Análisis de vulnerabilidades

CONCEPTOS DE VULNERABILIDADES

Presentado por Rodolfo Torija

Herramientas de vulnerabilidades

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.

Joomscan: Es una de las herramientas de código abierto más populares para ayudarlo a encontrar vulnerabilidades conocidas de Jooma Core, ósea, componentes e inyección SQL, ejecución de comandos.

Wpscan: Es un software de código abierto para Kali Linux, diseñado para escanear vulnerabilidades y fallos en un sitio web de WordPress.

Nessus Essentials: Es un escáner de vulnerabilidades, permite escanear la red domestica personal con la misma alta velocidad, evaluaciones a profundidad o buscar vulnerabilidades de forma automatizada.

Vega: herramienta gráfica de auditoría web gratuita y de código abierto, esta herramienta realiza diversas funciones tales como: Análisis de Vulnerabilidades.

Inteligencia Misceláneo

Gobuster: es una herramienta de enumeración a través de fuerza bruta, que nos permite buscar directorios es un dominio, enumeración de dns, enumeración de virtual host, etc.

Dumpster Diving: es el acto de acceder sin autorización a determinada información que pasa por la basura de una empresa, ya sea dentro o fuera del edificio. Hay un dicho famoso que la mayoría seguro han escuchado: «La basura de un hombre es el tesoro de otro».
Eso significa que lo que una persona considera inútil podría ser de gran valor para la otra. El concepto de Dumpster Diving se basa en esto.

Ingeniería Social: diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial de los usuarios. También está definida como un ataque basado en engañar a un usuario o administrador de un sitio en la internet, para poder ver la información que ellos quieren. Se hace para obtener acceso a sistemas o información útil. Los objetivos de la ingeniería social son el fraude y/o la intrusión de una red.

Inteligencia Activa

01 **Análisis de dispositivos y puertos con Nmap**

Es una herramienta para descubrir dispositivos en una red y determinar qué puertos están abiertos en esos dispositivos.

02 **Parametros opciones de escaneo de nmap**

Escáner personalizable, rango de puertos, velocidad del escaneo, entre otros.

03 **Full TCP scan**

Tipo de escaneo exhaustivo que analiza todos los puertos TCP de un dispositivo o una gama de estos en busca de puertos abiertos

04 **Stelth Scan**

Escaneo sigiloso, escaneos desapercibidos en la red

Inteligencia Activa

05 Fingerprintig

Técnica de identificar el sistema operativo, versión del software y otro detalles específicos de un dispositivo a través de patrones de solicitudes de red.

06 Zenmap

Una GUI más amigable de utilizar nmap y visualizar los resultados de los escaneos de red.

07 Análisis traceroute

Se utiliza para rastrear la ruta que sigue un paquete de datos desde su origen hasta su destino final en una red.

¡Gracias!