NMAP

☆ IP | Port | Scan Type | Scan Timings | Output Types

Commands

↳ always needed, rest will be default if not specified

↳ can also be subnet or CIDR

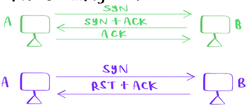
☆ Host Discovery

As Root user: (sends all)
- ICMP Echo Req
- TCP SYN - 443
- TCP ACK - 80
- ICMP T.S Req

As Local user:
- SYN - 443
- ACK - 80

If you know host is up & want to skip host discovery:
nmap -Pn 192.168.1.1

☆ How scanning works



Port OPEN
Port CLOSED
} TCP

☆ Target nmap _____

1. Single IP: nmap 1.2.3.4
2. Subnet range: nmap 1.2.3.4/8
3. IP range: nmap 1.2.3.4-8
4. Specific IPs: nmap 1.2.3.4 5.6.7.8
5. Text file: nmap -iL host.txt
6. Domain: nmap scanme.nmap.org

} Will use 1000 most common ports since not specified

☆ Ports: nmap 1.2.3.4 (Port(s))

1. Single Port: nmap 1.2.3.4 -p 80
2. Seq. Port: nmap 1.2.3.4 -p 20-30
3. Distributed only: nmap 1.2.3.4 -p 80,22,111
4. Service specific: nmap 1.2.3.4 -p http
5. Protocol specific: nmap 1.2.3.4 -p T:22,U:53 (T: TCP, U: UDP)
6. All ports: nmap 1.2.3.4 -p -

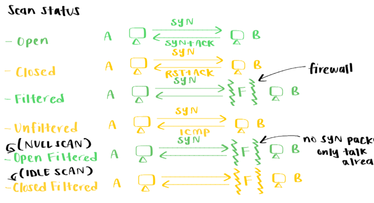
Extra: nmap 1.2.3.4 --top-ports 100

☆ Scan Techniques

- TCP Connect Scan -sT
- TCP SYN Scan -sS
- FIN Scan -sF
- XMAS Scan -sX
- Null Scan -sN
- Ping Scan -sP
- UDP Scan -sU
- ACK Scan -sA

⋮

☆ Scan status



Example rule for firewall (Linux):

sudo iptables -I INPUT -p tcp --dport=22 -j DROP

☆ Scan Timings:

T0	T1	T2	T3	T4	T5
Paranoid	Sneaky	Polite	Normal	Aggressive	Insane

Used in cases when there is an IDS — Fast — Even faster, but Accuracy ↓

nmap 1.2.3.4 -T1

Host Timeout: nmap --host-timeout 500ms 1.2.3.4

Scan Delay: nmap --scan-delay 2s 1.2.3.4

☆ Output Types:

1. Normal Text output -oN
2. XML format -oX
3. Grepable Format -oG ← Not used anymore
4. Script kiddie Format -oS

☆ NMAP Script Engine (NSE)

- Firewall Bypass
- FTP Enum
- DNS Enum
- HTTP Enum

⋮

Scripts saved in: cd /usr/share/nmap/scripts

To use scripts: nmap scanme.nmap.org --script http-headers

☆ Extras

- Service Version: nmap -sV 1.2.3.4
- OS Detection: nmap -O 1.2.3.4
- Verbosity: nmap -v 1.2.3.4
- Service Version + OS Detection + Scanning + Trace route: nmap -A 1.2.3.4