UNIVERSIDAD AUTONOMA DE CHIAPAS
FACULTAD DE CONTADURIA Y ADMINISTRACIÓN
CAMPUS 1

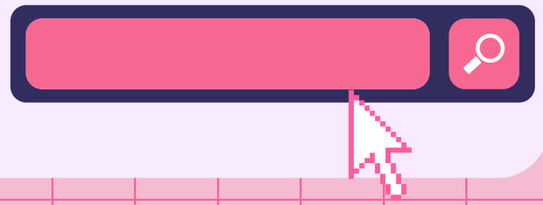
Nombre del alumno:
Gabriela Juárez Trujillo

Grado y Grupo:
7°M

Matricula:
A201083

Nombre de la materia:
Analisis De Vulnerabilidades

Nombre del docente:
Dr. Luis Gutiérrez Alfaro



Tuxtla Gutiérrez, Chiapas a 14 de Agosto del 2023

Herramientas de vulnerabilidades:

Nmap

Es una herramienta con las líneas de comando de Linux de código abierto, es utilizado para es canear las direcciones ip y los puertos, también funciona para detectar aplicaciones instaladas. Este permite a los administradores localizar los dispositivos que están en ejecución en su red, descubrir los puertos, servicios abiertos y detectar vulnerabilidades. Nmap también es conocida como una herramienta que facilita el mapeo de una red completa, ayudando a encontrar sus puertos y sus servicios abiertos.

Joomscan

Conocida como una herramienta de código abierto, destacando como una de las mas populares al momento de ayudar a localizar vulnerabilidades conocidas de Joomla core, componentes e inyección sql y ejecución de comandos. Esta herramienta no solo detecta vulnerabilidades ofensivas ya conocidas, también tiene la capacidad de detectar muchas configuraciones erróneas y deficiencias a nivel de administrador, los cuales se pueden usar para comprometer el sistema.

Wpscan

Es un software que contiene un código abierto para Kali Linux, fue diseñado para escanear vulnerabilidades y fallos en un sitio web de WordPress. Wpscan es una herramienta muy poderosa y capaz de dar la información detallada sobre una página web. Con ella se puede examinar sistemas, verificar su estado y corregir cada fallo que hay antes de que sea detectado para usarse en contra de la seguridad del sistema.

Nessus Essentials

Es una herramienta utilizada principalmente para escanear vulnerabilidades, utilizado para identificar y evaluar riesgos en los sistemas informáticos y redes, lo que ayuda a proteger los activos digitales. También puede realizar pruebas para encontrar fallos de seguridad pública, es compatible con cualquier host.

Vega

Es un escáner de seguridad web, de código abierto y también es una plataforma en la cual se puede probar la seguridad de las aplicaciones web. Vega puede encontrar vulnerabilidades tales como: secuencias de comandos entre sitios reflejadas, secuencias de comandos entre sitios almacenadas, inyección ciega de SQL, inclusión remota de archivos, inyección de shell y otras. Vega también investiga la configuración de seguridad de TLS/SSL e identifica oportunidades para mejorar la seguridad de sus servidores TLS.

Inteligencia Misceláneo:

Gobuster

Gobuster es una herramienta que se utiliza para la fuerza bruta: URI (directorios y archivos) en sitios web, subdominios DNS (con compatibilidad con comodines), nombres de host virtual en servidores web de destino, cubos abiertos de Amazon S3, cubos abiertos de Google Cloud y servidores TFTP.
Gobuster es útil para pentesters, hackers éticos y expertos forenses. También se puede utilizar para pruebas de seguridad.

Dumpster Diving

es el proceso de buscar basura para obtener información útil sobre una persona o empresa que luego se puede utilizar con el propósito de piratear.
Este ataque está dirigido principalmente a grandes organizaciones o negocios para llevar a cabo phishing mediante el envío de correos electrónicos falsos a las víctimas que parecen provenir de una fuente legítima. La información obtenida al comprometer la confidencialidad de la víctima se utiliza para fraudes de identidad.

Ingeniería Social

Es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.

Inteligencia Activa:

Análisis de dispositivos y puertos con Nmap

Nmap es la mejor herramienta de escaneo de puertos y descubrimiento de hosts que existe actualmente. Nmap nos permitirá obtener una gran cantidad de información sobre los equipos de nuestra red, es capaz de escanear qué hosts están levantados, e incluso comprobar si tienen algún puerto abierto, si están filtrando los puertos (tienen un firewall activado), e incluso saber qué sistema operativo está utilizando un determinado objetivo.

Parametros opciones de escaneo de nmap

-Seleccionar objetivos: Direcciones o rangos IP, nombres de sistemas, redes, etc.
-Descubrir sistemas.
-Técnicas de análisis de puertos.
-Puertos a analizar y orden de análisis.
-Duración y ejecución:
-Detección de servicios y versiones.
-Evasión de Firewalls/IDS.

Full TCP scan

es una técnica utilizada en seguridad informática y pruebas de penetración para identificar puertos abiertos en un sistema o red. En un escaneo TCP, se envían paquetes de solicitud a los puertos del destino y se observa la respuesta del sistema objetivo. Esto permite determinar qué puertos están abiertos y son susceptibles de recibir conexiones.

Stelth Scan

es una técnica de exploración utilizada en seguridad informática y pruebas de penetración para identificar puertos abiertos en un sistema o red de una manera más sigilosa y discreta, con el objetivo de evitar la detección por parte de sistemas de seguridad o firewalls. Esta técnica busca minimizar las huellas que deja en la red, el objetivo de un Stealth Scan es recopilar información sobre los puertos abiertos en un sistema o red sin alertar a los mecanismos de seguridad del objetivo

Fingerprintig

es una técnica utilizada en seguridad Esta técnica consiste en recolectar información directamente de los sistemas informáticos de una persona o empresa para conocer más sobre su comportamiento y configuración. Los datos obtenidos permiten determinar de manera inequívoca el dispositivo empleado y, de esta forma, poder llegar a perfilar y conocer la actividad del usuario, ya sea una persona física o jurídica.

Zenmap

es una herramienta gratuita utilizada para escanear los puertos. Con ella se puede saber cuáles son los que estan abiertos, para evitar problemas a la hora de usar algunos programas o acceder a un servidor. Se trata de la interfaz gráfica del popular programa de código abierto Nmap, que permite hacer un escaneo de puertos completo de cualquier equipo conectado.

Análisis traceroute

es una herramienta y técnica utilizada para determinar la ruta tomada por los paquetes de datos desde un punto de origen hasta un destino en una red. El objetivo principal de realizar un análisis de traceroute es identificar los saltos intermedios que los paquetes hacen a través de diferentes nodos y routers en la red, así como medir los tiempos de respuesta (latencia) en cada uno de estos saltos.