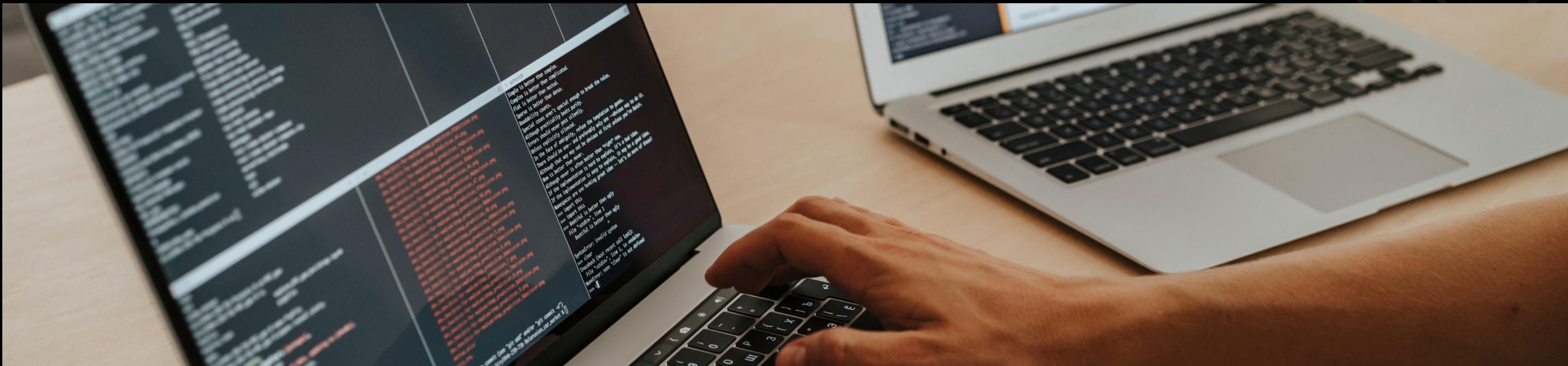




UNIVERSIDAD AUTÓNOMA DE CHIAPAS  
LICENCIATURA EN INGENIERÍA EN DESARROLLO Y TECNOLOGÍAS DE  
SOFTWARE  
ANÁLISIS DE VULNERABILIDADES  
DOCENTE: DR. LUIS GUTIÉRREZ ALFARO  
INVESTIGAR LOS CONCEPTOS DE VULNERABILIDADES (HERRAMIENTAS  
DE VULNERABILIDADES)  
RUBEN OCTAVIO RODRÍGUEZ CANO – A200113  
7° N



# NMAP

NMAP por sus siglas en inglés “Network Mapper”. Se refiere a una herramienta de línea de comandos de Linux de código abierto, el cual sirve para el escaneo de direcciones IP y de puertos de una red, así como también nos servirá para detectar aplicaciones instaladas.

Nmap les permite a los administradores de red el monitorear los dispositivos que se están ejecutando dentro de su red, así como también descubrir puertos y servicios abiertos y también poder detectar vulnerabilidades.



# OTRAS CARACTERÍSTICAS DE NMAP INCLUYEN

- Capacidad para reconocer rápidamente todos los dispositivos, incluidos servidores, enrutadores, conmutadores, dispositivos móviles, etc. en redes únicas o múltiples.
- Ayuda a identificar los servicios que se ejecutan en un sistema, incluidos los servidores web, los servidores DNS y otras aplicaciones comunes. Nmap también puede detectar versiones de aplicaciones con una precisión razonable para ayudar a detectar vulnerabilidades existentes.
- Nmap puede encontrar información sobre el sistema operativo que se ejecuta en los dispositivos. Puede proporcionar información detallada, como las versiones del sistema operativo, lo que facilita la planificación de enfoques adicionales durante las pruebas de penetración.



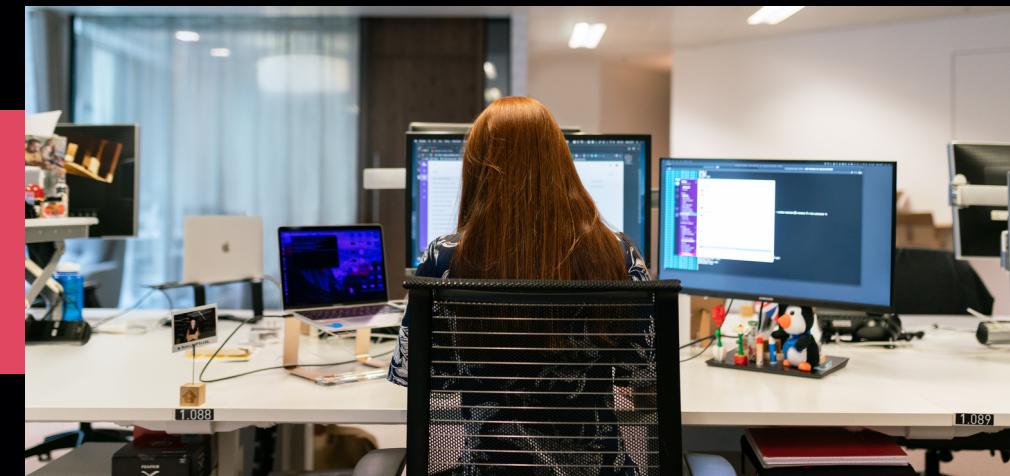
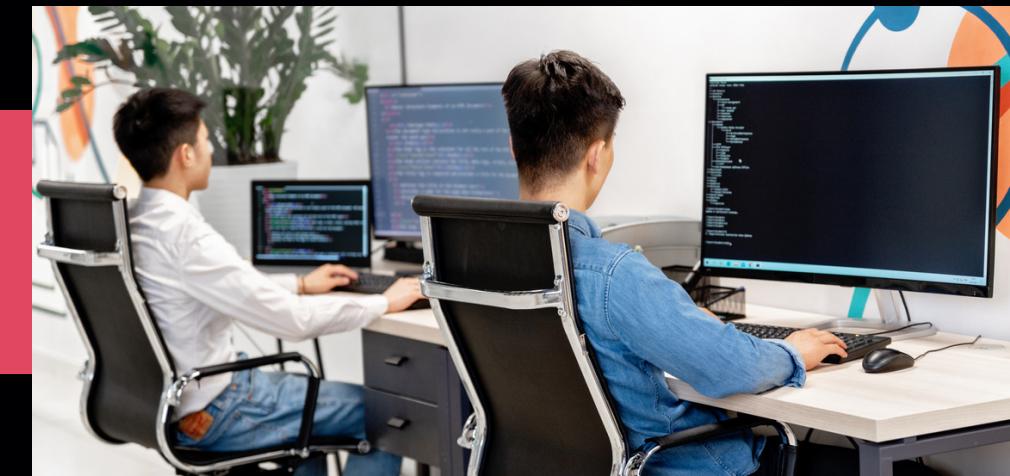
# JOOMSCAN

El escáner de seguridad JOOMSCAN se refiere a una herramienta de auditoría 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.



## VARIAS DE SUS PRINCIPALES CARACTERÍSTICAS DE JOOMLA SON LAS SIGUIENTES



- Detección de versiones de Joomla.

- Detección y enumeración de componentes, complementos y módulos vulnerables.

- Publicar una nota defensiva para proteger adecuadamente su sitio web.



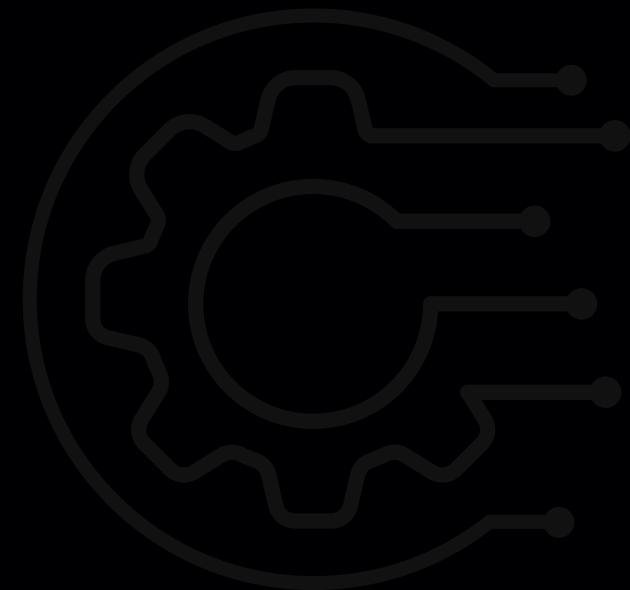
# WPSCAN

## Application

Wpscan por sus siglas en ingles se refiere a “WordPress Security Scanner” es un escáner de seguridad en línea. Este es útil si el sitio web está en una red privada o en una intranet en la cual el internet no está disponible.

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





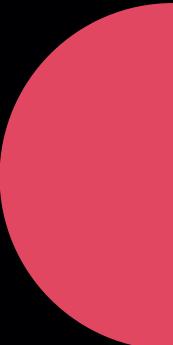
# NESUS ESSENTIALS

Como parte de la familia Tenable Nessus, Tenable Nessus Essentials le permite escanear su entorno (hasta 16 direcciones IP por escáner) con la misma velocidad, evaluaciones exhaustivas y la misma comodidad de escaneo sin agentes que disfrutan los suscriptores de Nessus.



## ¿Qué escanea?

- 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