NMAP RIFERIMENTO RAPIDO

Scansione porte, scoperta host, rilevamento servizi e script NSE

Scansioni di Base

Target di Scansione

```
nmap 192.168.1.1              # host singolo
nmap 192.168.1.0/24           # intera sottorete
nmap 192.168.1.1-50           # intervallo IP
nmap -iL targets.txt          # host da file
```

Specificare i Target

`192.168.1.1`	Indirizzo IP singolo
`192.168.1.0/24`	Notazione CIDR (256 host)
`192.168.1.1-254`	Intervallo IP
`example.com`	Hostname (risolto in IP)
`-iL file.txt`	Legge i target da file
`--exclude 192.168.1.1`	Esclude host specifici
`--excludefile skip.txt`	Esclude host da file

Scansione delle Porte

Tipi di Scansione

`-sS`	Scansione TCP SYN (default, discreta, richiede root)
`-sT`	Scansione TCP connect (handshake completo, senza root)
`-sU`	Scansione UDP (lenta, spesso filtrata)
`-sA`	Scansione TCP ACK (rileva firewall)
`-sN`	Scansione TCP NULL (nessun flag)
`-sF`	Scansione TCP FIN (solo flag FIN)
`-sX`	Scansione Xmas (flag FIN+PSH+URG)

Selezione delle Porte

```
nmap -p 80,443 target         # porte specifiche
nmap -p 1-1000 target         # intervallo di porte
nmap -p- target               # tutte le 65535 porte
nmap --top-ports 100 target   # le 100 porte più comuni
```

Stati delle Porte

`open`	L'applicazione accetta connessioni
`closed`	Porta raggiungibile ma nessun servizio in ascolto
`filtered`	Firewall blocca, impossibile determinare lo stato
`unfiltered`	Porta accessibile, stato aperto/chiuso sconosciuto
`open|filtered`	Impossibile determinare se aperta o filtrata

Scoperta degli Host

Metodi di Scoperta

`-sn`	Solo ping scan (senza scansione porte)
`-Pn`	Salta la scoperta host (tratta tutti come attivi)
`-PS 80,443`	Scoperta TCP SYN sulle porte
`-PA 80`	Scoperta TCP ACK
`-PU 53`	Scoperta UDP
`-PE`	Richiesta echo ICMP
`-PR`	Scoperta ARP (rete locale)

Sweep di Rete

```
nmap -sn 192.168.1.0/24       # ping sweep sottorete
nmap -sn -n 10.0.0.0/24       # sweep, salta DNS
nmap -sn -PR 192.168.1.0/24   # scansione ARP (più veloce)
```

Rilevamento dei Servizi

Rilevamento della Versione

```
nmap -sV target               # rileva versioni dei servizi
nmap -sV --version-intensity 5 target  # probing più approfondito
nmap -sV --version-all target  # prova ogni probe (lento)
nmap -A target                 # OS + versione + script + traceroute
```

Flag dei Servizi

`-sV`	Interroga le porte aperte per servizio/versione
`--version-intensity 0-9`	Intensità del probing (default 7)
`--version-light`	Probing leggero (intensità 2)
`--version-all`	Prova ogni probe (intensità 9)
`-A`	Aggressivo: -sV -O --script=default -traceroute
`-sC`	Esegue gli script NSE predefiniti

Rilevamento OS

Fingerprinting OS

```
nmap -O target                # rilevamento OS (richiede root)
nmap -O --osscan-limit target # solo host promettenti
nmap -O --osscan-guess target # supposizione aggressiva OS
nmap -A target                # include rilevamento OS
```

Flag per il Rilevamento OS

`-O`	Abilita il rilevamento OS
`--osscan-limit`	Salta host senza porte TCP aperte+chiuse
`--osscan-guess`	Indovina OS in modo più aggressivo
`--max-os-tries N`	Tentativi massimi di rilevamento OS per host

Script (NSE)

Utilizzo degli Script

```
nmap --script=default target   # categoria predefinita
nmap --script=vuln target      # script di vulnerabilità
nmap --script=http-headers target
nmap --script="http-*" target  # corrispondenza con wildcard
```

Categorie degli Script

`default`	Script sicuri e utili (scorciatoia -sC)
`vuln`	Controlla vulnerabilità note
`safe`	Script non intrusivi
`intrusive`	Può causare crash o attivare IDS
`discovery`	Scoperta di rete e servizi
`auth`	Controlli relativi all'autenticazione
`brute`	Test di credenziali a forza bruta
`exploit`	Tentativi di sfruttamento attivo

Script Utili

`http-title`	Recupera i titoli delle pagine web
`ssl-cert`	Mostra i dettagli del certificato SSL
`ssh-hostkey`	Mostra le impronte delle chiavi host SSH
`dns-brute`	Enumera i sottodomini DNS
`smb-os-discovery`	Rileva OS Windows tramite SMB
`vuln`	Esegue tutti i controlli di vulnerabilità

Formati di Output

Opzioni di Output

```
nmap -oN scan.txt target      # output testo normale
nmap -oX scan.xml target      # output XML
nmap -oG scan.gnmap target    # output grepabile
nmap -oA scan_all target      # tutti i formati insieme
```

Flag di Output

`-oN file`	Output normale su file
`-oX file`	Output XML (per strumenti/parsing)
`-oG file`	Output grepabile (un host per riga)
`-oA basename`	Tutti e tre i formati (basename.nmap/xml/gnmap)
`-v`	Aumenta la verbosità (-vv per di più)
`-d`	Output di debug (-dd per di più)
`--open`	Mostra solo le porte aperte
`--reason`	Mostra il motivo dello stato della porta

Timing e Prestazioni

Template di Timing

`-T0 (paranoid)`	Molto lento, evasione IDS (5 min tra i probe)
`-T1 (sneaky)`	Lento, evasione IDS (15 sec tra i probe)
`-T2 (polite)`	Velocità ridotta, meno banda
`-T3 (normal)`	Timing predefinito
`-T4 (aggressive)`	Veloce, presuppone rete affidabile
`-T5 (insane)`	Massima velocità, può perdere risultati

Regolazione Fine

`--min-rate 1000`	Invia almeno 1000 pacchetti/sec
`--max-rate 500`	Limite a 500 pacchetti/sec
`--max-retries 2`	Max ritrasmissioni dei probe
`--host-timeout 30m`	Salta host se la scansione supera 30 min
`--scan-delay 1s`	Ritardo tra i probe
`--min-parallelism 10`	Gruppi minimi di probe paralleli

Evasione Firewall

Tecniche di Evasione

`-f`	Frammenta i pacchetti (blocchi da 8 byte)
`-D RND:5`	Scansione con 5 IP casuali come decoy
`-S spoof_ip`	Falsifica IP sorgente (richiede raw packets)
`-e eth0`	Usa un'interfaccia di rete specifica
`--source-port 53`	Usa porta sorgente specifica (es. DNS)
`--data-length 25`	Aggiunge dati casuali ai pacchetti
`--spoof-mac 0`	Randomizza l'indirizzo MAC

Esempi di Evasione

```
nmap -f -D RND:3 target       # frammenti + decoy
nmap --source-port 53 target  # porta DNS (spesso consentita)
nmap -T1 --scan-delay 5s target  # lento per eludere IDS
```

Pattern Comuni

Ricognizione Rapida

```
nmap -T4 -F target            # porte comuni veloci
nmap -T4 -A -v target         # rilevamento OS + servizi
nmap -sV --top-ports 1000 target  # top 1000 + versioni
```

Scansione Completa

```
# TCP completo + servizi + OS + script
nmap -sS -sV -O -sC -p- -T4 -oA full target
# Scansione UDP sulle porte comuni
nmap -sU --top-ports 50 target
```

Audit Server Web

```
nmap -p 80,443 --script=http-title,http-headers,\
ssl-cert,http-methods target
# Controlla proxy aperti e vulnerabilità
nmap -p 80,443,8080 --script=http-open-proxy,vuln target
```

Inventario di Rete

```
# Scopri tutti gli host attivi con info OS
nmap -sn 192.168.1.0/24 -oG - | grep "Up"
# Inventario servizi per sottorete
nmap -sV -T4 192.168.1.0/24 -oX inventory.xml
```