## 🔍 Network Scanning Report

**Target IP**: 192.168.0.102 (Metasploitable2)
**Tool Used**: nmap -A -T4 192.168.0.102
**Scan Type**: Aggressive scan (OS detection, version detection, script scanning, traceroute)

---

### ✅ 1. Ping Results

The target is **online** and responded to ICMP echo requests with **0% packet loss**:

| Metric | Value |
|---|---|
| Packets Sent | 4 |
| Packets Received | 4 |
| RTT Min | 1.22 ms |
| RTT Avg | 1.80 ms |
| RTT Max | 2.47 ms |

---

### 📊 2. Open Ports & Services

| Port | State | Service | Version/Notes |
|---|---|---|---|
| 21 | open | FTP | vsftpd 2.3.4 (Anonymous login allowed) |
| 22 | open | SSH | OpenSSH 4.7p1 (Debian) |
| 23 | open | Telnet | Linux telnetd |
| 25 | open | SMTP | Postfix (SSLv2 supported) |
| 53 | open | DNS | BIND 9.4.2 |
| 80 | open | HTTP | Apache 2.2.8 (Ubuntu) |
| 111 | open | RPC | rpcbind 2 |
| 139 | open | NetBIOS | Samba smbd (WORKGROUP) |

| Port | State | Service | Version/Notes |
|---|---|---|---|
| 445 | open | SMB | Samba 3.0.20-Debian |
| 512 | open | exec | netkit-rsh rexecd |
| 513 | open | login | - |
| 514 | open | tcpwrapped | - |
| 1099 | open | Java RMI | GNU Classpath grmiregistry |
| 1524 | open | Bind Shell | Metasploitable root shell |
| 2049 | open | NFS | Version 2-4 |
| 2121 | open | FTP | ProFTPD 1.3.1 |
| 3306 | open | MySQL | v5.0.51a |
| 5432 | open | PostgreSQL | 8.3.0 - 8.3.7 |
| 5900 | open | VNC | Protocol 3.3 |
| 6000 | open | X11 | Access denied |
| 6667 | open | IRC | UnrealIRCd |
| 8009 | open | AJP13 | Apache Jserv Protocol v1.3 |
| 8180 | open | HTTP | Apache Tomcat 5.5 (Coyote JSP engine) |

---

### 🧠 3. OS & Host Info

| Field | Value |
|---|---|
| OS Detected | Linux 2.6.9 - 2.6.33 |
| Hostname | metasploitable.localdomain |
| NetBIOS Name | METASPLOITABLE |
| MAC Address | 08:00:27:EE:48:04 (VirtualBox) |
| Distance | 1 hop |

---

🛑 **4. Vulnerability Indicators**

- **Anonymous FTP Access** (port 21)
- **Outdated OpenSSH** and **Postfix SMTP** with SSLv2 support
- **Remote Shells** open on ports like 512, 513, 1524
- **Databases exposed**: MySQL (3306), PostgreSQL (5432)
- **Tomcat Manager** possibly accessible on port 8180
- **SMB signing disabled** (insecure)
- **Public IRC server** (6667 UnrealIRCd)
- **Known vulnerable services** used for CTF/pentesting practice

---

🌐 **5. Traceroute**

Only **1 hop** detected — target is on the **same local network**.

---

# RAW REPORT :

┌──(virus㉿virus)-[~]

└─$ ping 192.168.0.102

PING 192.168.0.102 (192.168.0.102) 56(84) bytes of data.

64 bytes from 192.168.0.102: icmp_seq=1 ttl=64 time=2.47 ms

64 bytes from 192.168.0.102: icmp_seq=2 ttl=64 time=1.58 ms

64 bytes from 192.168.0.102: icmp_seq=3 ttl=64 time=1.92 ms

64 bytes from 192.168.0.102: icmp_seq=4 ttl=64 time=1.22 ms

^C

--- 192.168.0.102 ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 3439ms

rtt min/avg/max/mdev = 1.215/1.797/2.474/0.463 ms

```
┌──(virus㉿virus)-[~]
└─$ nmap -A -T4 192.168.0.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 09:57 EDT
Nmap scan report for 192.168.0.102
Host is up (0.0015s 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:
| FTP server status:
|      Connected to 192.168.0.101
|      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

|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2_DES_64_CBC_WITH_MD5

| SSL2_RC4_128_WITH_MD5

| SSL2_RC2_128_CBC_WITH_MD5

| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

| SSL2_DES_192_EDE3_CBC_WITH_MD5

|_ SSL2_RC4_128_EXPORT40_WITH_MD5

| 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: 2025-07-30T13:58:24+00:00; +7s from scanner time.

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-title: Metasploitable2 - Linux

|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2

111/tcp open rpcbind 2 (RPC #100000)

| rpcinfo:

```
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      45263/udp   mountd
|   100005  1,2,3      50817/tcp   mountd
|   100021  1,3,4      33383/tcp   nlockmgr
|   100021  1,3,4      53308/udp   nlockmgr
|   100024  1          52899/udp   status
|_  100024  1          60340/tcp   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  tcpwrapped
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, SwitchToSSLAfterHandshake, SupportsTransactions, LongColumnFlag, Speaks41ProtocolNew, ConnectWithDatabase, SupportsCompression

| Status: Autocommit

|_ Salt: #ga2p`q7]MJlb%1f/U@"

5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7

| 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: 2025-07-30T13:58:24+00:00; +7s from scanner time.

5900/tcp open vnc VNC (protocol 3.3)

| vnc-info:

| Protocol version: 3.3

| Security types:

|_ VNC Authentication (2)

6000/tcp open X11 (access denied)

6667/tcp open irc UnrealIRCd

| irc-info:

| users: 1

| servers: 1

| lusers: 1

| lservers: 0

| server: irc.Metasploitable.LAN

| version: Unreal3.2.8.1. irc.Metasploitable.LAN

| uptime: 0 days, 0:06:11

| source ident: nmap

| source host: C80EEC81.F0D9233E.FFFA6D49.IP

|_ error: Closing Link: zmovurxoy[192.168.0.101] (Quit: zmovurxoy)

8009/tcp open ajp13 Apache Jserv (Protocol v1.3)

|_ajp-methods: Failed to get a valid response for the OPTION request

8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1

|_http-title: Apache Tomcat/5.5

|_http-favicon: Apache Tomcat

|_http-server-header: Apache-Coyote/1.1

MAC Address: 08:00:27:EE:48:04 (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: 1h00m07s, deviation: 2h00m00s, median: 6s

|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

| smb-security-mode:

| account_used: <blank>

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

|_smb2-time: Protocol negotiation failed (SMB2)

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|_ System time: 2025-07-30T09:58:16-04:00

TRACEROUTE

HOP RTT ADDRESS

1 1.52 ms 192.168.0.102

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 23.24 seconds