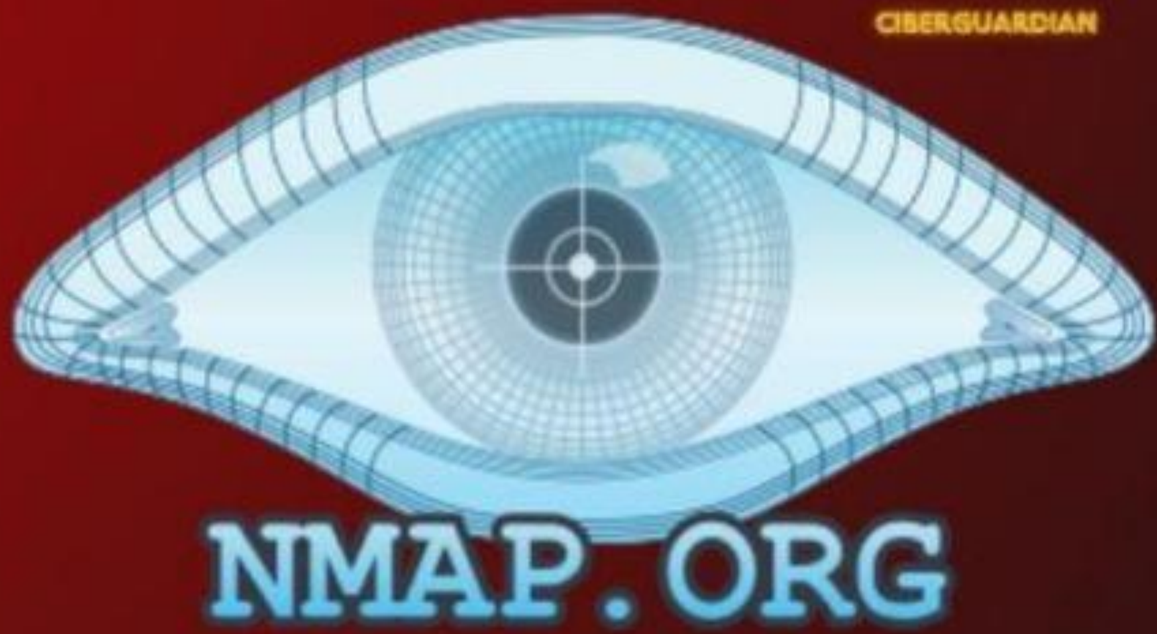
Top comandos

COMANDOS BÁSICOS EN NMAP

CIBERGUARDIAN



Escaneo de puertos específicos:

nmap -p [puerto1],[puerto2] [dirección_IP]

Significado: Escanea puertos específicos en lugar de los predeterminados.

Escaneo de todos los puertos:

nmap -p- [dirección_IP]

Significado: Escanea todos los puertos (1-65535).

Detección de sistema operativo:

nmap -O [dirección_IP]

Significado: Intenta identificar el sistema operativo del host.

Detección de versiones de servicios:

nmap -sV [dirección_IP]

Significado: Detecta las versiones de los servicios en ejecución en

Escaneo con traceroute:

nmap --traceroute [dirección_IP]

Significado: Muestra la ruta que toman los paquetes hasta el destino.

Escaneo de múltiples IPs:

nmap [IP1] [IP2] [IP3]

Significado: Escanea varias direcciones IP a la vez.

Escaneo de un rango de IPs:

nmap [inicio_IP]-[fin_IP]

Significado: Escanea un rango de direcciones IP.

Detectar servicios y versiones:

nmap -sV -sS [dirección_IP]

Significado: Realiza un escaneo sigiloso y detecta versiones de

normal.

CIBERGUARDIAN

Escaneo de red Wi-Fi (si está habilitado):

nmap --wifi [dirección_IP]
Significado: Realiza un escaneo en redes Wi-Fi (opción puede no estar disponible en todas las versiones).

Escaneo de TCP y UDP:

nmap -sS -sU [dirección_IP]
Significado: Realiza escaneos tanto de puertos TCP como de puertos UDP.

Obtener información de la red:

nmap -sn [dirección_IP]
Significado: Realiza un escaneo de "ping" para descubrir qué hosts están activos sin escanear puertos.