NMAP CHEAT SHEETS

by iTrox

NETWORK SCAN

Scan network range

sudo nmap 10.129.2.0/24 -sn -oA net | grep "for" | cut -d " " -f5

IP LIST SCAN

Scan a list of IPs with X.X.X.0 or X.X.X.Y

sudo nmap -sn -oA net -iL hosts.txt | grep for | cut -d " " -f5

HOST SCAN

Basic scan

sudo nmap 10.129.2.18 -sn -oA host

Basic scan - multi IP address

sudo nmap 10.129.2.18 10.129.2.19 -sn -oA hosts | grep for | cut -d" " -f5

Scan with ICMP packet forwarding

sudo nmap 10.129.2.18 -sn -PE -oA host

Scan with packet traffic analysis

sudo nmap 10.129.2.18 -sn -PE --packet-trace -oA host

Scan showing the reason for a result

sudo nmap 10.129.2.18 -sn -PE --reason -oA host

Scan with ARP ping disabled

sudo nmap 10.129.2.18 -sn -PE --packet-trace --disable-arp-ping -oA host

---

PORT SCAN

Scan of the main ports

sudo nmap 10.129.2.28 --top-ports=10

Port scan with packet sniffing

sudo nmap 10.129.2.28 -p 21 --packet-trace -Pn -n --disable-arp-ping

TCP port scan

sudo nmap 10.129.2.28 -p 443 -sT -Pn -n --reason --packet-trace --disable-arp-ping

Filtered port scan (status= filtered)

sudo nmap 10.129.2.28 -p 139 --packet-trace --disable-arp-ping -Pn -n

UDP port scan

sudo nmap 10.129.2.28 -sU -F

Port version scan

sudo nmap 10.129.2.28 -sV -Pn -n --disable-arp-ping --packet-trace -p 445 --reason

---

SAVE RESULTS

Scan in .nmap format

sudo nmap 10.129.2.28 -p- -oN target

Scan in .gnmap format

sudo nmap 10.129.2.28 -p- -oG target

Scan in .xml format

sudo nmap 10.129.2.28 -p- -oX target

Create XML report from -oX format

xsltproc target.xml -o target.html

SERVICE ENUMERATION

Port version scan

sudo nmap 10.129.2.28 -p- -sV

Scan with output delay

sudo nmap 10.129.2.28 -p- -sV --stats-every=5s

Verbosity level scan

- *sudo nmap 10.129.2.28 -p- -sV -v*

Scanning with capture service banners

- *sudo nmap 10.129.2.28 -p- -sV*
- *sudo nmap 10.129.2.28 -p- -sV -Pn -n --disable-arp-ping --packet-trace*
- *sudo tcpdump -i eth0 host 10.10.14.2 and 10.129.2.28*
- *nc -nv 10.129.2.28 25*

SCAN WITH SCRIPT EXECUTION

Scanning with default scripts

- *sudo nmap 10.129.2.28 -sC*

Scanning with specific script

- *sudo nmap 10.129.2.28 --script vuln*

Scanning with general group of scripts

- *sudo nmap 10.129.2.28 --script vuln,brute,version*

Scanning with group of subscripts per port

- *sudo nmap 10.129.2.28 -p 25 --script banner,smtp-commands*

Aggressive scanning

- *sudo nmap 10.129.2.28 -p 80 -A*

SCAN WITH PERFORMANCE MANAGEMENT

Optimized scanning

- *Use: --min-rate, --min-parallelism X, --min-rtt-timeout X*

FIREWALL AND IDS/IPS EVASION

SYN Scan

- *sudo nmap 10.129.2.28 -p 21,22 -sS -Pn -n --disable-arp-ping

ACK Scan

- *sudo nmap 10.129.2.28 -p 21,22 -sA -Pn -n --disable-arp-ping

Scanning with alternate IP address decoy

- *sudo nmap 10.129.2.28 -p 80 -sS -Pn -n --disable-arp-ping --packet-trace-D RND:5*

Scan from a different source IP

- *sudo nmap 10.129.2.28 -n -Pn -p 445 -O -S 10.129.2.200 -e tun0*

DNS Proxy with SYN-Scan of a filtered port

- *sudo nmap 10.129.2.28 -p50000 -sS -Pn -n --disable-arp-ping --packet-trace*

- **DNS Proxy with SYN-Scan from DNS port as source**
  - *sudo nmap 10.129.2.28 -p50000 -sS -Pn -n --disable-arp-ping --packet-trace --source-port 53*
- **Connection to netcat to confirm filtered port**
  - *ncat -nv --source-port 53 10.129.2.28 50000*

PARÁMETROS GENERALES

Parámetros de escaneo	Descripción
-sn	Desactiva el escaneo de puertos
-oA	Almacena los resultados en todos los formatos (.nmap, grepeable y xml)
-oN	Almacena el resultado en formato .nmap
-oG	Almacena el resultado en formato .gnmap (grepeable)
-oX	Almacena el resultado en formato .xml
-iL	Realiza análisis definidos contra una lista proporcionada
-PE	Realiza el escaneo de ping utilizando solicitudes ICMP contra el objetivo
--packet-trace	Muestra todos los paquetes enviados y recibidos
--disable-arp-ping	Deshabilita el ping ARP
--reason	Muestra el motivo de un resultado específico
--top-ports=10	Explora los puertos principales especificados que se han definido como más frecuentes (10, 100 ó 1000)
-p	Explora sólo el puerto especificado
-p-	Explora los 65535 puertos
--open	Explora solo los puertos abiertos
-n	Desactiva la resolución DNS
-sT	TCP Connect Scan. Envía un paquete SYN al destino. Recibe un SYN/ACK. Envía un ACK confirmando conexión. Recibe un Data con info. Envía un RST para finalizar. Si se completa indica puerto abierto. Si recibe RST indica puerto cerrado. Es más confiable pero menos sigiloso que el SYN scan
-sS	TCP SYN Scan. Envía un paquete SYN. Si recibe un SYN/ACK indica puerto abierto. Si recibe un RST indica puerto cerrado. Este escaneo es sigiloso, ya que no completa el proceso de conexión TCP
-sA	TCP ACK Scan. Envía un paquete ACK. Si recibe un RST indica puerto cerrado. Si no recibe respuesta, puede indicar que el puerto está filtrado. Es útil para eludir firewalls, ya que no establece una conexión completa
-sU	Realiza un escaneo UDP

Parámetros de escaneo	Descripción
-Pn	Deshabilita las solicitudes de eco ICMP
-F	Escanea los 100 puertos principales
-sV	Realiza la detección de la versión del servicio en puertos específicos
--stats-every=5s	Muestra el progreso del escaneo cada 5 segundos
-v / -vv / -vvv	Aumenta el detalle de la información mostrada por output en el escaneo
-sC	Escaneo que aplica la ejecución de scripts NSE predeterminados
--script	Utiliza secuencias de comandos NSE específicos para escaneos por scripts
--traceroute	Rastrea la ruta de un paquete ICMP para mostrar los nodos intermedios
-O	Detecta el sistema operativo del objetivo
-A	Escaneo agresivo. Aplica automáticamente -sV, -O --traceroute y -sC
-T X	Velocidad de escaneo en relación a paquetes enviados al objetivo (0 mas baja, 5 mas alta)
--initial-rtt-timeout Xms	Establece el valor de tiempo especificado como tiempo de espera inicial de RTT (Round-Trip-Time- RTT / Tiempo de ida y vuelta de un paquete)
--min-parallelism X	Establece el valor especificado como la frecuencia mínima de envío de paquetes sobre el objetivo
--max-parallelism X	Establece el valor especificado como la frecuencia máxima de envío de paquetes sobre el objetivo
--min-rtt-timeout X	Establece el valor de tiempo especificado como tiempo de espera mínimo de RTT
--max-rtt-timeout X	Establece el valor de tiempo especificado como tiempo de espera máximo de RTT
--min-rate X	Establece el número mínimo de paquetes que se enviarán por segundo de forma simultanea
--max-rate X	Establece el número máximo de paquetes que se enviarán por segundo de forma simultanea
--max-retries X	Establece el número de reintentos que se realizarán durante el análisis
-D RND:X	Genera X direcciones IP aleatorias que indican la IP de origen de la que proviene la conexión
-S 10.129.2.20	Escanea el objetivo utilizando una dirección IP de origen diferente
-e tun0	Envía todas las solicitudes a través de la interfaz especificada
--source-port 53	Realiza los análisis desde un puerto el origen especificado

STATUS PORTS

Estado de un puerto	Descripción
open	Indica que se ha establecido la conexión con el puerto escaneado. Estas conexiones pueden ser conexiones TCP , datagramas UDP y asociaciones SCTP
closed	El protocolo TCP indica que el paquete que recibimos contiene una flag RST. Este método de escaneo también se puede utilizar para determinar si nuestro objetivo está vivo o no.
filtered	Nmap no puede identificar correctamente si el puerto escaneado está abierto o cerrado porque no se devuelve ninguna respuesta del destino para el puerto o recibimos un código de error del destino.
unfiltered	Este estado de un puerto solo ocurre durante el escaneo TCP-ACK y significa que el puerto es accesible, pero no se puede determinar si está abierto o cerrado.
open|filtered	Si no obtenemos respuesta para un puerto concreto, Nmap lo establece en este estado. Esto indica que un firewall o un filtro de paquetes pueden proteger el puerto.
closed|filtered	Este estado solo ocurre en los escaneos inactivos de ID de IP e indica que fue imposible determinar si el puerto escaneado está cerrado o filtrado por un firewall.

GRUPOS DE SCRIPTS PARA ANÁLISIS CON --script

Categoría	Descripción
auth	Determinación de credenciales de autenticación.
broadcast	Los scripts, que se utilizan para el descubrimiento de hosts mediante la transmisión y los hosts descubiertos, se pueden agregar automáticamente a los análisis restantes.
brute	Ejecuta scripts que intentan iniciar sesión en el servicio respectivo mediante fuerza bruta con credenciales.
default	Scripts predeterminados ejecutados usando la -sCopción.
discovery	Evaluación de servicios accesibles.
dos	Estos scripts se utilizan para comprobar los servicios en busca de vulnerabilidades de denegación de servicio y se utilizan menos porque dañan los servicios.
exploit	Esta categoría de scripts intenta explotar vulnerabilidades conocidas del puerto escaneado.
external	Scripts que utilizan servicios externos para su posterior procesamiento.
fuzzer	Utiliza scripts para identificar vulnerabilidades y manejo inesperado de paquetes mediante el envío de diferentes campos, lo que puede llevar mucho tiempo.

Categoría	Descripción
intrusive	Scripts intrusivos que podrían afectar negativamente al sistema de destino.
malware	Comprueba si algún malware infecta el sistema de destino.
safe	Scripts defensivos que no realizan accesos intrusivos y destructivos.
version	Extensión para detección de servicios.
vuln	Identificación de vulnerabilidades específicas.

PLANTILLA DE TIEMPOS DE ENVÍO Y EFECTOS

	T0	T1	T2	T3	T4	T5
Name	Paranoid	Sneaky	Polite	Normal	Aggressive	Insane
min-rtt-timeout	100 ms	100 ms	100 ms	100 ms	100 ms	50 ms
max-rtt-timeout	5 minutes	15 seconds	10 seconds	10 seconds	1250 ms	300 ms
initial-rtt-timeout	5 minutes	15 seconds	1 second	1 second	500 ms	250 ms
max-retries	10	10	10	10	6	2
Initial (and minimum) scan delay (--scan-delay)	5 minutes	15 seconds	400 ms	0	0	0
Maximum TCP scan delay	5 minutes	15,000	1 second	1 second	10 ms	5 ms
Maximum UDP scan delay	5 minutes	15 seconds	1 second	1 second	1 second	1 second
host-timeout	0	0	0	0	0	15 minutes
script-timeout	0	0	0	0	0	10 minutes
min-parallelism	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates
max-parallelism	1	1	1	Dynamic	Dynamic	Dynamic

	T0	T1	T2	T3	T4	T5
min-hostgroup	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates
max-hostgroup	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates	Dynamic, not affected by timing templates
min-rate	No minimum rate limit	No minimum rate limit	No minimum rate limit	No minimum rate limit	No minimum rate limit	No minimum rate limit
max-rate	No maximum rate limit	No maximum rate limit	No maximum rate limit	No maximum rate limit	No maximum rate limit	No maximum rate limit
defeat-rst-ratelimit	Not enabled by default	Not enabled by default	Not enabled by default	Not enabled by default	Not enabled by default	Not enabled by default

RESPUESTA DE FIREWALL

Paquetes	Descripción
dropped	Nmap envía paquetes pero no recibe respuesta, pueden ser bloqueados por firewalls, IDS o congestión de red
rejected	Nmap recibe una respuesta explícita de rechazo del host de destino, indicando que el puerto está closed o filtered. Devuelve una flag RST

ERRORES DE RESPUESTA DE FIREWALL

Errores	Descripción
Net Unreachable	El destino no puede alcanzarse debido a problemas en la red entre el origen y el destino
Net Prohibited	La red entre el origen y el destino está prohibida, probablemente debido a reglas de firewall
Host Unreachable	El destino no puede ser alcanzado, posiblemente porque está apagado o no está en la red
Host Prohibited	La comunicación con el host está prohibida, probablemente por reglas de firewall o configuración de seguridad

Errores	Descripción
Port Unreachable	El destino está disponible pero el puerto específico no está abierto o accesible
Proto Unreachable	El protocolo especificado no es compatible o está bloqueado en el destino