```
┌──(kali123㉿kali)-[~]
└─$ nmap -sC -sV 192.168.207.133
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-24 22:17 IST
Nmap scan report for 192.168.207.133
Host is up (0.0017s 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 192.168.207.132
|      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
```

| 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

| sslv2:

| SSLv2 supported

| ciphers:

| SSL2_RC4_128_WITH_MD5

| SSL2_RC4_128_EXPORT40_WITH_MD5

| SSL2_DES_64_CBC_WITH_MD5

| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5

| SSL2_DES_192_EDE3_CBC_WITH_MD5

|_   SSL2_RC2_128_CBC_WITH_MD5

|_ssl-date: 2026-02-24T16:48:19+00:00; +2s 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   34710/udp   mountd

| 100005 1,2,3   50083/tcp   mountd

| 100021 1,3,4   46411/tcp   nlockmgr

| 100021 1,3,4 60404/udp nlockmgr

| 100024 1 46829/udp status

|_ 100024 1 58661/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 OpenBSD or Solaris rlogind

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: SupportsCompression, SwitchToSSLAfterHandshake, SupportsTransactions, Speaks41ProtocolNew, LongColumnFlag, Support41Auth, ConnectWithDatabase

| Status: Autocommit

|_ Salt: N3S)nsur][/y6=qD?OO|

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: 2026-02-24T16:48:19+00:00; +3s 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, 0:06:01

| source ident: nmap

| source host: A23ACDD5.EFDF92B4.FFFA6D49.IP

|_ error: Closing Link: fjwaxywlh[192.168.207.132] (Quit: fjwaxywlh)

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-favicon: Apache Tomcat

|_http-title: Apache Tomcat/5.5

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

MAC Address: 00:0C:29:36:EC:05 (VMware)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:

| smb-os-discovery:

| OS: Unix (Samba 3.0.20-Debian)

| Computer name: metasploitable

| NetBIOS computer name:

| Domain name: localdomain

| FQDN: metasploitable.localdomain

|_ System time: 2026-02-24T11:48:10-05:00

|_smb2-time: Protocol negotiation failed (SMB2)

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

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

|_clock-skew: mean: 1h15m02s, deviation: 2h30m00s, median: 2s

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

Nmap done: 1 IP address (1 host up) scanned in 22.64 seconds