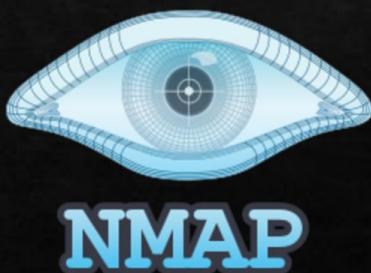


Herramientas de vulnerabilidades

Brian Juárez Arguello

Nmap

- ❖ Nmap (Network Mapper): es una herramienta de código abierto muy utilizada para el escaneo de redes y el descubrimiento de dispositivos, así como para la auditoría de seguridad. Nmap se utiliza para evaluar la seguridad de una red, descubrir hosts en una red y encontrar puertos abiertos en esos hosts. Es útil especialmente para:
- ❖ Escaneo de redes: Descubre dispositivos y direcciones IP en una red, incluso detrás de cortafuegos.



JoomScan

JoomScan es una herramienta de código abierto desarrollada para analizar sitios web que utilizan Joomla! como plataforma de gestión de contenidos. Esta herramienta se centra en buscar posibles vulnerabilidades y debilidades en las instalaciones de Joomla! para ayudar a los administradores de sistemas y a los profesionales de seguridad a mejorar la seguridad de sus sitios web.

Características clave de JoomSca:

1. Detección de versiones: JoomScan puede identificar la versión exacta de Joomla! que se está utilizando en el sitio web, lo que es fundamental para determinar si el sitio está actualizado y si podría ser vulnerable a exploits conocidos dirigidos a versiones anteriores.
2. Búsqueda de vulnerabilidades conocidas: JoomScan puede buscar en su base de datos de vulnerabilidades conocidas para Joomla! y verificar si el sitio web es vulnerable a exploits conocidos. Esto permite a los administradores tomar medidas para corregir estas vulnerabilidades.
3. Enumeración de componentes: La herramienta puede enumerar los componentes, módulos, plugins y temas instalados en el sitio web. Esto es importante para identificar posibles puntos de entrada para un atacante.
4. Escaneo de directorios: JoomScan también puede realizar un escaneo de directorios en busca de archivos sensibles o información que podría ser utilizada por atacantes para obtener acceso no autorizado.
5. Informes de seguridad: La herramienta puede generar informes detallados sobre las vulnerabilidades y los hallazgos de seguridad en el sitio web, lo que facilita la comprensión de las áreas que necesitan ser corregidas.

WPScan

- ❖ WPScan es una herramienta de código abierto determinada específicamente para analizar la seguridad de los sitios web que utilizan WordPress, uno de los sistemas de gestión de contenidos (CMS) más populares del mundo. WPScan se enfoca en buscar posibles vulnerabilidades en el core de WordPress, así como en temas (themes) y plugins comunes, lo que ayuda a los administradores y profesionales de seguridad mantener a sus sitios web más seguros. Características clave de WPScan
- ❖ Escaneo de Vulnerabilidades: WPScan busca activamente vulnerabilidades conocidas en el software subyacente de WordPress, así como en temas (themes) y plugins instalados. Esto ayuda a los administradores de sitios web a identificar y solucionar posibles problemas de seguridad



Nessus Essentials

- ❖ Nessus Essentials, anteriormente conocido como Nessus Home, es una versión gratuita para uso personal y pequeñas redes de Nessus, una potente herramienta de análisis de vulnerabilidades desarrollada por Tenable. Nessus es ampliamente utilizado en la industria de la ciberseguridad para identificar y evaluar las vulnerabilidades en sistemas, redes y aplicaciones. Aquí hay algunas características clave de Nessus Essentials:
- ❖ Escaneo de vulnerabilidades: Nessus Essentials permite a los usuarios realizar escaneos de seguridad en sus sistemas y redes para identificar posibles vulnerabilidades. Puede detectar problemas de seguridad en sistemas operativos, aplicaciones, servicios de red y más.



Vega

- ❖ Vega es una herramienta de prueba de seguridad de código abierto diseñado para ayudar a los profesionales de la seguridad a encontrar y validar vulnerabilidades en aplicaciones web. Está diseñado para realizar pruebas automáticas y manuales en aplicaciones web y, en particular, se enfoca en identificar vulnerabilidades en la capa de aplicación, como inyecciones de SQL, cross-site scripting (XSS), entre otros. Aquí hay algunas características clave de Vega:
- ❖ Escaneo Automático: Vega puede realizar escaneos automáticos de aplicaciones web para buscar vulnerabilidades conocidas, como inyecciones de SQL, vulnerabilidades de scripting, exposición de archivos y más.

