CONCEPTOS DE VULNERABILIDAD

Op. 2 – Análisis de Vulnerabilidades
Gomez Hernandez Julio Manuel | A200350 | 7 - M

HERRAMIENTAS DE VULNERABILIDADES

Gordon Lyon
Creador de Mapa de N y escritor de libros, sitios web.

NMAP

NMAP (Network Mapper) es un software de código abierto que se utiliza para escanear una red y sus puertos con el objetivo de obtener información importante sobre la misma para controlar y gestionar su seguridad.

JOOMSCAN

Joomscan es un escáner de vulnerabilidades en la red utilizado para detectar la ejecución de comandos, inyección SQL y otros ataques contra aplicaciones web. Escanea sitios web creados con Joomla. Joomscan localiza las carpetas navegables, localiza cada archivo para identificar la versión de un componente instalado.

WPSCAN

WPScan es un software de código abierto para Kali Linux, diseñado para escanear vulnerabilidades y fallos en un sitio web de WordPress. Es una herramienta muy poderosa y capaz de darte información detallada sobre una página web

HERRAMIENTAS DE VULNERABILIDADES

NESSUS ESSENTIALS

Nessus es una herramienta de escaneo de seguridad remota, que escanea una computadora y genera una alerta si descubre cualquier vulnerabilidad que los piratas informáticos maliciosos puedan usar para obtener acceso a cualquier computadora que haya conectado a una red.

VEGA

Un escáner de Vulnerabilidades de código abierto para probar la seguridad de sitios/aplicaciones web, en la cual nos puede ayudar a encontrar y validar las Inyecciones SQL, Cross-Site Scripting (XSS), Shell Injection, Local File Inclusion, Integer Overflow, entre otras vulnerabilidades.

INTELIGENCIA MISCELÁNEO

ROBUSTER

Es una herramienta open source que permite la identificación de contenido web como directorios o ficheros que pudiesen estar accesibles u ocultos en un portal web. Esto lo realiza a través de solicitudes http con un diccionario o por fuerza bruta, y detectará la existencia de las mismas en función del código de respuesta obtenido.

DUMSPTER DIVING

Se refiere a la exploración de la papelera de un sistema con el fin de encontrar detalles para que un pirata informático pueda realizar un ciberataque. El primer paso para realizar un ataque a un servicio de redes sociales es bucear en el contenedor. Y la fase de ingeniería social vendrá después, cuando los usuarios en línea son llevados a una trampa para que revelen datos privados sobre ellos.

INGENIERIA SOCIAL

Es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo.

INTELIGENCIA ACTIVA

ANÁLISIS DE DISPOSITIVOS Y PUERTOS CON NMAP

Es principalmente una aplicación para el mapeo de puertos de una red, aunque incluye diferentes funcionalidades que le permite obtener mucha otra información.

PARÁMETROS OPCIONES DE ESCANEO DE NMAP

Pueden ser a través de segmentos TCP, datagramas UDP o paquetes ICMP, además, permite realizar escaneos de forma oculta para que sean difíciles de detectar por los firewalls. podremos hacer escaneo de puertos sobre ciertos puertos en concreto, entre rangos de puertos, rangos de direcciones IP, posibilidad de usar paquetes TCP null, FIN, Xmas y ACK.

FULL TCP SCAN

Un escaneo abierto completo establece un apretón de manos TCP de tres vías antes de realizando cualquier puerto escanea el sistema de destino, con el objetivo de determinar su estado si están abiertos y cerrados.
Puede determinar rápidamente si un puerto está abierto o cerrado porque establece un apretón de manos de tres vías TCP con el objetivo.

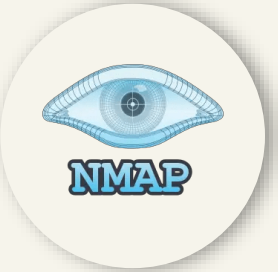
INTELIGENCIA ACTIVA

STEALTH SCAN

Puede realizar rápidamente, escaneando miles de puertos por segundo en una red rápida no obstaculizada por intrusos cortafuegos. Escaneo SYN es relativamente discreto y sigiloso, ya que nunca completa TCP conexiones. También permite claro, diferenciación confiable entre open, closed, y filtered estados.

FINGERPRINTIG

Consiste en recolectar información directamente de los sistemas informáticos de una persona o empresa para conocer más sobre su comportamiento y configuración.



ZENMAP

Es la GUI oficial del escáner de seguridad Nmap.
Tiene como objetivo hacer que Nmap sea fácil de usar para principiantes proporciona características avanzadas para usuarios experimentados de Nmap. Escaneos de uso frecuente se puede guardar como perfiles para facilitar su ejecución repetida.

INTELIGENCIA ACTIVA

ANÁLISIS TRACEROUTE

Es un comando de red que se puede ejecutar en tu computadora, en casos en que experimentes problemas de ruta. Rastrea los "hops" entre tu computadora y el destino final. Por cada hop, la traceroute diagnosticará dónde se encuentra el problema.