



File Actions Edit View Help

(kali@kali)~

\$ nmap -ss 192.168.1.1

Nmap 7.93 (<https://nmap.org>)

Usage: nmap [Scan Type(s)] [Options] {target specification}

TARGET SPECIFICATION:

- Can pass hostnames, IP addresses, networks, etc.
- Ex: scanner.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
- iI <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:

- sI: List Scan - simply list targets to scan
- sn: Ping Scan - disable port scan
- Ps: Treat all hosts as online -- skip host discovery
- PS/PA/PW/PY[portlist]: TCP SYN/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/sM/sM: TCP SYN/Connect()/ACK/Window/Minimal scans
- sU: UDP Scan
- sN/sF/sX: TCP Null, FIN, and Xmas scans
- scanflags <flags>: Customize TCP scan flags
- sI <romble host[:probeport]>: Idle scan
- sV/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: -p21; -p1-65535; -p U:50,111,127,T:21-25,80,135,8080,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 directories, script-files or script-categories
- script-args=<n1=v1[,n2=v2,...]>: provide arguments to scripts
- script-args-file=filename: provide NSE script args in a file
- script-trace: Show all data sent and received

File Actions Edit View Help

```

--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
FORMATTING, OUTPUT AND SPOOFING:
-f/--format <value>: Fragment packets (optionally w/given MD5)
-r <decoy[,decoy[,MD5],...>: Cloak a scan with decoys
-s <IP Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--proxies <url[,url[,...>: Relay connections through HTTP/SOCKS proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum

```

OUTPUT:

```

--m/-x/-a/-p/-d <files>: Output scan in normal, XML, nmapScript kiddie,
and Greppable format, respectively, to the given filenames.
-o <filename>: 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 interaction via keyboard
--stylesheet <path/URI>: XSL stylesheet to transform XML output to HTML
--webui: Reference stylesheet from Nmap.org for more portable XML
--no-stylesheet: Prevent auto-loading of XSL stylesheet w/XML output

```

NMAP:

```

-B: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datafile <filename>: 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 scans.nmap.org
nmap -v -sn 192.168.0.0/24 -p 80,8080
nmap -v -iR 100000 -Pu -p 80

```

SEE THE WWW PAGE (<https://nmap.org/book/man.html>) FOR MORE OPTIONS AND EXAMPLES
 Scantype is not supported

```

kali@kali:~$

```

```

kali@kali: ~
File Actions Edit View Help

(hali@kali) (~)
$ nmap -ss 192.168.1.1
nmap 7.92 ( 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
  -iI <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
  -Po Treat all hosts as online -- skip host discovery
  -PA/PN/PU/PI[portlist]: TCP SYN/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 <server1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/T/A/W/S/M: 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 <probe 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,T:21-25,00,100,8080,519
  --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=<scriptes>: <scriptes> is a comma separated list of
    directories, script-files or script-categories
  --script-args=<val1[,val2,...]>: provide arguments to scripts
  --script-args-file <filename>: provide NSE script args in a file
  --script-trace: Show all data sent and received

```

```

File Actions Edit View Help
--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--min-rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
#iprwall/100 IPv4wall Add spoofing
-f|--mtu <size>: Fragment packets (optionally w/given MTU)
-O <decoy1,decoy2[,MTI],...>: Click a scan with decoys
-s <IP-Address>: Spoof source address
-i <iface>: Use specified interface
-p/--source-port <portnum>: Use given port number
--proxies <url1[,url2],...>: Relay connections through HTTP/SOCKS proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified IP options
-mti <mask>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/ICMP checksum
#OUTPUT
-oM/oM/oM/oM <files>: Output scan in normal, XML, vncscript kiosk,
and Greppable format, respectively, to the given filename.
-oA <basenames>: 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
#NISC
-B: Enable IPv6 scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--data-dir <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
Scantype is not supported

```

```

root@kali:~#

```

```

kali@kali ~
File Actions Edit View Help

kali@kali:~$ nmap -st 192.168.1.1
nmap: option '-st' is ambiguous; possibilities: '-stylesheet' '-stats-every'
See the output of nmap -h for a summary of options.

kali@kali:~$ nmap -ss 192.168.1.1
Nmap 7.93 ( 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:
  -sn: List Scan - simply list targets to scan
  -pm: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PV/PP[<portlist>]: TCP SYN/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/-N: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <servers[,servers],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host

SCAN TECHNIQUES:
  -sS/sT/sA/sM/sO: TCP SYN/Connect()/ACK/Window/FinScan scans
  -sU: UDP Scan
  -sM/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <probe host[:<probeport>]>: Idle scan
  -sV/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 0/13,113,137,7/21-25,88,135,8080,819
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -V: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan number's 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 SCANS:
  -sC: equivalent to --script=default

```



File Actions Edit View Help

```

--scan-delay/--max-scan-delay <time>: Adjust delay between probes
--rate <number>: Send packets no slower than <number> per second
--max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS Evasion AND SPOOFING:
-f/--mitm <url>: Fragment packets (optionally w/given MTU)
-B <decrypl,decrypr[,URL],...>: Clink a scan with decoys
-S <IP.Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--proxies <url[,url],...>: Delay connections through HTTP/socks4 proxies
--data <hex string>: Append a custom payload to sent packets
--data-string <string>: Append a custom ASCII string to sent packets
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your Mac address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
-m/-M/-m/-M <file>: Output scan in normal, XML, nmapst, nmapst,
and Grepable format, respectively, to the given filename.
-o <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
--xhtml: Reference stylesheet from Nmap.org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
-s: Enable IPid scanning
-A: Enable OS detection, version detection, script scanning, and traceroute
--datafile <filename>: 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 -s -A scanme.nmap.org
nmap -v -sn 192.168.0.0/24 19.0.0.0/8
nmap -v -iR 19999 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype is not supported

```

kali@kali:~\$

4

File Machine View Input Devices Help



kali@kali -

File Actions Edit View Help

```
(kali@kali)-[~]  
└─$ nmap -pn 192.168.1.1  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-29 12:09 IST  
Failed to resolve "pn".  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 0.05 seconds
```

```
(kali@kali)-[~]  
└─$ nmap -sn 192.168.1.1  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-29 12:09 IST  
Failed to resolve "sn".  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 0.06 seconds
```

```
(kali@kali)-[~]  
└─$ nmap -pr 192.168.1.1  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-29 12:09 IST  
Failed to resolve "pr".  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 0.05 seconds
```

```
(kali@kali)-[~]  
└─$ nmap -n 192.168.1.1  
Starting Nmap 7.91 ( https://nmap.org ) at 2023-04-29 12:09 IST  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 0.04 seconds
```

```
(kali@kali)-[~]  
└─$
```

```

File Actions Edit View Help
--(root@kali)-[~]
--$ nmap -i 192.168.1.1
Starting Nmap 7.90 ( https://nmap.org ) at 2022-04-29 11:02:55
Status: 0:00:15 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:15:45 remaining)
Status: 0:00:16 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:15:46 remaining)
Status: 0:00:16 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:15:52 remaining)
Status: 0:00:19 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:16:00 remaining)
Status: 0:00:21 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:16:06 remaining)
Status: 0:00:22 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:16:06 remaining)
Status: 0:00:25 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:16:21 remaining)
Status: 0:00:26 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:16:30 remaining)
Status: 0:00:27 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:16:31 remaining)
Status: 0:00:28 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:16:34 remaining)
Status: 0:00:29 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:16:37 remaining)
Status: 0:00:30 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:16:38 remaining)
Status: 0:00:31 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:16:41 remaining)
Status: 0:00:32 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:16:44 remaining)
Status: 0:00:33 elapsed; 0 hosts completed (0 up), 0 undergoing Ping Scan
Ping Scan Timing: About 25.000s done; 0% (0/1) (0:16:47 remaining)
Note: Host seems down. It is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.08 seconds

```

1000

File Machine View Input Devices Help

```
File Actions Edit View Help
kali@kali:~$
kali@kali:~$ nmap -T1 192.168.1.1
Starting Nmap 7.90 ( https://nmap.org ) at 2023-04-29 13:01 IST
Stats: 0:00:15 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 0.00% done
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 15.00 seconds

kali@kali:~$
kali@kali:~$ nmap -T1 192.168.1.1
Starting Nmap 7.90 ( https://nmap.org ) at 2023-04-29 13:03 IST
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.43 seconds

kali@kali:~$
kali@kali:~$ nmap -T1 192.168.1.1
Starting Nmap 7.90 ( https://nmap.org ) at 2023-04-29 13:04 IST
nmap_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.00 seconds
```