

REFERENSI CEPAT NMAP

Pemindaian port, penemuan host, deteksi layanan, dan skrip NSE

Scan Dasar

Target Scan

```
nmap 192.168.1.1 # host tunggal
nmap 192.168.1.0/24 # seluruh subnet
nmap 192.168.1.1-50 # rentang IP
nmap -iL targets.txt # host dari file
```

Spesifikasi Target

```
192.168.1.1 Alamat IP tunggal
192.168.1.0/24 Notasi CIDR (256 host)
192.168.1.1-254 Rentang IP
example.com Hostname (di-resolve ke IP)
-iL file.txt Baca target dari file
--exclude 192.168.1.1 Kecualikan host tertentu
--excludefile skip.txt Kecualikan host dari file
```

Pemindaian Port

Tipe Scan

```
-sS Scan TCP SYN (default, siluman, perlu root)
-sT Scan TCP connect (handshake penuh, tanpa root)
-sU Scan UDP (lambat, sering difilter)
-sA Scan TCP ACK (deteksi firewall)
-sN Scan TCP NULL (tanpa flag)
-sF Scan TCP FIN (hanya flag FIN)
-sX Scan Xmas (flag FIN+PSH+URG)
```

Pemilihan Port

```
nmap -p 80,443 target # port tertentu
nmap -p 1-1000 target # rentang port
nmap -p- target # semua 65535 port
nmap --top-ports 100 target # 100 port paling umum
```

Status Port

```
open Aplikasi menerima koneksi
closed Port dapat dijangkau tapi tidak ada layanan
filtered Firewall memblokir, status tidak dapat ditentukan
unfiltered Port dapat diakses, status terbuka/tertutup tidak diketahui
open|filtered Tidak dapat menentukan apakah terbuka atau difilter
```

Penemuan Host

Metode Penemuan

```
-sn Ping scan saja (tanpa scan port)
-Pn Lewati penemuan host (anggap semua aktif)
-PS 80,443 Penemuan TCP SYN pada port
-PA 80 Penemuan TCP ACK
-PU 53 Penemuan UDP
-PE ICMP echo request
-PR Penemuan ARP (jaringan lokal)
```

Network Sweep

```
nmap -sn 192.168.1.0/24 # ping sweep subnet
nmap -sn -n 10.0.0.0/24 # sweep, Lewati DNS
nmap -sn -PR 192.168.1.0/24 # scan ARP (tercepat)
```

Deteksi Layanan

Deteksi Versi

```
nmap -sV target # deteksi versi layanan
nmap -sV --version-intensity 5 target # probing lebih dalam
nmap -sV --version-all target # coba semua probe (lambat)
nmap -A target # OS + versi + skrip + traceroute
```

Flag Layanan

```
-sV Probe port terbuka untuk layanan/versi
--version-intensity 0-9 Intensitas probe (default 7)
--version-light Probing ringan (intensitas 2)
--version-all Coba semua probe (intensitas 9)
-A Agresif -sV -O --script=default-traceroute
-sC Jalankan skrip NSE default
```

Deteksi OS

OS Fingerprinting

```
nmap -O target # deteksi OS (perlu root)
nmap -O --osscan-limit target # scan host yang menjanjikan saja
nmap -O --osscan-guess target # tebak OS secara agresif
nmap -A target # termasuk deteksi OS
```

Flag Deteksi OS

```
-O Aktifkan deteksi OS
--osscan-limit Lewati host tanpa port TCP terbuka/tertutup
--osscan-guess Tebak OS lebih agresif
--max-os-tries N Maksimum percobaan deteksi OS per host
```

Skrip (NSE)

Penggunaan Skrip

```
nmap --script=default target # kategori default
nmap --script=vuln target # skrip kerentanan
nmap --script=http-headers target
nmap --script="http-*" target # pencocokan wildcard
```

Kategori Skrip

```
default Skrip aman dan berguna (singkatan -sC)
vuln Periksa kerentanan yang diketahui
safe Skrip tidak intrusif
intrusive Dapat merusak target atau memicu IDS
discovery Penemuan jaringan & layanan
auth Pemeriksaan terkait autentikasi
brute Pengujian kredensial brute-force
exploit Percobaan eksploitasi aktif
```

Skrip Berguna

```
http-title Ambil judul halaman web
ssl-cert Tampilkan detail sertifikat SSL
```

```
ssh-hostkey Tampilkan fingerprint host key SSH
dns-brute Enumerasi subdomain DNS
smb-os-discovery Deteksi OS Windows via SMB
vuln Jalankan semua pemeriksaan kerentanan
```

Format Output

Opsi Output

```
nmap -oN scan.txt target # output teks normal
nmap -oX scan.xml target # output XML
nmap -oG scan.gnmap target # output greppable
nmap -oA scan_all target # semua format sekaligus
```

Flag Output

```
-oN file Output normal ke file
-oX file Output XML (untuk tools/parsing)
-oG file Output greppable (satu host per baris)
-oA basenane Semua tiga format (basenane.nmap/xml/gnmap)
-vJ Tingkatkan verbositas (-vv untuk lebih)
-d Output debug (-dd untuk lebih)
--open Tampilkan hanya port terbuka
--reason Tampilkan alasan status port
```

Timing & Performa

Template Timing

```
-T0 (paranoid) Sangat lambat, menghindari IDS (5 menit antar probe)
-T1 (sneaky) Lambat, menghindari IDS (15 detik antar probe)
-T2 (polite) Kecepatan dikurangi, bandwidth lebih hemat
-T3 (normal) Timing default
-T4 (aggressive) Cepat, asumsikan jaringan andal
-T5 (insane) Tercepat, mungkin melewati hasil
```

Penyesuaian Detail

```
--min-rate 1000 Kirim minimal 1000 paket/detik
--max-rate 500 Batas 500 paket/detik
--max-retries 2 Maksimum transmisi ulang probe
--host-timeout 30m Lewati host jika scan melebihi 30 menit
--scan-delay 1s Jeda antar probe
--min-parallelism 10 Grup probe paralel minimum
```

Penghindaran Firewall

Teknik Penghindaran

```
-f Fragmentasi paket (potongan 8-byte)
-D RND:5 Scan decoy dengan 5 IP acak
-S spoof_ip Spoofing IP sumber (perlu paket raw)
-e eth0 Gunakan interface jaringan tertentu
--source-port 53 Gunakan port sumber tertentu (mis. DNS)
--data-length 25 Tambahkan data acak ke paket
--spoof-mac 0 Acak alamat MAC
```

Contoh Penghindaran

```
nmap -f -D RND:3 target # fragmentasi + decoy
nmap --source-port 53 target # port DNS (sering diizinkan)
nmap -T1 --scan-delay 5s target # lambat untuk menghindari IDS
```

Pola Umum

Rekon Cepat

```
nmap -T4 -F target # port umum cepat
nmap -T4 -A -v target # deteksi OS + layanan
nmap -sV --top-ports 1000 target # top 1000 + versi
```

Scan Komprehensif

```
# TCP penuh + layanan + OS + skrip
nmap -sS -sV -O -sC -p- -T4 -oA full target
# Scan UDP pada port umum
nmap -sU --top-ports 50 target
```

Audit Web Server

```
nmap -p 80,443 --script=http-title,http-headers,\
ssl-cert,http-methods target
# Periksa proxy terbuka dan kerentanan
nmap -p 80,443,8080 --script=http-open-proxy,vuln target
```

Inventaris Jaringan

```
# Temukan semua host aktif dengan info OS
nmap -sn 192.168.1.0/24 -oG - | grep "Up"
# Inventaris layanan untuk subnet
nmap -sV -T4 192.168.1.0/24 -oX inventory.xml
```