UNIVERSIDAD AUTÓNOMA DE CHIAPAS

Act. 1. 1 Investigar conceptos

Alumno	Erick Francisco Palacios Trejo
Semestre y grupo	7°M
Materia:	Analisis de vulnerabilidades
Docente	GUTIERREZ ALFARO LUIS
Fecha	25/01/2024

Herramientas de vulnerabilidades:

- **Nmap (Network Mapper):** Nmap es una herramienta de escaneo de red que se utiliza para descubrir hosts y servicios en una red, así como para crear un mapa de la topología de la red. También puede ser utilizado para detectar puertos abiertos, servicios en ejecución y otras características de los sistemas en una red.
- **Joomscan:** Es una herramienta especializada en la detección de vulnerabilidades en sitios web que utilizan el sistema de gestión de contenido (CMS) Joomla. Joomscan busca posibles debilidades y proporciona información sobre la seguridad de un sitio Joomla.
- **Wpscan:** Similar a Joomscan, Wpscan está diseñado para detectar vulnerabilidades en sitios web, pero se centra en sitios que utilizan el CMS WordPress. Puede identificar versiones de WordPress, temas y plugins, y buscar vulnerabilidades conocidas asociadas con ellos.
- **Nessus Essentials:** Nessus es una herramienta de escaneo de vulnerabilidades que identifica y evalúa posibles debilidades en sistemas, redes y aplicaciones. Nessus Essentials es la versión gratuita de Nessus y proporciona funcionalidades esenciales para el escaneo de vulnerabilidades.
- **Vega:** Vega es una herramienta de evaluación de seguridad de aplicaciones web que realiza análisis de seguridad automatizado. Puede ayudar a identificar vulnerabilidades en aplicaciones web mediante el escaneo de URLs y formularios en busca de posibles riesgos de seguridad.

Inteligencia Misceláneo:

- **Gobuster:** Gobuster es una herramienta de enumeración que se utiliza para descubrir recursos ocultos en servidores web mediante ataques de fuerza bruta o diccionario. Puede ser utilizado para buscar directorios, archivos y otros recursos que no deberían estar públicamente accesibles.
- **Dumpster Diving:** Aunque no es una herramienta de software, el "dumpster diving" se refiere a la práctica de buscar información valiosa en la basura física de una organización. Esto podría incluir documentos impresos, discos duros, dispositivos de almacenamiento y otros elementos desechados que podrían contener información sensible.
- **Ingeniería Social:** La ingeniería social es una técnica en la que los atacantes manipulan a las personas para obtener información confidencial o realizar acciones específicas. Esto puede incluir la manipulación psicológica, la obtención de contraseñas a través de interacciones engañosas, o la persuasión para realizar acciones que podrían comprometer la seguridad.

Inteligencia Activa:

Análisis de dispositivos y puertos con Nmap:

Nmap (Network Mapper): Es una herramienta de código abierto utilizada para el descubrimiento de dispositivos y el mapeo de puertos en una red. Puede realizar escaneos de red para identificar hosts, servicios y puertos abiertos.

Parámetros y opciones de escaneo de Nmap:

Nmap proporciona una amplia variedad de opciones y parámetros que permiten personalizar los escaneos según las necesidades del usuario. Algunas opciones comunes incluyen:

- -p: Especifica los puertos a escanear.
- -A: Realiza un escaneo detallado, incluyendo la detección de servicios y sistemas operativos.
- -sS: Escaneo de tipo stealth (TCP SYN scan).
- -sV: Realiza la detección de versiones de servicios.
- -O: Intenta identificar el sistema operativo del objetivo.
- --traceroute: Realiza un traceroute durante el escaneo.

Full TCP Scan:

Un escaneo TCP completo (Full TCP Scan) implica la verificación de todos los puertos TCP en un host. Puede ser más intrusivo y lleva más tiempo que un escaneo rápido, pero proporciona información detallada sobre todos los servicios disponibles.

Stealth Scan:

Un escaneo stealth, como el TCP SYN scan (-sS en Nmap), trata de ser discreto y minimizar la detección. En lugar de completar la conexión TCP, solo inicia el proceso de conexión y analiza las respuestas.

Fingerprinting:

Nmap y otras herramientas pueden realizar fingerprinting para identificar el sistema operativo y las versiones de servicios en los hosts escaneados. Esto implica analizar las respuestas y comportamientos de los servicios para hacer suposiciones educadas sobre la tecnología subyacente.

Zenmap:

Zenmap es una interfaz gráfica de usuario (GUI) para Nmap que facilita la configuración y ejecución de escaneos. Proporciona una representación visual de los resultados del escaneo.

Análisis de traceroute:

El análisis de traceroute implica rastrear la ruta que toma un paquete desde la fuente hasta el destino, mostrando todos los saltos intermediarios. Esto puede ayudar a identificar posibles cuellos de botella o puntos de falla en la red.