

```
root@kali: ~/Desktop
root@kali: ~/Desktop237x54

root@kali)~/Desktop]
nmap
Nmap 7.94SVN ( 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/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/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 <ombie 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 U:55,111,137,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
    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
  --script-updatedb: Update the script database.
  --script-help=<lua scripts>: Show help about scripts.
```

```
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output

MISC:
-b: 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

```
root@kali: ~/Desktop
```

```
# ip addr show
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:0a:1d:58 brd ff:ff:ff:ff:ff:ff
    inet 192.168.182.120/24 brd 192.168.182.255 scope global dynamic noprefixroute eth0
        valid_lft 12098sec preferred_lft 12098sec
    inet6 fe80::e7d4:4405:112:c7d1/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

```
root@kali: ~/Desktop
```

```
# ip route show | head -n 3
```

```
default via 192.168.182.2 dev eth0 proto dhcp src 192.168.182.128 metric 100
192.168.182.0/24 dev eth0 proto kernel scope link src 192.168.182.128 metric 100
```

```
root@kali: ~/Desktop
```

```
# nmap -SS 192.168.182.0/24 -oN ~/nmap.quick.nmap
```

Starting Nmap 7.94SVN (<https://nmap.org>) at 2025-09-22 09:59 EDT

Nmap scan report for 192.168.182.1

Host is up (0.0018s latency).

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

PORT	STATE	SERVICE
------	-------	---------

135/tcp	open	msrpc
---------	------	-------

139/tcp	open	netbios-ssn
---------	------	-------------

445/tcp	open	microsoft-ds
---------	------	--------------

3306/tcp	open	mysql
----------	------	-------

MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.182.2

Host is up (0.00038s latency).

Not shown: 999 closed tcp ports (reset)

PORT	STATE	SERVICE
------	-------	---------

53/tcp	open	domain
--------	------	--------

Screenshot taken

New image

Power Manager
Your Battery is charging

```
root@kali: ~/Desktop
root@kali: ~/Desktop 237x34

root@kali) ~/Desktop
# nmap -sS 192.168.182.0/24 -oN ~/nmap_quick.nmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-22 09:59 EDT
Nmap scan report for 192.168.182.1
Host is up (0.0018s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
MAC Address: 00:50:56:CD:00:08 (VMware)

Nmap scan report for 192.168.182.2
Host is up (0.00038s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:FA:67:22 (VMware)

Nmap scan report for 192.168.182.254
Host is up (0.00037s latency).
All 1000 scanned ports on 192.168.182.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F7:A8:DA (VMware)

Nmap scan report for 192.168.182.128
Host is up (0.000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.66 seconds

root@kali) ~/Desktop
# less ~/nmap_quick.nmap
zsh: suspended less ~/nmap_quick.nmap

root@kali) ~/Desktop
# grep "open" ~/nmap_quick.nmap
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
3306/tcp open  mysql
53/tcp open  domain
80/tcp open  http

root@kali) ~/Desktop
# nmap -sS -sV -O -p- -T4 -oA ~/nmap_fullscan 192.168.182.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-22 10:06 EDT
Stats: 0:00:59 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 72.14% done; ETC: 10:07 (0:00:22 remaining)
Nmap scan report for 192.168.182.1
```

Screenshot taken

View image

```

root@kali: ~/Desktop
root@kali: ~/Desktop 237x54
Screenshot taken
View image
root@kali: ~/Desktop
# nmap -sS -sV -O -p- -T4 -oA -/nmap_fullscan 192.168.182.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2025-09-22 18:06 EDT
Stats: 0:00:59 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 72.14% done; ETC: 18:07 (0:00:22 remaining)
Nmap scan report for 192.168.182.1
Host is up (0.0013s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
3306/tcp   open  mysql        MySQL (unauthorized)
33060/tcp  open  mysqlx?
49668/tcp  open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port33060-TCP:V=7.94SVN|I=74D=9/22X|me=68D15836P=x86_64-pc-linux-gnu|
SF:|00L|,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(GenericInsc,g,"x05|0|0|0|x
SF:|0b|x08|x05|x1a|0"Jxr(GetRequest,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(HTT
SF:|Options,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(HTTPSRequest,g,"x05|0|0|0|
SF:|x0b|x08|x05|x1a|0"Jxr(RPCCheck,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(DNSV
SF:|ersionBindReqTCP,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(DNSStatusRequestTC
SF:|P,28,"x05|0|0|0|x0b|x08|x05|x1a|0|x1e|0|0|0|x01|x08|x01|x10|x88|x1a|x
SF:|0fInvalid|x20message|"x05HY000"Jxr(Help,g,"x05|0|0|0|x0b|x08|x05|x1a|
SF:|0"Jxr(SSLSessionReq,28,"x05|0|0|0|x0b|x08|x05|x1a|0|x1e|0|0|0|x01|x08|
SF:|x01|x10|x88|x1a|x0fInvalid|x20message|"x05HY000"Jxr(TerminalServerCon
SF:|ie,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(TLSSessionReq,28,"x05|0|0|0|x0
SF:|b|x08|x05|x1a|0|x1e|0|0|0|x01|x08|x01|x10|x88|x1a|x0fInvalid|x20messag
SF:|e|"x05HY000"Jxr(Kerberos,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(SMBProgNe
SF:|g,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(X11Probe,28,"x05|0|0|0|x0b|x08|x
SF:|05|x1a|0|x1e|0|0|0|x01|x08|x01|x10|x88|x1a|x0fInvalid|x20message|"x05
SF:|HY000"Jxr(FourHFourRequest,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(LPDStri
SF:|ng,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(LDAPSearchReq,28,"x05|0|0|0|x0b
SF:|x08|x05|x1a|0|x1e|0|0|0|x01|x08|x01|x10|x88|x1a|x0fInvalid|x20messag
SF:|"x05HY000"Jxr(LDAPBindReq,46,"x05|0|0|0|x0b|x08|x05|x1a|0|x09|0|0|0|x
SF:|01|x08|x01|x10|x88|x1a|x0fInvalid|x20message|"x05HY000"Jxr(SIPOptions,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(
SF:|LAWDesk-RC,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(TerminalServer,g,"x05|0
SF:|0|0|x0b|x08|x05|x1a|0"Jxr(NCP,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(Note
SF:|SPRC,28,"x05|0|0|0|x0b|x08|x05|x1a|0|x1e|0|0|0|x01|x08|x01|x10|x88|x1
SF:|a|x0fInvalid|x20message|"x05HY000"Jxr(JavaRMI,g,"x05|0|0|0|x0b|x08|x0
SF:|5|x1a|0"Jxr(MMSRequest,g,"x05|0|0|0|x0b|x08|x05|x1a|0"Jxr(oracle-tns,3
SF:|2,"x05|0|0|0|x0b|x08|x05|x1a|0|x09|0|0|0|x01|x08|x01|x10|x88|x1a|x16Inva
SF:|lid|x20message-Frame.1"x05HY000"Jxr(ms-sql-s,g,"x05|0|0|0|x0b|x08|x0
SF:|5|x1a|0"Jxr(afp,28,"x05|0|0|0|x0b|x08|x05|x1a|0|x1e|0|0|0|x01|x08|x01|
SF:|x10|x88|x1a|x0fInvalid|x20message|"x05HY000");
MAC Address: 08:50:56:00:00:00 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: General purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 11|2022|10|Phone|2008|7|8.1|Vista (94%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008::spl cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_10:1511 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::opt
Aggressive OS guesses: Microsoft Windows 11 21H2 (94%), Microsoft Windows Server 2022 (90%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows Server 2008 SP1 (87%), Microsoft Windows Embedded Standard 7 (87%), Microsoft Windows 10 1703 (86%), Microsoft Windows 10 1607 (85%), Microsoft Windows 10 1511 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%)

```

```
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 11|2022|10|Phone|2008|7|8.1|Vista (94%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_10:1511 cpe:/o:microsoft:windows_8.1 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
Aggressive OS guesses: Microsoft Windows 11 21H2 (94%), Microsoft Windows Server 2022 (90%), Microsoft Windows 10 (90%), Microsoft Windows Phone 7.5 or 8.0 (88%), Microsoft Windows Server 2008 SP1 (87%), Microsoft Windows 7 (87%), Microsoft Windows 10 1703 (86%), Microsoft Windows 10 1607 (85%), Microsoft Windows 10 1511 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.182.2
Host is up (0.0000s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  dnsmasq 2.51
MAC Address: 00:50:56:F7:A8:22 (VMware)
Device type: specialized
Running: VMware Player
OS CPE: cpe:/a:vmware:player
OS details: VMware Player virtual NAT device
Network Distance: 1 hop

Nmap scan report for 192.168.182.254
Host is up (0.00043s latency).
All 65535 scanned ports on 192.168.182.254 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)
MAC Address: 00:50:56:F7:A8:DA (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 192.168.182.128
Host is up (0.00014s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.62 ((Debian))
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVNGE=43D=9/222OT=80XCT=1XCU=30117XPV=Y2DS=0XDC=L36=YXTM=68D1
OS:587DXP=x86_64-pc-linux-gnu)SEQ(SP=106XGCD=1XISR=109XTI=ZKCI=ZKII=ITTS=A)
OS:SEQ(SP=106XGCD=1XISR=10ASTI=ZKCI=ZKII=ITTS=A)OPS(OI=MF7D/ST11M7XQ2=MF7D
OS:ZST11M7XQ3=MF7D/NT11M7XQ4=MF7D/ST11M7XQ5=MF7D/ST11M7XQ6=MF7D/ST11M7
OS:1M7XQ7=82D0XQ8=82D0XQ9=82D0XQ10=82D0XQ11=82D0XQ12=82D0XQ13=82D0XQ14=82D0XQ15=82D0XQ16=82D0XQ17=82D0XQ18=82D0XQ19=82D0XQ20=82D0XQ21=82D0XQ22=82D0XQ23=82D0XQ24=82D0XQ25=82D0XQ26=82D0XQ27=82D0XQ28=82D0XQ29=82D0XQ30=82D0XQ31=82D0XQ32=82D0XQ33=82D0XQ34=82D0XQ35=82D0XQ36=82D0XQ37=82D0XQ38=82D0XQ39=82D0XQ40=82D0XQ41=82D0XQ42=82D0XQ43=82D0XQ44=82D0XQ45=82D0XQ46=82D0XQ47=82D0XQ48=82D0XQ49=82D0XQ50=82D0XQ51=82D0XQ52=82D0XQ53=82D0XQ54=82D0XQ55=82D0XQ56=82D0XQ57=82D0XQ58=82D0XQ59=82D0XQ60=82D0XQ61=82D0XQ62=82D0XQ63=82D0XQ64=82D0XQ65=82D0XQ66=82D0XQ67=82D0XQ68=82D0XQ69=82D0XQ70=82D0XQ71=82D0XQ72=82D0XQ73=82D0XQ74=82D0XQ75=82D0XQ76=82D0XQ77=82D0XQ78=82D0XQ79=82D0XQ80=82D0XQ81=82D0XQ82=82D0XQ83=82D0XQ84=82D0XQ85=82D0XQ86=82D0XQ87=82D0XQ88=82D0XQ89=82D0XQ90=82D0XQ91=82D0XQ92=82D0XQ93=82D0XQ94=82D0XQ95=82D0XQ96=82D0XQ97=82D0XQ98=82D0XQ99=82D0XQ100=82D0XQ101=82D0XQ102=82D0XQ103=82D0XQ104=82D0XQ105=82D0XQ106=82D0XQ107=82D0XQ108=82D0XQ109=82D0XQ110=82D0XQ111=82D0XQ112=82D0XQ113=82D0XQ114=82D0XQ115=82D0XQ116=82D0XQ117=82D0XQ118=82D0XQ119=82D0XQ120=82D0XQ121=82D0XQ122=82D0XQ123=82D0XQ124=82D0XQ125=82D0XQ126=82D0XQ127=82D0XQ128=82D0XQ129=82D0XQ130=82D0XQ131=82D0XQ132=82D0XQ133=82D0XQ134=82D0XQ135=82D0XQ136=82D0XQ137=82D0XQ138=82D0XQ139=82D0XQ140=82D0XQ141=82D0XQ142=82D0XQ143=82D0XQ144=82D0XQ145=82D0XQ146=82D0XQ147=82D0XQ148=82D0XQ149=82D0XQ150=82D0XQ151=82D0XQ152=82D0XQ153=82D0XQ154=82D0XQ155=82D0XQ156=82D0XQ157=82D0XQ158=82D0XQ159=82D0XQ160=82D0XQ161=82D0XQ162=82D0XQ163=82D0XQ164=82D0XQ165=82D0XQ166=82D0XQ167=82D0XQ168=82D0XQ169=82D0XQ170=82D0XQ171=82D0XQ172=82D0XQ173=82D0XQ174=82D0XQ175=82D0XQ176=82D0XQ177=82D0XQ178=82D0XQ179=82D0XQ180=82D0XQ181=82D0XQ182=82D0XQ183=82D0XQ184=82D0XQ185=82D0XQ186=82D0XQ187=82D0XQ188=82D0XQ189=82D0XQ190=82D0XQ191=82D0XQ192=82D0XQ193=82D0XQ194=82D0XQ195=82D0XQ196=82D0XQ197=82D0XQ198=82D0XQ199=82D0XQ200=82D0XQ201=82D0XQ202=82D0XQ203=82D0XQ204=82D0XQ205=82D0XQ206=82D0XQ207=82D0XQ208=82D0XQ209=82D0XQ210=82D0XQ211=82D0XQ212=82D0XQ213=82D0XQ214=82D0XQ215=82D0XQ216=82D0XQ217=82D0XQ218=82D0XQ219=82D0XQ220=82D0XQ221=82D0XQ222=82D0XQ223=82D0XQ224=82D0XQ225=82D0XQ226=82D0XQ227=82D0XQ228=82D0XQ229=82D0XQ230=82D0XQ231=82D0XQ232=82D0XQ233=82D0XQ234=82D0XQ235=82D0XQ236=82D0XQ237=82D0XQ238=82D0XQ239=82D0XQ240=82D0XQ241=82D0XQ242=82D0XQ243=82D0XQ244=82D0XQ245=82D0XQ246=82D0XQ247=82D0XQ248=82D0XQ249=82D0XQ250=82D0XQ251=82D0XQ252=82D0XQ253=82D0XQ254=82D0XQ255=82D0XQ256=82D0XQ257=82D0XQ258=82D0XQ259=82D0XQ260=82D0XQ261=82D0XQ262=82D0XQ263=82D0XQ264=82D0XQ265=82D0XQ266=82D0XQ267=82D0XQ268=82D0XQ269=82D0XQ270=82D0XQ271=82D0XQ272=82D0XQ273=82D0XQ274=82D0XQ275=82D0XQ276=82D0XQ277=82D0XQ278=82D0XQ279=82D0XQ280=82D0XQ281=82D0XQ282=82D0XQ283=82D0XQ284=82D0XQ285=82D0XQ286=82D0XQ287=82D0XQ288=82D0XQ289=82D0XQ290=82D0XQ291=82D0XQ292=82D0XQ293=82D0XQ294=82D0XQ295=82D0XQ296=82D0XQ297=82D0XQ298=82D0XQ299=82D0XQ300=82D0XQ301=82D0XQ302=82D0XQ303=82D0XQ304=82D0XQ305=82D0XQ306=82D0XQ307=82D0XQ308=82D0XQ309=82D0XQ310=82D0XQ311=82D0XQ312=82D0XQ313=82D0XQ314=82D0XQ315=82D0XQ316=82D0XQ317=82D0XQ318=82D0XQ319=82D0XQ320=82D0XQ321=82D0XQ322=82D0XQ323=82D0XQ324=82D0XQ325=82D0XQ326=82D0XQ327=82D0XQ328=82D0XQ329=82D0XQ330=82D0XQ331=82D0XQ332=82D0XQ333=82D0XQ334=82D0XQ335=82D0XQ336=82D0XQ337=82D0XQ338=82D0XQ339=82D0XQ340=82D0XQ341=82D0XQ342=82D0XQ343=82D0XQ344=82D0XQ345=82D0XQ346=82D0XQ347=82D0XQ348=82D0XQ349=82D0XQ350=82D0XQ351=82D0XQ352=82D0XQ353=82D0XQ354=82D0XQ355=82D0XQ356=82D0XQ357=82D0XQ358=82D0XQ359=82D0XQ360=82D0XQ361=82D0XQ362=82D0XQ363=82D0XQ364=82D0XQ365=82D0XQ366=82D0XQ367=82D0XQ368=82D0XQ369=82D0XQ370=82D0XQ371=82D0XQ372=82D0XQ373=82D0XQ374=82D0XQ375=82D0XQ376=82D0XQ377=82D0XQ378=82D0XQ379=82D0XQ380=82D0XQ381=82D0XQ382=82D0XQ383=82D0XQ384=82D0XQ385=82D0XQ386=82D0XQ387=82D0XQ388=82D0XQ389=82D0XQ390=82D0XQ391=82D0XQ392=82D0XQ393=82D0XQ394=82D0XQ395=82D0XQ396=82D0XQ397=82D0XQ398=82D0XQ399=82D0XQ400=82D0XQ401=82D0XQ402=82D0XQ403=82D0XQ404=82D0XQ405=82D0XQ406=82D0XQ407=82D0XQ408=82D0XQ409=82D0XQ410=82D0XQ411=82D0XQ412=82D0XQ413=82D0XQ414=82D0XQ415=82D0XQ416=82D0XQ417=82D0XQ418=82D0XQ419=82D0XQ420=82D0XQ421=82D0XQ422=82D0XQ423=82D0XQ424=82D0XQ425=82D0XQ426=82D0XQ427=82D0XQ428=82D0XQ429=82D0XQ430=82D0XQ431=82D0XQ432=82D0XQ433=82D0XQ434=82D0XQ435=82D0XQ436=82D0XQ437=82D0XQ438=82D0XQ439=82D0XQ440=82D0XQ441=82D0XQ442=82D0XQ443=82D0XQ444=82D0XQ445=82D0XQ446=82D0XQ447=82D0XQ448=82D0XQ449=82D0XQ450=82D0XQ451=82D0XQ452=82D0XQ453=82D0XQ454=82D0XQ455=82D0XQ456=82D0XQ457=82D0XQ458=82D0XQ459=82D0XQ460=82D0XQ461=82D0XQ462=82D0XQ463=82D0XQ464=82D0XQ465=82D0XQ466=82D0XQ467=82D0XQ468=82D0XQ469=82D0XQ470=82D0XQ471=82D0XQ472=82D0XQ473=82D0XQ474=82D0XQ475=82D0XQ476=82D0XQ477=82D0XQ478=82D0XQ479=82D0XQ480=82D0XQ481=82D0XQ482=82D0XQ483=82D0XQ484=82D0XQ485=82D0XQ486=82D0XQ487=82D0XQ488=82D0XQ489=82D0XQ490=82D0XQ491=82D0XQ492=82D0XQ493=82D0XQ494=82D0XQ495=82D0XQ496=82D0XQ497=82D0XQ498=82D0XQ499=82D0XQ500=82D0XQ501=82D0XQ502=82D0XQ503=82D0XQ504=82D0XQ505=82D0XQ506=82D0XQ507=82D0XQ508=82D0XQ509=82D0XQ510=82D0XQ511=82D0XQ512=82D0XQ513=82D0XQ514=82D0XQ515=82D0XQ516=82D0XQ517=82D0XQ518=82D0XQ519=82D0XQ520=82D0XQ521=82D0XQ522=82D0XQ523=82D0XQ524=82D0XQ525=82D0XQ526=82D0XQ527=82D0XQ528=82D0XQ529=82D0XQ530=82D0XQ531=82D0XQ532=82D0XQ533=82D0XQ534=82D0XQ535=82D0XQ536=82D0XQ537=82D0XQ538=82D0XQ539=82D0XQ540=82D0XQ541=82D0XQ542=82D0XQ543=82D0XQ544=82D0XQ545=82D0XQ546=82D0XQ547=82D0XQ548=82D0XQ549=82D0XQ550=82D0XQ551=82D0XQ552=82D0XQ553=82D0XQ554=82D0XQ555=82D0XQ556=82D0XQ557=82D0XQ558=82D0XQ559=82D0XQ560=82D0XQ561=82D0XQ562=82D0XQ563=82D0XQ564=82D0XQ565=82D0XQ566=82D0XQ567=82D0XQ568=82D0XQ569=82D0XQ570=82D0XQ571=82D0XQ572=82D0XQ573=82D0XQ574=82D0XQ575=82D0XQ576=82D0XQ577=82D0XQ578=82D0XQ579=82D0XQ580=82D0XQ581=82D0XQ582=82D0XQ583=82D0XQ584=82D0XQ585=82D0XQ586=82D0XQ587=82D0XQ588=82D0XQ589=82D0XQ590=82D0XQ591=82D0XQ592=82D0XQ593=82D0XQ594=82D0XQ595=82D0XQ596=82D0XQ597=82D0XQ598=82D0XQ599=82D0XQ600=82D0XQ601=82D0XQ602=82D0XQ603=82D0XQ604=82D0XQ605=82D0XQ606=82D0XQ607=82D0XQ608=82D0XQ609=82D0XQ610=82D0XQ611=82D0XQ612=82D0XQ613=82D0XQ614=82D0XQ615=82D0XQ616=82D0XQ617=82D0XQ618=82D0XQ619=82D0XQ620=82D0XQ621=82D0XQ622=82D0XQ623=82D0XQ624=82D0XQ625=82D0XQ626=82D0XQ627=82D0XQ628=82D0XQ629=82D0XQ630=82D0XQ631=82D0XQ632=82D0XQ633=82D0XQ634=82D0XQ635=82D0XQ636=82D0XQ637=82D0XQ638=82D0XQ639=82D0XQ640=82D0XQ641=82D0XQ642=82D0XQ643=82D0XQ644=82D0XQ645=82D0XQ646=82D0XQ647=82D0XQ648=82D0XQ649=82D0XQ650=82D0XQ651=82D0XQ652=82D0XQ653=82D0XQ654=82D0XQ655=82D0XQ656=82D0XQ657=82D0XQ658=82D0XQ659=82D0XQ660=82D0XQ661=82D0XQ662=82D0XQ663=82D0XQ664=82D0XQ665=82D0XQ666=82D0XQ667=82D0XQ668=82D0XQ669=82D0XQ670=82D0XQ671=82D0XQ672=82D0XQ673=82D0XQ674=82D0XQ675=82D0XQ676=82D0XQ677=82D0XQ678=82D0XQ679=82D0XQ680=82D0XQ681=82D0XQ682=82D0XQ683=82D0XQ684=82D0XQ685=82D0XQ686=82D0XQ687=82D0XQ688=82D0XQ689=82D0XQ690=82D0XQ691=82D0XQ692=82D0XQ693=82D0XQ694=82D0XQ695=82D0XQ696=82D0XQ697=82D0XQ698=82D0XQ699=82D0XQ700=82D0XQ701=82D0XQ702=82D0XQ703=82D0XQ704=82D0XQ705=82D0XQ706=82D0XQ707=82D0XQ708=82D0XQ709=82D0XQ710=82D0XQ711=82D0XQ712=82D0XQ713=82D0XQ714=82D0XQ715=82D0XQ716=82D0XQ717=82D0XQ718=82D0XQ719=82D0XQ720=82D0XQ721=82D0XQ722=82D0XQ723=82D0XQ724=82D0XQ725=82D0XQ726=82D0XQ727=82D0XQ728=82D0XQ729=82D0XQ730=82D0XQ731=82D0XQ732=82D0XQ733=82D0XQ734=82D0XQ735=82D0XQ736=82D0XQ737=82D0XQ738=82D0XQ739=82D0XQ740=82D0XQ741=82D0XQ742=82D0XQ743=82D0XQ744=82D0XQ745=82D0XQ746=82D0XQ747=82D0XQ748=82D0XQ749=82D0XQ750=82D0XQ751=82D0XQ752=82D0XQ753=82D0XQ754=82D0XQ755=82D0XQ756=82D0XQ757=82D0XQ758=82D0XQ759=82D0XQ760=82D0XQ761=82D0XQ762=82D0XQ763=82D0XQ764=82D0XQ765=82D0XQ766=82D0XQ767=82D0XQ768=82D0XQ769=82D0XQ770=82D0XQ771=82D0XQ772=82D0XQ773=82D0XQ774=82D0XQ775=82D0XQ776=82D0XQ777=82D0XQ778=82D0XQ779=82D0XQ780=82D0XQ781=82D0XQ782=82D0XQ783=82D0XQ784=82D0XQ785=82D0XQ786=82D0XQ787=82D0XQ788=82D0XQ789=82D0XQ790=82D0XQ791=82D0XQ792=82D0XQ793=82D0XQ794=82D0XQ795=82D0XQ796=82D0XQ797=82D0XQ798=82D0XQ799=82D0XQ800=82D0XQ801=82D0XQ802=82D0XQ803=82D0XQ804=82D0XQ805=82D0XQ806=82D0XQ807=82D0XQ808=82D0XQ809=82D0XQ810=82D0XQ811=82D0XQ812=82D0XQ813=82D0XQ814=82D0XQ815=82D0XQ816=82D0XQ817=82D0XQ818=82D0XQ819=82D0XQ820=82D0XQ821=82D0XQ822=82D0XQ823=82D0XQ824=82D0XQ825=82D0XQ826=82D0XQ827=82D0XQ828=82D0XQ829=82D0XQ830=82D0XQ831=82D0XQ832=82D0XQ833=82D0XQ834=82D0XQ835=82D0XQ836=82D0XQ837=82D0XQ838=82D0XQ839=82D0XQ840=82D0XQ841=82D0XQ842=82D0XQ843=82D0XQ844=82D0XQ845=82D0XQ846=82D0XQ847=82D0XQ848=82D0XQ849=82D0XQ850=82D0XQ851=82D0XQ852=82D0XQ853=82D0XQ854=82D0XQ855=82D0XQ856=82D0XQ857=82D0XQ858=82D0XQ859=82D0XQ860=82D0XQ861=82D0XQ862=82D0XQ863=82D0XQ864=82D0XQ865=82D0XQ866=82D0XQ867=82D0XQ868=82D0XQ869=82D0XQ870=82D0XQ871=82D0XQ872=82D0XQ873=82D0XQ874=82D0XQ875=82D0XQ876=82D0XQ877=82D0XQ878=82D0XQ879=82D0XQ880=82D0XQ881=82D0XQ882=82D0XQ883=82D0XQ884=82D0XQ885=82D0XQ886=82D0XQ887=82D0XQ888=82D0XQ889=82D0XQ890=82D0XQ891=82D0XQ892=82D0XQ893=82D0XQ894=82D0XQ895=82D0XQ896=82D0XQ897=82D0XQ898=82D0XQ899=82D0XQ900=82D0XQ901=82D0XQ902=82D0XQ903=82D0XQ904=82D0XQ905=82D0XQ906=82D0XQ907=82D0XQ908=82D0XQ909=82D0XQ910=82D0XQ911=82D0XQ912=82D0XQ913=82D0XQ914=82D0XQ915=82D0XQ916=82D0XQ917=82D0XQ918=82D0XQ919=82D0XQ920=82D0XQ921=82D0XQ922=82D0XQ923=82D0XQ924=82D0XQ925=82D0XQ926=82D0XQ927=82D0XQ928=82D0XQ929=82D0XQ930=82D0XQ931=82D0XQ932=82D0XQ933=82D0XQ934=82D0XQ935=82D0XQ936=82D0XQ937=82D0XQ938=82D0XQ939=82D0XQ940=82D0XQ941=82D0XQ942=82D0XQ943=82D0XQ944=82D0XQ945=82D0XQ946=82D0XQ947=82D0XQ948=82D0XQ949=82D0XQ950=82D0XQ951=82D0XQ952=82D0XQ953=82D0XQ954=82D0XQ955=82D0XQ956=82D0XQ957=82D0XQ958=82D0XQ959=82D0XQ960=82D0XQ961=82D0XQ962=82D0XQ963=82D0XQ964=82D0XQ965=82D0XQ966=82D0XQ967=82D0XQ968=82D0XQ969=82D0XQ970=82D0XQ971=82D0XQ972=82D0XQ973=82D0XQ974=82D0XQ975=82D0XQ976=82D0XQ977=82D0XQ978=82D0XQ979=82D0XQ980=82D0XQ981=82D0XQ982=82D0XQ983=82D0XQ984=82D0XQ985=82D0XQ986=82D0XQ987=82D0XQ988=82D0XQ989=82D0XQ990=82D0XQ991=82D0XQ992=82D0XQ993=82D0XQ994=82D0XQ995=82D0XQ996=82D0XQ997=82D0XQ998=82D0XQ999=82D0XQ1000=82D0XQ1001=82D0XQ1002=82D0XQ1003=82D0XQ1004=82D0XQ1005=82D0XQ1006=82D0XQ1007=82D0XQ1008=82D0XQ1009=82D0XQ1010=82D0XQ1011=82D0XQ1012=82D0XQ1013=82D0XQ1014=82D0XQ1015=82D0XQ1016=82D0XQ1017=82D0XQ1018=82D0XQ1019=82D0XQ1020=82D0XQ1021=82D0XQ1022=82D0XQ1023=82D0XQ1024=82D0XQ1025=82D0XQ1026=82D0XQ1027=82D0XQ1028=82D0XQ1029=82D0XQ1030=82D0XQ1031=82D0XQ1032=82D0XQ1033=82D0XQ1034=82D0XQ1035=82D0XQ1036=82D0XQ1037=82D0XQ1038=82D0XQ1039=82D0XQ1040=82D0XQ1041=82D0XQ1042=82D0XQ1043=82D0XQ1044=82D0XQ1045=82D0XQ1046=82D0XQ1047=82D0XQ1048=82D0XQ1049=82D0XQ1050=82D0XQ1051=82D0XQ1052=82D0XQ1053=82D0XQ1054=82D0XQ1055=82D0XQ1056=82D0XQ1057=82D0XQ1058=82D0XQ1059=82D0XQ1060=82D0XQ1061=82D0XQ1062=82D0XQ1063=82D0XQ1064=82D0XQ1065=82D0XQ1066=82D0XQ1067=82D0XQ1068=82D0XQ1069=82D0XQ1070=82D0XQ1071=82D0XQ1072=82D0XQ1073=82D0XQ1074=82D0XQ1075=82D0XQ1076=82D0XQ1077=82D0XQ1078=82D0XQ1079=82D0XQ1080=82D0XQ1081=82D0XQ1082=82D0XQ1083=82D0XQ1084=82D0XQ1085=82D0XQ1086=82D0XQ1087=82D0XQ1088=82D0XQ1089=82D0XQ1090=82D0XQ1091=82D0XQ1092=82D0XQ1093=82D0XQ1094=82D0XQ1095=82D0XQ1096=82D0XQ1097=82D0XQ1098=82D0XQ1099=82D0XQ1100=82D0XQ1101=82D0XQ1102=82D0XQ1103=82D0XQ1104=82D0XQ1105=82D0XQ1106=82D0XQ1107=82D0XQ1108=82D0XQ1109=82D0XQ1110=82D0XQ1111=82D0XQ1112=82D0XQ1113=82D0XQ1114=82D0XQ1115=82D0XQ1116=82D0XQ1117=82D0XQ1118=82D0XQ1119=82D0XQ1120=82D0XQ1121=82D0XQ1122=82D0XQ1123=82D0XQ1124=82D0XQ1125=82D0XQ1126=82D0XQ1127=82D0XQ1128=82D0XQ1129=82D0XQ1130=82D0XQ1131=82D0XQ1132=82D0XQ1133=82D0XQ1134=82D0XQ1135=82D0XQ1136=82D0XQ1137=82D0XQ1138=82D0XQ1139=82D0XQ1140=82
```



```
root@kali: ~/Desktop
root@kali: ~/Desktop237x54

(root@kali) ~/Desktop
# less ~/nmap_fullscan.nmap

zsh: suspended less ~/nmap_fullscan.nmap

(root@kali) ~/Desktop
# grep "Nmap scan report for" ~/nmap_fullscan.nmap | wc -l
4

(root@kali) ~/Desktop
# grep "open" ~/nmap_fullscan.nmap | wc -l
9

(root@kali) ~/Desktop
# nmap -n -sS -sV -p!-1024 -T4 -oN ~/nmap_noping.nmap 192.168.182.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-22 10:10 EDT
Found no matches for the service mask 'l-1024' and your specified protocols
QUITTING!

(root@kali) ~/Desktop
# tcpdump -i eth0 -w ~/scan_capture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C38 packets captured
38 packets received by filter
0 packets dropped by kernel

(root@kali) ~/Desktop
# wireshark ~/scan_capture.pcap &
[3] 26759

(root@kali) ~/Desktop
# nmap -sS 192.168.182.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-22 10:40 EDT
Nmap scan report for 192.168.182.1
Host is up (0.0013s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.182.2
Host is up (0.00034s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:FA:67:22 (VMware)

Nmap scan report for 192.168.182.254
Host is up (0.00038s latency).
All 1000 scanned ports on 192.168.182.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F7:A8:DA (VMware)
```

```
root@kali: ~/Desktop
root@kali: ~/Desktop237x54

root@kali)~/Desktop
# nmap -Pn -sS -sV -p1-1024 -T4 -oN ~/map.noping.nmap 192.168.182.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-22 10:16 EDT
Found no matches for the service mask '1-1024' and your specified protocols
QUITTING!

root@kali)~/Desktop
# tcpdump -i eth0 -w ~/scan_capture.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C38 packets captured
38 packets received by filter
0 packets dropped by kernel

root@kali)~/Desktop
# wireshark ~/scan_capture.pcap &
[3] 26759

root@kali)~/Desktop
# nmap -sS 192.168.182.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-22 10:40 EDT
Nmap scan report for 192.168.182.1
Host is up (0.0013s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.182.2
Host is up (0.00034s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:FA:67:22 (VMware)

Nmap scan report for 192.168.182.254
Host is up (0.00038s latency).
All 1000 scanned ports on 192.168.182.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F7:A8:DA (VMware)

Nmap scan report for 192.168.182.128
Host is up (0.00013s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 256 IP addresses (4 hosts up) scanned in 8.75 seconds

root@kali)~/Desktop
#
```