conceptos de vulnerabilidad

análisis de vulnerabilidad

ANA YAZMIN VELEZ GARCIA – 7° “N”–
INGENIERÍA EN DESARROLLO Y TECNOLOGÍA DE SOFTWARE.

herramientas de vulnerables

NMAP: Es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon y cuyo desarrollo se encuentra hoy a cargo de una comunidad.

JOOMSCAN: E**s una herramienta de auditoría de sitios web para Joomla**. Está escrito en Perl y es capaz de detectar más de 550 vulnerabilidades como inclusiones de archivos, inyecciones de SQL, Defectos de RFI, BIA, Defecto XSS, inyección ciega de SQL, protección de directorios y otros.

WPSCAN: Es un software gratuito que le ayuda a identificar los problemas relacionados con la seguridad en su sitio de WordPress.

NESSUS ESSENTIALS: Es un escáner de vulnerabilidades gratuito que proporciona un punto de entrada para la evaluación de vulnerabilidades.

VEGA: Es una aplicación de código abierto que permite realizar escaneos automatizados con una interfaz gráfica intuitiva

INTELIGENCIA MISCELÁNEO

Gobuster:

Es una herramienta de software para directorios de fuerza bruta en servidores web. No viene preinstalado con Kali Linux.

Bumpster diving:

consiste en investigar la «basura» de una persona u organización para encontrar información que pueda ser ~~util~~izada para atacar una red informática.

Ingenieria Social:

Es la práctica ilegítima de obtener información confidencial a través de la manipulación de usuarios legítimos.

Análisis traceroute:
Es un servicio basado en la nube que nos permite realizar una monitorización de sitios web, servidores, aplicaciones y otros servicios.

Stealth Scan:
Se implementan técnicas de escaneo sigiloso para eludir los firewalls o descubrir hosts activos sin ser detectados.

Fingerprinting
Es toda aquella información sistemática que dejamos sobre un dispositivo informático cada vez que lo utilizamos.

Zenmap
Es la interfaz gráfica de usuario oficial de Nmap Security Scanner.

INTELIGENCIA ACTIVA:

Análisis de dispositivo y puertos con Nmap:
Es la mejor herramienta de escaneo de puertos y descubrimiento de hosts que existe actualmente. Nmap nos permitirá obtener una gran cantidad de información sobre los equipos de nuestra red, es capaz de escanear qué hosts están levantados, e incluso comprobar si tienen algún puerto abierto.

Parámetros opcionales de escaneo de nmap:
Nmap puede instalarse en sistemas Unix, Unixlike y Windows. Nmap está disponible en dos versiones: versión de consola y gráfico.

Full TCP scan:
Es una técnica de exploración de puertos que consiste en enviar un paquete FIN a un puerto determinado, con lo cual deberíamos recibir un paquete de reset (RST) si dicho puerto está cerrado.