Etapa 5 – Capacidades técnicas, legales y de gestión para equipos blue team y red team

Cindy Viviana Solano Vanegas

Director de curso

Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia UNAD

Vicerrectoría Académica y de Investigación

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

2024

Resumen

Este informe técnico generalizado plasmara las estrategias necesarias vistas en el seminario especializado de ciberseguridad donde toda la dinámica consiste en la recreación de dos equipos de trabajo llamados red team y blue team.

Donde los cuales se encargara de velar por la seguridad plena de un sistema de información creando reglas, normas y pasos a seguir ante cualquier eventualidad que se identifique como anomalía o riesgo en la seguridad implementada.

Como también tener siempre un plan de contigencia actualizado y con los últimos estándares internacionales para contener o adelantarse a posibles amenazas que indique el análisis comparativo en el comportamiento de la red o conexiones de dispositivos, siempre amparados a registros ya pre establecidos en base de datos centralizadas para estar siempre un paso adelante ante cualquier posible amenaza.

Palabras claves: Amenaza , Blue team , Ciberseguridad, Red team

Indice

Lista de Tablas

Lista de Figuras

Glosario

Redteam: Equipo encargado de recrear situaciones de riesgo eminente para probar los sistemas de seguridad implementados en una organización.

Blueteam: Grupo de trabajo encargado de siempre prevenir y estar a la vanguardia de lo ultimo en tecnología de ciberseguridad para simpre poder identifigar y neutralizar cualquier posible riesgo antes que este sea ejecutado, recibiendo información de ayuda de parte del equipo Read team para el mejorameinto continuo.

S.O: El sistema operativo es un conjunto de aplicaciones contenidas en un sistema para poder manejar de manera eficaz y amigable el hardware que pueda contener cualquier dispositivo o maquina de computo.

Escaneo: Es un proceso muy importante en cualquier sistema de seguridad por que ayuda a indetificar y corregir cualquier movimiento o situación irregular que pueda conllevar a una posible amenaza haciéndolo de una manera eficaz en tiempo real.

Phishing: Consiste en la implementación de diferentes técnicas de ingeniería social que sirven para por medio del engaño y falcedad poder extraer información confidencial o sensibles de cualquier dispositivo a maquina.

Malware: Aplicación o sentecias maliciosas, empaquetadas en diferentes tipos de presentación para disuair y engañar sistemas de seguridad establecidos dejando un roto donde se pueda filtrar, modificar o borrar la información.

Firewall: Es una herramienta necesaria que su función es actuar como barrera entre una red interna y una red externa para evitar cualquier posible amenaza en conexiones o accesos abusivos no autorizados.

Introducción

En la actualidad vivimos en un mundo moderno que esta interconectados digitalmente a diversos sistemas de informacion computacionales donde se manejan un universo infinito de servicios que conllevan a la facilidad de la vida cotidiana en todos los seres humanos, es por ello la impotancia de estar simpre a la vanguardia de la seguridad aplicando los ultimos estándares y manejo de buenas practicas para estar adelante ante las posibles amenazas o ataques inminentes. Por ello la necesidad plena de que la seguridad lleve una evolución igualitaria a los avances de la tecnología.

Objetivos

Objetivo General

Crear un informe de capacidades técnicas y legales de la gestión para equipos blue team y red team.

Objetivos Especificos

- Identificar los aspectos que cooperan los equipos de red team y blue tem para el desarrollo de sus estrategia.
- Definir configuraciones de seguridad que contienen los diferentes sistemas operativos para la prevención inmediata ante cualquier insidente informatico.
- Diferenciar los frentes de trabajo como los son el de monitoriar y analizar cualquier anomalía en sistemas informáticos al otro ámbito que va en responder ante insidentes de ciber seguridad.

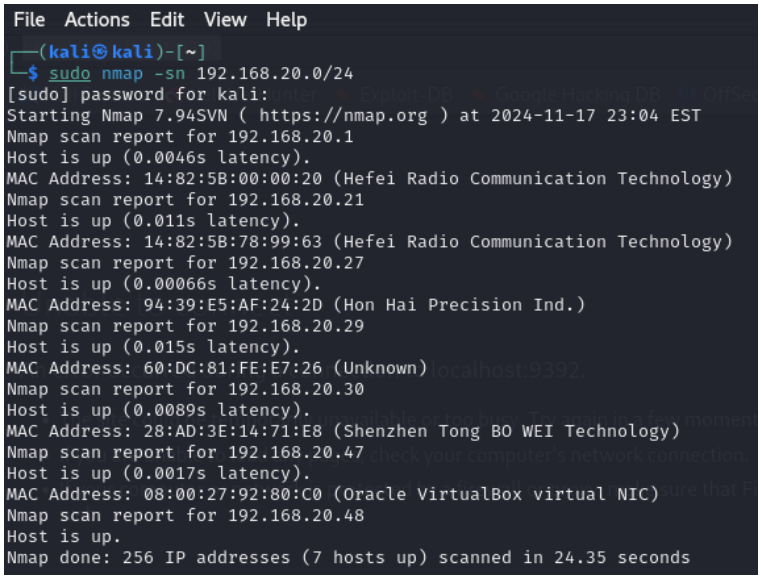
Desarrollo del informe

1. Análisis con acciones necesarias para contener un ataque en tiempo real.

La primera acción que realizaría seria indagar a la empresa si cuenta con un plan o guía de contigencia a seguir para estos casos y asi poder proteger la informacion y obviamente reportar a las áreas estipuladas en dicho documento, seguidamente evaluaría el funcionamiento de las herramientas existentes para la seguridad del sistema operativo como lo son el corta fuego y el antivirus principalmente.

Seguidamente revisaría la forma en que se esta asegurando la información es decir evaluaría el estado de las copias de seguridad existentes y que la información este contenida en ella, luego revisaría minusiosamente el estado de las conexiones de red que posee actualmente el equipo mediante la herramienta Nmap -sn 192.168.20.0/24. Imagen 1

Figura 1:Estado de la red

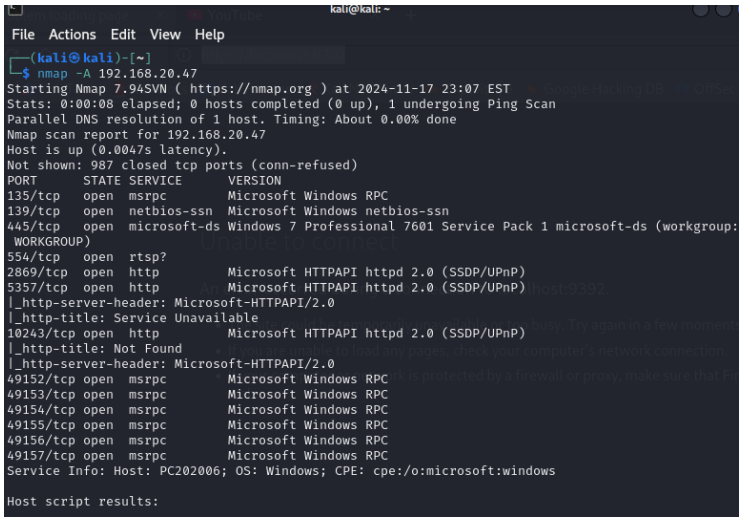


Fuente: Propia

posteriorente se requeriría el inventerio de direccionamientos ip de los dispositivos tecnológicos autorizados que se encuentran conectados a la red de la empresa y asi poder identificar fácilmente cualquier equipo no autorizado con acceso abusivo a la red.

En el caso de identificarlo se ejecutaria el comando nmap –A 192.168.20.47, para realizar el escaneo y asi obtener la detección de los puertos y servicios que tiene el equipo que esta haciendo atacado y asi deterinar e identificar el objetivo del ataque. Imagen 2

Figura 2: nmap –A 192.168.20.47



Fuente: Propia

2. **Informe de acciones de hardenización a implementar para evitar que sucedan ataques de seguridad informática.**

Para empezar se configura la funcionalidad de User Account Control para parametrizar los privililegios de acceso a las cuentas de usuarios del sistema operativo Windows como medida de control para evitar o mitigar los accesos abusivos no autorizados, también se puede elevar el nivel de seguridad por medio de la opción de configuracion de cuentas de usuario para que el sistema nos notifique o pida permiso de administrador, cuando alla cualquier evento de modificación de ficheros o instalación de programas y asi evitar el alojamiento o ejecución de aplicaciones maliciosas. Además se podría configurar la opción de biometría que trae también el Windows para validar accesos o permisos mediante la autenticacion biométrica.

Otra funcionalidad que podemos configurar para contener el riesgo es parametrizar el Bitlocker ya que permite cifrar las unidades de almacenamiento de información conectadas a la maquina para evitar fuga de datos; tambien podemos utilizar la herramienta AppLocker que nos ayuda a crear reglas donde podemos elegir el tipo de extensiones que se pueden ejecutar en el sistema operativo.

3. **Análisis sobre las diferencias entre el equipo de Blue Team y el equipo de respuesta a incidentes informáticos**

La diferencia entre el equipo Blue Team y el equipo de respuesta a incidentes informáticos en donde el equipo Blue Team es un grupo de personas espertas en el área de la

seguridad informtica que están en constante monitoreo de los diferentes sistemas tecnológicos que posea la compañía para poder detectar cualquier anomalía o acceso no autorizado en tiempo real y asi tomar medidas necesarias para mitigar el riesgo de perdida, copia, modificacion de la información contenida en toda la red de infraestructura tecnológica como también el constante mejoramiento de las políticas de seguridad y reglas establecidas en todo el sistema siempre en aras de mejorar la seguridad de los sistemas informáticos manejados por la compañía.

El equipo de respuesta de incidentes informáticos esta simpre a la espectactiva de la investigación, indagación en el mejoramiento y perfeccionamiento de la aseguridad informática para siempre estar a la vanguardia de las ultimas tendencias en seguridad teniendo siempre mejoras en reglas y políticas de seguridad a implementar con el fin de mitigar al máximo el riesgo que conlleva una red con acceso a internet pero también tiene mucha similitud con el equipo Blue Team por que deben estar alertas y disponibles en el momento de un ataque en tiempo real para poder identificar y restablecer las afectaciones que conlleven un ataque informatico y es aquí en donde este equipo de trabajo debe aplicar todas sus herramientas, reglas, mejoras y políticas aliadas en la investigación que vive constantemente para si restaurar de la mejor manera el buen funcinamiento de un sistema en el momento de ser atacado.

4. **Análisis sobre la pertinencia de trabajar con CIS "Center For Internet Security" como propuesta de aseguramiento por parte de un equipo de Blue Team.**

La aternativa de trabajar con CIS seria ideal como propuesta en la implementación de nuevos estadares a nivel mundial, mejorando las practivas en el uso de las tecnologías de la información y asi de esta manera elevar un poco mas el nivel de protección ante cualquier ataque y amaneza inminente, que pueda sufrir la compañía en sus sistemas implementados, además esto le daría un poco mas de apoyo en cualquier situación dada, por que dentro del plan de contingenia tendrían que estar estipulado el informar a dicha organización que se retroalimenta de diferentes reportes y contextos de todas empresas tecnológicas a nivel mundial, dándole un estatus y seguridad de estar siempre a la vanguardia en todo este ámbito de las tecnologías de la información.

Wasuo splut

5. **Análisis sobre las funciones y características principales de un SIEM.**

Para empezar debemos tener en claro que SIEM lleva contenidas dos tecnologías diferentes que son SIM (Security informatión Management) y SEM (Security Event Management) lo que nos indica que la primera tecnología SIM esta esplicitamente para monitoriar y administrar todo lo refetenes a la seguridad de la información, caso contrario de SEM que se encarga del monitoreo y administración de todos los eventos relacionados a la seguridad, en este orden de ideas un SIEM efectua ambas funciones simultáneamente al realizar el análisis y recolección de información de una manera centralizada para asi dar como resultado el poder mostrar eventos realizados según las actividades analisadas en los diferentes

movimientos generados y detectar amanazas inminentes en cuanto a la seguridad, dando respuestas en tiempo real ante cualquier incidente basándose en los moviminetos historicos cotidianos del sistema implementado y todos los dispositivos tecnológicos basados en el inventario tecnológico de hardware y software como uno de los aspectos a los que tiene encuenta para el análisis de conexiones y moviminetos en toda la red, de esta manera busca siempre a tener acciones anticipadas a tendencias inusuales según su comparación de análisis con los registros guardados y asi actuar de una manera muy rápida y contundente para prevenir cualquier tipo de ejecución malisiosa evitando que se convierta en amenaza para la seguridad de la información.

Tabla 1 *Funciones principales y características clves de SIEM*

FUNCIONES PRINCIPALES DE SIEM		**CARACTERISTICAS CLAVES DE SIEM**	
Recopilación de datos:	Crea registros de todo tipo de movimiento en la red tecnológica teniendo encuenta las fuentes de información como conexiones de todos los dispositivos autorizados, aplicaciones entre otros.	**Análisis de tiempo real:**	Detecta de manera muy rápida cualquier potencial amenaza basándose en los movimientos inusuales para dar respuesta en tiempo real.
Detección de amanezas:	Basándose en sentencias algorítmicas y en la creación de reglas de	**Visibilidad centralizada:**	La centralización de sus datos y la ilustración unificada permiten a los

	seguridad realiza simpre acciones anticipadas emitiendo alertas para las acciones oportunas ante cualquier riesgo o amenaza.		especialistas monitorear de una manera eficaz para identificar las amenazas y mitigarlas de una manera simultáneamente.
Correlacion de eventos:	Analiza cualquier tipo de actividad inusual en todo el sistema y lo correlaciona con sus registros históricos del comportamiento de la red para detectar cualquier amenaza potencial.	**Escabilidad**:	Capacidad de analizar metadatos y procesarlos de una manera fulminante y eficaz dando asi escabilidad y adactacion expontanea según las necesidades de la empresa.
Cumplimiento normativo:	Aplicando simpre estándares establecidos a nivel global encaminan a las empresas a cumplir con las normativas de seguridad y regulaciones realizando monitoreos constantes y auditorias periódicas al sistema	**Inteligencia artificial:**	Mediante lo ultimo en tecnología aplicada busca siempre la exactitud de la identificación de las amenazas minimizando las falsas alarmas.

	tecnológico de la informacion.		
Gestion de incidentes:	A través de la generación de informes de registros conlleva a la automatización de procesos para facilitar una respuesta rápida y oportuna a los incidentes que puedan ocurrir.	**Automatización de respuesta:**	Aplica herramientas como SOAR para la automatización de sus operaciones de seguridad en respuesta inmediata ante cualquier amenaza.

6. Informe de elección de 3 herramientas que permitan contener ataques informáticos

Firewalls : una de las principales herramientas que existen para contener ataques mediente conexiones fraudulentas no autorizadas crando siempre un muro entre las conexiones externas y cifrando los movimientos internos de los sistemas de información en los que este implementado de esta manera contraresta las posibles amenazas de acceso abusivo.

Cabe resaltar que esta eficaz herramienta esta tanto física como virtual (harware y software) y viene predetermidada en sistemas operativos Windows.

Gestores de contraseña: esta herramienta permite generar contraseñas de alto nivel de complejidad, también respalda el almacenamiento y protegiéndolas, de esta manera evita el uso de contraseñas de bajo nivel de seguridad basándose también en reglas preestablecidas.

Antivirus: fundamental aplicación de software especializado en la identificación, detención y corrección de cualquier setencia registro o conexión entre otras que considere maliciosas basándose en diferentes bases de datos centralizadas que contienen información retrolaimentada a nivel mundial y asi emitir una acción ya sea de alerta o mitigación de la amenaza o movimiento malicioso.

Conclusiones

Es de igual importancia la seguridad informática que el crecimiento digital y exponencial que estamos viviendo en nuestros mundos digitales, cada dia mas interconectados entre si y que por eso se llego a la necesidad de la creación de estadares internacionales y organismos de recolección de datos e insidentes en todo el mundo, para siempre estar a la vanguardia de la ciber seguridad proyectandoce siempre a estar un paso adelante ante millones de potenciales amanezas, que se dan a diario en el universo digital que hemos creado con el transcurso de los años.

Referencias Bibliográficas

(Copnia, 2003) Codigo de ética para el ejercicio de la ingenieria en general y susprofesiones afines y auxiliares. https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

(Ley-1273, 2009) pilicia código penal https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

(Guia, 2024) Guia para la gestión y clasificacion de incidentes de Ciberseguridad. 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

(Tecnicas, 2015) Técnicas de detenccion de ataques en un sistema SIEM (Segurity Information and Evenyt Management) https://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf