UNIVERSIDAD AUTÓNOMA DE CHIAPAS

LICENCAITURA EN INGENIERIA EN DESARROLLO Y TECNOLOGÍAS DE SOFTWARE

Materia: Análisis de vulnerabilidades

Docente: Dr.Luis Gutiérrez Alfaro

Actividad: Investigar los conceptos de vulnerabilidades-herramientas de vulnerabilidades

Alumno: Elian Guadalupe Díaz Balcázar

A200178

7° "N"

Tuxtla Gutierrez Chiapas a 15 de agosto del 2023

HERRAMIENTAS DE VULNERABILIDADES

01 NMAP

02 JOOMSCAN

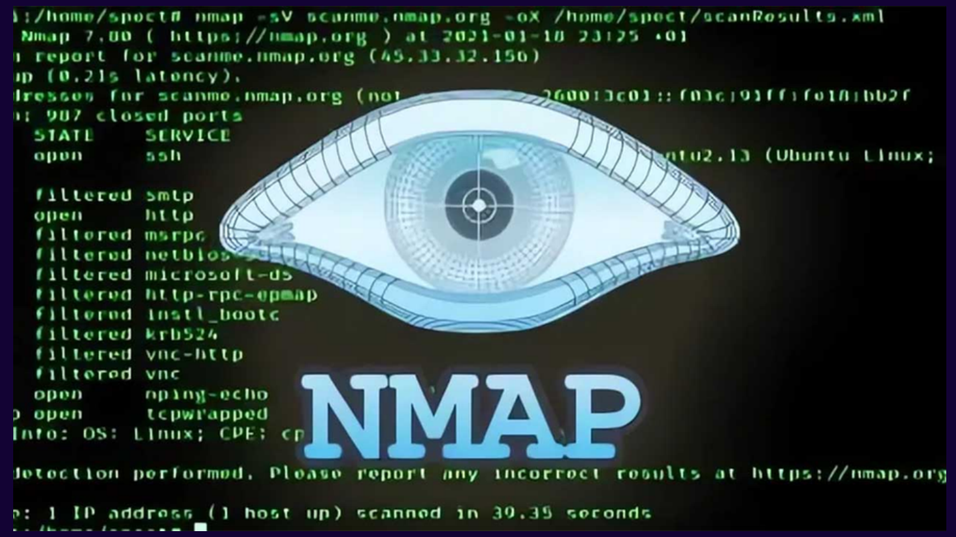
03 WPSCAN

04 NESSUS ESENTIALS

05 VEGA

NMAP

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. Es una aplicación que se utiliza normalmente para realizar auditorías de seguridad y monitoreo de redes.



TIPOS DE ESCANEO NMAP

- Ping/Arp son escaneos muy útiles a la hora de conocer qué host se encuentran activos en la red (Ping) o para obtener información específica sobre los host activos (Arp)
- TCP Connect sirve para realizar una conexión completa de todos los puertos.
- Sondeo de lista tiene la finalidad de obtener los nombres de equipo de los distintos dispositivos conectados a la red, sin la necesidad de enviar un paquete para ello (realiza una resolución inversa de DNS).
- FIN sirve para determinar si el host e encuentra tras un cortafuego.

JOOMSCAN

El servidor Joomla no configurado / reforzado correctamente puede ser vulnerable a muchos, incluida la ejecución remota de código, inyección SQL, secuencias de comandos entre sitios, fuga de información, etc.

El escáner de seguridad JOOMSCAN se refiere a una herramienta de auditoria de sitios web para Joomla. Este se encuentra en Perl y es capaz de detectar más de 550 vulnerabilidades como inclusiones de archivos, inyecciones de SQL, defectos de RFI, BIA, inyección ciega de SQL, protección de directorios, entre otros. Joomscan está destinado a profesionales de seguridad de TI, así como también para administradores de sitios de Joomla.

WPSCAN

WPScan es un software gratuito que le ayuda a identificar los problemas relacionados con la seguridad en su sitio de WordPress. Hace varias cosas como:

- Verifique si el sitio está usando una versión vulnerable de WP
- Compruebe si un tema y un complemento están actualizados o si se sabe que son vulnerables
- Compruebe Timthumbs
- Compruebe la copia de seguridad de la configuración, las exportaciones de bases de datos
- Ataque de fuerza bruta

NESSUS ESSENTIALS

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 (Todo lo que tenga sistema operativo, como sistemas embebidos, dispositivos considerados como parte del IoT, etc.)
Lo que escanea es:

- Puertos abiertos
- Versiones de los servicios
- Detecta e indica las vulnerabilidades de cada dispositivo y puertos

VEGA

Vega es un escaner de seguridad web y testeo de seguridad web. Vega puede encontrar y validar inyecciones de SQL, XSS y muchas otras vulnerabilidades. Podemos encontrarlo en Java, GUI e incluso correr sin problemas en Linux, OS X y WIndows