Act. 1.1 Investigar los conceptos de vulnerabilidades.

Mayra Elizabeth Moreno Velasquez - A200182.
Luis Gutierrez Alfaro.

Herramientas de vulnerabilidades.

nmap

Nmap es la abreviatura de Network Mapper. Es una herramienta de línea de comandos de Linux de código abierto que se utiliza para escanear direcciones IP y puertos en una red y para detectar aplicaciones instaladas.

Joopscan

Joomscan es un escáner de vulnerabilidades en la red utilizado para detectar la ejecución de comandos, inyección SQL y otros ataques contra aplicaciones web.

Wpscan

WPScan es un programa muy potente integrado en Kali Linux que nos permite comprobar las vulnerabilidades de nuestra página WordPress, analizando los plugins, themes...También es capaz de realizar ataques de fuerza bruta para verificar la robustez de las contraseñas de los usuarios, de este modo si la contraseña ha conseguido ser descifrada sería conveniente cambiarla por una mas segura.

Nessus Essentials

Nessus es un escáner de vulnerabilidades de red, es decir, una herramienta de seguridad que busca debilidades en los sistemas informáticos y redes. Fue creado por Renaud Deraison en 1998 y es una de las soluciones de seguridad más populares y utilizadas en todo el mundo.

Vega

Vega es una herramienta gráfica de auditoría web gratuita y de código abierto.
Esta herramienta realiza diversas funciones tales como:

- Análisis de Vulnerabilidades
- Crawler (copia del sitio web)
- Análisis de contenido
- Modificación manual de paquete HTTP (proxy)

Inteligencia Misceláneo:

Gobuster

Gobuster es una herramienta que se utiliza para forzar URI de fuerza bruta, incluidos directorios y archivos, así como subdominios DNS.

Dumpster Diving

El Dumpster diving (buceo en el contenedor) en informática se refiere a la exploración de la papelera de un sistema con el fin de encontrar detalles para que un pirata informático pueda realizar un ciberataque. El primer paso para realizar un ataque a un servicio de redes sociales es bucear en el contenedor.

Ingeniería Social

La ingeniería social es una técnica de manipulación que aprovecha el error humano para obtener información privada, acceso a sistemas u objetos de valor. En el caso del delito cibernético, estas estafas de "hackeo de humanos" tienden a hacer que los usuarios desprevenidos expongan datos, propaguen infecciones de malware o den acceso a sistemas restringidos. Los ataques pueden ocurrir en línea, en persona y a través de otras interacciones.

Inteligencia Activa

Análisis de dispositivos y puertos con Nmap

Nmap comenzó como un analizador de puertos eficiente, aunque ha aumentado su funcionalidad a través de los años, aquella sigue siendo su función primaria. La sencilla orden nmap <objetivo> analiza más de 1660 puertos TCP del equipo <objetivo>. Aunque muchos analizadores de puertos han agrupado tradicionalmente los puertos en dos estados: abierto o cerrado, Nmap es mucho más descriptivo. Se dividen a los puertos en seis estados distintos: abierto, cerrado, filtrado, no filtrado, abierto|filtrado, o cerrado|filtrado.

Análisis traceroute

Se trata de un comando que se ejecuta directamente en la consola del sistema operativo, y sirve para encontrar y diagnosticar problemas que pueda haber en tu red doméstica o empresarial, o en tu conexión con Internet.

Full TCP scan

La exploración de conexión TCP es el tipo de exploración TCP predeterminado cuando la exploración SYN no es una opción. Este es el caso cuando un usuario no tiene privilegios de paquetes sin procesar o está escaneando redes IPv6. En lugar de escribir paquetes sin procesar como lo hacen la mayoría de los otros tipos de escaneo, Nmap le pide al sistema operativo subyacente que establezca una conexión con la máquina y el puerto de destino mediante la emisión de la connectllamada al sistema.

Stelth Scan

El escaneo SYN es la opción de escaneo predeterminada y más popular por una buena razón. Se puede realizar rápidamente, escaneando miles de puertos por segundo en una red rápida que no se ve obstaculizada por firewalls intrusivos.

Fingerprintig

El fingerprinting o huellas digitales son las pequeñas crestas, espirales y patrones de valle en la punta de cada dedo. Se forman por la presión sobre los dedos pequeños y en desarrollo del bebé en el útero. No se ha encontrado que dos personas tengan las mismas huellas digitales, son totalmente únicas.

Zenmap

Zenmap es la GUI oficial de Nmap Security Scanner. Es una aplicación gratuita y de código abierto multiplataforma

Bibliografia:

- https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/
- https://noticiasseguridad.com/tutoriales/joomscan-escaneo-de-sitios-web-en-joomla/
- https://nosololinux.es/auditar-seguridad-de-tu-wordpress-con-wpscan/
- https://ciberseguridad.club/que-es-nessus-y-como-utilizarlo/
- https://academy.seguridadcero.com.pe/blog/escaneo-vulnerabilidades-web-vega
- https://www.kali.org/tools/gobuster/
- https://ciberseguridad.com/amenzas/dumpster-diving/
- https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering
- https://www.xataka.com/basics/tracert-traceroute-que-como-funciona-como-se-utiliza