

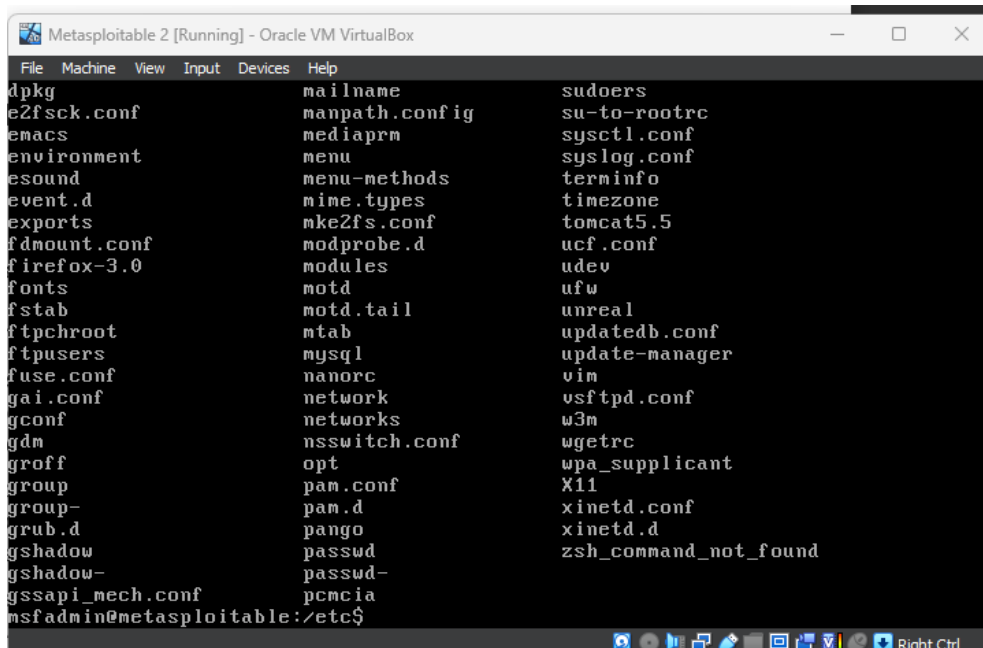
Metasploitable 2

INTERNSHIP

MICHELLE PANTELOURIS

Task 1


To locate the etc directory '`cd /etc`' is used. Once in the command '`ls`' is used to list all of the files within etc.



```
Metasploitable 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
dpkg mailname sudoers
e2fsck.conf manpath.config su-to-rootrc
emacs mediaprm sysctl.conf
environment menu syslog.conf
esound menu-methods terminfo
event.d mime.types timezone
exports nke2fs.conf tomcat5.5
fdmount.conf modprobe.d ucf.conf
firefox-3.0 modules udev
fonts motd ufw
fstab motd.tail unreal
ftprchroot ntab updatedb.conf
ftpusers mysql update-manager
fuse.conf nanorc vim
gai.conf network vsftpd.conf
gconf networks w3m
gdm nsswitch.conf wgetrc
groff opt wpa_supplicant
group pam.conf X11
group- pam.d xinetd.conf
grub.d pango xinetd.d
gshadow passwd zsh_command_not_found
gshadow- passwd-
gssapi_mech.conf pcmcia
msfadmin@metasploitable:/etc$
```

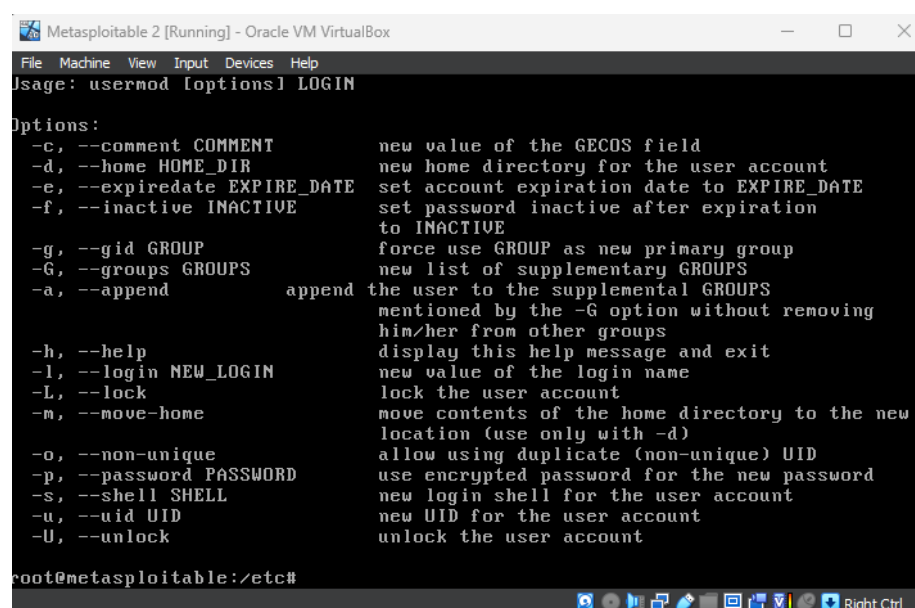
Task 2

To create a new user and password '`useradd -d /home/intern -p password secure123`' is used.



```
passwd: unknown user secure123
root@metasploitable:/etc# useradd -d /home/intern -p password secure123
root@metasploitable:/etc#
```

To add it to the sudo group '`sudo usermod -aG intern`' is used.



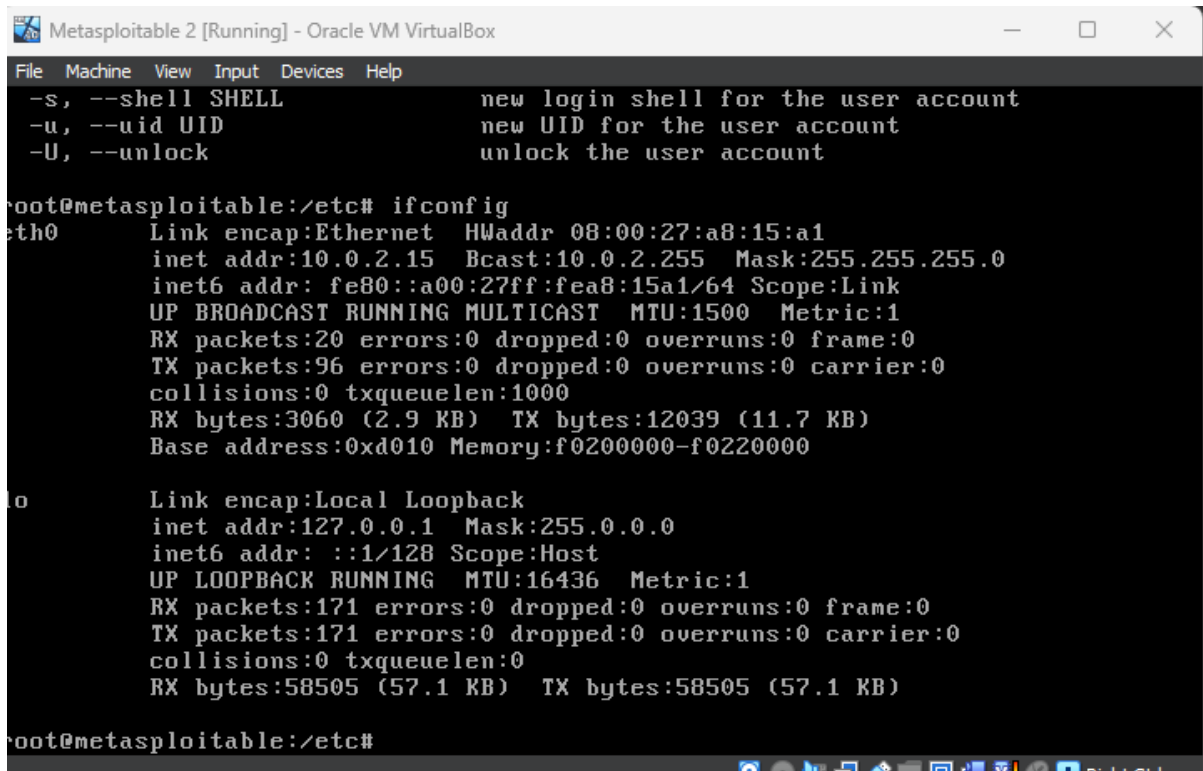
```
Metasploitable 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Usage: usermod [options] LOGIN

Options:
  -c, --comment COMMENT      new value of the GECOS field
  -d, --home HOME_DIR        new home directory for the user account
  -e, --expiredate EXPIRE_DATE set account expiration date to EXPIRE_DATE
  -f, --inactive INACTIVE    set password inactive after expiration
                              to INACTIVE
  -g, --gid GROUP            force use GROUP as new primary group
  -G, --groups GROUPS        new list of supplementary GROUPS
  -a, --append               append the user to the supplemental GROUPS
                              mentioned by the -G option without removing
                              him/her from other groups
  -h, --help                 display this help message and exit
  -l, --login NEW_LOGIN      new value of the login name
  -L, --lock                 lock the user account
  -m, --move-home            move contents of the home directory to the new
                              location (use only with -d)
  -o, --non-unique            allow using duplicate (non-unique) UID
  -p, --password PASSWORD    use encrypted password for the new password
  -s, --shell SHELL          new login shell for the user account
  -u, --uid UID              new UID for the user account
  -U, --unlock               unlock the user account

root@metasploitable:/etc#
```

Task 3

To identify the IP Address of the Metasploitable machine '*ifconfig*' is used.



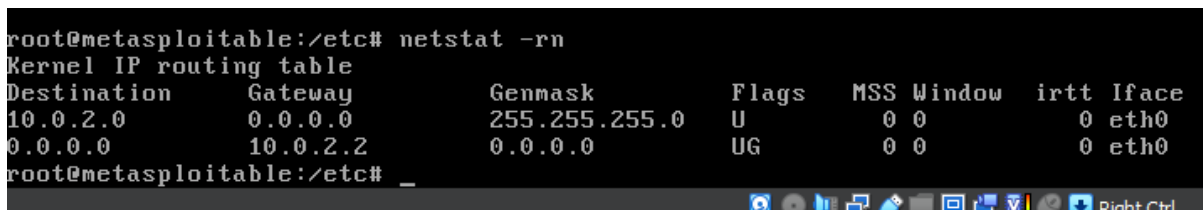
```
Metasploitable 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
-s, --shell SHELL          new login shell for the user account
-u, --uid UID              new UID for the user account
-U, --unlock              unlock the user account

root@metasploitable:/etc# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a8:15:a1
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea8:15a1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:96 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3060 (2.9 KB)  TX bytes:12039 (11.7 KB)
          Base address:0xd010 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:171 errors:0 dropped:0 overruns:0 frame:0
          TX packets:171 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:58505 (57.1 KB)  TX bytes:58505 (57.1 KB)

root@metasploitable:/etc#
```

To check the routing table, '*netstat -rn*' is used.



```
root@metasploitable:/etc# netstat -rn
Kernel IP routing table
Destination      Gateway         Genmask         Flags        MSS Window  irtt  Iface
10.0.2.0         0.0.0.0        255.255.255.0   U           0 0        0     eth0
0.0.0.0         10.0.2.2      0.0.0.0         UG          0 0        0     eth0

root@metasploitable:/etc#
```

Task 4

To identify packages, 'Dpkg -list' is used.

```
i xserver-xorg-v 1:2.8.3-2ubunt X.Org X server -- NSC Geode GX1 display driv
i xserver-xorg-v 1:2.1.8-1ubunt X.Org X server -- NV display driver
i xserver-xorg-v 1:0.2.901-0ubu X.Org X server -- VIA display driver
i xserver-xorg-v 0.2.1-1ubuntu3 2D graphics driver for Poulsbo
i xserver-xorg-v 1:4.1.3.dfsg.1 X.Org X server -- Rendition display driver
i xserver-xorg-v 1:0.5.0-4 X.Org X server -- legacy S3 display driver
i xserver-xorg-v 1:1.9.1-7 X.Org X server -- S3 ViRGE display driver
i xserver-xorg-v 1:2.1.3-5 X.Org X server -- Savage display driver
i xserver-xorg-v 1:1.5.1-3 X.Org X server -- SiliconMotion display driv
i xserver-xorg-v 1:0.9.3-6 X.Org X server -- SiS display driver
i xserver-xorg-v 1:0.8.1-9 X.Org X server -- SiS USB display driver
i xserver-xorg-v 1:1.3.0-6 X.Org X server -- tdfx display driver
i xserver-xorg-v 1:1.1.0-9ubunt X.Org X server -- TGA display driver
i xserver-xorg-v 1:1.2.4-1 X.Org X server -- Trident display driver
i xserver-xorg-v 1:1.1.1-4 X.Org X server -- Tseng display driver
i xserver-xorg-v 1:0.1.1-6ubunt X.Org X server -- Video 4 Linux display driv
i xserver-xorg-v 1:1.3.0-4ubunt X.Org X server -- VESA display driver
i xserver-xorg-v 1:4.1.0-8 X.Org X server -- VGA display driver
i xserver-xorg-v 1:0.2.2-5 X.Org X server -- VIA display driver
i xserver-xorg-v 1:10.15.2-1ubu X.Org X server -- VMware display driver
i xserver-xorg-v 1:1.1.1-5 X.Org X server -- Voodoo display driver
i xterm 229-1ubuntu1.1 X terminal emulator
i zlib1g 1:1.2.3.3.dfsg compression library - runtime
i zlib1g-dev 1:1.2.3.3.dfsg compression library - development
root@metasploitable:~/home/msfadmin# _
```

For example, we can see firefox 3.6.17 is installed, which has a plethora of vulnerabilities, listed here:

<https://www.mozilla.org/en-US/security/advisories/mfsa2011-22/>

root@metasploitable: ~ x	root@kali: /home/kali x	root@kali: /home/kali x
ii diffstat	1.45-2	produces graph of changes introduced by a diff file
ii distcc	2.18.3-4.1ubuntu1	Simple distributed compiler client and server
ii dmidecode	2.9-1ubuntu1	Dump Desktop Management Interface data
ii dmsetup	2:1.02.20-2ubuntu2	The Linux Kernel Device Mapper userspace library
ii dnsutils	1:9.4.2-10	Clients provided with BIND
ii dosfstools	2.11-2.3ubuntu1	Utilities to create and check MS-DOS FAT filesystems
ii dpkg	1.14.16.6ubuntu3	package maintenance system for Debian
ii dpkg-dev	1.14.16.6ubuntu4.1	package building tools for Debian
ii e2fslibs	1.40.8-2ubuntu2	ext2 filesystem libraries
ii e2fsprogs	1.40.8-2ubuntu2	ext2 file system utilities and libraries
ii ecj	3.3.0+0728-5	standalone version of the Eclipse Java compiler
ii ecj-gcj	3.3.0+0728-5	standalone version of the Eclipse Java compiler (native version)
ii ed	0.7-1ubuntu1	The classic unix line editor
ii eject	2.1.5-6	ejects CDs and operates CD-Changers under Linux
ii esound-common	0.2.38-0ubuntu9	Enlightened Sound Daemon - Common files
ii eterm	0.9.4.0debian1-2ubuntu3	Enlightened Terminal Emulator
ii ethtool	6-0	display or change ethernet card settings
ii fakeroot	1.9ubuntu1.1	Gives a fake root environment
ii fastjar	2:0.95-1ubuntu2	Jar creation utility
ii fdutils	5.5-20060227-1.1	Linux floppy utilities
ii figlet	2.2.2-1ubuntu1	Frank, Ian & Glenn's Letters
ii file	4.21-3	Determines file type using "magic" numbers
ii filezilla	3.0.11.1-0ubuntu1-hardy1	Port of the famous Win32 graphical FTP client
ii filezilla-common	3.0.11.1-0ubuntu1-hardy1	Architecture independent files for filezilla
ii findutils	4.2.32-1ubuntu2	utilities for finding files--find, xargs
ii firefox	3.6.17+build3+nobinonly-0ubuntu0.8.04.1	safe and easy web browser from Mozilla
ii firefox-3.0	3.6.17+build3+nobinonly-0ubuntu0.8.04.1	dummy upgrade package for firefox-3.0 -> firefox
ii firefox-branding	3.6.17+build3+nobinonly-0ubuntu0.8.04.1	Package that ships the firefox branding
ii fluxbox	1.1.1-1-hardy1	Highly configurable and low resource X11 Window manager
ii fontconfig	2.5.0-2ubuntu3	generic font configuration library - support binaries
ii fontconfig-config	2.5.0-2ubuntu3	generic font configuration library - configuration
ii friendly-recovery	0.1	Make recovery more user-friendly
ii ftp	0.17-16build1	The FTP client
rc ftpd	0.17-27	FTP server
ii fuse-utils	2.7.2-1ubuntu2	Filesystem in Userspace (utilities)

Task 5

Ps - aux will show us the running services:

```

root@metasploitable:/home/msfadmin# ps -aux
Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
USER          PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.0  2844  1692 ?        Ss   07:03   0:00 /sbin/init
root           2  0.0  0.0      0   0 ?        Ss   07:03   0:00 [kthreadd]
root           3  0.0  0.0      0   0 ?        Ss   07:03   0:00 [migration/0]
root           4  0.0  0.0      0   0 ?        Ss   07:03   0:00 [ksoftirqd/0]
root           5  0.0  0.0      0   0 ?        Ss   07:03   0:00 [watchdog/0]
root           6  0.0  0.0      0   0 ?        Ss   07:03   0:00 [events/0]
root           7  0.0  0.0      0   0 ?        Ss   07:03   0:00 [khelper]
root          41  0.0  0.0      0   0 ?        Ss   07:03   0:00 [kblockd/0]
root          44  0.0  0.0      0   0 ?        Ss   07:03   0:00 [kacpid]
root          45  0.0  0.0      0   0 ?        Ss   07:03   0:00 [kacpi_notify]
root          88  0.0  0.0      0   0 ?        Ss   07:03   0:00 [kseriod]
root         126  0.0  0.0      0   0 ?        Ss   07:03   0:00 [pdflush]
root         127  0.0  0.0      0   0 ?        Ss   07:03   0:00 [pdflush]
root         128  0.0  0.0      0   0 ?        Ss   07:03   0:00 [kswapd0]
root         170  0.0  0.0      0   0 ?        Ss   07:03   0:00 [aio/0]
root        1126  0.0  0.0      0   0 ?        Ss   07:03   0:00 [ksnapd]
root        1324  0.0  0.0      0   0 ?        Ss   07:03   0:00 [ata/0]
root        1327  0.0  0.0      0   0 ?        Ss   07:03   0:00 [ata_aux]
root        2005  0.0  0.0      0   0 ?        Ss   07:03   0:00 [scsi_eh_0]
root        2006  0.0  0.0      0   0 ?        Ss   07:03   0:00 [scsi_eh_1]
root        2218  0.0  0.0      0   0 ?        Ss   07:03   0:00 [kjournald]
root        2372  0.0  0.0  2092   620 ?        Ss   07:03   0:00 /sbin/udevd --daemon
root        2568  0.0  0.0      0   0 ?        Ss   07:03   0:00 [kpsmouse]
root        3477  0.0  0.0      0   0 ?        Ss   07:03   0:00 [kjournald]
daemon        3646  0.0  0.0  1836   524 ?        Ss   07:03   0:00 /sbin/portmap
statd         3662  0.0  0.0  1900   724 ?        Ss   07:03   0:00 /sbin/rpc.statd
root        3668  0.0  0.0      0   0 ?        Ss   07:03   0:00 [rpciod/0]
root        3683  0.0  0.0  3648   564 ?        Ss   07:03   0:00 /usr/sbin/rpc.idmapd
root        3909  0.0  0.0  1716   488 tty4      Ss+  07:03   0:00 /sbin/getty 38400 tty4
root        3910  0.0  0.0  1716   488 tty5      Ss+  07:03   0:00 /sbin/getty 38400 tty5
root        3916  0.0  0.0  1716   484 tty2      Ss+  07:03   0:00 /sbin/getty 38400 tty2
root        3919  0.0  0.0  1716   492 tty3      Ss+  07:03   0:00 /sbin/getty 38400 tty3
root        3922  0.0  0.0  1716   492 tty6      Ss+  07:03   0:00 /sbin/getty 38400 tty6
syslog        3958  0.0  0.0  1936   644 ?        Ss   07:03   0:00 /sbin/syslogd -u syslog
root        3993  0.0  0.0  1872   540 ?        Ss   07:03   0:00 /bin/dd bs 1 if /proc/kmsg of /var/run/klogd/kmsg
klog          3995  0.0  0.1  3284  2100 ?        Ss   07:03   0:00 /sbin/klogd -P /var/run/klogd/kmsg
bind          4010  0.0  0.3  35400  7680 ?        Ssl  07:03   0:00 /usr/sbin/named -u bind
root        4117  0.0  0.0  2768  1308 ?        Ss   07:03   0:00 /bin/sh /usr/bin/mysqld_safe
mysql         4159  0.0  0.8 127560 17024 ?        Sl   07:03   0:00 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --user=mysql --pid-file=/var/run/mysqld/mysqld.pid --skip-external
root        4161  0.0  0.0  1700   560 ?        Ss   07:03   0:00 logger -p daemon.err -t mysqld_safe -i -t mysqld
postgres     4238  0.0  0.2  41340  5068 ?        Ss   07:03   0:00 /usr/lib/postgresql/8.3/bin/postgres -D /var/lib/postgresql/8.3/main -c config_file=/etc/postgresql/8.3/main/postgresql.conf
postgres     4241  0.0  0.0  41340  1376 ?        Ss   07:03   0:00 postgres: writer process
postgres     4242  0.0  0.0  41340  1188 ?        Ss   07:03   0:00 postgres: wal writer process
postgres     4243  0.0  0.0  41340  1384 ?        Ss   07:03   0:00 postgres: autovacuum launcher process
postgres     4244  0.0  0.0  12660  1128 ?        Ss   07:03   0:00 postgres: stats collector process
daemon       4264  0.0  0.0  2316   420 ?        Ss   07:03   0:00 distccd --daemon --user daemon --allow 0.0.0.0/0

```

We can restart the apache web service using the command below:

`/etc/init.d/apache2 restart`

```

root@metasploitable:/home/msfadmin# /etc/init.d/apache2 restart
* Restarting web server apache2
... done.
root@metasploitable:/home/msfadmin#

```

Task 6

`/etc/shadow` should be as follows:

```

root@metasploitable:/home/msfadmin# exit
exit
msfadmin@metasploitable:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
msfadmin@metasploitable:~$ ls -la /etc/shadow
-rw-r----- 1 root shadow 1273 2024-02-08 12:36 /etc/shadow
msfadmin@metasploitable:~$

```

The permissions should be set to 600, which is achievable by using the following command: `'chmod /etc/shadow 600'`

Task 7

```
# cat script.sh
#!/bin/bash

set -x
warning: Never expose this VM to an untrusted network!

VAR1=$(df / | grep / | awk '{ print $5}' | sed 's/%//g')
THRESHOLD=80
echo "VAR1=$VAR1, THRESHOLD=$THRESHOLD"
if [ "$VAR1" -gt "$THRESHOLD" ] ; then
mail -s 'Disk Space Alert' michelle@EMAILREDACTED << EOF
Disk space is running low
EOF
fi
```

Task 8

Run an nmap scan using Kali Linux or similar. The commands would be as follows:

nmap -p- -T5 -sCV (TCP scan)

```
(root@kali)-[/home/kali]
# nmap -p- -T5 -sV 192.168.0.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-10 07:52 EST
Nmap scan report for 192.168.0.122
Host is up (0.000060s latency).
Not shown: 65506 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
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 rshcd
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
3632/tcp  open  distccd  distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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 (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc      UnrealIRCd (Admin email admin@Metasploitable.LAN)
8009/tcp  open  ajp13    Apache Jserv (Protocol v1.3)
8180/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb      Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
32849/tcp open  status   1 (RPC #100024)
40284/tcp open  mountd   1-3 (RPC #100005)
43735/tcp open  nlockmgr 1-4 (RPC #100021)
50331/tcp open  java-rmi  GNU Classpath grmiregistry
MAC Address: 08:00:27:A8:15:A1 (Oracle VirtualBox virtual NIC)
Service Info: Host: metasploitable.localdomain; 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 127.60 seconds
```

nmap -p- -T5 -sCVU (UDP scan)

Any ports that are open and need to be closed can be closed using ufw. For example if we need to close SSH (port 22) we can use:

```
ufw deny 22/tcp
ufw deny 22/udp
```

```
root@metasploitable:~# ufw deny 22/tcp
Rules updated
root@metasploitable:~# ufw deny 22/udp
Rules updated
root@metasploitable:~#
```