Conceptos de vulnerabilidades

Yahir Emmanuel Ramirez Diaz
7 “M”

Herramientas de vulnerabilidades

1. Nmap: Network Mapper es una herramienta de código abierto utilizada para descubrir hosts y servicios en una red, creando un mapa de la topología.
2. Joomscan: Es una herramienta específicamente diseñada para escanear y evaluar la seguridad de sitios web construidos en el CMS Joomla.
3. Wpscan: Es una herramienta diseñada para evaluar la seguridad de sitios web basados en WordPress. Escanea sitios en busca de vulnerabilidades en el CMS, plugins y temas utilizados en la instalación.
4. Nessus Essentials: Es una herramienta de escaneo de vulnerabilidades que identifica debilidades en sistemas y aplicaciones.
5. Vega: Es una plataforma de pruebas de seguridad web que se utiliza para evaluar la seguridad de aplicaciones web. Puede realizar escaneos de seguridad automatizados e identificar vulnerabilidades.

Inteligencia Miscelánea

1. Gobuster: Es una herramienta de línea de comandos utilizada para realizar ataques de fuerza bruta o enumeración de directorios y archivos en un sitio web. También ayuda a descubrir contenido oculto o archivos/directorios mal configurados en servicios web.
2. Dumpster Diving: Se refiere a la práctica de buscar información valiosa, como contraseñas o documentos confidenciales, en la basura física o digital de una organización.
3. Ingeniería Social: Es una técnica en la que un atacante manipula a las personas para obtener información confidencial o acceso no autorizado a sistemas. Aquí se hace uso de psicologia y manipulación para engañar a los usuarios y obtener información valiosa.

Inteligencia Activa

1. Análisis de Dispositivos y Puertos con Nmap: Utilizando Nmap, se realiza un escaneo en una red para identificar dispositivos activos y los puertos abiertos en esos dispositivos.
2. Parámetros y Opciones de Escaneo de Nmap: Nmap ofrece una variedad de opciones de escaneo, como escaneos TCP, UDP, scripts personalizados, etc. Los parámetros permiten ajustar el alcance y la profundidad del escaneo.
3. Full TCP Scan: Un escaneo TCP completo implica escanear todos los puertos TCP en un objetivo, lo que proporciona una visión completa de los servicios disponibles en el dispositivo.
4. Stealth Scan: Un escaneo sigiloso, como “Stealth Scan” en Nmap, utiliza técnicas para ocultar el escaneo y parecer menos intrusivo para el objetivo.
5.

5. Fingerprinting: En seguridad informática, el fingerprinting implica identificar el sistema operativo, software y versiones utilizadas en un objetivo, Esto puede ayudar a los atacantes a seleccionar vulnerabilidades específicas para explotar.

6. Zenmap: Es una interfaz gráfica de usuario para Nmap. Facilita la visualización y el análisis de los resultados de los escaneos de red realizados con Nmap.

7. Análisis Traceroute: Es una herramienta utilizada para rastrear la ruta que sigue un paquete de datos desde una fuente hasta un destino en una red. También ayuda a identificar los nodos intermedios por los que pasa el tráfico y a diagnosticar problemas de conectividad.