Universidad Autónoma de Chiapas
Facultad de contaduría y administración C-I

Carrera:
Lic. En ing en desarrollo y tecnologías de software.

Materia:
Análisis de vulnerabilidades.

Catedrático:
Mtro. Luis Gutiérrez Alfaro.

Nombre del alumno:
González Aguilar Eduardo - A211154

Semestre: 7. **Grupo:** M.

Nombre de la actividad:
Investigar los conceptos de vulnerabilidades.

Fecha de entrega:
26/01/2024.

Herramientas de vulnerabilidades.

nmap:

Nmap es una herramienta de código abierto que se utiliza para analizar redes y escanear puertos. Es una de las herramientas más populares en el mundo de la Ciberseguridad debido a su facilidad de uso y su capacidad para identificar vulnerabilidades en los sistemas.

Joomscan:

JoomScan es una herramienta de escaneo de vulnerabilidades para sitios web creados con Joomla. Esta herramienta de código abierto está escrita en Perl y es capaz de detectar más de 550 vulnerabilidades, como inyecciones de SQL, inclusiones de archivos, defectos de RFI, BIA, defectos XSS, inyección ciega de SQL, protección de directorios y otros.

Wpsscan:

WPScan es una herramienta de escaneo de vulnerabilidades para sitios web creados con WordPress. Esta herramienta de código abierto es capaz de detectar más de **18,000** vulnerabilidades, como inyecciones de SQL, inclusiones de archivos, defectos de RFI, BIA, defectos XSS, inyección ciega de SQL, protección de directorios y otros

Nessus Essentials:

Esta herramienta te permite escanear tu entorno con la misma velocidad y profundidad que los suscriptores de Nessus, pero no admite comprobaciones de cumplimiento, resultados en vivo ni el uso del dispositivo virtual Nessus. Puedes escanear hasta **16 direcciones IP por escáner** con Nessus Essentials

Vega:

Vega es una herramienta de escaneo de vulnerabilidades para sitios web. Es una herramienta de código abierto que se utiliza para encontrar y solucionar vulnerabilidades en aplicaciones web. Vega es capaz de detectar vulnerabilidades como **injection points**, **reflected cross-site scripting**, **stored cross-site scripting**, **blind SQL injection**, **remote file include**, **shell injection**, y otros. Vega también sondea la configuración de seguridad TLS/SSL y detecta oportunidades para mejorar la seguridad de los servidores TLS. Vega incluye un escáner automatizado para pruebas rápidas y un proxy de interceptación para inspección táctica. Vega es una herramienta escrita en Java, basada en GUI y se ejecuta en Linux, OS X y Windows.

Inteligencia misceláneo.

Gobuster:

Gobuster es una herramienta de escaneo agresiva que ayuda a encontrar directorios ocultos, subdominios y buckets S3. Es una herramienta de fuerza bruta rápida para descubrir URLs, archivos y directorios ocultos dentro de sitios web. Los desarrolladores web a menudo exponen archivos sensibles, rutas de URL o incluso subdominios mientras construyen o mantienen un sitio. Esto es un gran vector de ataque para actores malintencionados. Gobuster ayuda a encontrar vectores de ataque y podemos usarlo para defendernos.

Dumbster Diving:

El término “dumpster diving” en ciberseguridad se refiere a la práctica de investigar la basura de una persona u organización para encontrar información que pueda ser utilizada para atacar una red informática . Los ciberdelincuentes pueden obtener información sensible a través de la basura de una persona, como códigos de acceso y contraseñas, números de teléfono, correos electrónicos y direcciones domiciliarias de clientes, socios comerciales, proveedores y familiares, diseños de productos, planos y borradores de planes de negocio, números de tarjetas de crédito y cuentas bancarias del personal y clientes comerciales, CD, DVD, USB y otros dispositivos de almacenamiento portátiles.

ingeniería social:

La **ingeniería social** es el arte de manipular a las personas para que realicen acciones que violen los protocolos de seguridad. Esta técnica se utiliza en ciberseguridad para obtener información sensible a través de la manipulación de las personas, como contraseñas, números de teléfono, correos electrónicos y direcciones domiciliarias de clientes, socios comerciales, proveedores y familiares, entre otros. La ingeniería social se basa en la explotación de aspectos de la interacción humana y de la toma de decisiones, y esto se conoce como sesgo cognitivo.

Inteligencia Activa.

Análisis de dispositivos y puertos con Nmap:

Nmap es una herramienta de escaneo de puertos y descubrimiento de hosts que se utiliza para obtener información sobre los equipos de una red. Con Nmap, puedes escanear qué hosts están levantados, 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

- **nmap -sP 192.168.1.0/24**: Escanea todos los dispositivos en la red 192.168.1.0/24 y muestra los dispositivos que están activos.
- **nmap -sS 192.168.1.1**: Escanea el dispositivo 192.168.1.1 y muestra los puertos abiertos.
- **nmap -O 192.168.1.1**: Escanea el dispositivo 192.168.1.1 y muestra el sistema operativo que está utilizando.

Parametros opciones de escaneo de nmap:

- **-sT** para realizar un escaneo de conexión TCP, que establece una conexión completa con cada puerto abierto.
- -**sS** para realizar un escaneo SYN, que envía un paquete SYN a cada puerto y espera una respuesta SYN/ACK o RST. Este tipo de escaneo es más rápido y furtivo que el anterior, pero requiere privilegios de administrador.
- **-sU** para realizar un escaneo UDP, que envía un paquete UDP a cada puerto y espera una respuesta ICMP o UDP. Este tipo de escaneo es útil para detectar servicios que usan el protocolo UDP, como DNS o SNMP, pero suele ser más lento y menos confiable que los escaneos TCP.
- **-p** para especificar el rango o la lista de puertos que quieres escanear. Por ejemplo, -p 1-1024 escanea los primeros 1024 puertos, y -p 22,80,443 escanea solo los puertos 22, 80 y 443.
- **-F** para realizar un escaneo rápido, que solo escanea los 100 puertos más comunes según el archivo nmap-services.
- **-A** para realizar un escaneo agresivo, que incluye la detección de servicios, versiones, sistemas operativos, scripts y traceroute. Este tipo de escaneo es muy completo, pero también puede ser más ruidoso y lento que otros.
- **-v** para aumentar el nivel de verbosidad, que te muestra más información sobre el progreso y los resultados del escaneo. Puedes usar varios -v para incrementar el nivel de detalle, o -vvv para el máximo nivel.
- **-o** para guardar los resultados del escaneo en un archivo con un formato específico. Por ejemplo, -oN guarda los resultados en formato normal, -oX en formato XML, -oG en formato grepable, y -oA en todos los formatos anteriores.

Full TCP scan:

Este tipo de escaneo es el más común y completo. Escanea todos los puertos TCP en un dispositivo.

Stelth Scan:

Este tipo de escaneo es más silencioso que el Full TCP scan. Escanea los puertos sin dejar rastro en los registros del dispositivo.

Fingerprintig:

Esta técnica se utiliza para identificar el sistema operativo y las aplicaciones que se ejecutan en un dispositivo.

Zenmap:

Es una interfaz gráfica de usuario para Nmap que permite a los usuarios visualizar los resultados de los escaneos de Nmap.

Análisis traceroute:

Esta técnica se utiliza para identificar la ruta que sigue un paquete de datos desde su origen hasta su destino.