CONCEPTOS DE VULNERABILIDADES

EDGAR ALEJANDRO VELAZQUEZ MARTÍNEZ

A200114

HERRAMIENTAS DE VULNERABILIDADES

- Una herramienta de análisis de vulnerabilidades o un software de análisis de vulnerabilidades ejecuta los análisis automáticamente para inspeccionar los endpoints en una empresa y para detectar y mostrar una lista detallada del software que funciona en ellos junto con todas sus 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 Joomla Core, 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. WPScan es una herramienta muy poderosa y capaz de darte información detallada sobre una página web.

Nessus Essentials (Escáner de vulnerabilidades) permite escanear la red doméstica personal con la misma alta velocidad, evaluaciones a profundidad o buscar vulnerabilidades de forma automatizada. Esta enfocado a analizar las redes informáticas.

Vega es una herramienta gráfica de auditoría web gratuita y de código abierto. Esta herramienta realiza diversas funciones tales como: Análisis de Vulnerabilidades, Crawler (copia del sitio web), Análisis de contenido, Modificación manual de paquete HTTP (proxy).

INTELIGENCIA MISCELÁNEO

Gobuster es una herramienta de código abierto utilizada en pruebas de penetración y evaluaciones de seguridad para buscar y enumerar recursos ocultos en un servidor web. Principalmente, se utiliza para descubrir directorios, archivos y subdominios que podrían no estar enlazados directamente desde la página principal del sitio web.

"Dumpster Diving" (buceo en los contenedores de basura) es una técnica de ingeniería social que implica buscar información confidencial o valiosa en la basura física de una organización o individuo.

La ingeniería social es un método utilizado por los atacantes para manipular a las personas y obtener información confidencial o acceso a sistemas. Implica la explotación de la psicología humana, la confianza y la interacción social para obtener acceso no autorizado o información sensible.

INTELIGENCIA ACTIVA

El análisis de dispositivos y puertos con Nmap es una técnica utilizada en seguridad informática para descubrir qué dispositivos están activos en una red y qué puertos de red están abiertos o cerrados en esos dispositivos. Nmap es una herramienta de código abierto ampliamente utilizada para realizar escaneos de red y recopilar información sobre sistemas remotos.

Parámetros y Opciones de Escaneo de Nmap: Nmap ofrece una variedad de parámetros y opciones para configurar sus escaneos de red. Estos parámetros permiten ajustar la velocidad, el tipo y la profundidad del escaneo. Algunos ejemplos de parámetros comunes son -sS (escaneo TCP SYN), -sU (escaneo UDP), -A (escaneo de detección de sistema operativo), -p (especificación de puertos), entre otros.

Full TCP Scan: También conocido como escaneo completo de TCP, este tipo de escaneo verifica todos los puertos TCP de un objetivo para determinar su estado (abierto, cerrado o filtrado). Utiliza técnicas como el envío de paquetes SYN, ACK y RST para recopilar información sobre los puertos y los servicios que están en funcionamiento.

Stealth Scan: Un escaneo sigiloso, como el escaneo SYN (-sS), es un tipo de escaneo que trata de ser menos intrusivo y más discreto. Utiliza paquetes TCP SYN para determinar si un puerto está abierto o cerrado, sin completar completamente la conexión. Esto puede ayudar a minimizar la visibilidad del escaneo en los registros del objetivo.

Fingerprinting: El fingerprinting, o huella digital, es el proceso de identificar el sistema operativo, la versión del software y otros detalles sobre un dispositivo a través de la observación y el análisis de su comportamiento en la red. Nmap puede realizar fingerprinting utilizando técnicas como análisis de respuestas de puertos y comportamiento de protocolos.

Zenmap: Zenmap es una interfaz gráfica de usuario (GUI) para Nmap. Proporciona una forma más intuitiva de interactuar con las capacidades de Nmap. Permite a los usuarios configurar y ejecutar escaneos de red, visualizar los resultados en forma de gráficos y tablas, y realizar análisis básicos de la información recopilada.

Análisis Traceroute: El análisis Traceroute es una técnica para rastrear la ruta que los paquetes de datos siguen a través de una red desde la fuente hasta el destino. Ayuda a identificar los saltos intermedios y los posibles cuellos de botella en la red. Nmap también puede realizar un análisis de rutas mediante el uso de comandos y opciones adecuadas.