



```
Metasploitable

metasploitable:~$ tree
tree: command not found

metasploitable:~$ ifconfig
Link encap:Ethernet HWaddr 7a:dd:4f:0c:8c:eb
inet addr:192.168.1.101 Bcast:192.168.1.255 M
inet6 addr: fe80::78dd:4fff:fe0c:8ceb/64 Scope:
UP BROADCAST RUNNING MULTICAST MTU:1500 Metri
RX packets:464 errors:0 dropped:0 overruns:0 fr
TX packets:133 errors:0 dropped:0 overruns:0 ca
collisions:0 txqueuelen:1000
RX bytes:42932 (41.9 KB) TX bytes:17258 (16.8
Base address:0xc000 Memory:febc0000-febe0000

Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:139 errors:0 dropped:0 overruns:0 fr
TX packets:139 errors:0 dropped:0 overruns:0 ca
collisions:0 txqueuelen:0
RX bytes:42153 (41.1 KB) TX bytes:42153 (41.1

metasploitable:~$ _
```

Kali Linux 2023

kali@kali: ~

File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.1.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-29 12:21 PDT
Nmap scan report for 192.168.1.101 (192.168.1.101)
Host is up (0.00070s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?        192.168.1.101
513/tcp   open  login        192.168.1.11
514/tcp   open  tcpwrapped   192.168.1.101
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
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 7A:DD:4F:0C:8C:EB (Unknown)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE
: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 63.57 seconds

(kali@kali)-[~]
$
```