CONCEPTOS DE VULNERABILIDAD

LUIS EDUARDO GONZALEZ GUILLEN

¿Que es una vulnerabilidad?

Una vulnerabilidad en el ámbito de las redes informáticas se refiere a una debilidad en un sistema o red que puede ser explotada por un atacante. Esta explotación puede permitir al atacante realizar acciones no autorizadas, como acceder a datos confidenciales, interrumpir servicios o ejecutar código malicioso.

Herramientas de vulnerabilidad

Nmap

Una vulnerabilidad en el ámbito de las redes informáticas se refiere a una debilidad en un sistema o red que puede ser explotada por un atacante. Esta explotación puede permitir al atacante realizar acciones no autorizadas, como acceder a datos confidenciales, interrumpir servicios o ejecutar código malicioso.

nmap se emplea extensamente para realizar escaneos de puertos, identificación de sistemas operativos, ejecución de scripts personalizados y exploración de servicios en una red.

JoomScan

Joomscan se especializa en la identificación de vulnerabilidades específicas en sitios web desarrollados en Joomla, un sistema de gestión decontenidos. La herramienta realiza análisis de seguridad exhaustivos, buscandodebilidades comunes y específicas de este CMS.

Su aplicación principal radica en la detección de vulnerabilidades conocidas en sitios web Joomla a través de escaneos especializados

Wpscan

Wpscan se ha diseñado para evaluar la seguridad de sitios web basados en WordPress. Realiza escaneos minuciosos en busca de vulnerabilidades, configuraciones débiles y otras amenazas potenciales en la plataforma.

Es utilizado habitualmente para identificar y corregir vulnerabilidades en sitios web que utilizan WordPress, así como para llevar a cabo auditorías de seguridad

Nessus Essential

Nessus es una herramienta integral de escaneo de vulnerabilidades que ayuda en la identificación proactiva de amenazas en sistemas informáticos. Nessus Essentials, su versión gratuita, proporciona funcionalidades avanzadas para realizar escaneos de seguridad en redes, sistemas y aplicaciones.

Nessus Essentials se utiliza comúnmente para realizar evaluaciones de seguridad exhaustivas, identificar vulnerabilidades y fortalecer la postura de seguridad de una infraestructura.

Vega

Vega es una herramienta de prueba de seguridad para aplicaciones web que simplifica la identificación y explotación de vulnerabilidades. Ofrece funciones específicas para analizar sitios web en busca de fallos de seguridad, lo que facilitala corrección proactiva de las debilidades identificadas.

Inteligencia Misceláneo

GoBuster

Gobuster, una herramienta de fuerza bruta, se emplea para descubrir directorios y archivos ocultos en servidores web. Durante las fases de enumeración en pruebas de penetración, Gobuster permite identificar recursos no accesibles de manera convencional

Dumpster Diving

Dumpster Diving involucra la búsqueda de información valiosa en desechos físicos de una organización, como documentos impresos o discos duros desechados. Esta práctica puede revelar datos sensibles que podrían haber sido descartados de manera inadecuada.

Ingeniería Social

La ingeniería social implica la manipulación de individuos para obtener información confidencial o realizar acciones específicas. Utiliza tácticas no tecnológicas, como engaños y manipulación psicológica, para explotar aspectos comportamentales y sociales

Inteligencia Activa

Análisis de dispositivos y puertos con nmap: Nmap se utiliza para realizar análisis activos de dispositivos y puertos en una red. Proporciona detalles sobre los servicios en ejecución y los sistemas operativos presentes, facilitando la evaluación de la postura de seguridad

Full TCP Scan: Un escaneo TCP completo con Nmap implica la exploración de todos los 65,535 puertos TCP posibles en un sistema. Este enfoque exhaustivo permite identificar todos los servicios en ejecución, brindando una visión completa de la infraestructura

Inteligencia Activa

Stealth Scan: El "Stealth Scan" en Nmap, conocido también como escaneo sigiloso, busca minimizar la detección al no enviar paquetes que puedan alertar a los sistemas de seguridad. Esta técnica es valiosa en entornos sensibles a la detección de escaneos intrusivos

Fingerprinting: El fingerprinting implica la identificación de servicios y sistemas operativos en una red mediante el análisis de las respuestas de los servicios a paquetes específicos. Esto permite obtener información detallada sobre las configuraciones y versiones de software presentes.

Inteligencia Activa

Zenmap: Zenmap, una interfaz gráfica de usuario para Nmap, simplifica la configuración y ejecución de escaneos de seguridad. Proporciona una representación visual de los resultados, facilitando la interpretación y el análisis de la información recopilada.

Análisis Traceroute: El análisis de traceroute implica rastrear la ruta que sigue un paquete de datos desde el origen hasta el destino. Muestra todos los nodos intermedios (routers) a lo largo del camino, proporcionando una visión detallada de la topología de la red y posibles puntos de congestión o vulnerabilidades