

Singapore Polytechnic
ST2613 Securing Linux
Assignment

Lecturer: Mr Karl Kwan

Done by:

Lim Yong Kang, Bryan (P1707139)
Trovald Ong Chu Hao (P1703218)

Class:

DISM/FT/2B/21

Problem 1: Recover or reset root password.	4
Figure 1.0(bios settings)	4
Figure 1.1(VM iso image settings)	5
Figure 1.2(Troubleshoot screen)	5
Figure 1.3(Rescue screen)	6
Figure 1.4(Rescue mode)	7
Figure 1.5(Shell screen)	7
Problem 2: Setting an IP address to static.	8
Figure 2.0(Nmtui screen)	8
Figure 2.1(Edit settings)	9
Figure 2.2(Edit connection)	9
Problem 3: Changing the message at the login prompt.	10
Figure 3.0 (Message prompt)	10
Figure 3.1 (Editing message)	10
Problem 4: Viewing web pages on the web server.	10
Figure 4.0 (netstat)	10
Figure 4.1 (ls webpages)	10
Figure 4.2 (edit webpages)	11
Figure 4.3 (nginx config)	11
Problem 5: Help Bill and Bob regarding passwords and file permissions in web pages.	12
Figure 5.0 (password change)	12
Problem 6: Allow Bill and Bob to have access to server remotely and have access only to Department A's web pages.	12
Figure 6.0 (edit samba)	12
Figure 6.1 (making samba config)	13
Problem 7: Disabling the web server from accessing Bob's directory.	13
Figure 7.0(Nginx config deny)	13
Problem 8: Department C unable to view the web pages.	13
Figure 8.0(ls)	14
Figure 8.1(ls in webpages)	14
Figure 8.2(remap)	14
Problem 9: Records disappearing from the /var/log/secure file.	14

Figure 9.0 (var/spool)	14
Figure 9.1 (commenting the cronjob)	15
Figure 9.2(checking whether logs are there)	15
Problem 10: FTP is able to download files from other directories, only allow FTP to to download files from /var/ftp/pub.	15
Figure 10.0 (changin anon root)	15
Figure 10.1(enable local)	16
Problem 11: Configure a server for any file that is downloaded using FTP will be logged into a file.	16
Figure 11.0(enable loggings)	16
Figure 11.1(logging)	16
Problem 12: Why is date not working, what is wrong with ssh and disabling TFTP.	16
Figure 12.0(echo \$PATH)	17
Figure 12.1(which -a)	17
Figure 12.2(editing .bash_profile)	17
Figure 12.3(checking date command)	18
Figure 12.4(ssh localhost)	18
Figure 12.5(editing sshd_config)	18
Figure 12.6(connection reset by peer)	18
Figure 12.7(edit hosts.deny)	19
Figure 12.8(checking sshd)	19
Figure 12.9(netstat 69)	19
Figure 12.10(checking files for tftp)	20
Figure 12.11(editing xinetd.d)	20
Problem 13: Enable firewall and deny any IPv4 traffic to the server from a computer in Department D.	20
Figure 13.0 (rich rules)	21
Figure 13.1 (firewall changes)	21

Problem 1: Recover or reset root password.

We are first greeted with a server that we have no access to. To reset the root password or to recover to root password we first have to boot up grub menu. However the previous administrator has disabled grub or has set grub to only appear for 0s. This means that the option to reset the password using grub is invalid. To counter this problem we need to go into troubleshoot mode.

- Boot up the VM machine.
- Access the BIOS menu by repeatedly pressing the F2 key.
- Once BIOS has started, navigate to boot and set "CD-ROM" Drive as the first priority.

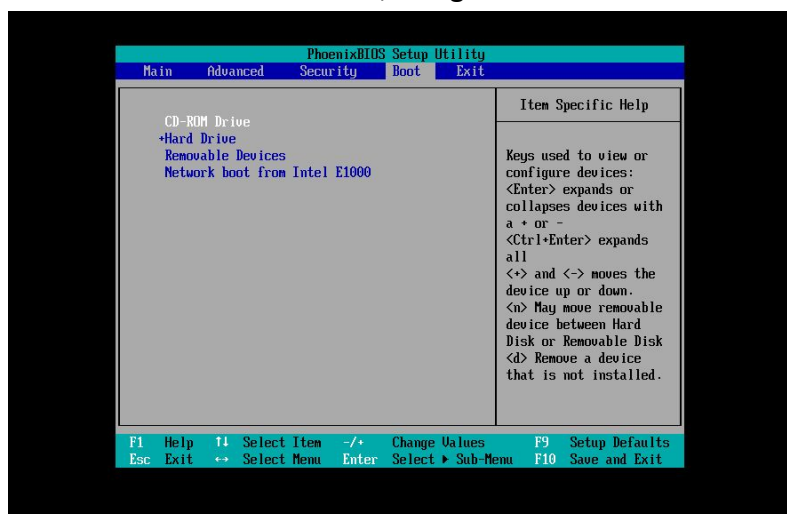


Figure 1.0(bios settings)

- Use an ISO image file from your file system and connect it to the VM machine.

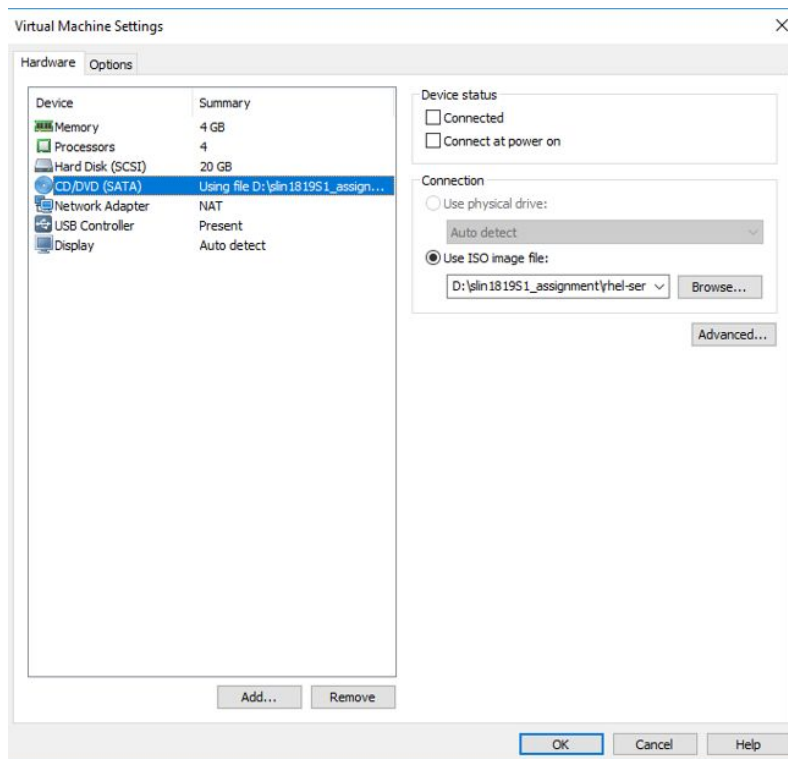


Figure 1.1(VM iso image settings)

- Restart the VM machine.
- When the VM machine has been started up once again, we will see a different menu.
- This menu is known as troubleshoot menu.

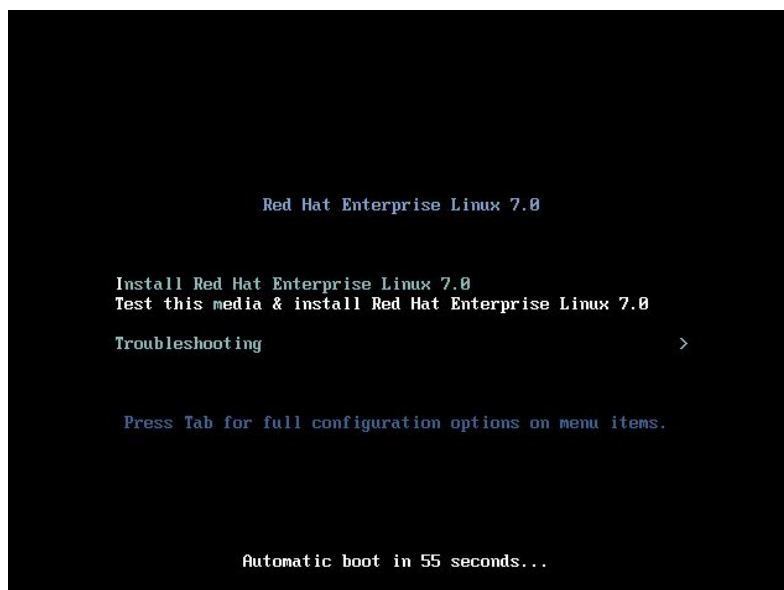


Figure 1.2(Troubleshoot screen)

- Navigate to the “Troubleshooting” option. Using Up/Down arrow key.

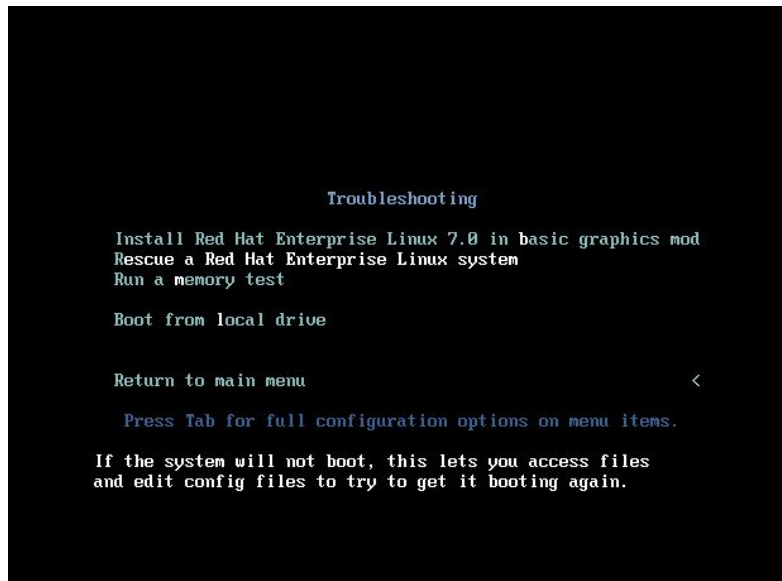


Figure 1.3(Rescue screen)

- Navigate to “Rescue a Red Hat Enterprise Linux System”

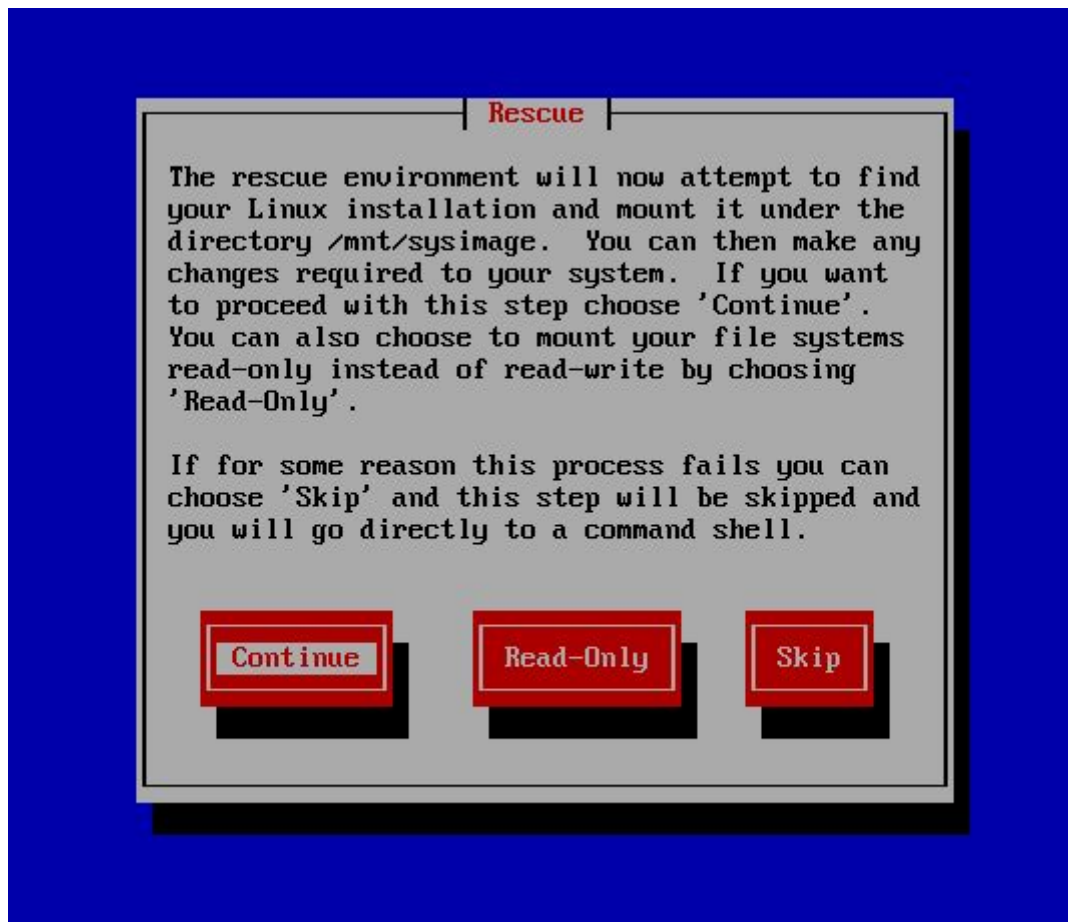


Figure 1.4(Rescue mode)

- You will now reach this screen. Just use the enter key and click continue.

```
Starting installer, one moment...
anaconda 19.31.79-1 for Red Hat Enterprise Linux 7.0 started.

Your system is mounted under the /mnt/sysimage directory.
When finished please exit from the shell and your system will reboot.

sh-4.2# _
```

Figure 1.5(Shell screen)

- This will lead you to a shell command prompt. As shown above in Figure 1.5.
- Enter the following command: **chroot /mnt/sysimage** , this will change the file system.
- Now that we have enter the bash shell we can now change the password. Using the command **passwd root**. This will allow the password to be change.
- Next enter this command: **rm -f /.autorelabel** , to prevent a time-consuming SELinux relabel of the disk.

- Enter the exit command subsequently to exit the chroot environment, finish the system boot and reboot your VM machine.

Problem 2: Setting an IP address to static.

- Use the command: **nmtui** to enter a GUI for editing network connections and systems.

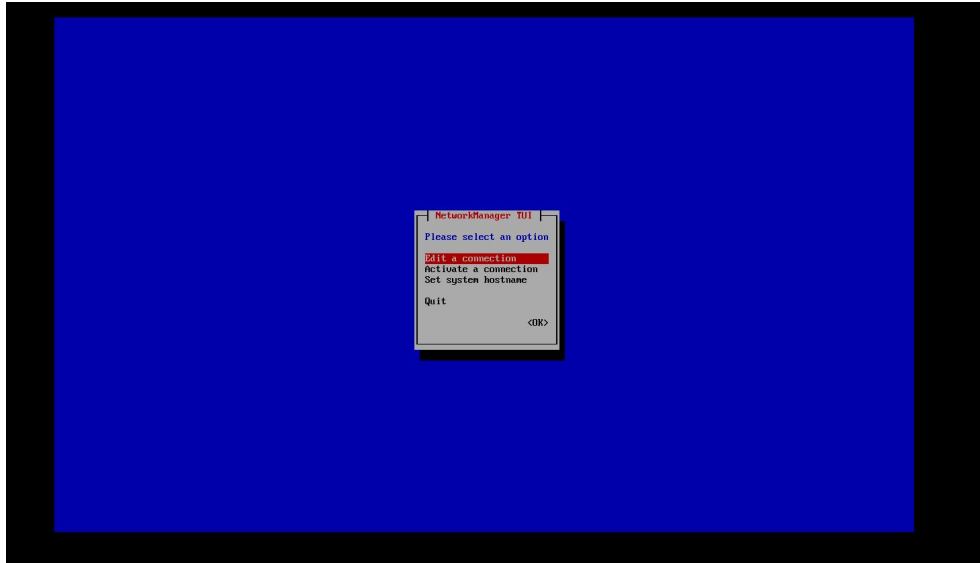


Figure 2.0(Nmtui screen)

- Click on “Edit a connection”.

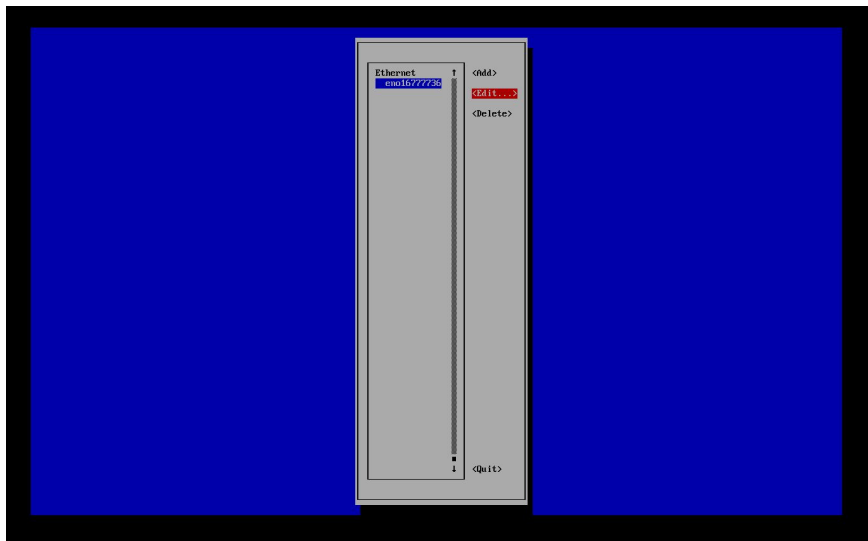


Figure 2.1(Edit settings)

- Click on “Edit”.

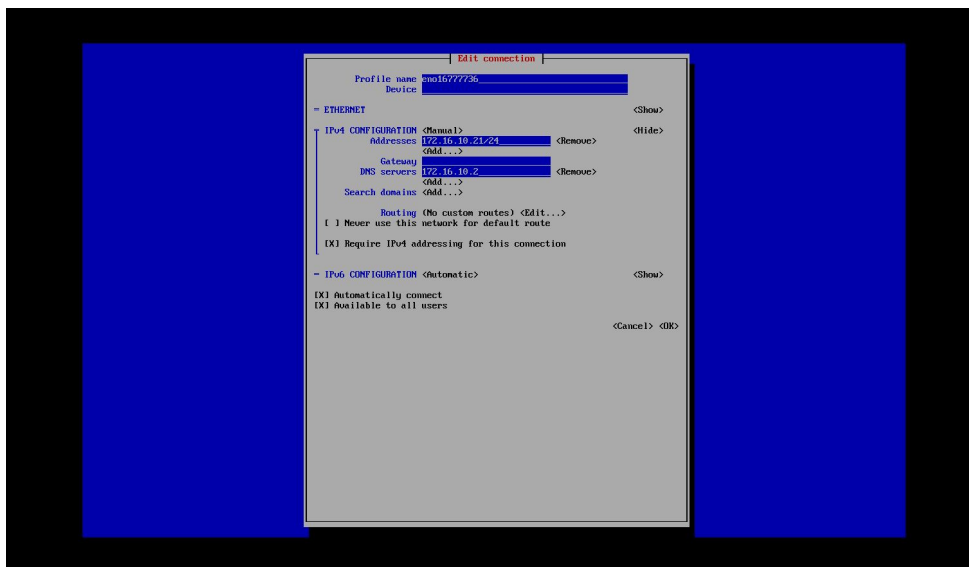


Figure 2.2(Edit connection)

- You will be brought to this screen above, move down to the IPv4 configuration section and set it to automatic.
- Remove the addresses and DNS servers.
- Click ok and exit from nmtui.
- Check to see if there is a new given ip address by using the command: **ip addr**.
- If there is, go back to nmtui to edit the current ip address by setting it back to manual.
- Use the command: **nmcli connection modify eno16777736 ipv4.addresses “<set current IP and subnet mask and gateway>” ipv4.dns <set current DNS server>** to set it to static.

Problem 3: Changing the message at the login prompt.

```
root@server etc]# vim /etc/issue
```

Figure 3.0 (Message prompt)

- Enter command: **vim /etc/issue**.
- This will lead to the file where it contains the current message at the login prompt.

```
Welcome to server!  
IP 192.168.94.23/24  
  
Legal Notice  
Unauthorized access is strictly prohibited and will be investigated. Your activities may be monitored and logged.
```

Figure 3.1 (Editing message)

- Edit the file and change it to the message to “Legal Notice” “Unauthorized access is strictly prohibited and will be investigated. Your activities may be monitored or logged”
- Save and quit the file.

Problem 4: Viewing web pages on the web server.

```
root@server conf.d]# netstat -tunap | grep 80  
tcp        0      0 0.0.0.0:80 0.0.0.0:*    LISTEN     1300/nginx: master
```

Figure 4.0 (netstat)

- Firstly, identify what web server, the server is using. Command: **netstat -tunap | grep 80** . This will show us that httpd service is using the nginx server to run its web pages.
- Go to the nginx config files by changing the directory to: **cd /usr/share/nginx/html**
- Afterwards, we will see a file called, “index.html”.

```
root@server html]# ls  
50x.html  DeptA  DeptB  DeptC  index.html  index.html.bak
```

Figure 4.1 (ls webpages)

```
Welcome to ABC Organisation!!<br><br>
<a href=DeptA/index.html>Department A</a><br>
<a href=DeptB/index.html>Department B</a><br>
<a href=DeptC/index.html>Department C</a><br>
ABC Company, Singapore
```

Figure 4.2 (edit webpages)

- Edit the file index.html and add the line “ABC Company, Singapore” below the file.
Command: **vim index.html**
- Afterwards, change directory to the location of the nginx file which can be found in **/etc/nginx/conf.d/default.conf**
- Edit the nginx configuration file to remap to the correct directory, edit the line which is contain in location /{


```
root /usr/pages/html;
index index.html index.htm;
}
```
- change root/usr/pages/html to **“/usr/share/nginx/html”** which is the correct file location of the webpages

```
server {
    listen      80;
    server_name localhost;

    #charset koi8-r;
    #access_log /var/log/nginx/log/host.access.log  main;

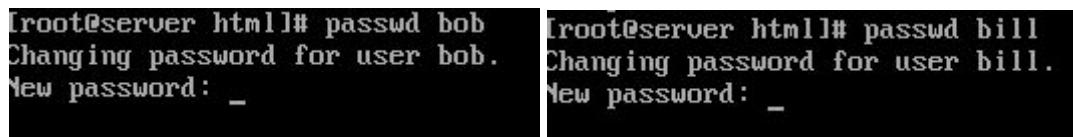
    location / {
        root    /usr/share/nginx/html;
        index   index.html index.htm;
    }

    location ~ ^/~(.*?)~(.*)?$ {
        alias /home/$1/public_html$2;
        index index.html
        autoindex on;
        deny all;
    }
}
```

Figure 4.3 (nginx config)

- Restart the nginx service to make changes to the file permanent. Command:
systemctl restart nginx

Problem 5: Help Bill and Bob regarding passwords and file permissions in web pages.



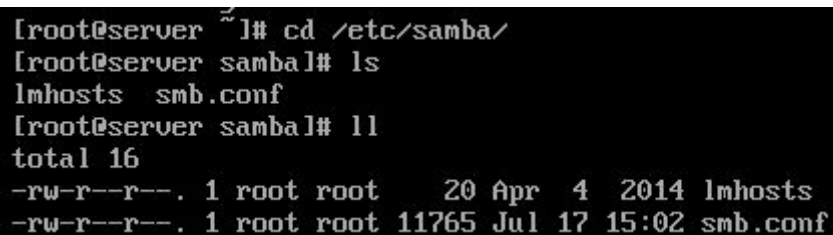
The figure consists of two side-by-side terminal window screenshots. The left window shows the command 'passwd bob' being executed, with the prompt 'Changing password for user bob.' and 'New password: _'. The right window shows the command 'passwd bill' being executed, with the prompt 'Changing password for user bill.' and 'New password: _'.

Figure 5.0 (password change)

- Since Bob and Bill do not know their account passwords, we will reset and give them a new password. Command: **passwd bob** and **passwd bill**
- To allow Bob and Bill to have access only to Department A pages. Firstly we will create a new group for bob and bill
- Command for creating new group: **groupadd webdesign**
- Next we will assign bob and bill the group to webdesign
- Command: **usermod -g webdesign bill** and **usermod -g webdesign bob**
- After giving bob and bill the group we will now allow users in the group **webdesign** to create and edit files in the directory and their respective files in the folder **/usr/share/nginx/html/DeptA**
- This command we will use is: **chown root:webdesign /usr/share/nginx/html/DeptA/**
- Next use **setfacl -m u:<nameofuser>:rwX /usr/share/nginx/html/DeptA/index.html**
- Now su to user bob or bill to test whether you can edit the webpage you should be successful

Problem 6: Allow Bill and Bob to have access to server remotely and have access only to Department A's web pages.

- Change the directory location to the samba configuration file location. Command: **cd /etc/samba**
- Edit the samba configuration file which is located in the “/etc/samba” directory. Command: **vim smb.conf**



The screenshot shows a terminal session where the user navigates to the /etc/samba directory and lists its contents. The output shows two files: lmhosts and smb.conf.

```
[root@server ~]# cd /etc/samba/
[root@server samba]# ls
lmhosts  smb.conf
[root@server samba]# ll
total 16
-rw-r--r--. 1 root root  20 Apr  4 2014 lmhosts
-rw-r--r--. 1 root root 11765 Jul 17 15:02 smb.conf
```

Figure 6.0 (edit samba)

- Append at the end of the configuration file to allow Bill and Bob to have access of the server remotely and only have access to Department A's web pages.

```
[Bill Bob]
path = /usr/share/nginx/html/DeptA
valid users = Bob bill
public = no
writable = yes
printable = no
create mask = 0770
```

Figure 6.1 (making samba config)

Recommendations for security in problem 6

- To allow Bob and Bill to have access only to Department A, using the Samba sharing service for file sharing in the server is one recommendation. Configuring the configuration files in Samba, can allow Bob and Bill to only gain access to Department A directory remotely.

Problem 7: Disabling the web server from accessing Bob's directory.

Method 1:

- We will need to change directory to Bob's directory. Command: **cd /home/bob**
- We will change the file permissions to a file called, "public_html" and set the root and user to have access to the file only. Command: **chmod 770 public_html**
- Restart the nginx service to make changes permanent. Command: **systemctl restart nginx**

Method 2:

- Having found out that the web server is using nginx. We could go into nginx configuration file and configure the web server to not allow others to view Bob's secret notes.
- Navigate into nginx config file. Command: **cd /etc/nginx/conf.d**
- Next edit the nginx config file. Command: **vim default.conf**
- Edit the part of the file in which the line starts with "location ~ ^/^(.+?)(/.*)?\$". Add a **deny all** at the bottom of it.

```
location ~ ^/~(.*?)(/.*)?$ {
    alias /home/$1/public_html$2;
    index index.html
    autoindex on;
    deny all;
}
```

Figure 7.0(Nginx config deny)

Problem 8: Department C unable to view the web pages.

- Change the directory to the html file that store the web pages. Command: **cd /usr/share/nginx/html**
- We will then need to check the security context of Department C file. Command: **ls -Z**

```
[root@server html]# ls -Z
-rw-r--r--. root root system_u:object_r:usr_t:s0 50x.html
drwxr-xr-x. root root unconfined_u:object_r:usr_t:s0 DeptA
drwxr-xr-x. root root unconfined_u:object_r:usr_t:s0 DeptB
lrwxrwxrwx. root root unconfined_u:object_r:usr_t:s0 DeptC -> /webpages/DeptC
-rw-r--r--. root root unconfined_u:object_r:usr_t:s0 index.html
-rw-r--r--. root root system_u:object_r:usr_t:s0 index.html.bak
```

Figure 8.0(ls)

- Afterwards, we change the directory to “/webpages/DeptC” to compare the security context of both files. Command: **cd /webpages/DeptC**

```
[root@server DeptC]# ls -Z
-rw-r--r--. root root unconfined_u:object_r:default_t:s0 index.html
```

Figure 8.1(ls in webpages)

- We will realise that the security context type for index.html in /webpages/DeptC is different from the security context type in Department C. Command: **ls -Z**
- Since the security context is different, we will change the security context type to “usr_t”. Command: **chcon -R -t usr_t /webpages**
- Afterwards, change the file permissions for “/webpages/DeptC” and “/webpages/DeptC/index.html”. Command: **chmod 777 /webpages/DeptC** and **chmod 777 /webpages/DeptC/index.html**
- Finally, remap the directory location in “/usr/share/nginx/html/DeptC/index.html” Command: **vim /usr/share/nginx/html/DeptC/index.html**
- Edit the file and change “Back to CBA Organisation” to “Back to ABC Organisation”.

```
Welcome to Department C<br><br>
This is a very nice web page, isn't it?<br><br>
<a href=../index.html>Back to ABC Organisation Home Page</a><br>
```

Figure 8.2(remap)

Problem 9: Records disappearing from the /var/log/secure file.

- The reason why the records are disappearing is most likely due to cron jobs running in the server.
- Change the directory to “/var/spool/cron” as this directory is where individual user crontabs are live. Command: **cd /var/spool/cron**

```
[root@server ~]# cd /var/spool/cron/  
[root@server cron]# ls  
john root
```

Figure 9.0 (var/spool)

- When listing out the directory, there will be 2 files called, “john” and “root”. Edit the “john” file. Command: **vim john**

```
## * * * * tail -2 /var/log/secure > /tmp/secure; cat /tmp/secure > /var/log/secure
```

Figure 9.1 (commenting the cronjob)

- Comment out the cron job that is running in the file by putting a “#” in front of the command.
- Exit the server to the login page and login as Bob and Bill a few times, to check that the records will be permanent and recorded in /var/log/secure file.

```
[root@server ~]# cat /var/log/secure  
Sep 23 01:01:06 server login: pam_unix(login:session): session opened for user root by LOGIN(uid=0)  
Sep 23 01:01:06 server login: ROOT LOGIN ON tty1  
Jul 17 20:52:44 server login: pam_unix(login:session): session closed for user root  
Jul 17 20:52:47 server login: pam_unix(login:session): session opened for user bob by LOGIN(uid=0)  
Jul 17 20:52:47 server login: LOGIN ON tty1 BY bob  
Jul 17 20:52:49 server login: pam_unix(login:session): session closed for user bob  
Jul 17 20:52:52 server login: pam_unix(login:session): session opened for user bill by LOGIN(uid=0)  
Jul 17 20:52:52 server login: LOGIN ON tty1 BY bill  
Jul 17 20:52:54 server login: pam_unix(login:session): session closed for user bill  
Jul 17 20:52:57 server login: pam_unix(login:session): session opened for user bob by LOGIN(uid=0)  
Jul 17 20:52:57 server login: LOGIN ON tty1 BY bob  
Jul 17 20:52:59 server login: pam_unix(login:session): session closed for user bob  
Jul 17 20:53:01 server login: pam_unix(login:session): session opened for user bob by LOGIN(uid=0)  
Jul 17 20:53:01 server login: LOGIN ON tty1 BY bob
```

Figure 9.2(checking whether logs are there)

- Records are being printed out and stayed permanent in the file.

Problem 10: FTP is able to download files from other directories, only allow FTP to download files from /var/ftp/pub.

- Check the FTP configuration files, by going to “/etc/vsftpd/vsftpd.conf”. Command: **vim /etc/vsftpd/vsftpd.conf**

```
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES
anon_root=
```

Figure 10.0 (changen anon root)

- Change the anon_root file path to “/var/ftp/pub”.

```
# Uncomment this to allow local users to log in.
# When SELinux is enforcing check for SE bool ftp_home_dir
local_enable=NO
```

Figure 10.1(enable local)

- Change the local_enable from “NO” to “YES”. This is to enable other users in the server to ftp to the directory other than anonymous.
- Restart the vsftpd service. Command: **systemctl restart vsftpd**
- Test it out by having another machine to ftp to the server they should be only able to download from /var/ftp/pub

Problem 11: Configure a server for any file that is downloaded using FTP will be logged into a file.

- Check the FTP configurations file in “/etc/vsftpd/vsftpd.conf”. Command: **vim /etc/vsftpd/vsftpd.conf**
- We will need to activate the logging of uploads and downloads through the use of FTP. Edit out the line “xferlog_enable=NO” to “xferlog_enable=YES”.

```
# Activate logging of uploads/downloads.
xferlog_enable=YES
```

Figure 11.0(enable loggings)

- Afterwards uncomment out this other 2 lines, so that every file that is downloaded using FTP will be logged under “/var/log/xferlog”.


```
# You may override where the log file goes if you like. The default is shown
# below.
xferlog_file=/var/log/xferlog
#
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
xferlog_std_format=YES
```

Figure 11.1(logging)

- Restart the vsftpd service to make the file changes permanent. Command: **systemctl restart vsftpd**

Problem 12: Why is date not working, what is wrong with ssh and disabling TFTP.

We have run into the issue of harry not being able to run the date command. This issue is only applicable to the user harry. Upon running the “date” command the system will print out a preset date message for harry.

- To find out what is wrong with the date command we first **su - harry** if you don’t know what harry password is su to root and reset the password using **passwd harry**. Next we use this command: **echo \$PATH**. \$PATH is a list in which Redhat will look at for executable files.

```
[harry@server ~]$ echo $PATH
/bin:/usr/local/bin:/bin:/usr/bin:/usr/local/sbin:/usr/sbin:/home/harry/.local/bin:/home/harry/bin
```

Figure 12.0(echo \$PATH)

- Upon running the command you will encounter something like the image above. The above image shows that when you try to run a program or script (eg: ping, ftp, date etc), Redhat will look in /usr/local/bin then /bin, /usr/bin etc.
- Next we will attempt to find out which date command is being used command: **which -a date**

```
[harry@server ~]$ which -a date
/data/date
/bin/date
/usr/bin/date
```

Figure 12.1(which -a)

- Upon inspecting the file contents of /bin/date we will find the original message inside “/bin/date” which is the wrong file to be executing.
- However why is it executing “/date/date” we will have to check the file contents of “.bash_profile”. To do this we will have cd to harry’s home directory. Command **cd /home/harry**

- Next we will use the command **vim .bash_profile**

```
# .bash_profile

# Get the aliases and functions
if [ -f ~/.bashrc ]; then
    . ~/.bashrc
fi

# User specific environment and startup programs

PATH=$PATH:$HOME/.local/bin:$HOME/bin
PATH=/data:$PATH

export PATH
```

Figure 12.2(editing .bash_profile)

- Upon revealing the contents of “.bash_profile” we will see that the path was set wrongly. On the line starting with “PATH=/data :\$PATH”
- Change this line with **PATH=/bin:\$PATH** and save the file. Go back to root by using **su root**. And restart all cronjob services using the command **systemctl restart crond**. The date command will be working now.
- To check simply log in as harry and run the date command

```
[harry@server ~]$ date
Sun Jul 22 16:28:17 SGT 2018
[harry@server ~]$ _
```

Figure 12.3(checking date command)

Now for the next issue why is SSH not working.

- To figure out why ssh is not working firstly we will try to ssh localhost. Command **ssh localhost**

```
[root@server ~]# ssh localhost
ssh: connect to host localhost port 22: Connection refused
[root@server ~]#
```

Figure 12.4(ssh localhost)

- From the image above we will see that port 22 connection has been refused. To solve this we will change the port by editing the file in “/etc/ssh/sshd_config”. Command: **vim /etc/ssh/sshd_config**

```
#Port 22
Port 9022
#AddressFamily any
```

Figure 12.5(editing sshd_config)

- Remove the “#” symbol from Port 22 and add “#” symbol for port 9022
- Next restart ssh service and attempt to ssh localhost again we will encounter another problem. Which is the connection being reset by peer.

```
[root@server ssh]# ssh localhost
ssh_exchange_identification: read: Connection reset by peer
```

Figure 12.6(connection reset by peer)

- This issue is mainly cost by issue in the “/etc/hosts.deny” file. We will now attempt to verify what is the issue inside the file. To do this use the command **vim /etc/hosts.deny**

```
#
# hosts.deny      This file contains access rules which are used to
#                 deny connections to network services that either use
#                 the tcp_wrappers library or that have been
#                 started through a tcp_wrappers-enabled xinetd.
#
#                 The rules in this file can also be set up in
#                 /etc/hosts.allow with a 'deny' option instead.
#
#                 See 'man 5 hosts_options' and 'man 5 hosts_access'
#                 for information on rule syntax.
#                 See 'man tcpd' for information on tcp_wrappers
#
sshd: ALL
```

Figure 12.7(edit hosts.deny)

- Upon editing the file we will see that the deny file has deny everybody to use ssh. To fix this remove the line “sshd: ALL”. And restart the ssh service
- SSH will now be working. To test this out attempt to ssh localhost again

```
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is a8:ac:ac:ea:d8:f9:4e:7a:19:4b:9e:5e:15:a1:e5:78.
Are you sure you want to continue connecting (yes/no)?
```

Figure 12.8(checking sshd)

- SSH is now successful

Disabling TFTP

- Harry left a note stating to disable tftp. We do not know whether tftp is turn off or on so we will first use the command **netstat -an | grep 69**

- This command will allow us to know whether “TFTP” is running

```
[root@server ~]# netstat -an | grep 69
udp        0      0 0.0.0.0:69          0.0.0.0:*
udp        0      0 0.0.0.0:51069       0.0.0.0:*
```

Figure 12.9(netstat 69)

- As you can see from the image above “TFTP” is listening to everything.
- Also we do not know what are the files that are included upon the installation of “TFTP” thus we will use the command **rpm -ql tftp-server** to see what files are included.

```
[root@server ~]# rpm -ql tftp-server
/etc/xinetd.d/tftp
/usr/lib/systemd/system/tftp.service
/usr/lib/systemd/system/tftp.socket
/usr/sbin/in.tftpd
/usr/share/doc/tftp-server-5.2
/usr/share/doc/tftp-server-5.2/CHANGES
/usr/share/doc/tftp-server-5.2/README
/usr/share/doc/tftp-server-5.2/README.security
/usr/share/man/man8/in.tftpd.8.gz
/usr/share/man/man8/tftpd.8.gz
/var/lib/tftpboot
[root@server ~]#
```

Figure 12.10(checking files for tftp)

- After locating the files that are included we know that “TFTP” is done via command line. We can conclude that to disable or enable “TFTP” we will have to configure the file “/etc/xinetd.d/tftp”
- Use the command **vim /etc/xinetd.d/tftp** we will see the contents of the file

```
# default: off
# description: The tftp server serves files using the trivial file transfer \
#               protocol. The tftp protocol is often used to boot diskless \
#               workstations, download configuration files to network-aware printers, \
#               and to start the installation process for some operating systems.
service tftp
{
    socket_type        = dgram
    protocol           = udp
    wait               = yes
    user               = root
    server             = /usr/sbin/in.tftpd
    server_args        = -s /var/lib/tftpboot
    disable            = no
    per_source         = 11
    cps                = 100 2
    flags              = IPv4
```

Figure 12.11(editing xinetd.d)

- To disable “TFTP” change the file where the line starts with “disable = no” change it to “disable = yes”
- “TFTP” is now disable.

Problem 13: Enable firewall and deny any IPv4 traffic to the server from a computer in Department D.

- Startup the firewall service in the server. Command: **systemctl start firewalld**
- Afterwards, enable the firewall service. Command: **systemctl enable firewalld**
- We will need to reject all incoming IPv4 traffic by setting a rich rule in the firewall service. Command: **firewall-cmd --zone=public --permanent --add-rich-rule='rule family="ipv4" source address="192.168.88.255" reject'**
- For the ip address 192.168.88.255 this ip address is DeptD ip address

```
[root@server ~]# firewall-cmd --zone=public --permanent --add-rich-rule='rule family="ipv4" source address="192.168.88.255" reject'
success
```

Figure 13.0 (rich rules)

- To allow webpages to load so that clients can still have access to the web server, we will need to allow a permanent port in the firewall. And the port number for webpages to load is port 80 since the web server is running on the nginx server. Command: **firewall-cmd --permanent --zone=public --add-port=80/tcp**
- However, we need to allow SSH and FTP services hence we need to allow both of their ports. Port 22 is to allow SSH to run. Command: **firewall-cmd --permanent --zone=public --add-port=22/tcp**
- Next, allowing FTP service to run in the server hence we need to open port 20. Command: **firewall-cmd --permanent --zone=public --add-port=20/tcp**
- Restart the firewall service, to make changes permanent. Command: **firewall-cmd --reload**
- Confirm that the changes have been made in the firewall. Command: **firewall-cmd --list-all**

```
[root@server ~]# firewall-cmd --list-all
public (default, active)
  interfaces: eno16777736
  sources:
  services: dhcpv6-client ssh
  ports: 80/tcp 8008/tcp 22/tcp 20/tcp
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
    rule family="ipv4" source address="192.168.88.255" reject
[root@server ~]# _
```

Figure 13.1 (firewall changes)

Problem 14: Propose any 2 recommendation to improve security of the server

- The first recommendation will be that the server needs a Intrusion Detection System(IDS). IDS Is software that monitors a system or network for unauthorized activity. By installing IDS on the server system, it enhances the security of the server. IDS is a sure way to know whether or not your file system has been altered or modified by some users or other processes. With that being implemented the SYSadmin can be sure about the integrity of the file system
- The second recommendation will be using remote logging for the server. Remote logging allow the users of the server to write their log files to a remote computer rather than writing it locally. Remote logging allows administrators to have a sense of privacy when checking the log files for the server. This is to prevent other users to have access and read the contents of the log files. As such, other users will not know who are the other users that have access to a file or resources. Keeping and protecting the user's privacy while allowing the administrator's to rectify errors in privacy too.