Capacidades Técnicas y Legales de Gestión para Equipos Blue Team & Red Team

Leiner Bracho Ortega

Tutor

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

Durante el seminario "Equipos Estratégicos en Ciberseguridad: Red Team y Blue Team", realizamos actividades para aprender sobre las técnicas y procedimientos de estos equipos, que son fundamentales para detectar y corregir problemas de seguridad en las organizaciones. La UNAD nos proporcionó escenarios, bancos de trabajo y guías de configuración que facilitaron nuestro trabajo en cada fase, lo que nos permitió llevar a cabo las tareas de manera efectiva. En este documento, presentamos un breve resumen de las etapas y aspectos clave de las actividades que nos ayudaron a aprender más sobre los equipos Red Team y Blue Team, para ofrecer al lector una visión general de estos procesos.

Durante este tiempo, profundizamos en las leyes colombianas relacionadas con la seguridad informática y se creó un entorno de trabajo en varias versiones para hacer pruebas. En la segunda etapa, encontramos problemas en los acuerdos de confidencialidad entre las empresas, lo que puede dar lugar a abusos. En la tercera etapa, realizamos un ataque a los equipos configurados para detectar vulnerabilidades, usando diferentes herramientas de escaneo. En la cuarta etapa, implementamos controles para proteger las brechas encontradas y planeamos medidas a seguir en caso de un ataque al sistema. Finalmente, destacaremos lo más importante de cada etapa y ofreceremos consejos sobre diferentes casos, para que el lector pueda comprenderlos mejor y en la etapa final todo se concluye con las recomendaciones que se le pueden hacer a la Empresa para evitar ataque a su organización y el uso de herramienta que nos brinda seguridad para contener todos esos ataques y estar atento a cualquier acto sospechoso y sobre todo concientizar a todos sus empleados de la amenazas que pueden ser un ataque cibernético en nuestra organización .

Palabra claves: Amenazas, incidentes, seguridad, vulnerabilidades.

Abstract

During the seminar "Strategic Teams in Cybersecurity: Red Team and Blue Team", we carried out activities to learn about the techniques and procedures of these teams, which are essential to detect and correct security problems in organizations. UNAD provided us with scenarios, workbenches, and setup guides that facilitated our work in each phase, allowing us to carry out the tasks effectively. In this document, we present a brief summary of the stages and key aspects of the activities that helped us learn more about Red Team and Blue Team, to give the reader an overview of these processes.

During this time, we delved into Colombian laws related to computer security and created a working environment in several versions for testing. In the second stage, we find problems in confidentiality agreements between companies, which can lead to abuses. In the third stage, we perform an attack on computers configured to detect vulnerabilities, using different scanning tools. In the fourth stage, we implement controls to protect the gaps found and plan measures to follow in the event of an attack on the system. Finally, we will highlight the most important aspects of each stage and offer advice on different cases, so that the reader can understand them better and in the final stage everything is concluded with the recommendations that can be made to the Company to avoid an attack on your organization and the use of a tool that provides us with security to contain all these attacks and be attentive to any suspicious act and above all raise awareness among all your employees of the threats that can be a cyberattack on our organization.

Keywords: Threats, incidents, security, vulnerabilities.

CONTENIDO

Introducción 10

Objetivos 11

Aspectos al Desarrollo 12

Aspecto Red Team 12

Habilidades y Perfiles de los Miembros 12

Pentesting Prueba de Penetración 13

Ingenieria Social 13

Escala de Privilegio 13

Movilidad Lateral 13

OSINT Open Source Intelligence 13

Escaneo de Infraestructuta 13

Estrategia de un RedTeam 13

Planificación y Preparación 14

Analisis de la Organización Investigación Inicial 14

Estrategia pata el Blue Team 17

Configuraciones Seguras 17

Seguridad Perimetral 17

Aspecto Blue Team 18

Habilidades y Perfil de los Miembros del Blue Team 18

Gestión de Vulnerabilidades y Parches 18

Gestion Proactiva de Vulnerabilidades 18

Estrategias Protección Predictiva 19

Mejoras en la Respuestas a incidente y Gestion de Crisis 19

Planificación y Procedimiento Claros 19

Analisis Forense y Recuperación 20

Recomendaciones para el Planteamiento 20

Evaluación de Riesgo y Amenzas 20

Endurecimiento de los Sistemas Operativos y Servidores 21

Supervisión y Detección de Instruso 21

Seguridad de la Redes 21

Control de Acceso a la Red 23

Seguridad en Aplicaciones y Desarrollo 23

Pruebas de penetración 24

Uso de WAF Web Application Firewall 24

Monitoreo y Detección de Amenazas 22

Implementación de SIEM 24

Monitoreo de Comportamiento 24

Planificación y Simulación de Respuesta a Incidentes 25

Plan de Respuesta a Incidentes 25

Análisis post-incidente 25

Concientización y Formación Continua 25

Formación en Seguridad Cibernética 26

Simulaciones de Phishing 26

Cumplimiento Normativo y Auditorías 26

Cumplimiento con estándares de seguridad.....26

Conclusiones que Permitan la Construcción.....27

Ciberseguridad es un Proceso Continuo y Evolutivo 27

Importancia de un Enfoque Integral 27

Colaboración entre Equipos de Seguridad.....28

Defensa Profunda.....28

Redes Privadas Virtuales 29

Inteligencia de Amenazas 29

Cumplimiento Normativo y Estándares de Seguridad.....29

Conclusiones.....30

Recomendaciones 31

Bibliografía.....33

LISTA DE FIGURAS

pág.

Figura 1 Escaneo de Puerto Maquina Victima 15
Figura 3 Escaneo de Puerto Maquina Victima 16

GLOSARIO

Ataque informático: es un intento o una acción liberada para robar, exponer modificar, desactivar la seguridad de un equipo o varios con el fin de causar daños intencionados que afecten su funcionamiento lo cual accede sin permiso a una red

Blue Team: es un grupo de especialista en ciberseguridad que se compromete de proteger los sistemas de una empresa de posibles ciberataques.

Ciberseguridad: consiste en proteger computadoras, redes, aplicaciones, sistemas importantes y datos de amenazas digitales. Las empresas deben cuidar estos datos para sostener la confianza de sus clientes y seguir las leyes.

Delitos informáticos: son acciones ilegales que se realizan usando computadoras, redes o Internet. Pueden ir desde entrar sin permiso a datos hasta fraudes complicados y sabotajes. Estos delitos impactan tanto a personas como a empresas y gobiernos.

Exploit: es una herramienta o técnica que utiliza una falla en un sistema, aplicación o red para conseguir un objetivo no permitido, como acceder sin autorización, ejecutar código dañino, robar datos o interrumpir el servicio.

Hardenización: es el proceso de mejorar la seguridad de sistemas, dispositivos y redes para hacerlos menos vulnerables a amenazas. Esto incluye quitar configuraciones inseguras, desactivar servicios que no se necesitan y seguir prácticas que reduzcan las debilidades.

Malware: es un programa o código creado para dañar, interrumpir o controlar sistemas, redes o dispositivos sin permiso del usuario. Los atacantes lo usan para robar datos, espiar, sabotear o ganar dinero de actividades ilegales.

Metasploit: es una de las herramientas más popular y usadas en ciberseguridad para pruebas de penetración y evaluación de vulnerabilidades. Fue creada por H.D. Moore.

Nmap: Es una herramienta de open source muy usada para escanear redes y obtener información sobre sistemas, servicios y vulnerabilidades, es clave para administradores de sistemas y expertos en ciberseguridad en auditorías, monitoreo y pruebas de penetración.

Seguridad Informática: es un conjunto de expertos, en tecnologías y procesos que protegen sistemas, redes, dispositivos y datos de ataques, daños, entradas no autorizados o interrupciones.

Red Team: es un grupo de especialistas en ciberseguridad que simula ataques para evaluar la seguridad de una organización. Su objetivo principal es encontrar debilidades en sistemas, redes y procesos a través de simulaciones de ciberataques reales, con el fin de mejorar la seguridad general de la empresa.

INTRODUCCIÓN

La tecnología avanza a diario y se desarrolla a nivel global, haciendo que los sistemas informáticos sean fundamentales para el progreso humano, organizacional y social. Estos sistemas protegen datos valiosos, por lo que las organizaciones deben estar preparadas para posibles amenazas. En este contexto, los equipos Red Team y Blue Team son cruciales, ya que se encargan de garantizar la seguridad; uno simula ataques y el otro se defiende. Los integrantes del Red Team utilizan tácticas de ciberdelincuentes para intentar acceder a datos, mientras que el Blue Team debe tener habilidades para resistir estos ataques y estar atento a cualquier acto sospechoso que puedan vulnerabilidad nuestra defensa.

Ninguna empresa está a salvo de ciberataques, por lo que es esencial implementar medidas de control que minimicen sus efectos y vulnerabilidades. Los equipos especializados ayudan a identificar debilidades y mejorar la seguridad. Aunque este enfoque no se centra solo en pruebas de penetración, aborda temas relacionados y se orienta a proteger los recursos informáticos desde aspectos legales, operativos y técnicos, usando herramientas para pruebas, análisis y gestión de incidentes. .

OBJETIVOS

Objetivo General

Realizar las actividades propuesta para adquirir las habilidades necesarias, identificando vulnerabilidades y cómo fortalecerlas, así como corregir fallos de seguridad dentro de una organización para así contrarrestar los ataques o ser víctima de vulnerabilidades.

Objetivos Específicos

Sugerir estrategias efectivas para mejorar la seguridad en una empresa frente a incidentes informáticos y así evitar futuros ataques.

Sustentar desde el desarrollo del seminario especializado un video con nuestros puntos de vistas acerca de la desarrollado en el curso.

Realizar las actividades propuestas para adquirir las habilidades necesarias, identificando vulnerabilidades y cómo fortalecerlas, así como corregir fallos de seguridad dentro de una empresa.

Aspectos que Aporten al Desarrollo de Estrategias de Red Team & Blue Team.

El desarrollo de estrategias eficaces para los equipos de Red Team y Blue Team requiere una comprensión clara de sus roles, objetivos y la interacción entre ambos. Cada equipo desempeña una función clave en la protección de la infraestructura de TI de una organización: el Red Team simula ataques reales para reconocer vulnerabilidades, mientras que el Blue Team defiende activamente los sistemas ante esos ataques. Para que ambos equipos trabajen de manera eficiente y complementaria, se deben tener en cuenta varios aspectos clave que aporten al desarrollo de sus estrategias.

Aspecto Red Team: Aquí tienes algunas estrategias clave para un Red Team que te ayudarán a realizar evaluaciones ofensivas efectivas y a poner a prueba las defensas de una organización. Red team se refiere no solo a sus habilidades y roles, sino también a cómo se organiza y realiza las actividades de simulación de ataques en una organización. El Red Team está compuesto generalmente por expertos en ciberseguridad con una gran capacidad ofensiva. A continuación, te doy una visión más detallada de los aspectos clave de un Red Team, incluyendo el enfoque estratégico, las habilidades técnicas y la organización. Reconocimiento: en cualquier evaluación ofensiva es seleccionar la mayor cantidad de información posible.

Aspectos clave del Red Team serían los siguientes:

Habilidades y Perfiles de los Miembros del Red Team: los miembros del Red Team suelen ser profesionales altamente capacitados, con experiencia en tácticas, técnicas y procedimientos (TTPs) utilizados por atacantes reales. Sus habilidades incluyen

Pentesting (Pruebas de Penetración): Realizan evaluaciones de seguridad para identificar vulnerabilidades en sistemas, aplicaciones web y redes.

Ingeniería Social: Utilizan tácticas como phishing, vishing (phishing por voz), y smishing (phishing por SMS) para mentir a los usuarios y obtener acceso a sistemas o información.

Desarrollo de exploits: Crean y modifican herramientas de explotación para vulnerabilidades conocidas, e incluso explotan vulnerabilidades de día cero.

Escalada de Privilegios: Una vez que consiguen acceso, buscan maneras de obtener mayores privilegios en el sistema comprometido.

Movilidad Lateral: Se desplazan por la red comprometida para acceder a otros sistemas, utilizando herramientas de post-explotation.

OSINT (Open Source Intelligence): Según (Yong-Woon, 2022) Se refiere al proceso en el que cualquiera puede reunir y examinar información de código
abierto para generar datos útiles. Antes de hablar sobre OSINT, definimos cada término
de esta manera.

Escaneo de Infraestructura: Mapear puertos abiertos y servicios activos con herramientas como Nmap o Masscan. Analizar tecnologías usadas (CMS, frameworks, servidores) con Wappalyzer o WhatWeb.

Estrategia de un Red Team: se basa en simular ataques reales, utilizando tácticas, técnicas y procedimientos (TTPs) que emulan a los atacantes más avanzados. Su objetivo principal es identificar vulnerabilidades en la infraestructura de seguridad de una empresa, exponer puntos débiles y probar la capacidad de detección y respuesta de los equipos de defensa (Blue Team). Aquí te detallo las principales fases y componentes de la estrategia de un Red Team:

Planificación y Preparación: Antes de que comience cualquier ataque, el Red Team realiza una fase de planificación. Esta es crucial porque establece los objetivos y los límites del ejercicio. Las actividades que involucra son

Análisis de la Organización: Investigación Inicial: El Red Team realiza una recolección de información exhaustiva sobre la organización, buscando datos públicos (reconocimiento pasivo) que podrían facilitar el ataque.

Reconocimiento: El reconocimiento es la fase en la que el Red Team recopila la mayor cantidad de información posible sobre la empresa objetivo. Puede dividirse en dos tipos

Reconocimiento pasivo: recolección de información pública:

Redes sociales: Buscar perfiles de empleados para obtener detalles sobre contraseñas débiles o patrones de comportamiento.

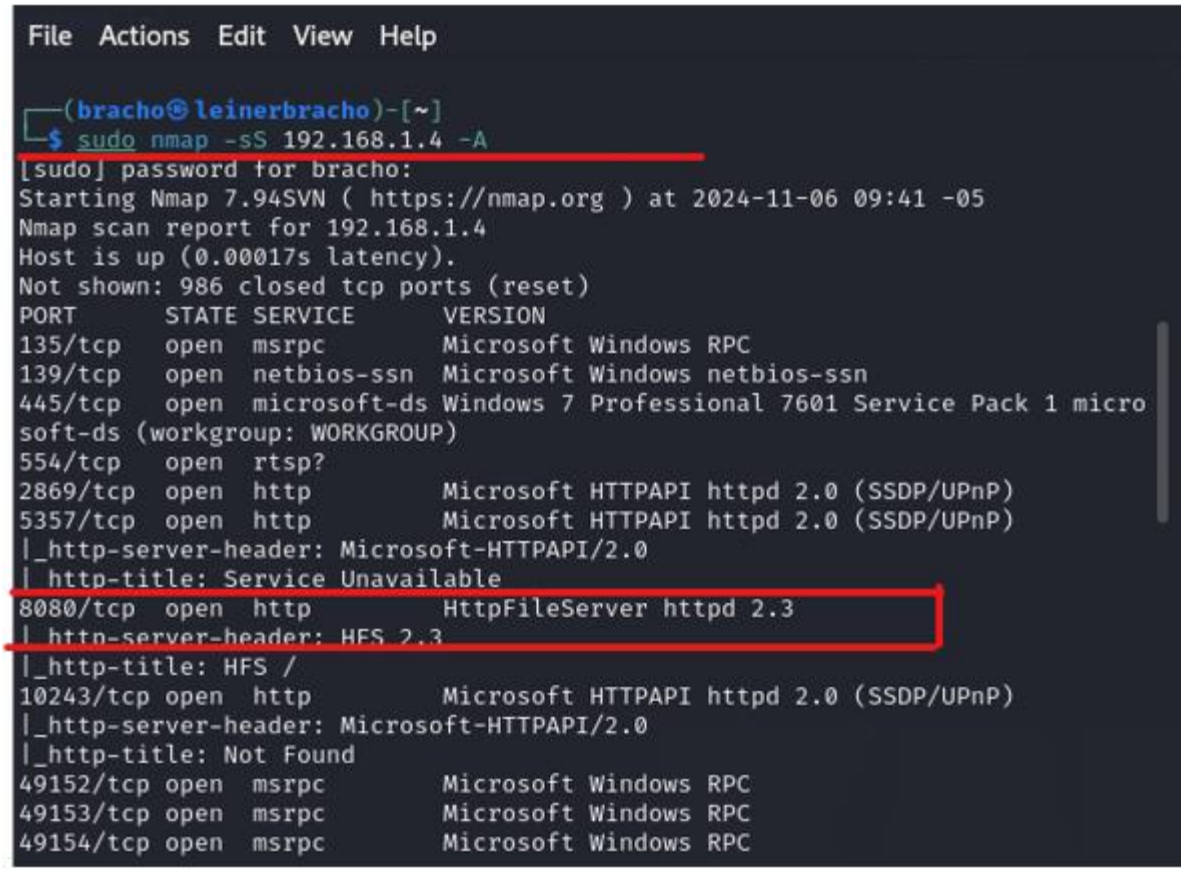
Reconocimiento activo:

Escaneo de red: Uso de herramientas como Nmap para mapear la red y detectar dispositivos conectados, puertos abiertos y servicios activos.

Escaneo de vulnerabilidades: Identificación de sistemas que puedan tener fallos de seguridad.

Figura1

Escaneo del puerto de nuestra maquina victima

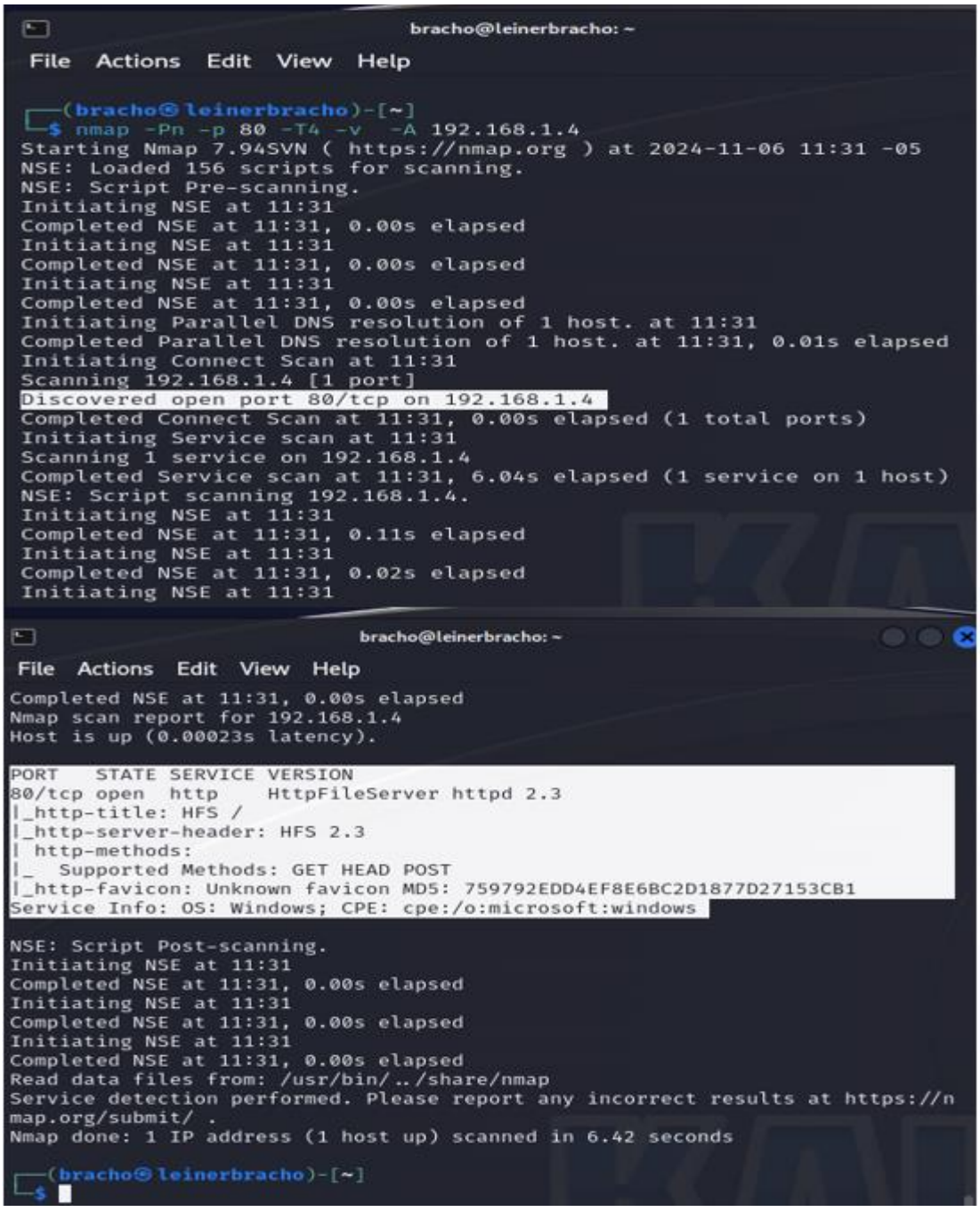


Nota: Leiner Bracho Ortega

Como podemos ver en nuestra figura con el comando sudo Nmap -sS 192.168.1.4 -A nos muestra la información de sus puertos y su estado indicado el 8080 esta abierto y podemos realizar nuestro ataque por ese puerto al parecer tiene una vulnerabilidad.

Figura 2

Escaneo puertos a nuestra maquina atacada



Nota Leiner Bracho Ortega

Como se puede ver en la figura anterior escaneamos los puertos con una serie de comando que nos arroja información mas detallada de nuestra maquina victima puerto abierto que es el 80 servicio y la versión y también nos muestra información del S.O.

Estrategias para el Blue Team: se encarga de proteger, monitorear y responder a las amenazas contra la infraestructura de una organización. Para lograrlo, necesita implementar estrategias sólidas y bien estructuradas. A continuación, se presentan las principales estrategias para un Blue Team eficaz:

Fortalecimiento Proactivo de la Infraestructura (Hardening): Asegurar los sistemas, aplicaciones y redes antes de que ocurra un ataque

Gestión de parches: Mantener sistemas y software actualizados contra vulnerabilidades conocidas.

Configuraciones Seguras: Deshabilitar servicios innecesarios, usar contraseñas robustas y limitar permisos de usuarios.

Seguridad Perimetral: Configurar firewalls, IDS/IPS y segmentar redes críticas.

Monitoreo y Detección de Amenazas: El monitoreo constante es clave para detectar actividades sospechosas.

SIEM (Security Information and Event Management): Centralizar y analizar logs de diferentes sistemas para identificar patrones anómalos. Configurar alertas basadas en indicadores de compromiso (IoCs).

Threat Hunting: Realizar búsquedas proactivas de amenazas ocultas en el entorno. Utilizar herramientas como Splunk, ELK Stack o Sentinel.

Podemos identificar como nos muestra las imágenes los escaneos de los puertos

Aspecto Blue Team: El Blue Team es el grupo encargado de defender los sistemas y activos digitales de una organización contra ataques cibernéticos. A diferencia del Red Team, cuyo enfoque es simular un atacante, el Blue Team se centra en proteger, detectar, y responder a las amenazas. El aspecto de un Blue Team abarca tanto las habilidades técnicas como las estrategias y herramientas utilizadas para salvaguardar la infraestructura de TI. Damos unos de los aspectos que debe tener el blue team desde sus habilidades técnicas hasta estrategias técnicas.

Habilidades y Perfil de los Miembros del Blue Team: el Blue Team está compuesto por profesionales de ciberseguridad con habilidades en áreas clave de defensa, detección y respuesta. Algunas de las principales habilidades y perfiles incluyen:

Gestión de Vulnerabilidades y Parches: son componentes clave en cualquier estrategia de seguridad informática, especialmente en un Blue Team. Ambas prácticas se centran en identificar, evaluar, corregir y mitigar riesgos asociados con fallos de seguridad en sistemas, aplicaciones y redes. La gestión de vulnerabilidades se refiere al proceso de descubrir y corregir debilidades en los sistemas, mientras que la gestión de parches se enfoca en actualizar los sistemas para corregir estas fallas.

Gestión Proactiva de Vulnerabilidades

Escaneo regular de vulnerabilidades: Implementar escaneos periódicos de la infraestructura utilizando herramientas como Nessus, Qualys o OpenVAS para identificar vulnerabilidades y remediarlas de manera priorizada.

Automatización del parcheo: Utilizar herramientas de gestión de parches para asegurar que todas las actualizaciones de seguridad se apliquen de manera oportuna y sin interrupciones en el negocio.

Estrategias de Protección Predictiva

Inteligencia predictiva: Utilizar herramientas de análisis predictivo que apliquen machine learning y big data para identificar patrones sospechosos y comportamientos anómalos en los sistemas de manera preventiva.

Reducción de superficie de ataque: Minimizar las áreas vulnerables mediante segmentación de red y limitación de acceso innecesario a recursos sensibles.

Mejoras en la Respuesta a Incidentes y Gestión de Crisis: son componentes fundamentales en cualquier estrategia de seguridad informática. Estos procesos permiten a las organizaciones gestionar de manera eficiente los eventos de seguridad, minimizar el impacto de los ataques y recuperar rápidamente las operaciones normales. Mejorar estos aspectos es crucial para reducir el tiempo de inactividad, proteger los activos críticos y asegurar la continuidad del negocio. Aquí te explico algunas de las mejores prácticas y estrategias que pueden mejorar la respuesta a incidentes y la gestión de crisis en tu organización.

Planificación y Procedimientos Claros

Planes de Respuesta a Incidentes (IRP): Desarrollar y mantener un plan detallado de respuesta a incidentes que defina roles, responsabilidades y pasos a seguir durante un ataque cibernético. Este plan debe ser actualizado regularmente según las nuevas amenazas.

Procedimientos de comunicación: Definir los procedimientos de comunicación durante un incidente, tanto para el equipo de respuesta interna como para la alta dirección, proveedores y posibles actores externos (fuerzas de seguridad, autoridades regulatorias).

Análisis Forense y Recuperación

Técnicas de análisis forense: Mejorar las habilidades en herramientas forenses como FTK Imager y EnCase para investigar el origen del ataque y recuperar evidencias digitales. Estrategias de recuperación y resiliencia: Asegurarse de que el equipo tenga conocimientos sólidos en planificación de recuperación ante desastres (DRP) y planificación de continuidad de negocio (BCP) para garantizar que los sistemas se restauren rápidamente después de un ataque.

Recomendaciones para el Planteamiento de Estrategias que Permitan Endurecer los Aspectos de Seguridad en una Organización

El endurecimiento de la seguridad (o "hardening") es un proceso crítico para mejorar la defensa de los sistemas de una empresa frente a posibles amenazas. Este proceso consiste en reforzar los controles de seguridad en todos los niveles de la infraestructura tecnológica, desde los sistemas operativos hasta las aplicaciones, redes y dispositivos. Para plantear estrategias eficaces que ayuden a endurecer la seguridad, es importante seguir un enfoque integral que abarque tanto la prevención, detección como la respuesta a incidentes. Podemos plantar unos aspectos que nos ayudaran para el planteamiento de estrategias que nos ayudan a fortalecer todos los aspectos de seguridad en una empresa como son:

Evaluación de Riesgo y Amenazas: Según codster (2021, 22 febrero) es una forma de identificar, clasificar y priorizar las debilidades de una aplicación, servicio u organización. Hacer este análisis puede ayudar a proteger su organización de posibles amenazas. Siguiendo estos pasos, podrá encontrar los riesgos más importantes y crear un plan para reducirlos y proteger sus activos clave.

Antes de realizar cualquier estrategia de endurecimiento, es esencial realizar una evaluación de riesgos para reconocer las amenazas más relevantes y las vulnerabilidades dentro de la infraestructura de la organización. Esto suministrará una base sólida sobre la cual construir las políticas y controles de seguridad.

Evaluación de vulnerabilidades: Realizar escaneos regulares con herramientas como Nessus, OpenVAS o Qualys para identificar vulnerabilidades en sistemas, aplicaciones y redes.

Análisis de impacto: Evaluar las consecuencias que tendría la explotación de cada vulnerabilidad para priorizar las acciones de remediación.

Identificación de amenazas internas y externas: Una de las medidas más fundamentales es endurecer los sistemas operativos y servidores de la organización para reducir las posibles superficies de ataque. Esto implica deshabilitar servicios innecesarios, aplicar parches de seguridad y configurar adecuadamente los sistemas.

Endurecimiento de los Sistemas Operativos y Servidores: Según Ciset (2022, 4 octubre) El "hardening" o endurecimiento informático es el proceso de reducir las vulnerabilidades en un sistema. Se logra implementando medidas de seguridad para estar preparados ante posibles ataques informáticos.

Una de las medidas más fundamentales es endurecer los sistemas operativos y servidores de la organización para reducir las posibles superficies de ataque. Esto implica deshabilitar servicios innecesarios, aplicar parches de seguridad y configurar adecuadamente los sistemas.

También nos recomienda para así aumentar nuestros sistemas informáticos

Cambiar la todas la claves cada 60 días y contraseñas fuertes

Desinstalación aplicaciones que no tenga sus licencias

Cerrar los puertos que no se estén utilizando

Actualización de S.O. y así obtener los parches de seguridad

Implementación de DLP y así impedir fuga de datos

Instalación de firewall

Deshabilitar servicios no necesarios

Hardening específico para servidores

Monitoreo de acceso

Supervisión y Detección de Intrusos: IBM (2024, 26 marzo) La disciplina de ciberseguridad que se encarga de cómo los usuarios acceden a los recursos digitales y qué pueden hacer con ellos se llama gestión de identidades y accesos (IAM). Estos sistemas protegen contra hackers y aseguran que cada usuario tenga solo los permisos necesarios para realizar su trabajo.

El control de acceso adecuado es clave para proteger los datos y sistemas más sensibles. Implementar controles estrictos de acceso basado en el principio de "mínimos privilegios" ayudará a limitar las oportunidades de explotación.

Unos de las principales detecciones de intrusos serian:

Autenticación multifactor (MFA)

Gestión de Identidades

Principio de menor privilegio

Seguridad de las Redes: Endurecer la seguridad de la red es esencial para proteger los activos organizacionales contra entrada no autorizados, ataques DDoS, malware, etc.

Según IBM (2024, 26 noviembre) Evitar que personas no autorizadas accedan a la red, identificar y detener ciberataques y problemas de seguridad, y asegurar que los usuarios autorizados puedan acceder de forma segura a los recursos que necesitan en el momento que los requieren.

La creación de sistemas de seguridad de red incluye el uso de las siguientes herramientas.

Segmentación de Redes: Crear redes separadas para diferentes funciones (por ejemplo, redes para usuarios, servidores y datos sensibles) y aplicar políticas de acceso estrictas entre ellas

Uso de firewalls y IDS/IPS: Implementar firewalls de nueva generación (NGFW) y sistemas de detección/preventivos de intrusiones (IDS/IPS) para filtrar tráfico malicioso y proteger la red.

VPN y cifrado: Asegurarse de que las comunicaciones de los usuarios remotos se realicen a través de una VPN cifrada. Utilizar protocolos de cifrado como TLS para proteger los datos en tránsito.

Control de Acceso a la Red: Utilizar herramientas de NAC (Network Access Control) para garantizar que solo los dispositivos autorizados puedan acceder a la red.

Sistemas de Detección y Prevención de Intrusiones (IDPS): Un sistema de detección y prevención de intrusiones, que también se llama sistema de prevención de intrusiones, se puede colocar justo después de un firewall para revisar el tráfico que entra en busca de amenazas. Estas herramientas son una evolución de los sistemas de detección de intrusos, que solo alertaban sobre actividades sospechosas para que se investigaran.

Según (red hat 2023, 27 septiembre) un sistema de detección y prevención de intrusiones (IDPS) es una herramienta que observa una red para identificar amenazas y actúa para detenerlas si las encuentra.

Seguridad en Aplicaciones y Desarrollo: La seguridad en las aplicaciones es crucial para proteger contra vulnerabilidades que podrían ser explotadas por atacantes. Esto incluye la implementación de prácticas de desarrollo seguro y la protección de aplicaciones web. Desarrollo seguro (Secure Coding): Implementar prácticas de codificación segura, como la validación de entradas, la prevención de inyección SQL y la protección contra cross-site scripting (XSS).

Pruebas de Penetración: Realizar pruebas de penetración (pentesting) regularmente en aplicaciones web, bases de datos y otras infraestructuras críticas para identificar y corregir vulnerabilidades.

Uso de WAF (Web Application Firewall): Implementar un WAF para proteger las aplicaciones web de ataques comunes, como inyección SQL o cross-site scripting.

Según (cloudflare 2024) Normalmente, defiende las aplicaciones de ataques como el engaño de sitios cruzados, el scripting entre sitios (XSS), la inclusión de archivos y la inyección de código SQL, entre otros

Monitoreo y Detección de Amenazas: Según (Hernández. J 2024) La mejor forma de disminuir los riesgos de las amenazas internas es enfocarse en la concienciación. Las iniciativas educativas ayudan a los miembros del equipo a saber cómo evitar errores graves. Además, les brindan el conocimiento para identificar posibles vulnerabilidades internas y qué hacer en esos casos.

Es crucial monitorear constantemente los sistemas para detectar cualquier actividad sospechosa que pueda indicar un ataque en curso o una vulnerabilidad explotada.
El proceso para detectar amenazas debe incluir varias actividades, como.

Implementación de SIEM: Usar soluciones de SIEM (como Splunk, ELK Stack o QRadar) para recopilar, analizar y correlacionar logs de seguridad en tiempo real, permitiendo una respuesta rápida ante incidentes.

Según (Exabeam 2024) se relaciona al proceso de poner en marcha y ajustar un sistema SIEM en la infraestructura de TI de una organización. Un sistema SIEM es una herramienta de seguridad que recolecta, analiza y relaciona datos de diferentes fuentes, como dispositivos de red, servidores y aplicaciones, para detectar y reaccionar ante posibles amenazas de seguridad en tiempo real.

Monitoreo de Comportamiento: Utilizar herramientas de EDR (Endpoint Detection and Response) y XDR (Extended Detection and Response) para monitorear el comportamiento de los endpoints y detectar actividades sospechosas.

Alertas y Respuesta Automática: Configurar alertas automáticas ante eventos críticos y definir procedimientos para la respuesta rápida a incidentes.

Planificación y Simulación de Respuesta a Incidentes: Aunque la prevención es fundamental, la capacidad de una empresa para responder rápidamente a un ataque es igualmente importante.

Plan de Respuesta a Incidentes: Desarrollar y mantener actualizado un plan de respuesta a incidentes (IRP) que detalle las acciones a seguir en caso de un ataque.

Simulaciones Regulares: Realizar ejercicios de simulación de incidentes, como tabletop exercises o simulaciones de ataques DDoS y ransomware, para sostener que los equipos de respuesta estén bien preparados.

Análisis Post-Incidente: Después de un incidente, realizar un análisis de root cause (causa raíz) para entender cómo se produjo el ataque y qué mejoras se pueden implementar.

Concientización y Formación Continua: los empleados son una de las mayores vulnerabilidades en cualquier organización, por lo que la formación en ciberseguridad es esencial.

Formación en Seguridad Cibernética: Ofrecer formación continua en ciberseguridad a todos los empleados, enfocándose en amenazas como phishing, malware y manejo seguro de contraseñas.

Simulaciones de Phishing: Realizar campañas regulares de simulación de phishing para educar a los empleados sobre cómo identificar correos electrónicos maliciosos y prevenir ataques de ingeniería social.

Según (Barracuda 2023) Proteja su organización de las amenazas de ingeniería social enseñando a sus empleados a reconocer y reportar estas situaciones. Los cibercriminales usan el phishing, que es un intento engañoso de robar información sensible como datos de tarjetas de crédito y contraseñas, haciéndose pasar por alguien de confianza en correos electrónicos.

Cumplimiento Normativo y Auditorías: cumplir con las normativas y regulaciones de seguridad es clave para asegurar que la organización cumpla con los estándares de la industria.

Cumplimiento con Estándares de Seguridad: Asegurarse de que la infraestructura y las políticas de seguridad estén alineadas con estándares como ISO/IEC 27001, NIST Cybersecurity Framework, GDPR, PCI-DSS, entre otros.

Auditorías regulares: Efectuar auditorías de seguridad periódicas (internas y externas) para evaluar la efectividad de las políticas de seguridad implementadas.

Correo electrónico seguro: Según (lacnic, 2012) el uso de certificados personales de empresa le permitirá proteger sus correos electrónicos. Así podrá firmar sus mensajes desde los clientes de correo más populares, asegurando su autenticidad e integridad.

Conclusiones que Permitan la Construcción del Conocimiento desde el Enfoque de la Ciberseguridad

La ciberseguridad es un campo en incesante evolución, impulsado por las amenazas emergentes, las nuevas tecnologías y la creciente interconexión de sistemas a nivel global. Construir conocimiento en ciberseguridad no solo implica aprender sobre herramientas y técnicas, sino también adoptar un enfoque integral que involucre tanto a las personas como a la tecnología, así como la gestión y la respuesta ante incidentes. A continuación, se presentan algunas conclusiones clave que pueden aportar significativamente a la construcción de un conocimiento robusto en este ámbito:

Ciberseguridad es un Proceso Continuo y Evolutivo: la ciberseguridad no es un conjunto de soluciones estáticas que una vez implementadas garantizan la protección de los sistemas a largo plazo. El panorama de amenazas está en constante cambio, con nuevas vulnerabilidades, vectores de ataque y tácticas de cibercriminales que surgen a diario. Por lo tanto, el enfoque hacia la ciberseguridad debe ser proactivo, con esfuerzos constantes de monitoreo, actualización y adaptación.

Importancia de un Enfoque Integral: Personas, Procesos y Tecnología: la ciberseguridad efectiva no depende únicamente de herramientas o tecnologías específicas, sino de un enfoque integral que abarque tres áreas clave:

Personas: Los usuarios finales son uno de los puntos más débiles de cualquier organización. La formación constante en ciberseguridad, la concienciación sobre riesgos (como phishing, ingeniería social) y el fomento de una cultura de seguridad son esenciales.

Procesos: Los procesos y políticas de seguridad deben estar bien definidos, estructurados y documentados, cubriendo aspectos como la gestión de vulnerabilidades, respuesta ante incidentes y gestión de identidades.

Tecnología: La tecnología es la herramienta que soporta las políticas y los procesos. Herramientas como firewalls, SIEM, EDR y WAF deben implementarse de manera adecuada y configurarse para maximizar su efectividad.

Colaboración entre Equipos de Seguridad: Red Team y Blue Team: El trabajo conjunto entre equipos ofensivos (Red Team) y defensivos (Blue Team) es clave para mejorar la postura de seguridad de una empresa. Mientras el Red Team finge ataques reales para descubrir vulnerabilidades, el Blue Team debe reforzar las defensas, aprender de los simulacros y ajustarlas de acuerdo con los hallazgos.

Defensa Profunda: (Ortegón. C,2019) según Es una estrategia critica en ciberseguridad que ayude a detectar, reducir y eliminar los ataques cibernéticos. Este término se aplica en diferentes áreas, incluyendo la seguridad de aplicaciones web. Ningún sistema o red debe depender de una sola barrera de seguridad; en cambio, deben aplicarse varias defensas en distintos niveles: perímetro, red, dispositivos, aplicaciones, datos y usuarios.

Es una estrategia crítica en ciberseguridad, que implica implementar múltiples capas de protección para minimizar el riesgo. Ningún sistema o red debe depender de una sola barrera de seguridad; en cambio, deben aplicarse varias defensas en distintos niveles: perímetro, red, dispositivos, aplicaciones, datos y usuarios.

Redes Privadas Virtuales: según (Viveros. J, 2015) Ofrecen seguridad a la red para usuarios lejanos, exigen autenticación y utilizan tecnologías para conectar a los recursos según sus reglas de acceso.

Respuesta Eficiente a Incidentes: Preparación y Simulación Constante: según (cci, 2023) es una guía que asegura que todos en la organización comprendan y puedan aplicar los pasos necesarios para responder a un ataque. Su objetivo es tener las herramientas adecuadas para identificar una amenaza y detener su expansión a otros equipos y sistemas de manera rápida.

Aunque las mejores medidas preventivas, los sucesos de seguridad seguirán ocurriendo. Por ello, es fundamental que las organizaciones tengan un plan de respuesta a incidentes bien definido y probado regularmente. Esto incluye procedimientos claros para detectar, contener, erradicar y recuperar de un ataque.

Inteligencia de Amenazas: Un Pilar Fundamental La inteligencia de amenazas proporciona información clave sobre las tácticas, técnicas y procedimientos (TTPs) utilizados por los atacantes. Las organizaciones deben integrar la inteligencia de amenazas para mantenerse al día con los riesgos emergentes y adaptar sus defensas de manera proactiva.

Cumplimiento Normativo y Estándares de Seguridad: Según (Globalsuite 2023, 25 septiembre) La ciberseguridad debe alinearse con las normativas y estándares de seguridad

pertinentes, como el RGPD, ISO/IEC 27001, PCI-DSS, NIST y otros marcos de referencia específicos. Cumplir con estos estándares no solo ayuda a mejorar la seguridad, sino que también minimiza el riesgo de sanciones y mejora la reputación de la organización.

CONCLUSIONES

Se realizo un informe detallado sobre el ataque, que incluyó la auditoría, las vulnerabilidades y la explotación. Todo esto se documentó para tener en cuenta futuros ataques similares. Aprendimos sobre la confidencialidad que deben tener todos sus empleados en todos momentos y debemos revisar todas las aplicaciones de nuestros sistemas para ver si una es vulnerable. Además, estudiamos un caso real de ciberataque y cómo, usando ciertas herramientas y procedimientos, pudimos encontrar los puntos de fuga de información. Esto nos ayudará a prevenir futuros ataques, ya que un solo puerto abierto puede poner en riesgo un sistema. También aprendimos a manejar un ataque en tiempo real y a proteger a una organización con herramientas que nos ayudarán a defendernos. En resumen, este trabajo mejoró nuestro entendimiento sobre los equipos de ataque y defensa, así como sobre las herramientas y controles a utilizar en estas situaciones.

RECOMENDACIONES

Es importante usar estrategias y métodos para reducir los ataques de hackers que intentan aprovecharse de organizaciones vulnerables, especialmente durante la pandemia. Aunque ningún sistema es totalmente seguro, se pueden implementar técnicas para disminuir el riesgo de ataques.

Se pide desarrollar y llevar a cabo una estrategia de ciberseguridad para evitar amenazas y proteger los recursos de las empresas. Hay herramientas de software y métodos que pueden ayudar a los usuarios a mejorar la seguridad en la empresa.

Es importante poner barreras físicas y seguir técnicas de control para proteger los recursos e información clasificada, así se pueden evitar problemas de ciberseguridad.

Como sugerencia final, es clave recordar los deberes y responsabilidades en la gestión de la seguridad de la empresa. Esto implica coordinar el proceso de seguridad, identificar y manejar riesgos, mantener la seguridad en orden, impulsar nuevos proyectos y garantizar que el sistema esté estable y protegido contra vulnerabilidades, tanto internas como externas.

Estar al día con las actuales amenazas y técnicas de ataque es crucial para defenderse bien y realizar actualizaciones periódicas a sus sistemas y también contar con un antivirus licenciados y actualizados.

También es importante contar con expertos en seguridad informáticas para realizar hacer auditorías de seguridad regularmente para encontrar y solucionar posibles vulnerabilidades antes de que sean aprovechadas por los atacantes.

Crear un manual de políticas de seguridad y buenas prácticas para evitar software malicioso y reducir el riesgo de amenazas donde se establezca restricciones como el uso de

memorias USB y las restricciones de página de mala procedencias y establecer contraseñas seguras y cada 60 días cambio de la misma.

BIBLIOGRAFÍAS

Barracuda (2023) Phishing Simulation https://www.barracuda.com/support/glossary/phishing-simulation

Blog (2022, 21 septiembre) Detección y Prevención de Amenazas Informáticas https://preyproject.com/es/blog/deteccion-y-prevencion-de-amenazas-su-guia-para-mantenerse-a-salvo

Cci (2023, 2 octubre) Plan de Respuesta a Incidentes de Ciberseguridad https://www.cci-es.org/plan-de-respuesta-a-incidentes-de-ciberseguridad/

CCN Cert. (2018). Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. (pp. 10-29). https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1617-ccn-stic-495-seguridad-en-ipv6/file.html

CIS Security. (2020). CIS Center for Internet Security. CIS Benchmarks. https://www.cisecurity.org/cis-benchmarks/

Codster (2021, 22 febrero) Cómo realizar un análisis de riesgos y vulnerabilidades https://codster.io/blog/seguridad-en-aplicaciones/aplication-vulnerability/como-realizar-analisis-de-riesgos-vulnerabilidades/

Cloudflare (2024) Qué es un WAF? | Explicación de Web Application Firewall https://www.cloudflare.com/es-es/learning/ddos/glossary/web-application-firewall-waf/

Exabeam (2024) SIEM Implementation in 4 Steps https://www.exabeam.com/explainers/siem/siem-implementation-in-4-steps/

Globalsuite (2023, 25 septiembre) Estándares y normas ISO para mejorar la ciberseguridad

https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/

Ibm (2024, 26 marzo) Qué es la gestión de identidades y accesos (IAM) https://www.ibm.com/es-es/topics/identity-access-management

Ibm (2024, 26 noviembre) Qué es la seguridad de red https://www.ibm.com/es-es/topics/network-security

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

Lacnic (2012) gestión de incidentes de seguridad informática https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

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

Ortegón. C. 2019 amenazas, vulnerabilidades, factores de riesgo y defensa en profundidad en aplicaciones web https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4913/00005093.pdf?sequence=1&isAllowed=y

Red hat (2023, 27 septiembre) What is an intrusion detection and prevention system (IDPS) https://www.redhat.com/en/topics/security/what-is-an-IDPS

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

Viveros, J. 2015 Defensa en profundidad para proteger la información de la red corporativa https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2930/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Yong-Woon. H, Im-Yeong. L, Hwankuk. K, Hyejung. L, Donghyun. K, 2022 *Current Status and Security Trend of OSINT https://onlinelibrary.wiley.com/doi/epdf/10.1155/2022/1290129*

Zambrano Hernández, Peña Hidalgo, H. J., & Cardenas Corral. (2024). Guía Para la Gestión y Clasificación de Incidentes de CiberseguridadAbrir este documento utilizando ReadSpeaker docReader . Sello Editorial UNAD. https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Gu%C3%ADa_para_la_Gesti%C3%B3n_y_Clasificaci%C3%B3n_de_un_Incidentes_de_Ciberseguridad.pdf

ANEXO

Enlace de Video: https://youtu.be/G9Sd1dr8WS4