



# UNIVERSIDAD AUTÓNOMA DE CHIAPAS

LICENCIATURA EN INGENIERIA EN DESARROLLO  
Y TECNOLOGIAS DE SOFTWARE

---

## ANALISIS DE VULNERABILIDADES

**Alumno: Luis Gerardo Mendoza Gómez**

**Docente: Dr. Luis Gutierrez Alfaro**

**Semestre: 7**

**Grupo: M**

**Matricula: A200004**

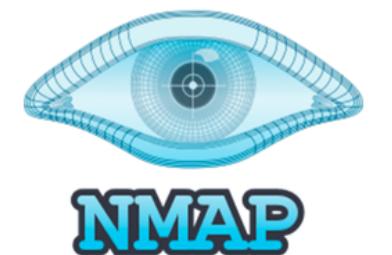
**Fecha de entrega: 15/08/23**



# HERRAMIENTAS DE VULNERABILIDADES:

## **NMAP(NETWORK MAPPER):**

Nmap es una herramienta de código abierto ampliamente utilizada para el escaneo de redes y la detección de hosts en una red. Proporciona capacidades de descubrimiento, escaneo de puertos y servicios, detección de sistemas operativos, entre otras características. Nmap es conocido por su flexibilidad y versatilidad en la identificación de dispositivos y la evaluación de la seguridad de una red.



## **JOOMSCAN:**

JoomScan es una herramienta diseñada específicamente para evaluar la seguridad de sitios web que utilizan el sistema de gestión de contenido Joomla. Realiza escaneos automatizados en busca de vulnerabilidades comunes en sitios web Joomla, como inyecciones SQL, exposición de archivos, problemas de configuración y más. Es una herramienta útil para administradores de seguridad y desarrolladores web que desean fortalecer la seguridad de sitios basados en Joomla.



## **WpsScan:**

WPScan es una herramienta destinada a la evaluación de la seguridad de sitios web que utilizan el sistema de gestión de contenido WordPress. Se enfoca en buscar vulnerabilidades en plugins, temas y configuraciones débiles en sitios WordPress. WPScan proporciona una amplia gama de pruebas de seguridad automatizadas y es una elección popular entre los profesionales de la seguridad que trabajan con sitios web WordPress.



# HERRAMIENTAS DE VULNERABILIDADES:

## **NESSUS ESSENTIALS:**

Nessus Essentials es una versión gratuita de la popular herramienta de evaluación de vulnerabilidades Nessus. Permite escanear redes en busca de vulnerabilidades conocidas en sistemas operativos, aplicaciones y servicios. Ofrece un amplio rango de escaneos y reportes detallados para ayudar a los administradores a identificar y abordar posibles problemas de seguridad en sus redes y sistemas.



## **VEGA:**

Vega es una herramienta de prueba de seguridad de aplicaciones web de código abierto y gratuita. Proporciona una interfaz gráfica para realizar pruebas de seguridad automatizadas en aplicaciones web. Vega puede ayudar a identificar vulnerabilidades como inyecciones SQL, cross-site scripting (XSS), cross-site request forgery (CSRF), entre otros problemas de seguridad comunes en aplicaciones web.



# INTELIGENCIA MISCELLANEA:

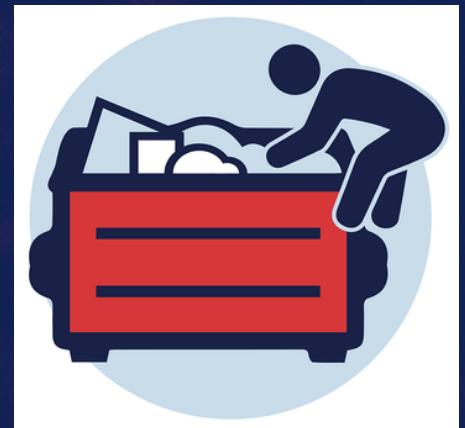
## **GOBUSTER:**

Gobuster es una herramienta de línea de comandos utilizada para realizar ataques de fuerza bruta y descubrimiento de contenido en aplicaciones web. Su función principal es buscar directorios y archivos ocultos o no enlazados en un sitio web o en un servidor. Puede ser utilizado por profesionales de seguridad para identificar posibles puntos de entrada y vulnerabilidades en una aplicación web, así como también para evaluar la exposición accidental de contenido que no debería ser público.



## **DUMPSTER DIVING:**

Dumpster diving (buceo en la basura) es una técnica utilizada en ingeniería social que implica buscar información valiosa en la basura física, como documentos desechados, facturas, correos, o cualquier otro tipo de material que contenga información sensible. Los atacantes pueden utilizar esta técnica para obtener información confidencial que podría usarse en intentos de phishing, suplantación de identidad u otros tipos de ataques.



## **INGENIERIA SOCIAL:**

La ingeniería social es una técnica que implica manipular a las personas para obtener información confidencial o para que realicen acciones que comprometan la seguridad. Los ataques de ingeniería social explotan aspectos psicológicos y sociales de las personas, como la confianza, la empatía o la falta de conocimiento de seguridad. Los atacantes pueden utilizar llamadas telefónicas, correos electrónicos, mensajes de texto u otros medios para engañar a las personas y obtener acceso a sistemas, contraseñas u otra información sensible.



# INTELIGENCIA ACTIVA:

## **ANALISIS DE PUERTOS Y DISPOSITIVOS CON NMAP:**

Nmap (Network Mapper) es una herramienta de código abierto utilizada para descubrir y mapear redes, además de identificar dispositivos y servicios en una red. Realiza escaneos de puertos y servicios para determinar qué sistemas están activos y qué puertos están abiertos. Esto ayuda a los administradores de seguridad a identificar posibles vulnerabilidades y configuraciones inseguras en los dispositivos de red.

## **PARAMETROS Y OPCIONES DE SCANEO CON NMAP:**

Nmap ofrece una variedad de opciones de línea de comandos para personalizar y ajustar los escaneos de acuerdo a las necesidades. Algunos parámetros comunes incluyen -sS para escaneo SYN (stealth scan), -sT para escaneo TCP, -sU para escaneo UDP, -A para detección de versión y sistema operativo, -p para especificar puertos, y muchos más.

## **FULL TCP SCAN:**

Un "Full TCP Scan" es un tipo de escaneo exhaustivo que verifica todos los puertos TCP de un objetivo. Nmap intenta establecer una conexión a cada puerto para determinar si está abierto, cerrado o filtrado por un firewall.

# INTELIGENCIA ACTIVA:

## **STEALTH SCAN:**

El "Stealth Scan", a menudo realizado utilizando el escaneo SYN (" -sS "), es un tipo de escaneo en el que Nmap intenta establecer una conexión de tres pasos solo hasta la etapa de envío de SYN, sin completar la conexión. Esto permite obtener información sobre los puertos abiertos sin generar un registro completo en los logs del objetivo.

## **FINGERPRINTING(ESCANEO DE HUELLAS):**

El "Fingerprinting" implica identificar el sistema operativo, las versiones de software y otros detalles sobre los servicios que se ejecutan en los puertos abiertos de un objetivo. Nmap utiliza técnicas de huellas digitales para obtener información sobre los sistemas y servicios identificados.

## **ZENMAP:**

Zenmap es la interfaz gráfica de usuario (GUI) para Nmap. Proporciona una forma más visual de configurar y ejecutar escaneos, lo que facilita el uso de Nmap para usuarios que no están familiarizados con la línea de comandos.

# INTELIGENCIA ACTIVA:

## **ANALISIS TRACEROUTE:**

El análisis traceroute (tracert en Windows) es una herramienta que rastrea la ruta que sigue un paquete de datos desde un origen hasta un destino a través de una red. Proporciona información sobre los saltos intermedios que el paquete toma, mostrando los dispositivos y routers que manejan el tráfico en el camino.