nmap 빠른 참조

포트 스캔, 호스트 탐색, 서비스 감지, NSE 스크립트

기본 스캔

스캔 대상

```
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
```

대상 지정

192.168.1.1	단일 IP 주소
192.168.1.0/24	CIDR 표기 (256 호스트)
192.168.1.1-254	IP 범위
example.com	호스트명 (IP로 해석)
-iL file.txt	파일에서 대상 읽기
--exclude 192.168.1.1	특정 호스트 제외
--excludefile skip.txt	파일에서 제외할 호스트 읽기

포트 스캔

스캔 유형

-sS	TCP SYN 스캔 (기본, 스텔스, root 필요)
-sT	TCP 연결 스캔 (전체 핸드셰이크, root 불필요)
-sU	UDP 스캔 (느림, 자주 필터링됨)
-sA	TCP ACK 스캔 (방화벽 감지)
-sN	TCP NULL 스캔 (플래그 없음)
-sF	TCP FIN 스캔 (FIN 플래그만)
-sX	Xmas 스캔 (FIN+PSH+URG 플래그)

포트 선택

```
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
```

포트 상태

open	애플리케이션이 연결 수락 중
closed	포트 도달 가능하지만 서비스 없음
filtered	방화벽 차단으로 상태 확인 불가
unfiltered	포트 접근 가능, open/closed 미확인
open|filtered	open인지 filtered인지 판단 불가

호스트 탐색

탐색 방법

-sn	핑 스캔만 수행 (포트 스캔 없음)
-Pn	호스트 탐색 건너뜀 (모두 활성으로 처리)
-PS 80,443	포트에서 TCP SYN 탐색
-PA 80	TCP ACK 탐색
-PU 53	UDP 탐색
-PE	ICMP 에코 요청
-PR	ARP 탐색 (로컬 네트워크)

네트워크 스윕

```
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)
```

서비스 감지

버전 감지

```
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
```

서비스 플래그

-sV	열린 포트에서 서비스/버전 탐색
--version-intensity 0-9	탐색 강도 (기본 7)
--version-light	가벼운 탐색 (강도 2)
--version-all	모든 탐색 시도 (강도 9)
-A	공격적: -sV -O --script=default -traceroute
-sC	기본 NSE 스크립트 실행

OS 감지

OS 핑거프린팅

```
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
```

OS 감지 플래그

-O	OS 감지 활성화
--osscan-limit	열린+닫힌 TCP 포트 없는 호스트 건너뜀
--osscan-guess	더 적극적으로 OS 추측
--max-os-tries N	호스트당 최대 OS 감지 시도 횟수

스크립트 (NSE)

스크립트 사용

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

스크립트 카테고리

default	안전하고 유용한 스크립트 (-sC 단축)
vuln	알려진 취약점 확인
safe	비침투적 스크립트
intrusive	대상 충돌 또는 IDS 트리거 가능
discovery	네트워크 및 서비스 탐색
auth	인증 관련 검사
brute	브루트포스 자격증명 테스트
exploit	적극적인 취약점 이용 시도

유용한 스크립트

http-title	웹 페이지 제목 가져오기
ssl-cert	SSL 인증서 상세 정보 표시
ssh-hostkey	SSH 호스트 키 핑거프린트 표시
dns-brute	DNS 서브도메인 열거
smb-os-discovery	SMB를 통해 Windows OS 감지
vuln	모든 취약점 검사 실행

출력 형식

출력 옵션

```
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
```

출력 플래그

-oN file	파일에 일반 텍스트 출력
-oX file	XML 출력 (도구/파싱용)
-oG file	그레퍼블 출력 (호스트당 한 줄)
-oA basename	세 가지 형식 모두 (basename.nmap/xml/gnmap)
-v	상세 출력 증가 (-vv로 더 많이)
-d	디버그 출력 (-dd로 더 많이)
--open	열린 포트만 표시
--reason	포트 상태의 이유 표시

타이밍 및 성능

타이밍 템플릿

-T0 (paranoid)	매우 느림, IDS 우회 (탐색 간 5분)
-T1 (sneaky)	느림, IDS 우회 (탐색 간 15초)
-T2 (polite)	속도 감소, 대역폭 절약
-T3 (normal)	기본 타이밍
-T4 (aggressive)	빠름, 안정적인 네트워크 가정
-T5 (insane)	최고속, 결과 누락 가능

세밀한 조정

--min-rate 1000	초당 최소 1000 패킷 전송
--max-rate 500	초당 최대 500 패킷
--max-retries 2	최대 탐색 재전송 횟수
--host-timeout 30m	30분 초과 시 호스트 건너뜀
--scan-delay 1s	탐색 간 지연
--min-parallelism 10	최소 병렬 탐색 그룹 수

방화벽 우회

우회 기법

-f	패킷 단편화 (8바이트 청크)
-D RND:5	무작위 IP 5개로 디코이 스캔
-S spoof_ip	소스 IP 스푸핑 (원시 패킷 필요)
-e eth0	특정 네트워크 인터페이스 사용
--source-port 53	특정 소스 포트 사용 (예: DNS)
--data-length 25	패킷에 임의 데이터 추가
--spoof-mac 0	MAC 주소 무작위화

우회 예시

```
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
```

일반 패턴

빠른 정찰

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

종합 스캔

```
# 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
```

웹 서버 감사

```
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
```

nmap 빠른 참조

네트워크 인벤토리

```
# 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
```