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

Pablo Emilio Medina Beltran

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2024

Dedicatoria

Dedico este trabajo a mis padres quienes me guiaron y me dieron todo lo necesario para salir adelante, me bridaron todo su amor y compañía y quisieron que fuera siempre una persona de bien, a mi esposa quien siempre me motivo a culminar mi carrera como ingeniero y con sus palabras su siempre darme una voz de aliento en los momentos difíciles, a mi hija quien ve en mi un ejemplo a seguir.

Agradecimientos

Ingeniero Ever Luis Arroyo Baron, quien es el director de curso del seminario especializado y quien me oriento en la construcción de este documento.

Resumen

Los equipos Red Team y Blue Team desempeñan roles complementarios en la seguridad de una organización. El Red Team simula ataques ofensivos para identificar vulnerabilidades y probar la eficacia de los controles de seguridad, mientras que el Blue Team se enfoca en la defensa, fortaleciendo las medidas de protección y respondiendo a las amenazas detectadas. Evaluar las acciones de ambos equipos desde una perspectiva ética y legal es esencial para garantizar que las simulaciones no comprometan la integridad del sistema ni afecten a terceros, además de respetar los límites establecidos por la organización. Desde un punto de vista legal, es crucial que las pruebas ofensivas del Red Team cuenten con autorización explícita y estén alineadas con las normativas vigentes, como las leyes de protección de datos y ciberseguridad. Igualmente, las acciones del Blue Team deben seguir protocolos éticos, como la gestión responsable de los incidentes y la protección de la privacidad. Ambos equipos deben actuar bajo un marco claro de transparencia y responsabilidad, garantizando que las pruebas y defensas contribuyan al fortalecimiento de la seguridad sin violar regulaciones o comprometer la confianza en la organización.

Palabras clave: Vulnerabilidades, simulaciones, ética, ciberseguridad

Abstract

The Red Team conducts simulated attacks on an organization's systems to identify vulnerabilities and test the security infrastructure. Their goal is to find potential weaknesses that malicious actors could exploit. Through penetration testing and various attack techniques, they emulate real threats to improve the organization's defensive measures. The Blue Team, on the other hand, focuses on defending the organization's systems. They monitor, detect, and respond to threats, using the insights from the Red Team to strengthen security. Both teams operate under ethical and legal frameworks, ensuring that simulations respect privacy policies and comply with regulations, contributing to responsible cybersecurity practices.

Keywords: Vulnerabilities, Simulations, Ethics, Cybersecurity

Tabla de contenido

Lista de Figuras

Introducción

La evaluación de las acciones de los equipos Red Team y Blue Team es esencial para garantizar una defensa integral en ciberseguridad dentro de una organización. Mientras que el Red Team simula ataques ofensivos para identificar vulnerabilidades, el Blue Team se encarga de la defensa, detección y respuesta a amenazas en tiempo real. Esta dinámica, además de mejorar la seguridad, debe alinearse con criterios éticos y legales para asegurar que las pruebas no afecten la integridad de los sistemas ni violen normativas o regulaciones. La colaboración entre ambos equipos, bajo un marco ético claro, fomenta una cultura de ciberseguridad responsable y transparente.

Justificación

El informe presentado se fundamenta en la necesidad de evaluar y mejorar las estrategias de ciberseguridad en CyberFort Technologies frente a un panorama de amenazas cada vez más sofisticadas. Las actividades realizadas por el Red Team han permitido identificar vulnerabilidades críticas en sistemas y aplicaciones, mientras que las acciones del Blue Team han demostrado la importancia de respuestas rápidas y efectivas para contener incidentes. Esta interacción entre equipos refuerza la capacidad de la organización para prevenir y mitigar riesgos, mejorando la resiliencia de los sistemas y asegurando la continuidad operativa. Además, la inclusión de aspectos legales asegura que las prácticas se realicen dentro de un marco ético, protegiendo la reputación de la organización y garantizando el cumplimiento normativo.

El análisis también responde a la importancia de adoptar un enfoque integral que contemple la gestión técnica, organizacional y legal de la seguridad informática. Proteger los activos críticos, minimizar las vulnerabilidades y actuar con responsabilidad ética no solo mitiga riesgos, sino que también fortalece la confianza de los clientes y socios comerciales. Este enfoque permite a la organización posicionarse como un referente en ciberseguridad, adaptándose a las exigencias del mercado y demostrando un compromiso con la innovación y la protección de datos en un entorno tecnológico en constante evolución.

Objetivos

Objetivo General

Desarrollar estrategias de actuación ética y legal mediante la evaluación y análisis de prácticas del Red Team y Blue Team para garantizar la integridad de los sistemas, la protección de los datos y el cumplimiento de las normativas.

Objetivos Específicos

Identificar las vulnerabilidades presentes en sistemas informáticos mediante simulaciones controladas realizadas por el Red Team, para fortalecer las medidas de protección frente a posibles ataques cibernéticos.

Analizar las respuestas defensivas del Blue Team utilizando herramientas de monitoreo y auditoría, para mejorar la capacidad de detección y mitigación de amenazas en tiempo real.

Diseñar protocolos éticos y legales para las actividades de ciberseguridad mediante el estudio de normativas y buenas prácticas, para asegurar el cumplimiento normativo y la confianza en la organización.

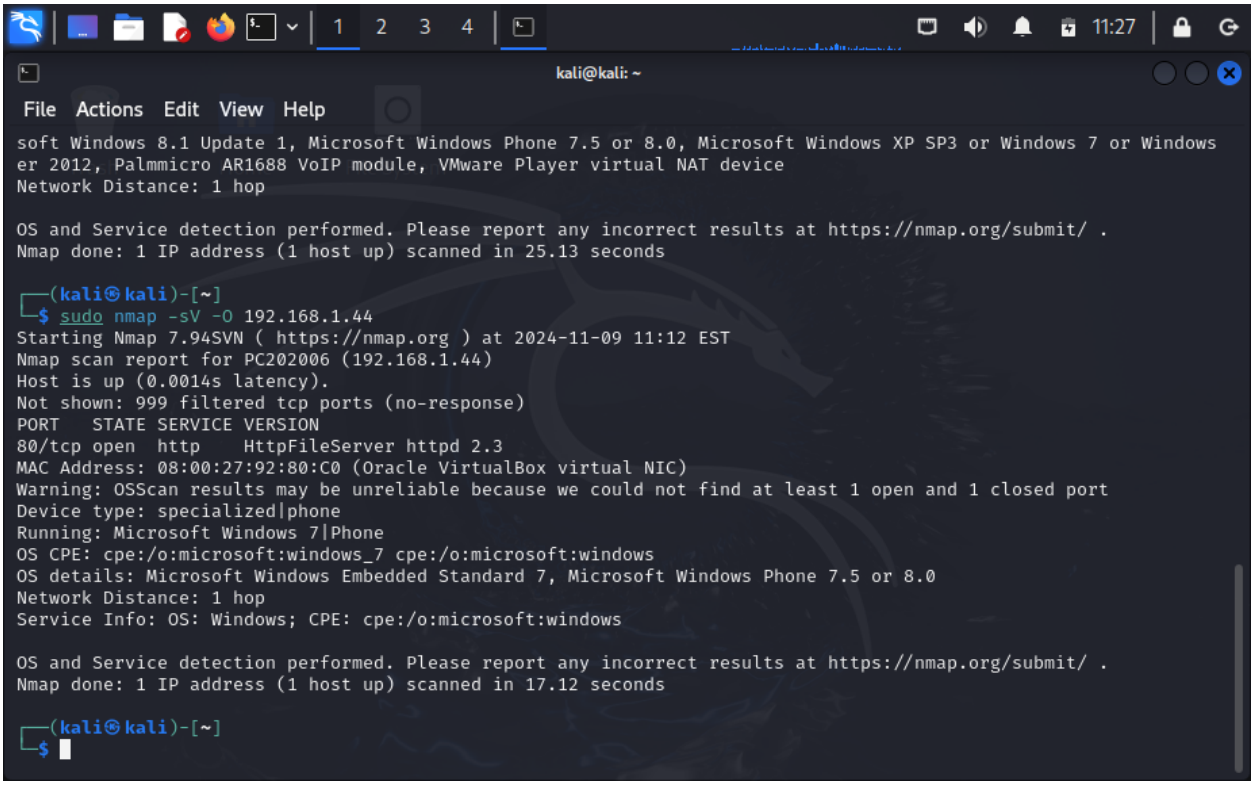
Informe Técnico

A continuación, se realizará la descripción de los escenarios simulados y el enfoque estratégico aplicado con el fin de presentar las acciones realizadas como parte del Red Team y Blue Team, y analizar los aspectos legales relacionados para fortalecer la seguridad organizacional durante el período de prueba.

Actividades Realizadas por el Red Team

Reconocimiento - Herramientas empleadas

Figura 1
Nmap: Escaneo de puertos para identificar servicios activos.



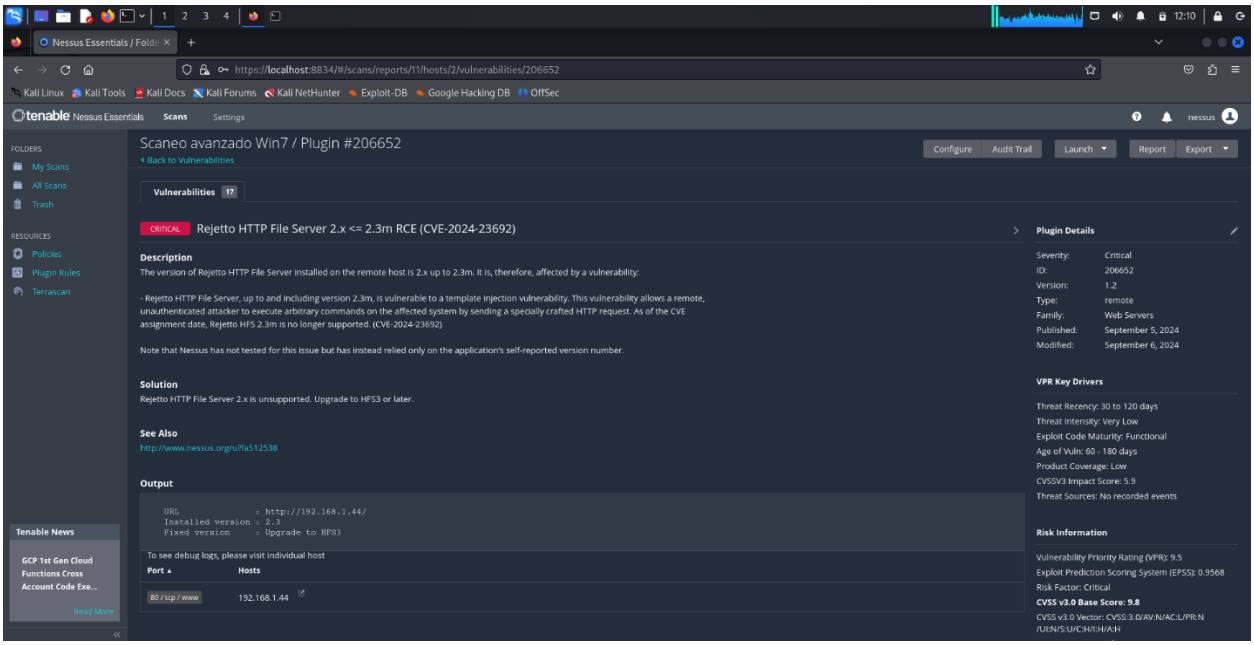
Fuente. El autor

Resultados: Identificación de una aplicación vulnerable (HFS versión 2.3) en el puerto 80.

Explotación de Vulnerabilidades - Herramientas utilizadas

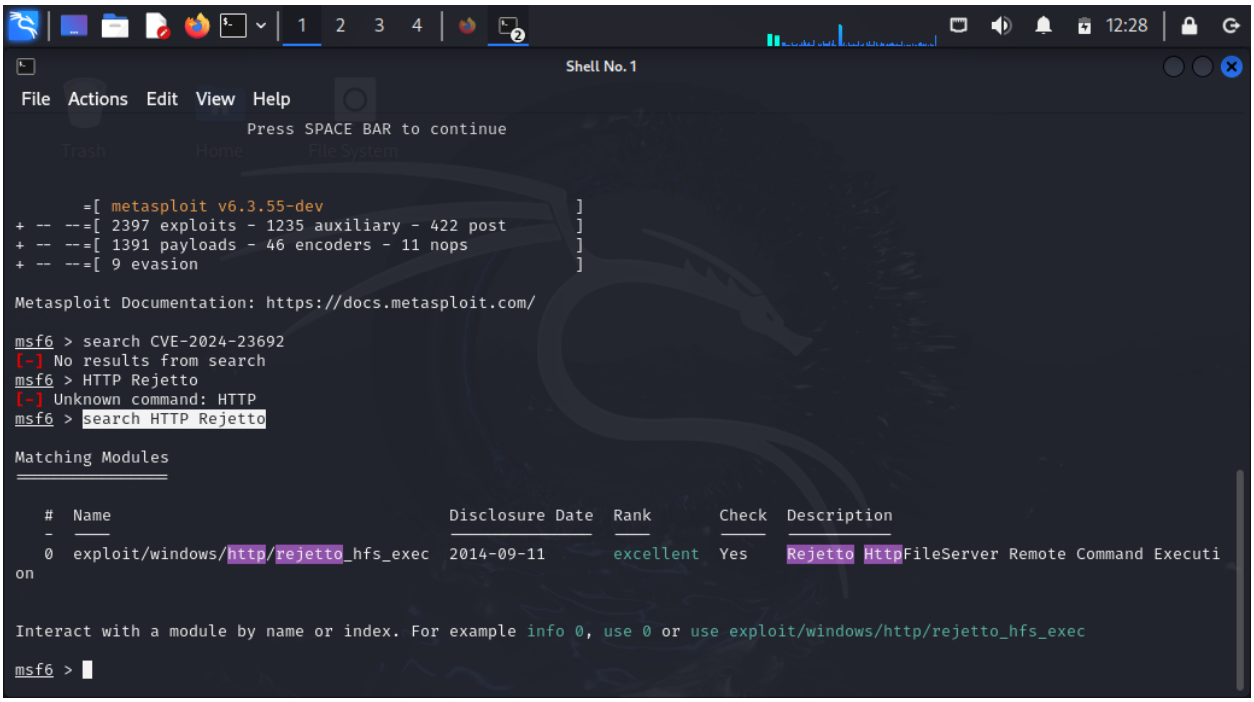
Figura 2

Nessus: Escaneo de vulnerabilidades críticas (CVE-2024-23692).



Fuente. El autor

Figura 3
Metasploit: Uso de exploits para lograr ejecución remota de comandos.



Fuente. El autor

Resultados: Obtención de acceso inicial mediante una shell remota

Escalada de Privilegios - Acciones realizadas

Figura 4
Creación de un usuario administrador.

Fuente. El autor

Verificación de persistencia mediante backdoors.

Impacto: Compromiso total del sistema objetivo.

Actividades Realizadas por el Blue Team

Respuesta Inicial al Incidente - Acciones ejecutadas:

Aislamiento de la máquina comprometida.

Análisis de procesos y conexiones activas mediante herramientas como Process Explorer.

Revisión de logs del sistema para identificar acciones maliciosas.

Medidas de Mitigación - Acciones realizadas:

Bloqueo del puerto 80 y detención del servicio vulnerable (HFS).

Implementación de parches de seguridad y actualización de software.

Propuestas de Endurecimiento (Hardenización)

Actualización o sustitución de la aplicación vulnerable.

Configuración de firewall con listas blancas de IPs.

Implementación de segmentación de red y monitoreo continuo con IDS/IPS.

Aspectos Legales

Normatividad Relevante

Aplicación de la Ley 1273 de 2009:

Artículo 269A: Acceso abusivo a sistemas informáticos.

Artículo 269C: Interceptación de datos informáticos.

Cláusulas Contractuales Analizadas

Identificación de cláusulas ilegales en acuerdos internos que podrían violar el deber de denuncia y obstruir la justicia.

Recomendaciones

Ajustar las políticas internas para cumplir con las normativas legales y éticas.

Garantizar la transparencia y responsabilidad en todas las acciones de ciberseguridad.

Conclusiones

Durante el período de prueba en CyberFort Technologies, las acciones realizadas por el Red Team y el Blue Team evidenciaron la importancia de mantener un enfoque proactivo y reactivo en ciberseguridad. Las simulaciones ofensivas identificaron vulnerabilidades críticas, como la ejecución remota de comandos a través de una aplicación desactualizada, resaltando la necesidad de una gestión eficiente de actualizaciones y parches. Asimismo, las respuestas del Blue Team demostraron la capacidad de contención y mitigación frente a incidentes, reforzando la importancia de herramientas como firewalls, IDS/IPS, y segmentación de red para proteger los activos críticos. Este enfoque combinado garantiza una defensa más robusta y resiliente ante amenazas emergentes.

En cuanto a los aspectos legales y éticos, se identificaron inconsistencias en las políticas internas que podrían comprometer la transparencia y el cumplimiento normativo. La revisión de los acuerdos internos y la alineación con marcos legales como la Ley 1273 de 2009 son fundamentales para fortalecer la confianza en la organización y prevenir sanciones legales. Este proceso destacó la necesidad de fomentar una cultura de ciberseguridad responsable, donde cada actor, desde los equipos técnicos hasta la alta dirección, actúe bajo principios éticos que garanticen tanto la seguridad de los sistemas como el respeto por los derechos de los usuarios.

Recomendaciones

Para fortalecer la postura de ciberseguridad en CyberFort Technologies, es prioritario implementar un plan integral de actualización y gestión de vulnerabilidades. Esto incluye la sustitución de aplicaciones obsoletas, como el HFS detectado, por alternativas más seguras y robustas, además de la aplicación constante de parches de seguridad en sistemas operativos y software. Se recomienda reforzar las configuraciones de red mediante firewalls avanzados, segmentación de redes críticas, y la adopción de herramientas de monitoreo continuo, como IDS/IPS, para identificar y mitigar posibles amenazas en tiempo real. Adicionalmente, integrar mecanismos de autenticación multifactor (MFA) y aplicar el principio de privilegios mínimos contribuirá a reducir riesgos de escalamiento de privilegios.

Desde el punto de vista organizacional y legal, se sugiere revisar y ajustar las políticas internas para alinearlas con las normativas vigentes, como la Ley 1273 de 2009, y eliminar cualquier cláusula que pueda ser percibida como ilegal o contraria a la ética profesional. Es fundamental implementar capacitaciones regulares para el personal en buenas prácticas de ciberseguridad, manejo ético de información y cumplimiento normativo, garantizando así un entendimiento común de las responsabilidades. Finalmente, establecer un canal claro de comunicación entre Red Team y Blue Team permitirá una colaboración más efectiva, potenciando la prevención y respuesta a incidentes de manera integral.

Referencias Bibliográficas

Andress, J., & Winterfeld, S. (2014). Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners, Un enfoque práctico sobre ciberseguridad ofensiva y defensiva. (2nd ed.). Syngress.

Bejtlich, R. (2013). The Practice of Network Security Monitoring: Understanding Incident Detection and Response. Guía técnica sobre monitoreo de seguridad y respuesta a incidentes.

Center for Internet Security. (2021). CIS Controls v8. CIS. Recuperado de https://www.cisecurity.org

Invicti. (s.f.). Remote code execution (RCE). Invicti. https://www.invicti.com/learn/remote-code-execution-rce/

Kaspersky Lab. (2022). Endpoint Security and Response Best Practices., Guía práctica sobre EDR y su uso en contención de amenazas. Kaspersky. https://www.kaspersky.com

Kaspersky. (2021). What is vulnerability scanning?. Kaspersky IT Encyclopedia. https://www.kaspersky.com/resource-center/definitions/vulnerability-scanning

Krutz, R. L., & Vines, R. D. (2010). Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Una referencia para la seguridad en entornos de almacenamiento y computación en la nube., Wiley.

Lyon, G. F. (2009). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.Com LLC.

NIST. (2020). Framework for Improving Critical Infrastructure Cybersecurity, Marco estándar para la gestión de riesgos de ciberseguridad. (Version 1.1). National Institute of Standards and Technology., https://www.nist.gov

Offensive Security. (s.f.). Metasploit Unleashed. Offensive Security. https://www.offensive-security.com/metasploit-unleashed/

Rehman, R. (2013). Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID., Referencia sobre herramientas de detección y contención en ciberseguridad. Prentice Hall.

Splunk Inc. (2023). Introduction to Splunk for SIEM., Manual técnico para la implementación de un SIEM. Splunk. https://www.splunk.com

Stallings, W., & Brown, L. (2018). Computer Security: Principles and Practice, Introducción completa a los principios de seguridad informática. (4th ed.). Pearson.

Tenable. (s.f.). Nessus User Guide. Tenable, Inc. https://docs.tenable.com/nessus/Content/NessusUserGuide.pdf

Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security, Un texto académico sobre fundamentos y estrategias de seguridad informática. (7th ed.). Cengage Learning.