```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:33:b7:33
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe33:b733/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5737 (5.6 KB)  TX bytes:3924 (3.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        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:109 errors:0 dropped:0 overruns:0 frame:0
          TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27661 (27.0 KB)  TX bytes:27661 (27.0 KB)

msfadmin@metasploitable:~$
```

metasploitable2 ip;
192.168.56.102

```
$ ip a
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 08:00:27:74:ae:89 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.103/24 brd 192.168.56.255 scope global dynamic eth0
       valid_lft 356sec preferred_lft 356sec
    inet6 fe80::a00:27ff:fe74:ae89/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
$
```

kali linux ip;
192.168.56.103

```
$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=1.17 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.503 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.418 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=0.396 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.412 ms
64 bytes from 192.168.56.102: icmp_seq=6 ttl=64 time=0.390 ms
64 bytes from 192.168.56.102: icmp_seq=7 ttl=64 time=0.470 ms
64 bytes from 192.168.56.102: icmp_seq=8 ttl=64 time=0.355 ms
64 bytes from 192.168.56.102: icmp_seq=9 ttl=64 time=0.409 ms
64 bytes from 192.168.56.102: icmp_seq=10 ttl=64 time=0.399 ms
64 bytes from 192.168.56.102: icmp_seq=11 ttl=64 time=0.602 ms
64 bytes from 192.168.56.102: icmp_seq=12 ttl=64 time=0.446 ms
64 bytes from 192.168.56.102: icmp_seq=13 ttl=64 time=0.564 ms
64 bytes from 192.168.56.102: icmp_seq=14 ttl=64 time=0.392 ms
64 bytes from 192.168.56.102: icmp_seq=15 ttl=64 time=0.444 ms
64 bytes from 192.168.56.102: icmp_seq=16 ttl=64 time=0.527 ms
64 bytes from 192.168.56.102: icmp_seq=17 ttl=64 time=0.442 ms
64 bytes from 192.168.56.102: icmp_seq=18 ttl=64 time=0.384 ms
64 bytes from 192.168.56.102: icmp_seq=19 ttl=64 time=0.415 ms
64 bytes from 192.168.56.102: icmp_seq=20 ttl=64 time=0.434 ms
64 bytes from 192.168.56.102: icmp_seq=21 ttl=64 time=0.369 ms
64 bytes from 192.168.56.102: icmp_seq=22 ttl=64 time=0.480 ms
64 bytes from 192.168.56.102: icmp_seq=23 ttl=64 time=0.471 ms
64 bytes from 192.168.56.102: icmp_seq=24 ttl=64 time=0.541 ms
64 bytes from 192.168.56.102: icmp_seq=25 ttl=64 time=0.405 ms
64 bytes from 192.168.56.102: icmp_seq=26 ttl=64 time=0.444 ms
64 bytes from 192.168.56.102: icmp_seq=27 ttl=64 time=0.484 ms
64 bytes from 192.168.56.102: icmp_seq=28 ttl=64 time=0.515 ms
64 bytes from 192.168.56.102: icmp_seq=29 ttl=64 time=0.427 ms
64 bytes from 192.168.56.102: icmp_seq=30 ttl=64 time=0.450 ms
64 bytes from 192.168.56.102: icmp_seq=31 ttl=64 time=0.474 ms
64 bytes from 192.168.56.102: icmp_seq=32 ttl=64 time=0.385 ms
64 bytes from 192.168.56.102: icmp_seq=33 ttl=64 time=0.383 ms
64 bytes from 192.168.56.102: icmp_seq=34 ttl=64 time=0.413 ms
64 bytes from 192.168.56.102: icmp_seq=35 ttl=64 time=0.536 ms
64 bytes from 192.168.56.102: icmp_seq=36 ttl=64 time=0.700 ms
```

```
$ nmap -sn 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-26 14:57 EDT
Nmap scan report for 192.168.56.1
Host is up (0.00041s latency).
MAC Address: 0A:00:27:00:00:0E (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.0013s latency).
MAC Address: 08:00:27:4F:C2:C5 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00096s latency).
MAC Address: 08:00:27:33:B7:33 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 28.16 seconds
```

live hosts and their ip
192.168.56.1

192.168.56.100

192.168.56.102

192.168.56.103

```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:33:B7:33 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 14.20 seconds
```

```
open ports top 5;
21/tcp ftp
22/tcp ssh
23/tcp telnet
25/tcp smtp
80/tcp http
```

```
$ nmap -sV 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-26 15:12 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00042s 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        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
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
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: 08:00:27:33:B7:33 (Oracle VirtualBox virtual NIC)
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 25.71 seconds
```

```
open ports version top 5;
21/tcp ftp   vsftpd 2.3.4
22/tcp ssh   OpenSSH 4.7p1
23/tcp telnet   Linux telneted
25/tcp  smtp   Postfix smtpd
80/tcp   http   Apache httpf 2.2.8
```

```
$ nmap -O 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-26 15:23 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00054s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:33:B7:33 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.82 seconds
```

```
operating system;
Linux 2.6.9 - 2.6.33
```

```
$ nc 192.168.56.102 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Sat, 26 Apr 2025 19:44:37 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html
```

```
$ nc 192.168.56.102 21
220 (vsFTPd 2.3.4)
```

```
http
server; Apache/2.2.8
ftp
220 (vsFTPd 2.3.4)
```