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

JONH ALEJANDRO GARZON PINZON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ D.C.
2020

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

JONH ALEJANDRO GARZON PINZON

seminario especializado equipos estratégicos en ciberseguridad: red team & blue team

Tutor (a):
John Freddy Quintero Tamayo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTÁ D.C.
2020

TABLA DE CONTENIDO

RESUMEN

Los activos informáticos son cada vez más valiosos teniendo en cuenta que muchos de los procesos misionales y de apoyo dentro de una organización son soportados por sistemas de información, bases de datos y sus comunicaciones son cada vez más dependientes de las redes informáticas ya que por ellas se transmite la mayoría de información entre sus dependencias y los actores externos como clientes proveedores.

Debido a la importancia de mantener protegidos estos activos para mantener su integridad y correcto funcionamiento podemos encontrar estrategias de protección como las brindadas por equipos de seguridad blue team y red team que desde diferentes enfoques proporcionan medidas y técnicas para implementar, probar y mejorar los controles de seguridad en la organización.

Mientras el equipo red team busca probar la efectividad de las defensas de una organización mediante técnicas como pruebas de penetración, los equipos blue team se dedican a establecer medidas de contención y mejoras en las defensas de los sistemas informáticos basado en los resultados que le proporcione el equipo red team y en el constante monitoreo de los eventos de seguridad de la red y sus dispositivos conectados.

En el presente documento se describen recursos usados por equipos blue team para la contención de ataques informáticos, y los del equipo red team desde el punto de vista de la metodología de pruebas de penetración PTES.

GLOSARIO

TTP: Son las siglas de una agrupación de tácticas, técnicas y procedimientos de un atacante informático utilizado comúnmente en la inteligencia de amenazas. Estos elementos representan aspectos diferentes que son las tácticas que son métodos de alto nivel para lograr un objetivo inicial (acceso a un sistema o exfiltracion), técnicas que se refieren a como se va a lograr el objetivo (phising, spear phishing entre otros) y los procedimientos que son pasos dados para lograr el objetivo.

Inteligencia de amenazas: Según Gartner, “La inteligencia de amenazas es conocimiento basado en evidencia, que incluye contexto, mecanismos, indicadores, implicaciones y consejos prácticos, sobre una amenaza o peligro existente o emergente para los activos que se puede utilizar para informar decisiones sobre la respuesta del sujeto a esa amenaza o peligro”[1].

PTES (Penetration Testing Execution Standard): Es una metodología compuesta de 7 fases que cubre todo lo relacionado con una prueba de penetración, desde el reconocimiento de la organización y recopilación de información, análisis de vulnerabilidades y su explotación y postexplotacion hasta la generación del informe de la prueba realizada

SIEM: Security Information and Event Management, es un sistema que permite la centralización y correlación de eventos de seguridad en una organización

[1] GARTNER. [sitio web]. Definition: Threat Intelligence. [consulta: 10 de octubre de 2020]. Disponible en: https://www.gartner.com/en/documents/2487216

1 INTRODUCCION

La ciberseguridad en las organizaciones es un aspecto cada vez más importante teniendo en cuenta que el uso de las tecnologías de la información para los procesos de negocio de una empresa es cada vez más amplio, dado que se simplifican y automatizan dichos procesos mediante la implementación de sistemas informáticos y redes de comunicación.

De acuerdo a lo anterior es necesario contar con estrategias que contribuyan al mejoramiento de ciberseguridad en la organización, las cuales pueden ser llevadas a cabo por equipos red team y blue team que proporcionan servicios de seguridad desde diferentes perspectivas por un lado blue team desarrollando estrategias de contención y defensa, mientras que red team desde el enfoque de prueba de los controles de seguridad de la organización, mediante el uso de técnicas de ataque y penetración de sistemas.

En este documento se identificarán los recursos que puedan ser útiles para el desarrollo de las estrategias en los blue team y red team, haciendo referencia a metodologías y herramientas que pueden ser usadas para la contención y defensa en redes y sistemas informáticos, así como para la ejecución pruebas de penetración o simulación de adversarios.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

- Identificar los recursos que permitan el mejoramiento y desarrollo de estrategias red team y blue team

2.2 OBJETIVOS ESPECIFICOS

- Mostrar herramientas y métodos que contribuyan al endurecimiento de las defensas en ciberseguridad de una organización
- Describir los métodos, procesos y metodologías que contribuyan al desarrollo de las actividades de un equipo red team

3 DESARROLLO DEL INFORME

Las estrategias de los equipos blue team y red team que se conformen en una organización deben tener las capacidades para contribuir a que una infraestructura de red sea defendible, lo que quiere decir que sus controles sean eficaces contra las intrusiones de seguridad que se puedan presentar.

Según Bejtlich[2], una red defendible debe tener ciertas especificaciones que contribuyen a la protección de la red entre las cuales se encuentran:

- monitoreada: Los datos o registros de logs de la red o de los equipos host deben ser capturados o centralizados.
- inventariada: Se debe tener conocimiento de todos los elementos que conforman la red.
- Controlada: Se refiere al control de tráfico de la red, admisión y control de acceso a la red, proxy entre otros controles que puedan ser aplicados a los elementos inventariados.
- Identificación de propietario: Es necesario conocer los propietarios de los activos informáticos en la organización, para establecer acciones de contención y recuperación.
- Minimización de impacto: una red defendible debe reducir la superficie de ataque en activos informáticos como servidores, aplicaciones entre otros.
- Evaluación: Consiste en identificar las vulnerabilidades y evaluar las defensas implementadas
- Actualización: Instalación de parches en vulnerabilidades conocidas.

Todas estas características de una red defendible pueden ser acogidas por las actividades de un equipo blue team al realizar acciones de defensa mediante el monitoreo de la red y planteamiento de controles de seguridad, a la vez que el equipo red team efectúa la evaluación de los controles implementados mediante pruebas de penetración o ejercicios de emulación de adversarios.

[2] BEJTLICH, Richard. Defensible Network Architecture 2.0. Disponible en: https://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html

3.1 RECURSOS PARA EL EQUIPO BLUE TEAM

Los controles de seguridad que se aplicaron al escenario de seguridad de máquinas Windows 7 vulnerables, consistieron en herramientas de seguridad propias del sistema operativo, como la configuración del firewall y el antivirus integrado, y en la ejecución de actualizaciones de seguridad realizando la instalación de los parches necesarios para subsanar las vulnerabilidades existentes, lo cual es una acción casi que obligatoria para todo tipo de sistemas informáticos.

Cabe señalar que las anteriores medidas de contención se tomaron a partir del lineamiento indicado de proponer medidas sin ningún costo en la solución, sin embargo, a pesar de que existe una gran oferta de herramientas de código abierto se requeriría de por lo menos la habilitación de una maquina dedicada a labores de seguridad e instalar las soluciones adecuadas.

También sería posible instalar dichas herramientas en los sistemas operativos, sin embargo, es recomendable, si se va a proteger toda la organización, que se cuente con un sitio centralizado que permita realizar la detección y análisis de todos los eventos de seguridad en la organización.

Para mejorar los aspectos de seguridad en la organización el equipo blue team puede hacer uso de los recursos que se exponen a continuación:

3.1.1 DISPOSITIVOS DE SEGURIDAD PARA CONTENCION DE ATAQUES INFORMÁTICOS

Firewall como defensa de perímetro de red

Defender el perímetro de red en la organización es uno de los aspectos más importantes a proteger por un blue team, ya que de las redes externas provienen muchos de los intrusos que puedan afectan los activos críticos de la organización.

Los firewall son herramientas activas de red que brindan protección perimetral a una red sin embargo, se pueden encontrar firewall personales que brindan protección solo al host, como el software integrado para sistemas operativos Windows.

Sus funciones consisten en permitir o denegar el tráfico de red mediante una serie de reglas definidas por un administrador de red.

Los tipos de firewall que se pueden encontrar son:

- El firewall de inspección de estados, que bloquea el trafico según los puertos, servicios y estados de red especificados, para ello hace uso de las reglas previamente definidas.

- Firewall de gestión unificada, que combina varios servicios de seguridad como las funciones de un firewall de inspección, antivirus, y sistemas de detección y prevención de intrusos.

- Firewall de última generación, lo cuales tienen funciones adicionales a un firewall tradicional que solo realiza filtrado e inspección de paquetes. Algunas de las funciones que debe incluir un Firewall de última generación son, funciones de firewall de inspección, prevención de intrusiones, detección de aplicaciones que puedan generar riesgos, técnicas contra amenazas de seguridad cambiantes entre otros.

Firewall para la protección de aplicaciones web - WAF

Los WAF (Web Application Firewall) son dispositivos especializados en la protección de aplicaciones web, que funcionan aplicando reglas de filtrado bloqueando trafico malicioso especifico que pueda afectar una aplicación como la inyección SQL, inyección de comandos o ataques de Cross Site Scripting(XSS).

Los WAF se diferencian de las funciones de un firewall tradicional al brindar protección específicamente a las aplicaciones web, mientras que el firewall bloquea o permite tráfico en una red de forma general.

Según el sitio web randed[3], los WAF pueden tener dos modos de funcionamiento, siguiendo un modelo de seguridad positivo el cual hace uso de listas blancas que solo permiten el tráfico que se estima que es seguro para la aplicación web; mientras que el modelo de seguridad negativo acepta todas las peticiones excepto las maliciosas.

Estas soluciones de defensa tienen un enfoque preventivo y no realiza acciones proactivas por lo cual se pueden ver limitaciones en su funcionamiento al ser demasiado restrictivo, o poder estar en riesgo en caso de que una amenaza reciente no se encuentre incluida en las excepciones de tráfico.

Plataformas de respuesta a incidentes

Las herramientas de respuesta a incidentes tienen como objetivo identificar, contener y eliminar las causas de un incidente informático y contribuir a que se eviten posibles huecos de seguridad en los sistemas y redes de una organización.

[3] RANDED. Firewall de Aplicaciones Web (WAF). Disponible en: https://randed.com/waf

Algunas de las características que debería tener una plataforma de respuesta a incidentes según el sitio web O'reilly[4] son:

- Recibir alertas y eventos e seguridad de diversas fuentes como herramientas SIEM
- Permitir la gestión de casos de incidentes informáticos donde el analista de seguridad pueda agregar información relevante al caso.

3.1.2 MONITOREO DE SEGURIDAD Y PREVENCIÓN

El monitoreo y prevención de la red es un aspecto sumamente importante para defender los sistemas y activos críticos de una organización de los ataques informáticos.

El monitoreo puede realizarse en la red donde se analiza el tráfico que circula a través de ella, así como el análisis de archivos de log de servicios como HTTP, DNS, SMB, FTP y en los equipos host que se encuentran en la red.

Las fuentes de información en el monitoreo de seguridad de una red pueden provenir de los logs de un firewall perimetral el cual contiene información de acciones bloqueadas o permitidas, o información de aplicaciones en el caso del firewall de nueva generación.

También se pueden encontrar registros de información de sistemas IDS/IPS que brindan información de posible tráfico malicioso, servidores proxy que informan acerca de las actividades del usuario y los logs de servicios web, FTP y demás servicios de red.

En el caso del monitoreo de seguridad en los equipos conectados en la red, la información proviene de herramientas como servicios de autenticación que muestren intentos válidos y fallidos de logueo, registros de antivirus que muestran las acciones maliciosas identificadas y logs de aplicaciones donde se pueden observar errores y advertencias.

Las herramientas como los IDS y los IPS, son herramientas esenciales para realizar estas actividades de prevención, contención y para brindar insumos de monitoreo de ataques informáticos.

Los IDS e IPS son herramientas de monitoreo de amenazas que son implementadas en diversos puntos de la red. Mientras que el IDS actúa como dispositivo pasivo y

[4] O' REILLY. Security incident response platforms (SIRP). Disponible en: https://www.oreilly.com/library/view/hands-on-security-in/9781788995504/326e7e8a-a4dc-4267-8bf7-12b8b7477d4f.xhtml

se ubica e estratégicamente normalmente en un puerto span de una VLAN para la escucha de tráfico[5], el IPS funciona de forma activa previniendo el trafico malicioso, implementado fuera de la red.

3.1.3 REGISTRO DE EVENTOS DE SEGURIDAD

De acuerdo a lo mostrado en la sección anterior, se puede evidenciar que el monitoreo de las redes, equipos y sistemas informáticos genera una gran cantidad de información de eventos de seguridad que individualmente son difíciles de utilizar para poder realizar un análisis de ellos y poder identificar, reportar y mitigar acciones maliciosas.

Es por ello que es de gran importancia hacer uso de herramientas que permitan el registro de eventos de seguridad de una forma centralizada y donde se pueda agregar y correlacionar toda la información recopilada por los sistemas de monitoreo y prevención.

Para centralizar y procesar la información de estas fuentes se encuentran las herramientas SIEM, que son sistemas que recopilan estos eventos de seguridad donde se realiza una correlación de los eventos, se categorizan y analizan para generar informes sobre incidentes de seguridad como autenticaciones fallidas, actividades de malware y otras acciones maliciosas, así como la generación de alertas ante la vulneración de una regla que pueda indicar un posible problema de seguridad.

Algunas de las capacidades que se pueden encontrar en un SIEM según el sitio web infotecs[6] son las siguientes:

- Agregación de datos: Esta capacidad busca la recopilación de eventos de seguridad de las redes, sistemas y aplicaciones monitoreadas en una organización.

- Correlación: Este aspecto de los SIEM es fundamental ya que lo que se busca es relacionar los eventos con atributos comunes y generar información útil para la gestión de incidentes en la red.

- Alertas: El SIEM debe tener la capacidad de generar alertas si se detecta algún problema de acuerdo a la información correlacionada de los eventos capturados.

---

[5] BOND, Robert. Network Security Design is Critical to Eliminating Security Gaps and Reducing Costs. Disponible en: https://secureops.com/networking/effective-network-security-design/

[6] INFOTECS. SIEM o Gestión de Eventos e Información de Seguridad. Disponible en: https://infotecs.mx/blog/SIEM-o-gestion-de-eventos-e-informacion-de-seguridad.html

- Cumplimiento: Los SIEM pueden generar informes que contribuyan a procesos de auditoria y los procesos de seguridad existentes.

3.1.4 USO DE BUENAS PRACTICAS EN CIBERSEGURIDAD

Para un blue team, el conocimiento de buenas prácticas en ciberseguridad es útil para poder aplicarlos a los diferentes recursos de contención, monitoreo y prevención que se pueden implementar para brindar defensas a una organización.

El Center for Internet Security (CIS) pone a disposición de las personas que lo requieran un conjunto de mejores prácticas para mejorar los aspectos de seguridad en los sistemas o redes de una organización. Este compilado de buenas practicas consta de 20 controles que definen una serie de herramientas y procedimientos que son explicados y detallados para su correcta implementación.

La organización CIS cuenta también con diferentes documentos que proveen de configuraciones sugeridas para una variedad de sistemas y software denominado CIS benchmarks. Estos documentos pueden ser utilizados como base para una configuración avanzada de la seguridad en sistemas operativos, bases de datos, servidores web entre otras plataformas informáticas. Su uso toma relevancia teniendo en cuenta que en la mayoría de los casos los sistemas informáticos son instalados con una configuración por defecto, lo cual puede dar lugar a huecos de seguridad en los sistemas.

3.2 RECURSOS PARA EL EQUIPO RED TEAM EN WHITE HOUSE SECURITY

El objetivo del equipo red team consiste en la evaluación de las defensas de la organización haciendo pruebas a los controles y buenas prácticas de seguridad que ha implementado el equipo blue team.

3.2.1 USO DE PRUEBAS DE PENETRACIÓN

Para la evaluación de las medidas de protección tomadas por una organización se puede hacer uso de metodologías para pruebas de penetración que brindan diversas etapas donde se debe recopilar ordenar y analizar información, para posteriormente ejecutar la evaluación de seguridad informática de la organización.

Existen varias metodologías de pruebas de penetración que se pueden aplicar de acuerdo a las necesidades de una organización. Teniendo en cuenta que se debe realizar una evaluación a todos los activos de red e informáticos que tenga la empresa se sugiere aplicar la metodología PTES, que brinda lineamientos para

realizar pruebas de red, aplicaciones web, redes inalámbricas, seguridad física e ingeniería social.

Las fases que componen esta metodología son:

Fase de Preacuerdo

Esta fase de la metodología busca establecer los objetivos y el alcance que se le dará a las pruebas de penetración

La determinación del alcance es un componente muy importante para realizar una prueba de penetración ya que al definir las actividades a realizar se evitarán inconvenientes como aumentos del alcance o clientes no satisfechos, por lo cual se debe llegar a un acuerdo con el cliente en las áreas a evaluar.

PTES[7] proporciona una serie de preguntas que tienen como objetivo comprender lo que quiere el cliente con la prueba de penetración y establecer correctamente el alcance, algunas de ellas son:

- ¿Por qué se realiza al cliente la prueba de penetración en su entorno?
- ¿Cuántas direcciones IP totales se están probando?
- ¿Cuántas aplicaciones web se están evaluando?
- ¿Cuántas ubicaciones físicas se están evaluando?

Para el reconocimiento de los objetivos se deben validar varios aspectos como por ejemplo si los objetivos son rangos de ip, dominios, o el cliente solo da como información el nombre de la organización, donde se debe validar si en realidad es propiedad del cliente, ya que acarrearía consecuencias legales explotar una vulnerabilidad y acceder sin autorización a otra organización que no es el objetivo.

Fase de reconocimiento

Esta fase consiste en recopilar toda la información posible del objetivo de la prueba de penetración, para usarla en las fases de evaluación y explotación de vulnerabilidades. Los aspectos a tener en cuenta en la fase de reconocimiento consisten en la identificación y denominación del objetivo verificando sus dominios, además de tener en cuenta las reglas de limitación en la prueba ya que si se realizan pruebas en objetivos fuera del alcance se puede tener consecuencias legales, ya que se llevaría a cabo un acceso intrusivo sin autorización del cliente.

En el reconocimiento de una prueba de penetración se debe contar con información corporativa de la organización como información de ubicaciones de sus sedes

[7] PENTEST-STANDARD. Pre-engagement Interactions. Disponible en: http://www.pentest-standard.org/index.php/Pre-engagement

físicas, las medidas de seguridad adoptadas, información sobre los registros en internet como datos de whois, registros DNS de correo electrónico o de los dominios asociados.

También se menciona la recopilación de información de las relaciones de la organización como por ejemplo con proveedores, socios y clientes y mucha otra información que puede ser útil para planear una evolución de forma adecuada.

Fase de modelado de amenazas

El modelado de amenazas en la metodología PTES consiste en mapear los activos y procesos de la organización contra las posibles amenazas que puedan afectarlas.

Esta fase es útil para dar más claridad en la priorización de los activos de la organización y mitigar los riesgos que se puedan generar de las amenazas.

El proceso de modelado de amenazas propuesto por la metodología, consiste en los siguientes pasos:

- Recopilar información relevante
- Identificar y clasificar los activos prioritarios
- Identificar y clasificar las amenazas
- Mapear las amenazas identificadas con los activos priorizados.

En el análisis de los activos y procesos de la empresa se revisan distintas categorías de información como datos organizacionales, que tienen que ver con información de políticas y planes de la empresa, información técnica, de productos, financiera, de cliente y otra información relevante a la organización

De igual forma también se realiza el análisis a los procesos de organización como los procesos de soporte técnico de la infraestructura tecnológica, procesos de administración de activos humanos entre otros.

Fase de análisis de vulnerabilidades

El análisis de vulnerabilidades consiste en descubrir posibles fallas en los sistemas de una organización, que un atacante pueda aprovechar. Puede haber diversas fuentes de una vulnerabilidad entre las cuales se puede mencionar una configuración incorrecta en un sistema o dispositivo de red, el diseño de una aplicación que pueda hacerla insegura entre otros.

PTES define tres tipos de análisis a realizar que son los de interacción activa, pasiva y validación de vulnerabilidades.

Análisis activo

Consiste en una interacción directa con el componente que se va evaluar, que puede ser un dispositivo de red, una aplicación web u otro elemento informático.

Entre las pruebas de tipo activo que se pueden realizar en un análisis de vulnerabilidades se encuentran:

Escaneo de vulnerabilidades en una red

Este es uno de los primeros pasos que se llevan a cabo en una prueba de penetración, ya que se puede obtener información de los servicios y host disponibles en la red, determinando si un puerto en el sistema evaluado puede recibir una conexión. Aquí también se obtiene información del protocolo de red involucrado y se puede establecer si una vulnerabilidad puede afectar el servicio en ese puerto de red.

Escaneo basado en servicios

Este escaneo va más allá de verificar si un puerto está ofreciendo un servicio y si está abierto a peticiones, ya que en este escaneo se busca más información acerca del servicio en un puerto abierto, por ejemplo, la identificación de un servicio web en un puerto que no es por defecto, por ejemplo 8382.

Una herramienta para el análisis de vulnerabilidades es OpenVAS Open Vulnerability Assessment System, el cual es un framework que ofrece una solución de escaneo de vulnerabilidades, mediante una serie de herramientas y servicios para un análisis y gestión de las vulnerabilidades. OPENVAS es basado en el software nessus, y es una herramienta de código abierto.

Escaneo de aplicaciones web

Los escáneres de aplicaciones web realizan un análisis de aplicaciones y servicios web en busca de fallas o vulnerabilidades y además realiza pruebas a la aplicación si se encuentra una potencial falla que la afecte, como una inyección de código o ataques XSS.

Se pueden encontrar en el mercado varias soluciones que funcionan como escáneres de aplicaciones web, como netsparker, webinspect de Hewlett Packard o Appscan de IBM todas ellas de código propietario por lo cual tienen un costo de adquisición.

También se pueden encontrar procesos de enumeración de directorios y fuerza bruta, donde se pueden rastrear directorios de una aplicación web usando una lista

de nombres comunes, donde se podría obtener acceso a carpetas con potencial información confidencial de la organización.

Dirbuster, por ejemplo, es una herramienta de código abierto que ejecuta un proceso de fuerza bruta en los nombres de archivos y directorios de una aplicación web. Su funcionamiento es similar al de herramientas de fuerza bruta de contraseñas al utilizar listas de nombres de directorios comunes que se pueden encontrar en una aplicación web

Análisis pasivo

Se pueden encontrar dos tipos de análisis y monitoreo:

Análisis de metadatos: Los metadatos, son datos que describen un archivo por ejemplo documentos de ofimática, videos o archivos de música. Los metadatos pueden contener información acerca del autor del documento, fechas de creación y modificación, la empresa y se podrían encontrar archivos con datos personalizados donde se puede encontrar información de ip, nombres y rutas de servidores.

Monitoreo de trafico: consiste en escuchar datos en una red y capturar datos que posteriormente se pueden analizar.

Un analizador de trafico de código abierto muy conocido es wireshark el cual se utiliza para la resolución de problemas de red, análisis de protocolos de red entre otras funcionalidades. Es un software multiplataforma por lo que puede ser usado en sistemas unix, Windows, mac y Solaris.

Validación de vulnerabilidades

Consiste en consultar información acerca de los hallazgos de vulnerabilidades, después de realizados los análisis de vulnerabilidad respectivos.

Las vulnerabilidades encontradas pueden relacionarse con una falla que ya ha sido documentada y que puede encontrarse en listas CVE y problemas conocidos de software.

También se pueden relacionar las fallas encontradas con categorías de cumplimiento de un estándar de seguridad especifico, por ejemplo, usuarios de equipos o servidores con contraseñas por defecto, que va en contra de lineamientos de complejidad de contraseña en el estándar NIST 800-53.

En la validación de vulnerabilidades se pueden encontrar una gran cantidad de recursos públicos en internet, donde se puede investigar acerca de las vulnerabilidades encontradas en el análisis, Algunas de ellas son:

- CVE (Common Vulnerabilities and Exposures) es un servicio que ofrece un listado de vulnerabilidades de ciberseguridad conocidas, las cuales tienen un identificador único (CVE000), y con el cual se puede consultar la descripción y los detalles de la vulnerabilidad reportada. CVE es mantenido por la organización MITRE, financiada por el gobierno de Estados Unidos. La información de vulnerabilidades en listados CVE se puede encontrar en sitios en internet como:

  - Sitio web de MITRE: https://cve.mitre.org/cve/search_cve_list.html
  - Sitio web de NIST: https://nvd.nist.gov/vuln/search
  - Sitio web CVE Details: https://www.cvedetails.com/

- Exploit DB (http://www.exploit-db.com) es una base de datos de exploits basados en vulnerabilidades que se encuentran listadas en bases de datos CVE. Este servicio brinda información acerca de la versión del software afectado, la fecha de publicación del exploit y referencias hacia reportes detallados de la vulnerabilidad en bases de datos CVE.

- En la validación de debilidades de estándares como por ejemplo de contraseñas se pueden encontrar sitios como:

  - http://cirt.net/passwords
  - http://www.passwordsdatabase.com

Fase de Explotación

La fase de explotación consiste en conseguir el acceso a un sistema, con base en el análisis de vulnerabilidades realizado. En la metodología PTES[8] se expone que, si el análisis de vulnerabilidades fue realizado correctamente, puede haber una alta probabilidad de éxito de identificar los puntos de entrada del sistema evaluado e identificar los activos de alto valor.

En la explotación de vulnerabilidades se deben considerar contramedidas para eludir los controles de prevención y seguridad que se encuentran en la red como antivirus, sistemas de encriptación y sistemas de prevención de intrusos como IDS o IPS.

Las técnicas de explotación a utilizar dependen del alcance de las pruebas de penetración, toda vez que una vulnerabilidad puede ser explotada debido a fallas de seguridad en un servicio, falta de políticas de contraseñas donde es posible

[8]PENTEST-STANDARD. Exploitation. Disponible en: http://www.pentest-standard.org/index.php/Exploitation

aplicar ataques de fuerza bruta o realizar “sniffing” en las redes de la organización con el fin de capturar posible información en texto plano y no se encuentre encriptada.

La metodología menciona diversos recursos técnicos de explotación, que pueden ser aplicados en distintos escenarios de explotación, donde se pueden mencionar algunos como:

- Explotación de vulnerabilidades en servicios y sistemas: La explotación de vulnerabilidades se puede dar en servicios, aplicaciones, sistemas operativos, bases de datos y otros activos informáticos que puedan tener alguna falla de seguridad ya sea por diseño, falta de actualizaciones de seguridad o malas configuraciones.

  Se pueden encontrar varias herramientas de explotación para su uso, uno de ellos es metasploit que es el framework más conocido de explotación de vulnerabilidades, el cual cuenta con una amplia colección de exploits en diversas plataformas.

- Ataques de fuerza bruta: Consisten en romper la seguridad de las contraseñas de los usuarios de los equipos host en una red. Algunas herramientas que ayudan en este proceso son Brutus, medusa o web brute.

Fase de postexplotacion

Según PTES[9], la fase de postexplotacion consiste en determinar el valor de la máquina comprometida y mantener el control de la máquina para su uso posterior, lo cual se determina por la criticidad del contenido de la maquina vulnerada como datos confidencialidad o servicios críticos prestados.

PTES describe una serie de métodos con los cuales se pueden identificar datos confidenciales, canales de comunicación y ajustes de configuración en el sistema comprometido, para ser documentados y que dicha información pueda ser usada para acceder al sistema posteriormente.

Las actividades que propone la metodología en la postexplotacion son bastantes, por lo cual a continuación se nombran algunas de ellas:

- Reglas de compromiso: Son reglas que se establecen para garantizar que los sistemas del cliente no corran riesgos de modificaciones, después de la explotación e intrusión por parte del pentester. Además, también se consideran reglas de protección para el experto que realiza la explotación,

[9] PENTEST-STANDARD. Post Exploitation. Disponible en: http://www.pentest-standard.org/index.php/Post_Exploitation

ya que los accesos intrusivos a los sistemas pueden ser considerados ilegales si no están descritos en un contrato o en el alcance de las pruebas de penetración.

- Análisis de la infraestructura de red: La máquina que ha sido explotada puede ser útil para identificar redes, equipos de red, servidores críticos y otro tipo de relaciones que pueda tener la maquina con el fin de aumentar la penetración en los sistemas del cliente.

Fase de informe

En esta fase se recopila toda la información relacionada con la ejecución de las anteriores fases, donde PTES recomienda algunos criterios básicos para estructurar un informe que proporcione valor al lector.

Las secciones que componen el informe recomendado por PTES consisten en un resumen ejecutivo y un reporte técnico de los hallazgos de la prueba de penetración.

El resumen ejecutivo consiste en mostrar los objetivos específicos y los resultados de alto nivel de la ejecución de la prueba

El reporte técnico muestra los detalles técnicos de la prueba, donde se describen el alcance, las rutas de ataque, el impacto y las sugerencias de corrección.

3.2.2 EMULACIÓN DE ADVERSARIOS

Strom, Schulz y Nickels[10] en su artículo "*Getting Started with ATT&CK: Adversary Emulation and Red Teaming*", definen la emulación de adversarios como una actividad de red teams que imitan amenazas conocidas para una organización combinando técnicas de inteligencia de amenazas para definir las acciones y comportamientos del red team.

Las actividades de emulación consisten en construir escenarios para probar aspectos de las tácticas, técnicas y procedimientos del adversario (TTP) y probar como las defensas pueden actuar contra el atacante emulado.

Un recurso de gran utilidad para la emulación de adversarios es el uso de ATT & CK (Adversarial Tactics, Techniques, and Common Knowledge) desarrollado por la organización MITRE, que brinda una base de conocimiento de tácticas y técnicas

[10] STROM, Blake; SCHULZ, Tim & NICKELS, Katie. Getting Started with ATT&CK: Adversary Emulation and Red Teaming. Disponible en: https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3

de atacantes del mundo real. En este sitio web además se pueden encontrar grupos de amenazas que han sido identificados por usar una serie tácticas y técnicas dirigidas a un sector de la industria, entre ellas se pueden encontrar las APT (Amenazas persistentes Avanzadas).

Strom, Schulz y Nickels también exponen tres niveles para la ejecución de emulación de adversarios, dependiendo de los recursos que dispone un red team en una organización.

Para efectos de mostrar la utilidad de usar la emulación de adversarios en un equipo red team consolidado y con recursos suficientes para su funcionamiento, se muestra a continuación el nivel tres descrito por Strom, Schulz y Nickels[11], que muestra un proceso de cinco pasos para formar un plan de emulación de adversarios.

- Recopilar información sobre las amenazas: En este paso el equipo red team selecciona al atacante de acuerdo a las amenazas que pueden afectar a la organización. Se realiza un proceso de inteligencia de amenazas que tiene como objetivo saber más acerca del comportamiento del atacante.

- Extraer técnicas de los atacantes: De acuerdo a lo recopilado con la inteligencia de amenazas, se realiza un mapeo de esta información con las técnicas de un grupo específico de atacantes que pueden ser encontrados en la base de conocimiento de ATT & CK.

- Analizar y organizar: Consiste en organizar toda la información recopilada y generar un flujo operativo.

- Desarrollar herramientas y procedimientos: este paso consiste en investigar cómo implementar el comportamiento del atacante. Para ello Strom, Schulz y Nickels mencionan consideraciones como: de que forma utilizo el grupo de atacantes las técnicas identificadas o que herramientas se pueden utilizar para replicar los TTP.

- Emular al atacante: Ya con un plan establecido con la información recogida el red team está en capacidad de ejecutar la emulación de un atacante en la organización.

[11] STROM, Blake; SCHULZ, Tim & NICKELS, Katie. Getting Started with ATT&CK: Adversary Emulation and Red Teaming. Disponible en: https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3

4 CONCLUSIONES

- El uso de una metodología de penetración en un equipo red team es un recurso de gran ayuda para evitar posibles problemas legales, al definir un alcance de las pruebas de acuerdo a las necesidades de la organización, lo cual establece hasta dónde puede llegar el pentester.

- Aplicar una metodología de penetración también ayuda a un equipo red team en la selección de las técnicas de análisis y explotación de vulnerabilidades más apropiadas de acuerdo al alcance que se ha establecido previamente.

- Si bien las pruebas de penetración y la emulación de adversarios buscan el mismo objetivo que es el examen de las defensas implementadas en una organización, la emulación de adversarios hace más énfasis en imitar lo más posible a un grupo de atacantes informáticos y de amenazas persistentes avanzadas de las cuales ya se han identificado las tácticas y técnicas que utilizan en bases de conocimiento como ATT&CK.

- Los recursos de contención de ataques informáticos que se describieron en este documento tienen sus características particulares para contribuir al mejoramiento de la seguridad en una organización, sin embargo, lo recomendable es combinar varias técnicas que cubran diferentes aspectos como la prevención, detección y acciones proactivas contra los ataques informáticos.

- A pesar de que en el mercado se puede encontrar un amplio portafolio de herramientas de código abierto, bases de conocimiento y frameworks para el uso en los equipos blue team y red team, una organización que quiera implementar estas estrategias debe pensar en una inversión razonable para la protección de sus activos informáticos, y no limitarse al uso de herramientas sin costo.

- El trabajo conjunto de los red team y blue team en una organización es esencial para brindar a la organización el conocimiento de posibles brechas de seguridad con base en las medidas de defensa adoptadas y la información que se obtiene al realizar pruebas de los controles implementados.

- La contención de ataques informáticos requiere de fuentes de información que brinden insumos para la identificación de ataques y tomar medidas ante ellos, por ello es de gran importancia el monitoreo de eventos seguridad de todos los elementos conectados a una ya que mediante ellos se puede recopilar información valiosa para las mejoras en ciberseguridad de una organización.

5 RECOMENDACIONES

- Para el ejercicio de funciones de un equipo red team es recomendable tener muy en cuenta la construcción de contratos o documentos legales donde consten las actividades a realizar y que alcance van a tener. Con ello se evitan posibles problemas legales ante un acceso indebido al sistema evaluado.

- Un equipo blue team debe tener entrenamiento específico en diferentes herramientas de monitoreo, de gestión eventos de seguridad y contención de ataques informáticos, teniendo en cuenta que se pueden tener muchas herramientas para defensa para la organización, pero si no son configuradas y administradas correctamente no tendrán al máximo las capacidades que brindan las herramientas implementadas.

- Para la protección total de una organización se recomienda hacer uso de software y hardware de seguridad en conjunto como por ejemplo el uso de un firewall y que este en conjunto con una herramienta SIEM que además interactúe con una plataforma de respuesta a incidentes.

- La configuración de las aplicaciones y sistemas informáticos que se encuentren en una organización deben contar con una configuración avanzada y evitar dejar las configuraciones por defecto, para ello es apropiado el uso de recursos como los CIS Benchmarks que proporcionan guías en configuraciones de seguridad de diversas plataformas informáticas.

6 REFERENCIAS

BEJTLICH, Richard. [Sitio web]. Defensible Network Architecture 2.0. [Consulta: 10 de octubre de 2020]. Disponible en: https://taosecurity.blogspot.com/2008/01/defensible-network-architecture-20.html

CISCO. [sitio web]. ¿Qué es un firewall? [Consulta: 10 de octubre de 2020]. Disponible en: https://www.cisco.com/c/es_es/products/security/firewalls/what-is-a-firewall.html

BOND, Robert. [Sitio web]. Network Security Design is Critical to Eliminating Security Gaps and Reducing Costs. [Consulta: 10 de octubre de 2020]. Disponible en: https://secureops.com/networking/effective-network-security-design/

CYBRHAWK. [sitio web]. Cybrhawk blue team stages. [consulta: 10 de octubre de 2020]. Disponible en: https://cybrhawk.com/security-assessment/blue-team/

SANS. [sitio web]. EC450: Blue Team Fundamentals: Security Operations and Analysis (Demo del curso). [consulta: 10 de octubre de 2020]. Disponible en: https://www.sans.org/cyber-security-courses/blue-team-fundamentals-security-operations-analysis/

PRATT, Mary. [sitio web]. What is SIEM Software? How It Works and How to Choose the Right Tool. [consulta: 10 de octubre de 2020]. Disponible en: https://adlumin.com/what-is-siem-software-how-it-works-and-how-to-choose-the-right-tool/

BLOG ENTERPRISE DETECTION & RESPONSE. [sitio web]. The pyramid of pain. [consulta: 10 de octubre de 2020]. Disponible en: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

GARTNER. [sitio web]. Definition: Threat Intelligence. [consulta: 10 de octubre de 2020]. Disponible en: https://www.gartner.com/en/documents/2487216

STROM, Blake; SCHULZ, Tim & NICKELS, Katie. [Sitio web]. Getting Started with ATT&CK: Adversary Emulation and Red Teaming. [consulta: 10 de octubre de 2020]. Disponible en: https://medium.com/mitre-attack/getting-started-with-attack-red-29f074ccf7e3

BORKAR, Pramod. [sitio web]. The Three Elements of Incident Response: Plan, Team, and Tools. [consulta: 10 de octubre de 2020]. Disponible en: https://www.exabeam.com/incident-response/the-three-elements-of-incident-response-plan-team-and-tools/

O' REILLY. [sitio web]. Security incident response platforms (SIRP). [consulta: 10 de octubre de 2020]. Disponible en: https://www.oreilly.com/library/view/hands-on-security-in/9781788995504/326e7e8a-a4dc-4267-8bf7-12b8b7477d4f.xhtml

RANDED. [sitio web]. Firewall de Aplicaciones Web (WAF). [consulta: 11 de octubre de 2020]. Disponible en: https://randed.com/waf

INFOTECS. [sitio web]. SIEM o Gestión de Eventos e Información de Seguridad. [consulta: 10 de octubre de 2020]. Disponible en: https://infotecs.mx/blog/SIEM-o-gestion-de-eventos-e-informacion-de-seguridad.html

PENTEST-STANDARD. [sitio web]. Post Exploitation. [consulta: 11 de octubre de 2020]. Disponible en: http://www.pentest-standard.org/index.php/Post_Exploitation

PENTEST-STANDARD. [sitio web]. Exploitation. [consulta: 11 de octubre de 2020]. Disponible en: http://www.pentest-standard.org/index.php/Exploitation
PENTEST-STANDARD. [sitio web]. Vulnerability Analysis. [consulta: 11 de octubre de 2020]. Disponible en: http://www.pentest-standard.org/index.php/Vulnerability_Analysis
PENTEST-STANDARD. [sitio web]. Pre-engagement Interactions. [consulta: 11 de octubre de 2020]. Disponible en: http://www.pentest-standard.org/index.php/Pre-engagement
Center for Internet security. [Sitio web]. CIS benchmarks. [Consulta: 11 de octubre de 2020]. Disponible en: https://www.cisecurity.org/cis-benchmarks/