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

Robinson Alvarez Cordoba

Código. 202337164-8

Asesor

Ever Luis Arroyo Baron

Universidad Nacional Abierta Y A Distancia – UNAD

Escuela De Ciencias Basicas, Tecnologia E Ingenieria ECBTI

Seminario Especializado: Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team

Villavicencio

2024

Resumen

Este informe detalla las estrategias de seguridad cibernética implementadas en la organización, enfocándose en las prácticas de Red Team y Blue Team para identificar y mitigar amenazas. El Red Team simula ataques cibernéticos utilizando herramientas como Metasploit y Nmap para detectar vulnerabilidades, mientras que el Blue Team se encarga de la defensa, implementando medidas como SIEM y MFA para mejorar la visibilidad y prevenir accesos no autorizados. Además, se discute la importancia del Análisis Forense para investigar incidentes y preservar pruebas, y cómo herramientas como VirtualBox facilitan la creación de entornos seguros para pruebas controladas. El informe también aborda la Ley 1273 de 2009, que regula los delitos informáticos en Colombia, penalizando el acceso no autorizado a sistemas, la interceptación de datos y el uso de software malicioso. La integración de estas estrategias y herramientas permite a la organización fortalecer su postura de seguridad, proteger la información sensible y cumplir con las normativas legales, promoviendo una cultura de ciberseguridad responsable.

Palabra clave: Blue Team, Metasploit, Nmap, Red Team.

Abstract

This report details the cybersecurity strategies implemented in the organization, focusing on Red Team and Blue Team practices to identify and mitigate threats. The Red Team simulates cyber attacks using tools like Metasploit and Nmap to detect vulnerabilities, while the Blue Team takes care of defense, implementing measures like SIEM and MFA to improve visibility and prevent unauthorized access. Additionally, the importance of Forensic Analysis for investigating incidents and preserving evidence is discussed, and how tools such as VirtualBox facilitate the creation of secure environments for controlled testing. The report also addresses Law 1273 of 2009, which regulates computer crimes in Colombia, penalizing unauthorized access to systems, data interception and the use of malicious software. The integration of these strategies and tools allows the organization to strengthen its security posture, protect sensitive information and comply with legal regulations, promoting a responsible cybersecurity culture.

Keyword: Blue Team, Metasploit, Nmap, Red Team.

Tabla De Contenido

Introducción

En un entorno digital altamente conectado, la ciberseguridad ha adquirido un papel fundamental para proteger la información sensible de organizaciones y gobiernos. Este informe técnico analiza las estrategias y herramientas utilizadas por los equipos Red Team y Blue Team para identificar, contener y mitigar amenazas cibernéticas, integrando una revisión ética y legal basada en la Ley 1273 de 2009 de Colombia, el informe toma como referencia actividades prácticas simuladas, incluyendo la explotación de vulnerabilidades críticas y la implementación de controles de defensa, así como análisis éticos en torno a contratos laborales y casos de ciberespionaje.

Justificación

La justificación de implementar un enfoque integral de seguridad en la organización, que incluya herramientas como Metasploit, VirtualBox, Análisis Forense, SIEM, y MFA, radica en la creciente sofisticación de las amenazas cibernéticas y la necesidad de proteger los datos y sistemas críticos. La adopción de estas estrategias permite no solo identificar y mitigar vulnerabilidades antes de que sean explotadas, sino también responder de manera rápida y efectiva ante cualquier incidente, minimizando el impacto en la operación. El análisis forense proporciona una capacidad de investigación exhaustiva que facilita la identificación de las causas de los ataques y la preservación de pruebas para acciones legales. Asimismo, el uso de SIEM centraliza el monitoreo de seguridad, mejorando la visibilidad de los eventos de seguridad y facilitando la detección temprana de amenazas.

Implementar MFA asegura una capa adicional de protección frente al acceso no autorizado, reforzando la seguridad de los sistemas. En conjunto, estas herramientas no solo mejoran la seguridad técnica, sino que también ayudan a cumplir con normativas legales y estándares éticos, garantizando que la organización actúe de manera responsable y en conformidad con las regulaciones de ciberseguridad.

Objetivos

Objetivo General

Proponer estrategias integrales de ciberseguridad que combinen enfoques ofensivos y defensivos, promoviendo prácticas éticas y cumpliendo con las normativas legales vigentes.

Objetivos Específicos

Analizar las fases de un ataque cibernético simulado, desde la identificación hasta la explotación de vulnerabilidades.

Describir las medidas de contención, monitoreo y recuperación implementadas por el Blue Team.

Evaluar las implicaciones éticas y legales de las prácticas en ciberseguridad basadas en contratos abusivos y ciberespionaje.

Proponer recomendaciones para fortalecer la cultura de ciberseguridad en organizaciones y gobiernos.

Desarrollo Del informe

Estrategias del Red Team: Pruebas de Penetración y Análisis Ofensivo

El Red Team opera simulando los métodos y herramientas utilizadas por actores maliciosos para identificar vulnerabilidades en sistemas y redes.

Fases del Pentesting Reconocimiento:

Recolección de información sobre el objetivo para identificar servicios y puertos abiertos, uso de Nmap para escanear un sistema Windows 7 con HTTP File Server (HFS) 2.3, en el sistema Windows 7 ejecutando HTTP File Server (HFS) 2.3 presenta una vulnerabilidad crítica conocida como CVE-2014-6287, que permite la ejecución remota de código (RCE) debido a una falla en la función `findMacroMarker`. Esta vulnerabilidad, explotada mediante solicitudes maliciosas, permite a un atacante remoto obtener control del sistema afectado sin necesidad de autenticación previa, comprometiendo la integridad, confidencialidad y disponibilidad de los datos alojados. La combinación de un sistema operativo obsoleto, como Windows 7, con software no actualizado como HFS 2.3, resalta la importancia de mantener una política de actualización rigurosa, especialmente en entornos donde se procesan datos sensibles o se depende de la estabilidad operativa. Este caso subraya la necesidad de migrar a tecnologías soportadas y robustas, además de implementar controles de seguridad proactivos que reduzcan la superficie de ataque. (Thapa, 2024)

Escaneo de Vulnerabilidades

El escaneo de vulnerabilidades es una etapa crucial dentro de las pruebas de seguridad y consiste en identificar debilidades en sistemas, aplicaciones y redes que puedan ser explotadas por atacantes. En el caso de un sistema Windows 7 ejecutando HTTP File Server (HFS) 2.3, esta fase se realizó utilizando herramientas como Nmap para detectar puertos abiertos y servicios

activos en la dirección IP objetivo, lo que permitió delimitar la superficie de ataque. Posteriormente, con el uso de Searchsploit, se localizaron exploits específicos asociados a la versión de HFS en ejecución, destacando la vulnerabilidad crítica CVE-2014-6287. Este análisis permitió identificar un vector de ataque que habilita la ejecución remota de código, lo que subraya la importancia de realizar escaneos periódicos como medida preventiva, implementando herramientas automatizadas y revisando constantemente las configuraciones para mitigar riesgos antes de que puedan ser aprovechados por actores malintencionados. (Fortra.com., 2022)

Identificación de puntos débiles en servicios activos.

Herramientas utilizadas.

Searchsploit para localizar exploits relacionados con la vulnerabilidad CVE-2014-6287. La vulnerabilidad CVE-2014-6287 afecta a HTTP File Server (HFS) 2.3, una herramienta utilizada para compartir archivos mediante una interfaz web. Esta falla crítica permite la ejecución remota de código (RCE) debido a un manejo inadecuado de las entradas en la función findMacroMarker en el archivo parserLib.pas. Un atacante puede enviar solicitudes especialmente diseñadas al servidor, utilizando una secuencia %00 para inyectar comandos maliciosos que se ejecutan con los permisos del sistema afectado, en la vulnerabilidad no requiere autenticación, lo que amplifica su severidad al facilitar el acceso remoto sin barreras iniciales. Este fallo puede ser explotado para comprometer completamente un sistema, permitiendo al atacante realizar acciones como el robo de datos, instalación de malware o incluso escalación de privilegios. (INCIBE., 2014)

Explotación

Ejecución de exploits mediante Metasploit para establecer un shell inverso y obtener acceso al sistema.

Creación de un usuario administrativo para maximizar el control sobre el sistema.

Escalación de Privilegios

Explotación de configuraciones incorrectas para acceder a datos sensibles y expandir el alcance del ataque.

Herramientas Clave

Nmap: Escaneo de redes para identificar superficies de ataque, en esta organización, el Análisis Forense se utiliza para investigar incidentes de seguridad mediante la recopilación y análisis de datos de sistemas y redes. Utilizando herramientas como Wireshark y Netstat, se identifican conexiones maliciosas y patrones sospechosos, lo que permite determinar el origen del ataque y preservar las evidencias necesarias para acciones legales. Este proceso es esencial para mejorar la seguridad y prevenir futuros incidentes. (manual)., 2024)

Metasploit: Plataforma para ejecutar exploits y administrar sesiones de ataque, En esta organización, Metasploit se utiliza como una herramienta clave para realizar pruebas de penetración y evaluaciones de seguridad. Permite a los equipos de seguridad simular ataques reales mediante la identificación y explotación de vulnerabilidades en sistemas, aplicaciones y redes. Metasploit proporciona un conjunto de exploits y payloads que facilitan la ejecución de ataques controlados, ayudando a los analistas a evaluar la resistencia de los sistemas ante posibles amenazas y a fortalecer las medidas de defensa antes de que un atacante real pueda explotarlas. (ciberseg1922., 2021)

VirtualBox: Creación de entornos virtuales controlados, VirtualBox se utiliza en esta organización para crear entornos virtualizados seguros donde se pueden realizar pruebas de seguridad y simulaciones de ataques sin comprometer los sistemas reales. Permite ejecutar múltiples sistemas operativos simultáneamente en una sola máquina física, lo que facilita la

realización de pruebas controladas, análisis forense y evaluación de vulnerabilidades en un entorno aislado. VirtualBox es esencial para probar configuraciones y herramientas de seguridad antes de su implementación en el entorno de producción. (VirtualBox., 2024)

Searchsploit: Base de datos de vulnerabilidades para localizar exploits específicos.

Impacto del Ataque Simulado

Compromiso de sistemas no actualizados (HFS 2.3).

Obtención de acceso privilegiado que permite modificar configuraciones críticas.

Estrategias del Blue Team: Contención y Defensa

El Blue Team se encarga de defender la infraestructura tecnológica mediante estrategias de contención, análisis forense y prevención.

Las estrategias del Blue Team para contención y defensa se centran en mitigar los efectos de los ataques y proteger los activos tecnológicos de la organización. Ante un incidente, la primera acción es aislar los sistemas comprometidos de la red para evitar la propagación de la amenaza, seguida de configuraciones de firewalls que bloqueen direcciones IP sospechosas. Posteriormente, se lleva a cabo un análisis forense utilizando herramientas como Wireshark y Netstat para monitorear el tráfico y detectar conexiones maliciosas. A medida que la amenaza se controla, se procede a la restauración de sistemas desde copias de seguridad seguras y a la actualización de parches para corregir vulnerabilidades, mientras se refuerzan las políticas de acceso con medidas como la autenticación multifactor (MFA). Estas acciones forman parte de un proceso continuo que busca fortalecer la infraestructura de seguridad y minimizar la posibilidad de futuros incidentes. (Founderz., 2024)

Contención de Ataques

Aislamiento de Sistemas Comprometidos

Desconexión de dispositivos afectados de la red para evitar la propagación del ataque, Bloqueo de direcciones IP sospechosas mediante firewalls.

Análisis Forense

En esta organización, el Análisis Forense se implementa como una herramienta esencial para la investigación y resolución de incidentes de seguridad. Este proceso involucra la recopilación, preservación, análisis e interpretación de datos de sistemas y redes con el objetivo de identificar el origen, los métodos y el impacto de un ataque cibernético. Durante un análisis forense, se revisan logs, archivos y otros artefactos digitales utilizando herramientas especializadas como Wireshark y Netstat para identificar tráfico sospechoso, conexiones maliciosas y cualquier alteración no autorizada. Además, el análisis forense ayuda a preservar las evidencias necesarias para acciones legales, garantizando que la integridad de los datos no sea comprometida durante la investigación. Esta práctica es clave para entender cómo ocurrió el incidente, mitigar futuros riesgos y reforzar las políticas de seguridad. (Aurora., 2023)

Uso de herramientas como Wireshark y Netstat para identificar conexiones maliciosas y analizar tráfico anómalo.

Preservación de evidencias digitales para investigaciones posteriores.

Restauración y Mejora Continua

Restauración de sistemas desde respaldos seguros, Implementación de actualizaciones de seguridad y autenticación multifactor (MFA).

En esta organización, la Autenticación Multifactor (MFA) se implementa como una capa adicional de seguridad para proteger el acceso a sistemas y datos sensibles. MFA requiere que

los usuarios proporcionen más de un factor de autenticación, combinando algo que saben (como una contraseña), algo que tienen (un dispositivo que genera un código único, como un teléfono móvil) y, en algunos casos, algo que son (características biométricas como huellas dactilares o reconocimiento facial). Esta medida fortalece la seguridad al dificultar el acceso no autorizado, incluso si un atacante obtiene la contraseña, ya que se requiere un segundo o tercer factor para completar la autenticación. (TechTarget., 2021)

Hardenización de Sistemas

Migración de sistemas operativos desactualizados a versiones soportadas (e.g., Windows 10/11).

Configuración de políticas de acceso basadas en privilegios mínimos.

Segmentación de redes críticas para minimizar el impacto de intrusiones.

Monitoreo y Respuesta

Implementación de SIEM para correlación de eventos de seguridad y alertas, uso de IPS (e.g., Snort, Suricata) para detectar y bloquear amenazas en tiempo real.

La implementación de un sistema SIEM (Security Information and Event Management) en la organización es esencial para fortalecer la seguridad cibernética, mejorar la visibilidad de los eventos de seguridad y facilitar una respuesta rápida a incidentes. El SIEM centraliza la recolección, el análisis y la correlación de logs provenientes de diversas fuentes, como firewalls, sistemas de detección de intrusiones (IDS), servidores, aplicaciones y dispositivos de red. Al integrar esta solución, la organización puede detectar patrones sospechosos, identificar amenazas avanzadas como APT (Advanced Persistent Threats) y generar alertas en tiempo real, lo que permite una respuesta más rápida a incidentes de seguridad. Para implementarlo correctamente, se debe iniciar con la selección de la plataforma SIEM adecuada, considerando factores como la

escalabilidad, las capacidades de correlación y la integración con las herramientas existentes en la infraestructura. Una vez seleccionado, se debe configurar la recolección de logs de todas las fuentes relevantes, establecer reglas de correlación para identificar amenazas específicas y ajustar los umbrales de alerta para evitar la sobrecarga de notificaciones. El equipo de seguridad debe ser capacitado en el uso de la plataforma para realizar investigaciones forenses, analizar tendencias de amenazas y generar informes para auditorías internas y el cumplimiento de normativas. Además, es crucial implementar un proceso de monitoreo continuo, utilizando el SIEM para realizar un análisis constante de eventos y detectar cualquier anomalía en tiempo real. La implementación de un SIEM no solo mejora la capacidad de detección de amenazas, sino que también contribuye al cumplimiento de normativas de seguridad, como GDPR o HIPAA, garantizando la protección de datos sensibles y la auditoría de acciones dentro de la infraestructura tecnológica. (TEAM, s.f.)

Consideraciones Éticas y Legales

Análisis Ético de Contratos Abusivos

CyberFort Technologies utilizó contratos con cláusulas que limitan derechos laborales y restringen la denuncia de actividades ilícitas.

Estas prácticas contravienen principios éticos y violan disposiciones legales de la Ley 1273 de 2009, la regula los delitos informáticos y establece sanciones para quienes cometan actos ilícitos relacionados con el uso de tecnologías de la información. Esta ley penaliza el acceso no autorizado a sistemas informáticos (Artículo 269A), la interceptación ilegal de datos (Artículo 269C), el uso de software malicioso (Artículo 269E) y la violación de datos personales (Artículo 269F). También sanciona la obstaculización ilegítima de sistemas (Artículo 269B) y establece agravantes punitivas cuando los delitos tienen un impacto significativo en la seguridad

nacional o el orden público. La ley busca proteger la privacidad, garantizar la integridad de los sistemas informáticos y promover un entorno seguro en el ciberespacio en Colombia. (Normativo., 2015)

Artículo 269A: Acceso abusivo a sistemas informáticos.

Artículo 269C: Interceptación no autorizada de datos.

Caso de Ciberespionaje

El acceso no autorizado a datos gubernamentales resalta la necesidad de implementar controles de acceso y monitoreo exhaustivo.

Medidas recomendadas

Registro detallado de actividades.

Políticas de trazabilidad y auditorías internas.

Respuesta legal inmediata en casos de espionaje corporativo.

Conclusiones

En conclusión, la implementación de estrategias de seguridad proactivas y reactivas, como el uso de Metasploit, VirtualBox, Análisis Forense, y la integración de herramientas como SIEM y MFA, son fundamentales para proteger los activos digitales de la organización ante amenazas cibernéticas cada vez más sofisticadas. Estas prácticas no solo permiten identificar y mitigar vulnerabilidades, sino que también fortalecen la capacidad de respuesta ante incidentes, garantizando la protección de datos sensibles y la continuidad operativa. Además, el análisis forense y las simulaciones de ataques proporcionan una visión clara sobre posibles vectores de ataque, lo que permite a los equipos de seguridad ajustar sus estrategias y prevenir futuros incidentes. Al adoptar un enfoque integral que combine tecnología avanzada con una sólida cultura de ciberseguridad, la organización puede mejorar continuamente su postura de seguridad y minimizar riesgos, asegurando el cumplimiento de normativas legales y estándares éticos.

Recomendaciones

Colaboración Estratégica: Fomentar ejercicios conjuntos entre Red Team y Blue Team para identificar áreas de mejora en las defensas.

Capacitación Continua: Entrenar al personal en análisis forense, hardenización de sistemas y gestión de incidentes.

Estandarización: Adoptar guías de configuración segura como benchmarks CIS para reducir vulnerabilidades comunes.

Simulaciones Frecuentes:

Realizar pruebas de penetración periódicas para validar y reforzar las defensas implementadas.

Referencias

Alvarez, R. (30 de noviembre de 2024). *Fase 5 Seminario Especializado Red Team Y Blue Team* [Archivo de video]. https://youtu.be/p8qgaRKM3hM

Aurora. (18 de 06 de 2023). *¿Qué es el análisis forense en ciberseguridad? - ID Bootcamps. ID Digital School - Bootcamps.* . Obtenido de https://iddigitalschool.com/bootcamps/que-es-el-analisis-forense-en-ciberseguridad/

ciberseg1922. (13 de 12 de 2021). *¿Qué es Metasploit Framework y cómo funciona? Ciberseguridad.* . Obtenido de https://ciberseguridad.com/herramientas/pruebas-penetracion/metasploit-framework/

Fortra.com. (2022). *Qué es el escaneo de vulnerabilidades y cómo funciona.* . Obtenido de https://www.fortra.com/es/blog/escaneo-vulnerabilidades

Founderz., B. T. (08 de 02 de 2024). *Founderz.* . Obtenido de https://founderz.com/es/blog/blue-team-seguridad-cibernetica/

INCIBE., C.-2.-6. |.-C. (2014). *Incibe.es.* . Obtenido de https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2014-6287

manual)., G. d. (2024). *Nmap.org.* . Obtenido de https://nmap.org/man/es/index.html

Normativo., L. 1.-G. (12 de 2015). *Funcionpublica.gov.co.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

TEAM, A. (s.f.). *¿Qué significa SIEM y cómo funciona?* . Obtenido de Ambit-Bst.com. : https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona

TechTarget., C. d. (2021). *Autenticación multifactor o MFA. ComputerWeekly.es; TechTarget.* . Obtenido de https://www.computerweekly.com/es/definicion/Autenticacion-multifactor-o-MFA

Thapa, A. (04 de 06 de 2024). *Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2). Exploit Database.* Obtenido de https://www.exploit-db.com/exploits/39161

VirtualBox., O. (2024). *Oracle.com.* . Obtenido de https://www.oracle.com/co/virtualization/virtualbox/

Apéndices

Apéndice A

Video Explicativo sobre Ciberseguridad

Este video proporciona una explicación detallada sobre las mejores prácticas en ciberseguridad, que complementa los puntos tratados en el documento. Se puede acceder al video a través del siguiente enlace:

https://youtu.be/p8qgaRKM3hM