241356-89

UNIVERSITY of GREENWICH

Course	COMP1691: Enterprise Server Mngt & Sec	Course School/Level	H/UG
Coursework	COMP1691 Logbook	Assessment Weight	50.00%
Tutor	M Pelc	Submission Deadline	15/11/2018

Logbook comprising of weekly uploads

Coursework is receipted on the understanding that it is the student's own work and that it has not, in whole or part, been presented elsewhere for assessment. Where material has been used from other sources it has been properly acknowledged in accordance with the University's Regulations regarding Cheating and Plagiarism.

000725619

Tutor's comments

Grade Awarded___________ ***For Office Use Only***__________ ***Final Grade***_________

Moderation required: *yes/no* ***Tutor***_______________________ ***Date*** ________________

Contents

Group number 29

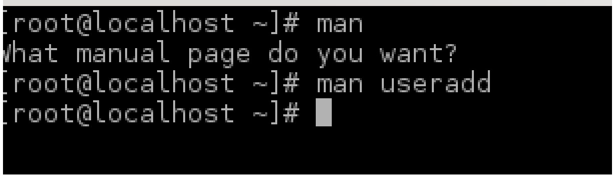
001033505

001032949

000725619

LAB 1

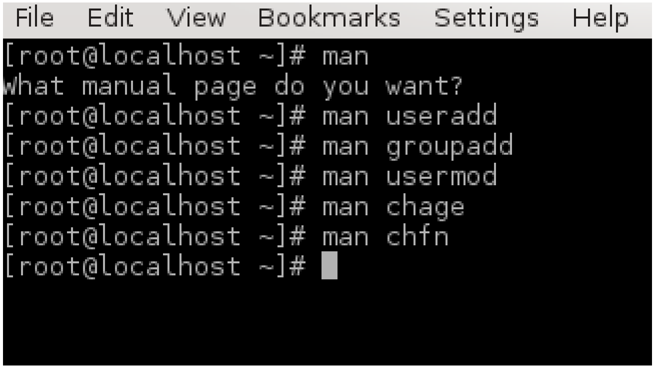
EXERCISE



```
[root@localhost ~]# man
What manual page do you want?
[root@localhost ~]# man useradd
[root@localhost ~]# 
```

Figure 1

The man program was working fine I did not have to install it.



```
[root@localhost ~]# man
What manual page do you want?
[root@localhost ~]# man useradd
[root@localhost ~]# man groupadd
[root@localhost ~]# man usermod
[root@localhost ~]# man chage
[root@localhost ~]# man chfn
[root@localhost ~]# 
```

Figure 2

I was able to view how the commands in figure 2 are used for different things on the system.

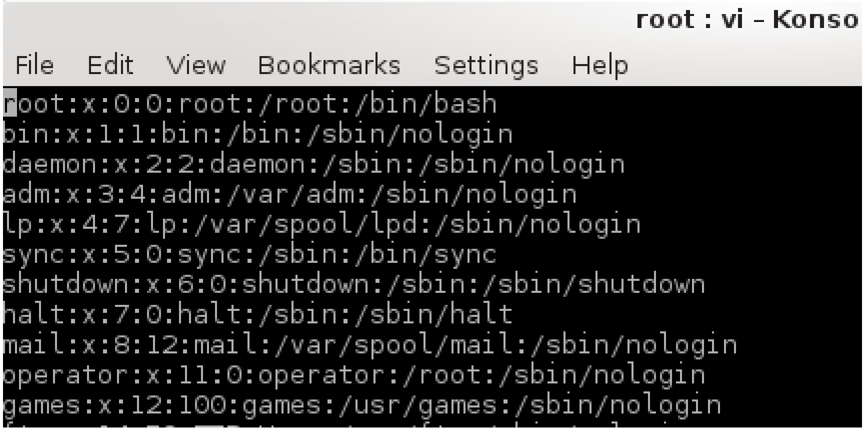
Useradd: is used to create accounts. It also creates a group with the same name in the background.

Groupadd: is used to create groups on the system.

Usermod: modifies some information about a user account.

Chage: is used to change the account aging information.

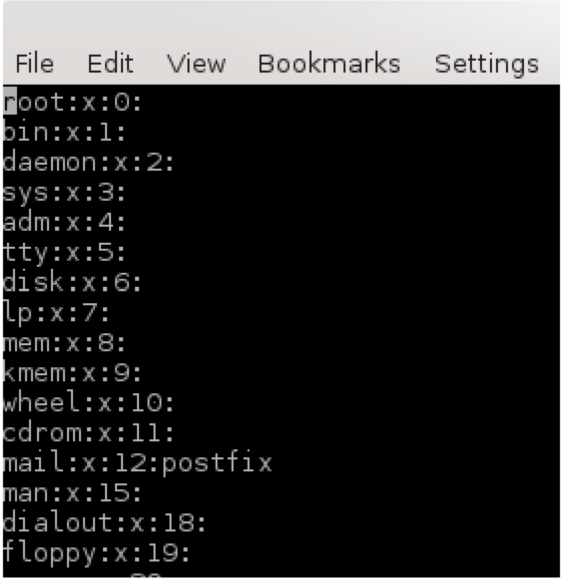
Chfn: is used to change finger information like full names and phone numbers.



```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
```

Figure 3

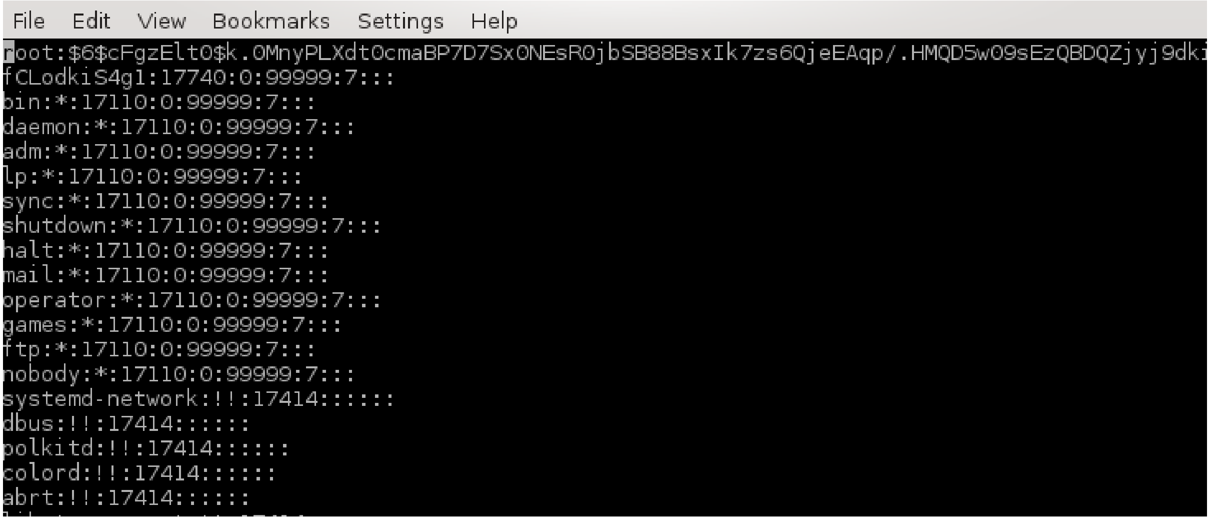
The /etc/passwd file is used to keep user information for accounts in the following order; username, password, user id, group id, finger information, home directory and shell.



```
root:x:0:
bin:x:1:
daemon:x:2:
sys:x:3:
adm:x:4:
tty:x:5:
disk:x:6:
lp:x:7:
mem:x:8:
kmem:x:9:
wheel:x:10:
cdrom:x:11:
mail:x:12:postfix
man:x:15:
dialout:x:18:
floppy:x:19:
```

Figure 4

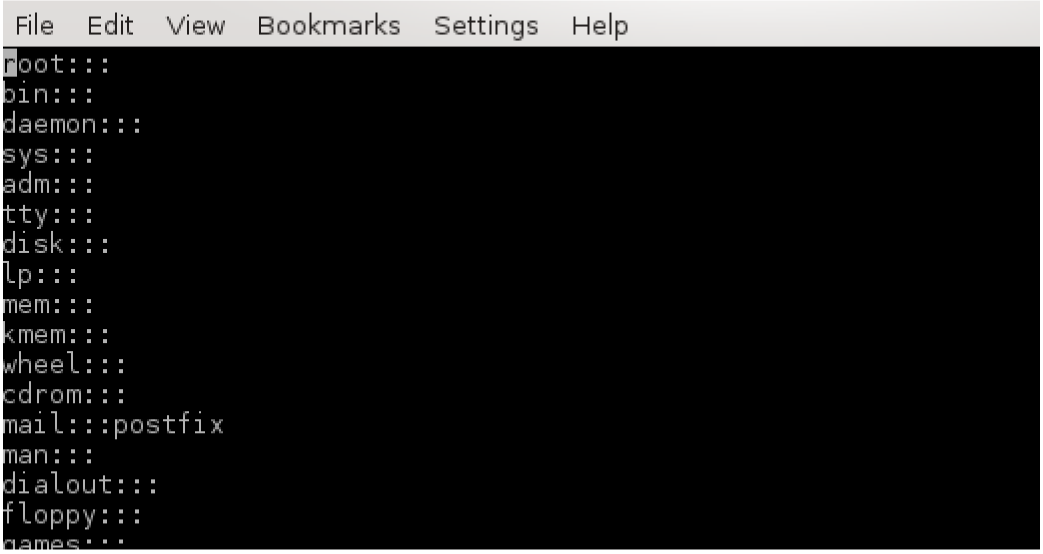
The /etc/group file is used to keep group information in the following order; group name, password, group id and members.



```
root:$6$cFgzElt0$k.0MnyPLXdt0cmaBP7D7Sx0NEsR0jbSB88BsxIk7zs6QjeEAqp/.HMQD5w09sEzQBDQZjyj9dki
fCLodkiS4g1:17740:0:99999:7:::
bin:*:17110:0:99999:7:::
daemon:*:17110:0:99999:7:::
adm:*:17110:0:99999:7:::
lp:*:17110:0:99999:7:::
sync:*:17110:0:99999:7:::
shutdown:*:17110:0:99999:7:::
halt:*:17110:0:99999:7:::
mail:*:17110:0:99999:7:::
operator:*:17110:0:99999:7:::
games:*:17110:0:99999:7:::
ftp:*:17110:0:99999:7:::
nobody:*:17110:0:99999:7:::
systemd-network:!!:17414::::::
dbus:!!:17414::::::
polkitd:!!:17414::::::
colord:!!:17414::::::
abrt:!!:17414::::::
```

Figure 5

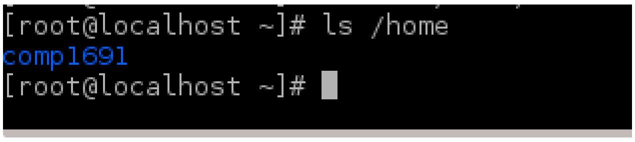
The /etc/shadow is used to keep password information for user accounts in the following order username, password, password change, minimum days, maximum days, warning days, inactive days and expiry.



```
root:::
bin:::
daemon:::
sys:::
adm:::
tty:::
disk:::
lp:::
mem:::
kmem:::
wheel:::
cdrom:::
mail:::postfix
man:::
dialout:::
floppy:::
games:::
```

Figure 6

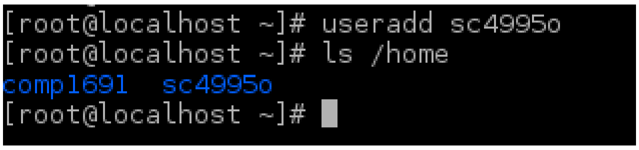
The /etc/gshadow stores password information for groups in the order; group, password, admin, members.



```
[root@localhost ~]# ls /home
comp1691
[root@localhost ~]#
```

Figure 7

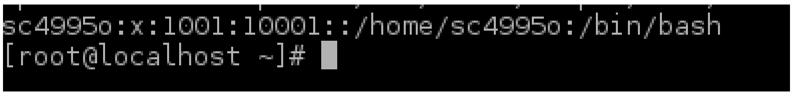
The /home directory contained the folders for users except root.



```
[root@localhost ~]# useradd sc49950
[root@localhost ~]# ls /home
comp1691  sc49950
[root@localhost ~]#
```

Figure 8

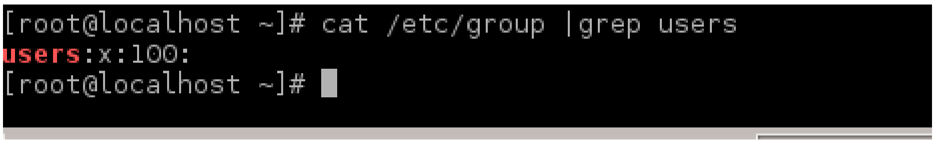
We added the user account and checked to see if the folder was added to the directory.



```
sc49950:x:1001:10001::/home/sc49950:/bin/bash
[root@localhost ~]#
```

Figure 9

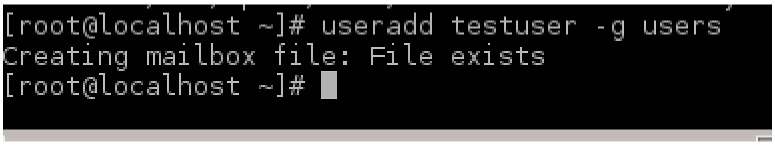
The /etc/passwd file was also updated as shown above.



```
[root@localhost ~]# cat /etc/group |grep users
users:x:100:
[root@localhost ~]#
```

Figure 10

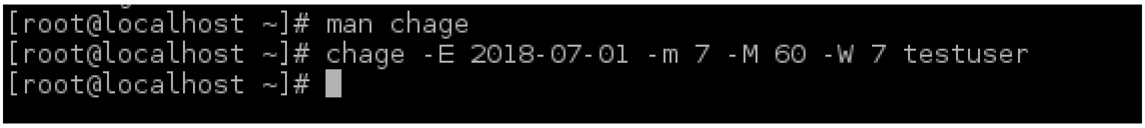
The users group was existing.



```
[root@localhost ~]# useradd testuser -g users
Creating mailbox file: File exists
[root@localhost ~]#
```

Figure 11

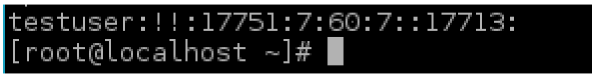
The user account was added and set the users group as the initial group.



```
[root@localhost ~]# man chage
[root@localhost ~]# chage -E 2018-07-01 -m 7 -M 60 -W 7 testuser
[root@localhost ~]#
```

Figure 12

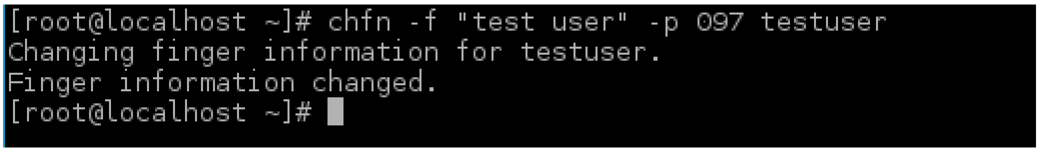
I was able to change the account aging information.



```
testuser:!!:17751:7:60:7::17713:
[root@localhost ~]#
```

Figure 13

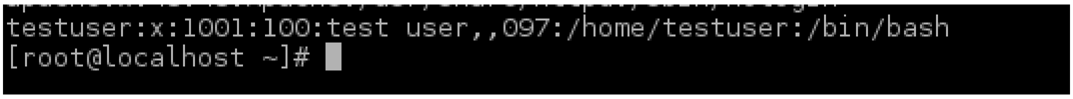
The /etc/shadow file was updated as shown above seeing the different places the numbers were inserted.



```
[root@localhost ~]# chfn -f "test user" -p 097 testuser
Changing finger information for testuser.
Finger information changed.
[root@localhost ~]#
```

Figure 14

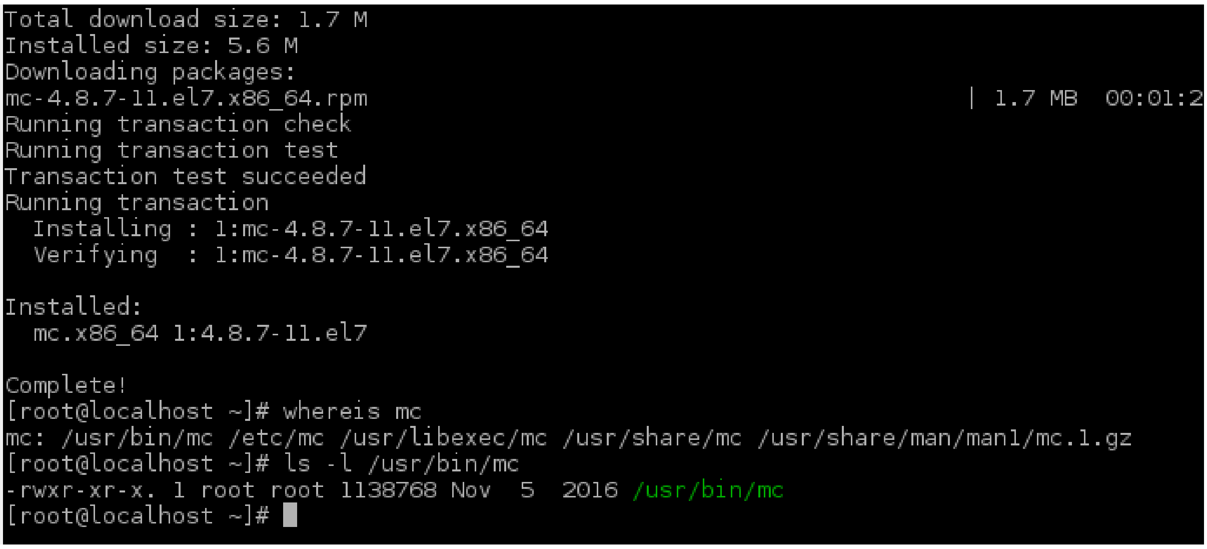
I was able to add finger information to the testuser account.



```
testuser:x:1001:100:test user,,097:/home/testuser:/bin/bash
[root@localhost ~]#
```

Figure 15

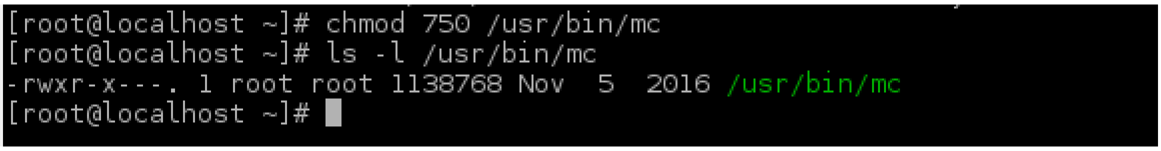
The account was updated in the /etc/passwd file.



```
Total download size: 1.7 M
Installed size: 5.6 M
Downloading packages:
mc-4.8.7-11.el7.x86_64.rpm                                              | 1.7 MB  00:01:2
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 1:mc-4.8.7-11.el7.x86_64
  Verifying  : 1:mc-4.8.7-11.el7.x86_64

Installed:
  mc.x86_64 1:4.8.7-11.el7

Complete!
[root@localhost ~]# whereis mc
mc: /usr/bin/mc /etc/mc /usr/libexec/mc /usr/share/mc /usr/share/man/man1/mc.1.gz
[root@localhost ~]# ls -l /usr/bin/mc
-rwxr-xr-x. 1 root root 1138768 Nov  5  2016 /usr/bin/mc
[root@localhost ~]#
```

Figure 16

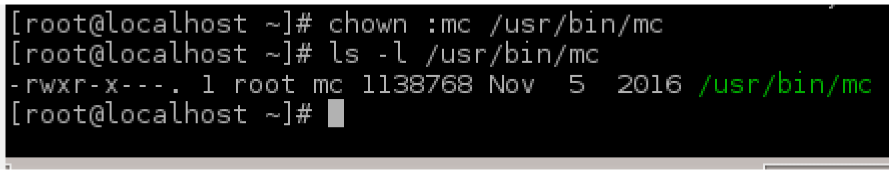
We installed the mc program and located it.



```
[root@localhost ~]# chmod 750 /usr/bin/mc
[root@localhost ~]# ls -l /usr/bin/mc
-rwxr-x---. 1 root root 1138768 Nov  5  2016 /usr/bin/mc
[root@localhost ~]#
```

Figure 17

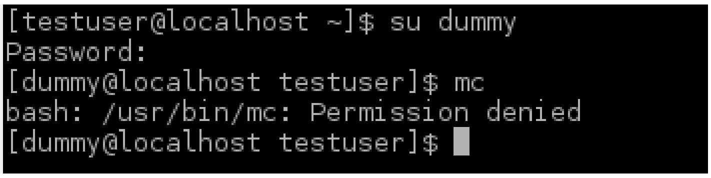
The permissions were changed for the program to only allow the owner and group to have access to the mc.



```
[root@localhost ~]# chown :mc /usr/bin/mc
[root@localhost ~]# ls -l /usr/bin/mc
-rwxr-x---. 1 root mc 1138768 Nov  5  2016 /usr/bin/mc
[root@localhost ~]#
```

Figure 18

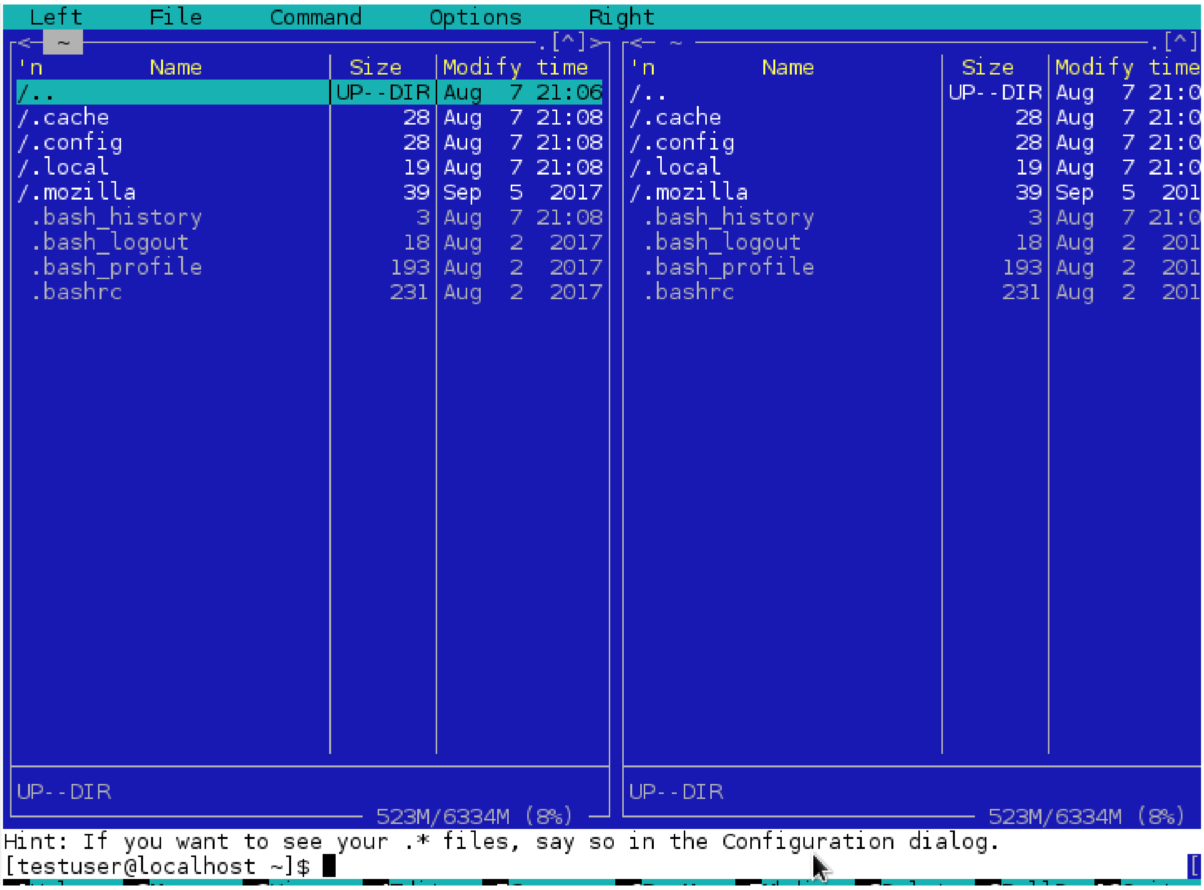
The ownership was also changed to group mc for the mc program.



```
[testuser@localhost ~]$ su dummy
Password:
[dummy@localhost testuser]$ mc
bash: /usr/bin/mc: Permission denied
[dummy@localhost testuser]$
```

Figure 19

When running the program as user dummy who is not part of the mc group, the program denied to execute.

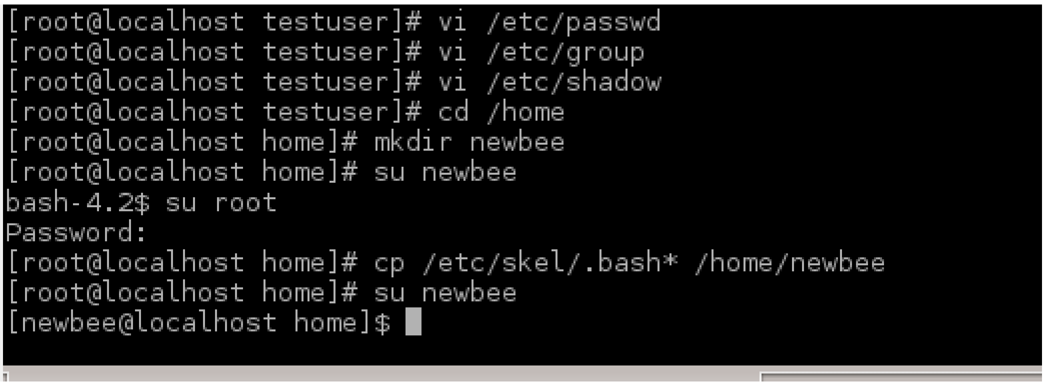


```
<- ~ ----------------------.[^]>  <- ~ ---------------------------.[^]
'n           Name         Size   Modify time  'n           Name          Size   Modify time
/..                      UP--DIR Aug  7 21:06 /..                       UP--DIR Aug  7 21:0
/.cache                       28 Aug  7 21:08 /.cache                        28 Aug  7 21:0
/.config                      28 Aug  7 21:08 /.config                       28 Aug  7 21:0
/.local                       19 Aug  7 21:08 /.local                        19 Aug  7 21:0
/.mozilla                     39 Sep  5  2017 /.mozilla                      39 Sep  5  201
 .bash_history                 3 Aug  7 21:08  .bash_history                  3 Aug  7 21:0
 .bash_logout                 18 Aug  2  2017  .bash_logout                  18 Aug  2  201
 .bash_profile               193 Aug  2  2017  .bash_profile                193 Aug  2  201
 .bashrc                     231 Aug  2  2017  .bashrc                      231 Aug  2  201

UP--DIR                                       UP--DIR
                      523M/6334M (8%)                               523M/6334M (8%)
Hint: If you want to see your .* files, say so in the Configuration dialog.
[testuser@localhost ~]$
```

Figure 20

When running it with testuser, the program was able to start.

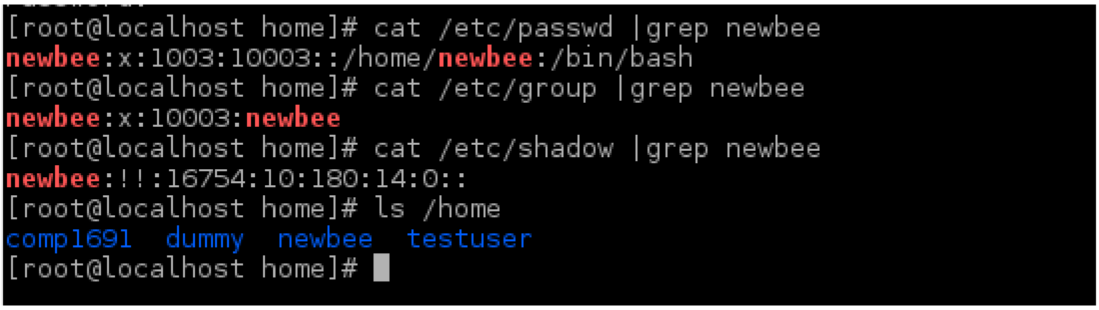
TASK



```
[root@localhost testuser]# vi /etc/passwd
[root@localhost testuser]# vi /etc/group
[root@localhost testuser]# vi /etc/shadow
[root@localhost testuser]# cd /home
[root@localhost home]# mkdir newbee
[root@localhost home]# su newbee
bash-4.2$ su root
Password:
[root@localhost home]# cp /etc/skel/.bash* /home/newbee
[root@localhost home]# su newbee
[newbee@localhost home]$
```

Figure 21

We edited the /etc/passwd,group and shadow then created the relevant directory with the same name and then copied the skel files into the newbee folder.

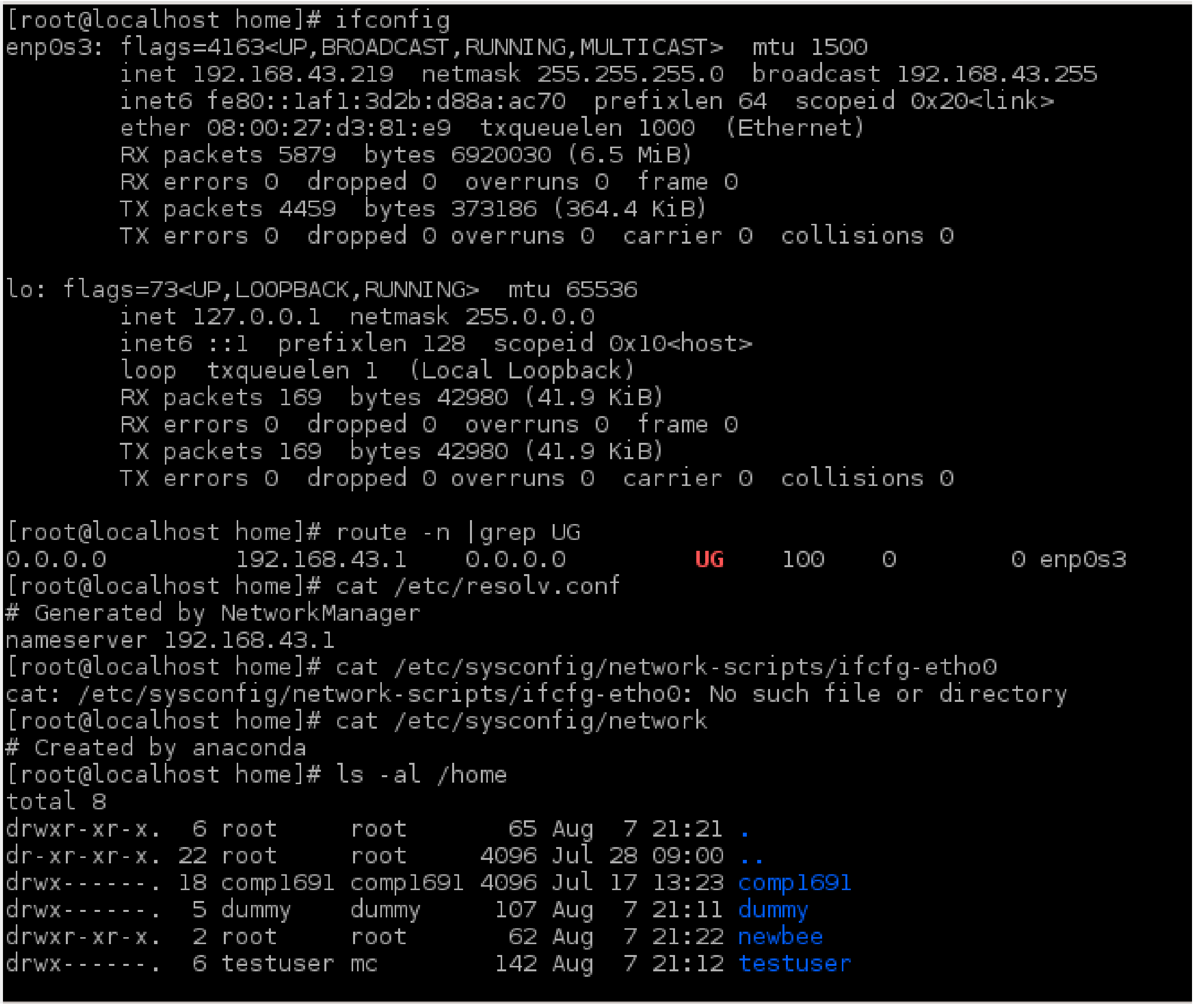


```
[root@localhost home]# cat /etc/passwd |grep newbee
newbee:x:1003:10003::/home/newbee:/bin/bash
[root@localhost home]# cat /etc/group |grep newbee
newbee:x:10003:newbee
[root@localhost home]# cat /etc/shadow |grep newbee
newbee:!!:16754:10:180:14:0::
[root@localhost home]# ls /home
comp1691  dummy  newbee  testuser
[root@localhost home]# █
```

Figure 22

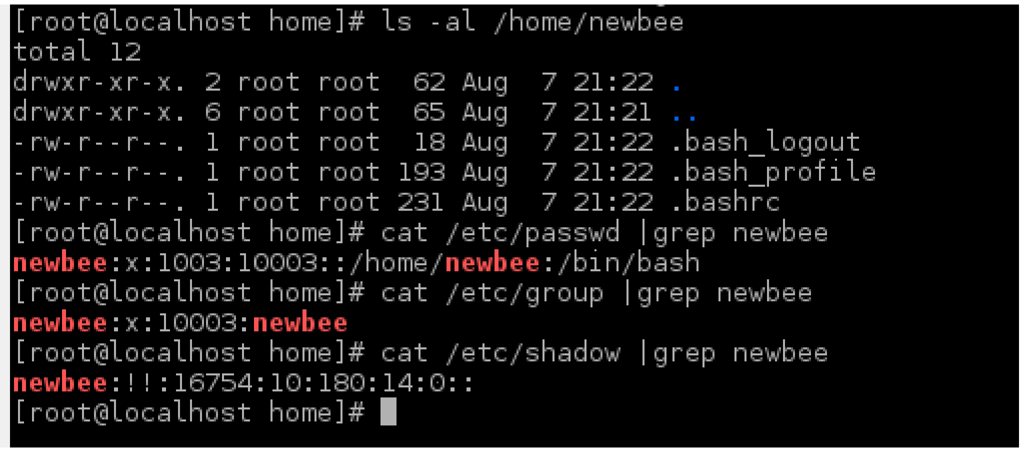
Figure 22 shows how the files were edited.

TESTING



```
[root@localhost home]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.219  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 fe80::1af1:3d2b:d88a:ac70  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d3:81:e9  txqueuelen 1000  (Ethernet)
        RX packets 5879  bytes 6920030 (6.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4459  bytes 373186 (364.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 169  bytes 42980 (41.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 169  bytes 42980 (41.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost home]# route -n |grep UG
0.0.0.0         192.168.43.1    0.0.0.0         UG    100    0        0 enp0s3
[root@localhost home]# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.43.1
[root@localhost home]# cat /etc/sysconfig/network-scripts/ifcfg-etho0
cat: /etc/sysconfig/network-scripts/ifcfg-etho0: No such file or directory
[root@localhost home]# cat /etc/sysconfig/network
# Created by anaconda
[root@localhost home]# ls -al /home
total 8
drwxr-xr-x.  6 root     root       65 Aug  7 21:21 .
dr-xr-xr-x. 22 root     root     4096 Jul 28 09:00 ..
drwx------. 18 comp1691 comp1691 4096 Jul 17 13:23 comp1691
drwx------.  5 dummy    dummy     107 Aug  7 21:11 dummy
drwxr-xr-x.  2 root     root       62 Aug  7 21:22 newbee
drwx------.  6 testuser mc        142 Aug  7 21:12 testuser
```

Figure 23



```
[root@localhost home]# ls -al /home/newbee
total 12
drwxr-xr-x. 2 root root  62 Aug  7 21:22 .
drwxr-xr-x. 6 root root  65 Aug  7 21:21 ..
-rw-r--r--. 1 root root  18 Aug  7 21:22 .bash_logout
-rw-r--r--. 1 root root 193 Aug  7 21:22 .bash_profile
-rw-r--r--. 1 root root 231 Aug  7 21:22 .bashrc
[root@localhost home]# cat /etc/passwd |grep newbee
newbee:x:1003:10003::/home/newbee:/bin/bash
[root@localhost home]# cat /etc/group |grep newbee
newbee:x:10003:newbee
[root@localhost home]# cat /etc/shadow |grep newbee
newbee:!!:16754:10:180:14:0::
[root@localhost home]# 
```

Figure 24

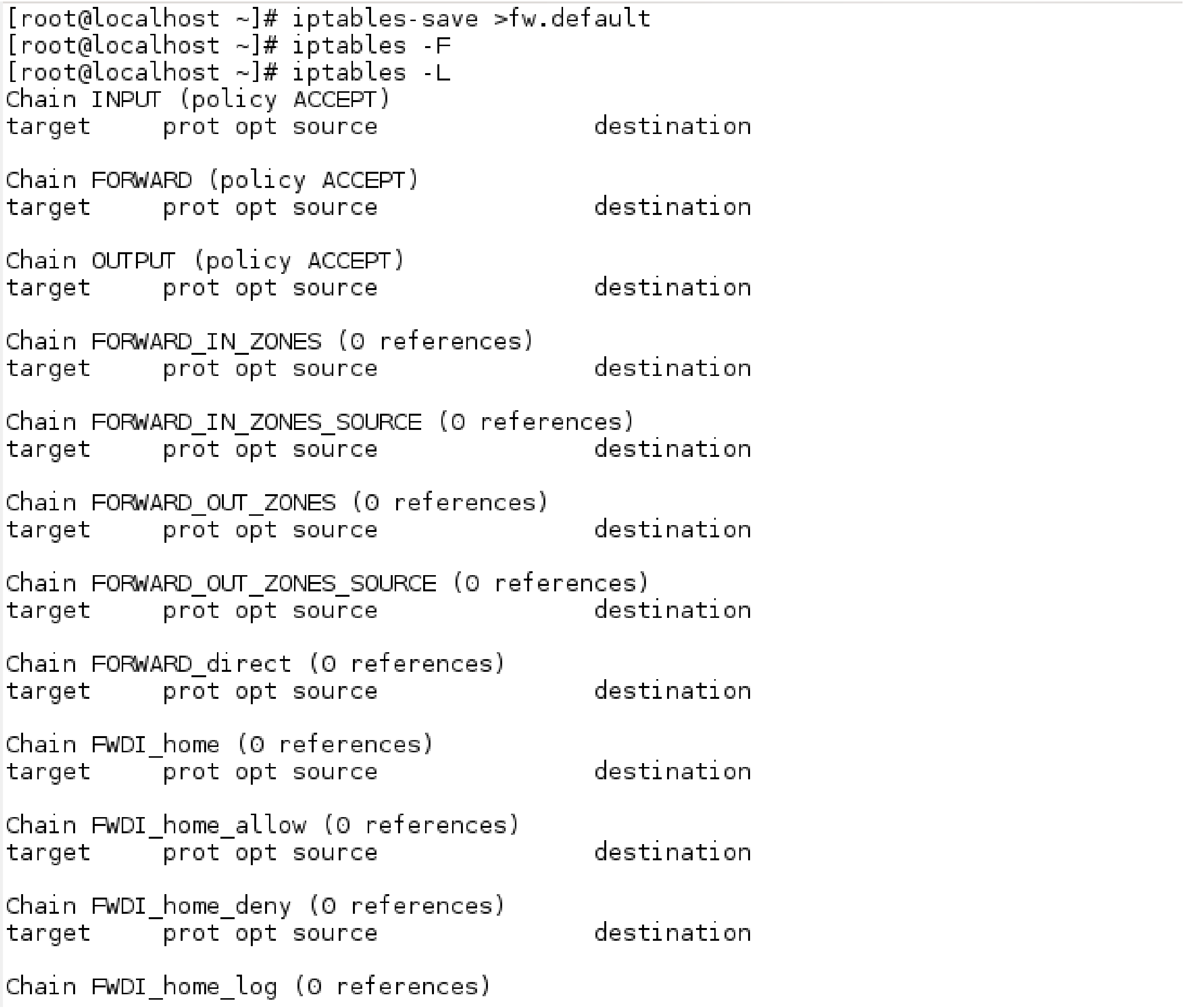
EVALUATION

I was able to accomplish the lab with my group members. This lab was not easy because the task section required a lot from us. I did learn a lot of things in the process of finishing the lab in that I was able to see exactly how the different files in the /etc/ directory play a role in the Linux operating system management of accounts and group (linuxhelp, 2)s. I was also able to see how the different files in the operating system are linked and the kind of information they store (techbrown, 1). Restricting user accounts from running applications was also learnt in the process.

LAB 2

EXERCISE

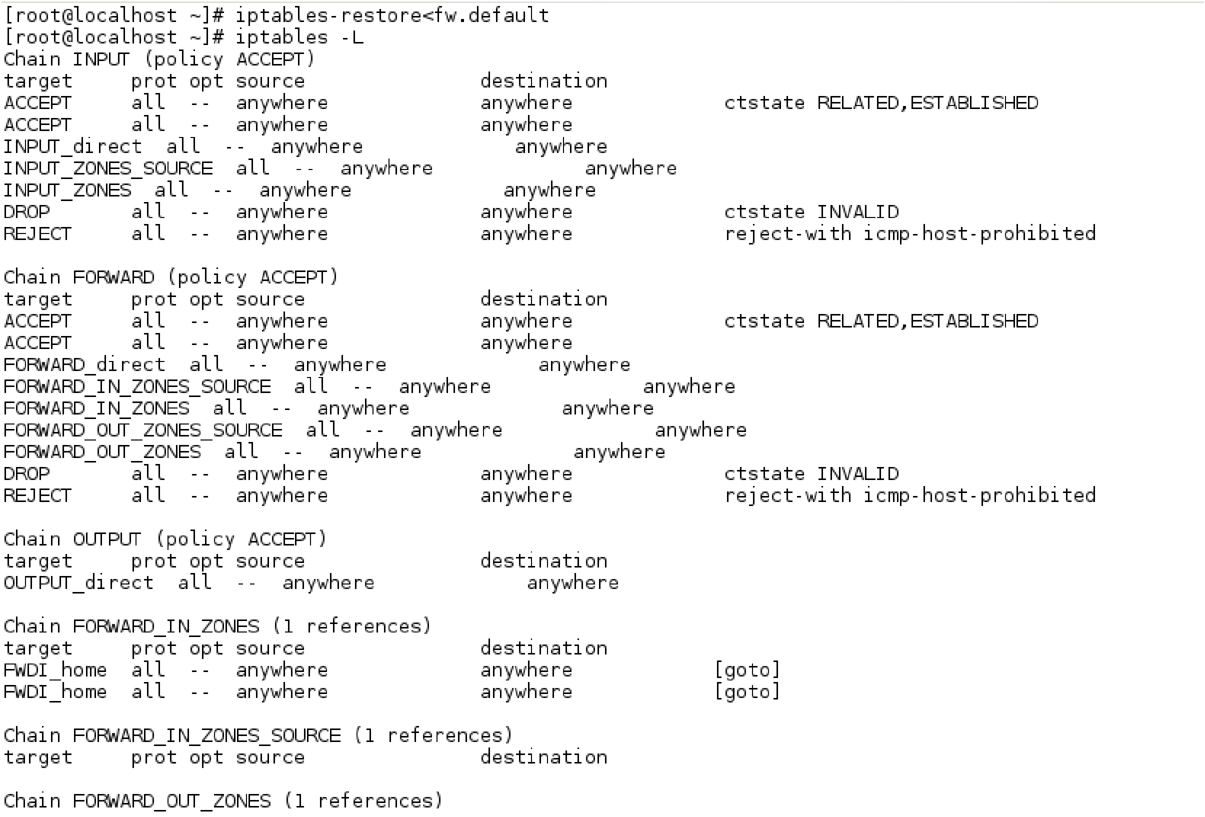
Guest account with password guest was created and we went on to view the firewall rules.



```
[root@localhost ~]# iptables-save >fw.default
[root@localhost ~]# iptables -F
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD_IN_ZONES (0 references)
target     prot opt source               destination

Chain FORWARD_IN_ZONES_SOURCE (0 references)
target     prot opt source               destination

Chain FORWARD_OUT_ZONES (0 references)
target     prot opt source               destination

Chain FORWARD_OUT_ZONES_SOURCE (0 references)
target     prot opt source               destination

Chain FORWARD_direct (0 references)
target     prot opt source               destination

Chain FWDI_home (0 references)
target     prot opt source               destination

Chain FWDI_home_allow (0 references)
target     prot opt source               destination

Chain FWDI_home_deny (0 references)
target     prot opt source               destination

Chain FWDI_home_log (0 references)
```

Figure 25

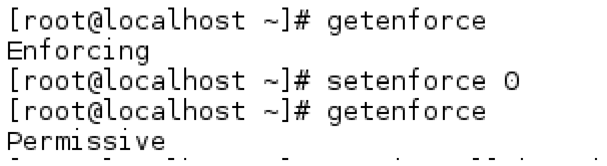
I created a backup of the rules and then emptied the firewall rules as shown above.



```
[root@localhost ~]# iptables-restore<fw.default
[root@localhost ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
INPUT_direct  all  --  anywhere             anywhere
INPUT_ZONES_SOURCE  all  --  anywhere             anywhere
INPUT_ZONES  all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere             ctstate INVALID
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
FORWARD_direct  all  --  anywhere             anywhere
FORWARD_IN_ZONES_SOURCE  all  --  anywhere             anywhere
FORWARD_IN_ZONES  all  --  anywhere             anywhere
FORWARD_OUT_ZONES_SOURCE  all  --  anywhere             anywhere
FORWARD_OUT_ZONES  all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere             ctstate INVALID
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
OUTPUT_direct  all  --  anywhere             anywhere

Chain FORWARD_IN_ZONES (1 references)
target     prot opt source               destination
FWDI_home  all  --  anywhere             anywhere            [goto]
FWDI_home  all  --  anywhere             anywhere            [goto]

Chain FORWARD_IN_ZONES_SOURCE (1 references)
target     prot opt source               destination

Chain FORWARD_OUT_ZONES (1 references)
```

Figure 26

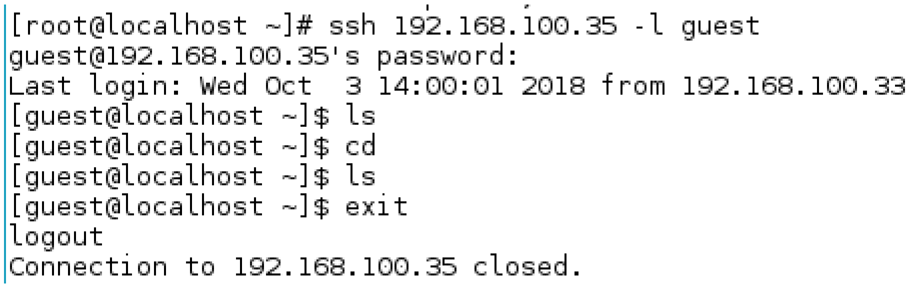
Iptables-restore was used to bring back firewall rules while iptables-save was used to create a backup of the rules. Listing the rules as shown above shows that this was what actually happened.



```
[root@localhost ~]# getenforce
Enforcing
[root@localhost ~]# setenforce 0
[root@localhost ~]# getenforce
Permissive
```

Figure 27

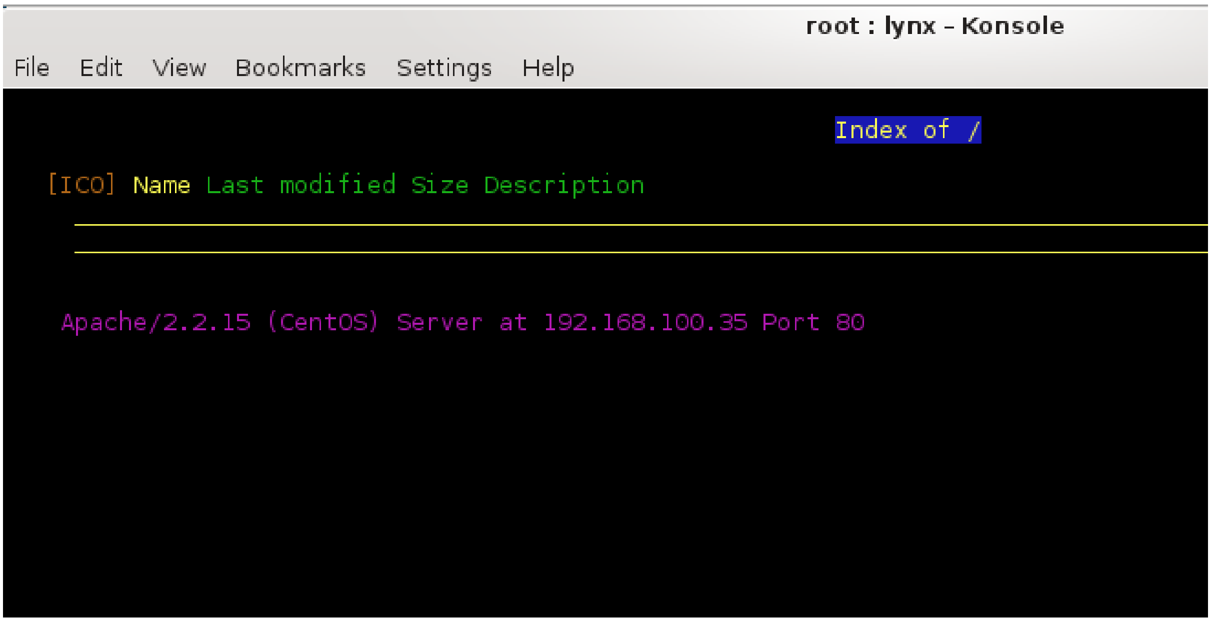
I was able to switch off the SELinux mechanism on Centos.



```
[root@localhost ~]# ssh 192.168.100.35 -l guest
guest@192.168.100.35's password:
Last login: Wed Oct  3 14:00:01 2018 from 192.168.100.33
[guest@localhost ~]$ ls
[guest@localhost ~]$ cd
[guest@localhost ~]$ ls
[guest@localhost ~]$ exit
logout
Connection to 192.168.100.35 closed.
```

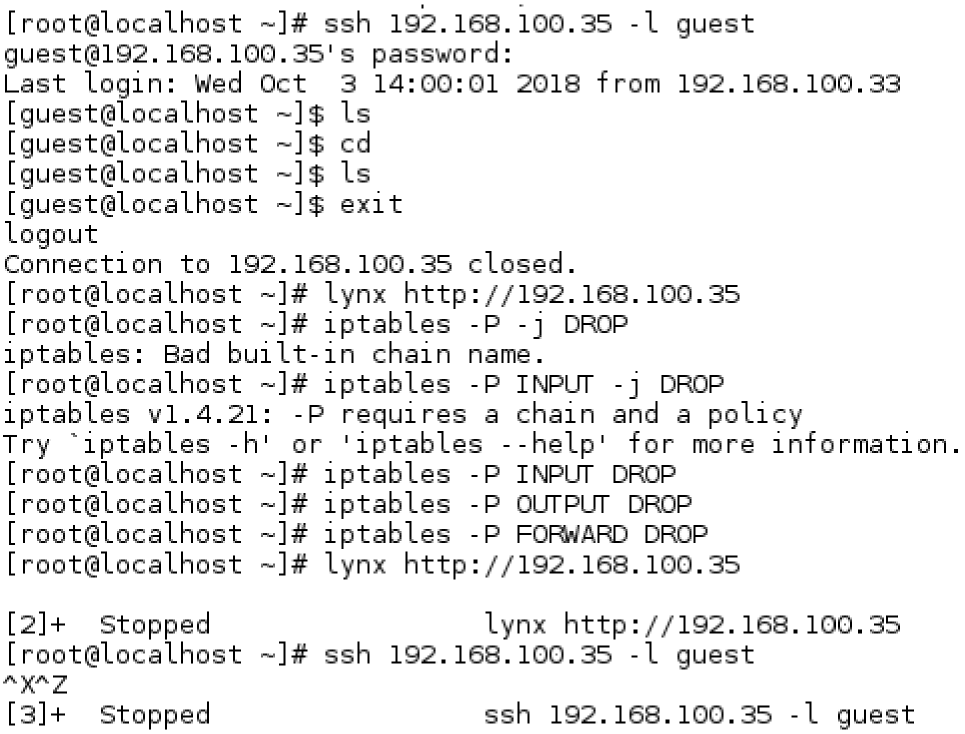
Figure 28

Connecting to the services on the other machine was possible.



```
                                                   Index of /

  [ICO] Name Last modified Size Description

   Apache/2.2.15 (CentOS) Server at 192.168.100.35 Port 80
```

Figure 29



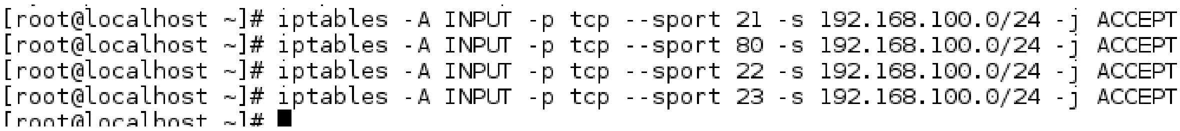
```
[root@localhost ~]# ssh 192.168.100.35 -l guest
guest@192.168.100.35's password:
Last login: Wed Oct  3 14:00:01 2018 from 192.168.100.33
[guest@localhost ~]$ ls
[guest@localhost ~]$ cd
[guest@localhost ~]$ ls
[guest@localhost ~]$ exit
logout
Connection to 192.168.100.35 closed.
[root@localhost ~]# lynx http://192.168.100.35
[root@localhost ~]# iptables -P -j DROP
iptables: Bad built-in chain name.
[root@localhost ~]# iptables -P INPUT -j DROP
iptables v1.4.21: -P requires a chain and a policy
Try `iptables -h' or 'iptables --help' for more information.
[root@localhost ~]# iptables -P INPUT DROP
[root@localhost ~]# iptables -P OUTPUT DROP
[root@localhost ~]# iptables -P FORWARD DROP
[root@localhost ~]# lynx http://192.168.100.35

[2]+  Stopped                 lynx http://192.168.100.35
[root@localhost ~]# ssh 192.168.100.35 -l guest
^X^Z
[3]+  Stopped                 ssh 192.168.100.35 -l guest
```

Figure 30

The default policy of DROP had the effect of restricting all the traffic including the SSH, HTTP and FTP that was initially accepting.

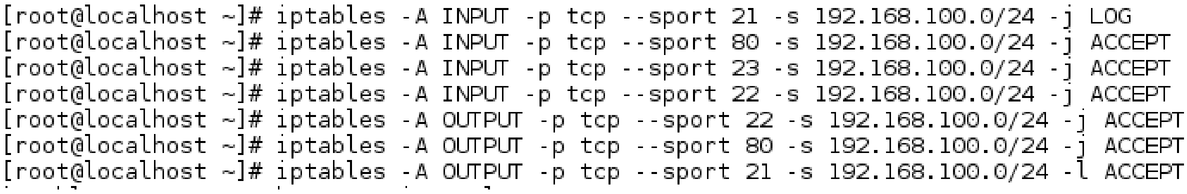
TASK

http through port 80, ssh through port 22 and ftp through ports 21 and 20 were allowed by allowing traffic on the INPUT and OUTPUT chains while making sure that both the source and destination ports were accessible. I then logged the traffic.



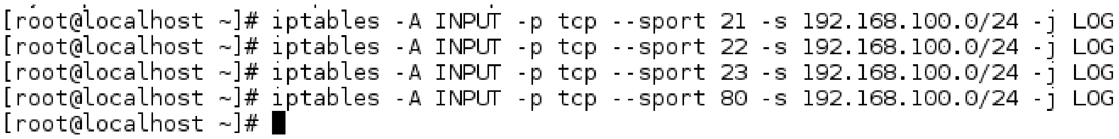
```
[root@localhost ~]# iptables -A INPUT -p tcp --sport 21 -s 192.168.100.0/24 -j ACCEPT
[root@localhost ~]# iptables -A INPUT -p tcp --sport 80 -s 192.168.100.0/24 -j ACCEPT
[root@localhost ~]# iptables -A INPUT -p tcp --sport 22 -s 192.168.100.0/24 -j ACCEPT
[root@localhost ~]# iptables -A INPUT -p tcp --sport 23 -s 192.168.100.0/24 -j ACCEPT
[root@localhost ~]# █
```

Figure 31



```
[root@localhost ~]# iptables -A INPUT -p tcp --sport 21 -s 192.168.100.0/24 -j LOG
[root@localhost ~]# iptables -A INPUT -p tcp --sport 80 -s 192.168.100.0/24 -j ACCEPT
[root@localhost ~]# iptables -A INPUT -p tcp --sport 23 -s 192.168.100.0/24 -j ACCEPT
[root@localhost ~]# iptables -A INPUT -p tcp --sport 22 -s 192.168.100.0/24 -j ACCEPT
[root@localhost ~]# iptables -A OUTPUT -p tcp --sport 22 -s 192.168.100.0/24 -j ACCEPT
[root@localhost ~]# iptables -A OUTPUT -p tcp --sport 80 -s 192.168.100.0/24 -j ACCEPT
[root@localhost ~]# iptables -A OUTPUT -p tcp --sport 21 -s 192.168.100.0/24 -l ACCEPT
```

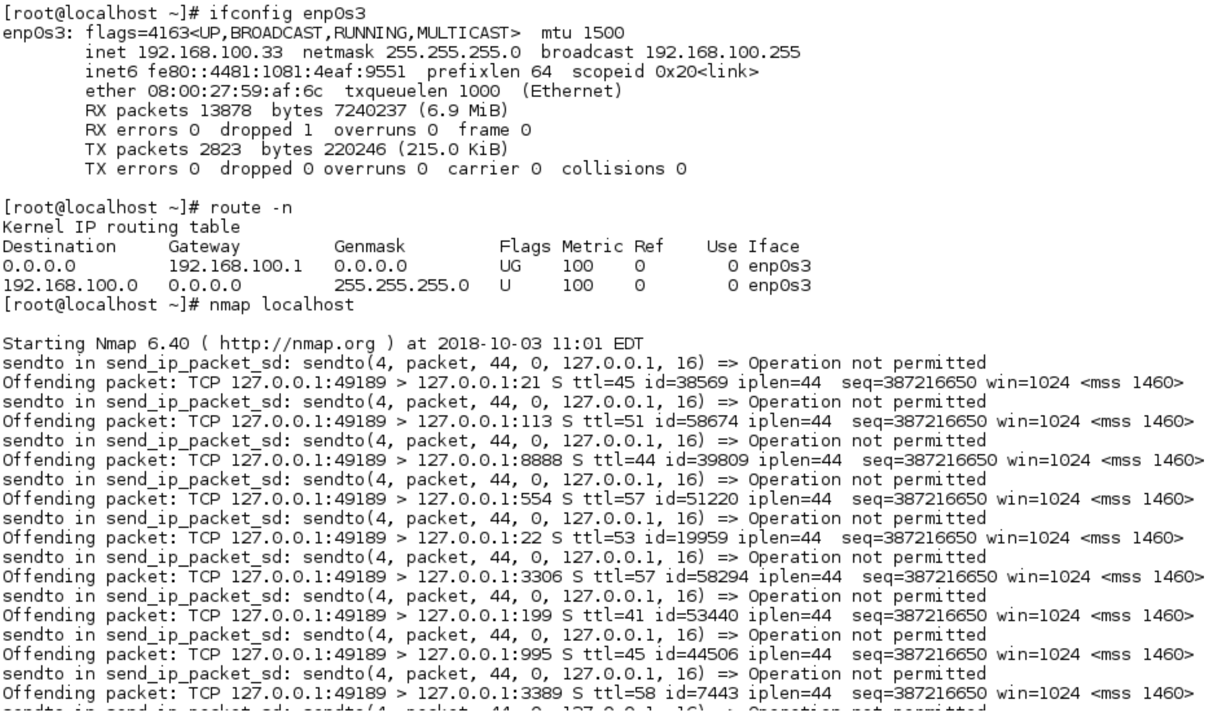
Figure 32



```
[root@localhost ~]# iptables -A INPUT -p tcp --sport 21 -s 192.168.100.0/24 -j LOG
[root@localhost ~]# iptables -A INPUT -p tcp --sport 22 -s 192.168.100.0/24 -j LOG
[root@localhost ~]# iptables -A INPUT -p tcp --sport 23 -s 192.168.100.0/24 -j LOG
[root@localhost ~]# iptables -A INPUT -p tcp --sport 80 -s 192.168.100.0/24 -j LOG
[root@localhost ~]# █
```

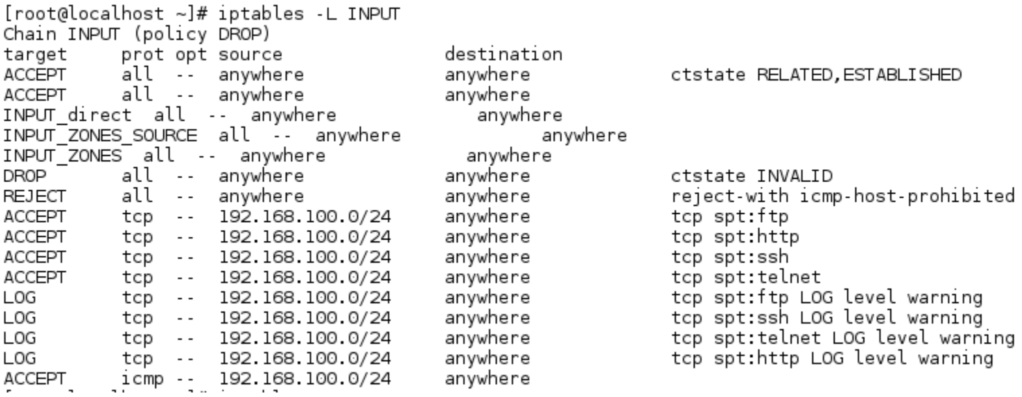
Figure 33

TESTING



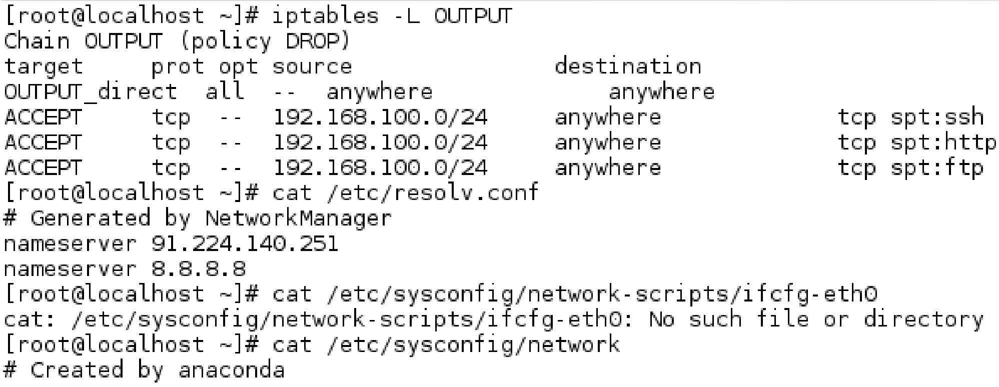
```
[root@localhost ~]# ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.33  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::4481:1081:4eaf:9551  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:59:af:6c  txqueuelen 1000  (Ethernet)
        RX packets 13878  bytes 7240237 (6.9 MiB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 2823  bytes 220246 (215.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost ~]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.100.1   0.0.0.0         UG    100    0        0 enp0s3
192.168.100.0   0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
[root@localhost ~]# nmap localhost

Starting Nmap 6.40 ( http://nmap.org ) at 2018-10-03 11:01 EDT
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:49189 > 127.0.0.1:21 S ttl=45 id=38569 iplen=44  seq=387216650 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:49189 > 127.0.0.1:113 S ttl=51 id=58674 iplen=44  seq=387216650 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:49189 > 127.0.0.1:8888 S ttl=44 id=39809 iplen=44  seq=387216650 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:49189 > 127.0.0.1:554 S ttl=57 id=51220 iplen=44  seq=387216650 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:49189 > 127.0.0.1:22 S ttl=53 id=19959 iplen=44  seq=387216650 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:49189 > 127.0.0.1:3306 S ttl=57 id=58294 iplen=44  seq=387216650 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:49189 > 127.0.0.1:199 S ttl=41 id=53440 iplen=44  seq=387216650 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:49189 > 127.0.0.1:995 S ttl=45 id=44506 iplen=44  seq=387216650 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
Offending packet: TCP 127.0.0.1:49189 > 127.0.0.1:3389 S ttl=58 id=7443 iplen=44  seq=387216650 win=1024 <mss 1460>
sendto in send_ip_packet_sd: sendto(4, packet, 44, 0, 127.0.0.1, 16) => Operation not permitted
```

Figure 34



```
[root@localhost ~]# iptables -L INPUT
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere             ctstate RELATED,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere
INPUT_direct  all  --  anywhere             anywhere
INPUT_ZONES_SOURCE  all  --  anywhere             anywhere
INPUT_ZONES  all  --  anywhere             anywhere
DROP       all  --  anywhere             anywhere             ctstate INVALID
REJECT     all  --  anywhere             anywhere             reject-with icmp-host-prohibited
ACCEPT     tcp  --  192.168.100.0/24     anywhere             tcp spt:ftp
ACCEPT     tcp  --  192.168.100.0/24     anywhere             tcp spt:http
ACCEPT     tcp  --  192.168.100.0/24     anywhere             tcp spt:ssh
ACCEPT     tcp  --  192.168.100.0/24     anywhere             tcp spt:telnet
LOG        tcp  --  192.168.100.0/24     anywhere             tcp spt:ftp LOG level warning
LOG        tcp  --  192.168.100.0/24     anywhere             tcp spt:ssh LOG level warning
LOG        tcp  --  192.168.100.0/24     anywhere             tcp spt:telnet LOG level warning
LOG        tcp  --  192.168.100.0/24     anywhere             tcp spt:http LOG level warning
ACCEPT     icmp --  192.168.100.0/24     anywhere
```

Figure 35



```
[root@localhost ~]# iptables -L OUTPUT
Chain OUTPUT (policy DROP)
target     prot opt source               destination
OUTPUT_direct  all  --  anywhere             anywhere
ACCEPT     tcp  --  192.168.100.0/24     anywhere             tcp spt:ssh
ACCEPT     tcp  --  192.168.100.0/24     anywhere             tcp spt:http
ACCEPT     tcp  --  192.168.100.0/24     anywhere             tcp spt:ftp
[root@localhost ~]# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 91.224.140.251
nameserver 8.8.8.8
[root@localhost ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
cat: /etc/sysconfig/network-scripts/ifcfg-eth0: No such file or directory
[root@localhost ~]# cat /etc/sysconfig/network
# Created by anaconda
```

Figure 36

EVALUATION

I was able to learn how to use the iptables program to make policies and rules on how traffic should be managed on this firewall (Ramesh natarajan, 3). I was also able to learn and see the effects of a default policy of DROP which basically blocked everything unless there was an explicit rule that allowed it. Even ping messages on ICMP were not able to go through. It was a good lab and had a lot of insight ().

LAB 3

/etc/sysconfig/network-script/ifcfg-eth0

This file is used to configure the Ethernet interfaces on the system. It has a number of settings that are filled in either manually or using DHCP. Examples are as follows;

BROADCAST= sets the broadcast address.

DEVICE= sets the interface name.

IPADDR = sets the interface ip address

MACADDR = the mac address

/etc/sysconfig/network

This is used to configure how the system works with the network. Some options are as follow;

GATEWAY = the default gateway of the device.

HOSTNAME = the hostname or Fully Qualified Domain Name

NETWORK = whether configuring should be on or automatic.

GATEWAYDEV = the interface for traffic. The default interface.

/etc/nsswitch.conf

Sets where the system retrieves information such as password. Some options are as follows;

Passwd:files

In this example the password is got from the files.

Hosts:dns files

In this example host names are resolved by named then if not then files.

/etc/host.conf

Controls the services the resolver can use. Examples are as follows;

Order: bind, hosts

This shows that the bind package is the first to be checked for name resolutions followed by host files, /etc/hosts.

Multi: on

This shows that multihoming is enabled and so the device can have multiple IP addresses because of multiple interfaces

/etc/hosts

Used for resolving hostnames to IP addresses. Considered obsolete.

```
10.0.29.1        group29
```

This shows that the ip address is translated to group29.

/etc/resolv.conf

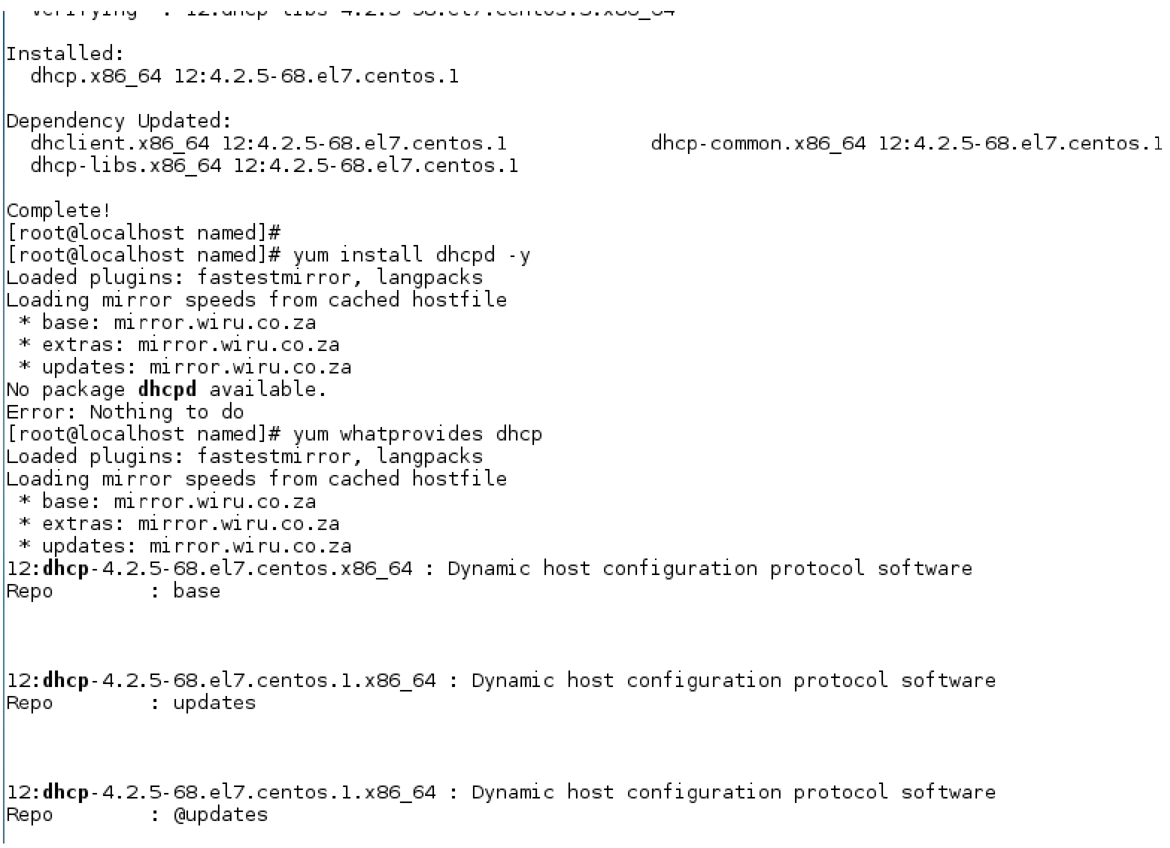
Used to specify the nameservers the system should use.

Nameserver 8.8.4.4

This means requests will be passed to 8.8.4.4 for name resolution.

LAB 4

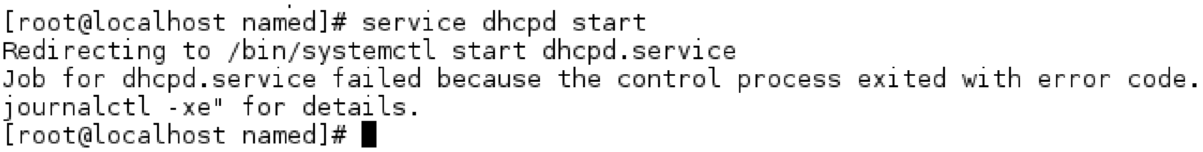
EXERCISE



```
  Verifying  : 12:dhcp-libs-4.2.5-58.el7.centos.3.x86_64

Installed:
  dhcp.x86_64 12:4.2.5-68.el7.centos.1

Dependency Updated:
  dhclient.x86_64 12:4.2.5-68.el7.centos.1            dhcp-common.x86_64 12:4.2.5-68.el7.centos.1
  dhcp-libs.x86_64 12:4.2.5-68.el7.centos.1

Complete!
[root@localhost named]#
[root@localhost named]# yum install dhcpd -y
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.wiru.co.za
 * extras: mirror.wiru.co.za
 * updates: mirror.wiru.co.za
No package dhcpd available.
Error: Nothing to do
[root@localhost named]# yum whatprovides dhcp
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirror.wiru.co.za
 * extras: mirror.wiru.co.za
 * updates: mirror.wiru.co.za
12:dhcp-4.2.5-68.el7.centos.x86_64 : Dynamic host configuration protocol software
Repo        : base



12:dhcp-4.2.5-68.el7.centos.1.x86_64 : Dynamic host configuration protocol software
Repo        : updates



12:dhcp-4.2.5-68.el7.centos.1.x86_64 : Dynamic host configuration protocol software
Repo        : @updates
```

Figure 37

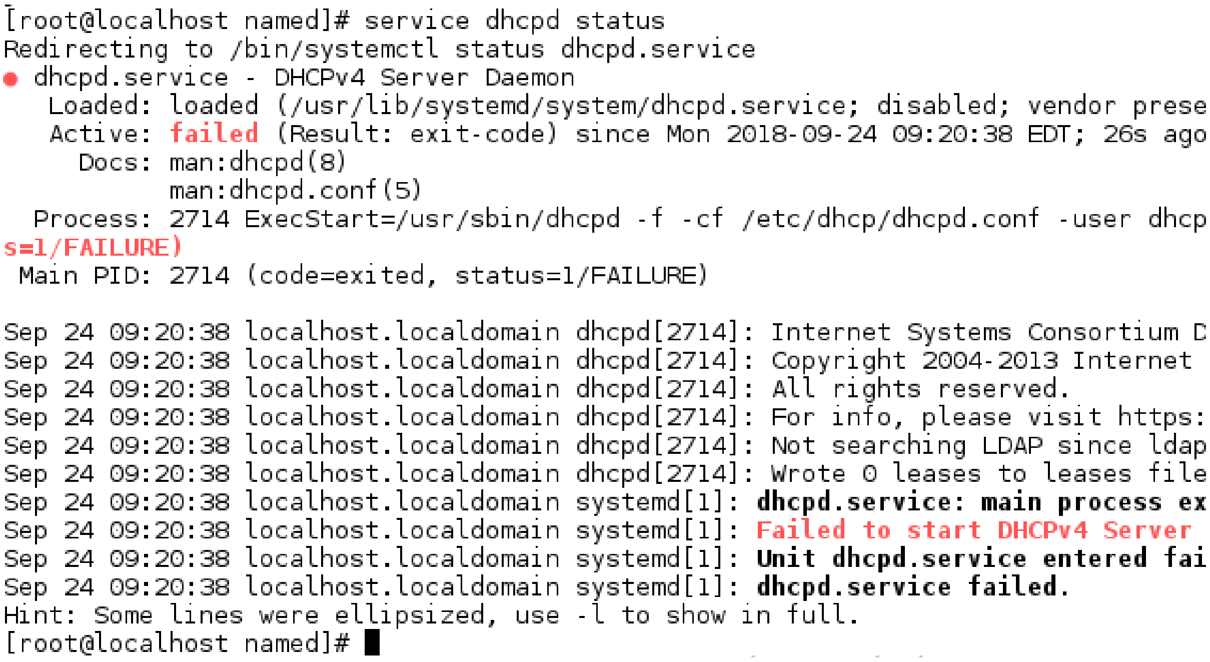
The dhcpd package was now available. Instead I was offered dhcp as a package with the service. I installed that instead.



```
[root@localhost named]# service dhcpd start
Redirecting to /bin/systemctl start dhcpd.service
Job for dhcpd.service failed because the control process exited with error code.
journalctl -xe" for details.
[root@localhost named]# █
```

Figure 38

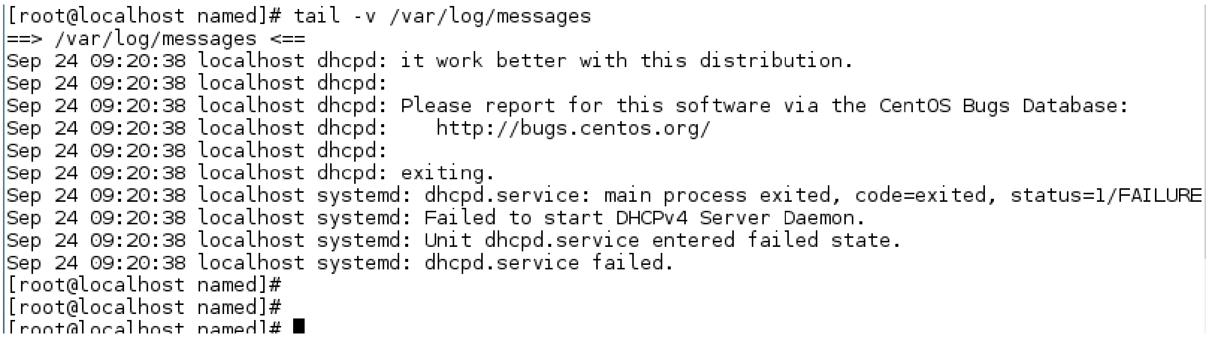
Trying to start the service failed as seen in the figure above.



```
[root@localhost named]# service dhcpd status
Redirecting to /bin/systemctl status dhcpd.service
● dhcpd.service - DHCPv4 Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; disabled; vendor prese
   Active: failed (Result: exit-code) since Mon 2018-09-24 09:20:38 EDT; 26s ago
     Docs: man:dhcpd(8)
           man:dhcpd.conf(5)
  Process: 2714 ExecStart=/usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcp
s=1/FAILURE)
 Main PID: 2714 (code=exited, status=1/FAILURE)

Sep 24 09:20:38 localhost.localdomain dhcpd[2714]: Internet Systems Consortium D
Sep 24 09:20:38 localhost.localdomain dhcpd[2714]: Copyright 2004-2013 Internet
Sep 24 09:20:38 localhost.localdomain dhcpd[2714]: All rights reserved.
Sep 24 09:20:38 localhost.localdomain dhcpd[2714]: For info, please visit https:
Sep 24 09:20:38 localhost.localdomain dhcpd[2714]: Not searching LDAP since ldap
Sep 24 09:20:38 localhost.localdomain dhcpd[2714]: Wrote 0 leases to leases file
Sep 24 09:20:38 localhost.localdomain systemd[1]: dhcpd.service: main process ex
Sep 24 09:20:38 localhost.localdomain systemd[1]: Failed to start DHCPv4 Server
Sep 24 09:20:38 localhost.localdomain systemd[1]: Unit dhcpd.service entered fai
Sep 24 09:20:38 localhost.localdomain systemd[1]: dhcpd.service failed.
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost named]# █
```

Figure 39

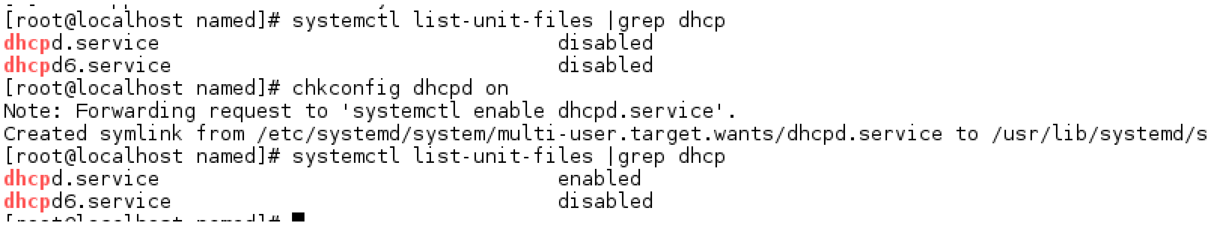
I then checked the status to see if it was already running. In this case it was not running.



```
[root@localhost named]# tail -v /var/log/messages
==> /var/log/messages <==
Sep 24 09:20:38 localhost dhcpd: it work better with this distribution.
Sep 24 09:20:38 localhost dhcpd:
Sep 24 09:20:38 localhost dhcpd: Please report for this software via the CentOS Bugs Database:
Sep 24 09:20:38 localhost dhcpd:     http://bugs.centos.org/
Sep 24 09:20:38 localhost dhcpd:
Sep 24 09:20:38 localhost dhcpd: exiting.
Sep 24 09:20:38 localhost systemd: dhcpd.service: main process exited, code=exited, status=1/FAILURE
Sep 24 09:20:38 localhost systemd: Failed to start DHCPv4 Server Daemon.
Sep 24 09:20:38 localhost systemd: Unit dhcpd.service entered failed state.
Sep 24 09:20:38 localhost systemd: dhcpd.service failed.
[root@localhost named]#
[root@localhost named]#
[root@localhost named]# █
```

Figure 40

I opened the log file to look for any problems. The only clue was that the interface was not registered. That message was not present in the log.



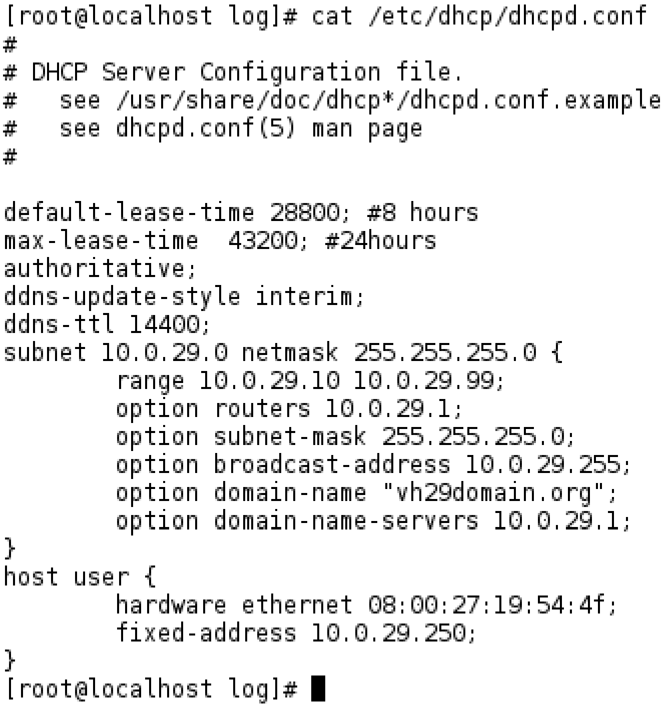
```
[root@localhost named]# systemctl list-unit-files |grep dhcp
dhcpd.service                                 disabled
dhcpd6.service                                disabled
[root@localhost named]# chkconfig dhcpd on
Note: Forwarding request to 'systemctl enable dhcpd.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/dhcpd.service to /usr/lib/systemd/s
[root@localhost named]# systemctl list-unit-files |grep dhcp
dhcpd.service                                 enabled
dhcpd6.service                                disabled
[root@localhost named]# █
```

Figure 41

I finally set the service to be starting with the operating system on the system boot.

TASK

The configuration file was set as follows to accomplish the lab.

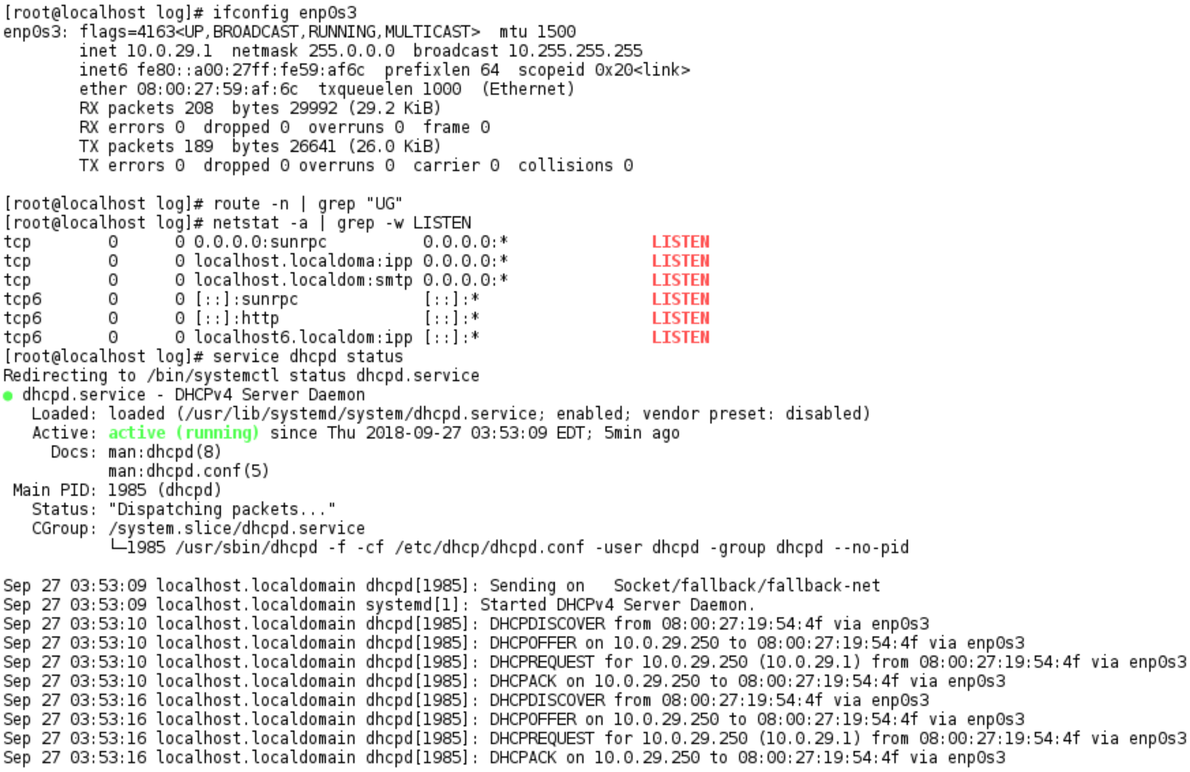


```
[root@localhost log]# cat /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#

default-lease-time 28800; #8 hours
max-lease-time  43200; #24hours
authoritative;
ddns-update-style interim;
ddns-ttl 14400;
subnet 10.0.29.0 netmask 255.255.255.0 {
        range 10.0.29.10 10.0.29.99;
        option routers 10.0.29.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 10.0.29.255;
        option domain-name "vh29domain.org";
        option domain-name-servers 10.0.29.1;
}
host user {
        hardware ethernet 08:00:27:19:54:4f;
        fixed-address 10.0.29.250;
}
[root@localhost log]# █
```

Figure 42

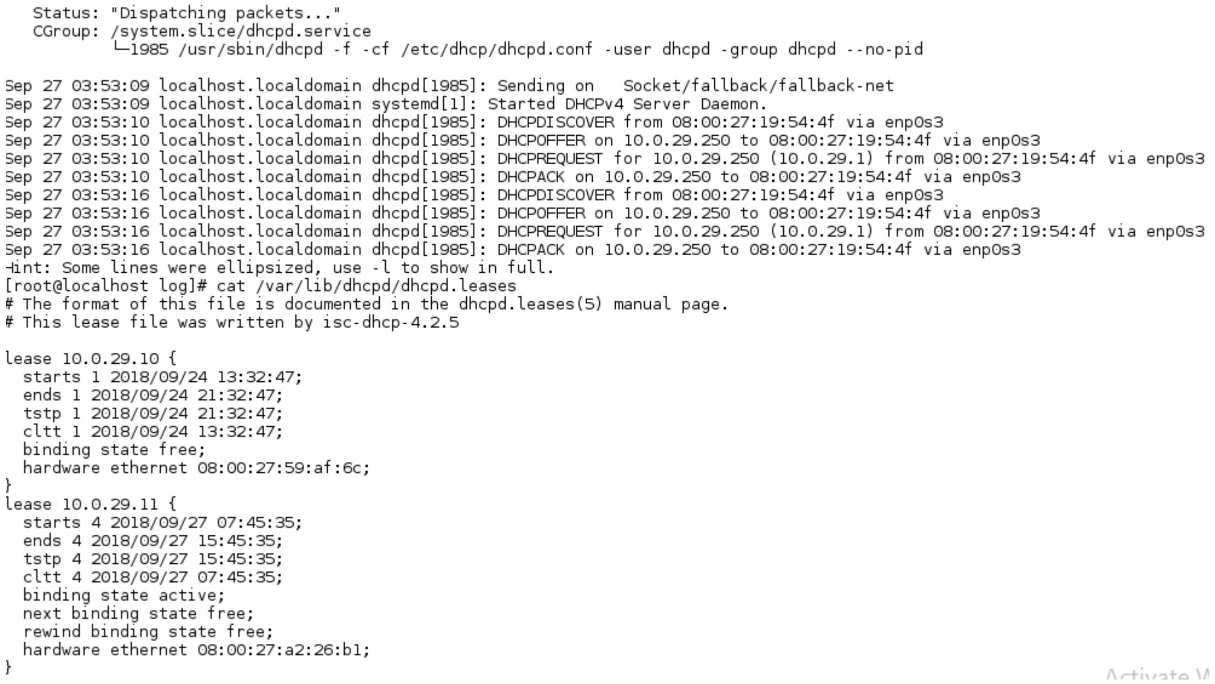
TESTING

SERVER



```
[root@localhost log]# ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.29.1  netmask 255.0.0.0  broadcast 10.255.255.255
        inet6 fe80::a00:27ff:fe59:af6c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:59:af:6c  txqueuelen 1000  (Ethernet)
        RX packets 208  bytes 29992 (29.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 189  bytes 26641 (26.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost log]# route -n | grep "UG"
[root@localhost log]# netstat -a | grep -w LISTEN
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdoma:ipp 0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*               LISTEN
tcp6       0      0 [::]:sunrpc             [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 localhost6.localdom:ipp [::]:*                  LISTEN
[root@localhost log]# service dhcpd status
Redirecting to /bin/systemctl status dhcpd.service
● dhcpd.service - DHCPv4 Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2018-09-27 03:53:09 EDT; 5min ago
     Docs: man:dhcpd(8)
           man:dhcpd.conf(5)
 Main PID: 1985 (dhcpd)
   Status: "Dispatching packets..."
   CGroup: /system.slice/dhcpd.service
           └─1985 /usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group dhcpd --no-pid

Sep 27 03:53:09 localhost.localdomain dhcpd[1985]: Sending on   Socket/fallback/fallback-net
Sep 27 03:53:09 localhost.localdomain systemd[1]: Started DHCPv4 Server Daemon.
Sep 27 03:53:10 localhost.localdomain dhcpd[1985]: DHCPDISCOVER from 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:10 localhost.localdomain dhcpd[1985]: DHCPOFFER on 10.0.29.250 to 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:10 localhost.localdomain dhcpd[1985]: DHCPREQUEST for 10.0.29.250 (10.0.29.1) from 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:10 localhost.localdomain dhcpd[1985]: DHCPACK on 10.0.29.250 to 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:16 localhost.localdomain dhcpd[1985]: DHCPDISCOVER from 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:16 localhost.localdomain dhcpd[1985]: DHCPOFFER on 10.0.29.250 to 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:16 localhost.localdomain dhcpd[1985]: DHCPREQUEST for 10.0.29.250 (10.0.29.1) from 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:16 localhost.localdomain dhcpd[1985]: DHCPACK on 10.0.29.250 to 08:00:27:19:54:4f via enp0s3
```

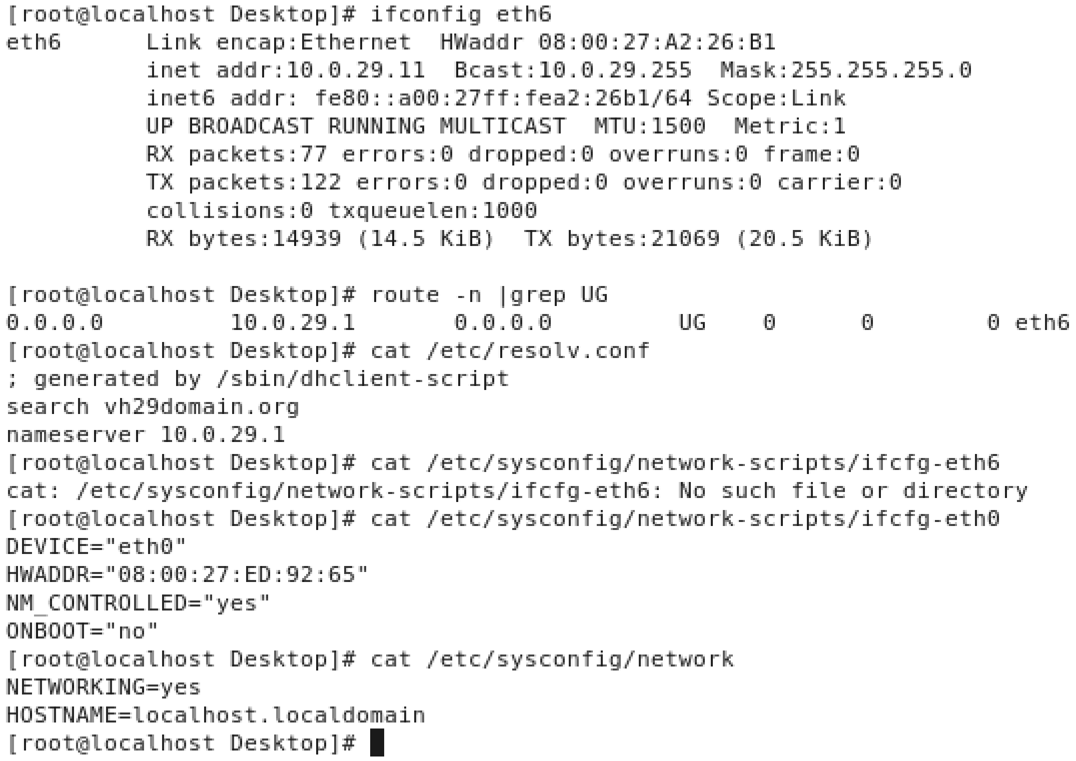
Figure 43



```
   Status: "Dispatching packets..."
   CGroup: /system.slice/dhcpd.service
           └─1985 /usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group dhcpd --no-pid

Sep 27 03:53:09 localhost.localdomain dhcpd[1985]: Sending on   Socket/fallback/fallback-net
Sep 27 03:53:09 localhost.localdomain systemd[1]: Started DHCPv4 Server Daemon.
Sep 27 03:53:10 localhost.localdomain dhcpd[1985]: DHCPDISCOVER from 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:10 localhost.localdomain dhcpd[1985]: DHCPOFFER on 10.0.29.250 to 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:10 localhost.localdomain dhcpd[1985]: DHCPREQUEST for 10.0.29.250 (10.0.29.1) from 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:10 localhost.localdomain dhcpd[1985]: DHCPACK on 10.0.29.250 to 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:16 localhost.localdomain dhcpd[1985]: DHCPDISCOVER from 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:16 localhost.localdomain dhcpd[1985]: DHCPOFFER on 10.0.29.250 to 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:16 localhost.localdomain dhcpd[1985]: DHCPREQUEST for 10.0.29.250 (10.0.29.1) from 08:00:27:19:54:4f via enp0s3
Sep 27 03:53:16 localhost.localdomain dhcpd[1985]: DHCPACK on 10.0.29.250 to 08:00:27:19:54:4f via enp0s3
Hint: Some lines were ellipsized, use -l to show in full.
[root@localhost log]# cat /var/lib/dhcpd/dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.2.5

lease 10.0.29.10 {
  starts 1 2018/09/24 13:32:47;
  ends 1 2018/09/24 21:32:47;
  tstp 1 2018/09/24 21:32:47;
  cltt 1 2018/09/24 13:32:47;
  binding state free;
  hardware ethernet 08:00:27:59:af:6c;
}
lease 10.0.29.11 {
  starts 4 2018/09/27 07:45:35;
  ends 4 2018/09/27 15:45:35;
  tstp 4 2018/09/27 15:45:35;
  cltt 4 2018/09/27 07:45:35;
  binding state active;
  next binding state free;
  rewind binding state free;
  hardware ethernet 08:00:27:a2:26:b1;
}
```

Figure 44

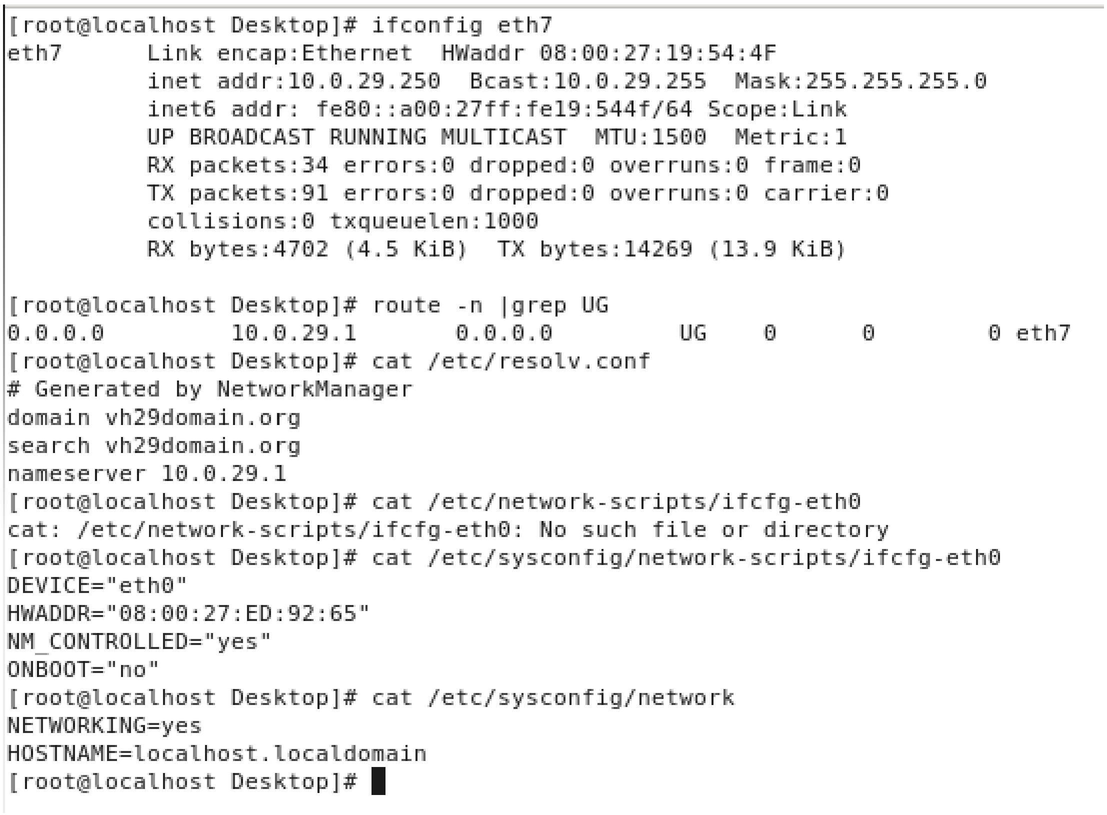
VM1 TESTING



```
[root@localhost Desktop]# ifconfig eth6
eth6      Link encap:Ethernet  HWaddr 08:00:27:A2:26:B1
          inet addr:10.0.29.11  Bcast:10.0.29.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea2:26b1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77 errors:0 dropped:0 overruns:0 frame:0
          TX packets:122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14939 (14.5 KiB)  TX bytes:21069 (20.5 KiB)

[root@localhost Desktop]# route -n |grep UG
0.0.0.0         10.0.29.1       0.0.0.0         UG    0      0        0 eth6
[root@localhost Desktop]# cat /etc/resolv.conf
; generated by /sbin/dhclient-script
search vh29domain.org
nameserver 10.0.29.1
[root@localhost Desktop]# cat /etc/sysconfig/network-scripts/ifcfg-eth6
cat: /etc/sysconfig/network-scripts/ifcfg-eth6: No such file or directory
[root@localhost Desktop]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
HWADDR="08:00:27:ED:92:65"
NM_CONTROLLED="yes"
ONBOOT="no"
[root@localhost Desktop]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=localhost.localdomain
[root@localhost Desktop]# █
```

Figure 45

VM2 TESTING



```
[root@localhost Desktop]# ifconfig eth7
eth7      Link encap:Ethernet  HWaddr 08:00:27:19:54:4F
          inet addr:10.0.29.250  Bcast:10.0.29.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe19:544f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:34 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4702 (4.5 KiB)  TX bytes:14269 (13.9 KiB)

[root@localhost Desktop]# route -n |grep UG
0.0.0.0         10.0.29.1       0.0.0.0         UG    0      0        0 eth7
[root@localhost Desktop]# cat /etc/resolv.conf
# Generated by NetworkManager
domain vh29domain.org
search vh29domain.org
nameserver 10.0.29.1
[root@localhost Desktop]# cat /etc/network-scripts/ifcfg-eth0
cat: /etc/network-scripts/ifcfg-eth0: No such file or directory
[root@localhost Desktop]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE="eth0"
HWADDR="08:00:27:ED:92:65"
NM_CONTROLLED="yes"
ONBOOT="no"
[root@localhost Desktop]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=localhost.localdomain
[root@localhost Desktop]# 
```

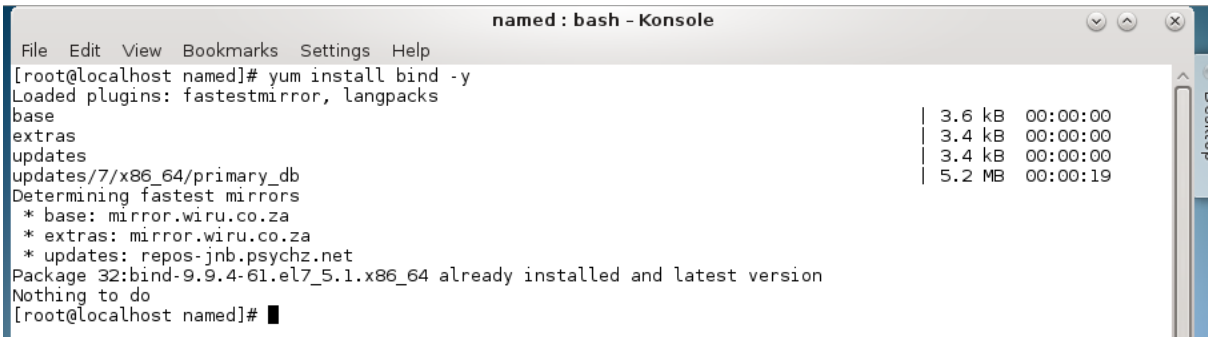
Figure 46

EVALUATION

I was able to learn how to configure the dhcp service. This was not as difficult as I initially thought and setting a fixed IP address was easy. The lab was straight forward an I achieved it (isc, 4).

LAB 5

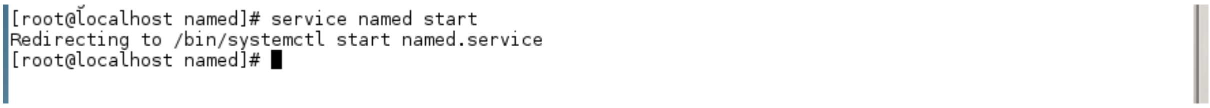
EXERCISE



```
[root@localhost named]# yum install bind -y
Loaded plugins: fastestmirror, langpacks
base                                                                     | 3.6 kB  00:00:00
extras                                                                   | 3.4 kB  00:00:00
updates                                                                  | 3.4 kB  00:00:00
updates/7/x86_64/primary_db                                              | 5.2 MB  00:00:19
Determining fastest mirrors
 * base: mirror.wiru.co.za
 * extras: mirror.wiru.co.za
 * updates: repos-jnb.psychz.net
Package 32:bind-9.9.4-61.el7_5.1.x86_64 already installed and latest version
Nothing to do
[root@localhost named]# 
```

Figure 47

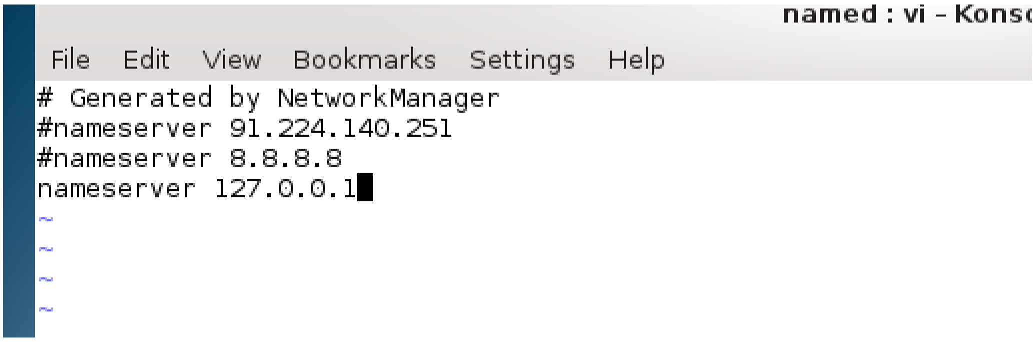
As shown in the image above, I was able to have the bind package installed which had the relevant packages.



```
[root@localhost named]# service named start
Redirecting to /bin/systemctl start named.service
[root@localhost named]# █
```

Figure 48

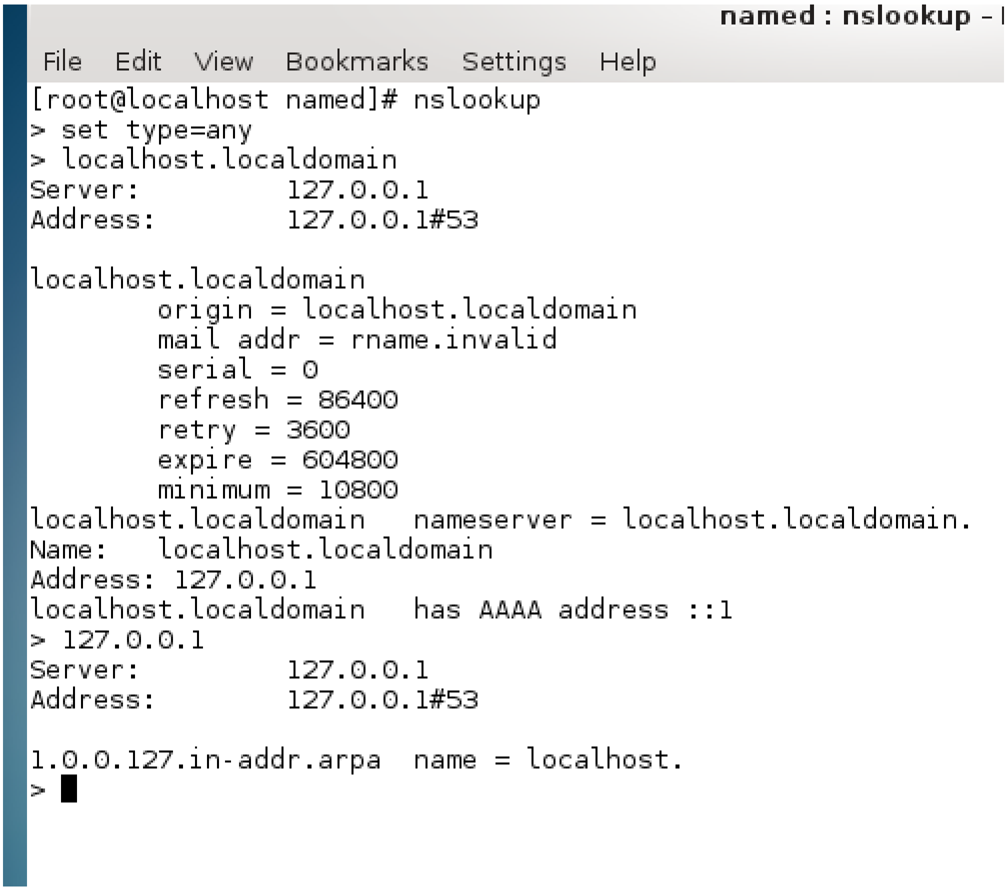
I then started the named service as shown above.



```
# Generated by NetworkManager
#nameserver 91.224.140.251
#nameserver 8.8.8.8
nameserver 127.0.0.1█
~
~
~
~
```

Figure 49

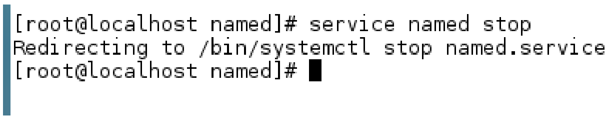
I then made my machine the resolver for DNS requests by modifying the /etc/resolv.conf.



```
[root@localhost named]# nslookup
> set type=any
> localhost.localdomain
Server:         127.0.0.1
Address:        127.0.0.1#53

localhost.localdomain
        origin = localhost.localdomain
        mail addr = rname.invalid
        serial = 0
        refresh = 86400
        retry = 3600
        expire = 604800
        minimum = 10800
localhost.localdomain   nameserver = localhost.localdomain.
Name:   localhost.localdomain
Address: 127.0.0.1
localhost.localdomain   has AAAA address ::1
> 127.0.0.1
Server:         127.0.0.1
Address:        127.0.0.1#53

1.0.0.127.in-addr.arpa  name = localhost.
> █
```

Figure 50

I then tested to see if my machine could resolve names using nslookup as shown above. It was able to resolve the name localhost.localdomain as shown in the image above.



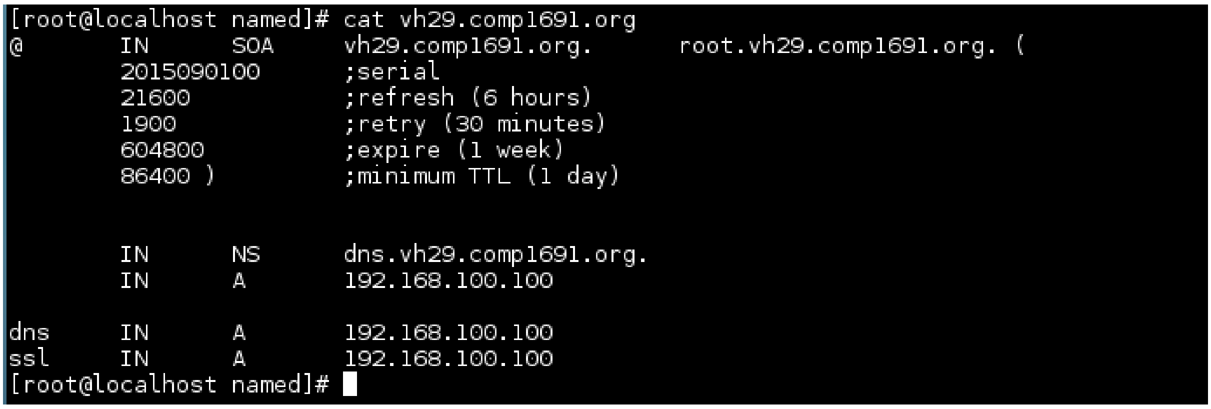
```
[root@localhost named]# service named stop
Redirecting to /bin/systemctl stop named.service
[root@localhost named]# █
```

Figure 51

I then stopped the service.

TASK

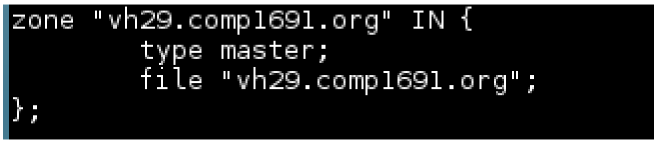
I entered the /var/named directory and created the zone file responsible for resolving the new name as shown below with the settings specified in the lab document.



```
[root@localhost named]# cat vh29.comp1691.org
@       IN      SOA     vh29.comp1691.org.      root.vh29.comp1691.org. (
        2015090100      ;serial
        21600           ;refresh (6 hours)
        1900            ;retry (30 minutes)
        604800          ;expire (1 week)
        86400 )         ;minimum TTL (1 day)


        IN      NS      dns.vh29.comp1691.org.
        IN      A       192.168.100.100

dns     IN      A       192.168.100.100
ssl     IN      A       192.168.100.100
[root@localhost named]# █
```

Figure 52

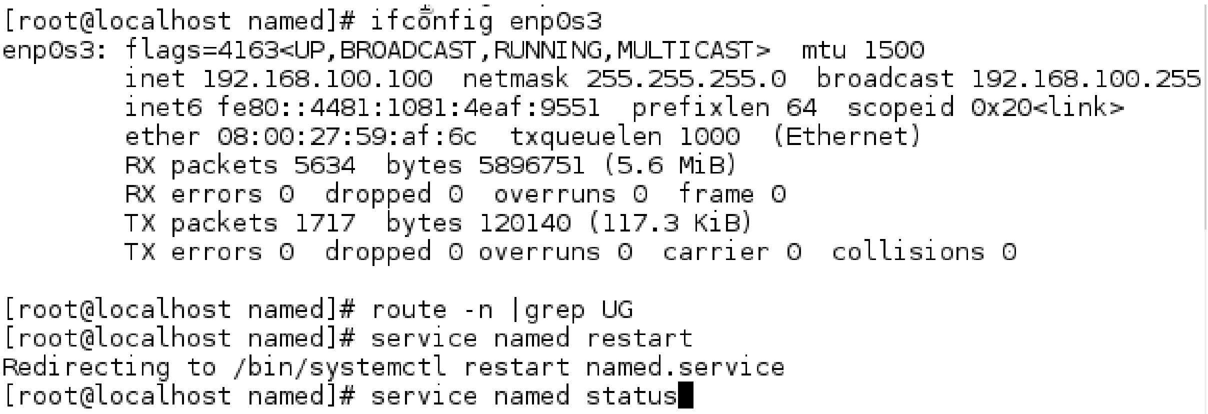
I then had to make an entry in the /etc/named.conf as shown below to point to that zone file.



```
zone "vh29.comp1691.org" IN {
        type master;
        file "vh29.comp1691.org";
};
```

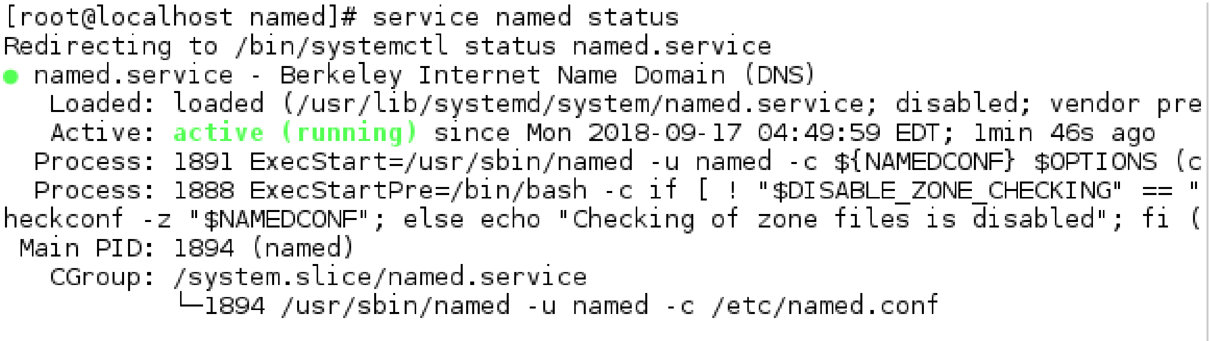
Figure 53

TESTING



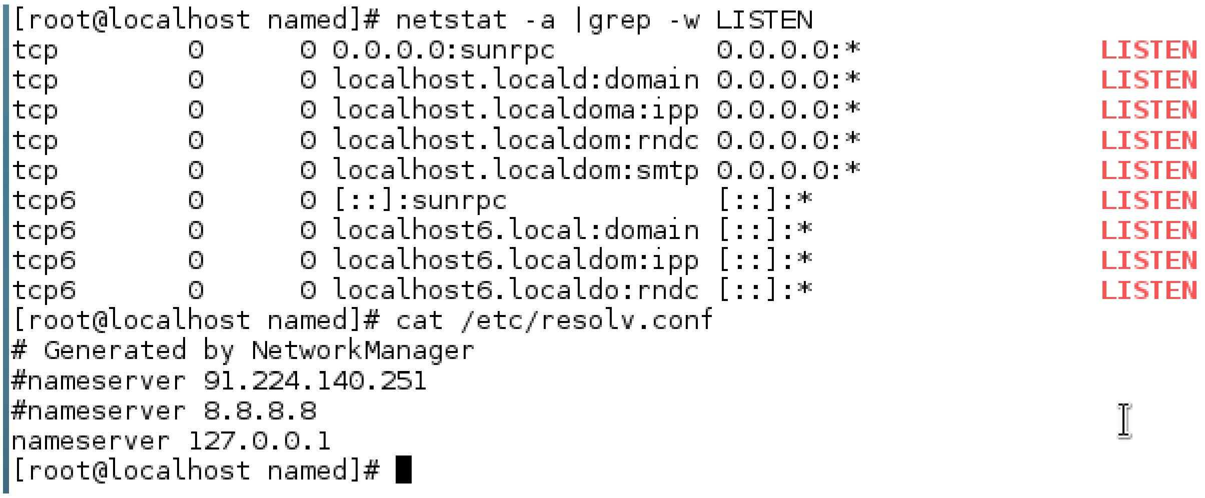
```
[root@localhost named]# ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.100  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::4481:1081:4eaf:9551  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:59:af:6c  txqueuelen 1000  (Ethernet)
        RX packets 5634  bytes 5896751 (5.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1717  bytes 120140 (117.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost named]# route -n |grep UG
[root@localhost named]# service named restart
Redirecting to /bin/systemctl restart named.service
[root@localhost named]# service named status
```

Figure 54



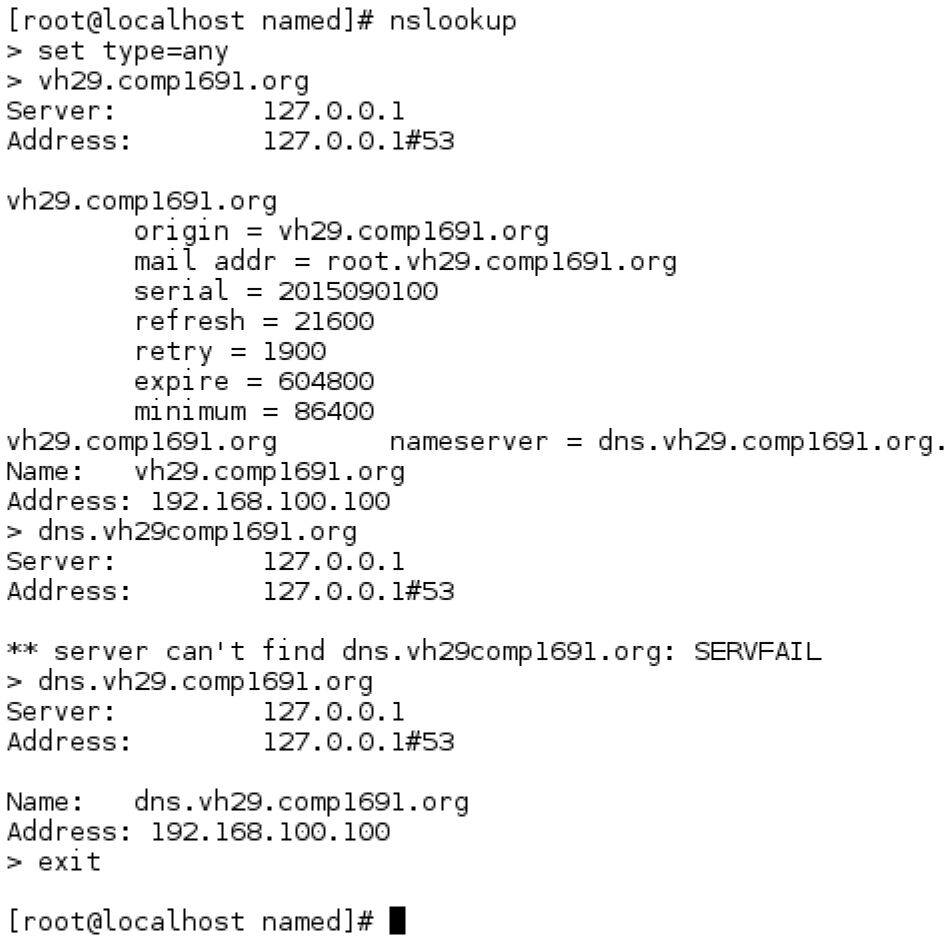
```
[root@localhost named]# service named status
Redirecting to /bin/systemctl status named.service
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; disabled; vendor pre
   Active: active (running) since Mon 2018-09-17 04:49:59 EDT; 1min 46s ago
  Process: 1891 ExecStart=/usr/sbin/named -u named -c ${NAMEDCONF} $OPTIONS (c
  Process: 1888 ExecStartPre=/bin/bash -c if [ ! "$DISABLE_ZONE_CHECKING" == "
heckconf -z "$NAMEDCONF"; else echo "Checking of zone files is disabled"; fi (
 Main PID: 1894 (named)
   CGroup: /system.slice/named.service
           └─1894 /usr/sbin/named -u named -c /etc/named.conf
```

Figure 55



```
[root@localhost named]# netstat -a |grep -w LISTEN
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 localhost.locald:domain 0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdoma:ipp 0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdom:rndc 0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*               LISTEN
tcp6       0      0 [::]:sunrpc             [::]:*                  LISTEN
tcp6       0      0 localhost6.local:domain [::]:*                  LISTEN
tcp6       0      0 localhost6.localdom:ipp [::]:*                  LISTEN
tcp6       0      0 localhost6.localdo:rndc [::]:*                  LISTEN
[root@localhost named]# cat /etc/resolv.conf
# Generated by NetworkManager
#nameserver 91.224.140.251
#nameserver 8.8.8.8
nameserver 127.0.0.1
[root@localhost named]#
```

Figure 56



```
[root@localhost named]# nslookup
> set type=any
> vh29.comp1691.org
Server:         127.0.0.1
Address:        127.0.0.1#53

vh29.comp1691.org
        origin = vh29.comp1691.org
        mail addr = root.vh29.comp1691.org
        serial = 2015090100
        refresh = 21600
        retry = 1900
        expire = 604800
        minimum = 86400
vh29.comp1691.org       nameserver = dns.vh29.comp1691.org.
Name:   vh29.comp1691.org
Address: 192.168.100.100
> dns.vh29comp1691.org
Server:         127.0.0.1
Address:        127.0.0.1#53

** server can't find dns.vh29comp1691.org: SERVFAIL
> dns.vh29.comp1691.org
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   dns.vh29.comp1691.org
Address: 192.168.100.100
> exit

[root@localhost named]# █
```

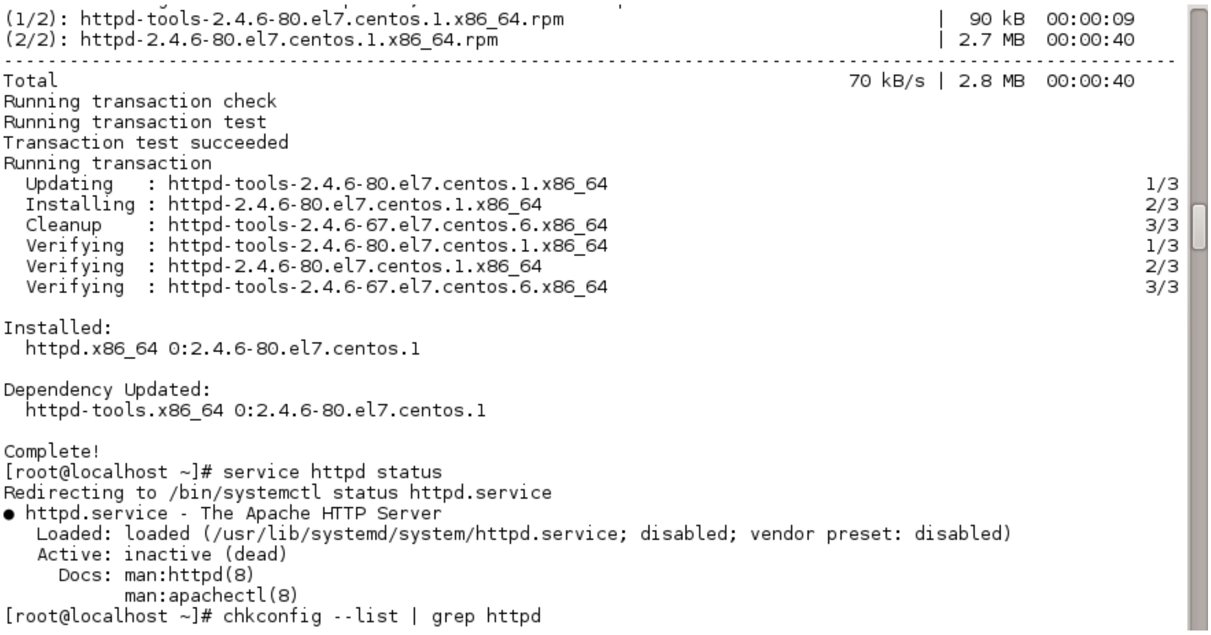
Figure 57

EVALUATION

I learnt how to install and configure the named service which does DNS. I was able to see how the files work and how to create a new zone from scratch (centos, 5).

LAB 6

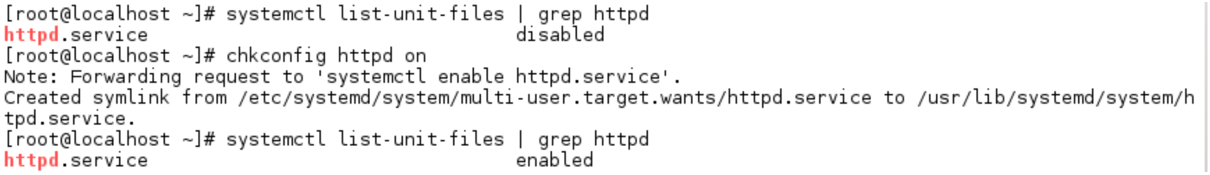
EXERCISE



```
(1/2): httpd-tools-2.4.6-80.el7.centos.1.x86_64.rpm                                    |  90 kB  00:00:09
(2/2): httpd-2.4.6-80.el7.centos.1.x86_64.rpm                                          | 2.7 MB  00:00:40
-----------------------------------------------------------------------------------------------------------
Total                                                                          70 kB/s | 2.8 MB  00:00:40
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Updating   : httpd-tools-2.4.6-80.el7.centos.1.x86_64                                                 1/3
  Installing : httpd-2.4.6-80.el7.centos.1.x86_64                                                       2/3
  Cleanup    : httpd-tools-2.4.6-67.el7.centos.6.x86_64                                                 3/3
  Verifying  : httpd-tools-2.4.6-80.el7.centos.1.x86_64                                                 1/3
  Verifying  : httpd-2.4.6-80.el7.centos.1.x86_64                                                       2/3
  Verifying  : httpd-tools-2.4.6-67.el7.centos.6.x86_64                                                 3/3

Installed:
  httpd.x86_64 0:2.4.6-80.el7.centos.1

Dependency Updated:
  httpd-tools.x86_64 0:2.4.6-80.el7.centos.1

Complete!
[root@localhost ~]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd(8)
           man:apachectl(8)
[root@localhost ~]# chkconfig --list | grep httpd
```

Figure 58

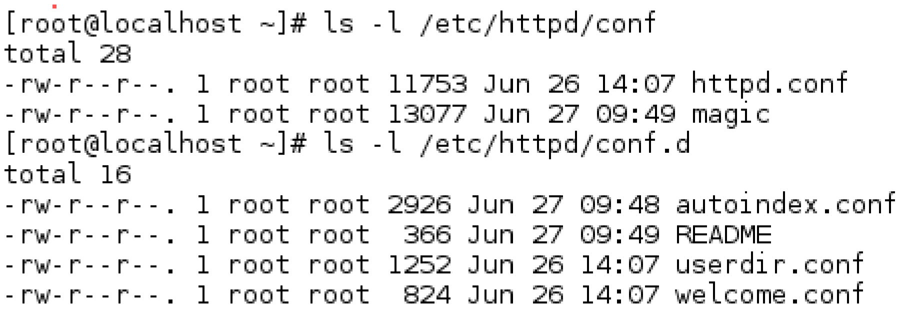
I installed the HTTP service as shown above. I also checked to see that it was not already running.



```
[root@localhost ~]# systemctl list-unit-files | grep httpd
httpd.service                                 disabled
[root@localhost ~]# chkconfig httpd on
Note: Forwarding request to 'systemctl enable httpd.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/h
tpd.service.
[root@localhost ~]# systemctl list-unit-files | grep httpd
httpd.service                                 enabled
```

Figure 59

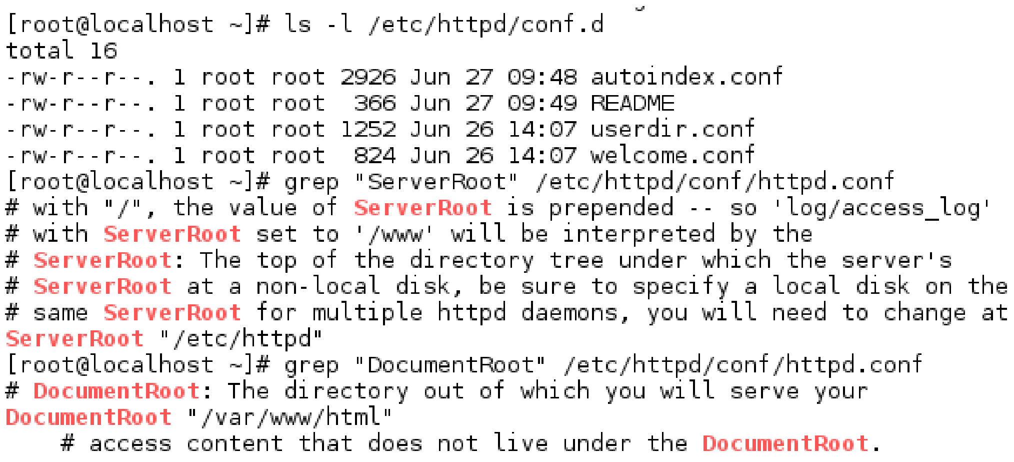
I then made sure that the service was able to start with the system as it booted so that I do not have to start it manually everytime.



```
[root@localhost ~]# ls -l /etc/httpd/conf
total 28
-rw-r--r--. 1 root root 11753 Jun 26 14:07 httpd.conf
-rw-r--r--. 1 root root 13077 Jun 27 09:49 magic
[root@localhost ~]# ls -l /etc/httpd/conf.d
total 16
-rw-r--r--. 1 root root 2926 Jun 27 09:48 autoindex.conf
-rw-r--r--. 1 root root  366 Jun 27 09:49 README
-rw-r--r--. 1 root root 1252 Jun 26 14:07 userdir.conf
-rw-r--r--. 1 root root  824 Jun 26 14:07 welcome.conf
```

Figure 60

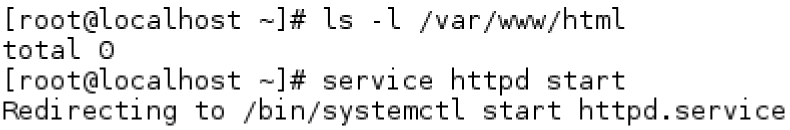
I then checked the location of the configuration files as shown above in the two directories.



```
[root@localhost ~]# ls -l /etc/httpd/conf.d
total 16
-rw-r--r--. 1 root root 2926 Jun 27 09:48 autoindex.conf
-rw-r--r--. 1 root root  366 Jun 27 09:49 README
-rw-r--r--. 1 root root 1252 Jun 26 14:07 userdir.conf
-rw-r--r--. 1 root root  824 Jun 26 14:07 welcome.conf
[root@localhost ~]# grep "ServerRoot" /etc/httpd/conf/httpd.conf
# with "/", the value of ServerRoot is prepended -- so 'log/access_log'
# with ServerRoot set to '/www' will be interpreted by the
# ServerRoot: The top of the directory tree under which the server's
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# same ServerRoot for multiple httpd daemons, you will need to change at
ServerRoot "/etc/httpd"
[root@localhost ~]# grep "DocumentRoot" /etc/httpd/conf/httpd.conf
# DocumentRoot: The directory out of which you will serve your
DocumentRoot "/var/www/html"
    # access content that does not live under the DocumentRoot.
```

Figure 61

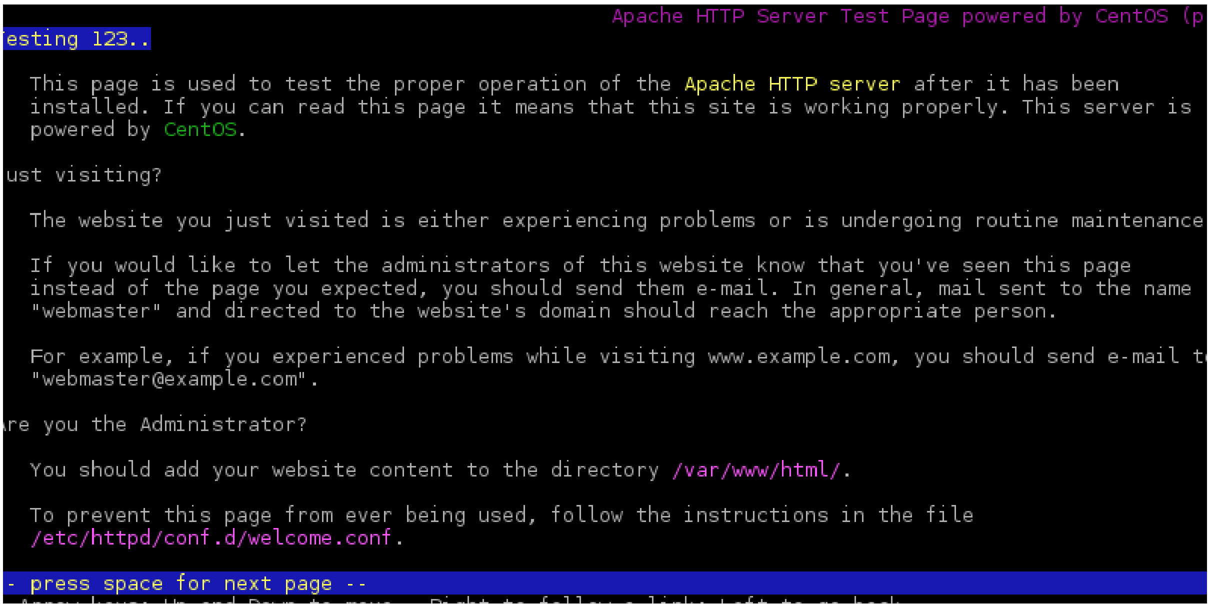
I was then able to open /etc/httpd/conf/httpd.conf and view the DocumentRoot as well as the ServerRoot. They are for the directories for the webpages and the location of the httpd binary.



```
[root@localhost ~]# ls -l /var/www/html
total 0
[root@localhost ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
```

Figure 62

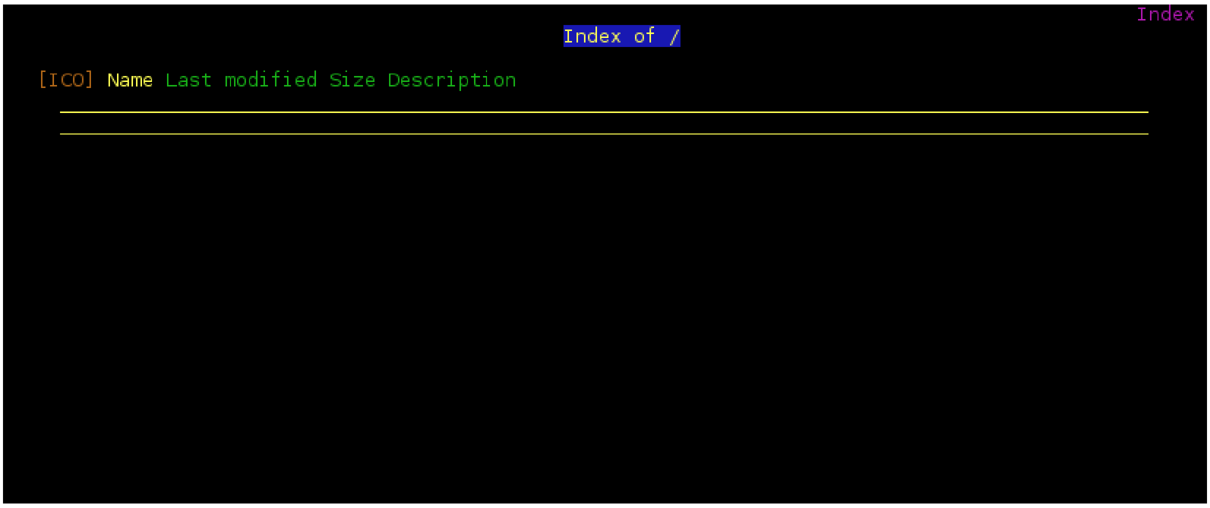
I then saw that the DocumentRoot wasy empty as shown above.



```
                                                   Apache HTTP Server Test Page powered by CentOS (p
esting 123..

  This page is used to test the proper operation of the Apache HTTP server after it has been
  installed. If you can read this page it means that this site is working properly. This server is
  powered by CentOS.

ust visiting?

  The website you just visited is either experiencing problems or is undergoing routine maintenance

  If you would like to let the administrators of this website know that you've seen this page
  instead of the page you expected, you should send them e-mail. In general, mail sent to the name
  "webmaster" and directed to the website's domain should reach the appropriate person.

  For example, if you experienced problems while visiting www.example.com, you should send e-mail t
  "webmaster@example.com".

re you the Administrator?

  You should add your website content to the directory /var/www/html/.

  To prevent this page from ever being used, follow the instructions in the file
  /etc/httpd/conf.d/welcome.conf.

- press space for next page --
```

Figure 63

I opened the localhost page and it still loaded a default page because of the configuration in the /etc/httpd/conf.d/welcome.conf file. To disable this page I simply commented all the lines in the file.



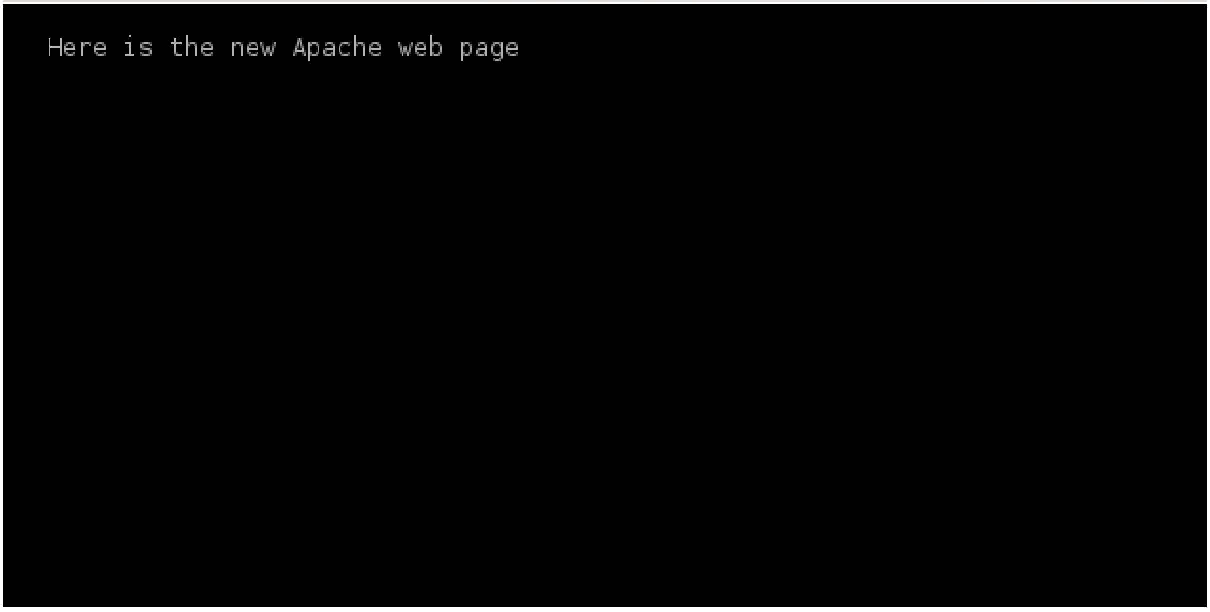
```
                                                  Index
                         Index of /

[ICO] Name Last modified Size Description
```

Figure 64

The image above shows the result of opening localhost with a disabled start page.

TASK

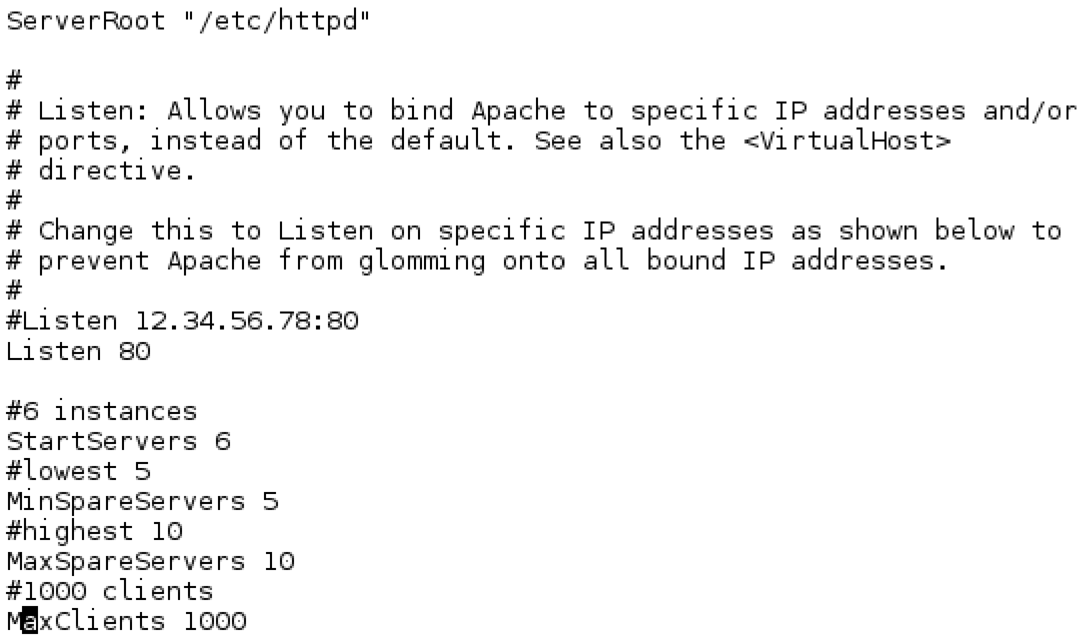
To do the task 1 I had to create a new index.html page in the DocumentRoot.



```
Here is the new Apache web page
```

Figure 65

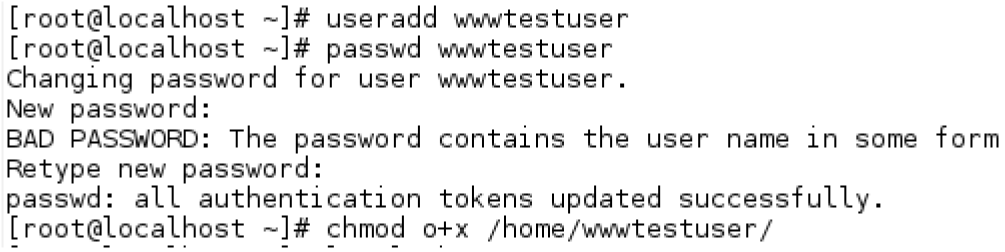
The figure above shows the file when I opened localhost.



```
ServerRoot "/etc/httpd"

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 80

#6 instances
StartServers 6
#lowest 5
MinSpareServers 5
#highest 10
MaxSpareServers 10
#1000 clients
MaxClients 1000
```

Figure 66

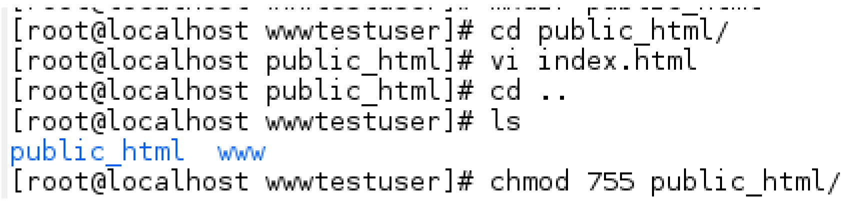
I then enabled the service to run with the set number of instances and clients in the /etc/httpd/conf/httpd.conf file as shown above.



```
[root@localhost ~]# useradd wwwtestuser
[root@localhost ~]# passwd wwwtestuser
Changing password for user wwwtestuser.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# chmod o+x /home/wwwtestuser/
```

Figure 67

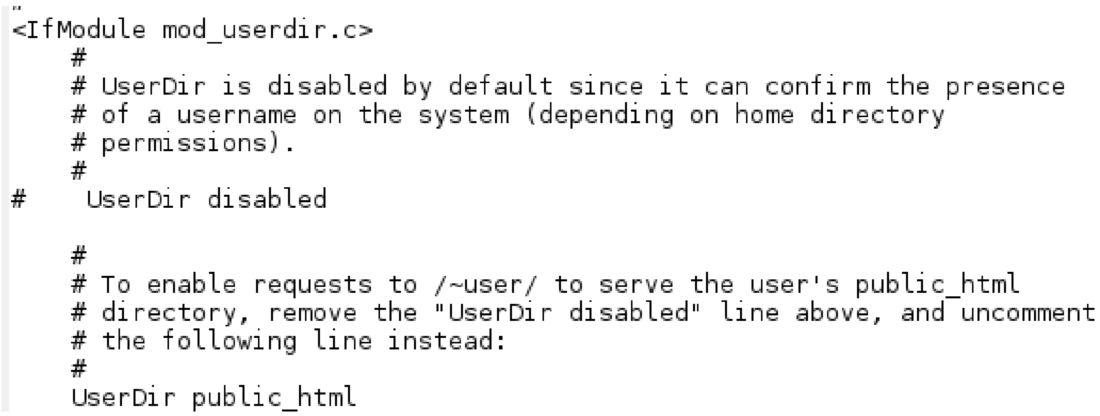
I then added the user account and set the permissions on the home directory to allow access from the outside by other users.



```
[root@localhost wwwtestuser]# cd public_html/
[root@localhost public_html]# vi index.html
[root@localhost public_html]# cd ..
[root@localhost wwwtestuser]# ls
public_html  www
[root@localhost wwwtestuser]# chmod 755 public_html/
```

Figure 68

I was then able to create the directory for the web pages and added an index page in it. I also added some permissions to the public_html directory I created.

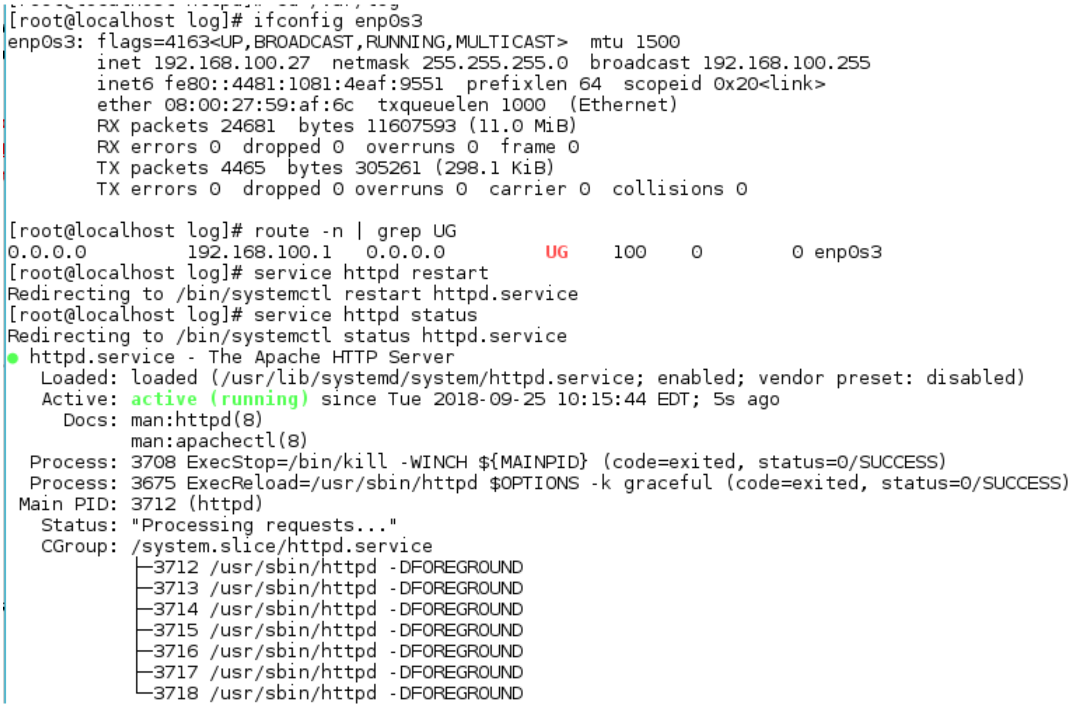


```
<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
#    UserDir disabled

    #
    # To enable requests to /~user/ to serve the user's public_html
    # directory, remove the "UserDir disabled" line above, and uncomment
    # the following line instead:
    #
    UserDir public_html
```

Figure 69

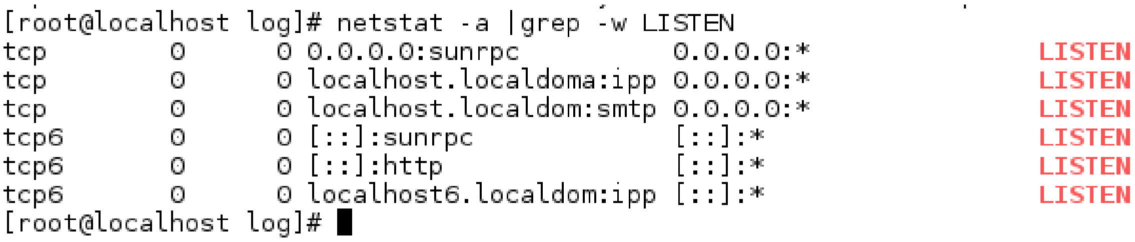
I then opened the /etc/httpd/conf.d/userdir.conf and enabled the home directories.

TESTING



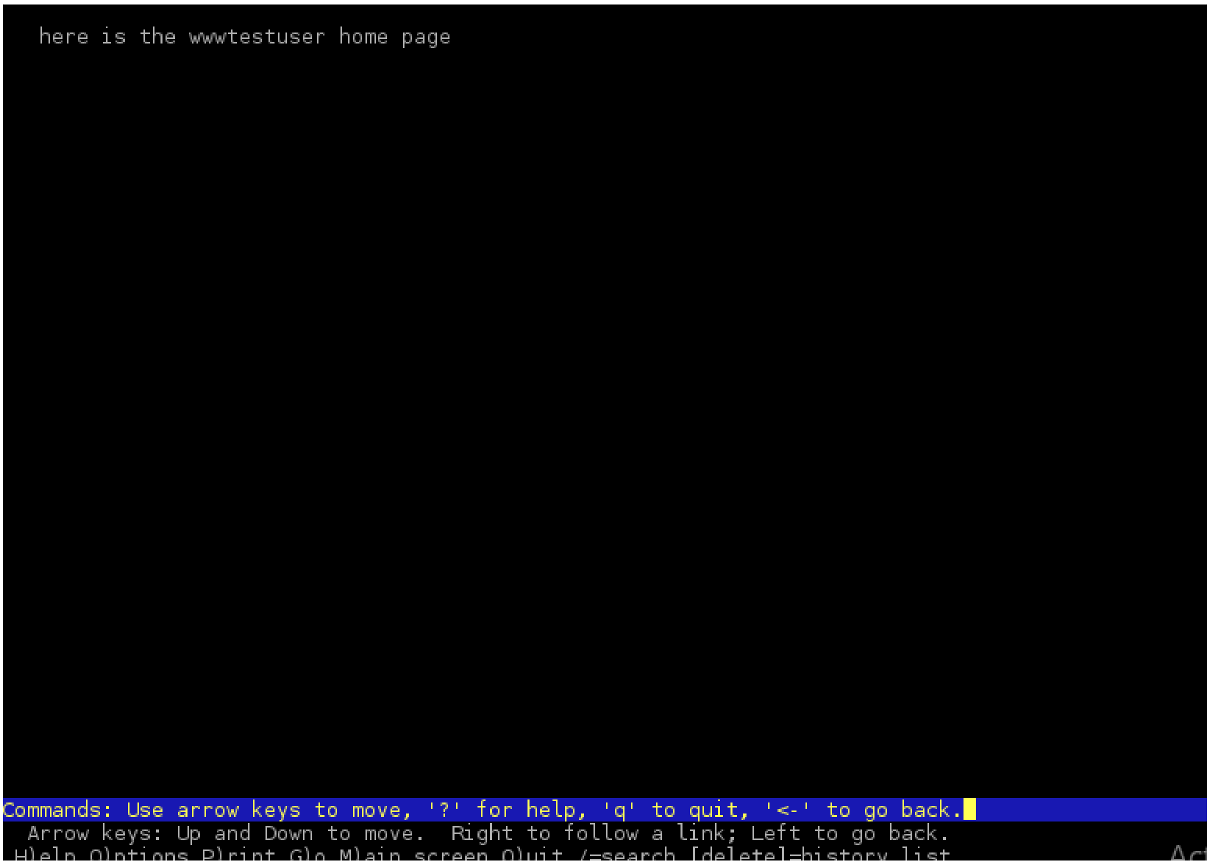
```
[root@localhost log]# ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.27  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::4481:1081:4eaf:9551  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:59:af:6c  txqueuelen 1000  (Ethernet)
        RX packets 24681  bytes 11607593 (11.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4465  bytes 305261 (298.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost log]# route -n | grep UG
0.0.0.0         192.168.100.1   0.0.0.0         UG    100    0        0 enp0s3
[root@localhost log]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@localhost log]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2018-09-25 10:15:44 EDT; 5s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 3708 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
  Process: 3675 ExecReload=/usr/sbin/httpd $OPTIONS -k graceful (code=exited, status=0/SUCCESS)
 Main PID: 3712 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─3712 /usr/sbin/httpd -DFOREGROUND
           ├─3713 /usr/sbin/httpd -DFOREGROUND
           ├─3714 /usr/sbin/httpd -DFOREGROUND
           ├─3715 /usr/sbin/httpd -DFOREGROUND
           ├─3716 /usr/sbin/httpd -DFOREGROUND
           ├─3717 /usr/sbin/httpd -DFOREGROUND
           └─3718 /usr/sbin/httpd -DFOREGROUND
```

Figure 70



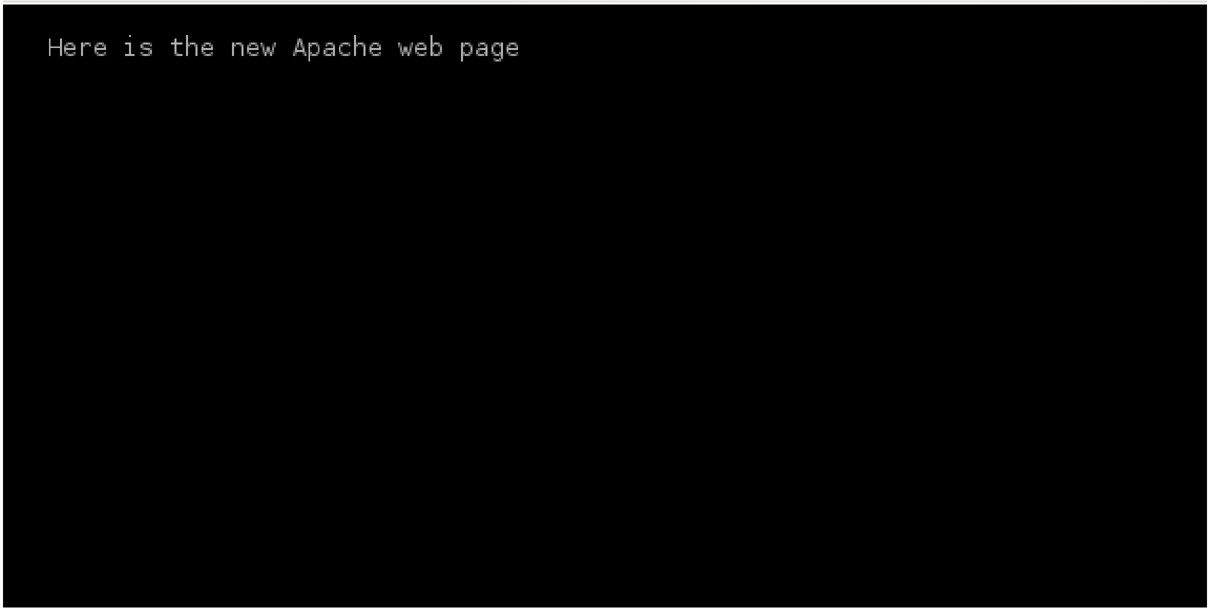
```
[root@localhost log]# netstat -a |grep -w LISTEN
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdoma:ipp 0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*               LISTEN
tcp6       0      0 [::]:sunrpc             [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 localhost6.localdom:ipp [::]:*                  LISTEN
[root@localhost log]# █
```

Figure 71



```
here is the wwwtestuser home page













Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<-' to go back.
 Arrow keys: Up and Down to move.  Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list
```

Figure 72



```
Here is the new Apache web page
```

Figure 73

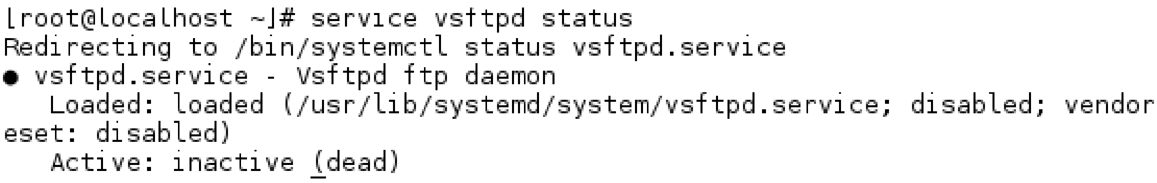
EVALUATION

I was able to learn how to configure the web service on a linux system and was able to view the locations of the different configuration files. I learnt how to configure certain options (redhat, 6). I saw some more options in the configuration files and I feel I know how to handle HTTP on Centos.

LAB 7

EXERCISE

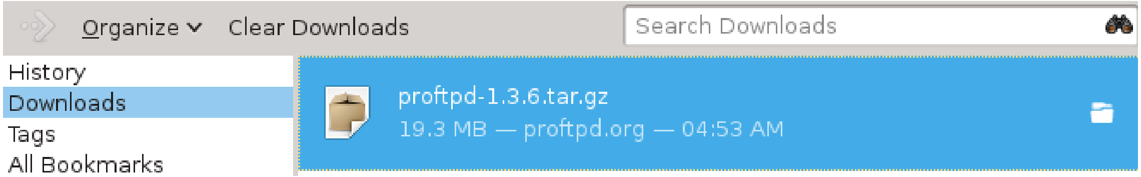
I was able to stop the vsftpd service as shown below it is not running.



```
[root@localhost ~]# service vsftpd status
Redirecting to /bin/systemctl status vsftpd.service
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; vendor
eset: disabled)
   Active: inactive (dead)
```

Figure 74

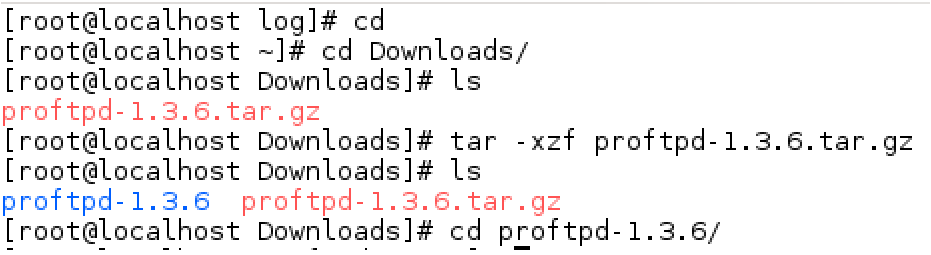
I was then able to download the proftpd service as shown in the image below.



proftpd-1.3.6.tar.gz
19.3 MB — proftpd.org — 04:53 AM

Figure 75

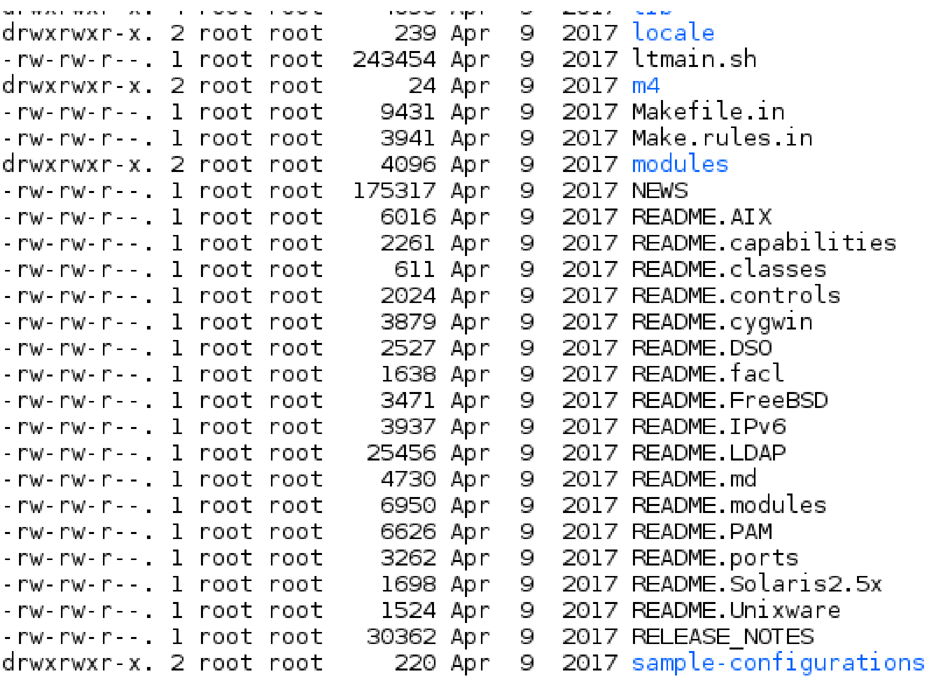
I extracted the archive and viewed the files that were extracted.



```
[root@localhost log]# cd
[root@localhost ~]# cd Downloads/
[root@localhost Downloads]# ls
proftpd-1.3.6.tar.gz
[root@localhost Downloads]# tar -xzf proftpd-1.3.6.tar.gz
[root@localhost Downloads]# ls
proftpd-1.3.6  proftpd-1.3.6.tar.gz
[root@localhost Downloads]# cd proftpd-1.3.6/
```

Figure 76

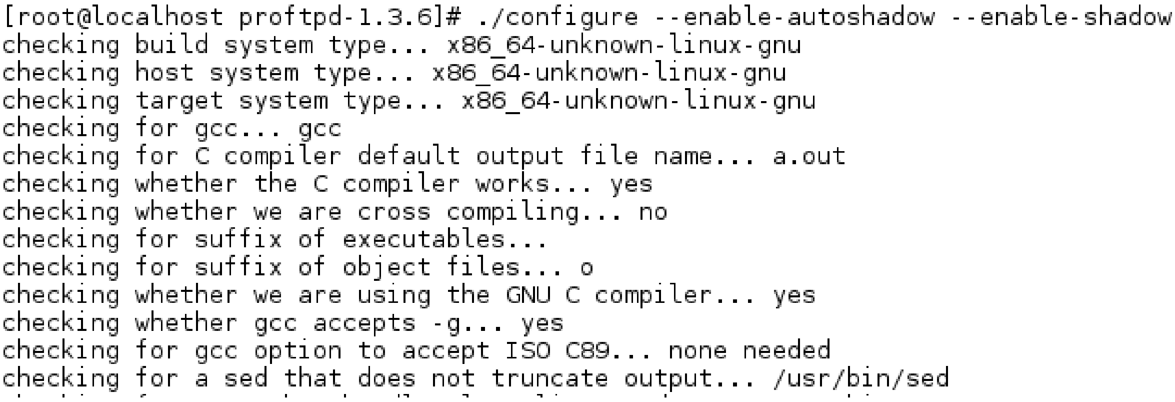
The folder had a number of files and others allow developers to customise the program before compilation while others were read me files and header files.



```
drwxrwxr-x. 2 root root     239 Apr  9  2017 locale
-rw-rw-r--. 1 root root  243454 Apr  9  2017 ltmain.sh
drwxrwxr-x. 2 root root      24 Apr  9  2017 m4
-rw-rw-r--. 1 root root    9431 Apr  9  2017 Makefile.in
-rw-rw-r--. 1 root root    3941 Apr  9  2017 Make.rules.in
drwxrwxr-x. 2 root root    4096 Apr  9  2017 modules
-rw-rw-r--. 1 root root  175317 Apr  9  2017 NEWS
-rw-rw-r--. 1 root root    6016 Apr  9  2017 README.AIX
-rw-rw-r--. 1 root root    2261 Apr  9  2017 README.capabilities
-rw-rw-r--. 1 root root     611 Apr  9  2017 README.classes
-rw-rw-r--. 1 root root    2024 Apr  9  2017 README.controls
-rw-rw-r--. 1 root root    3879 Apr  9  2017 README.cygwin
-rw-rw-r--. 1 root root    2527 Apr  9  2017 README.DSO
-rw-rw-r--. 1 root root    1638 Apr  9  2017 README.facl
-rw-rw-r--. 1 root root    3471 Apr  9  2017 README.FreeBSD
-rw-rw-r--. 1 root root    3937 Apr  9  2017 README.IPv6
-rw-rw-r--. 1 root root   25456 Apr  9  2017 README.LDAP
-rw-rw-r--. 1 root root    4730 Apr  9  2017 README.md
-rw-rw-r--. 1 root root    6950 Apr  9  2017 README.modules
-rw-rw-r--. 1 root root    6626 Apr  9  2017 README.PAM
-rw-rw-r--. 1 root root    3262 Apr  9  2017 README.ports
-rw-rw-r--. 1 root root    1698 Apr  9  2017 README.Solaris2.5x
-rw-rw-r--. 1 root root    1524 Apr  9  2017 README.Unixware
-rw-rw-r--. 1 root root   30362 Apr  9  2017 RELEASE_NOTES
drwxrwxr-x. 2 root root     220 Apr  9  2017 sample-configurations
```

Figure 77

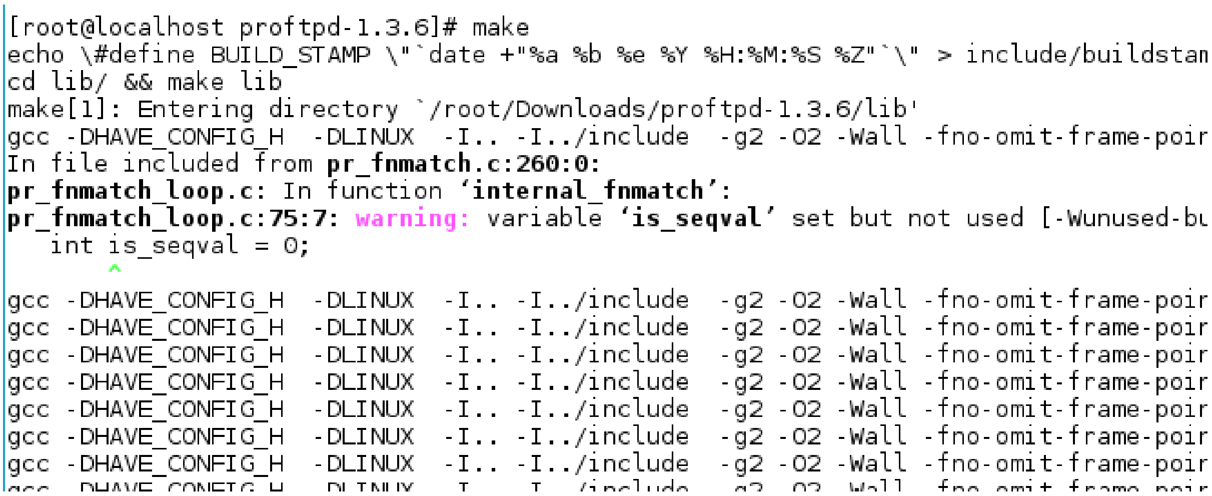
I then ran the configuration script as shown with the password access options enable shadow and enable auto shadow to grant access to the proftpd daemon towards the passwords.



```
[root@localhost proftpd-1.3.6]# ./configure --enable-autoshadow --enable-shadow
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking target system type... x86_64-unknown-linux-gnu
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking for a sed that does not truncate output... /usr/bin/sed
```

Figure 78

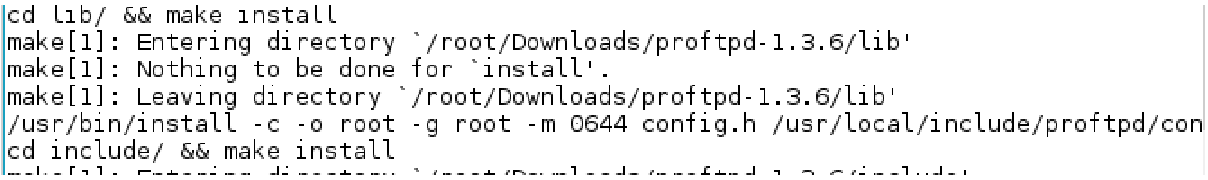
I was then able to compile the program as shown.



```
[root@localhost proftpd-1.3.6]# make
echo \#define BUILD_STAMP \"`date +"%a %b %e %Y %H:%M:%S %Z"`\" > include/buildstam
cd lib/ && make lib
make[1]: Entering directory `/root/Downloads/proftpd-1.3.6/lib'
gcc -DHAVE_CONFIG_H  -DLINUX  -I.. -I../include  -g2 -O2 -Wall -fno-omit-frame-poir
In file included from pr_fnmatch.c:260:0:
pr_fnmatch_loop.c: In function ‘internal_fnmatch’:
pr_fnmatch_loop.c:75:7: warning: variable ‘is_seqval’ set but not used [-Wunused-bu
   int is_seqval = 0;
       ^

gcc -DHAVE_CONFIG_H  -DLINUX  -I.. -I../include  -g2 -O2 -Wall -fno-omit-frame-poir
gcc -DHAVE_CONFIG_H  -DLINUX  -I.. -I../include  -g2 -O2 -Wall -fno-omit-frame-poir
gcc -DHAVE_CONFIG_H  -DLINUX  -I.. -I../include  -g2 -O2 -Wall -fno-omit-frame-poir
gcc -DHAVE_CONFIG_H  -DLINUX  -I.. -I../include  -g2 -O2 -Wall -fno-omit-frame-poir
gcc -DHAVE_CONFIG_H  -DLINUX  -I.. -I../include  -g2 -O2 -Wall -fno-omit-frame-poir
gcc -DHAVE_CONFIG_H  -DLINUX  -I.. -I../include  -g2 -O2 -Wall -fno-omit-frame-poir
gcc -DHAVE_CONFIG_H  -DLINUX  -I.. -I../include  -g2 -O2 -Wall -fno-omit-frame-poir
gcc -DHAVE_CONFIG_H  -DLINUX  -I.. -I../include  -g2 -O2 -Wall -fno-omit-frame-poir
```

Figure 79

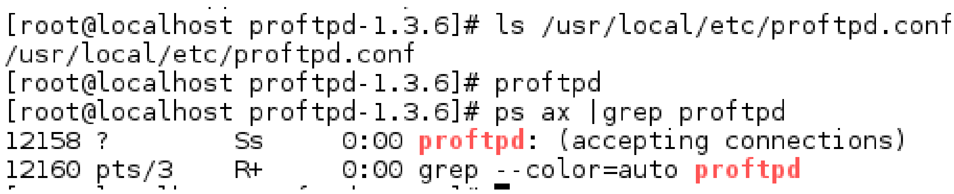
I installed the program after compiling.



```
cd lib/ && make install
make[1]: Entering directory `/root/Downloads/proftpd-1.3.6/lib'
make[1]: Nothing to be done for `install'.
make[1]: Leaving directory `/root/Downloads/proftpd-1.3.6/lib'
/usr/bin/install -c -o root -g root -m 0644 config.h /usr/local/include/proftpd/con
cd include/ && make install
make[1]: Entering directory `/root/Downloads/proftpd-1.3.6/include'
```

Figure 80

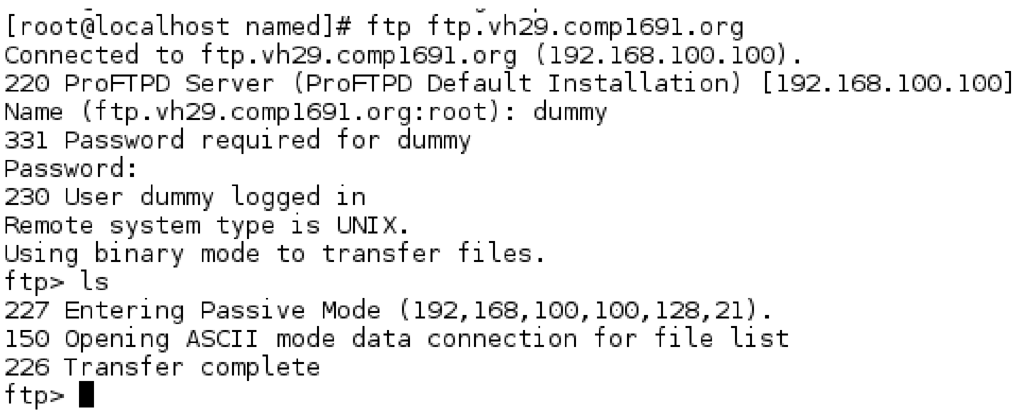
The configuration script was created and the service started fine. The process listing shows the daemon was fine.



```
[root@localhost proftpd-1.3.6]# ls /usr/local/etc/proftpd.conf
/usr/local/etc/proftpd.conf
[root@localhost proftpd-1.3.6]# proftpd
[root@localhost proftpd-1.3.6]# ps ax |grep proftpd
12158 ?        Ss     0:00 proftpd: (accepting connections)
12160 pts/3    R+     0:00 grep --color=auto proftpd
```

Figure 81

The configuration file was created and showed that the service was installed without an issue. I was then able to start the daemon.



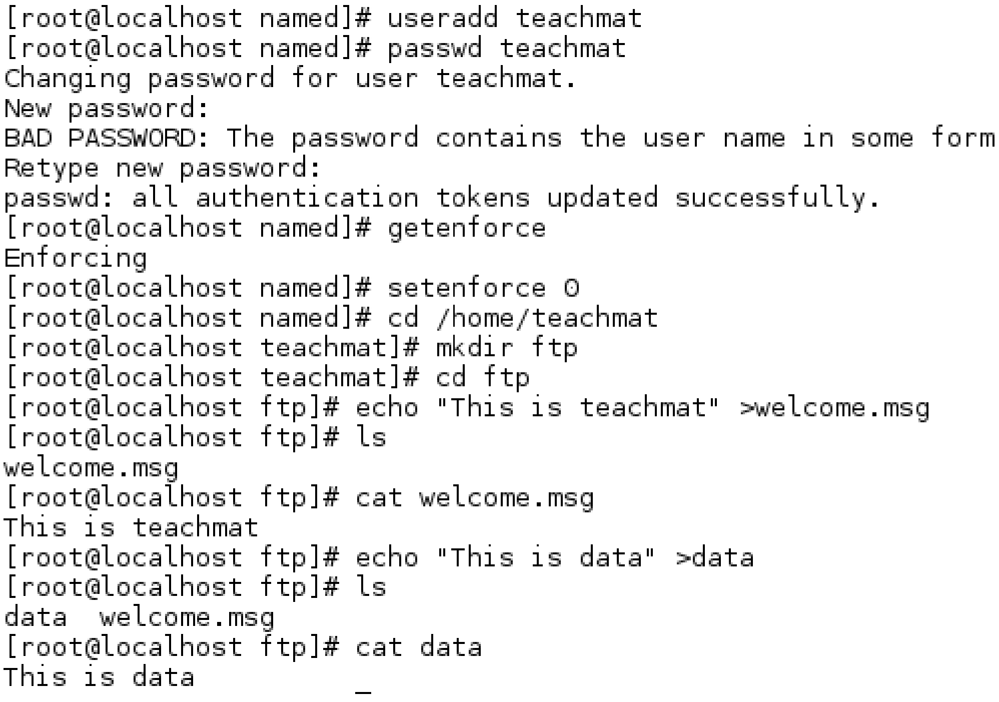
```
[root@localhost named]# ftp ftp.vh29.comp1691.org
Connected to ftp.vh29.comp1691.org (192.168.100.100).
220 ProFTPD Server (ProFTPD Default Installation) [192.168.100.100]
Name (ftp.vh29.comp1691.org:root): dummy
331 Password required for dummy
Password:
230 User dummy logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (192,168,100,100,128,21).
150 Opening ASCII mode data connection for file list
226 Transfer complete
ftp> █
```

Figure 82

I was also able to connect to the service even though the default configuration was not listing anything.

TASK

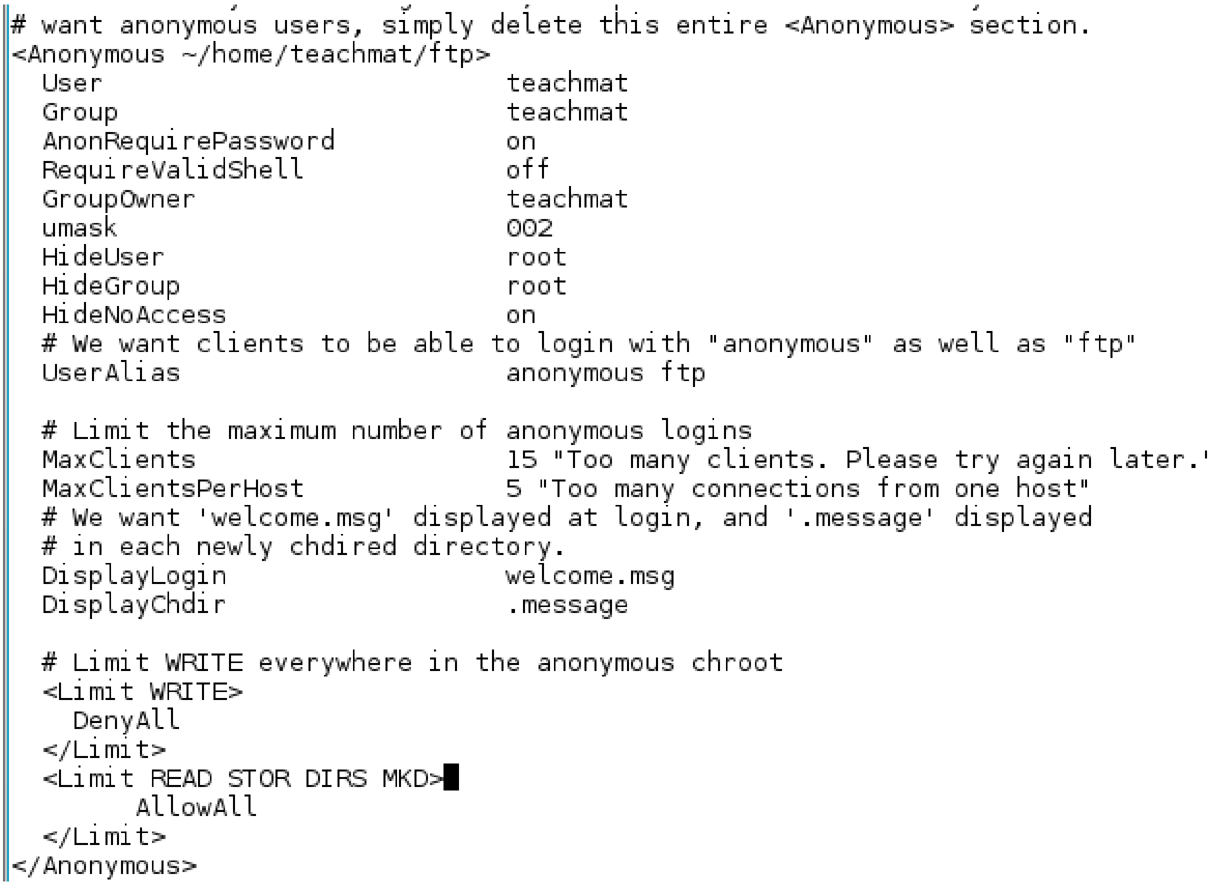
I completed the task by doing the following things in the screenshots. I added teachmat account, I removed selinux and created a directory called ftp in teachmat home. I also added the relevant message file and the sample data file.



```
[root@localhost named]# useradd teachmat
[root@localhost named]# passwd teachmat
Changing password for user teachmat.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost named]# getenforce
Enforcing
[root@localhost named]# setenforce 0
[root@localhost named]# cd /home/teachmat
[root@localhost teachmat]# mkdir ftp
[root@localhost teachmat]# cd ftp
[root@localhost ftp]# echo "This is teachmat" >welcome.msg
[root@localhost ftp]# ls
welcome.msg
[root@localhost ftp]# cat welcome.msg
This is teachmat
[root@localhost ftp]# echo "This is data" >data
[root@localhost ftp]# ls
data  welcome.msg
[root@localhost ftp]# cat data
This is data          _
```

Figure 83

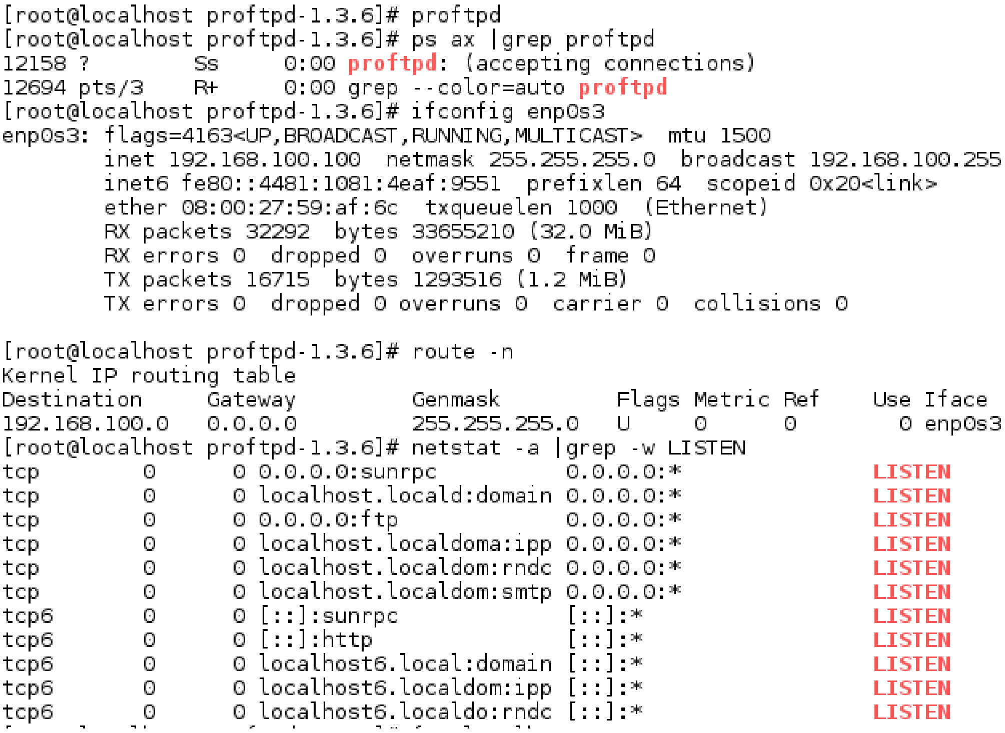
I then proceeded to create edit the /usr/local/etc/proftpd.conf as shown below.



```
# want anonymous users, simply delete this entire <Anonymous> section.
<Anonymous ~/home/teachmat/ftp>
  User                          teachmat
  Group                         teachmat
  AnonRequirePassword           on
  RequireValidShell             off
  GroupOwner                    teachmat
  umask                         002
  HideUser                      root
  HideGroup                     root
  HideNoAccess                  on
  # We want clients to be able to login with "anonymous" as well as "ftp"
  UserAlias                     anonymous ftp

  # Limit the maximum number of anonymous logins
  MaxClients                    15 "Too many clients. Please try again later.'
  MaxClientsPerHost             5 "Too many connections from one host"
  # We want 'welcome.msg' displayed at login, and '.message' displayed
  # in each newly chdired directory.
  DisplayLogin                  welcome.msg
  DisplayChdir                  .message

  # Limit WRITE everywhere in the anonymous chroot
  <Limit WRITE>
    DenyAll
  </Limit>
  <Limit READ STOR DIRS MKD>
        AllowAll
  </Limit>
</Anonymous>
```

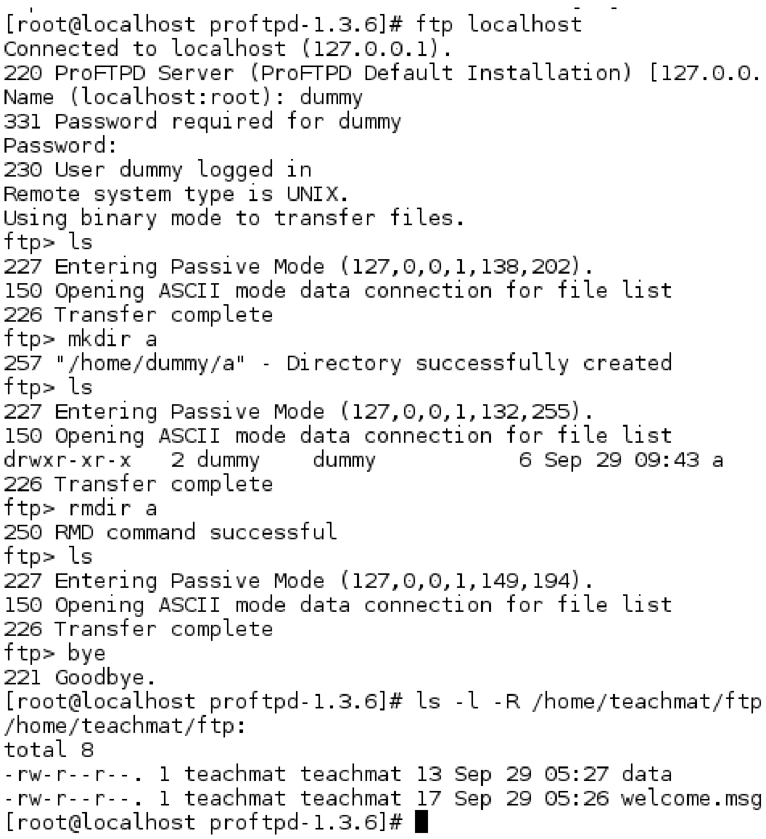
Figure 84

TESTING



```
[root@localhost proftpd-1.3.6]# proftpd
[root@localhost proftpd-1.3.6]# ps ax |grep proftpd
12158 ?        Ss     0:00 proftpd: (accepting connections)
12694 pts/3    R+     0:00 grep --color=auto proftpd
[root@localhost proftpd-1.3.6]# ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.100  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::4481:1081:4eaf:9551  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:59:af:6c  txqueuelen 1000  (Ethernet)
        RX packets 32292  bytes 33655210 (32.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16715  bytes 1293516 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@localhost proftpd-1.3.6]# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.100.0   0.0.0.0         255.255.255.0   U     0      0        0 enp0s3
[root@localhost proftpd-1.3.6]# netstat -a |grep -w LISTEN
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 localhost.locald:domain 0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:ftp             0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdoma:ipp 0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdom:rndc 0.0.0.0:*               LISTEN
tcp        0      0 localhost.localdom:smtp 0.0.0.0:*               LISTEN
tcp6       0      0 [::]:sunrpc             [::]:*                  LISTEN
tcp6       0      0 [::]:http               [::]:*                  LISTEN
tcp6       0      0 localhost6.local:domain [::]:*                  LISTEN
tcp6       0      0 localhost6.localdom:ipp [::]:*                  LISTEN
tcp6       0      0 localhost6.localdo:rndc [::]:*                  LISTEN
```

Figure 85



```
[root@localhost proftpd-1.3.6]# ftp localhost
Connected to localhost (127.0.0.1).
220 ProFTPD Server (ProFTPD Default Installation) [127.0.0.1]
Name (localhost:root): dummy
331 Password required for dummy
Password:
230 User dummy logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (127,0,0,1,138,202).
150 Opening ASCII mode data connection for file list
226 Transfer complete
ftp> mkdir a
257 "/home/dummy/a" - Directory successfully created
ftp> ls
227 Entering Passive Mode (127,0,0,1,132,255).
150 Opening ASCII mode data connection for file list
drwxr-xr-x   2 dummy    dummy           6 Sep 29 09:43 a
226 Transfer complete
ftp> rmdir a
250 RMD command successful
ftp> ls
227 Entering Passive Mode (127,0,0,1,149,194).
150 Opening ASCII mode data connection for file list
226 Transfer complete
ftp> bye
221 Goodbye.
[root@localhost proftpd-1.3.6]# ls -l -R /home/teachmat/ftp
/home/teachmat/ftp:
total 8
-rw-r--r--. 1 teachmat teachmat 13 Sep 29 05:27 data
-rw-r--r--. 1 teachmat teachmat 17 Sep 29 05:26 welcome.msg
[root@localhost proftpd-1.3.6]# █
```

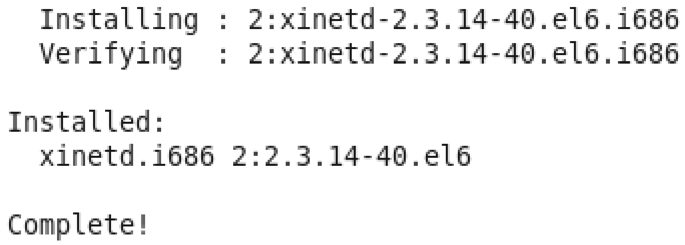
Figure 86

EVALUATION

The lab was very good and practicle. The different aspects of the task are realistic in that they are the most likely options to configure when deploying the service in the real world. The lab was fun because it had a different installation method from the others while still being easy enough to be carried out (doxer, 7).

LAB 8

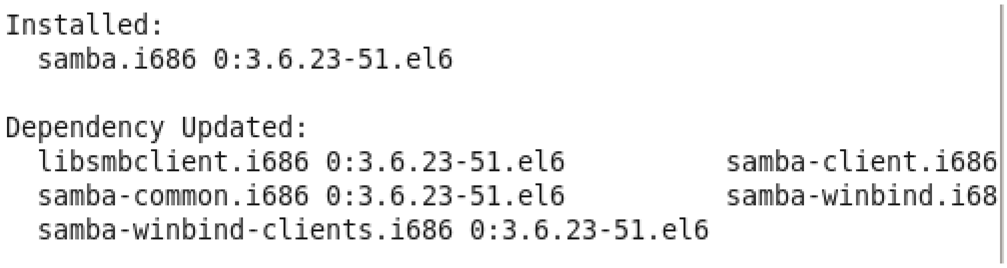
EXERCISE



```
  Installing : 2:xinetd-2.3.14-40.el6.i686
  Verifying  : 2:xinetd-2.3.14-40.el6.i686

Installed:
  xinetd.i686 2:2.3.14-40.el6

Complete!
```

Figure 87

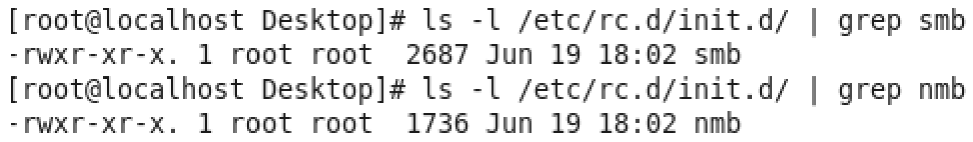
We installed the xinetd package.



```
Installed:
  samba.i686 0:3.6.23-51.el6

Dependency Updated:
  libsmbclient.i686 0:3.6.23-51.el6          samba-client.i686
  samba-common.i686 0:3.6.23-51.el6          samba-winbind.i68
  samba-winbind-clients.i686 0:3.6.23-51.el6
```

Figure 88

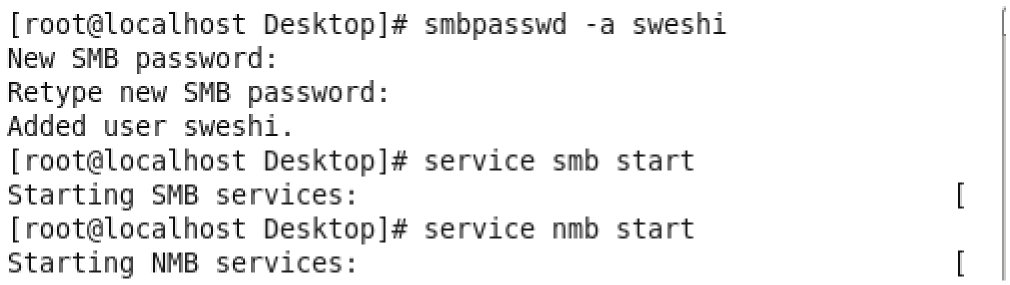
We also installed the samba service.



```
[root@localhost Desktop]# ls -l /etc/rc.d/init.d/ | grep smb
-rwxr-xr-x. 1 root root  2687 Jun 19 18:02 smb
[root@localhost Desktop]# ls -l /etc/rc.d/init.d/ | grep nmb
-rwxr-xr-x. 1 root root  1736 Jun 19 18:02 nmb
```

Figure 89

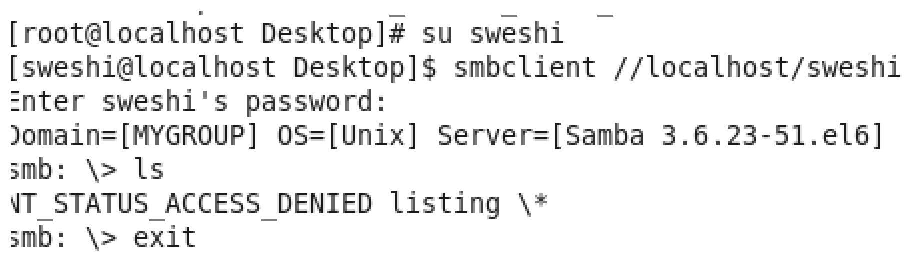
The files were present in the directory, both nmb and smb.



```
[root@localhost Desktop]# smbpasswd -a sweshi
New SMB password:
Retype new SMB password:
Added user sweshi.
[root@localhost Desktop]# service smb start
Starting SMB services:                                     [
[root@localhost Desktop]# service nmb start
Starting NMB services:                                     [
```

Figure 90

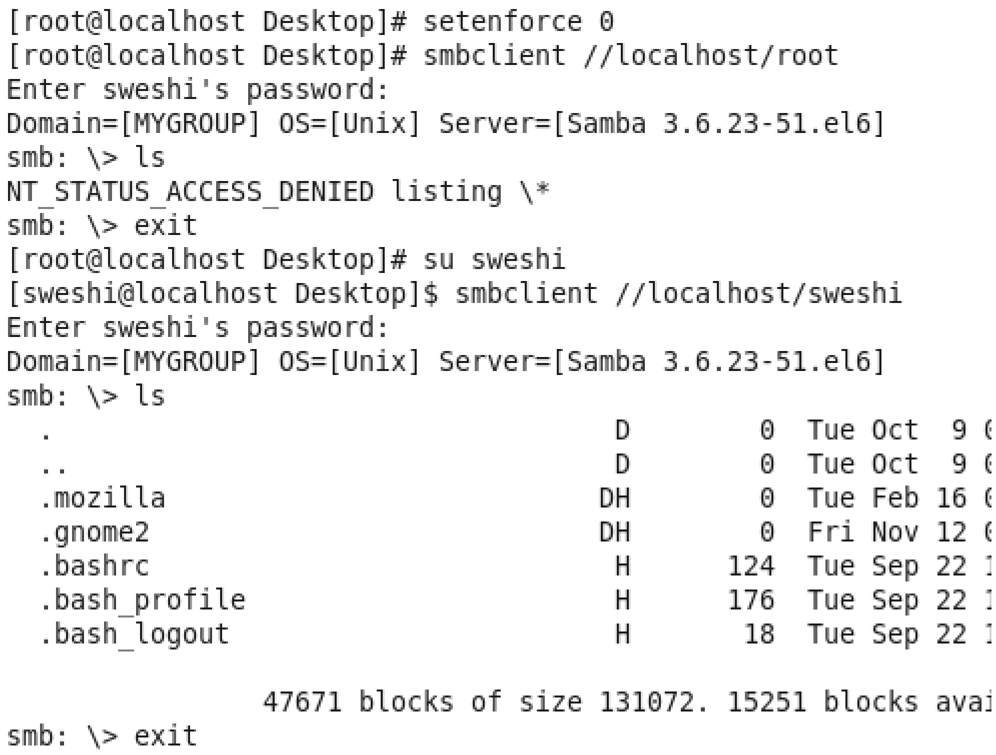
The user account was added to the system and then to the service.



```
[root@localhost Desktop]# su sweshi
[sweshi@localhost Desktop]$ smbclient //localhost/sweshi
Enter sweshi's password:
Domain=[MYGROUP] OS=[Unix] Server=[Samba 3.6.23-51.el6]
smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*
smb: \> exit
```

Figure 91

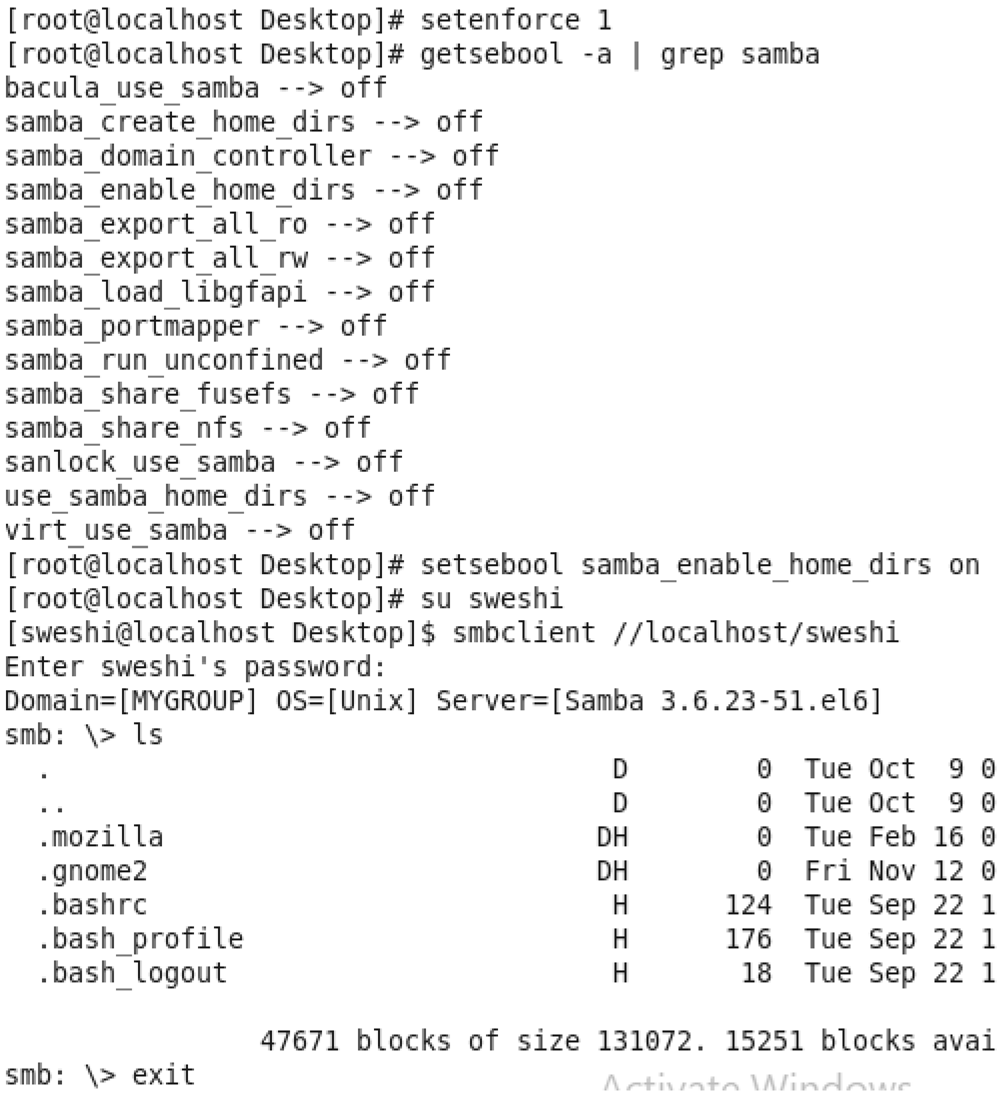
After setting browseable to yes, I tried logging on and listing. It denied to list.



```
[root@localhost Desktop]# setenforce 0
[root@localhost Desktop]# smbclient //localhost/root
Enter sweshi's password:
Domain=[MYGROUP] OS=[Unix] Server=[Samba 3.6.23-51.el6]
smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*
smb: \> exit
[root@localhost Desktop]# su sweshi
[sweshi@localhost Desktop]$ smbclient //localhost/sweshi
Enter sweshi's password:
Domain=[MYGROUP] OS=[Unix] Server=[Samba 3.6.23-51.el6]
smb: \> ls
  .                                   D        0  Tue Oct  9 0
  ..                                  D        0  Tue Oct  9 0
  .mozilla                           DH        0  Tue Feb 16 0
  .gnome2                            DH        0  Fri Nov 12 0
  .bashrc                             H      124  Tue Sep 22 1
  .bash_profile                       H      176  Tue Sep 22 1
  .bash_logout                        H       18  Tue Sep 22 1

                47671 blocks of size 131072. 15251 blocks avai
smb: \> exit
```

Figure 92

I then switched SELinux off and then tried to do it again. This time it managed.

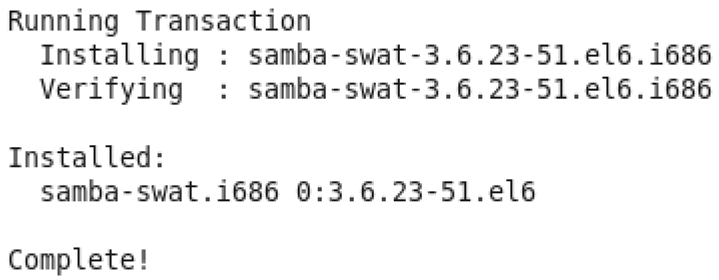


```
[root@localhost Desktop]# setenforce 1
[root@localhost Desktop]# getsebool -a | grep samba
bacula_use_samba --> off
samba_create_home_dirs --> off
samba_domain_controller --> off
samba_enable_home_dirs --> off
samba_export_all_ro --> off
samba_export_all_rw --> off
samba_load_libgfapi --> off
samba_portmapper --> off
samba_run_unconfined --> off
samba_share_fusefs --> off
samba_share_nfs --> off
sanlock_use_samba --> off
use_samba_home_dirs --> off
virt_use_samba --> off
[root@localhost Desktop]# setsebool samba_enable_home_dirs on
[root@localhost Desktop]# su sweshi
[sweshi@localhost Desktop]$ smbclient //localhost/sweshi
Enter sweshi's password:
Domain=[MYGROUP] OS=[Unix] Server=[Samba 3.6.23-51.el6]
smb: \> ls
  .                                   D        0  Tue Oct  9 0
  ..                                  D        0  Tue Oct  9 0
  .mozilla                           DH        0  Tue Feb 16 0
  .gnome2                            DH        0  Fri Nov 12 0
  .bashrc                             H      124  Tue Sep 22 1
  .bash_profile                       H      176  Tue Sep 22 1
  .bash_logout                        H       18  Tue Sep 22 1

                47671 blocks of size 131072. 15251 blocks avai
smb: \> exit
```

Figure 93

I then switched it off again. I looked for samba_enable_home_dirs and switched it on then tried the process again. This time it worked because I had enabled the home directory flag.

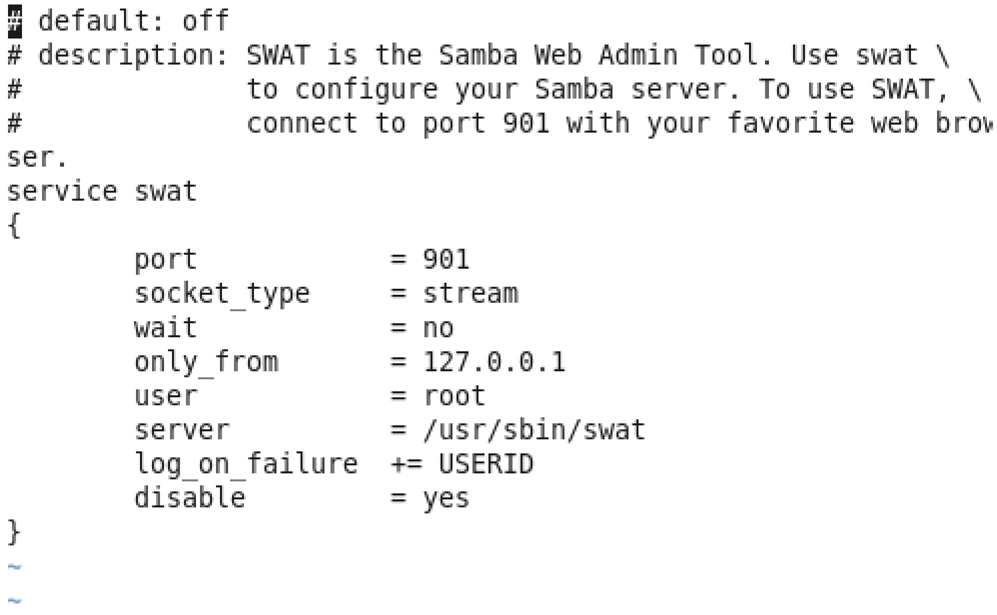
TASK



```
Running Transaction
  Installing : samba-swat-3.6.23-51.el6.i686
  Verifying  : samba-swat-3.6.23-51.el6.i686

Installed:
  samba-swat.i686 0:3.6.23-51.el6

Complete!
```

Figure 94

I installed samba-swat.

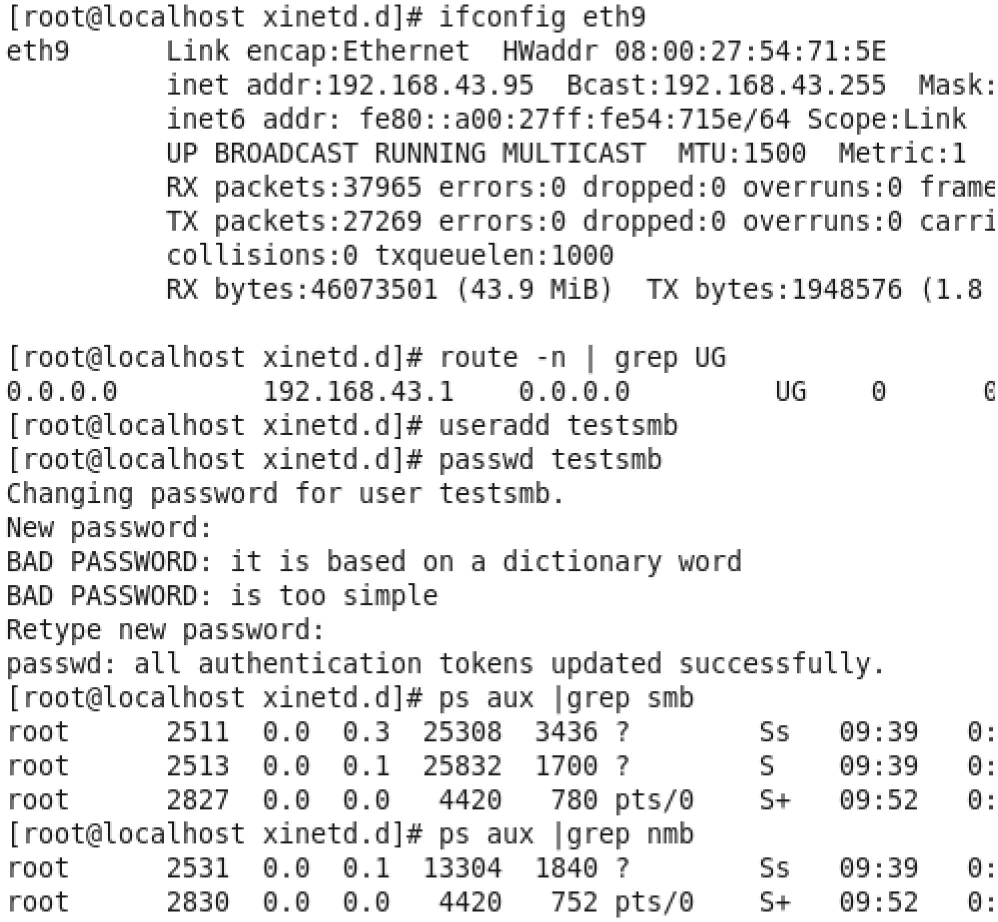


```
# default: off
# description: SWAT is the Samba Web Admin Tool. Use swat \
#              to configure your Samba server. To use SWAT, \
#              connect to port 901 with your favorite web brow
ser.
service swat
{
        port            = 901
        socket_type     = stream
        wait            = no
        only_from       = 127.0.0.1
        user            = root
        server          = /usr/sbin/swat
        log_on_failure  += USERID
        disable         = yes
}
~
~
```

Figure 95

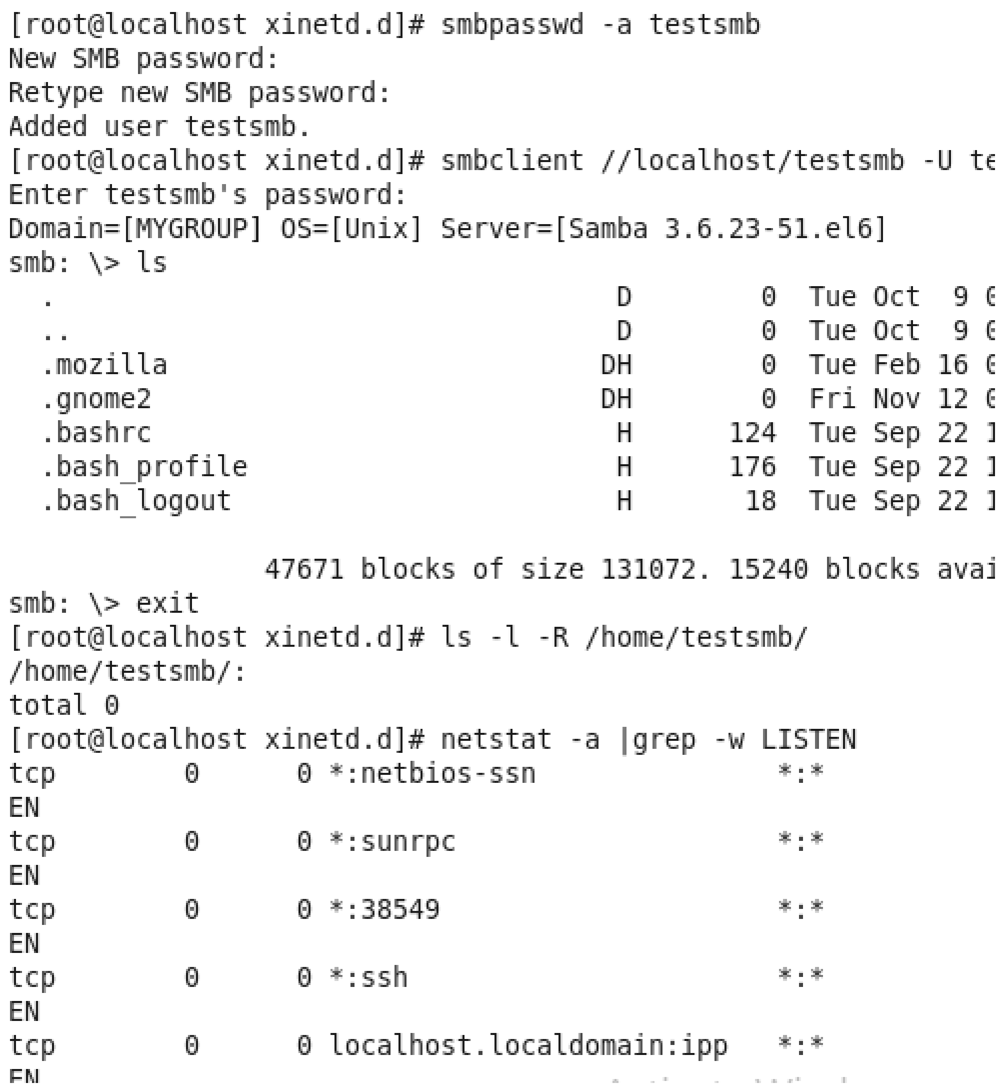
The configuration in /etc/xinetd.d was as shown above.

TESTING



```
[root@localhost xinetd.d]# ifconfig eth9
eth9      Link encap:Ethernet  HWaddr 08:00:27:54:71:5E
          inet addr:192.168.43.95  Bcast:192.168.43.255  Mask:
          inet6 addr: fe80::a00:27ff:fe54:715e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37965 errors:0 dropped:0 overruns:0 frame
          TX packets:27269 errors:0 dropped:0 overruns:0 carri
          collisions:0 txqueuelen:1000
          RX bytes:46073501 (43.9 MiB)  TX bytes:1948576 (1.8

[root@localhost xinetd.d]# route -n | grep UG
0.0.0.0         192.168.43.1    0.0.0.0         UG    0      0
[root@localhost xinetd.d]# useradd testsmb
[root@localhost xinetd.d]# passwd testsmb
Changing password for user testsmb.
New password:
BAD PASSWORD: it is based on a dictionary word
BAD PASSWORD: is too simple
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost xinetd.d]# ps aux |grep smb
root      2511  0.0  0.3  25308  3436 ?        Ss   09:39   0:
root      2513  0.0  0.1  25832  1700 ?        S    09:39   0:
root      2827  0.0  0.0   4420   780 pts/0    S+   09:52   0:
[root@localhost xinetd.d]# ps aux |grep nmb
root      2531  0.0  0.1  13304  1840 ?        Ss   09:39   0:
root      2830  0.0  0.0   4420   752 pts/0    S+   09:52   0:
```

Figure 96



```
[root@localhost xinetd.d]# smbpasswd -a testsmb
New SMB password:
Retype new SMB password:
Added user testsmb.
[root@localhost xinetd.d]# smbclient //localhost/testsmb -U te
Enter testsmb's password:
Domain=[MYGROUP] OS=[Unix] Server=[Samba 3.6.23-51.el6]
smb: \> ls
  .                                   D        0  Tue Oct  9 0
  ..                                  D        0  Tue Oct  9 0
  .mozilla                           DH        0  Tue Feb 16 0
  .gnome2                            DH        0  Fri Nov 12 0
  .bashrc                             H      124  Tue Sep 22 1
  .bash_profile                       H      176  Tue Sep 22 1
  .bash_logout                        H       18  Tue Sep 22 1

                47671 blocks of size 131072. 15240 blocks avai
smb: \> exit
[root@localhost xinetd.d]# ls -l -R /home/testsmb/
/home/testsmb/:
total 0
[root@localhost xinetd.d]# netstat -a |grep -w LISTEN
tcp        0      0 *:netbios-ssn               *:*
EN
tcp        0      0 *:sunrpc                    *:*
EN
tcp        0      0 *:38549                     *:*
EN
tcp        0      0 *:ssh                       *:*
EN
tcp        0      0 localhost.localdomain:ipp   *:*
EN
```

Figure 97

EVALUATION

The samba service was easy to configure. I was able to set the service running correctly in a few minutes with the group (unix, 8). I was able to see the SELinux section in theee /etc/samba/smb.conf. I was able to enable home directories. I also saw how the SELinux was being used to restrict samba listing of directories which is for security. Overall, the lab was easy to follow and I learnt a number of things while doing it (rbgeek, 9).

REFERENCES

1. Techbrown, How to create a user without using the useradd command on Linux, https://www.techbrown.com/create-user-without-using-useradd-command-linux/ - 9/9/2018
2. Linuxhelp, creating an account without the user add on linux system, https://www.linuxhelp.com/how-to-create-a-user-without-useradd-command, - 9/9/2018
3. Ramesh Natarajan, Linux IPtables: How to Add Firewall Rules (With Allow SSH Example), https://www.thegeekstuff.com/2011/02/iptables-add-rule, 10/9/2018

4. Isc, dhcpd.conf, https://www.isc.org/wp-content/uploads/2017/08/dhcp41conf.html, - 15/9/2018
5. Centos, /etc/named.conf, https://www.centos.org/docs/5/html/Deployment_Guide-en-US/s1-bind-namedconf.html, - 20/9/2018
6. Redhat, starting and stopping the httpd service, https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/5/html/deployment_guide/s1-apache-startstop, - 23/9/2018
7. Doxfer, ProFTPD server, https://doxfer.webmin.com/Webmin/ProFTPD_Server- 25/9/2018
8. Unix, install and Configure Samba Server in Centos 7, https://www.unixmen.com/install-configure-samba-server-centos-7/ , 1/10/2018
9. Rbgeek, How to install Samba server on CentOS 6, https://rbgeek.wordpress.com/2012/05/25/how-to-install-samba-server-on-centos-6/ - 6/9/2018