

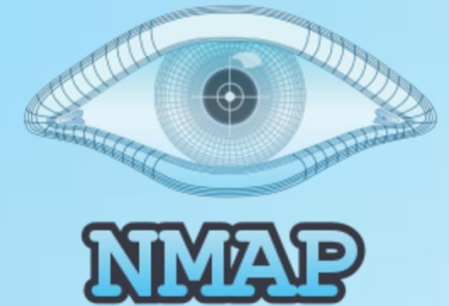
INTELIGENCIA ACTIVA

MARCOS JAVIER CANCINO HERNÁNDEZ - A200353
ANÁLISIS DE VULNERABILIDADES - 7° "N"

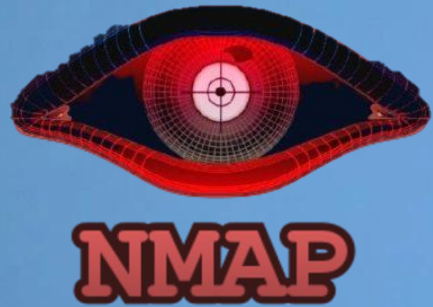


ANALISIS DE DISPOSITIVOS Y PUERTOS CON NMAP

- Nmap (Network Mapper) es una herramienta de escaneo de redes que se utiliza para descubrir dispositivos y servicios en una red. Permite a los profesionales de seguridad identificar dispositivos activos, puertos abiertos y servicios en ejecución. Nmap ofrece una variedad de opciones y parámetros que permiten a los usuarios personalizar los escaneos según sus necesidades.



PARAMETROS Y OPCIONES DE ESCANEO DE NMAP



Nmap ofrece una amplia gama de opciones de escaneo, que incluyen escaneos TCP, UDP, SYN, ACK, entre otros. Los parámetros de Nmap permiten especificar qué tipo de escaneo realizar, el rango de direcciones IP a escanear, los puertos a explorar y más. Algunos de los parámetros comunes incluyen `-sS` para un escaneo SYN (half-open), `-sT` para un escaneo TCP completo, `-sU` para escaneo UDP, y más.

FULL TCP SCAN

Un escaneo TCP completo (Full TCP Scan) en Nmap implica el escaneo de todos los 65,535 puertos TCP posibles en un dispositivo o rango de direcciones IP. Esto proporciona una visión completa de todos los servicios y puertos abiertos en la máquina objetivo, lo que puede ayudar a identificar posibles vulnerabilidades y configuraciones inseguras.



STEALTH SCAN



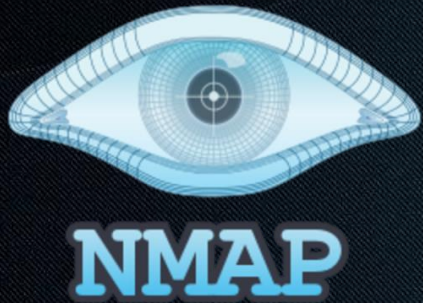
Un "stealth scan" (escaneo sigiloso) en Nmap se refiere a un escaneo en el que se intenta minimizar la detección por parte de sistemas de seguridad, como firewalls y sistemas de detección de intrusiones (IDS). Esto se logra enviando paquetes de escaneo de una manera más discreta, como utilizando escaneos SYN (-sS) en lugar de escaneos TCP completos (-sT).

FINGERPRINTING

El "fingerprinting" (huella digital) en el contexto de Nmap se refiere a la identificación de sistemas operativos, versiones de software y otros detalles sobre un dispositivo o servicio. Nmap puede intentar adivinar esta información analizando las respuestas de los dispositivos a ciertos paquetes de escaneo.



ZENMAP




Zenmap es una interfaz gráfica de usuario (GUI) para Nmap que facilita la configuración y ejecución de escaneos de red. Proporciona una forma más amigable de utilizar las capacidades de Nmap y ofrece una visualización más intuitiva de los resultados del escaneo.

ANÁLISIS TRACEROUTE

El análisis de traceroute implica el uso de herramientas como traceroute o tracert para rastrear la ruta que sigue un paquete desde el origen hasta el destino a través de múltiples saltos de red. Esto puede ayudar a identificar posibles cuellos de botella, retrasos y rutas inusuales en la red.





ESTOS ELEMENTOS Y TÉCNICAS DE INTELIGENCIA ACTIVA SON FUNDAMENTALES PARA LA IDENTIFICACIÓN Y MITIGACIÓN DE POSIBLES VULNERABILIDADES EN SISTEMAS Y REDES. SIN EMBARGO, ES IMPORTANTE UTILIZAR ESTAS HERRAMIENTAS Y TÉCNICAS CON RESPONSABILIDAD Y EN ENTORNOS DONDE TENGAS EL PERMISO ADECUADO PARA LLEVAR A CABO PRUEBAS DE SEGURIDAD.