Nmap Scan Report - Scanned at Thu Jan 16 22:09:10 2025

Port State (toggle closed [0] | filtered [0]) Service Reason Product Version Extra info 21 tcp open ftp syn-ack vsftpd 2.3.4   ftp-anon

```
Anonymous FTP login allowed (FTP code 230)
```

ftp-syst

```
  STAT:
FTP server status:
     Connected to 192.168.50.101
     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 syn-ack 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 syn-ack Linux telnetd   25 tcp open smtp syn-ack Postfix smtpd   smtp-commands

```
metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
```

53 tcp open domain syn-ack ISC BIND 9.4.2   dns-nsid

```
  bind.version: 9.4.2
```

80 tcp open http syn-ack 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 syn-ack 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      38107/tcp   mountd
100005  1,2,3      49853/udp   mountd
100021  1,3,4      57306/tcp   nlockmgr
100021  1,3,4      60067/udp   nlockmgr
100024  1          38654/udp   status
100024  1          49984/tcp   status
```

139 tcp open netbios-ssn syn-ack Samba smbd 3.X - 4.X workgroup: WORKGROUP 445 tcp open netbios-ssn syn-ack Samba smbd 3.0.20-Debian workgroup: WORKGROUP 512 tcp open exec syn-ack netkit-rsh rexecd   513 tcp open login syn-ack   514 tcp open shell syn-ack Netkit rshd   1099 tcp open java-rmi syn-ack GNU Classpath grmiregistry   1524 tcp open bindshell syn-ack Metasploitable root shell   2049 tcp open nfs syn-ack 2-4 RPC #100003 2121 tcp open ftp syn-ack ProFTPD 1.3.1   3306 tcp open mysql syn-ack MySQL 5.0.51a-3ubuntu5   mysql-info

```
Protocol: 10
Version: 5.0.51a-3ubuntu5
Thread ID: 369
Capabilities flags: 43564
Some Capabilities: Support41Auth, ConnectWithDatabase, SwitchToSSLAfterHandshake, SupportsTransactions, LongColumnFlag, SupportsCompression, Speaks41ProtocolNew
Status: Autocommit
Salt: Q)t15V3;n<ztY>j|Q]_F
```

5432 tcp open postgresql syn-ack 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

```
2025-01-16T21:12:15+00:00; +1m48s from scanner time.
```

5900 tcp open vnc syn-ack VNC   protocol 3.3 vnc-info

```
Protocol version: 3.3
Security types:
  VNC Authentication (2)
```

6000 tcp open X11 syn-ack   access denied 6667 tcp open irc syn-ack UnrealIRCd   8009 tcp open ajp13 syn-ack Apache Jserv   Protocol v1.3 ajp-methods

```
Failed to get a valid response for the OPTION request
```

8180 tcp open http syn-ack Apache Tomcat/Coyote JSP engine 1.1   http-favicon

```
Apache Tomcat
```

http-title

```
Apache Tomcat/5.5
```