SAD - U4.1. Seguridad en redes

Descargar estos apuntes

Índice

- 1. Seguridad en redes
  - 1.1. Fases de un ataque
  - 1.2. Inteligencia de fuentes abiertas (OSINT)
  - 1.3. Escaneo de dispositivos y servicios
  - 1.4. Escaneo de vulnerabilidades

1. Seguridad en redes

La **seguridad en redes** es una disciplina que se encarga de proteger la información y los sistemas informáticos de posibles amenazas. La seguridad en redes abarca diferentes aspectos, como la seguridad física, la seguridad lógica, la seguridad de la información y la seguridad de los sistemas. La seguridad en redes es fundamental para garantizar la confidencialidad, la integridad y la disponibilidad de la información y los sistemas informáticos.

1.1. Fases de un ataque

Un ataque informático es un intento de acceder, dañar o robar información de un sistema informático sin autorización. Los ataques informáticos pueden ser realizados por personas malintencionadas, como hackers, crackers o ciberdelincuentes, con el objetivo de obtener beneficios económicos, políticos o personales. Los ataques informáticos pueden ser realizados a través de diferentes métodos, como la ingeniería social, el phishing, el malware, el ransomware o la explotación de vulnerabilidades.

Los ataques informáticos suelen seguir una serie de fases, que pueden variar en función del tipo de ataque y del objetivo del atacante. Algunas de las fases más comunes de un ataque informático son:

- **Reconocimiento** y **escaneo**: el atacante recopila información sobre el sistema objetivo, como direcciones IP, nombres de dominio, usuarios, contraseñas, puertos abiertos, servicios activos, etc.
  Una vez conocidos algunos objetivos, el atacante identifica los puntos débiles del sistema objetivo, como vulnerabilidades, puertos abiertos, servicios activos, etc.
- **Prepación**: el atacante prepara los recursos necesarios para llevar a cabo el ataque, como herramientas, scripts, malware, etc.
- **Distribución**: el atacante distribuye el malware o el ataque a través de diferentes medios, como correos electrónicos, mensajes, enlaces, etc.
- **Explotación**: el atacante explota las vulnerabilidades del sistema objetivo para obtener acceso no autorizado, robar información o dañar los sistemas.
- **Instalación**: el atacante instala el malware o el ataque en el sistema objetivo para mantener el acceso y control del sistema.
- **Comando y control**: el atacante envía comandos al sistema objetivo para controlarlo, robar información, dañar los sistemas, etc.

- **Acciones sobre el objetivo**: el atacante realiza acciones sobre el sistema objetivo, como robar información, dañar los sistemas, bloquear el acceso, etc.

1.2. Inteligencia de fuentes abiertas (OSINT)

La inteligencia de fuentes abiertas (OSINT) es una disciplina que se encarga de recopilar, analizar y utilizar información de fuentes abiertas para obtener inteligencia sobre un objetivo. La inteligencia de fuentes abiertas se basa en la recopilación de información de fuentes públicas, como sitios web, redes sociales, foros, blogs, etc., para obtener información sobre un objetivo, como direcciones IP, nombres de dominio, usuarios, contraseñas, puertos abiertos, servicios activos, etc.

Hay marcos de trabajo que permiten organizar y estructurar la información recopilada, como el ciclo de inteligencia de fuentes abiertas (OSINT), que entre otras, tiene las siguientes fases:

- **Recolección**: recopilación de información de fuentes abiertas sobre un objetivo, como direcciones IP, nombres de dominio, usuarios, contraseñas, puertos abiertos, servicios activos, etc.
- **Análisis**: análisis de la información recopilada para identificar patrones, tendencias, relaciones, etc., que permitan obtener inteligencia sobre el objetivo.
- **Producción**: elaboración de informes, análisis, conclusiones, etc., que permitan utilizar la inteligencia obtenida para tomar decisiones, planificar acciones, etc.

Podemos ver un conjunto de herramientas que permiten recopilar información de fuentes abiertas, como buscadores, motores de búsqueda, redes sociales, foros, blogs, etc., en la página de OSINT framework.

La distro Kali Linux también tiene preinstaladas algunas herramientas que nos ayudan con esta tarea.

> **Actividad 4.1**
>
> Accede a este curso SEGURIDAD: OSINT INVESTIGACIÓN EN FUENTES ABIERTAS e investiga sobre las herramientas que se utilizan en la inteligencia de fuentes abiertas (OSINT).
>
> Completa al menos hasta el módulo 4.
>
> Documenta los Google Dorks que has utilizado en el módulo 3.
> Haz un listado de las herramientas que has visto en el módulo 4.

1.3. Escaneo de dispositivos y servicios

El escaneo de dispositivos y servicios es una técnica que se utiliza para identificar los dispositivos y servicios activos en una red, como direcciones IP, nombres de dominio, puertos abiertos, servicios activos, etc. El escaneo de dispositivos y servicios se puede realizar mediante diferentes herramientas y técnicas, como el escaneo de puertos, el escaneo de servicios, el escaneo de vulnerabilidades, etc.

Es práctica común entre los ciberdelincuentes escanear puertos para encontrar vulnerabilidades que aprovechar. A la hora de establecer un punto seguro en cualquier servidor o aplicación con acceso a la red debemos tener en cuenta lo siguiente:

- Abre exclusivamente los puertos necesarios.
- Cierra o silencia todos los puertos que no estés usando.
- Utiliza puertos que no sean un estándar.
- Protege todos los servicios susceptibles de ser atacados con sistemas de autentificación adecuados.
- Emplea cortafuegos.

- Oculta información.
- Información como versión del servicio que se está ejecutando, pantalla de acceso y/o registro de WordPress, , logs del servicio,- cambiar las rutas de acceso o administración, ...
- Manten el software actualizado.
- Mantente al día sobre las últimas mejoras de seguridad.

A nivel global ya hemos visto como la web Shodan nos permite buscar dispositivos conectados a Internet y ver información sobre ellos, como direcciones IP, puertos abiertos, servicios activos, etc.

Si nos centrarnos en una red local, podemos utilizar herramientas como `nmap` o `zenmap` para escanear los dispositivos y servicios activos en una red. En la distro Kali Linux también tenemos herramientas como `netdiscover` o `arp-scan` que nos permiten identificar los dispositivos activos en una red.

Actividad 4.2 Escáner de red

También se puede usar **nmap** con su interfaz gráfico **Zenmap** en Windows.

Explica su principio básico de funcionamiento

¿Qué utilidades no lícitas tiene esta herramienta?

Podemos ver ejemplos de uso de `nmap` para escanear los dispositivos y servicios activos en una red en la web Uso básico de Nmap

Además, también podemos usar el comando `netstat` para ver las conexiones activas en un sistema Windows. Podemos ver ejemplos de uso de `netstat` en la web Uso básico de Netstat

Actividad 4.3 Comprobación de puertos

Comprueba los puertos abiertos en tu máquina con el comando `netstat` y realiza capturas de pantalla.

a) Los puertos abiertos en tu máquina.
b) Las aplicaciones que se conectan al exterior.
c) Qué aplicaciones han iniciado un proceso en concreto.
d) Mostrar todas las conexiones.
e) Ver estadísticas de conexiones por protocolos.
f) Ver los puertos y direcciones de origen en formato numérico.
g) Ver conexiones solo del protocolo TCPv4.
h) Ver los puertos abiertos a la escucha.
i) Ver los puertos y conexiones establecidas.
j) Crear un informe de las conexiones establecidas.
k) Aplicaciones involucradas en conexiones con el exterior.

> Ayuda: Infografía netstat

1.4. Escaneo de vulnerabilidades

El escaneo de vulnerabilidades es una técnica que se utiliza para identificar las vulnerabilidades de un sistema informático, como fallos de seguridad, errores de configuración, puertos abiertos, servicios activos, etc. El escaneo de vulnerabilidades se puede realizar mediante diferentes herramientas y técnicas, como el escaneo de puertos, el escaneo de servicios, el escaneo de vulnerabilidades, etc.

Con nmap podemos realizar un escaneo de vulnerabilidades con el comando `nmap --script vuln <dirección IP>`. Este comando ejecuta los scripts de nmap que buscan vulnerabilidades en el sistema objetivo.

En Kali tenemos scripts de nmap que buscan vulnerabilidades en sistemas Windows, Linux, Unix, etc. Estos scripts se encuentran en la carpeta `/usr/share/nmap/scripts/` y se pueden ejecutar con el comando `nmap --script <script> <dirección IP>`.

Por ejemplo, podemos ejecutar el script `smb-vuln-ms17-010` para buscar la vulnerabilidad `MS17-010` en un sistema Windows con el comando `nmap --script smb-vuln-ms17-010 <dirección IP>`.

En Kali Linux podemos usar herramientas como `OpenVAS` o "Nessus" que nos permiten realizar un escaneo de vulnerabilidades en un sistema objetivo. OpenVAS es un escáner de vulnerabilidades de código abierto que permite identificar las vulnerabilidades de un sistema informático y proporcionar recomendaciones para corregirlas.

Podemos ver ejemplos de uso de `OpenVAS` para realizar un escaneo de vulnerabilidades en un sistema objetivo en la web OpenVAS y de Nessus en la web Nessus.

Actividad 4.4 Escáner de vulnerabilidades

Realiza un escaneo de vulnerabilidades en tu máquina con la herramienta `OpenVAS` o `Nessus`.

a) Instala la herramienta en tu máquina.
b) Realiza un escaneo de vulnerabilidades en tu máquina.
c) Documenta las vulnerabilidades encontradas.
d) Proporciona recomendaciones para corregir las vulnerabilidades encontradas.