CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

ÓSCAR ALFREDO STUART QUIROZ

Tutor

EVER LUIS ARROYO BARÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERIA ECBTI

ESPECIALIZACION EN SEGURIDAD INFORMÁTICA

BOGOTÁ – 2024

Resumen

El informe desarrollado para CyberFort Technologies detalla un análisis exhaustivo de riesgos y vulnerabilidades en su infraestructura TI, empleando metodologías colaborativas entre los equipos Blue Team y Red Team, complementadas con evaluaciones legales. Las actividades llevadas a cabo incluyeron pruebas de penetración, simulaciones de ataques internos y externos, auditorías de configuración y análisis de cumplimiento normativo.

El análisis reveló vulnerabilidades críticas, como configuraciones débiles en firewalls, políticas insuficientes de control de acceso y falta de monitoreo constante en sistemas clave. Estas brechas representan riesgos significativos para la disponibilidad, integridad y confidencialidad de la información.

A partir de los hallazgos, se han diseñado estrategias de contención robustas, entre las que destacan la implementación de segmentación de redes basada en roles, la actualización y refuerzo de políticas de acceso con autenticación multifactorial, y la realización de simulaciones regulares de ataques (red teaming). Asimismo, se recomienda fortalecer el sistema de respuesta a incidentes mediante la capacitación continua del personal, la automatización de procesos clave y la adopción de herramientas avanzadas de detección y mitigación de amenazas.

Estas propuestas están alineadas con los estándares de seguridad y mejores prácticas internacionales, asegurando que la organización no solo mitigue riesgos

actuales, sino también establezca una base sólida para afrontar amenazas futuras de manera proactiva.

Tabla de contenido

Tabla de figuras

Glosario

ACTIVOS DE INFORMACIÓN: Recurso de información con valor para una organización que contiene datos críticos para sus operaciones y requiere protección ante posibles riesgos de seguridad

AMENAZA: Posible peligro que puede explotar una vulnerabilidad causando daño a una organización.

ANÁLISIS DE RIESGOS: Proceso para identificar y evaluar las amenazas, vulnerabilidades e impactos a los que está expuesta una organización.

CIBERSEGURIDAD: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.

CIFRADO: El cifrado es el proceso de codificar información para hacerla ininteligible e inaccesible a toda persona que no posea la llave de descifrado correcta.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

DELITO INFORMÁTICO: Conducta ilegal y no ética relacionada con el uso de tecnologías de información y comunicación para acceder sin autorización comprometiendo la

confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes o datos con el fin de causar un perjuicio.

ETHICAL HACKING: es una práctica común que consiste en hackear los sistemas informáticos propios para reforzar su seguridad.

HACKER: Usuario no autorizado que intenta o consigue acceder a un sistema de información.

INGENIERÍA SOCIAL: Conjunto de técnicas para manipular a las personas con el fin de obtener acceso no autorizado a un sistema y obtener información confidencial.

INTEGRIDAD: Es la característica que propende por mantener el estado de la información, la cual garantiza que no ha sido alterada y que se ha mantenido intacto el documento original que contenía dicha información.

MALWARE: Software dañino diseñado con propósitos maliciosos para comprometer sistemas y redes.

PRUEBAS DE PENETRACIÓN: Simulación autorizada de ataques a un sistema para identificar vulnerabilidades explotables antes que los atacantes.

RED TEAM: Grupo de expertos en ciberseguridad que emula tácticas y técnicas de atacantes reales con el objetivo de evaluar la seguridad de un sistema o una red de una organización.

VULNERABILIDAD: Debilidad en un sistema de seguridad informática que puede ser aprovechada por una amenaza para comprometer la confidencialidad, integridad o disponibilidad de los activos.

Introducción

La creciente dependencia de las infraestructuras tecnológicas para las operaciones críticas en organizaciones como CyberFort Technologies requiere de un análisis profundo de riesgos y vulnerabilidades. Este documento tiene como objetivo formular estrategias de contención a partir de la identificación y evaluación de amenazas potenciales en entornos de TI, asegurando la integridad, disponibilidad y confidencialidad de los activos digitales.

En el contexto del periodo de prueba realizado por CyberFort Technologies, este informe presenta un análisis integral desde las perspectivas del equipo Blue Team y Red Team, destacando hallazgos clave, debilidades identificadas y propuestas de mejora. Asimismo, se incorporan aspectos legales relevantes, alineados con los estándares de la industria, para garantizar la conformidad normativa y la protección de la organización frente a incidentes cibernéticos.

Además, se busca que las estrategias propuestas no solo mitiguen los riesgos existentes, sino que también fortalezcan la capacidad de respuesta ante futuros incidentes. Esto permitirá a la organización desarrollar una postura de seguridad proactiva, aumentando su resiliencia frente a un entorno cibernético en constante evolución.

Objetivos

Objetivo General

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

Objetivos Específicos

- Identificar riesgos y vulnerabilidades en la infraestructura TI mediante la ejecución de análisis técnico y simulaciones con equipos Blue Team y Red Team.
- Diseñar estrategias de contención específicas basadas en los resultados del análisis de riesgos, considerando los estándares de ciberseguridad y mejores prácticas legales.
- Generar un informe técnico gerencial que detalle los hallazgos y estrategias propuestas para su revisión en el área de Seguridad de CyberFort Technologies.

Desarrollo de la actividad

Actividad 1

Aspectos que aporten al desarrollo de estrategias de Red Team & BlueTeam.

Aspecto normativo y legal

A continuación, relaciono algunos artículos de la ley 1273 donde se regula delitos informáticos en Colombia.

Artículo 2. Interceptación de datos: El artículo tipifica el acceso y la interceptación de datos informáticos sin la autorización del titular. Si la organización o receptora utiliza sin autorización la información, evidenciamos que estaría vulnerado el artículo.

Artículo 3. Daño informático: Se refiere a las sanciones, cuando se afecta el sistema, la información y el software. Vulneración, los receptores dan uso indebido de la información confidencial de CyberFort Technologies, lo cual es un delito.

Artículo 4. Suplantación de identidad: Si los receptores llegan a utilizar la información confidencial, con el fin de actuar en nombre de la organización. Este acto vulnera este artículo.

Artículo 5. Protección de datos personales: Si los receptores no le dan el manejo adecuado a la información confidencial por lo establecido en la ley, corren el riesgo de incurrir en violación.

Artículo 6. Deber de confidencialidad: Si hay divulgación de datos a terceros por parte de los receptores, se estaría vulnerando este artículo.

Estrategias del Red Team

1. Reconocimiento y Recolección de Información: Identificar vulnerabilidades y puntos débiles en la infraestructura de CyberFort Technologies.

Métodos:

Escaneo de Red: Utilización de herramientas como **Nmap** para mapear la red y descubrir dispositivos y servicios activos.

Figura 1. Análisis de Nmap, para detección del sistema operativo y la versión.

```
# nmap -A -T4 scanme.nmap.org saladejuegos

Starting nmap ( https://nmap.org/ )
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11
Uptime 33.908 days (since Thu Jul 21 03:38:03 2005)

Interesting ports on saladejuegos.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
389/tcp  open  ldap?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
1002/tcp open  windows-icfw?
1025/tcp open  msrpc         Microsoft Windows RPC
1720/tcp open  H.323/Q.931   CompTek AquaGateKeeper
5800/tcp open  vnc-http      RealVNC 4.0 (Resolution 400x250; VNC TCP port: 5900)
5900/tcp open  vnc           VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```

Fuente: https://nmap.org/man/es/index.html

Ingeniería Social: Técnicas para obtener información confidencial a través de la manipulación psicológica de empleados.

Análisis de Inteligencia de Amenazas: Recolección de datos sobre amenazas conocidas y posibles vectores de ataque.

2. Explotación de Vulnerabilidades

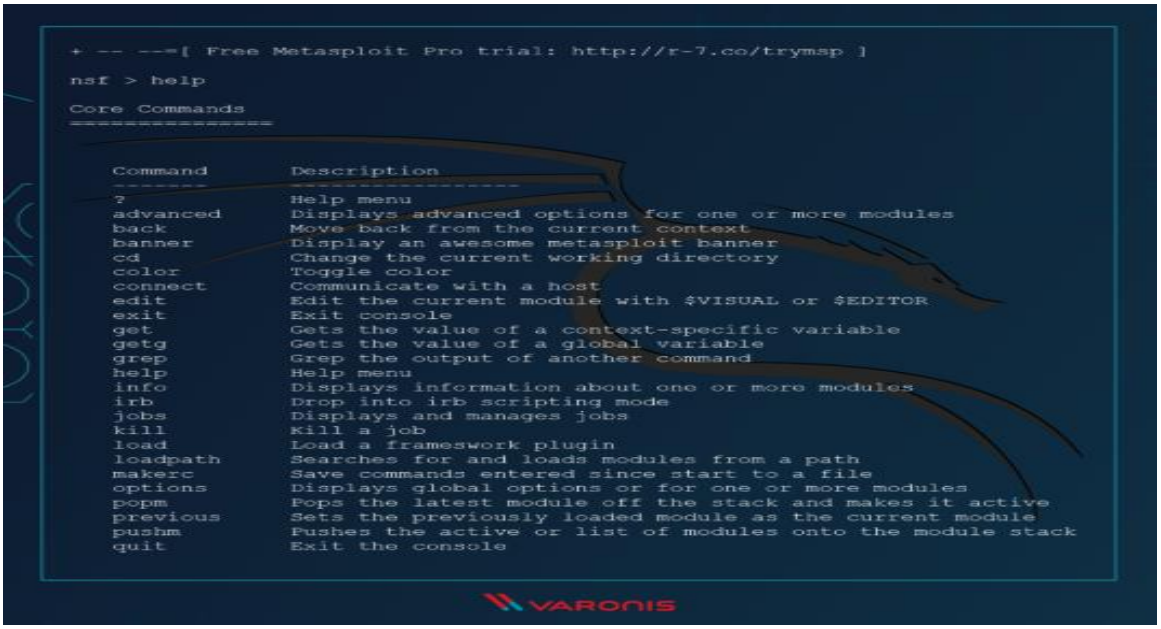
Objetivo: Comprobar la efectividad de las defensas actuales y la capacidad de respuesta del Blue Team.

Métodos:

Ataques Simulados: Ejecución de ataques controlados como phishing, explotación de software desactualizado y ataques de fuerza bruta.

Pruebas de Penetración: Uso de herramientas como **Metasploit** para explotar vulnerabilidades y obtener acceso no autorizado.

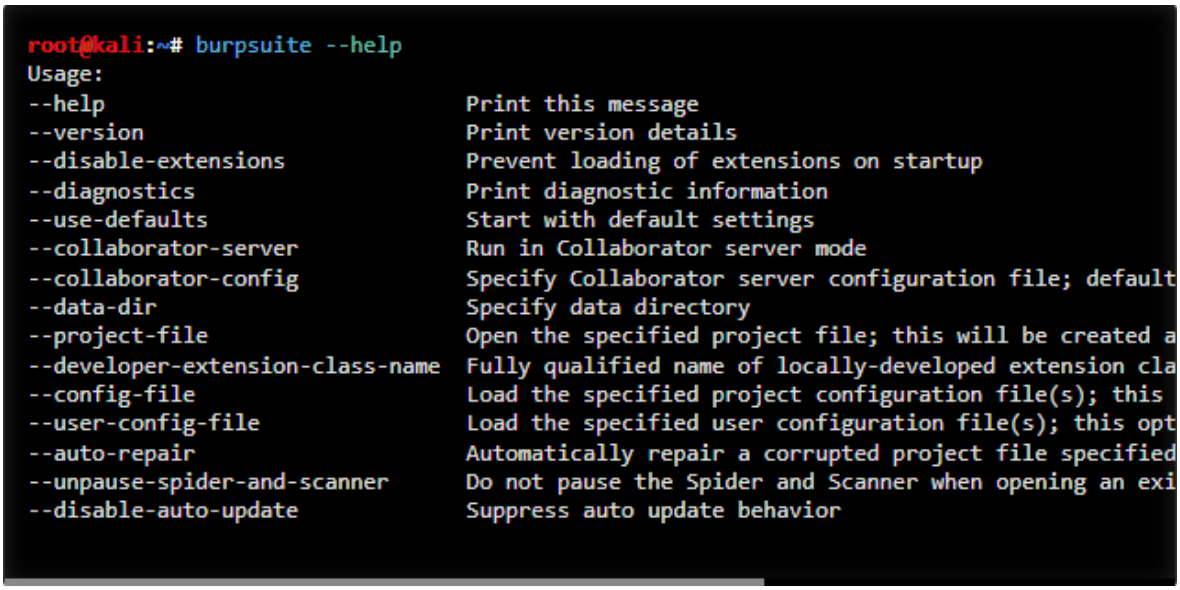
Figura 2. Descripción de comandos en Metasploit con help.



Fuente: https://www.varonis.com/blog/what-is-metasploit

Evaluación de Seguridad de Aplicaciones: Análisis de aplicaciones web y móviles para identificar y explotar fallos de seguridad utilizando herramientas como **Burp Suite.**

Figura 3. Comandos con su debida descripción de Burp Suite.



Fuente: https://www.kali.org/tools/burpsuite/

3. **Persistencia y Evasión**

Objetivo: Mantener acceso prolongado sin ser detectado.

Métodos: Ofuscación: Técnicas para ocultar la presencia de malware y actividades maliciosas.

Rootkits y Backdoors: Instalación de software que permite el acceso remoto y persistente al sistema comprometido.

Movimientos Laterales: Estrategias para moverse dentro de la red comprometida y acceder a otros sistemas y datos.

Estrategias del Blue Team

1. Monitoreo y Detección:

Objetivo: Identificar actividades sospechosas y anomalías en tiempo real.

Métodos:

Sistemas de Detección de Intrusos (IDS): Implementación de soluciones como **Snor**t para detectar tráfico de red anómalo.

Figura 4. Snort 3, funcionalidades para un desempeño más eficiente.

Fuente: https://www.snort.org/snort3

Análisis de Logs: Revisión y análisis de registros de eventos para identificar patrones de comportamiento inusuales.

Inteligencia Artificial: Uso de algoritmos de aprendizaje automático para detectar amenazas emergentes y comportamientos anómalos.

2. Respuesta a Incidentes:

Objetivo: Mitigar el impacto de los ataques y restaurar la normalidad operativa.

Métodos: Planes de Respuesta a Incidentes: Desarrollo de procedimientos detallados para responder a diferentes tipos de incidentes de seguridad.

Ejercicios de Simulación: Realización de simulacros de ataque para evaluar y mejorar la capacidad de respuesta.

Análisis Forense Post-Incidente: Investigación detallada de los incidentes para entender cómo ocurrieron y prevenir futuros ataques.

3. Fortalecimiento de la Seguridad:

Objetivo: Mejorar continuamente las defensas y reducir la superficie de ataque.

Métodos:

Actualización Regular de Software: Asegurar que todos los sistemas y aplicaciones estén actualizados con los últimos parches de seguridad.

Políticas de Seguridad Estrictas: Implementación de políticas claras y estrictas sobre el uso de contraseñas, acceso a datos y uso de dispositivos.

Formación Continua del Personal: Capacitación regular de los empleados en prácticas de seguridad y concienciación sobre amenazas.

Recomendaciones para el planteamiento de estrategias quepermitan endurecer los aspectos de seguridad en una organización.

Evaluación de Riesgos

Objetivo: Identificar y priorizar las amenazas y vulnerabilidades.

Métodos: Realizar evaluaciones periódicas de riesgos utilizando herramientas como OCTAVE y FAIR.

Implementación de Controles de Seguridad

Objetivo: Establecer medidas preventivas y correctivas.

Métodos: Utilizar frameworks como NIST CSF y ISO/IEC 27001 para implementar controles técnicos y administrativos.

Capacitación y Concienciación

Objetivo: Asegurar que todos los empleados estén informados y capacitados en prácticas de seguridad.

Métodos: Desarrollar programas de formación continua y simulacros de phishing.

Monitoreo y Respuesta a Incidentes

Objetivo: Detectar y responder rápidamente a incidentes de seguridad.

Métodos: Implementar sistemas de detección de intrusos (IDS) como Snort y soluciones SIEM como Splunk.

Gestión de Accesos e Identidades

Objetivo: Controlar el acceso a la información y sistemas críticos.

Métodos: Implementar soluciones de gestión de identidades y accesos (IAM) como Okta y Microsoft Azure AD.

La implementación de estas recomendaciones permitirá a la organización fortalecer su postura de seguridad, reducir riesgos y mejorar su capacidad de respuesta ante incidentes.

Conclusiones

La colaboración y el aprendizaje mutuo entre el Red Team y el Blue Team son esenciales para el desarrollo de una estrategia de ciberseguridad robusta. Las lecciones aprendidas de los ejercicios de Red Team deben ser utilizadas para fortalecer las defensas del Blue Team y viceversa. Este enfoque integral asegura que CyberFort Technologies esté mejor preparada para enfrentar y mitigar amenazas cibernéticas.

Conclusión técnica y operativa

El desarrollo de estrategias para Red Team y Blue Team en el contexto planteado por CyberFort Technologies requiere un enfoque integral que combine aspectos técnicos, operativos y legales. A partir del análisis realizado durante el período de prueba, se identificaron los siguientes aportes clave:

Para el Red Team:

La simulación de ataques realistas permitió identificar vulnerabilidades críticas en la infraestructura tecnológica, destacando la importancia de la planificación previa de escenarios que emulen amenazas actuales y futuras.

La incorporación de herramientas automatizadas para la evaluación de brechas, junto con la creatividad del equipo, fue determinante para la efectividad de los ejercicios.

Para el Blue Team:

La capacidad de respuesta ante incidentes se fortaleció al implementar un modelo de comunicación basado en tiempos de reacción medibles y la colaboración interdepartamental.

La importancia de un monitoreo continuo y el uso de inteligencia de amenazas en tiempo real fueron esenciales para mitigar riesgos proactivamente.

Estos hallazgos resaltan la necesidad de un enfoque coordinado, donde ambos equipos no solo operen como entidades independientes, sino también como partes de un ciclo iterativo de mejora en seguridad.

Conclusión estratégica y gerencial

La experiencia obtenida en el desarrollo de escenarios para CyberFort Technologies evidenció que una estrategia efectiva de seguridad cibernética debe basarse en la complementariedad entre el Red Team y el Blue Team. Entre los principales aprendizajes destacan:

Fortalecimiento de la planificación estratégica:

Los escenarios diseñados para el Red Team permitieron visibilizar áreas críticas que requerían intervenciones inmediatas, reforzando la importancia de entender al adversario y sus posibles vectores de ataque. Para el Blue Team, la incorporación de simulaciones

periódicas promovió una cultura de mejora continua y aprendizaje frente a incidentes simulados.

Impacto en la toma de decisiones gerenciales:

Los resultados obtenidos subrayan la relevancia de reportes claros y ejecutivos, útiles para decisiones informadas por parte de los analistas en Seguridad.

Asimismo, se destacó la necesidad de integrar aspectos legales y normativos en el diseño de estrategias, asegurando cumplimiento y protección frente a posibles repercusiones jurídicas.

En conclusión, la combinación de capacidades ofensivas (Red Team) y defensivas (Blue Team), junto con una visión alineada a los objetivos organizacionales, constituye la base para el fortalecimiento de la ciberseguridad corporativa.

Recomendaciones

Identificar y priorizar las amenazas y vulnerabilidades.

Realizar evaluaciones periódicas de riesgos utilizando herramientas como OCTAVE y FAIR.

Establecer medidas preventivas y correctivas.

Utilizar frameworks como NIST CSF y ISO/IEC 27001 para implementar controles técnicos y administrativos.

Asegurar que todos los empleados estén informados y capacitados en prácticas de seguridad.

Desarrollar programas de formación continua y simulacros de phishing.

Detectar y responder rápidamente a incidentes de seguridad.

Implementar sistemas de detección de intrusos (IDS) como Snort y soluciones SIEM como Splunk.

Controlar el acceso a la información y sistemas críticos.

Implementar soluciones de gestión de identidades y accesos (IAM) como Okta y Microsoft Azure AD.

La implementación de estas recomendaciones permitirá a la organización fortalecer su postura de seguridad, reducir riesgos y mejorar su capacidad de respuesta ante incidentes.

Referencias Bibliográficas

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

S2 Grupo. (2024). Red team: definición, funciones y diferencias con blue team. Recuperado de https://s2grupo.es/red-team-definicion-funciones-y-diferencias-con-blue-team/

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/

Policía. (2009). Ley 1273 [LEY_1273_2009]. Policía. (pp. 1-4). https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

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

Turner, J. (2015). Recon-ng: Web Reconnaissance Framework. GitHub.

Alberts, C., & Dorofee, A. (2003). Managing Information Security Risks: The OCTAVE Approach. Addison-Wesley.

Jones, J., & Ashenden, D. (2019). Measuring and Managing Information Risk: A FAIR Approach. Butterworth-Heinemann.

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. NIST.

International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. ISO.

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

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

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital Identity Guidelines. NIST.

Microsoft. (2021). Azure Active Directory Identity Management. Microsoft.

SANS Institute. (2020). Security Awareness Training. SANS.

KnowBe4. (2021). Phishing Security Test. KnowBe4.