CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

JOHN FREDY LIZCANO OBANDO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CIUDAD
2021

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUETEAM Y REDTEAM

JOHN FREDY LIZCANO

Seminario de Especialización para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

M.Sc John F. Quintero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CIUDAD
2021

CONTENIDO

pág.

TABLA DE IMAGENES

INTRODUCCIÓN

En el siguiente trabajo se dará conocer la importancia de las estrategias por equipos de RED TEAM y BLUE TEAM en la evaluación y mantenimiento de la postura de seguridad de las organizaciones, por medio del estudio de un incidente de fuga de información, presentado por la empresa WhiteHouse, con lo cual se desarrollará un informe técnico como resultado del estudio de las causas del incidente y las contramedidas que se deben efectuar para evitar que este tipo de hechos se repitan en las organizaciones

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En la actualidad se ha acelerado la transformación digital, por lo cual muchas empresas ya tienen presencia en internet, ofreciendo diferentes servicios, esto sin duda genera una alta exposición a ciberataques. En el año 2020 se presentaron pérdidas por más de 4000 millones de dólares.

Dado este escenario la ciberseguridad en las diferentes organizaciones ha cobrado una gran importancia hasta el punto de que fue declarada como una de las principales preocupaciones en el 2020.

Aunque muchas organizaciones han implantado controles técnicos para proteger su información, en muchas ocasiones estos controles no operan de forma eficiente, esta situación no se hace evidente hasta que ocurren ciberataques, en la mayoría de los casos el vector del ataque ha sido una mala configuración y/o desactualización de un sistema informático y los ciberataques.

Como consecuencia de este panorama es de vital importancia realizar una constante evaluación de controles y vulnerabilidades por medio de pruebas de intrusión mediante equipos de Redteam, y a su vez verificar que tanta visibilidad y respuesta ante ciberataques por medio de equipos de Blueteam. de esta forma se podrá mejorar la postura de seguridad ante posibles ciberataques.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo enfrentar un incidente de ciberseguridad haciendo uso de las capacidades Técnicas, legales y de los equipos de BLUE TEAM y RED TEAM?

2 JUSTIFICACIÓN

En los últimos meses el 19% de las empresas en Colombia han sido afectadas por ciberataques los principales vectores han sido phishing y vulnerabilidades no identificados y/o gestionadas incorrectamente, teniendo en cuenta que las vulnerabilidades son el pan de cada día de los sistemas informáticos es fundamental contar con pruebas de intrusión mediante equipo de Redteam y detención de amenazas mediante equipo de Blueteam

Dado el impacto económico que ha tenido durante los últimos años los ciberataques, estimado en una pérdida de 4000 millones de dólares para el 2020 se convierte en una necesidad para mejorar la postura de seguridad de las organizaciones, ya que dan una visual más realista del nivel de ciberseguridad en las organizaciones y que tan preparadas están ante un ciberataque real.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Evidenciar mediante un informe técnico las estrategias y capacidades de los equipos de RED TEAM y BLUE TEAM, como una herramienta en la Evaluación y mejoramiento de la postura de seguridad de las organizaciones

3.2 OBJETIVOS ESPECÍFICOS

- Abordar los aspectos éticos y legales relacionados con los ejercicios de BLUE TEAM y RED TEAM

- Identificar y experimentación de las fases para la realización de pruebas de pentesting como parte de las capacidades técnicas de los Equipos de RED TEAM explotación

- Conocer las capacidades de identificación y contención de incidentes de ciberseguridad usadas por equipo de BLUETEAM

- Identificar las estrategias usadas para evitar un ciberincidente

4 MARCO TEÓRICO

Descubrir las debilidades del sistema y evaluar las ciberdefensas existentes son las mejores formas que tienen las organizaciones para frustrar las posibles ciberamenazas y mantener la seguridad operativa. Sin embargo, a la mayoría de las organizaciones les resulta difícil detectar nuevas infiltraciones cibernéticas y rutas de ataque adoptadas por los ciberdelincuentes para violar las defensas de TI organizativas de todo el sistema. Aquí es donde entra en juego un ejercicio cibernético del equipo Red & Blue para proteger los puntos de infiltración de datos y parchear las vulnerabilidades de la red.

En ciberseguridad, los términos equipos rojo y azul se usan para describir las habilidades para imitar un vector de ataque que un hacker (Red Team) podría usar mientras la línea de defensa (Blue Team) usa sus habilidades para defender el sistema. El escenario puede ser muy desafiante, con los principales cerebros enfrentados entre sí. Para perfeccionar sus habilidades como experto en ciberseguridad, es mejor utilizar la plataforma adecuada para obtener una comprensión más profunda del proceso.

4.1 ¿QUÉ ES EL RED TEAM?

Según lo define la Agencia de Seguridad Nacional de EE. UU. (NSA), un Red Team es un equipo que se especializa en la adquisición de información clasificada y sin dejar rastro. En el ámbito cibernético, los equipos de Red se centran en las pruebas de penetración de diferentes sistemas y sus niveles de seguridad. Ayudan a detectar, prevenir y eliminar debilidades al tiempo que destacan las vulnerabilidades evidentes. Un Red Team hace esto imitando el uso cibernético del mundo real de todas las técnicas de penetración de datos / redes existentes. Esto ayuda a las organizaciones a identificar las vulnerabilidades que pueden representar una amenaza para su sistema.

Figura 1 Equipo Red Team

Fuente: Red team Disponible en: https://www.segurilatam.com/tecnologias-y-servicios/ciberseguridad/el-red-team-como-metodo-de-prevencion-de-ataques-dirigidos_20170401.html

4.2 ¿QUÉ ES EL BLUE TEAM?

A la par con el Red Team, un Blue Team tiene la tarea de salvaguardar la seguridad de la red de una organización y descubrir posibles vulnerabilidades. A diferencia del Red Team, al Blue Team se le confía el refuerzo de la defensa de la red, al tiempo que garantiza una respuesta rápida a incidentes en caso de un ciberataque exitoso, independientemente del daño infligido.

Figura 2 Blue Team

Fuente: Blue Team Disponible en: https://codespaceacademy.com/blog/tecnicas-blueteam-nuevas-amenazas/

4.3 PRINCIPALES HABILIDADES DEL RED TEAM Y AZUL

Los equipos rojos y los equipos azules difieren de manera única en su enfoque, principalmente debido a las técnicas y los parámetros operativos. Una comprensión profunda de las técnicas de cada equipo le brindará más información sobre sus respectivos roles y propósitos. Con este artículo, también obtendrá una comprensión más profunda de sus habilidades y si coinciden con la descripción del trabajo o no.

4.4 HABILIDADES DEL RED TEAM

Los miembros del Red Team deben comprender cómo funciona la mente de un atacante y ponerse en el lugar del atacante, entendiendo su creatividad de vector de ataque.

- Enfoque listo para usar

La característica principal de un Red Team es pensar de manera innovadora, ya que siempre están buscando nuevas herramientas y técnicas para infiltrarse en puntos de datos vulnerables y, al mismo tiempo, brindar más claridad para proteger mejor los sistemas. Como miembro del Red Team, irás en contra de las reglas y la legalidad mientras sigues técnicas de sombrero blanco para mostrarle a la gente las fallas en sus sistemas.

- Conocimiento profundo de los sistemas

Para ser parte de un equipo Red exitoso, debe poseer un conocimiento profundo de los sistemas informáticos, bibliotecas, protocolos y metodologías conocidas.

También necesitará conocer servidores y bases de datos para poder ejercer múltiples opciones de ataque cuando se trata de descubrir la vulnerabilidad de un sistema.

- Desarrollo de software

Hay beneficios sustanciales si sabe cómo desarrollar sus propias herramientas. El software de escritura necesita mucho aprendizaje y práctica evolucionados, pero será útil para realizar las mejores tácticas ofensivas.

- Pruebas de penetración

Las pruebas de penetración son la simulación de un ataque a los sistemas de red para evaluar su seguridad. Pentesting ayuda a descubrir vulnerabilidades y amenazas potenciales para proporcionar una evaluación de riesgos completa. Por lo tanto, es importante que los equipos rojos puedan realizar pentesting, y está incluso entre sus procedimientos estándar.

- Ingeniería social

Durante las auditorías de seguridad, los equipos rojos deben poder manipular a las personas para que realicen acciones que puedan conducir a la exposición de datos confidenciales. Esto se debe a que el error humano se encuentra entre las causas de las filtraciones y filtraciones de datos.

4.5 HABILIDADES DE BLUE TEAM

Un Blue team debe tener la capacidad de cerrar puertas traseras y debilidades que la mayoría de la gente desconoce.

- Organizado y orientado a los detalles

Encajará mejor en un Blue team si sigue las reglas y prefiere usar métodos probados y confiables. Debe estar orientado a los detalles para no dejar brechas en la infraestructura de seguridad de una organización.

- Análisis de ciberseguridad y perfil de amenazas

Durante la evaluación de la seguridad de una organización, necesitará la habilidad para crear un perfil de riesgo o amenaza. Un buen perfil de amenazas comprende todos los datos, incluidos los atacantes de amenazas potenciales y los escenarios de amenazas de la vida real, y una preparación minuciosa para futuros ataques trabajando en las partes vulnerables del sistema.

- Técnicas de endurecimiento

Antes de que una organización pueda estar totalmente preparada para cualquier ataque, se necesitan técnicas de endurecimiento técnico de todos los sistemas para reducir la superficie de ataque que los piratas informáticos pueden explotar.

- Conocimiento de los sistemas de detección

Un Blue team debe estar familiarizado con las aplicaciones de software para rastrear la red en busca de cualquier actividad inusual y maliciosa. Si sigue todo el filtrado de paquetes, el tráfico de red, los cortafuegos existentes, etc., podrá controlar mejor todas las actividades de los sistemas de red.

- Gestión de eventos e información de seguridad (SIEM)

Este es un sistema que proporciona análisis en tiempo real de eventos de seguridad. Con este software, puede recopilar datos de fuentes externas

5 DESARROLLO DEL INFORME

5.1 ASPECTOS LEGALES Y ETICOS EN LOS EQUIPOS DE RED TEAM Y BLUE TEAM

De acuerdo con la problemática de la empresa WhiteHouse, Los equipos de RED TEAM Y BLUE TEAM deben tener en cuenta que en la legislación colombiana se contemplan los delitos informáticos y por lo cual se expidió la ley 1273 de 2009 esta ley debe ser el marco de actuación tanto para la ejecución de los ejercicios de equipo de Red Team como para la identificación de posibles delitos informáticos por parte del Blue Team. esta ley indica los siguiente:

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones. 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para sí o para un tercero. 6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave.

Por otra parte, las profesiones relacionadas con la ingeniería, que son generalmente las profesiones que ostentan los integrantes de los equipos de RED TEAM y BLUE TEAM, tiene un código de actuación ética que es expedido por el COPNIA (Consejo Profesional Nacional de Ingeniera), el cual es el ente que vela por el ejercicio ético de la ingeniería en Colombia y se debe tener en cuenta que como ingeniero se está obligado a cumplir en este código el menciona que no se debe facilitar, permitir y/o tolerar ejercicios ilegales de la profesión.

5.2 FASES PARA EL DESARROLLO DE LAS PRUEBAS DE PENTESTING DESARROLLADAS POR EL EQUIPO DE REDTEAM

Para la prueba de pentesting desarrollada para la empresa WhiteHouse con el fin de identificar la brecha de seguridad que permito la exfiltración de información se llevaron a cabo las siguientes fases.

5.2.1 Interacciones previas al compromiso

Esta fase a menudo se pasa por alto, sin embargo, es una de las fases esenciales de las pruebas de penetración. Aquí, el pentester aprende todo lo que puede sobre la empresa objetivo. El pentester trabaja con sus empleados para comprender a fondo su postura de riesgo, cultura organizacional y, en consecuencia, la mejor estrategia de prueba de penetración para implementar.

También se conoce como la fase de recopilación de información. Es la etapa en la que el pentester planifica el ejercicio de prueba y alinea los objetivos organizacionales con los resultados específicos del pentesting.

5.2.2 Reconocimiento

También llamado recopilación de inteligencia de código abierto (OSINT), el reconocimiento implica el uso de la información recopilada para acumular inteligencia adicional sobre los objetivos potenciales de fuentes disponibles públicamente. Esta etapa es importante porque permite que el pentester recopile información adicional que puede haberse pasado por alto anteriormente.

El pentester aplica una extensa lista de verificación para descubrir puntos de entrada abiertos y fallas dentro de la organización. OSINT Framework ofrece características específicas para fuentes de información abiertas.

El tipo de prueba de lápiz que acuerde determinará cómo el evaluador puede recopilar varias formas de información sobre su organización para determinar los puntos de entrada y las debilidades en su entorno.
Algunas de las metodologías estándar de recopilación de inteligencia incluyen ingeniería social, consultas en motores de búsqueda, seguimiento, registros de

impuestos, búsquedas de nombres de dominio / búsquedas de WHOIS o huellas de Internet (por ejemplo, direcciones de correo electrónico, DNS inverso, nombres de usuario, rastreo de paquetes, redes sociales o barridos de ping), etc.
.

5.2.3 Modelado de amenazas e identificación de vulnerabilidades

La siguiente fase es el modelado de amenazas y el análisis de vulnerabilidades. Aquí, el pentester señala los objetivos y mapea los vectores de ataque. Los escáneres de vulnerabilidades detectan las amenazas a la seguridad que plantean las lagunas al descubierto. Posteriormente, el probador determinará si los defectos descubiertos son explotables.

Los probadores de penetración mapearán e identificarán los activos comerciales de una organización y clasificarán los activos de alto valor, como datos de clientes, datos de empleados y datos técnicos. El evaluador también identificará y clasificará las amenazas internas (proveedores, empleados o administración) y amenazas externas (tráfico de red, puertos, protocolos de red o aplicaciones web).

5.2.4 Explotación

Toda la información se reúne y el pentester comienza a probar los exploits ubicados dentro de su aplicación, red y datos. Esta fase tiene como objetivo comprender con precisión cómo los atacantes pueden ingresar a su entorno y evadir la detección. El pentester puede realizar ingeniería social, ataques a aplicaciones web, ataques físicos, ataques a la red y ataques basados en la memoria, entre otros, como tácticas de explotación.

5.2.5 Post explotación

Los procesos posteriores a la explotación implican análisis de riesgos y recomendaciones. Esta fase de las pruebas de penetración tiene como objetivo registrar las técnicas explotadas para obtener acceso a los activos críticos de una organización. El probador determina la importancia del sistema comprometido y la importancia de los datos recopilados.

Posteriormente, el pentester hace recomendaciones basadas en estos hallazgos. El probador también debe realizar limpiezas después del ejercicio de prueba. Esto puede incluir eliminar cualquier rootkit instalado en el entorno, eliminar cualquier cuenta de usuario inventada para conectarse al sistema violado, eliminar archivos temporales, scripts, etc.

5.2.6 Presentación de Informes

El pentester recopila todos los detalles de la explotación y documenta las técnicas explotadas para obtener acceso al activo crítico de una organización. El hacker ético

prepara un informe detallado que cubre todas las actividades en las cinco fases anteriores de los esfuerzos de pruebas de penetración. Incluye cómo se detectaron y explotaron las vulnerabilidades. Aparte de esto, el informe también le informará sobre las metodologías de prueba, los resultados y las recomendaciones para las correcciones.

Seguir una serie de fases de forma organizada para la ejecución de las pruebas de pentesting es una estrategia que garantiza la ejecución efectiva de pruebas por parte del RED TEAM

5.2.7 Herramientas comúnmente usadas por los equipos de REDTEAM

5.2.7.1 Metasploit

es el marco de automatización de pruebas de penetración más utilizado en el mundo. Metasploit ayuda a los equipos profesionales a verificar y gestionar las evaluaciones de seguridad, mejora la conciencia y arma y permite a los defensores estar un paso adelante en el juego

Figura 3 Metasploit

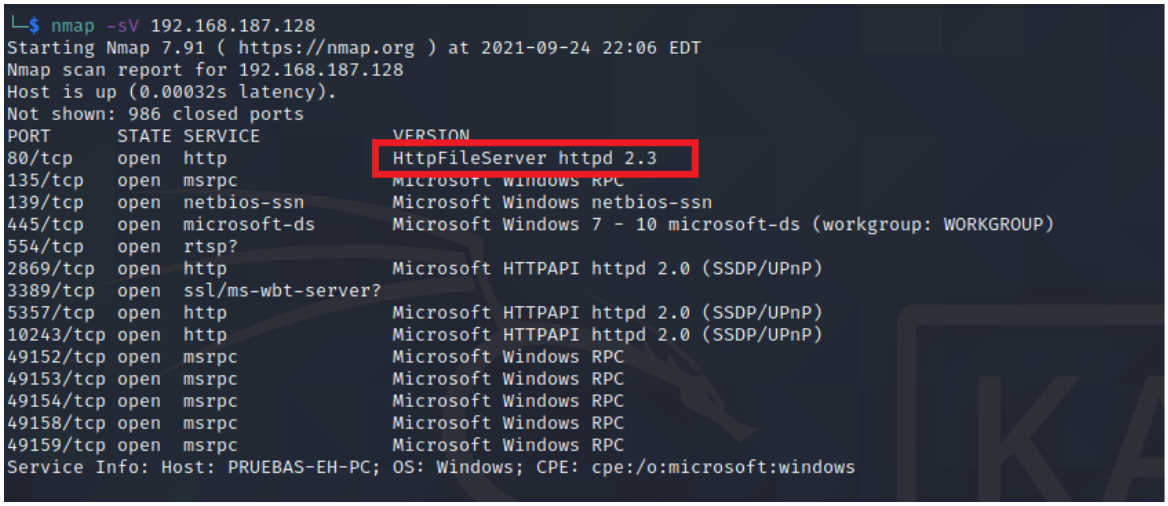
Fuente: Autor

5.2.7.2 Nmap:

es la abreviatura de Network Mapper. Es una herramienta de línea de comandos de Linux de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas.

Nmap permite a los administradores de red encontrar qué dispositivos se están ejecutando en su red, descubrir puertos y servicios abiertos y detectar vulnerabilidades.

Figura 4 Nmap



Fuente: Autor

5.2.7.3 Kali Linux

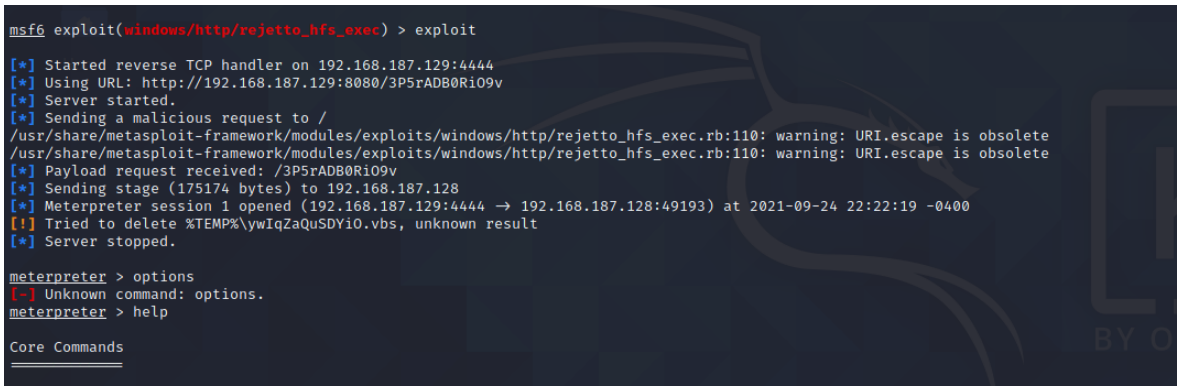
es una distribución de Linux de código abierto basada en Debian destinada a las pruebas de penetración avanzadas y la auditoría de seguridad.

Kali Linux contiene varios cientos de herramientas dirigidas a diversas tareas de seguridad de la información, como pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa. Kali Linux es una solución multiplataforma, accesible y disponible gratuitamente para los profesionales y aficionados a la seguridad de la información.

5.2.7.4 Payloads

En términos simples, son scripts simples que los piratas informáticos utilizan para interactuar con un sistema pirateado. Utilizando cargas útiles, pueden transferir datos a un sistema víctima.

Figura 5 Payload http Rejetto



Fuente: autor

5.3 IDENTIFICACIÓN Y CONTENCIÓN DE UN CIBERATAQUE

5.3.1 Identificación de incidente

Ante incidente de ciberseguridad se deben contar el equipo de Blueteam deber contar con lo siguiente:

Herramientas que permitan la identificación en tiempo real de ciberataque como lo son:

5.3.1.1 SIEM

son plataformas de software que agregan datos de registro de eventos en múltiples sistemas y aplicaciones, servidores y dispositivos de seguridad. Los datos de registro históricos y los eventos en tiempo real también se pueden combinar con información contextual sobre usuarios, activos, amenazas y vulnerabilidades.

5.3.1.2 Firewall de Red

Un firewall es un sistema de seguridad de red que monitorea y controla el tráfico entrante y saliente según los parámetros de seguridad preestablecidos. El firewall monitorea todo el tráfico de la red y tiene la capacidad de identificar y bloquear el tráfico no deseado

5.3.1.3 Software de antivirus

El software de protección antivirus está diseñado para prevenir, detectar y ayudar a eliminar amenazas de los sistemas informáticos. Estas amenazas toman la forma de virus de software y otro malware como Ransomware, gusanos, troyanos y adware.

5.3.1.4 Proxy

Los servidores proxy actúan esencialmente como puentes entre un usuario e Internet. En lugar de tener que conectarse directamente a un sitio web u otro usuario, se conecta a un servidor proxy y el proxy se comunicará con el sitio web en su nombre.

Los proxies proporcionan una valiosa capa de seguridad. Se pueden configurar como filtros web o cortafuegos, protegiendo su computadora de amenazas de Internet como malware

5.3.2 Contención de un incidente

Por otra parte, ante un incidente de ciberseguridad ya materializado el BLUETEAM debe contar con la capacidad para la contención rápida del incidente de esta forma mitigar el impacto del incidente sobre la infraestructura y la información de la organización contando con acciones rápidas como son:

- Aislar el equipo de la red lo a través de la configuración de reglas de firewall que impidan el acceso a internet y otras redes productivas de la maquina afectada

- Iniciar el equipo afectado en modo seguro para asegurar que solo los procesos necesarios se ejecuten y evitar que el proceso malicioso se ejecute

- Instalación de un antimalware para la ejecución de un escaneo profundo para detectar y colocar en cuarentena el software malicioso

5.4 ESTRATEGIAS PARA EVITAR UN INCIDENTE CIBERINCIDENTE

El equipo BLUTEAM dentro de sus funciones está la de generar acciones para evitar la materialización de un ciberincidente las cuales son:

- Establecer contraseñas robusta mínimo de 10 caracteres con el uso de mayúsculas, minúsculas y caracteres especiales, el uso de contraseñas robustas permite evitar que un atacante realice ataques de fuerza bruta para obtener contraseñas validas.

- Activar y configurar el firewall de host y red, por medio de la configuración de las reglas de acceso a nivel de red tanto en el firewall del host, como en el firewall de la red, para que solo se permita el acceso desde, y hacia las redes o IPs necesarias adicionalmente solo permitiendo los puertos de red necesarios para el funcionamiento adecuado de los sistemas, evitando tener permisos excesivos o innecesarios.

- Desactivar el acceso remoto, se debe deshabilitar el acceso remoto bien sea por aplicaciones de terceros o por clientes propios de cada sistema, se pueden crear excepciones, pero exclusivamente para administradores y solamente desde equipo de la red local nunca desde internet.

- Instalar herramientas de protección antivirus que se mantenga actualizadas y las cuales estén configuradas para realizar escaneos de malware de forma diaria y con escaneos profundos de forma semanal

- Habilitar las actualizaciones de seguridad de forma periódica para el sistema operativo, se debe establecer un plan de actiualizaciones de seguridad para se aplican los parches de seguridad una vez al mes, bien sea por medio de un sistema centralizado como un WSUS o directamente desde internet.

- Configurar copias de seguridad de los archivos, se deben establecer procedimientos para que se realizan copias de respaldo a la información crítica de forma diaria a nivel incremental y semanalmente de forma completa

- Usar el cifrado de los datos en reposo y en tránsito, implementar tecnologías que cifren los datos en reposo por medio de la encripcion de los discos duros, adicionalmente implementar el cifrado de los datos en tránsito usando protocolos y tecnologías como los son: HTTPS, TLS1.3, VPN SSL.

- Configurar las cuentas de usuario con el minino de privilegios.

6 CONCLUSIONES

- En las labores de ciberseguridad en especial las relacionadas con hacking ético se deben tener en cuenta los aspectos éticos y legales que involucran estas actividades ya que pueden llevar a la comisión de delitos en el desempeño de la labor profesional.

- En las labores de ciberseguridad realizas por los equipos de Red Team se utilizan diferentes herramientas, las cuales también son usadas por los ciberdelincuentes esto con el fin de comprender mejor los ataques y poder preparar a las organizaciones para afrontar de la mejor forma cualquier incidente de ciberseguridad.

- La implementación de buenas prácticas de seguridad en la configuración de los diferentes sistemas es una estrategia efectiva para evitar ciberincidente

- En las labores de ciberseguridad en especial las relacionadas contenciones de ataques informáticos se deben tener en cuenta las estrategias y herramientas para la contención efectiva ante un incidente informático.

7 RECOMENDACIONES

- Las organizaciones deben implementar ejercicios de RED TEAM esto con el fin de probar su postura de seguridad ente ataque informáticos

- En las organizaciones se deben contar con una estrategia que incluya personal capacitado y herramientas tecnologías para evitar la ocurrencia de un ciberincidente

- Ante un incidente informático se debe contar con una estrategia de acciones rápida por parte del equipo de BLUETEAM para la contención efectiva de un incidente informático.

- Se debe contar con actividades de hardenización basadas en buenas prácticas sobre los activos tecnológicos de una organización.

BIBLIOGRAFÍA

Allen, Mateus. Hacking ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la rama judicial, seccional armenia. Stadium UNAD {En línea}. {2017}. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf.

Álvarez, Vilma. Propuesta de una metodología de pruebas de penetración orientada a riesgos. {En línea}. {2018}. Disponible en: https://pdfs.semanticscholar.org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf.

BANACH, Z. Red Team Vs Blue Team Testing for Cybersecurity {En línea}. {2019}. Disponible en: https://www.netsparker.com/blog/web-security/red-team-vs-blue-team

Copnia. Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. {En línea}. {2018}. Disponible en: https://copnia.gov.co/sites/default/files/uploads/codigo_etica.pdf.

CIS Security. CIS Center for Internet Security CIS Benchmarks. {En línea}. {2020}. Disponible en: https://www.cisecurity.org/cisbenchmarks/

CAMPOS Pablo. Metasploit básico. {En línea}. {2020}. Disponible en: https://secmotic.com/metasploitbasico/#gref.

CIS Security. CIS Center for Internet Security CIS Benchmarks. {En línea}. {2020}. Disponible en: https://www.cisecurity.org/cisbenchmarks/

CCN Cert. Guía de seguridad de las TIC (CCN-STIC-495) Seguridad en IPv6. CCN Cert. {En línea}. {2018}. Disponible en: 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

EC-Council. "What is Ethical Hacking | Types of Ethical Hacking | EC-Council", EC-Council, {En línea}. {2020}. Disponible en: https://www.eccouncil.org/ethical-hacking/

Gaviria, Raúl. Guía práctica para pruebas de pentest basada en la metodología OSSTMM v2.1 y la guía OWASP v3.0. Repositorio Unilibre Pereira. {En línea}. {2015}. Disponible en:

http://repositorio.unilibrepereira.edu.co:8080/pereira/bitstream/handle/123456789/622/GU%C3%8DA%20PR%C3%81CTICA%20PARA%20PRUEBAS.pdf?sequence=1

Incibe. OWASP Testing Guide v4.0. Guia de seguridad en aplicaciones Web. {En línea}. {2014}. Disponible en: https://www.incibe-cert.es/blog/owasp-4.

Incibe. ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. {En línea}. {2019}. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

LOGRHYTHM. Security Information and Event Management (SIEM). {En línea}. {2020}. Disponible en: https://logrhythm.com/solutions/security/siem/

MACKENZIE, P. How to Best Utilize Security Efforts through Red TeamBlue Team Exercises {En línea}. {2019}. Disponible en: https://medium.com/@mackenziepech/one-team-two-team-red-team-blue-teamand-also-purple-team-8b9eb5e87fc1

Mintic. Guía de Auditoria. {En línea}. {2018}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles5482_G15_Auditoria.pdf.

Mintic. Guía de Transición de IPv4 a IPv6 para Colombia. {En línea}. {2018}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf.

MINTIC. Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. {En línea}. {2018}. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.

Mintic. Guía de aseguramiento del Protocolo IPv6. Mintic. {En línea}. {2018}.

Moreno, Patricio. Técnicas de detección de ataques en un sistema SIEM {En línea}. {2015}. Disponible en: http://repositorio.usfq.edu.ec/bitstream/23000/4911/1/120801.pdf

Morales Jose Alfari. Pruebas de vulnerabilidad. {En línea}. {2020}. Disponible en: http://hdl.handle.net/10596/10219

PandaSecurity. Pentesting: Una herramienta muy valiosa para tu empresa. Panda Security Mediacenter. {En línea}. {2018}. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/pentesting-herramienta-empresa/

Quintero, J. F. Red Team y Blue Team al interior de una organización. {En línea}. {2020}. Disponible en: https://repository.unad.edu.co/handle/10596/35497

Revista Seguridad. Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. {En línea}. {2018}. Disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-framework

SHEWARD. The Art of Writing Penetration Test Reports {En línea}. {2012}. Disponible en: https://resources.infosecinstitute.com/writingpenetration-testing-reports/

WeLiveSecurity. (2020). Ciberataques: una de las principales amenazas para el 2020 {En línea}. {2020}. disponible en: https://www.welivesecurity.com/la-es/2020/02/13/ciberataques-principales-amenazas-2020/

EC-COINCIL (2020) What is Penetration Testing (Pent Testing)? - Benefits, Tools, Pen Tester Responsibilities Disponible https://www.eccouncil.org/what-is-penetration-testing/