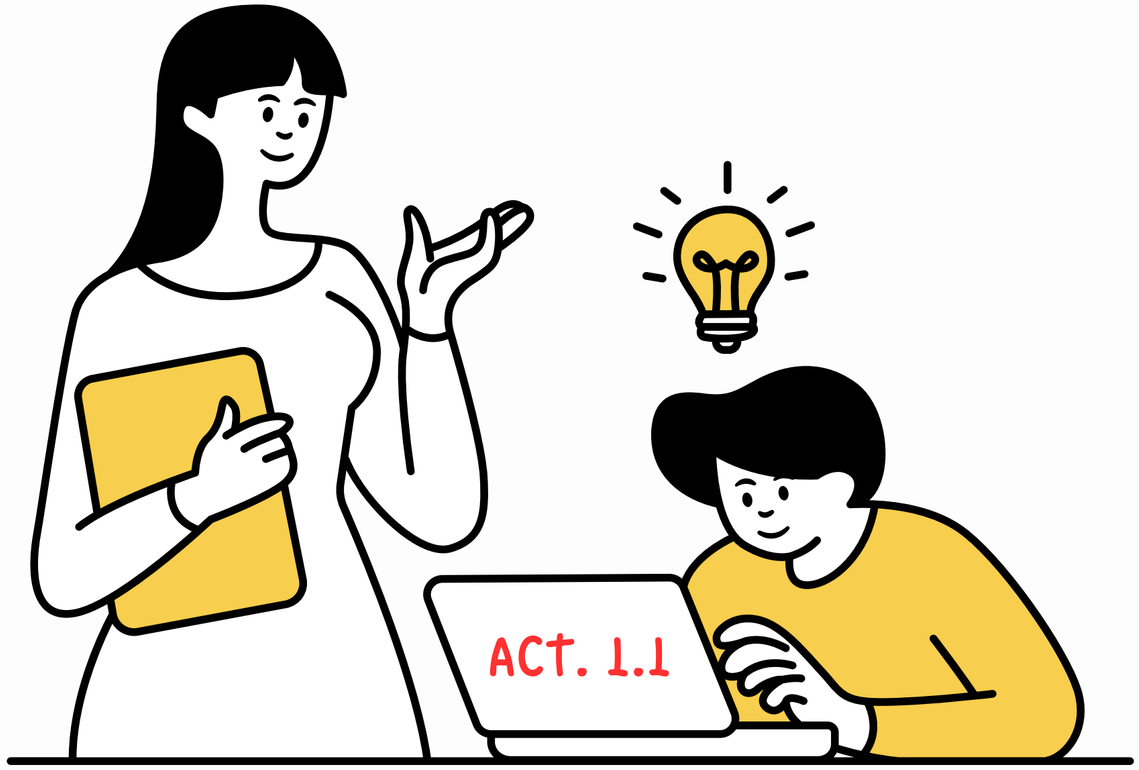
UNIVERSIDAD AUTONOMA DE CHIAPAS




# CONCEPTOS DE VULNERABILIDAD

*Alumna:* **Paola Culebro López**

**Docente: Dr. Luis Gutiérrez Alfaro**

**Análisis de Vulnerabilidades**

**LIDTS 7M**

**14/08/2023**

# HERRAMIENTAS DE VULNERABILIDADES

Estas son herramientas diseñadas para descubrir debilidades en sistemas y redes, ayudando a identificar posibles puntos de entrada para ataques maliciosos.

## NMAP

Es una herramienta de escaneo de red que te permite descubrir qué dispositivos están conectados a una red y qué puertos están abiertos en esos dispositivos. Es como un mapa de la red que muestra los lugares donde podrían existir vulnerabilidades.

## JOOMSCAN

Se utiliza para analizar sitios web basados en Joomla, un sistema de gestión de contenido. Identifica posibles vulnerabilidades específicas de Joomla, lo que es útil para proteger un sitio web contra ataques.

## WPSCAN

Esta herramienta está enfocada en WordPress (plataforma de sitios web). Busca vulnerabilidades en sitios web basados en WordPress, incluyendo plugins y temas, para garantizar que estén protegidos contra amenazas.

## NESSUS ESSENTIALS

Nessus es un escáner de vulnerabilidades que verifica los sistemas en busca de debilidades conocidas. La versión Essentials es gratuita y es como un inspector que busca puertas y ventanas mal cerradas en tu sistema.

## VEGA

Es una herramienta para probar la seguridad de aplicaciones web. Analiza las aplicaciones en busca de posibles problemas y vulnerabilidades, permitiéndonos corregirlos antes de que sean aprovechados por atacantes.

# INTELIGENCIA MISCELÁNEO

Estas estrategias se utilizan para recopilar información útil sobre sistemas y personas, que luego se puede utilizar para tomar decisiones informadas.

## GOBUSTER

Es una herramienta que busca archivos y directorios ocultos en sitios web. Como un explorador digital, ayuda a encontrar información que podría no ser visible en la superficie.

## DUMPSTER DIVING

Se refiere a buscar información valiosa en la basura, ya sea física o digital. En el contexto digital, significa encontrar datos útiles en archivos descartados o información desestimada.

## INGENIERÍA SOCIAL

Es el arte de manipular a las personas para obtener información. Esto puede incluir hacer preguntas o usar tácticas persuasivas para obtener datos confidenciales o acceso a sistemas.

# INTELIGENCIA ACTIVA

Estas estrategias implican explorar y mapear sistemas y redes para comprender su funcionamiento y potenciales vulnerabilidades.

## ANÁLISIS DE DISPOSITIVOS Y PUERTOS CON NMAP

Nmap examina los dispositivos en una red y los puertos abiertos en esos dispositivos. Proporciona una visión completa de cómo está estructurada una red y qué servicios están disponibles.

## PARÁMETROS OPCIONES DE ESCANEO DE NMAP

Nmap tiene opciones que nos permite personalizar el proceso de escaneo, como elegir la velocidad del escaneo, la agresividad y otros factores que pueden influir en los resultados.

## FULL TCP SCAN

Es un tipo de escaneo exhaustivo que analiza todos los puertos TCP en un dispositivo. Puede ser más lento pero revela información detallada sobre los servicios disponibles.

## STEALTH SCAN

También conocido como escaneo sigiloso o furtivo, este enfoque busca minimizar la detección mientras se escanea una red. Es útil para investigaciones más discretas.

## FINGERPRINTING

Se trata de recopilar detalles sobre un sistema, como su sistema operativo y versión de software. Esto puede ayudar a los atacantes a encontrar vulnerabilidades específicas.

## ZENMAP

Es una interfaz gráfica para Nmap que facilita la visualización de los resultados del escaneo. Te muestra gráficos y detalles para entender mejor lo que ha encontrado Nmap.

## ANÁLISIS TRACEROUTE

Esta técnica se utiliza para rastrear la ruta que los paquetes de datos siguen a través de una red, desde tu dispositivo hasta el destino. Esto puede ayudarte a entender cómo funciona la red y a identificar posibles cuellos de botella o problemas.