conceptos de vulnerabilidades

JOSE EDUARDO ZARATE AVALOS

15/08/2023

7M

Herramientas de vulnerabilidades

Son aquellas utilidades que sirven para identificar posibles riesgos dentro de una organización, aplicación móvil o aplicación web, que los hackers pueden explotar para obtener información valiosa de tus clientes o de tu empresa.

Nmap:

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.

Joomscan:

es una de las herramientas de código abierto más populares para ayudarlo a encontrar vulnerabilidades conocidas de Joomla Core, Componentes e Inyección SQL, ejecución de comandos.

Wpscan:

es una herramienta muy poderosa y capaz de darte información detallada sobre una página web.

Nessus Essentials:

permite escanear la red doméstica personal con la misma alta velocidad, evaluaciones a profundidad o buscar vulnerabilidades de forma automatizada.

Vega:

es una herramienta que permite realizar escaneos proactivos y además tiene -como no podría ser de otra forma- un proxy para interceptar y modificar peticiones.

Inteligencia Misceláneo

Son para guardar información que sirven para el sistema y las personas.

Gobuster:

es una herramienta utilizada para realizar fuerza bruta a: URIs (directorios y archivos) en sitios web, subdominios DNS (con soporte de comodines), y nombres de hosts virtuales en los servidores web.

Dumpster Diving:

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.

Ingeniería Social:

s 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

Permite que la información más actualizada esté disponible en el momento más importante: ahora. Ya sea impulsando métricas y conocimientos automatizados en los cuadros de mando o integrándolos directamente en procesos automáticos, la inteligencia activa combina datos en reposo con datos en movimiento, por lo que refleja el pulso de los datos y proporciona conocimientos en cada oportunidad estratégica de negocio.

Análisis de dispositivos y puertos con 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:

se utiliza para descubrir hosts y servicios de una red informática, creando así una especie de mapa de red.

Full TCP scan:

Es una técnica de exploración de puertos que consiste en enviar un paquete FIN a un puerto determinado, con lo cual deberíamos recibir un paquete de reset (RST) si dicho puerto esta cerrado.

Stelth Scan:

Es muy útil para conocer que hosts se encuentran activos sin que seamos detectados.

Fingerprintig:

Da información sistemática que dejamos sobre un dispositivo informático cada vez que lo utilizamos.

Zenmap:

proporcionar mapeos de red visuales, Zenmap también te permite guardar y buscar tus escaneos para uso futuro.

Análisis traceroute:

se ejecuta en la consola de símbolo de sistema en los sistemas operativos Windows. Gracias a este comando, podremos seguir la pista a los paquetes que vienen desde un host.

Cuando ejecutamos el comando "Tracert" obtenemos una estadística de la latencia de red de esos paquetes, lo que es una estimación de la distancia (en saltos) a la que están los extremos de la comunicación.