de fuerza bruta y otros intentos maliciosos al analizar logs y aplicar reglas de bloqueo automática

- Bloque automático de IPs maliciosas
- Reducción de impacto
- Respuesta dinámica (Ken Hess, 2020)

OPNsense

Es un firewall y enrutador de código abierto que permite crear zonas de red aisladas, bloqueo de tráfico y permite limitar conexiones entrantes y salientes

- Segmentación de red
- Filtrado de trafico
- Gestión de accesos (OPNsense, 2025)

Etapa 5 socialización de informe técnico

Aspectos que aporten al desarrollo de estrategias de RedTeam & BlueTeam

Aspectos que presento a continuación son claves para el desarrollo y fortalecimiento de estratégicos Red Team y Blue Team

RedTeam (Ataque / simulación)

Lograr simulaciones de ataques reales con el fin de evaluar la postura de seguridad de la organización desde la perspectiva de un antagonista.

1. **Planificación y alcance:**

   En la primera etapa es necesario establecer los límites, objetivos y expectativas de las pruebas de penetración. Definir que se va a avaluar (redes o sistemas), y sus objetivos específicos ejemplo accesos a bases de datos, filtración información

financiara), que acciones están permitidas y cuales no, un cronograma y los entregables del proyecto.

2. **Reconocimiento y recolección de información:**

   Realizar investigación pasiva ósea sin interacción directa y luego una investigación activa con interacción controlada para identificar vectores de ataques potenciales, la idea es buscar información sobre la organización objetivo como:

   - Identificación de servicios y puertos abiertos
   - Descubrimiento de subdominios y direcciones IP
   - Información sobre empleados
   - tecnologías utilizadas.

3. **Modelado de Amenazas y planificación de ataques:**

Al tener la información recopilada, se evalúa vectores que son más probables o críticos para lograr los objetivos. Se planea las técnicas a utilizar, emulando el comportamiento de adversarios reales.

4. **simulación de ataques realistas y ejecución de tácticas técnicas y procedimientos (TTPs):**

El RedTeam ejecuta los TTPs planeados para lograr comprometer los sistemas y alcanzar los objetivos. Esto va más allá de solo encontrar vulnerabilidades, busca explotarlas de manera controlada y demostrar el impacto. (VPN Unlimited, 2025)

5. **Evasión de defensas:**

Un RedTeam efectivo debe ser capaz de eludir las soluciones seguridad existente de las organizaciones para probar que tan fuertes son.

6. **Uso de herramientas avanzadas:**

El RedTeam utiliza herramientas especializadas para llevar a cabo sus simulaciones de manera efectiva.

7. **Reporte con enfoque constructivo:**

El objetico principal del RedTeam no es “ganar”, si no ayudar el BlueTeam a mejorar un informe detallado es el entregable más importante.

BlueTeam (defensa y respuesta a incidentes)

Lograr detectar, responder y mitigar ataques en curso y futuros, protegiendo los activos de las empresas u organizaciones.

1. **Monitoreo continuo y visibilidad completa:**

Una visibilidad de lo que ocurre en todos los activos de información es fundamental para detectar actividades sospechosas en tiempo real.

2. **Detección basada en comportamientos y correlación de eventos:**

Aún más allá de las firmas, el BlueTeam busca patrones de comportamiento anómalos que puedan indicar un ataque.

3. **Gestión de vulnerabilidades proactivas y fortalecimiento:**

Lograr identificar y corregir vulnerabilidades antes de que sean explotadas reduce drásticamente el área de ataques.

4. **Respuesta a incidentes:**

Contar con un plan de acciones bien definido y ensayado para cuando ocurra un incidente de seguridad.

5. **Caza de amenazas:**

Realizar una búsqueda proactiva y manual de amenazas que han podido eludir los sistemas de detección automatizados.

6. **Seguridad en profundidad:**

   Lograr no depender de una unida línea de defensa, si no implementar múltiples capas de seguridad para ralentizar y dificultar el avance de un atacante.

7. **Inteligencia de amenazas**

   Conocer las amenazas más relevantes para la organización, incluyendo los TTPs de los atacantes. Las vulnerabilidades emergentes y los vectores de ataque comunes, permitirían al BlueTeam priorizar sus defensas e implementar o crear contramedidas proactivas.

Aspectos comunes y de colaboración (Purple teaming)

Lograr mejorar la comunicación y el aprendizaje continuo de RedTeam y BlueTeam, optimizando la postura de seguridad de las organizaciones.

1. **Simulación conjuntas y ejercicios (purple Team)**

   Al realizar estos ejercicios fusionan las capacidades del RedTeam y BlueTeam en tiempo real. Al hacer que el RedTeam ejecute TTPs específicos mientras el BlueTeam intenta detectarlos y responder. Esto permitiría un ajuste y mejorar inmediatamente las herramientas, reglas y procesos de defensa (Picus Security, 2025)

2. **Evaluaciones basadas en MITRE&ATTA**

   Tener en cuenta que al proporcionar un lenguaje en común y una metodología estandarizada para evaluar la capacidad de detección contra TTPs de adversarios reales (MITRE ATT&CK, 2025).

3. **Automatización de ataques/ detección para pruebas**

   Permite probar y lograr validar la efectividad de los controles de forma repetible y a escala.

4. **KPIs (Key Performance Indicators) y métricas de seguridad claros:**

   Medir el rendimiento de ambos equipos y la mejora general con respecto a la seguridad de las empresas u organizaciones (Sydle, 2023).

5. **Cultura y mejora continua y "Lessons Learned":**

   Cada ejercicio de RedTeam, cada incidente real, debe ser una oportunidad para aprender y mejorar

Recomendaciones y estrategias para endurecer los aspectos de seguridad en una organización

Aunque el endurecimiento (hardening) de la seguridad en una organización o empresa es un proceso continuo requiere de una estrategia bien definida por eso se plantean una serie de recomendaciones claves para planear estrategias en el endurecimiento de la seguridad de las organizaciones

Evaluación y establecimiento de una línea base

Diagnostico integral de la postura actual: antes de endurecer, primera se debe saber dónde se está, realizar una evaluación completa de la seguridad actual incluyendo auditorias de seguridad, pruebas de penetración, escaneos de vulnerabilidad, análisis de la configuración de sistemas y revisión de políticas existentes.

Identificación de activos críticos y priorización de riesgos: ya que no todos los activos tienen el mismo valor. Identificar cuáles son los datos, sistemas y procesos más críticos para la operación y misión de la organización. Para después priorizar los riesgos asociados a estos activos.

Definición de objetivos de seguridad claros y medibles: establecer metas claras y medibles con plazos definidos para el endurecimiento.

Estrategias de endurecimiento técnico

Implementación de políticas de hardening de configuración: establecer estándares de configuración segura en los sistemas operativos, bases de datos y dispositivos de red. Esto incluye deshabilitar servicios innecesarios, cambiar contraseñas predeterminadas y aplicar principios de mínimo privilegio.

Gestión proactiva de vulnerabilidades y parcheo: crear un ciclo de vida robusto para la gestión de las vulnerabilidades, escaneo regular, priorización de vulnerabilidades según riesgos, aplicación de parches y verificación de la corrección.

Segmentación de red y microsegmentación: divide la red en segmentos más pequeños y aislados limitando la comunicación entre ellos.

Implementación de autenticación multifactor: exigir para todos los accesos de sistemas críticos, VPNs, servicios en nube y aplicaciones sensibles

Control de accesos basado en el rol (RBAC) y principios de mínimo privilegio: otorgar a los usuarios y sistemas solo los permisos necesarios para la realización de su trabajo. Revisando y revocando periódicamente los privilegios.

Cifrado de datos en reposo y en tránsito: cifrar datos sensibles en almacenamiento y durante la transmisión.

Estrategias de endurecimiento y procesos y personas

Desarrollo e implementación de políticas y procedimientos de seguridad: crear y actualizar regularmente políticas de seguridad que abarquen desde el uso de recursos hasta la gestación de contraseñas, la respuesta a incidentes y el uso de dispositivos personales.

Programación de conciencia y capacitación continua en seguridad: realizar capacitaciones regulares sobre seguridad para todo el personal, incluyendo temas de phishing, ingeniería social, gestión de contraseñas y el manejo seguro de información.

Gestión de identidades y accesos (IAM) centradas: implementar sistemas centrados para gestionar las identidades de los usuarios y sus derechos de accesos a todos lo recursos de la empresa.

Planes de Respuesta a Incidentes (IR) y Continuidad del Negocio (BCP) Probados: desarrollar planes detallados para detectar, contener, y recuperase de incidentes de seguridad.

Auditorías de Seguridad Regulares e Independientes: contratar a terceros independientes para realizar auditorías de seguridad periódicas.

Integración y mejora continua

Adopción de un marco de Ciberseguridad (NIST CSF, ISO 27001): implementar un marco de ciberseguridad reconocido internacionalmente para estructurar el programa de seguridad de la empresa u organización.

Cultura de seguridad en toda la organización: fomentar la cultura donde la seguridad es responsabilidad de todos desde la alta dirección hasta el empleado de menor rango.

Conclusiones Clave para la Construcción del Conocimiento en Ciberseguridad

La ciberseguridad en un campo dinámico y de aprendizaje continuo: dado que las amenazas de ciberseguridad están en constante evolución, con nuevos vectores de ataque, malwares y técnicas de ingeniería social saliendo continuamente, esto exige que el conocimiento en ciberseguridad nos sea un estado final, lo contrario es un proceso de aprendizaje, adaptación y

actualización permanente, esto hace que se deba tener una mentalidad de estudiante perpetuo invirtiendo en formación continua.

El conocimiento debe ser holístico ósea más allá de lo técnico: si es cierto las habilidades técnicas son fundamentales el conocimiento efectivo en ciberseguridad se construye integrando aspectos legales, éticos, de procesos de negocios y comportamiento humano. Es necesario desarrollar una comprensión interdisciplinaria donde los expertos en ciberseguridad entiendan el impacto de sus decisiones en el negocio y viceversa.

La colaboración entre los equipos es el pilar de la mejora continua: la efectividad de un programa de ciberseguridad no se mide por la fortaleza de una sola persona o un solo equipos bien sea el BlueTeam o el Redteam. La interacción constante, retroalimentación y los ejercicios de purple team son muy importantes para la identificación de brechas y mejorar las estrategias de defensa ya que el conocimiento se construye colectivamente.

El enfoque en procesos y políticas endurecen la postura de seguridad: las mejores herramientas y tecnologías no son eficaces sin políticas y procedimientos claros. El endurecimiento de los sistemas de protección requiere la aplicación de estándares, auditorias continuas y una cultura de seguridad.

La ciberseguridad es una responsabilidad compartida y social. Dado que la protección de datos y la seguridad informática no recaen únicamente en los equipos de seguridad de la información. Cada usuario desde el gerente hasta el empleado de más bajo rango son un posible vector de ataque y un punto de defensa. La conciencia y la educación son herramientas poderosas para mitigar los riesgos.

Enlace video informe Técnico

https://drive.google.com/drive/folders/1_8v5mtUuxqAFBXyv86PQyzYUKBi9OT2w?usp=drive_link

Conclusiones

Se logro identificar el análisis de vulnerabilidades mediante Nessus para reconocer las múltiples vulnerabilidades críticas. Este ejercicio permitió no solo entender una parte del ciclo del pentesting, sino también dimensionar el impacto real que tendría un ataque sobre la infraestructura tecnológica comprometida.

El análisis del marco legal colombiano, en particular las leyes 1273 de 2009 y 1581 del 2012, permitió comprender la importancia de actuar conforme a principios éticos y normativos durante cualquier actividad por la legalidad informática. Se resalta que el conocimiento técnico debe estar respaldado por la legalidad, además el derecho de las personas por la protección de datos personales y la privacidad.

Se diseñaron y propusieron medidas de contención y estrategias de hardening como respuesta a las vulnerabilidades detectadas en el entorno virtual. Estas incluyeron la actualización de sistemas operativos obsoletos, la desactivación de protocolos inseguros como SMBv1, la implementación de controles de acceso y segmentación de red.

Recomendaciones

Fortalecer la formación continua en ciberseguridad ofensiva y defensiva, promoviendo ejercicios prácticos en entornos controlados que involucren metodologías de RedTeam y BlueTeam, con el fin de preparar profesionales frente a amenazas reales.

Actualizar y mantener los sistemas informáticos con parches de seguridad y configuraciones endurecidas, especialmente en entornos corporativos.

Establecer políticas organizacionales claras sobre el tratamiento de datos personales, en cumplimiento con las leyes colombianas, incluyendo capacitación constante en ética y legalidad para todo el personal no solo el TI.

Fomentar la colaboración entre equipos técnicos mediante estrategias de purple team, donde se promueva el trabajo el equipo para así mejorar los tiempos de detección y respuestas frente a amenazas.

Incluir cláusulas contractuales éticas en los servicios de ciberseguridad, que permitan asegurar el respeto por la privacidad, la integridad de los daros y el derecho a la denuncia.

Referencias Bibliográficas

Burdova, C. (2020, 18 de junio). ¿Qué es EternalBlue y por qué el exploit MS17-010 sigue siendo relevante? Avast. https://www.avast.com/es-es/c-eternalblue

CalCom Software. (s.f.). ¿Qué son los CIS Benchmarks y cómo usarlos? CalCom Software. https://calcomsoftware.com/que-son-los-cis-benchmarks-y-como-usarlos/

Castillo, A. M. (2018). Introducción a las pruebas de penetración. https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6863/Introducci%C3%B3n%20a%20las%20pruebas%20de%20penetraci%C3%B3n..pdf

Consejo Profesional Nacional de Ingeniería (COPNIA). (2003). Código de ética profesional. https://www.copnia.gov.co/sites/default/files/node/page/field_insert_file/codigo_etica.pdf

Exploit Database. (2025). Exploit Database. https://www.exploit-db.com/

Greenbone Vulnerability Management. (2025). OpenVAS. https://www.openvas.org/

IBM. (2025, mayo 18). Comando NETSTAT. https://www.ibm.com/docs/en/zvm/7.2?topic=information-netstat-command

IBM. (2025, mayo 18). SIEM (Security Information and Event Management). https://www.ibm.com/mx-es/topics/siem

ISN. (2025, mayo 18). Hardening. https://isnum.com/glosario-ciberseguridad/hardening/

Hess, K. (2020, junio 4). Protect your systems with Fail2Ban. Red Hat. https://www.redhat.com/es/blog/protect-systems-fail2ban

Metasploit. (2025). Metasploit. https://www.metasploit.com/

Ministerio del Interior. (2009, enero 5). Ley 1273 de 2009. Superintendencia de Industria y Comercio. https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2021, marzo 10). Resolución 500 de 2021. https://gobiernodigital.mintic.gov.co/692/articles-162625_recurso_2.pdf

MITRE Corporation. (2025). CVE List. https://cve.mitre.org/

Nmap. (2025). Manual de Nmap. https://nmap.org/man/es/index.html

National Vulnerability Database (NVD). (2025, mayo 5). CVE-1999-0524. https://nvd.nist.gov/vuln/detail/CVE-1999-0524

National Vulnerability Database (NVD). (2025, mayo 5). CVE-2016-0128. https://nvd.nist.gov/vuln/detail/CVE-2016-0128

National Vulnerability Database (NVD). (2025, mayo 5). CVE-2017-0143. https://nvd.nist.gov/vuln/detail/CVE-2017-0143

OPNsense. (2025, mayo 18). OPNsense. https://opnsense.org/

pfSense. (2025, mayo 18). pfSense. https://www.pfsense.org/

Congreso de Colombia. (2012, 17 de octubre). *Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales*. Diario Oficial No. 48.587. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

República de Colombia (2013, 27 de junio). *Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012*. Diario Oficial No. 48.834. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=53646

República de Colombia. (2022, 8 de marzo). *Decreto 338 de 2022: Por el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras*

disposiciones. Diario Oficial No. 51.951.

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866