



HERRAMIENTAS DE VULNERABILIDADES

UNIVERSIDAD AUTONOMA DE CHIAPAS
LIDTS

ANÁLISIS DE VULNERABILIDADES

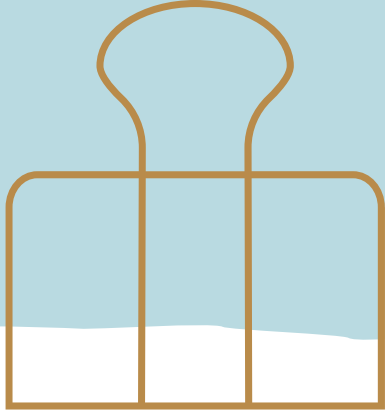
DOCENTE: DR. LUIS GUTIERREZ ALFARO

JAZMÍN MIJANGOS LÓPEZ

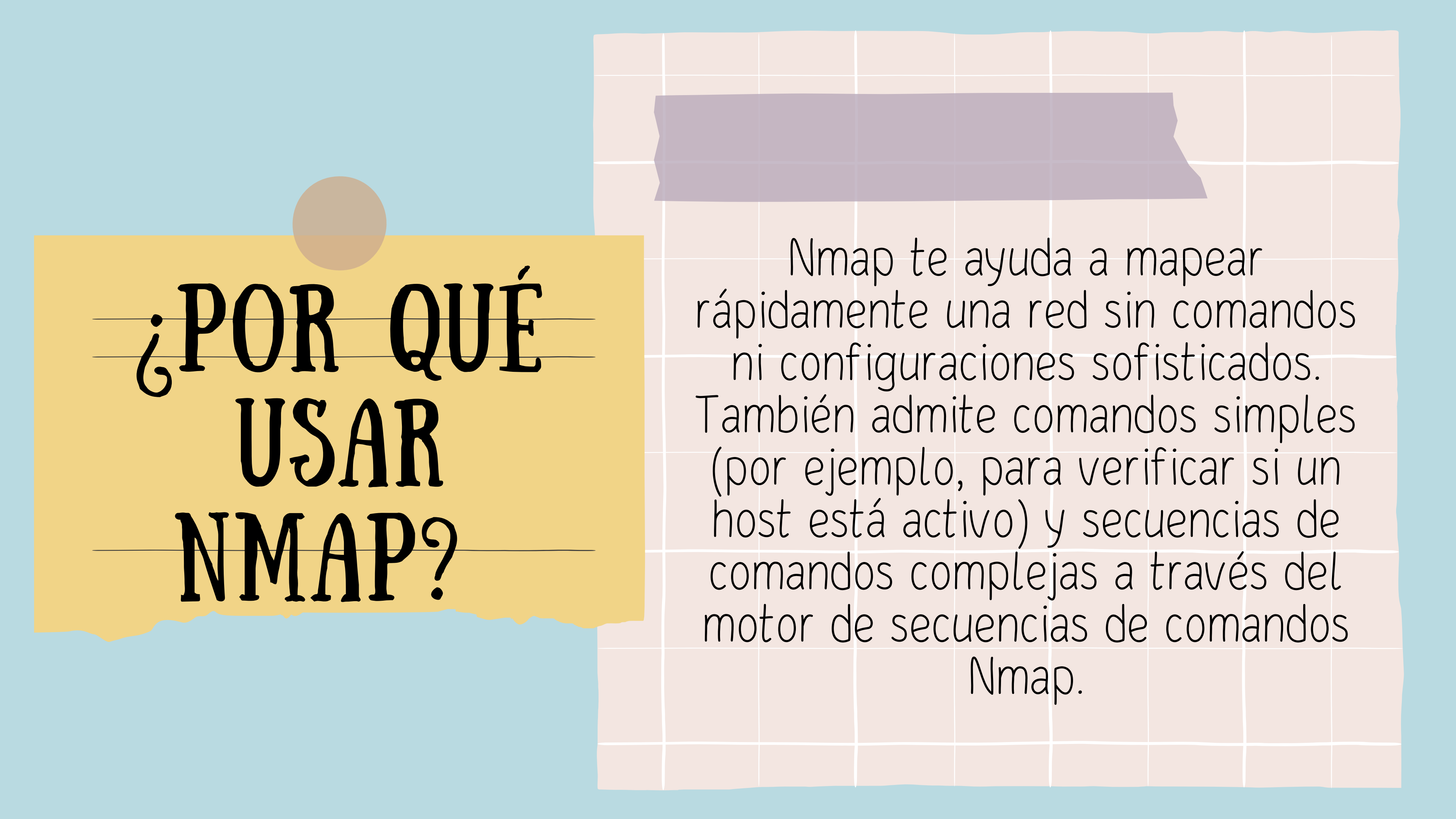
7° N Matricula: A200179



NMAP



Nmap es la abreviatura de Network Mapper (Mapeador de redes). Es una herramienta de línea de comandos de Linux de código abierto que se utiliza de comandos de de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas.



¿POR QUÉ USAR NMAP?

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.

OTRAS CARACTERÍSTICA S DE NMAP



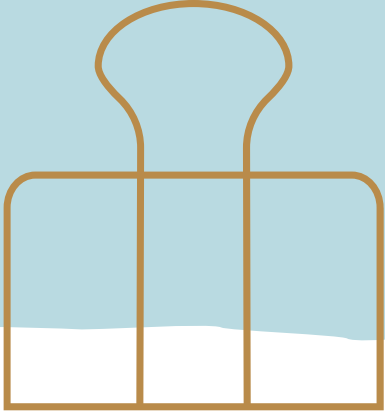
- Capacidad para reconocer rápidamente todos los dispositivos, incluidos servidores, enrutadores, conmutadores, dispositivos móviles, etc. en redes únicas o múltiples.
- Ayuda a identificar los servicios que se ejecutan en un sistema, incluidos los servidores web, los servidores DNS y otras aplicaciones comunes.

OTRAS CARACTERÍSTICA S DE NMAP



- Nmap puede encontrar información sobre el sistema operativo que se ejecuta en los dispositivos.
- Durante la auditoría de seguridad y el escaneo de vulnerabilidades, puedes usar Nmap para atacar sistemas usando scripts existentes del motor de scripting de Nmap.
- Nmap tiene una interfaz gráfica de usuario llamada Zenmap. Te ayuda a desarrollar mapeos visuales de una red para una mejor usabilidad y generación de informes.

JOOMSCAN



Joomscan es un escáner de vulnerabilidades en la red utilizado para detectar la ejecución de comandos, inyección SQL y otros ataques contra aplicaciones web. Como sugiere su nombre, Joomscan escanea sitios web creados con Joomla.



¿POR QUÉ USAR JOOMSCAN?

es capaz de detectar más de 550 vulnerabilidades como inclusiones de archivos, inyecciones de SQL, Defectos de RFI, BIA, Defecto XSS, inyección ciega de SQL, protección de directorios y otros.

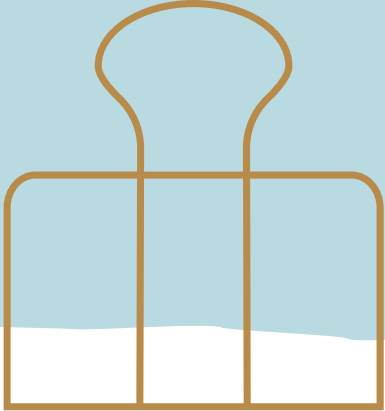
Joomscan está destinado a los profesionales de seguridad de TI y administradores de sitios Joomla.

CARACTERÍSTICAS DE JOOMLA



- Detección de versiones de Joomla.
- Detección y enumeración de componentes, complementos y módulos vulnerables.
- Publicar una nota defensiva para proteger adecuadamente su sitio web.

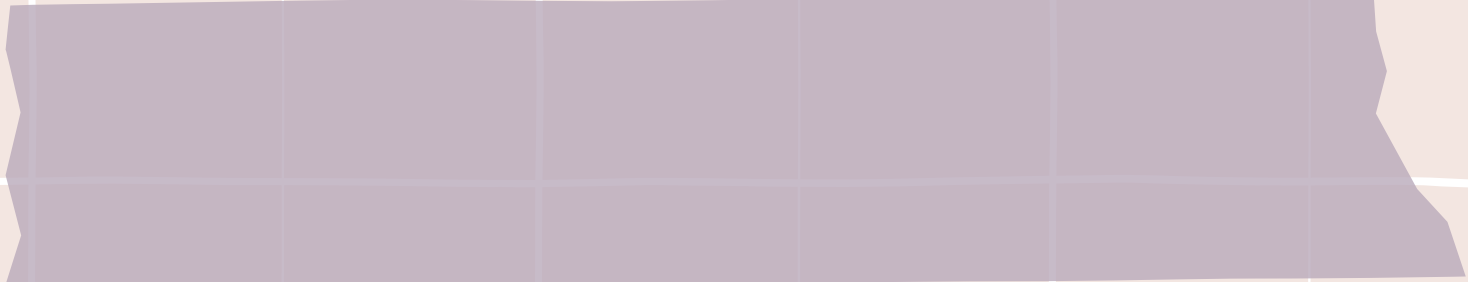
WPSCAN



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.



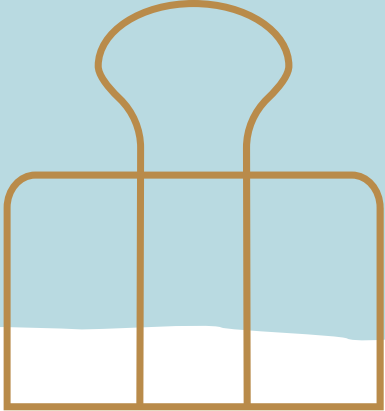
WPSCAN?



Con ella, puedes auditar sistemas, verificar su estado y corregir cada fallo que encuentres antes de que lo aproveche un delincuente.

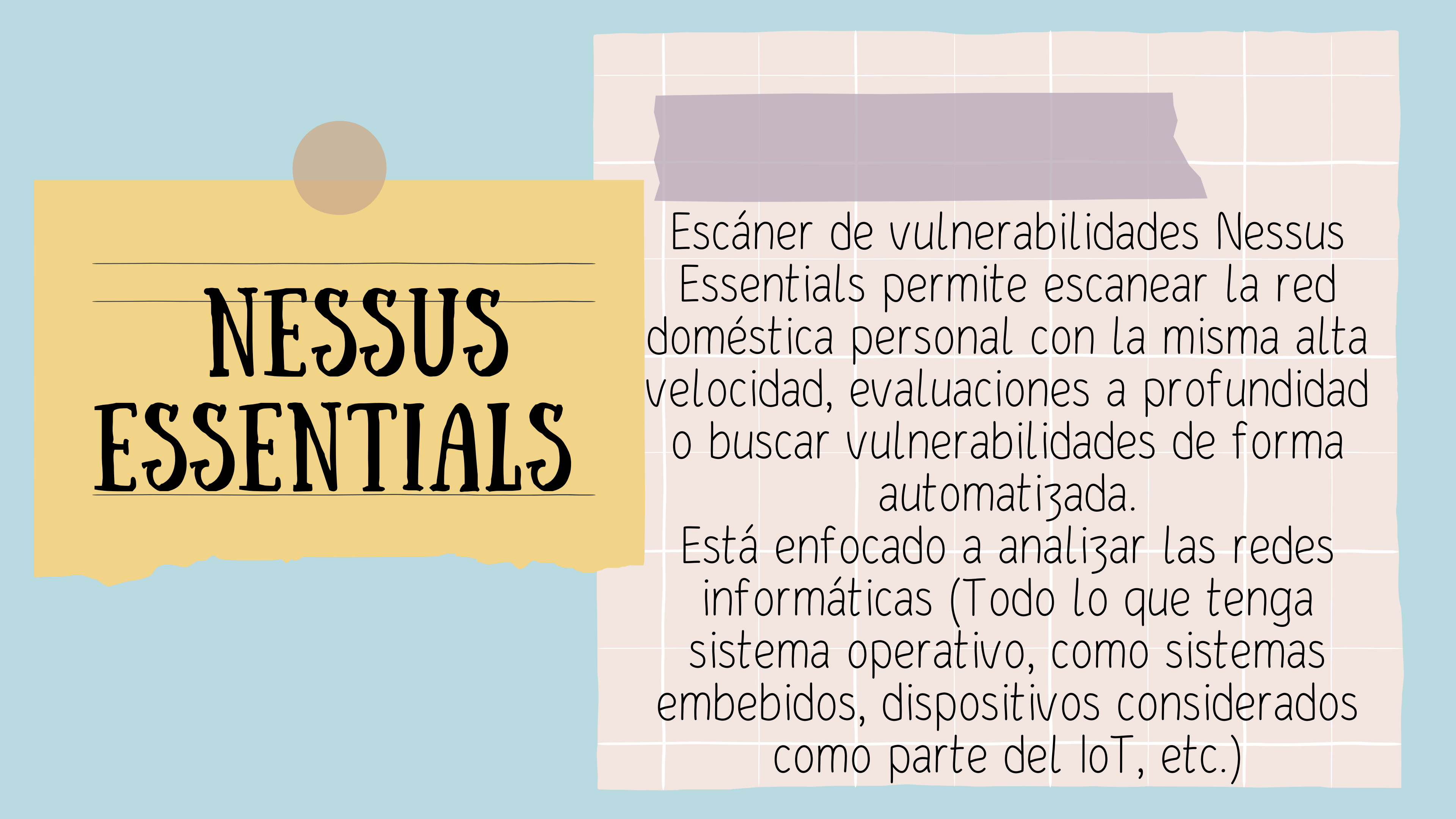
Algunos comandos WPSCAN:
vp, ap, p, vt, at, t, u.

NESSUS ESSENTIALS



Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos.

Consiste en un demonio o diablo, `nessusd`, que realiza el escaneo en el sistema objetivo, y `nessus`, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos.

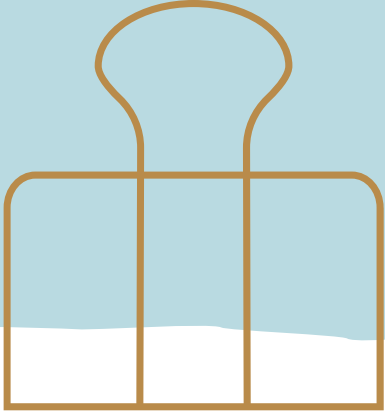


NESSUS ESSENTIALS

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.

Está enfocado a analizar las redes informáticas (Todo lo que tenga sistema operativo, como sistemas embebidos, dispositivos considerados como parte del IoT, etc.)

VEGA



Vega es una herramienta gráfica de auditoría web gratuita y de código abierto.

Esta herramienta realiza diversas funciones tales como:

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



¿POR QUÉ USAR VEGA?

Puede ayudarnos a encontrar y validar la inyección de SQL, la secuencia de comandos en sitios cruzados (XSS), la información confidencial revelada inadvertidamente y muchas otras vulnerabilidades.

El escáner de Vega hace que encontrar y comprender la gravedad de las vulnerabilidades de las aplicaciones web sea sencillo, ya que muestra de forma clara y concisa los recursos útiles en cada análisis