

```
Kali (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Apps Places
Aug 4 20:53
root@kali: /home/kali
root@kali: /home/kali
root@kali: /home/kali

cat: AggressiveScan-Results.txt: No such file or directory

(root@kali)-[/home/kali]
# 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 08:00:27:20:6d:14 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.113/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
        valid_lft 84689sec preferred_lft 84689sec
    inet6 fe80::a00:27ff:fe20:6d14/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(root@kali)-[/home/kali]
# sudo nmap -A 192.168.0.113/24 -oN AggressiveScan-Results.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 20:45 IST
Nmap scan report for 192.168.0.1
Host is up (0.017s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  tcpwrapped
MAC Address: CC:2D:21:EB:DA:80 (Tenda Technology,Ltd.Dongguan branch)
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   17.00 ms  192.168.0.1
```

Kali (Snapshot 1) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Apps Places

Aug 4 20:53

5% 41% ↑ 27 kB ↓ 0.0 kB

root@kali: /home/kali

root@kali: /home/kali

root@kali: /home/kali

```
(root@kali)-[/home/kali]
# sudo nmap -A 192.168.0.113/24 -oN AggressiveScan-Results.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-04 20:45 IST
Nmap scan report for 192.168.0.1
Host is up (0.017s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  tcpwrapped
MAC Address: CC:2D:21:EB:DA:80 (Tenda Technology,Ltd.Dongguan branch)
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS match for host
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   17.00 ms  192.168.0.1

Nmap scan report for 192.168.0.100
Host is up (0.00016s latency).
All 1000 scanned ports on 192.168.0.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: C0:35:32:50:6A:23 (Liteon Technology)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1   0.16 ms  192.168.0.100

Nmap scan report for 192.168.0.106
Host is up (0.0056s latency).
All 1000 scanned ports on 192.168.0.106 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

```
Kali (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Aug 4 20:54
root@kali: /home/kali
root@kali: /home/kali
root@kali: /home/kali

Device type: general purpose|media device|specialized
Running: Microsoft Windows 10|11|2016, Microsoft Xbox 360, NTI embedded
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2016 cpe:/h:microsoft:xbox_360_kernel
OS details: Microsoft Windows 10 - 11, Microsoft Windows Server 2016, Microsoft Xbox 360 Dashboard, NTI E-MICRO-TRHP temperature sensor
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 5.57 ms 192.168.0.106

Nmap scan report for 192.168.0.107
Host is up (0.020s latency).
All 1000 scanned ports on 192.168.0.107 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: EA:BB:3C:8A:23:56 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|media device|specialized
Running: Microsoft Windows 10|11|2016, Microsoft Xbox 360, NTI embedded
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2016 cpe:/h:microsoft:xbox_360_kernel
OS details: Microsoft Windows 10 - 11, Microsoft Windows Server 2016, Microsoft Xbox 360 Dashboard, NTI E-MICRO-TRHP temperature sensor
Network Distance: 1 hop

TRACEROUTE
HOP RTT ADDRESS
1 20.02 ms 192.168.0.107

Nmap scan report for 192.168.0.114
Host is up (0.00060s latency).
Not shown: 977 closed tcp ports (reset)
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
```



```
Kali (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Aug 4 20:54
root@kali: /home/kali
root@kali: /home/kali
root@kali: /home/kali

ftp-syst:
STAT:
FTP server status:
  Connected to 192.168.0.113
  Logged in as ftp
  TYPE: ASCII
  No session bandwidth limit
  Session timeout in seconds is 300
  Control connection is plain text
  Data connections will be plain text
  vsFTPD 2.3.4 - secure, fast, stable
_End of status
22/tcp open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp open  telnet       Linux telnetd
25/tcp open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_ ssl-date: 2025-08-04T15:19:32+00:00; -17s from scanner time.
|_ smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp open  domain       ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_ http-title: Metasploitable2 - Linux
111/tcp open  rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000    2                111/tcp    rpcbind
|   100000    2                111/udp    rpcbind
```

```
Kali (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Aug 4 20:55
root@kali: /home/kali
root@kali: /home/kali
root@kali: /home/kali

| 100005 1,2,3 34735/tcp mountd
| 100005 1,2,3 51985/udp mountd
| 100021 1,3,4 34224/tcp nlockmgr
| 100021 1,3,4 43719/udp nlockmgr
| 100024 1 46096/tcp status
| 100024 1 49098/udp status
|_ 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
|_ 445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
|_ 512/tcp open exec netkit-rsh rexecd
|_ 513/tcp open login?
|_ 514/tcp open shell Netkit rshd
|_ 1099/tcp open java-rmi GNU Classpath grmiregistry
|_ 1524/tcp open bindshell Metasploitable root shell
|_ 2049/tcp open nfs 2-4 (RPC #100003)
|_ 2121/tcp open ftp ProFTPD 1.3.1
|_ 3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
|_ mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 8
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsCompression, Speaks41ProtocolNew, LongColumnFlag, ConnectWithDatabase, SupportsTransactions, SwitchToSSLAfterHandshake
|   Status: Autocommit
|   Salt: 5A67#H"l}PU<k*,;%Fr.
|_ 5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ ssl-date: 2025-08-04T15:19:32+00:00; -18s from scanner time.
|_ ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Not valid before: 2010-03-17T14:07:45
|_ Not valid after: 2010-04-16T14:07:45
|_ 5900/tcp open vnc VNC (protocol 3.3)
|_ vnc-info:
|   Protocol version: 3.3
|   Security types:
```

Kali (Snapshot 1) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Aug 4 20:55

24% 41% ↑ 28 kB ↓ 0.0 kB

root@kali: /home/kali

root@kali: /home/kali

root@kali: /home/kali

```
| Protocol version: 3.3
| Security types:
|_ VNC Authentication (2)
6000/tcp open  X11          (access denied)
6667/tcp open  irc            UnrealIRCd
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown       Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
MAC Address: 08:00:27:46:F7:F9 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 59m43s, deviation: 2h00m01s, median: -17s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|   System time: 2025-08-04T11:18:55-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
|_smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge response: supported
```


