nmap Network scanner

CONCEPTS

Only scan hosts and networks you own or are explicitly authorised to test. Unauthorised scans can be illegal and set off alarms.

Targets hosts, CIDR
↓ discovery
Live hosts ping probes
↓ port scan
Port states open/closed/filtered
↓ -sV -O -sC
Details service, OS, scripts

Without root, nmap falls back to a TCP connect scan (-sT); raw-packet scans like -sS, -sU and -O need privileges.

TARGETS

nmap *<host>*
Scan one host

nmap *<host1>* *<host2>*
Scan several hosts

nmap *<net>*/24
Scan a whole subnet (CIDR)

nmap -iL *<file>*
Read targets from a file

HOST DISCOVERY

nmap -sn *<net>*/24
Ping scan only, no port scan

nmap -Pn *<host>*
Skip discovery, assume host is up

PORTS

nmap -p *<port>* *<host>*
Scan one port

nmap -p 22,80,443 *<host>*
Scan a port list

nmap -p 1-1023 *<host>*
Scan a port range

nmap -p- *<host>*
Scan all 65535 ports

nmap -F *<host>*
Fast: top 100 ports only

nmap --top-ports *<n>* *<host>*
Scan the n most common ports

SCAN TYPES

nmap -sS *<host>*
TCP SYN (half-open) scan

nmap -sT *<host>*
TCP connect scan

nmap -sU *<host>*
UDP scan

DETECTION

nmap -sV *<host>*
Detect service versions

nmap -O *<host>*
Detect the operating system

nmap -A *<host>*
OS, versions, scripts, traceroute

SCRIPTS (NSE)

nmap -sC *<host>*
Run default scripts

nmap --script *<name>* *<host>*
Run a named script

nmap --script *<category>* *<host>*
Run a category (safe, vuln...)

nmap --script "http-*" *<host>*
Run scripts by wildcard

NSE scripts are not sandboxed and categories like intrusive, brute, exploit and dos can disrupt services. Review scripts before running them and prefer safe.

TIMING & PERFORMANCE

nmap -T4 *<host>*
Faster scan on a reliable network

OUTPUT

nmap -v *<host>*
More verbose, repeat for more

nmap --open *<host>*
Show only open ports

nmap -oN *<file>* *<host>*
Save normal output

nmap -oX *<file>* *<host>*
Save XML output

nmap -oA *<base>* *<host>*
Save normal, XML and grepable