THAM KHẢO NHANH NMAP

Quét cổng, khám phá host, phát hiện dịch vụ và NSE scripts

Quét Cơ Bản

Mục Tiêu Quét

```
nmap 192.168.1.1              # single host
nmap 192.168.1.0/24           # entire subnet
nmap 192.168.1.1-50           # IP range
nmap -iL targets.txt          # hosts from file
```

Chỉ Định Mục Tiêu

`192.168.1.1`	Địa chỉ IP đơn
`192.168.1.0/24`	Ký hiệu CIDR (256 hosts)
`192.168.1.1-254`	Dải địa chỉ IP
`example.com`	Hostname (phân giải thành IP)
`-iL file.txt`	Đọc mục tiêu từ file
`--exclude 192.168.1.1`	Loại trừ host cụ thể
`--excludefile skip.txt`	Loại trừ hosts từ file

Quét Cổng

Loại Quét

`-sS`	TCP SYN scan (mặc định, ẩn, cần root)
`-sT`	TCP connect scan (handshake đầy đủ, không cần root)
`-sU`	UDP scan (chậm, thường bị lọc)
`-sA`	TCP ACK scan (phát hiện firewall)
`-sN`	TCP NULL scan (không có flags)
`-sF`	TCP FIN scan (chỉ FIN flag)
`-sX`	Xmas scan (FIN+PSH+URG flags)

Chọn Cổng

```
nmap -p 80,443 target         # specific ports
nmap -p 1-1000 target         # port range
nmap -p- target               # all 65535 ports
nmap --top-ports 100 target   # most common 100 ports
```

Trạng Thái Cổng

`open`	Ứng dụng đang nhận kết nối
`closed`	Cổng truy cập được nhưng không có service
`filtered`	Firewall chặn, không thể xác định
`unfiltered`	Cổng có thể truy cập, chưa rõ open/closed
`open|filtered`	Không thể phân biệt open hay filtered

Khám Phá Host

Phương Pháp Khám Phá

`-sn`	Chỉ quét ping (không quét cổng)
`-Pn`	Bỏ qua host discovery (coi tất cả là up)
`-PS 80,443`	TCP SYN discovery trên các cổng
`-PA 80`	TCP ACK discovery
`-PU 53`	UDP discovery
`-PE`	ICMP echo request
`-PR`	ARP discovery (mạng nội bộ)

Quét Dải Mạng

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

Phát Hiện Dịch Vụ

Phát Hiện Phiên Bản

```
nmap -sV target               # detect service versions
nmap -sV --version-intensity 5 target  # deeper probing
nmap -sV --version-all target  # try every probe (slow)
nmap -A target                 # OS + version + scripts +
traceroute
```

Flags Dịch Vụ

`-sV`	Thăm dò cổng mở để xác định service/phiên bản
`--version-intensity 0-9`	Cường độ thăm dò (mặc định 7)
`--version-light`	Thăm dò nhẹ (cường độ 2)
`--version-all`	Thử mọi probe (cường độ 9)
`-A`	Toàn diện: -sV -O --script=default -traceroute
`-sC`	Chạy NSE scripts mặc định

Phát Hiện OS

OS Fingerprinting

```
nmap -O target                # OS detection (needs root)
nmap -O --osscan-limit target # only scan promising hosts
nmap -O --osscan-guess target # aggressive OS guessing
nmap -A target                # includes OS detection
```

Flags Phát Hiện OS

`-O`	Bật phát hiện OS
`--osscan-limit`	Bỏ qua hosts không có cổng TCP open+closed
`--osscan-guess`	Đoán OS mạnh hơn
`--max-os-tries N`	Số lần thử phát hiện OS tối đa mỗi host

Scripts (NSE)

Sử Dụng Scripts

```
nmap --script=default target   # default category
nmap --script=vuln target      # vulnerability scripts
nmap --script=http-headers target
nmap --script="http-*" target  # wildcard match
```

Danh Mục Scripts

`default`	Scripts an toàn và hữu dụng (viết tắt -sC)
`vuln`	Kiểm tra lỗ hổng đã biết
`safe`	Scripts không xâm nhập
`intrusive`	Có thể gây crash hoặc kích hoạt IDS
`discovery`	Khám phá mạng và dịch vụ
`auth`	Kiểm tra liên quan xác thực
`brute`	Kiểm tra brute-force thông tin đăng nhập
`exploit`	Thử khai thác chủ động

Scripts Hữu Dụng

`http-title`	Lấy tiêu đề trang web
`ssl-cert`	Hiển thị chi tiết chứng chỉ SSL
`ssh-hostkey`	Hiển thị fingerprint SSH host key
`dns-brute`	Liệt kê subdomains DNS
`smb-os-discovery`	Phát hiện Windows OS qua SMB
`vuln`	Chạy tất cả kiểm tra lỗ hổng

Định Dạng Đầu Ra

Tùy Chọn Đầu Ra

```
nmap -oN scan.txt target      # normal text output
nmap -oX scan.xml target      # XML output
nmap -oG scan.gnmap target    # grepable output
nmap -oA scan_all target      # all formats at once
```

Flags Đầu Ra

`-oN file`	Đầu ra văn bản thường ra file
`-oX file`	Đầu ra XML (cho công cụ/phân tích)
`-oG file`	Đầu ra grepable (một host mỗi dòng)
`-oA basename`	Cả ba định dạng (basename.nmap/xml/gnmap)
`-v`	Tăng chi tiết (-vv để nhiều hơn)
`-d`	Đầu ra debug (-dd để nhiều hơn)
`--open`	Chỉ hiển thị cổng đang mở
`--reason`	Hiển thị lý do trạng thái cổng

Thời Gian & Hiệu Suất

Templates Thời Gian

`-T0 (paranoid)`	Rất chậm, tránh IDS (5 phút giữa các probe)
`-T1 (sneaky)`	Chậm, tránh IDS (15 giây giữa các probe)
`-T2 (polite)`	Tốc độ giảm, ít băng thông hơn
`-T3 (normal)`	Thời gian mặc định
`-T4 (aggressive)`	Nhanh, giả định mạng ổn định
`-T5 (insane)`	Nhanh nhất, có thể bỏ sót kết quả

Tinh Chỉnh Chi Tiết

`--min-rate 1000`	Gửi ít nhất 1000 gói/giây
`--max-rate 500`	Giới hạn 500 gói/giây
`--max-retries 2`	Số lần gửi lại probe tối đa
`--host-timeout 30m`	Bỏ qua host nếu quét quá 30 phút
`--scan-delay 1s`	Độ trễ giữa các probe
`--min-parallelism 10`	Nhóm probe song song tối thiểu

Vượt Qua Firewall

Kỹ Thuật Vượt Qua

`-f`	Phân mảnh gói tin (8-byte chunks)
`-D RND:5`	Decoy scan với 5 IP ngẫu nhiên
`-S spoof_ip`	Giả mạo IP nguồn (cần raw packets)
`-e eth0`	Dùng interface mạng cụ thể
`--source-port 53`	Dùng cổng nguồn cụ thể (vd: DNS)
`--data-length 25`	Thêm dữ liệu ngẫu nhiên vào gói tin
`--spoof-mac 0`	Ngẫu nhiên hoá địa chỉ MAC

Ví Dụ Vượt Qua

```
nmap -f -D RND:3 target       # fragments + decoys
nmap --source-port 53 target  # DNS port (often allowed)
nmap -T1 --scan-delay 5s target  # slow to evade IDS
```

Mẫu Phổ Biến

Trinh Sát Nhanh

```
nmap -T4 -F target            # fast common ports
nmap -T4 -A -v target         # OS + service detection
nmap -sV --top-ports 1000 target  # top 1000 + versions
```

Quét Toàn Diện

```
# Full TCP + service + OS + scripts
nmap -sS -sV -O -sC -p- -T4 -oA full target
# UDP scan on common ports
nmap -sU --top-ports 50 target
```

Kiểm Tra Web Server

```
nmap -p 80,443 --script=http-title,http-headers,\
ssl-cert,http-methods target
# Check for open proxies and vulns
nmap -p 80,443,8080 --script=http-open-proxy,vuln target
```

Kiểm Kê Mạng

```
# Discover all live hosts with OS info
nmap -sn 192.168.1.0/24 -oG - | grep "Up"
# Service inventory for subnet
nmap -sV -T4 192.168.1.0/24 -oX inventory.xml
```