Universidad Autónoma de Chiapas.

Herramientas de vulnerabilidades

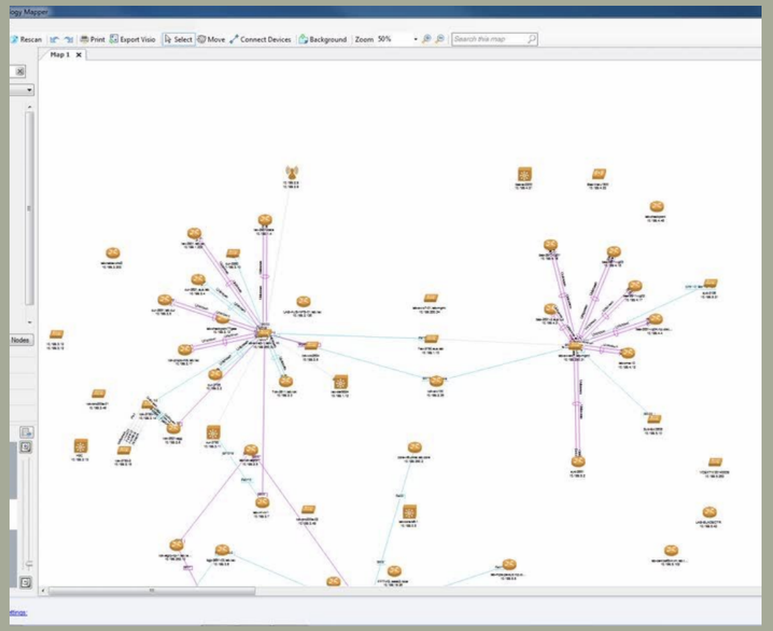
Dr. Luis Gtz Alfaro
Alexis Solís

Análisis de vulnerabilidades

Herramientas de vulnerabilidades

1	2	3	4	5
Nmap	Joomscan	Wpscan	Nessus Essentials	Vega

Nmap



Nmap, o conocido por su completo como "Network Mapper", es una herramienta de línea de comandos de Linux de código abierto que principalmente es usado para escanear direcciones IP, puertos en una red, así como también para hallar aplicaciones instaladas.

Entonces, NMap permite a los administradores de red encontrar qué dispositivos se están ejecutando en su red, el poder encontrar puertos y servicios abiertos para así detectar las vulnerabilidades de estas.

¿Por qué usar Nmap?

Dentro de las razones por la cual se recomienda usar Nmap se encuentra que facilita a mapear rápidamente una red sin comandos ni configuraciones sofisticados. También admite comandos simples (en donde verifica si un host está activo), así como también las secuencias de comandos complejas a través del motor de secuencias de comandos Network Mapper.

¿Por qué usar Nmap?

- Ayuda a identificar los servicios que se ejecutan en un sistema, en donde están incluidos lo que son los servidores web, servidores DNS, etc.
- Capacidad para reconocer rápidamente todos los dispositivos, como es el caso de los servidores, conmutadores, enrutadores, teléfonos, entre otros.
- Facilita el hallazgo de información sobre el sistema operativo que se están ejecutando en los dispositivos

Joomscan

Es una aplicación que ejecutada desde consola (a través de interface web), la cual permite localizar vulnerabilidades web conocidas para Joomla. Es bien conocida, porque está escrita en Perl (como todo buen script que se precie) y permite la actualización por SVN.

Características

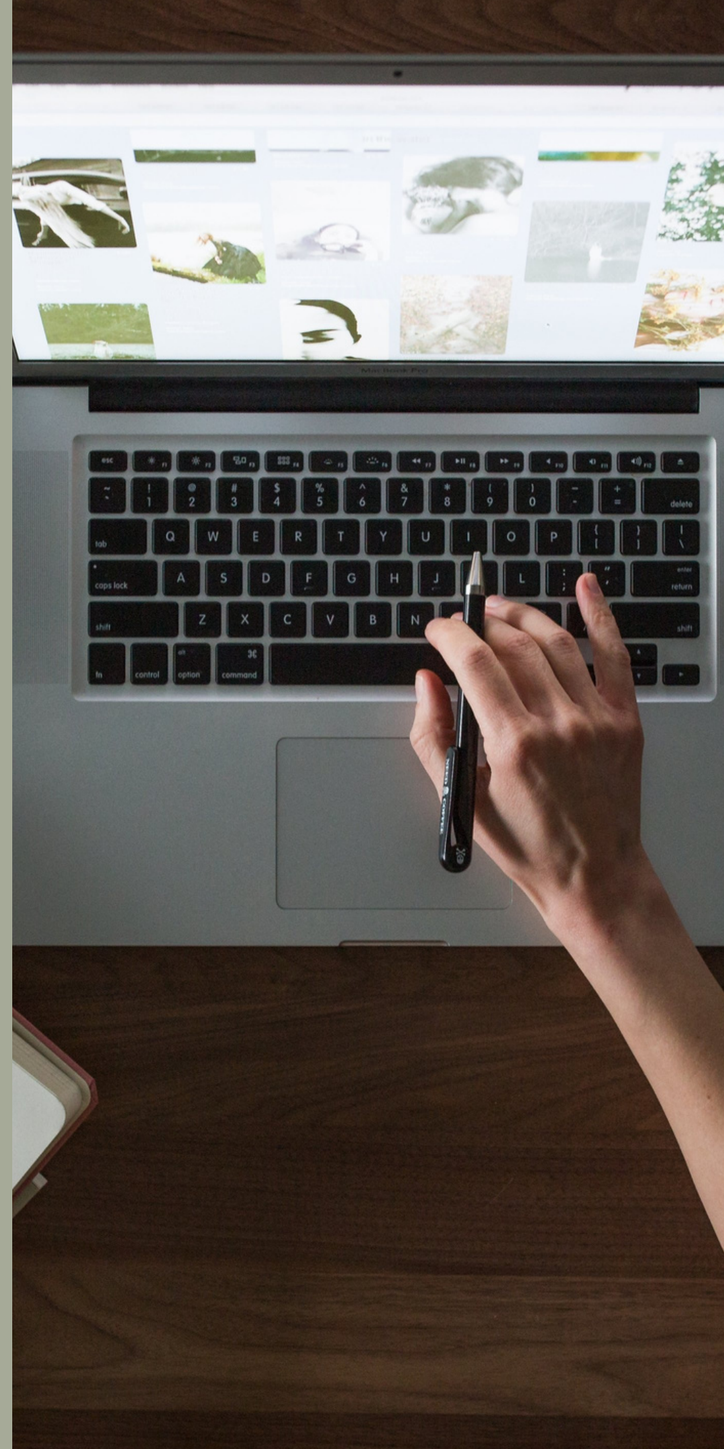
- Permite detectar la versión de Joomla que se está ejecutando.
- Escanea y localiza vulnerabilidades conocidas en Joomla y sus extensiones.
- Presenta informes en formato texto o HTML.
- Permite su actualización inmediata a través de un escáner o svn.
- Detecta vulnerabilidades de tipo: SQL injection, LFI, RFI, XSS entre otros.

Wpscan

Es un software de código abierto para Kali Linux, diseñado para escanear vulnerabilidades y fallos en un sitio web de WordPress. De igual forma, es una herramienta muy poderosa y capaz de darnos información detallada sobre una página web, y además que con eso, pues prácticamente se puede auditar sistemas, verificar su estado y corregir cada fallo que exista, esto con la finalidad de que antes no lo aproveche un delincuente.

WPScan y sus comandos..

- vp: vulnerable plugins. Sirve para detectar qué plugins usados en el sitio tienen vulnerabilidades. Asimismo, al ir al buscador, puedes encontrar cuáles son las fallas.
- ap: all plugins. Muestra todos los plugins que usa el sitio web, no solo los que tengan que ver con los vulnerables.
- p: popular plugins. Indica cuáles son los pluggins más solicitados.
- vt: vulnerable themes. Señala cuáles son los temas vulnerables que utiliza el sitio web. Es así como se puede buscar qué ataques funcionan, con la finalidad de protegerlos.



Nessus Essentials

Se puede decir que esta es una versión gratuita del escáner de vulnerabilidades Nessus. El código de activación no caduca, lo cual hace que se pueda utilizar durante el tiempo que uno lo requiera.

Ventajas y más..

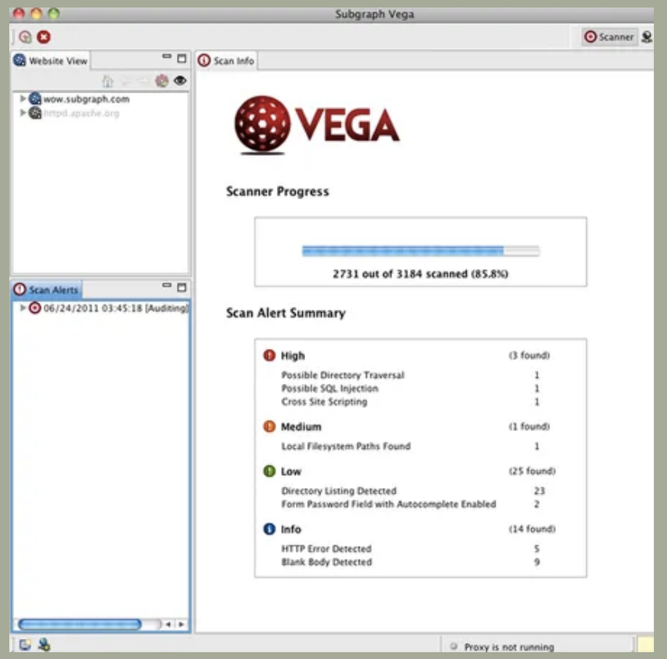
Nessus proporciona una forma rápida y fácil de usar para encontrar y corregir vulnerabilidades en muchos tipos de activos de Tecnologías de la Información, incluidos los recursos virtualizados y basados en la nube. De igual forma

nessus® Essentials

Vega.

A Vega se le puede conocer como una plataforma comercial de prueba de seguridad y escáner de vulnerabilidades de aplicaciones web desarrollada por Subgraph, en la cual la herramienta está diseñada para facilitar a los desarrolladores a hallar y validar la inyección XSS, SQL, entre otras más.

Vega.



Dentro de las ventajas es que ayuda a encontrar vulnerabilidades como : secuencias de comandos entre sitios reflejadas, secuencias de comandos entre sitios almacenadas, inclusión remota de archivos, inyección de SHELL. De igual forma, investiga la configuración de seguridad de TLS/SSL y así poder identificar oportunidades para mejorar la seguridad de sus servidores TLS.

Bibliografía.

Guía de referencia de NMAP (Página de manual). (s. f.). https://nmap.org/man/es/index.html#:~:text=Nmap%20(%E2%80%9Cmapeador%20de%20redes%E2%80%9D,del%20T.)

ESCANEO DE VULNERABILIDADES WEB CON VEGA SCANNER. (s. f.). https://academy.seguridadcero.com.pe/blog/escaneo-vulnerabilidades-web-vega

Lamalejo. (2010b, marzo 27). Escaneando vulnerabilidades en Joomla con JoomScan. luismendezalejo.es. https://luismendezalejo.es/escaneando-vulnerabilidades-en-joomla-con-joomscan/

KeepCoding, R. (2023, 23 enero). ¿Qué es WPSCAN? | KeepCoding Bootcamps. KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-wpscan-ciberseguridad/