

File Machine View Input Devices Help

```

(kali@kali)-[~]
$ nmap -pn192.168.1.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-03 10:08 EST
Found no matches for the service mask 'n192.168.1.1' and your specified protocols
QUITTING!

```

```

(kali@kali)-[~]
$ nmap -sn192.168.1.1
Nmap 7.95 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of

```

File Machine View Input Devices Help

--badsum: Send packets with a bogus TCP/UDP/SCTP checksum

OUTPUT:

-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIdidi3, and Grepable format, respectively, to the given filename.
 -oA <basename>: Output in the three major formats at once
 -v: Increase verbosity level (use -vv or more for greater effect)
 -d: Increase debugging level (use -dd or more for greater effect)
 --reason: Display the reason a port is in a particular state
 --open: Only show open (or possibly open) ports
 --packet-trace: Show all packets sent and received
 --iflist: Print host interfaces and routes (for debugging)
 --append-output: Append to rather than clobber specified output files
 --resume <filename>: Resume an aborted scan
 --noninteractive: Disable runtime interactions via keyboard
 --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
 --webxml: Reference stylesheet from Nmap.Org for more portable XML
 --no-stylesheet: Prevent associating of XSL stylesheet w/XML output

ISC:

-6: Enable IPv6 scanning
 -A: Enable OS detection, version detection, script scanning, and traceroute
 --datadir <dirname>: Specify custom Nmap data file location
 --send-eth/--send-ip: Send using raw ethernet frames or IP packets
 --privileged: Assume that the user is fully privileged
 --unprivileged: Assume the user lacks raw socket privileges
 -V: Print version number
 -h: Print this help summary page.

EXAMPLES:

nmap -v -A scanme.nmap.org
 nmap -v -sn 192.168.0.0/16 10.0.0.0/8
 nmap -v -iR 10000 -Pn -p 80

SEE THE MAN PAGE (<https://nmap.org/book/man.html>) FOR MORE OPTIONS AND EXAMPLES

cantype 1 not supported

—(kali@kali)-[~]

—\$ nmap -PR192.168.1.1

Unknown -P option -PR192.168.1.1.

QUITTING!

—(kali@kali)-[~]

—\$ nmap -n 192.168.1.1

Starting Nmap 7.95 (<https://nmap.org>) at 2025-12-03 10:10 EST

Nmap scan report for 192.168.1.1

Host is up (0.0025s latency).

Not shown: 996 filtered tcp ports (no-response)

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https
555/tcp	open	freeciv

Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds