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

Emerson Quintero De Castro

Tutor

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingenieria ECBTI

Especializacion en Seguridad Informática

2024

Resumen

En el contexto del análisis realizado para CyberFort Technologies, el informe identifica, evalúa y propone soluciones frente a riesgos y vulnerabilidades en la infraestructura TI, con el objetivo de mejorar la postura de seguridad y la resiliencia organizacional frente a ciberamenazas. A través de la colaboración de los equipos Blue Team y Red Team, y considerando aspectos legales y regulatorios, se desarrolló una evaluación integral que incluyó simulaciones de ataques, pruebas de penetración y auditorías detalladas de configuración y cumplimiento normativo.

Los hallazgos destacan brechas significativas en áreas como la gestión de accesos, la falta de segmentación de redes y una respuesta reactiva ante incidentes, lo que expone a la organización a posibles ciberataques de alta criticidad. Entre las vulnerabilidades encontradas, se identificaron configuraciones obsoletas en sistemas clave, ausencia de planes de contingencia robustos y una limitada conciencia de seguridad en el personal.

Como parte de las estrategias de contención, se sugiere la implementación de una segmentación de redes estricta basada en necesidades operativas, el refuerzo de políticas de acceso mediante autenticación avanzada y la actualización continua de sistemas y aplicaciones críticas. También se proponen simulaciones de ataque y evaluaciones periódicas, complementadas con entrenamientos especializados y campañas de sensibilización para empleados. Además, se recomienda optimizar los procesos de respuesta a incidentes mediante la automatización de acciones clave, el establecimiento de indicadores de desempeño (KPIs) de seguridad y la integración de herramientas avanzadas de detección de amenazas.

Estas medidas buscan no solo mitigar las vulnerabilidades actuales, sino también establecer un marco de mejora continua que permita a CyberFort Technologies mantenerse por delante de un panorama de amenazas en constante evolución.

Tabla de contenido

Resumen 2
Glosario 6
Introducción 7
Objetivos 8
Objetivo General 8
Objetivos Específicos 8
Desarrollo de la actividad 9
Actividad 1 9
Conclusiones 16
Recomendaciones 18
Recomendaciones Estratégicas con Énfasis en Operaciones Técnicas 18
Recomendaciones Estratégicas con Énfasis en Integración y Proactividad 19
Referencias Bibliográficas 20

Tabla de figuras

Figura 1. Herramienta NMAP.....10

Figura 2. Herramienta Shodan para reconocimiento pasivo.....11

Figura 3. Herramienta Metasploit.....11

Figura 4. Herramienta SIEM – Splunk.....12

Figura 5. Zero Trust Network Architecture.....13

Glosario

Análisis de Riesgos: Proceso para identificar, evaluar y priorizar riesgos que pueden afectar la infraestructura TI, basado en su probabilidad e impacto.

Blue Team: Equipo encargado de las defensas de ciberseguridad. Su objetivo principal es identificar, mitigar y contener vulnerabilidades y amenazas dentro de la infraestructura TI.

Ciberseguridad Legal: Conjunto de normativas y estándares que regulan las prácticas de seguridad informática dentro de una organización.

Estrategias de Contención: Acciones diseñadas para mitigar o neutralizar incidentes de seguridad, limitando su alcance e impacto.

Forense Digital: Proceso de investigación para recolectar y analizar evidencia digital con el fin de entender incidentes de seguridad.

Incidente de Seguridad: Evento que compromete la confidencialidad, integridad o disponibilidad de los activos de información.

Infraestructura TI: Conjunto de componentes tecnológicos, incluyendo hardware, software, redes y servicios, que soportan las operaciones de una organización.

Pruebas de Penetración: Simulaciones controladas de ciberataques realizadas por el Red Team para descubrir vulnerabilidades explotables.

Red Team: Grupo de expertos que simulan ataques reales para evaluar las defensas de seguridad. Ayudan a identificar puntos débiles en sistemas y procesos.

Vulnerabilidad: Debilidad en sistemas, redes o aplicaciones que puede ser explotada por amenazas para comprometer la seguridad.

Introducción

Las infraestructuras de TI enfrentan desafíos crecientes debido al avance de las ciberamenazas, lo que exige un enfoque estratégico para mitigar riesgos y fortalecer su seguridad. Este informe tiene como propósito central desarrollar estrategias de contención basadas en un análisis detallado de riesgos y vulnerabilidades, aplicando metodologías avanzadas de ciberseguridad.

Durante el periodo de evaluación en CyberFort Technologies, se llevaron a cabo acciones coordinadas de Blue Team y Red Team que permitieron identificar brechas de seguridad críticas y oportunidades de mejora. Este documento detalla dichas actividades, complementadas con un enfoque en aspectos legales, con el fin de proporcionar un panorama integral para la toma de decisiones estratégicas en la protección de activos tecnológicos.

El análisis y las estrategias propuestas tienen como objetivo no solo abordar las amenazas actuales, sino también establecer una cultura de seguridad sólida dentro de la organización. Esto incluye la capacitación continua del personal y la implementación de controles adaptativos que permitan anticiparse a posibles vulnerabilidades futuras..

Objetivos

Objetivo General

Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

Objetivos Específicos

- Analizar los escenarios de amenazas en la infraestructura TI utilizando técnicas avanzadas de Red Team y Blue Team.
- Desarrollar medidas de contención efectivas alineadas con las normativas legales y los estándares organizacionales.
- Presentar un informe técnico estructurado que incluya análisis, conclusiones y recomendaciones estratégicas, dirigido al equipo de análisis Senior de CyberFort Technologies.

Desarrollo de la actividad

Actividad 1

Aspectos que aporten al desarrollo de estrategias de RedTeam &BlueTeam.

Respuesta:

Aspecto legal

Dentro del marco legal, resaltamos varios articulo de la ley 1273 que regula delitos informáticos.

1. **Artículo 269A**: Obstrucción de sistemas informáticos. Quien, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos contenidos en él, o a una red de telecomunicaciones, incurrirá en pena de prisión de 48 a 96 meses y una multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
2. **Artículo 269B**: Interceptación de información. Quien intercepte, capture, o adquiera acceso a información, datos o comunicaciones electrónicas sin autorización, incurrirá en pena de prisión de 48 a 96 meses y una multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
3. **Artículo 269C**: Intrusión en sistemas informáticos. Quien acceda a un sistema informático sin autorización, incurrirá en pena de prisión de 36 a 72 meses y una multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
4. **El Articulo 269F** contempla la protección de datos personales contenidos en bases de datos, ficheros, los cuales no pueden ser sustraídos, vendidos, interceptados.
5. La suplantación de sitios Web con el fin de obtener datos personales este enunciado en el artículo **269G**, atiende a personas que clonen paginas legales o realicen desvió de información para beneficio propio.
6. **En los artículos 269 I y J** se contempla el hurto por medios informáticos y la transferencia no consentida de activos.

Enfoque Técnico-Operativo

1. **Identificación de Vulnerabilidades (Red Team)**

- **Reconocimiento Activo y Pasivo**:
    - El reconocimiento activo incluye el escaneo directo de redes y sistemas usando herramientas como **Nmap** o **Nessus**. Esto ayuda a identificar puertos abiertos, servicios activos y configuraciones inseguras.

Figura 1. Herramienta NMAP

Fuente: Nmap | Kali Linux Tools. (s. f.). Kali Linux. Recuperado 27 de noviembre de 2024, de https://www.kali.org/tools/nmap/

    - El reconocimiento pasivo se centra en recopilar información sin interactuar directamente con los sistemas objetivo, utilizando fuentes abiertas como **Shodan**, bases de datos públicas y análisis de perfiles en redes sociales (OSINT).

Figura 2. Herramienta Shodan para reconocimiento pasivo

Fuente: https://netcloudengineering.com/shodan-motor-busqueda/

- **Pruebas de Penetración**:
  - Ejecución de pruebas enfocadas, como inyecciones SQL, explotación de vulnerabilidades conocidas (CVE), y ataques de phishing personalizados.
  - Uso de frameworks como **Metasploit** y scripts personalizados para evaluar el impacto real de las vulnerabilidades encontradas.

Figura 3. Herramienta Metasploit

Fuente: https://www.kali.org/tools/metasploit-framework/

- **Reportes Detallados**:
    - Los reportes deben incluir descripciones claras del impacto potencial de las vulnerabilidades, pasos para replicar los hallazgos, y recomendaciones técnicas específicas para mitigarlas.

2. Defensa en Profundidad (Blue Team)

- **Monitorización Continua**:
    - Implementación de soluciones SIEM como **Splunk** o **ELK Stack** para correlacionar eventos y detectar patrones sospechosos en tiempo real.

Figura 4. Herramienta SIEM – Splunk

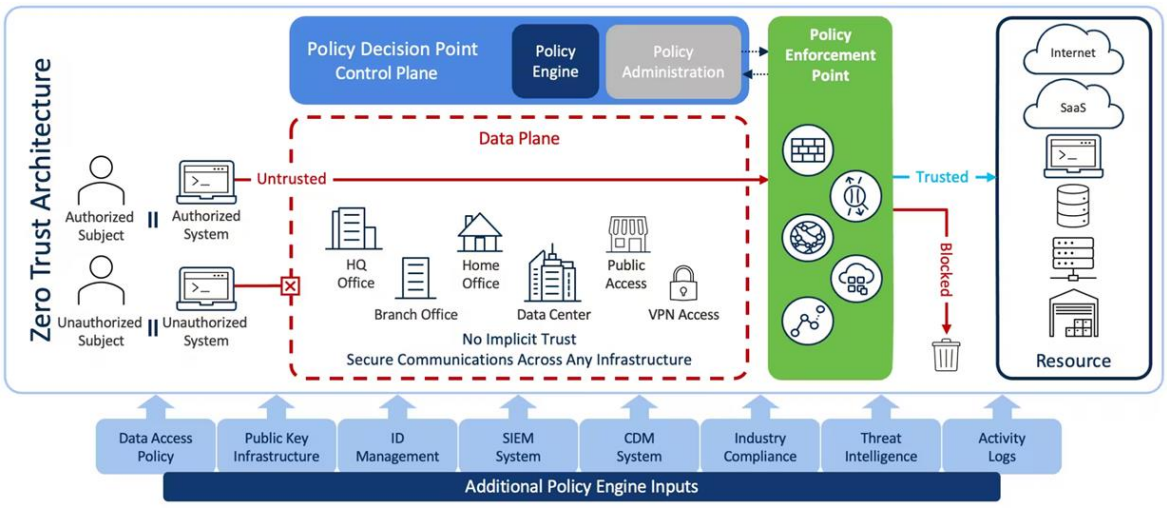
Fuente:[*https://www.splunk.com/content/dam/splunk2/en_us/images/screenshots/products/enterprise/imagery-modal/ent-ha-cm-insights.jpg*](https://www.splunk.com/content/dam/splunk2/en_us/images/screenshots/products/enterprise/imagery-modal/ent-ha-cm-insights.jpg)

- Configuración de alertas personalizadas basadas en el comportamiento anómalo de usuarios o sistemas.

- **Políticas de Respuesta**:
  - Diseño de planes de respuesta a incidentes (IRP) que incluyan fases de preparación, detección, contención, erradicación y recuperación.
  - Simulaciones de escenarios como ataques ransomware o DDoS para evaluar la efectividad del plan.

- **Fortalecimiento de Controles**:
  - Configuración avanzada de firewalls con reglas específicas para bloquear tráfico sospechoso.
  - Segmentación de redes críticas mediante VLANs o Zero Trust Network Architecture (ZTNA) para minimizar el impacto de brechas de seguridad.

Figura 5. Zero Trust Network Architecture



Fuente: https://accuknox.com/wp-content/uploads/zero-trust-architecture.png

3. Colaboración y Retroalimentación

- **Simulaciones de Incidentes**:
    - Ejercicios de Red Team/Blue Team en los que ambos equipos simulan un ataque y una defensa, generando aprendizajes inmediatos.
    - Análisis post-ejercicio para identificar áreas de mejora tanto en ofensiva como en defensiva.
- **Intercambio de Información**:
    - Uso de plataformas como **MITRE ATT&CK** para mapear tácticas y técnicas observadas durante las simulaciones.
    - Creación de un sistema interno de tickets para documentar hallazgos, acciones y retroalimentación en tiempo real.

Enfoque Integral y Estratégico

1. Planificación Estratégica

- **Análisis de Riesgos**:
    - Identificación de activos críticos, amenazas potenciales y vulnerabilidades específicas de la organización.
    - Uso de matrices de riesgo para priorizar las acciones basadas en el impacto y la probabilidad.
- **Objetivos Compartidos**:
    - Establecer métricas clave de desempeño (KPIs) que midan la efectividad de ambos equipos, como el tiempo de detección (MTTD) y el tiempo de respuesta (MTTR).
    - Asegurar que las estrategias de ciberseguridad estén alineadas con los objetivos de negocio, como la protección de datos de clientes y la continuidad operativa.
- **Presupuesto y Recursos**:
    - Justificación del ROI de las inversiones en ciberseguridad mediante la simulación del costo potencial de una brecha no mitigada.

- Asegurar un balance en los recursos asignados entre el Red Team y el Blue Team.

2. Capacitación y Cultura Organizacional

- **Entrenamientos Especializados**:
  - Programas para Red Team, como cursos de ethical hacking o explotación avanzada de vulnerabilidades.
  - Entrenamientos para Blue Team en análisis forense, respuesta a incidentes y configuración avanzada de herramientas de seguridad.
- **Conciencia de Seguridad**:
  - Iniciativas como simulaciones de phishing para sensibilizar a los empleados sobre las amenazas más comunes.
  - Talleres internos para promover prácticas seguras, como la creación de contraseñas robustas y la identificación de correos fraudulentos.
- **Evaluaciones de Desempeño**:
  - Revisiones trimestrales de los equipos mediante pruebas prácticas en escenarios simulados.
  - Retroalimentación continua para ajustar tácticas y estrategias en función de los resultados.

3. Marco Legal y Cumplimiento

- **Adopción de Normativas**:
  - Implementación de controles específicos basados en estándares internacionales como ISO 27001, NIST CSF.
  - Realización de auditorías internas y externas para garantizar el cumplimiento normativo.
- **Documentación**:
  - Registro detallado de actividades de ciberseguridad, incidentes y respuestas implementadas.
  - Creación de reportes gerenciales que incluyan análisis legales y técnicos para respaldar decisiones estratégicas.

Conclusiones

El análisis ejecutado en el contexto de CyberFort Technologies demostró la eficacia de implementar una estrategia integrada entre Blue Team y Red Team para mejorar la postura de seguridad de la organización. Técnicamente, el ejercicio permitió validar la capacidad del Red Team para ejecutar pruebas de penetración avanzadas, incluyendo técnicas de explotación específicas como privilege escalation, phishing dirigido y evasión de sistemas de detección, simulando ataques realistas en tiempo controlado. El Red Team utilizó herramientas como Metasploit para simular ataques dirigidos, evaluando específicamente los vectores de acceso inicial (initial access vectors) y técnicas de persistencia utilizadas por adversarios reales. Estas pruebas no solo identificaron vulnerabilidades críticas, sino que también sirvieron para evaluar la eficacia de los controles existentes.

El Blue Team, por su parte, demostró habilidades avanzadas en la detección de intrusiones mediante herramientas de monitoreo de eventos como SIEM (Security Information and Event Management), análisis forense digital y correlación de logs para identificar patrones de ataque. El uso de herramientas como EDR (Endpoint Detection and Response) y análisis proactivo de tráfico de red mediante tecnologías como Wireshark, Zeek y Suricata. Los análisis forenses permitieron reconstruir líneas de tiempo detalladas de los incidentes simulados, proporcionando datos accionables para cerrar brechas en la seguridad.

Las estrategias defensivas se reforzaron mediante la implementación de soluciones técnicas como segmentación de red, endurecimiento de sistemas (hardening) y ajuste de las reglas de firewall y sistemas de prevención de intrusiones (IPS).

La inclusión de un marco normativo y legal permitió evaluar la adherencia de las operaciones a regulaciones clave como NIST o ISO 27001. Esto aseguró que las medidas de seguridad técnica estuvieran alineadas con las mejores prácticas y estándares internacionales, mitigando no solo riesgos técnicos, sino también aquellos relacionados con la responsabilidad legal.

En términos operativos, la experiencia demostró que la integración de análisis proactivos, como la simulación de ataques (red teaming), con defensas dinámicas y basadas en datos, es crucial para construir un sistema resiliente que responda eficazmente a incidentes cibernéticos.

Recomendaciones

Recomendaciones Estratégicas con Énfasis en Operaciones Técnicas

1. Mejoras para el Blue Team (Defensa)

- **Implementar sistemas avanzados de monitoreo en tiempo real:** Adoptar herramientas de detección y respuesta extendida (XDR) para identificar amenazas emergentes con mayor precisión.
- **Fortalecimiento de políticas de acceso:** Revisar y actualizar las configuraciones de control de acceso y segmentación de redes para reducir el movimiento lateral de atacantes.
- **Capacitación continua:** Realizar simulaciones regulares de ataques cibernéticos para evaluar y mejorar las capacidades del equipo.

2. Mejoras para el Red Team (Ataque Simulado)

- **Ampliación de escenarios de ataque:** Crear y ejecutar pruebas basadas en amenazas reales y específicas para la industria a la que pertenece la organización.
- **Uso de herramientas de simulación de adversarios:** Incorporar plataformas como Cobalt Strike o Metasploit para realizar evaluaciones más completas de vulnerabilidades.
- **Análisis post-ataque:** Documentar detalladamente los hallazgos para traducirlos en acciones específicas de mitigación.

3. Recomendaciones Legales

- **Cumplimiento normativo:** Garantizar que todas las actividades estén alineadas con las regulaciones locales y estándares internacionales como ISO 27001 y NIST.
- **Gestión de incidentes:** Establecer un marco legal para la respuesta a incidentes que detalle las responsabilidades y comunicaciones con autoridades. Aplicación de la ISO 27035 que se encarga de la gestión de incidentes de seguridad.

Recomendaciones Estratégicas con Énfasis en Integración y Proactividad

1. Fortalecer la Cooperación entre Blue Team y Red Team

- **Implementar ejercicios de Purple Team:** Fomentar la colaboración entre equipos defensivos y ofensivos para cerrar brechas de seguridad de manera más eficaz.
- **Intercambio continuo de información:** Establecer protocolos regulares de retroalimentación y aprendizaje compartido entre ambos equipos.

2. Enfoque en Ciberseguridad Proactiva

- **Automatización de respuestas:** Incorporar tecnologías de inteligencia artificial y aprendizaje automático para detectar patrones anómalos y responder rápidamente.
- **Auditorías regulares:** Realizar revisiones periódicas de la infraestructura de TI para identificar y remediar puntos débiles antes de que sean explotados.

3. Concienciación y Cultura Organizacional

- **Formación a todos los niveles:** Implementar campañas de concienciación sobre ciberseguridad para todos los empleados.
- **Simulacros de crisis:** Realizar simulacros de respuesta a incidentes para medir la preparación general de la organización.

4. Marco Legal Integral

- **Gestión de riesgos legales:** Crear un equipo multidisciplinario que integre aspectos técnicos y legales para manejar riesgos complejos.
- **Contratos robustos con terceros:** Revisar y reforzar acuerdos de servicio para asegurar la protección de datos en toda la cadena de suministro.

Referencias Bibliográficas

Chuvakin, A., Schmidt, K., & Phillips, C. (2013). Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Syngress.

Beale, J., Baker, A., & Esler, J. (2007). Snort Intrusion Detection and Prevention Toolkit. Syngress.

Evans, R., Smith, J., & Taylor, P. (2023). Cyber Resilience through Continuous Testing: A Red Team Perspective. Journal of Cybersecurity Studies, 15(3), 25-40.

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Intelequia. (2021). Red Team y Blue Team - Funciones y Diferencias en Ciberseguridad. Recuperado de https://intelequia.com/es/blog/post/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

Kaspersen, H. (2022). Cybersecurity Governance: Legal and Ethical Dimensions. Springer.

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

Mandia, K., et al. (2014). Incident Response & Computer Forensics, Third Edition. McGraw-Hill Education.

Maynor, J. (2011). Metasploit Toolkit for Penetration Testing, Exploit Development, and Vulnerability Research. Syngress

MITRE. (2024). MITRE ATT&CK Framework. Recuperado de https://attack.mitre.org.

Moreno, Patricio. (2015). Técnicas de detección de ataques en un sistema SIEM (Security Information and Event Management. Usfq. (pp. 31-63)Abrir este documento utilizando ReadSpeaker docReader . http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

NIST. (2020). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.

Rajendran, J., Jyothi, V., & Karri, R. (2011). Blue team red team approach to hardware trust assessment. 2011 IEEE 29th International Conference on Computer Design (ICCD), 285-288. https://doi.org/10.1109/ICCD.2011.6081410

Veselin. (2023). Red Team y Blue Team: Roles y Estrategias en Ciberseguridad. Recuperado de https://veselin.es/red-team-y-blue-team-roles-y-estrategias-en-ciberseguridad/

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon University.