**Packet sniffing**

**SFTP vs FTP**

Testing site **Test.Rebex.Net**

*Credentials:*

**Username**: demo

**Password**: password

**Part 1:**

1. Install Wireshark on your testing computer.

2. **Start** Wireshark and begin to capture traffic from your active network card connection.

3. Start WinSCP and login to Test.Rebex.Net using FTP protocol which uses port 21.

4. Once you are logged in to test.Rebex.Net using WinSCP and the FTP protocol **stop** the Wireshark capture.

5. Capture the credentials used to login to the FTP site

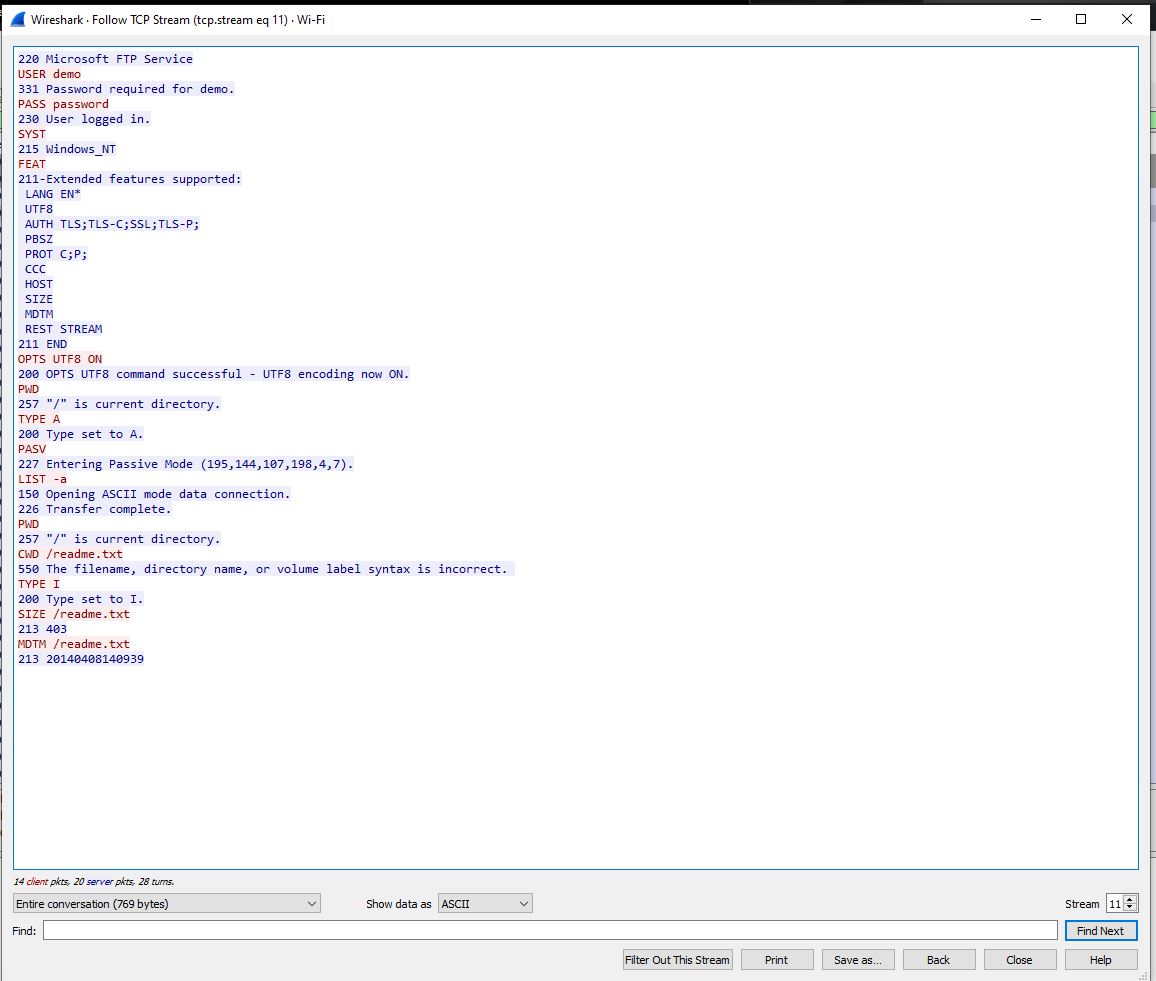
5. Were you able to capture and see the username and password you typed when you FTP into the site?

a) yes

10. Why?

a) Is not encrypted

11. Under this question provide a screen shot of the credentials captured that provided you the answer to the question above**.**

****

12. Once you are done you can close the FTP connection.

**Part 2:**

1. Now **start** Wireshark capture again without saving previous capture.

2. Repeat above process but now connecting to Test.Rebex.Net using SFTP on WINSCP. SFTP uses port 22.

3. Once you are logged in to the site test.Rebex.Net using WinSCP SFTP **stop** the Wireshark capture.

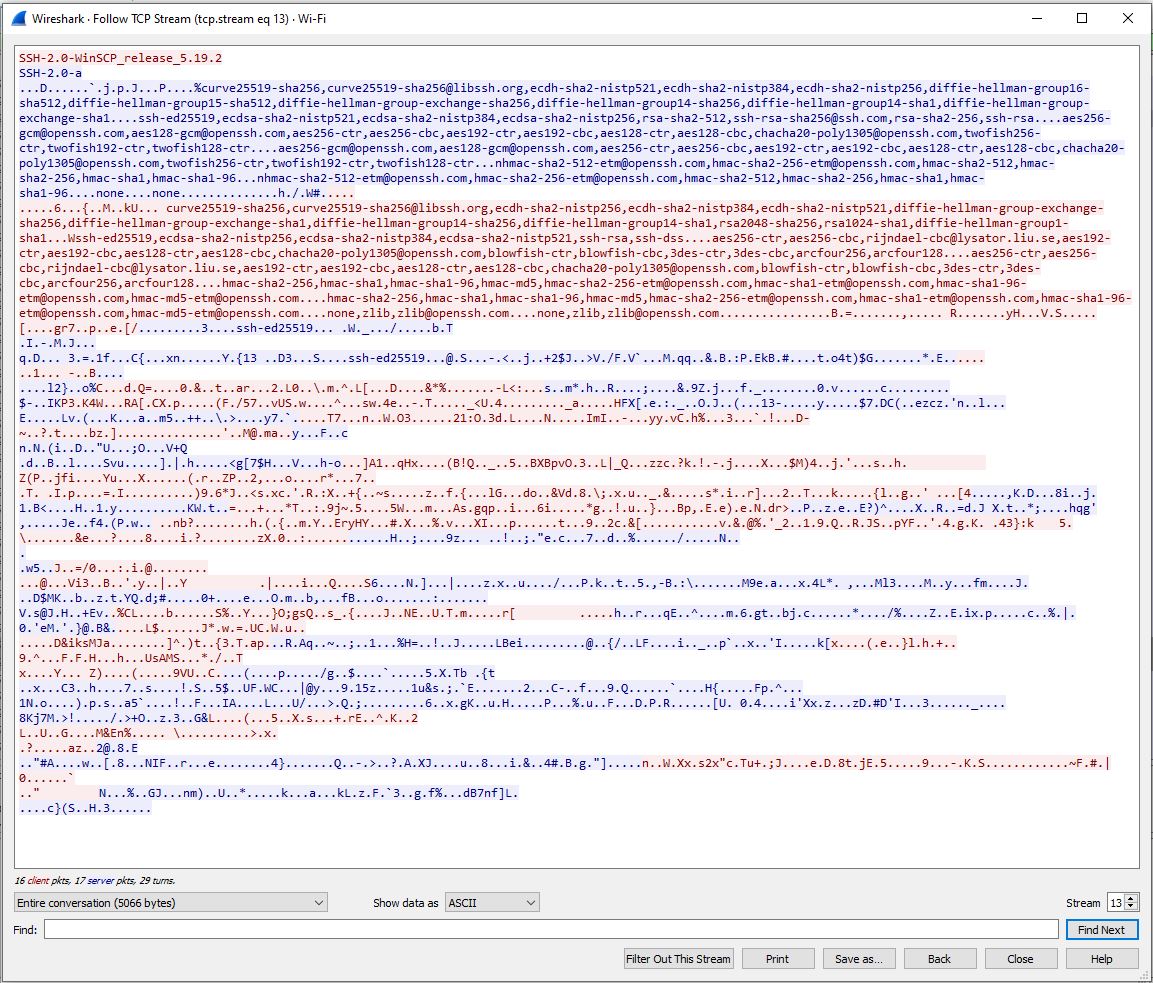
4. Were you able to capture and see the username and password?

a) no

5. Why?

a) Because the information is encrypted

6. Under this question provide a screen shot of your capture of the results that provided you the answer to the question above**.**

****

7. Once done you can close the SFTP connection.

**Part 3:**

**Http vs HTTPS**

Testing site [**http://testphp.vulnweb.com/login.php**](http://testphp.vulnweb.com/login.php)

*Credentials:*

**Username**: test

**Password**: test

1. **Start** Wireshark capture without saving previous captures

2. On your web browser open that following page [***http://testphp.vulnweb.com/login.php***](http://testphp.vulnweb.com/login.php)

3. Login using the above credentials.

4. Once you are logged in to this site **stop** the Wireshark capture.

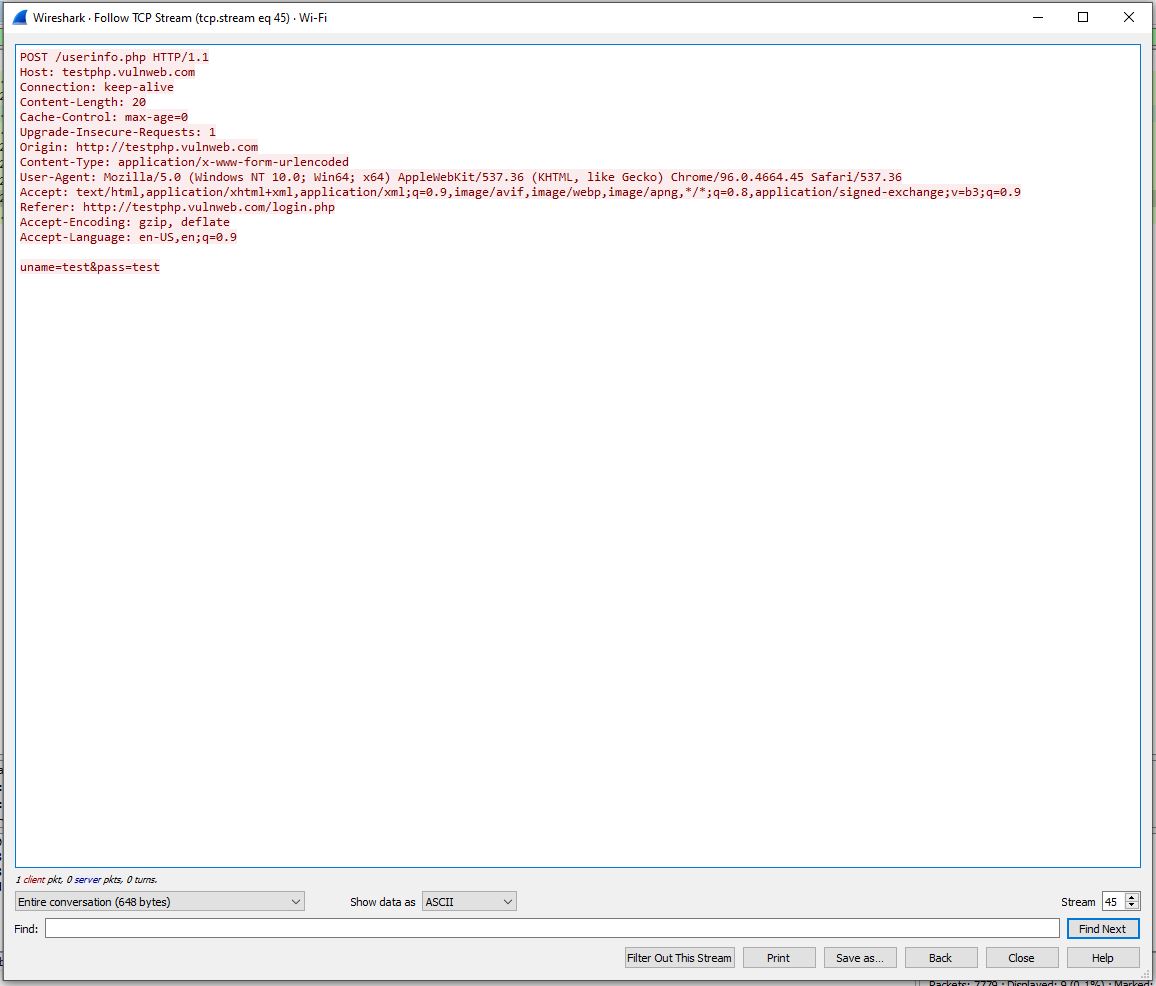
5. Were you able to capture and see the credentials in Wireshark?

a) yes

8. Why?

a) the connection to the website is not encrypted

9. Under this question provide a screen shot of your captured results that provided you the answer to the question above**.**

****

10. Once you are done you can close this site.

**Part 4:**

1. **Start** Wireshark capture

2. Do the same process above but now login in to blackboard. Blackboard page like any other secure website uses HTTPS port 443.

3. Once you are logged in to blackboard **stop** the Wireshark capture.

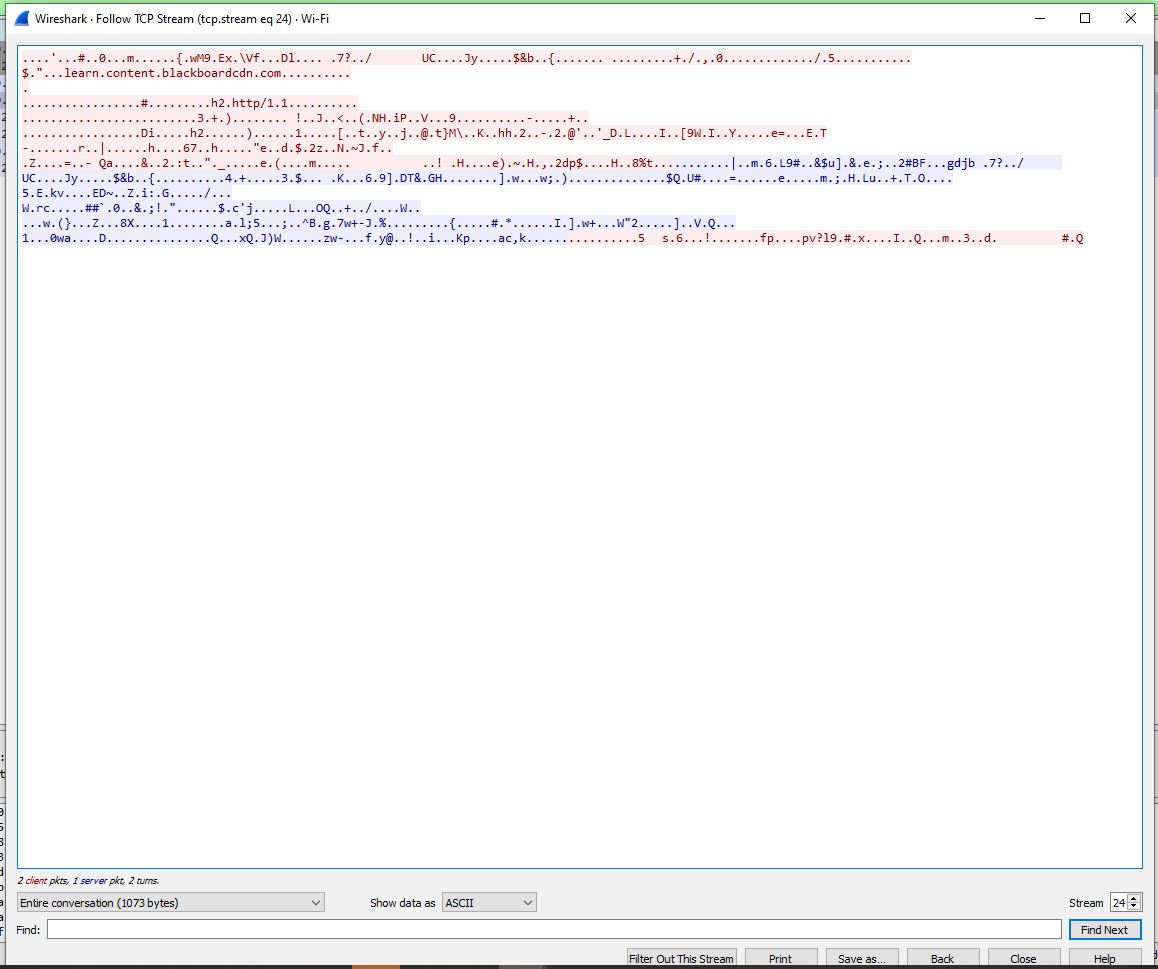
4. Were you able to capture and see the credentials you typed in Wireshark?

a) no

6. Why?

a) the website is encrypted

7. Under this question provide a screen shot of the “follow the stream page” results that provided you the answer to the question above**.**

****

**Luks Encrypting partition Lab:**

**Part 5:**

1. Download virtual box from this site **https://www.VirtualBox.org/wiki/Downloads** and install it on your testing computer.

2. Download centos 7 ISO to your testing computer from this website **https://www.centos.org/download/**

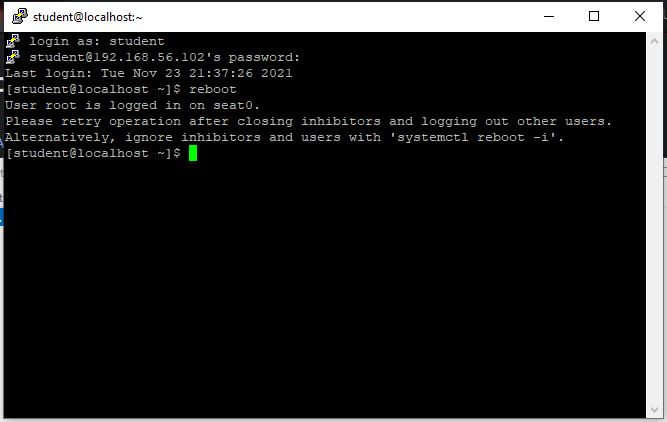
3. Create a Virtual Machine in virtual box and install the Centos 7 OS on it using the ISO just downloaded.

4. During installation process create a regular account name student with password student

5. During installation provide the root account a secure password you will remember.

6. Once OS installation completes login in to your server with the student account.

7. Once logged in using student account type reboot and **provide screen shot** of your results below.



8. Were you able to reboot?

a) no

9. Why?

a) because we don’t have root permissions

10. Switch to your root account from the student account.

11. What command did you use to switch to your root account from student?

a) su root

12. Now Reboot.

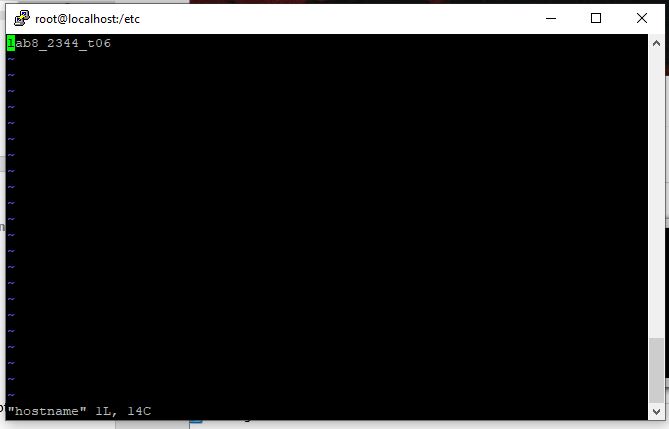
11. Were you able to reboot after switching to your root account?

a) yes

12. Why?

a) because root has root permissions

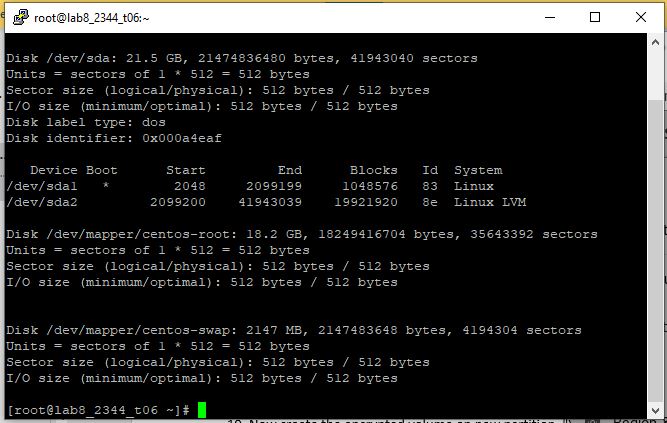
13. Once you reboot completes log back to the VM using root and change the server hostname to lab8\_2344\_t# where **#** is your team number and provide me the screen shot showing the new name.



14. What command did you use to change the servers hostname?

a) hostnamectl set-hostname lab8\_2344\_t06

14. Check how many disks and partitions you have on your virtual computer and provide a screen shot below this question?



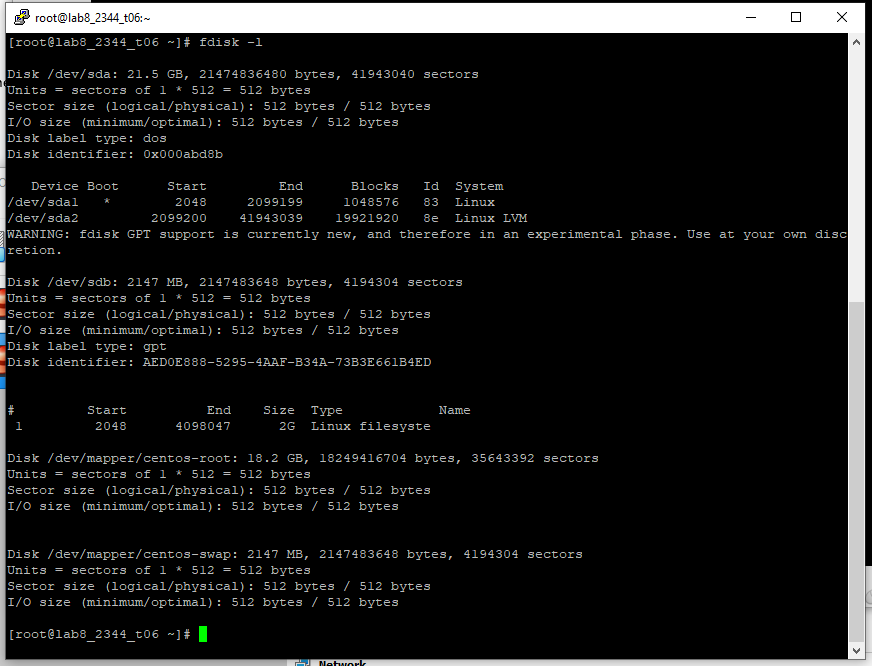
15. Add a second disk 2GB in size "you might need to reboot after adding the second disk for your VM to be able to see the new disk"

16. After adding the new disk what additional disks do you see now? Please provide the sd\* name absolute path on this question.

a) /dev/sdb

17. Format the new 2GB disk with only one partition “this partition is the one that will be encrypted”.

18. Provide a screen shot of the disks and partitions now showing on your VM?



19. Now create the encrypted volume on new partition. "You might need to install the crypt setup package" please install the package using yum if needed. You will need to make sure you have internet access on your VM"

20. What command you use to create encrypted volume?

a) cryptsetup luksFormat /dev/sdb1

21. Now open the encrypted volume in order to mount it and provide the name "encrypted" for the partition.

22. What command did you used to accomplish the above?

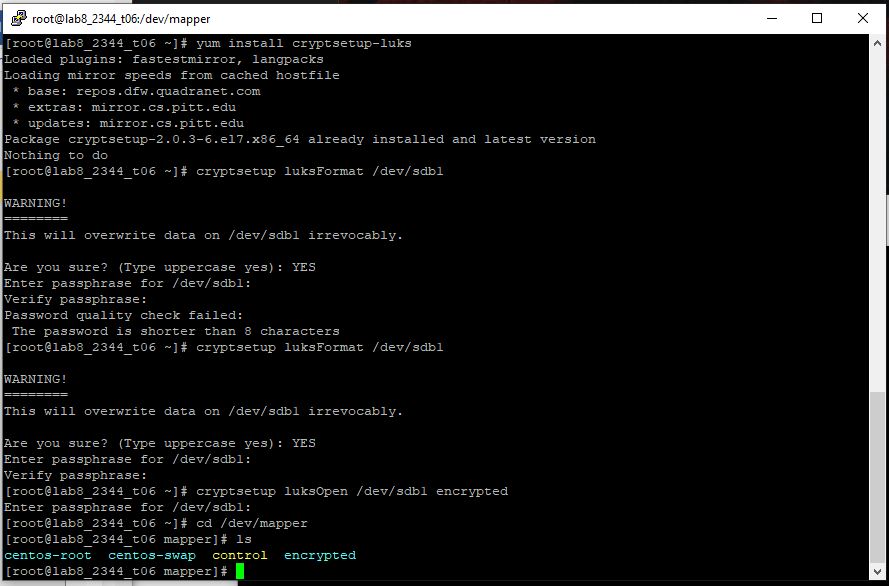
a) cryptsetup luksOpen /dev/sdb1 encrypted

23. Verify in this folder that it has the encrypted partition name /dev/mapper.

24. Do you see the name in the /dev/mapper folder?

a) yes

25. Please provide a screen shot?



26. Now that you have the encrypted partition open, please apply a file system ext4 to the partition.

26. What command did you use?

a) parted /dev/sdb1

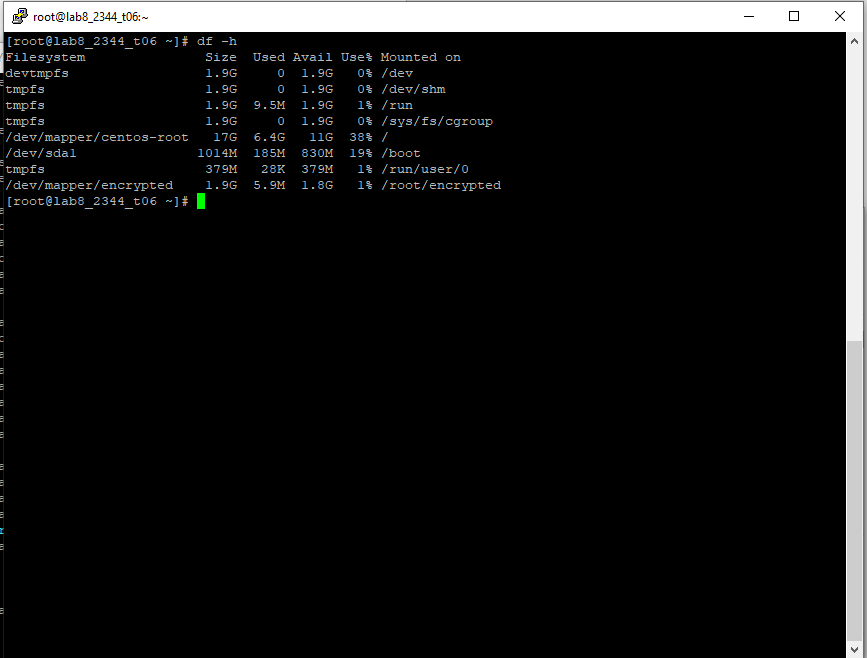
27. Now create a folder under root / name ***encrypted***, this folder will be use to mount the encrypted partition.

28. Mount the encrypted partition to the folder name encrypted using the mount command.

29. Do you see the mounted encrypted volume?

a) yes

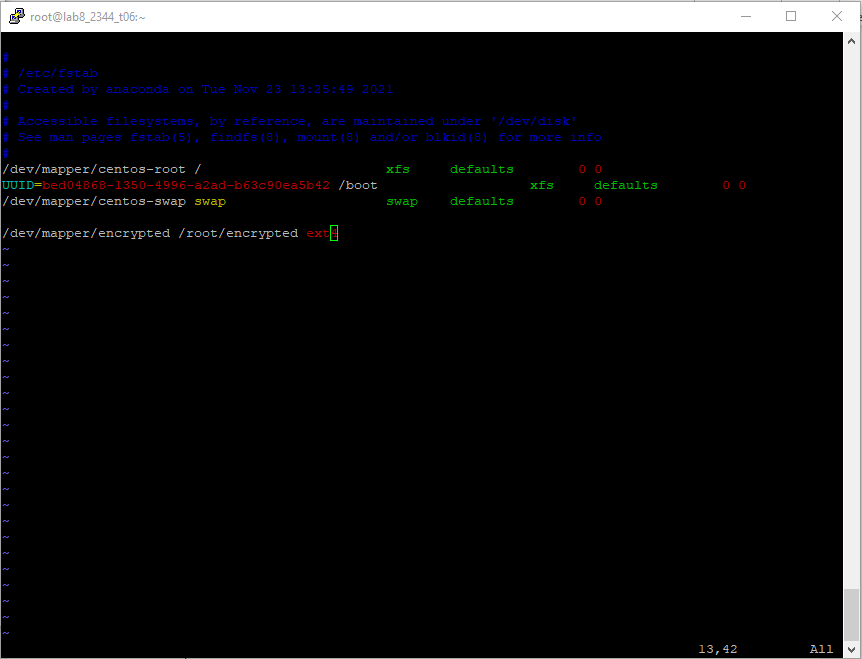
30. Show me the mounts on the server and provide a screen shot below this question as evidence that it is mounted.



31. Now go to the **/etc/fstab** file and enter the new encrypted partition parameters so that it auto mounts on a reboot.

32. What parameters did you put on the **/etc/fstab** file? Please provide a screen shot below this question as evidence.

a) /dev/mapper/encrypted /root/encrypted ext4



33. Now populate this file crypttab with the correct settings for the auto mount to work.

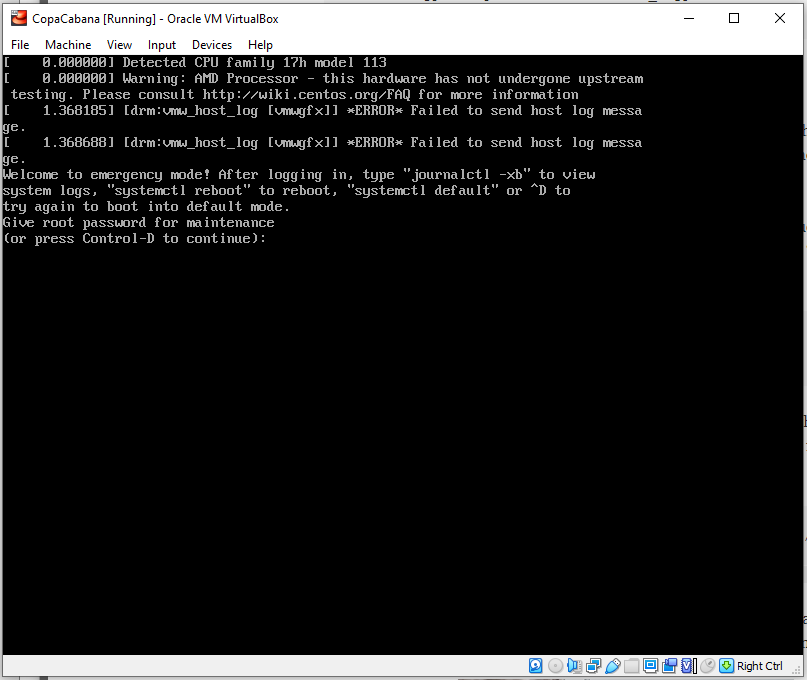
34. What did you put on this file and why this is needed?

a) encrypted /dev/disk/by-uuid/UUID=2e6df64d-c85d-472a-85db-fc5a3ff40480 none luks

b) so that the operating system can open the encrypted volume on startup/boot automatically

35. Now reboot.

36. After reboot send a screen that shows evidence that the partition is encrypted.



**Firewall**

1. Provide me the command that will block SSH traffic for IP address 192.168.1.100
   1. firewall-cmd --permanent --add-rich-rule="rule family='ipv4' source address='192.168.1.100' reject"
2. Provide me the command that will block all http traffic for every connection.
   1. firewall-cmd --permanent --remove-service=http
3. Provide me the command that will show all the ports the server is listening too.
   1. ss -lntu | grep LISTEN
4. Provide me the command that will show all the established connections on the computer.
   1. last -a | grep -i still
5. Provide the command that will show the firewall configuration on the server.
   1. firewall-cmd --list-all

***When done, submit lab8\_2344\_t# through Blackboard using the “Assignments” tool. Do Not email it. It will not be accepted.***