Scanning techniques

- Xmas scan
  - -sX
- TCP SYN scan
  - -sS
- Connect scan
  - -sT
- ACK scan
  - -sA
- Window scan
  - -sW
- Maimon scan
  - -sM
- UDP scan
  - -sU
- TCP Null scan
  - -sN
- FIN scan
  - -sF
- SCTP INIT scan
  - -sY
- COOKIE-ECHO scan
  - -sZ
- IP protocol scan
  - -sO

Host discovery

- List scan
  - -sL
- Ping scan
  - -sn
- Treat all hosts as online
  - -Pn
- Discovery to given ports: TCP SYN/ ACK, UDP, SCTP
  - -PS/PA/PU/PY <port list>
- ICMP echo, timestamp, and netmask request discovery probes
  - -PE/PP/PM
- IP Protocol ping
  - -PO <protocol list>
- DNS resolution: never/always (default: sometimes)
  - -n/R

OS detection

- Enable OS detection
  - -O
- Limit detection to promising targets
  - --osscan-limit
- Guess OS more aggressively
  - --osscan-guess

Timing & performance

- Serial, slowest
  - -T0
- Serial, slow
  - -T1
- Serial
  - -T2
- Parallel
  - -T3
- Parallel, fast
  - -T4

Target specification

- Input list of hosts/Networks from file
  - -iL <fileName.txt>
- Scan Random Hosts
  - -iR <number>
- Exclude host/Networks
  - --exclude <host>
- Exclude host/Networks from file
  - --excludefile <hostFile.txt>

Port specification & scan order

- Specify ports
  - -p <port>,<port>,<...>/<1-65535>
- Scan UDP ports
  - -p U:<port>
- Fast mode, scans few ports
  - -F
- Scan ports consecutively
  - -r
- Scan number of top ports
  - --top-ports <number>
- Scan ports more common than ratio given
  - -port-ratio <number>

NMAP output options

- Output normal
  - -oN
- Output XML
  - -oX
- Output greppable
  - -oG
- Output all 3 formats
  - -oA
- Verbose
  - -v
- Debuggung
  - -d/-dd

Service version detection

- Probe open ports to determine service/ version info
  - -sV
- Version intensity
  - --version-intensity <0-9>
- Limit to most likely probes (intensity 2)
  - --version-light
- Try all probes (intensity 9)
  - --version-all
- Show scan activity
  - --version-trace

Firewall/IDS evasion & spoofing

- Fragment IP packets (including ping scans). Can add offset size
  - -f [--mtu <value>]
- Cloak scanwith decoys
  - -D <decoy>,<decoy>
- Spoof source address
  - -S
- Use specified interface
  - -e
- Send packets with specified ip option
  - --ip-options <option>
- Set IP time to live field
  - --ttl <value>

HTTP service information

- Gather page titles from HTTP services
  - --script=http-title <host>
- Get HTTP headers of web services
  - --script=http-headers <host>
- Find web apps from known paths
  - --script=http-enum <host>

Script scan

- Script default
  - -sC
- Provide NSE script args in a file
  - -script-args-file=<filename>
- Show all data sent and received
  - --script-trace
- Show script help
  - --script-help="<Lua scripts>"
- Potential to crash servers/service
  - --script-args=unsafe=1

```
Not shown: 995 closed ports
PORT      STATE    SERVICE      VERSION
22/tcp    open     ssh          OpenSSH 5.3p1 Debian
(protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:5
69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85
80/tcp    open     http         Apache httpd 2.2.14 (
|_http-title: Go ahead and ScanMe!
646/tcp  filtered ldp
1720/tcp filtered H.323/Q.931
9929/tcp open     nping-echo  Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
```

Various TCP/IP protocols

Application layer:

- FTP, HTTP, SNMP, BOOTP, DHCP

Transport layer:

- TCP, UDP, ICMP, IGMP

Network layer:

- ARP, IP, RARP

Data link layer:

- SLIP, PPP

Script categories

- ALL
- AUTH
- DEFAULT
- DISCOVERY
- EXTERNAL
- INTRUSIVE
- MALWARE
- SAFE
- VULN, etc

https://github.com/cuanknaggs/nmap-docs