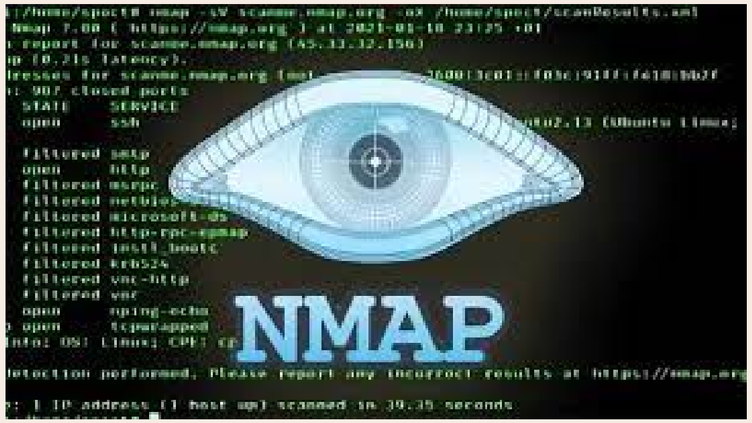
Herramientas de Vulnerabilidad

Alexis Valencia Ramirez

NMAP

Es una aplicación multiplataforma para Linux y Mac; ZenMap para Windows que permite rastrear puertos, descubrir hosts activos, analizar mediante scripts las versiones de los servicios e incluso determinar el sistema operativo que hace correr un host.



Se puede descubrir Vulnerabilidades en un sistema, escaneando los puertos que estas abiertos del mismo y identifica posteriormente a que servicio corresponde y tratando de averiguar si existe un exploit para ese servicio expuesto.

JOOMSCAN

Es una herramienta de auditoria de sitio web para joomla y es capaz de dectar mas de 550 vulnerabilidades como inclusiones de archivps, inyecciones de SQL, defectos de RFI, BIA defectos XSS, inyeccion ciega de SQL, proteccion de directorios y otros.

Es código abierto que es muy popular para ayudar a encontrar vulnerabilidades conocidas de joomla core, componentes e inyección SQL, ejecucion de comandos

WPSCAN

Es un escaner de vulnerabilidades de WorfPress de caja negra que se puede usar para escanear instalaciones remotas de WordPress para encontrar problemas de seguridad, esta herramienta usa una base de datos de 23,107 vulnerabilidades de WordPress.

- **Verifica si el sitio esta usando una versión vulnerable de WP**
- **Comprueba si un tema y un complemento estan 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**

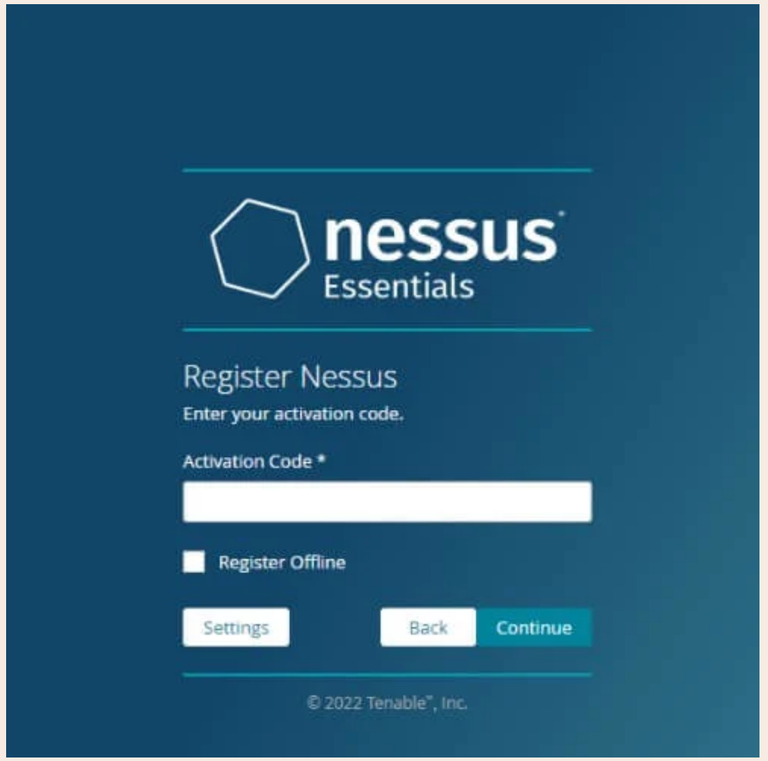
NESSUS ESSENTIALS

Permite escanear vulnerabilidades en la red domestica personal con la misma alta velocidad, evaluaciones a profundidad o buscar vulnerabilidades de forma automatizada.

esta enfocada a analizar las redes informáticas, todo lo que tenga sistema operativo, como sistemas embebidos, dispositivos considerados como parte del loT, etc.

- **puertos abiertos**
- **Versiones de los servidores**
- **Detecta e indica las vulnerabilidades de cada dispositivo y puertos**

Nessus no esta especializado en aplicaciones web



VEGA

Es una herramienta grafica de auditoria web gratuita y de código abierto.
Tiene modulos para realizar ataques tipicos del OWASP como XSS, SQL injection, Directorio transversal, URL injection, Deteccion de errores, etc
usa funciones como:

- **Análisis de Vulnerabilidades**
- **Crawler (Copia del sitio web)**
- **Análisis de contenido**
- **Modificación manual de paquete HTTP (proxy)**