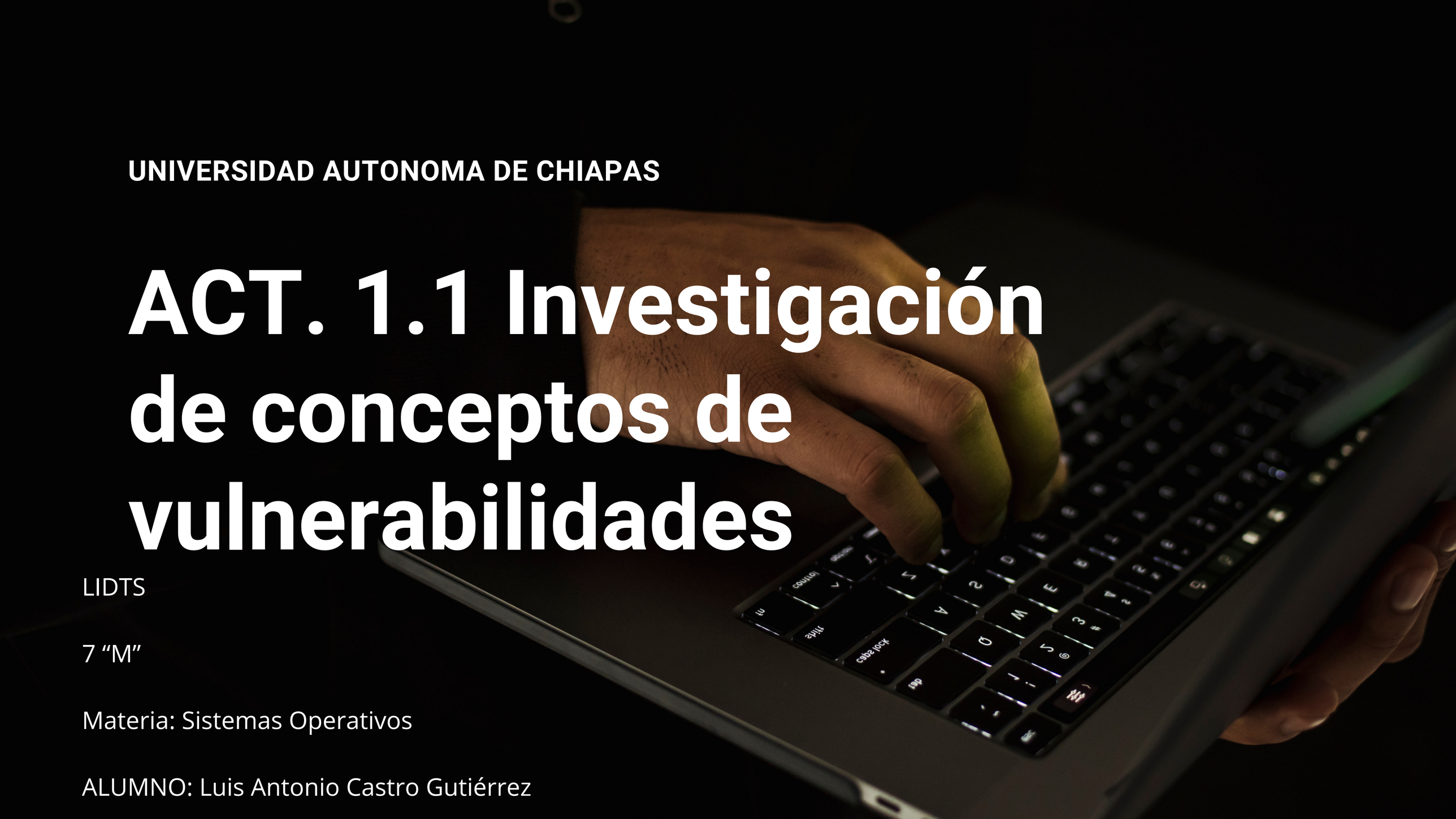

UNIVERSIDAD AUTONOMA DE CHIAPAS

ACT. 1.1 Investigación de conceptos de vulnerabilidades

LIDTS

7 “M”

Materia: Sistemas Operativos

ALUMNO: Luis Antonio Castro Gutiérrez

¿QUÉ SON?

Herramientas de vulnerabilidades

Las herramientas de vulnerabilidades, o escáneres de vulnerabilidades, son programas cruciales en ciberseguridad. Su función principal es identificar y analizar posibles debilidades en sistemas informáticos, redes o aplicaciones. Estas herramientas son esenciales para que los expertos en seguridad puedan detectar y corregir fallos antes de que puedan ser aprovechados por personas con intenciones maliciosas.

Algunas herramientas:

- Nmap
- Joomscan
- Wpscan
- Nessus Essentials
- Vega

Nmap

Nmap es una herramienta fundamental para escanear puertos y descubrir hosts en una red. Ofrece la capacidad de obtener información detallada sobre los equipos, identificando qué hosts están activos, verificando la apertura de puertos y determinando si hay filtros de firewall activados. Además, Nmap puede proporcionar detalles sobre el sistema operativo utilizado por un objetivo específico.

Joomscan

JoomScan es una herramienta de código abierto que detecta vulnerabilidades en Joomla, un CMS popular. Puede identificar más de 550 tipos de vulnerabilidades y ofrece funciones como la enumeración de componentes, la configuración de cookies, la simulación de agentes de usuario y la configuración de tiempos de espera. También permite el uso de un proxy para las conexiones. Genera informes en formatos de texto y HTML y está incluido en las distribuciones de Kali Linux.

Wpscan

WPScan es una herramienta de seguridad de código abierto específicamente creada para WordPress. Su función principal es realizar análisis de vulnerabilidades en sitios web basados en WordPress. Esta herramienta tiene la capacidad de identificar problemas de seguridad no solo en el núcleo de WordPress, sino también en los plugins y temas asociados.

Algunas de las características de WPScan incluyen2:

- Detección de vulnerabilidades en el núcleo de WordPress, plugins y temas.
- Enumeración de usuarios de WordPress.
- Detección de configuraciones de seguridad débiles.

Nessus Essentials

Nessus Essentials es una versión de la herramienta de escaneo de vulnerabilidades Nessus, desarrollada por Tenable. Ofrece la capacidad de escanear hasta 16 direcciones IP por escáner, proporcionando evaluaciones rápidas y exhaustivas, así como la comodidad de un escaneo sin agente. Esta versión es adecuada para uso educativo y para analizar la red doméstica personal. Además, Nessus Essentials ofrece un curso bajo demanda que permite a los estudiantes aprender a utilizar eficazmente la solución de evaluación de vulnerabilidades de Nessus.

Vega

Vega es una herramienta de código abierto que evalúa la seguridad de sitios web y aplicaciones, detectando y validando vulnerabilidades como inyecciones SQL, Cross-Site Scripting (XSS), Shell Injection, entre otras. Ofrece dos modos: proxy para interceptar peticiones, y escáner para detectar vulnerabilidades, proporcionando un examen recursivo y configurable de la estructura del sitio. Vega tiene una interfaz gráfica de usuario intuitiva, es compatible con varias plataformas y viene preinstalado en Kali Linux.

Inteligencia Misceláneo

LA TECNOLOGÍA INTERACTIVA EMPODERA A LOS EDUCADORES

Beneficios para los maestros

Gobuster

Herramienta de código abierto para identificar contenido web como directorios o archivos accesibles u ocultos en un portal web.
Realiza solicitudes HTTP con un diccionario o por fuerza bruta.
Útil para realizar fuerza bruta a URIs (directorios y archivos), subdominios DNS (con soporte de comodines) y nombres de hosts virtuales en servidores web.

Dumpster Diving

Dumpster Diving:

Técnica de ciberseguridad que implica investigar la basura de una persona u organización.
Busca obtener información que pueda utilizarse para atacar una red informática.

Ingeniería Social

Técnica de manipulación que aprovecha el error humano para obtener información privada o acceso a sistemas valiosos.
En el delito cibernético, estas estafas de hackeo " buscan que los usuarios expongan datos, propaguen malware o proporcionen acceso a sistemas restringidos.

Inteligencia Activa

Análisis de dispositivos y puertos con Nmap

Nmap es una herramienta de código abierto que permite analizar dispositivos y puertos en una red. Identifica dispositivos activos y puertos abiertos, y ofrece varios tipos de escaneos, incluyendo Ping/Arp, TCP Connect y FIN. Además, puede detectar servicios, proporcionar detalles de aplicaciones y versiones, realizar auditorías de seguridad y detectar sistemas operativos. Su utilidad se extiende desde redes domésticas hasta grandes redes con múltiples dispositivos y subredes, facilitando el control efectivo y la detección de accesos no autorizados.

Parametros opciones de escaneo de nmap

- -p: Permite especificar el rango de puertos a escanear. Por ejemplo, -p 1-100 escaneará los puertos del 1 al 100.
-
- -sS (TCP SYN scan): Este parámetro realiza un escaneo de tipo SYN, que es más discreto y rápido, pero puede ser detectado por algunos firewalls.
-
- -sT (TCP Connect scan): Realiza un escaneo de tipo Connect, estableciendo una conexión completa con cada puerto. Es más confiable pero menos sigiloso que el escaneo SYN.
-
- -sU (UDP scan): Escanea puertos UDP, utilizados por algunos servicios menos comunes.

Full TCP scan

El Full TCP scan, también llamado TCP Connect scan, es un tipo de escaneo en Nmap que realiza la conexión completa utilizando el proceso de 3-Way-Handshake en el protocolo TCP. Este escaneo, que es intrusivo, lleva a cabo un análisis exhaustivo al completar el handshake, enviando paquetes en las tres direcciones: SYN (del emisor al receptor), SYN-ACK (del receptor al emisor) y ACK (del emisor al receptor).

Stelth Scan

El Stealth Scan, también conocido como SYN scan, es un tipo de escaneo en Nmap que se utiliza para evaluar la seguridad de una red1. Este método de escaneo es más sigiloso que el Full TCP scan, ya que no completa el 3-Way-Handshake que se utiliza en una conexión normal TCP1.

En un Stealth Scan, se envía un paquete SYN al host objetivo como parte del inicio del 3-Way-Handshake. Si el puerto está abierto, el host objetivo responderá con un paquete SYN-ACK. En lugar de responder con un paquete ACK para completar el handshake (como se haría en una conexión TCP normal), el escáner envía un paquete RST para cerrar la conexión antes de que se complete1. Esto hace que el Stealth Scan sea menos probable de ser detectado por los sistemas de detección de intrusiones que el Full TCP scan1.

Fingerprintig

El Fingerprinting, también llamado huella digital del dispositivo, es una técnica que recopila información sistemática para identificar y singularizar un dispositivo. Esta información abarca detalles sobre el sistema operativo, navegador, aplicaciones instaladas y configuración del dispositivo.

El Fingerprinting se emplea para varios propósitos:

- Seguimiento de la actividad del usuario: Facilita el seguimiento de las actividades del usuario en la red al identificar de manera única un dispositivo.
- Perfilado del usuario: La información recopilada se utiliza para crear perfiles de usuarios, especialmente beneficioso en áreas como el marketing.
- Seguridad y prevención de fraudes: Contribuye a detectar actividades sospechosas o fraudulentas en Internet, mejorando la seguridad en línea.

Zenmap

Zenmap es la interfaz gráfica oficial de Nmap, diseñada para ofrecer una experiencia práctica, clara y organizada al utilizar el programa. Es ideal tanto para expertos como para principiantes, facilitando la ejecución de escaneos de puertos de manera visual y cómoda. Al igual que Nmap, Zenmap permite realizar escaneos múltiples y dirigidos a puertos específicos.

Análisis traceroute

El análisis Traceroute, o Tracert en Windows, es una herramienta de diagnóstico que determina la ruta de un paquete de datos desde su origen hasta su destino en una red. Este proceso implica enviar paquetes al destino y registrar los saltos que hacen a medida que atraviesan la red.

El análisis Traceroute ofrece información valiosa, incluyendo:

- Ruta del paquete: Revela la ruta exacta que sigue un paquete de datos desde el origen hasta el destino.
- Nombres de elementos intermedios: Identifica cada salto o nodo, como routers o switches, en la ruta del paquete.
- Latencia entre el origen y los puntos intermedios: Mide el tiempo que tarda un paquete en llegar a cada punto intermedio, permitiendo identificar posibles cuellos de botella en la red.

Referencia bibliográfica

- Espinosa, O. (2023, 30 noviembre). En qué consiste el comando Tracert o Traceroute. RedesZone. https://www.redeszone.net/tutoriales/internet/que-es-comando-tracert-traceroute/
- ¿Qué es el fingerprinting o la huella digital de nuestros dispositivos? (s. f.). LISA Institute. https://www.lisainstitute.com/blogs/blog/que-es-el-fingerprinting-huella-digital-de-nuestros-dispositivos
- ¿Qué es un escaneo de conexión TCP? (s. f.). helpr. https://es.helpr.me/16691-what-is-a-tcp-connect-scan
- BlackeyeB. (2023, 27 abril). Qué es NMAP y cómo usarlo: un tutorial para la mejor herramienta de escaneo de todos los tiempos. freeCodeCamp.org. https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/