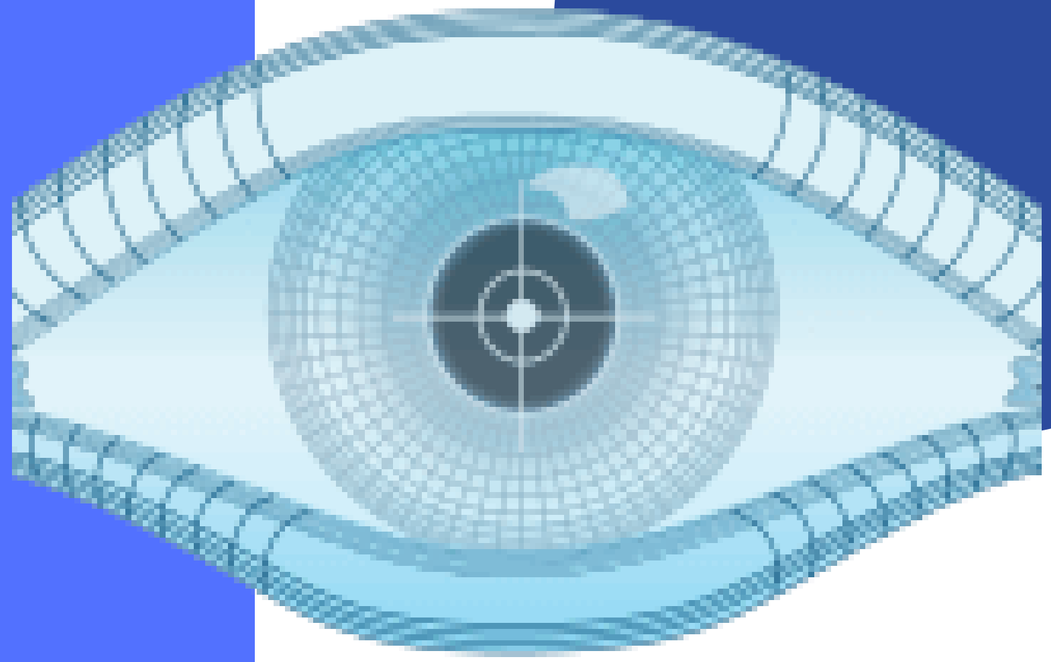
HERRAMIENTAS DE VULNERABILIDADES

MATERIA: ANALISIS DE VULNERABILIDADES
ALUMNO: SERGIO BENJAMÍN TORRES PÉREZ
GRADO Y GRUPO: 7-N
MATRICULA: A200248
DOCENTE: DR GUTIÉRREZ ALFARO LUIS

NMAP

NMAP ES LA HERRAMIENTA DE ESCANEO MÁS FAMOSA UTILIZADA POR LOS PENTESTERS. EN ESTE ARTÍCULO, VEREMOS ALGUNAS CARACTERÍSTICAS PRINCIPALES DE NMAP JUNTO CON ALGUNOS COMANDOS ÚTILES.



NMAP

¿QUÉ ES NMAP?

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. NMAP PERMITE A LOS ADMINISTRADORES DE RED ENCONTRAR QUÉ DISPOSITIVOS SE ESTÁN EJECUTANDO EN SU RED, DESCUBRIR PUERTOS Y SERVICIOS ABIERTOS Y DETECTAR VULNERABILIDADES.

¿POR QUÉ USAR NMAP?

HAY UNA SERIE DE RAZONES POR LAS QUE LOS PROFESIONALES DE LA SEGURIDAD PREFIEREN NMAP A OTRAS HERRAMIENTAS DE ANÁLISIS.
PRIMERO, NMAP TE AYUDA A MAPEAR RÁPIDAMENTE UNA RED SIN COMANDOS NI CONFIGURACIONES SOFISTICADOS. TAMBIÉN ADMITE COMANDOS SIMPLES (POR EJEMPLO, PARA VERIFICAR SI UN HOST ESTÁ ACTIVO) Y SECUENCIAS DE COMANDOS COMPLEJAS A TRAVÉS DEL MOTOR DE SECUENCIAS DE COMANDOS NMAP

JOOMSCAN

JOOMSCAN ES UNA HERRAMIENTA DE CÓDIGO ABIERTO ESCRITA EN PERL QUE SE UTILIZA PRINCIPALMENTE PARA EVALUAR LA SEGURIDAD DE SITIOS WEB CONSTRUIDOS CON JOOMLA, QUE ES UN POPULAR SISTEMA DE GESTIÓN DE CONTENIDOS. ESTA HERRAMIENTA SE CENTRA EN BUSCAR Y DETECTAR VULNERABILIDADES ESPECÍFICAS EN LAS VERSIONES DE JOOMLA INSTALADAS EN UN SITIO WEB.

CARACTERÍSTICAS

ESCANEO DE VERSIONES*: JOOMSCAN PUEDE IDENTIFICAR LA VERSIÓN DE JOOMLA QUE SE ESTÁ EJECUTANDO EN UN SITIO WEB, LO QUE PUEDE SER ÚTIL PARA DETERMINAR SI ESA VERSIÓN TIENE VULNERABILIDADES CONOCIDAS**.**

DETECCIÓN DE EXTENSIONES*: LA HERRAMIENTA PUEDE BUSCAR EXTENSIONES (PLUGINS, MÓDULOS, PLANTILLAS) INSTALADAS EN EL SITIO JOOMLA, Y VERIFICAR SI ALGUNA DE ESTAS TIENE PROBLEMAS DE SEGURIDAD CONOCIDOS.

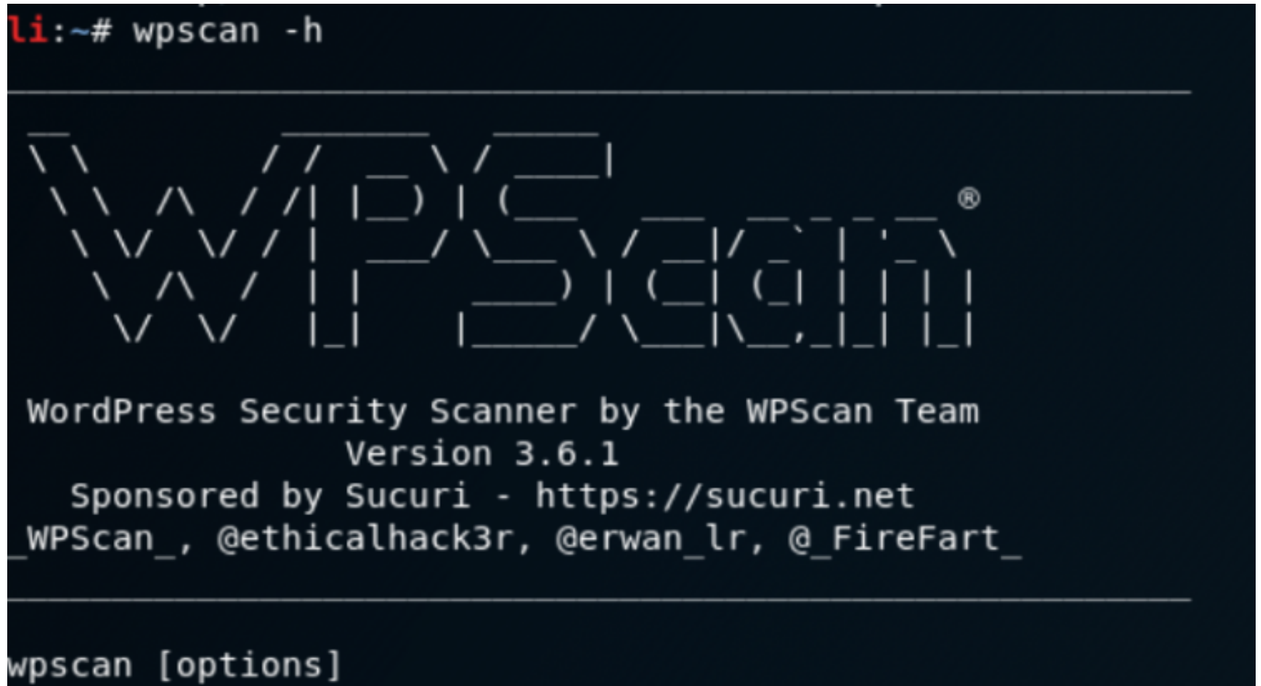
ENUMERACIÓN DE USUARIOS*: JOOMSCAN PUEDE INTENTAR RECOPILAR UNA LISTA DE USUARIOS REGISTRADOS EN EL SITIO WEB, LO QUE PUEDE SER ÚTIL PARA LA AUDITORÍA DE SEGURIDAD.

IDENTIFICACIÓN DE VULNERABILIDADES CONOCIDAS*: LA HERRAMIENTA ESTÁ DISEÑADA PARA BUSCAR VULNERABILIDADES CONOCIDAS Y EXPLOITS ESPECÍFICOS DE JOOMLA EN EL SITIO WEB OBJETIVO.

ESCANEO DE DIRECTORIOS*: JOOMSCAN PUEDE BUSCAR DIRECTORIOS Y ARCHIVOS SENSIBLES EN EL SITIO WEB, AYUDANDO A IDENTIFICAR POSIBLES PUNTOS DE ENTRADA PARA ATAQUES.

WPSCAN

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 Nessus Essentials permite escanear la red doméstica personal con la misma alta velocidad, evaluaciones a profundidad o buscar vulnerabilidades de forma automatizada.

Nessus puede realizar una evaluación de vulnerabilidades sin conexión automáticamente con cada actualización de plug-ins. Desde aquí, puede ejecutar fácilmente un escaneo para validar la presencia de la vulnerabilidad, lo que acelera la detección y la priorización exactas de los problemas.

VEGA

¿QUÉ ES VEGA VULNERABILITY SCANNER?

VEGA ES UNA HERRAMIENTA GRÁFICA DE AUDITORÍA WEB GRATUITA Y DE CÓDIGO ABIERTO.

- ANÁLISIS DE VULNERABILIDADES
- CRAWLER (COPIA DEL SITIO WEB)
- ANÁLISIS DE CONTENIDO
- MODIFICACIÓN MANUAL DE PAQUETE HTTP (PROXY)