Computer Science 328 -01

Lab Assignment 5

Due Date: Friday, March 1, 2024 (before midnight)

Objectives:

1. **Install NTP (Network Time Protocol) server and configure NTP client**
2. **Install and secure FTP server with SSL/TLS**
3. **Install and Configure OpenLDAP server**

Task 1: Installed NTP (Network Time Protocol) server and configure NTP client

Please refer to this link below for details:

https://geek-university.com/configure-ntp-server/

Notes:

- Make sure that you update repository list first before you install:
  $ sudo apt update
  $ sudo apt install ntp

- replace the servers' pool inside **/etc/ntp.conf** file

```
server 0.ubuntu.pool.ntp.org
server 1.ubuntu.pool.ntp.org
server 2.ubuntu.pool.ntp.org
server 3.ubuntu.pool.ntp.org
```

with

```
server 0.ca.pool.ntp.org
server 1.ca.pool.ntp.org
server 2.ca.pool.ntp.org
server 3.ca.pool.ntp.org
```

- No need to restrict only to allow one subnet to query the NTP server

  - use *sudo systemctl restart ntp (instead of reload)*

Use ***ntpq –p*** to check all NTP servers available for time synchronization on VM2 (ip: 192.168.13.22, hostname: vm2.cosc328.okc) , and it should produce the results similar like this below:

```
cs213@vm2:~$ sudo nano /etc/ntp.conf
[sudo] password for cs213:
cs213@vm2:~$ ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 ntp.ubuntu.com  .POOL.          16 p    -   64    0    0.000    0.000   0.000
 vm2.cosc328.okc .INIT.          16 u    - 1024    0    0.000    0.000   0.000
-stirling.fsck.c 132.246.11.227   3 u   69  128  377   84.860   -0.593   2.575
+time.cloudflare 10.69.8.92       3 u   34  128  377   32.195    2.253   0.603
*ntp2.torix.ca   .PTP0.           1 u   79  128  377   58.747   -0.467   2.621
+nms.switch.ca   206.108.0.131    2 u   12  128  377   21.442    1.000   0.569
-185.125.190.58  37.15.221.189    2 u   16  128  377  136.376    0.433   6.439
-185.125.190.56  194.121.207.249  2 u   21  128  377  136.309   -0.073   8.778
-185.125.190.57  201.68.88.106    2 u   69  128  377  136.512   -0.076   9.605
-alphyn.canonica 132.163.96.1     2 u   71  128  173   76.346    0.012   1.040
cs213@vm2:~$
```

Use ***ntpq –p*** to check the only NTP server available for time synchronization on VM1 , and it should produce the results similar like this below:

```
cs213@ldap:~$ sudo nano /etc/ntp.conf
cs213@ldap:~$ sudo service ntp restart
cs213@ldap:~$ sudo ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 vm2.cosc328.okc 206.108.0.132    2 u   13   64    1    1.437    1.020   0.000
cs213@ldap:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       ubuntu

192.168.13.11  ldap.cosc328.okc   ldap
192.168.13.22  vm2.cosc328.okc    vm2
```

When you finish installing NTP server on VM2 and configuring VM1 as a NTP client, take the similar two screen shots on your Ubuntu VM2 and VM1 and place them into the table below:

Screen shot 1:

VM2

```
herrycooly@ubuntu:~$ ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 ntp.ubuntu.com  .POOL.          16 p    -   64    0    0.000    0.000   0.000
 ntp2.torix.ca   .PTP0.           1 u   10   64   17   54.320    1.900   1.493
*time.cloudflare 10.69.8.92       3 u   10   64   17   17.578    1.571   1.069
 20.104.166.17   206.126.112.212  2 u    9   64   17   72.948    1.576   5.252
 s173-183-146-26 192.168.10.254   2 u    5   64   17   15.515   -0.123   0.979
 185.125.190.56  194.121.207.249  2 u    4   64   17  128.953    3.357   4.337
 alphyn.canonica 132.163.96.1     2 u   74   64   16   82.189    1.026   3.033
 185.125.190.58  86.23.195.30     2 u    4   64   17  149.590   -4.173   4.710
 185.125.190.57  201.68.88.106    2 u    3   64   17  147.517   -6.219   9.200
```

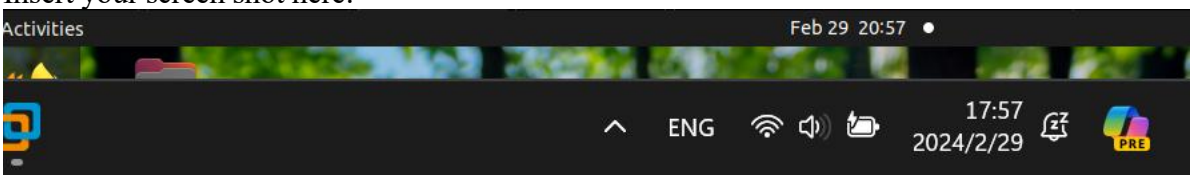
Screen shot 2:

VM1

```
herrycooly@ubuntu:~$ ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 192.168.58.22   185.125.190.57   3 u   15   64    6    0.280  -154.51   0.043
```

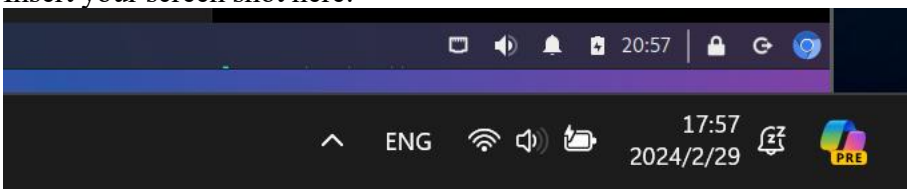
When you move your Ubuntu Server to a different time zone, you need to change the new time zone to your server at the command line. Now use the command line to change the time zone to America/Toronto on Ubuntu VM1, take a screen shot of the terminal including the display of the date and time at the top panel and the date time display of your host computer.

Insert your screen shot here:



Use the command line to change the time zone to America/Toronto on Kali VM, take a screen shot of the terminal including the display of the date and time at the top panel and the date time display of your host computer.

Insert your screen shot here:



Task 2: Install and secure FTP server with SSL/TLS

1. Start Ubuntu VM2 and open a terminal to install vsftpd server and ftp client:

```
$ sudo apt update
$ sudo apt install vsftpd ftp
```

2. Enable vsftpd service

```
$ sudo systemctl enable vsftpd
```

3. Launch vsftpd

```
$ sudo systemctl start vsftpd
```

4. Verify that vsftpd is running properly

```
$ sudo systemctl status vsftpd
```

5. Create two FTP users for their FTP sites using the same password “letmein”

```
$ sudo useradd -m ftpuser1
```

```
$ sudo useradd -m ftpuser2

$ sudo passwd ftpuser1
$ sudo passwd ftpuser2
```

6. Now we can open the configuration file with:

   $ sudo nano /etc/vsftpd.conf

   You can notice the following configuration which is enabled by default:

   # Allow anonymous FTP? (Disabled by default).
   anonymous_enable=NO
   # Uncomment this to allow local users to log in.
   local_enable=YES

   If we want to allow users to add, change, or remove files and directories we will need to uncomment the line **#write_enable=YES** by removing the # symbol.

   Next, you can create a list of users that will have access by adding the following lines at the end in the configuration:

   userlist_enable=YES
   userlist_file=/etc/vsftpd.userlist
   userlist_deny=NO

   /etc/vsftpd.userlist will be the file to which we can add users that we want to give access.

7. You can add the users (ftpuser1 and ftpuser2) to the userlist with the commands:

   $ echo "ftpuser1" | sudo tee -a /etc/vsftpd.userlist
   $ echo "ftpuser2" | sudo tee -a /etc/vsftpd.userlist

   Note: "sudo tee" allows us to write a file having sudo privilege except that the file is owned by the root.
   "sudo tee -a" allows us to write a file with all permissions even owned by the root.

Or you can simply open the file with your favorite file editor and add the name of the users each in a new line.

8. Create a text file "testfile.txt" and place it into ftpuser1's home directory first:
   $ sudo -u ftpuser1 sh -c 'echo "This is the content in the file." > /home/ftpuser1/testfile.txt'

   Note: "sh -c" means use sh command to execute

9. Open an FTP connection to the VSFTPD server running on localhost using "ftpuser1" account.

$ ftp localhost

```
ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.3)
Name (localhost:linode_user):
```

- you type "**ftpuser1**" for the Name prompt, and followed by "**letmein**" for the password prompt.

```
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

- Next list the home directory of ftpuser1 to verify that the text file "testfile.txt" created earlier is there:
  $ ls /home/ftpuser1/

Take a screen shot of the terminal showing the result from your ls command, and insert your screen shot below:

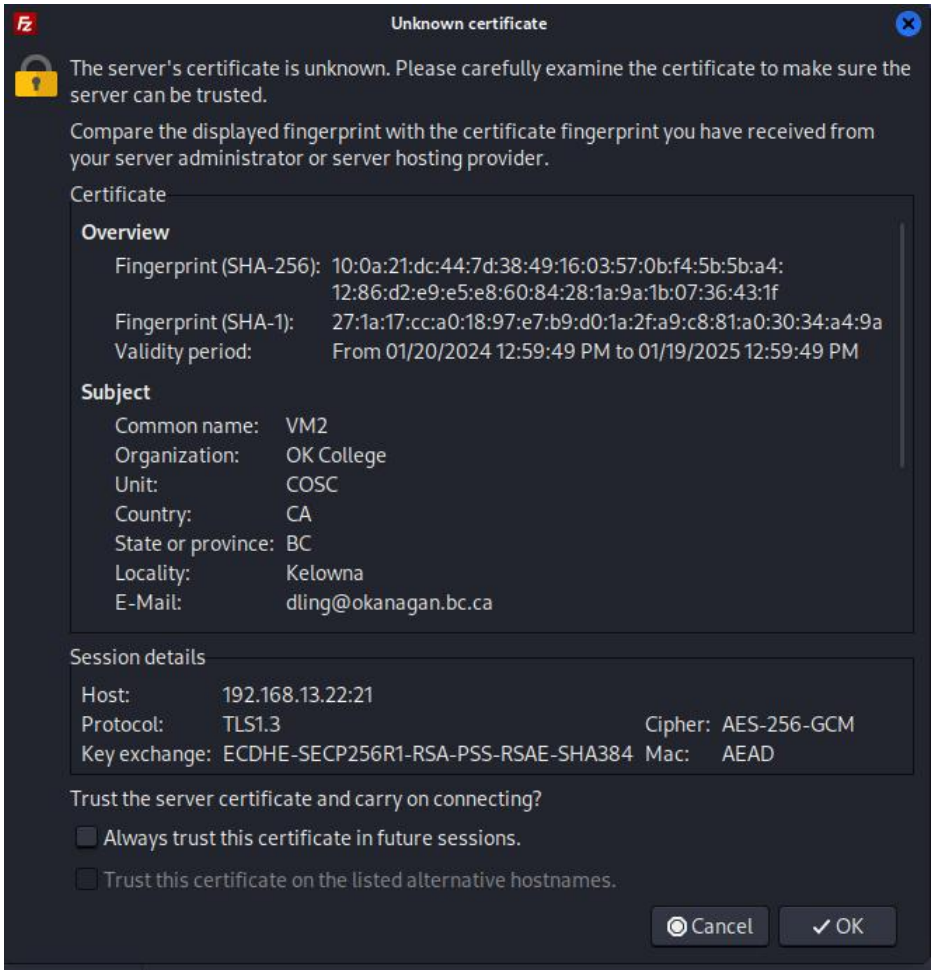
```
ftp> ls /home/ftpuser1/
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-r--    1 1004     1007           33 Feb 29 18:02 testfile.txt
226 Directory send OK.
```

- You can try using "**get**" and "**put**" commands for downloading and uploading file(s) between ftpuser1's home directory and your current user's home directory. Type "**exit**" to end the FTP session when you're done.

10. Next let's create a self-signed SSL certificate and configure it properly for securing FTP file transmissions

- create a self-signed SSL certificate look similar this below when a site connect to the vsftp server for first

time:



Use similar data information to create your self-signed SSL certificate except with your own email address.

$ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem

This will generate the certificate and private key in the /etc/ssl/private/ directory.

11. Now you will need to change the /etc/vsftpd.conf configuration file to the location of the certificate and the private key. Open the /etc/vsftpd.conf with an editor and change the values to the right location and make sure to enable SSL also.

```
  :
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
  :
```

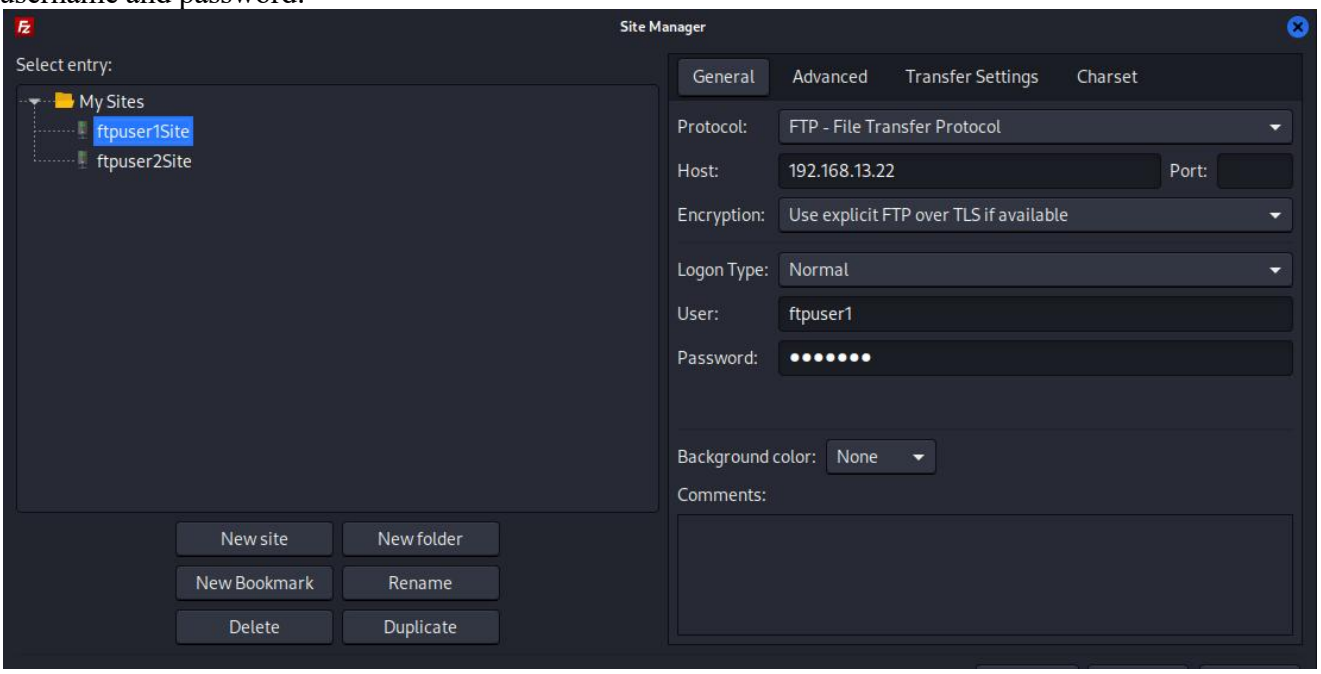
Save the file, and then restart vsftpd :

$ systemctl restart vsftpd

12. Choose a FTP client program (Filezilla) with SSL/TLS support and install it in Kali VM:
    - Start your Kali VM, and open a terminal to install "Filezilla"
      $ sudo apt update
13. $ sudo apt install filezilla

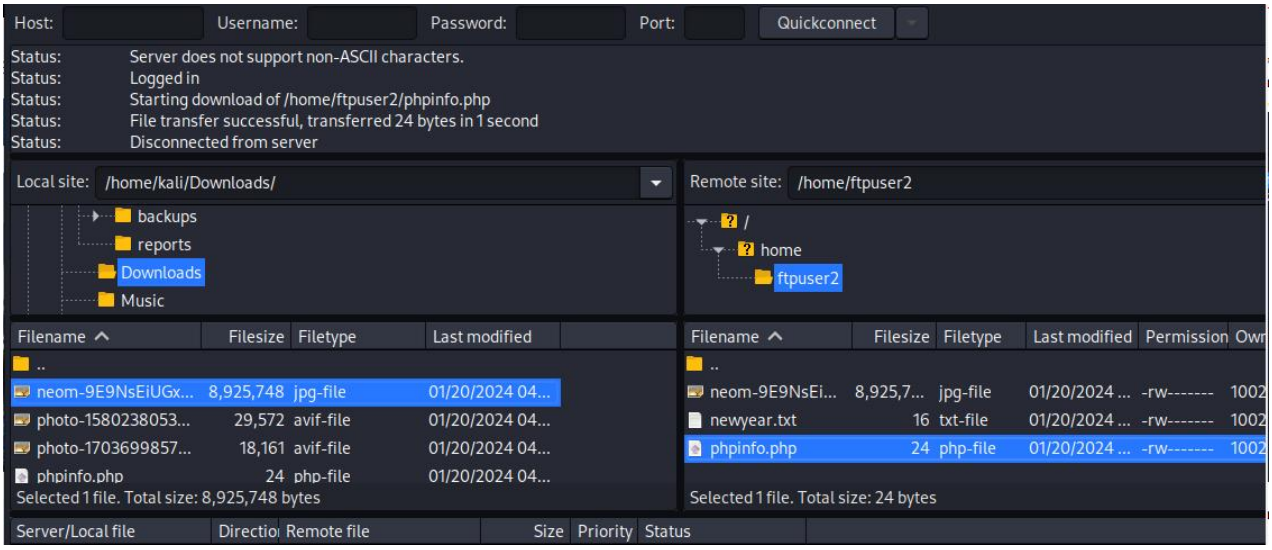
    - Run filezilla
      $ filezilla

- A Filezilla window will pop up => Click on File menu => choose **Site Manager ..** => Click on **New site** button => enter a site name (ftpuser1Site), and the connection information like ftp server's ip/hostname, username and password:

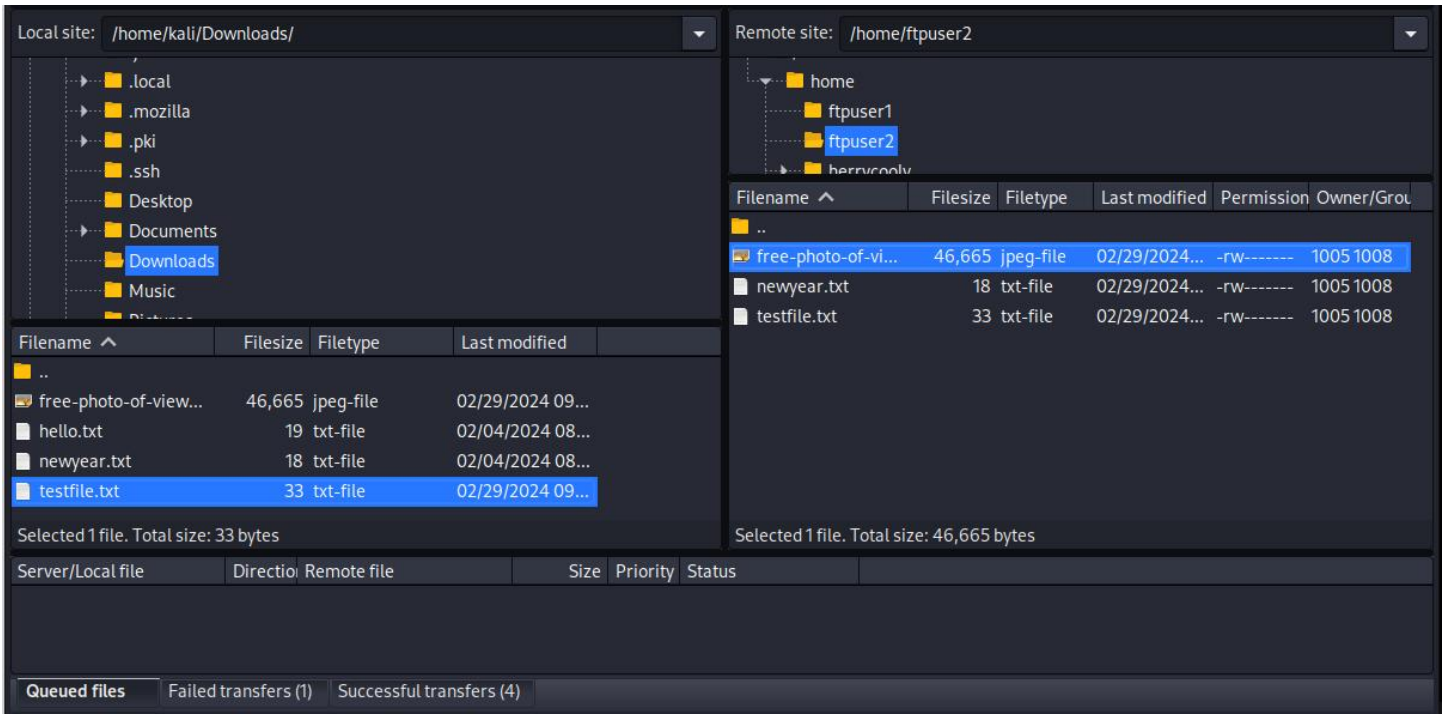


- Create another site (ftpuser2Site) using "ftpuser2" account.

- Next click on **ftpuser2Site** => click on **Connect** button => open a new terminal, and create a couple text files in Kali's home directory => Go to Filezilla's window, and then drag the two text files to ftpuser2's home directory (uploading files) => Open a browser, and download a couple image or sound files into Kali's Downloads folder => Drag one of the image/sound files from Kali's Downloads folder into ftpuser2's home directory (uploading) => Drag one of the text files from ftpuser2's home directory into Kali's Downloads folder (downloading) => Take a screen shot of your Filezilla Windows similar to the screen shot as shown below:



Insert your screen shot below:



Task 3: Install and Configure OpenLDAP server

- Please refer to the handout "***Setting hostnames for all VMs.pdf***" for setting proper hostnames for all your virtual machines first.

  Then open the web link below:

  https://computingforgeeks.com/install-and-configure-openldap-server-ubuntu/

- Please follow the steps from the web link above to install and configure a LDAP server on Ubuntu VM1 by replacing the domain name "**example.com**" with "**cosc328.okc**" , the ip address "192.168.18.50" with your own ip nnn.nnn.nnn.11 on VM1.

- Add the following step **before proceeding to Step 5 - Install LDAP Account Manager**.

  $ sudo nano /etc/ldap/ldap.conf

  Uncomment the line "BASE" and "URI" and change the domain name for your OpenLDAP server properly like this:

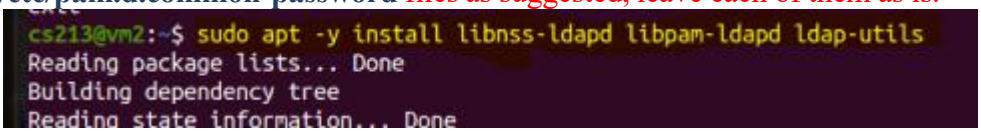
```
BASE dc=cosc328,dc=okc
URI  ldap://ldap.cosc328.okc
```

- Next proceed to Step 5 and follow the web link below to install LDAP Account Manager (LAM) for handling users and groups.
  https://computingforgeeks.com/install-and-configure-ldap-account-manager-on-ubuntu/

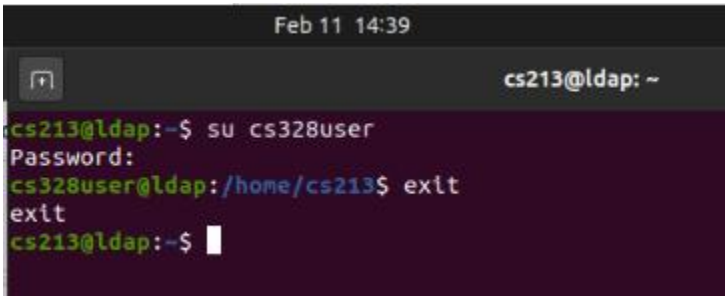
  ⇨ Create two ldap users with LAM: **cs328user** and **mdoe**

- Next proceed to Step 6 to configure the LDAP server machine (Ubuntu VM1) as a LDAP client.
  https://computingforgeeks.com/how-to-configure-ubuntu-as-ldap-client/

  Note: Please follow the suggested web link above, but use the following command for the installation of the LDAP client instead in order to avoid some issues! Also don't change **/etc/nsswitch.conf** and **/etc/pam.d.common-password** files as suggested, leave each of them as is.



After the installation of the LDAP client on VM1, take a screen shot of your terminal which looks similar to this:



- Next skip Step 7 (setting up SSL/TLS connection), instead repeat Step 6 to configure your Ubuntu VM2 as another LDAP client.
  Note: Please follow the suggested web link above, but use the following command for the installation of the LDAP client instead in order to avoid some issues! Also don't change **/etc/nsswitch.conf** and **/etc/pam.d.common-password** files as suggested, leave each of them as is.

```
cs213@vm2:~$ sudo apt -y install libnss-ldapd libpam-ldapd ldap-utils
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

After the installation of the LDAP client on VM2, take a screen shot of your terminal which looks similar to this:

```
Feb 11 14:42
cs213@vm2: ~
cs213@vm2:~$ su cs328user
Password:
cs328user@vm2:/home/cs213$ exit
exit
cs213@vm2:~$
```

Now your screen shot here:

```
$ exit
herrycooly@ubuntu:~$ su herrycooly
Password:
herrycooly@cosc328:~$
```

Can your VM2 be able to see the global directory information with the following command?

```
$ ldapsearch  -x  -b  dc=cosc328,dc=okc   -h   ldap.cosc328.okc
```

```
cs213@vm2:~$ ldapsearch -x -b dc=cosc328,dc=okc -h ldap.cosc328.okc
# extended LDIF
#
# LDAPv3
# base <dc=cosc328,dc=okc> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# cosc328.okc
dn: dc=cosc328,dc=okc
objectClass: top
objectClass: dcObject
objectClass: organization
o: cosc328.okc
dc: cosc328

# admin, cosc328.okc
dn: cn=admin,dc=cosc328,dc=okc
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# people, cosc328.okc
dn: ou=people,dc=cosc328,dc=okc
objectClass: organizationalUnit
ou: people

# groups, cosc328.okc
dn: ou=groups,dc=cosc328,dc=okc
objectClass: organizationalUnit
ou: groups

# cs328user, people, cosc328.okc
dn: uid=cs328user,ou=people,dc=cosc328,dc=okc
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: cs328user
sn: Cosc
loginShell: /bin/bash
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/cs328user
uid: cs328user

# cs328user, groups, cosc328.okc
dn: cn=cs328user,ou=groups,dc=cosc328,dc=okc
objectClass: posixGroup
cn: cs328user
gidNumber: 2000
memberUid: cs328user

# admins, groups, cosc328.okc
dn: cn=admins,ou=groups,dc=cosc328,dc=okc
objectClass: posixGroup
gidNumber: 10000
cn: admins

# Mary Doe, people, cosc328.okc
dn: cn=Mary Doe,ou=people,dc=cosc328,dc=okc
objectClass: shadowAccount
```

Your screen shot here:

```
# extended LDIF
#
# LDAPv3
# base <dc=okc> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# okc
dn: dc=okc
objectClass: top
objectClass: dcObject
objectClass: organization
o: okc
dc: okc

# admin, okc
dn: cn=admin,dc=okc
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# people, okc
dn: ou=people,dc=okc
objectClass: organizationalUnit
ou: people

# groups, okc
dn: ou=groups,dc=okc
objectClass: organizationalUnit
ou: groups

# computingforgeeks, people, okc
dn: uid=computingforgeeks,ou=people,dc=okc
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: herrycooly
sn: cosc
loginShell: /bin/bash
uidNumber: 2000
gidNumber: 2000
homeDirectory: /home/herrycooly
uid: computingforgeeks

# herrycooly, groups, okc
```

```
dn: cn=herrycooly,ou=groups,dc=okc
objectClass: posixGroup
cn: herrycooly
gidNumber: 2000
memberUid: herrycooly

# newgroup, groups, okc
dn: cn=newgroup,ou=groups,dc=okc
objectClass: posixGroup
cn: newgroup
gidNumber: 2000
memberUid: herrycooly

# group, okc
dn: ou=group,dc=okc
objectClass: organizationalUnit
ou: group

# Hacker, group, okc
dn: cn=Hacker,ou=group,dc=okc
objectClass: posixGroup
gidNumber: 10000
cn: Hacker

# cs328user, people, okc
dn: cn=cs328user,ou=people,dc=okc
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
loginShell: /bin/bash
homeDirectory: /home/cs328user
uid: cs328user
cn: cs328user
uidNumber: 10000
gidNumber: 10000
sn: cs328user

# mdoe, people, okc
dn: cn=mdoe,ou=people,dc=okc
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
loginShell: /bin/bash
homeDirectory: /home/mdoe
uid: mdoe
cn: mdoe
uidNumber: 10001
gidNumber: 10000
```

Are you able to ssh to the LDAP server with **cs328user** account like this?

```
Feb 11 14:52
cs328user@ldap: ~
cs213@vm2:~$ ssh cs328user@ldap.cosc328.okc
cs328user@ldap.cosc328.okc's password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.15.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

302 updates can be installed immediately.
1 of these updates is a security update.
To see these additional updates run: apt list --upgradable

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Sun Feb 11 14:10:30 2024 from 192.168.13.22
cs328user@ldap:~$
```

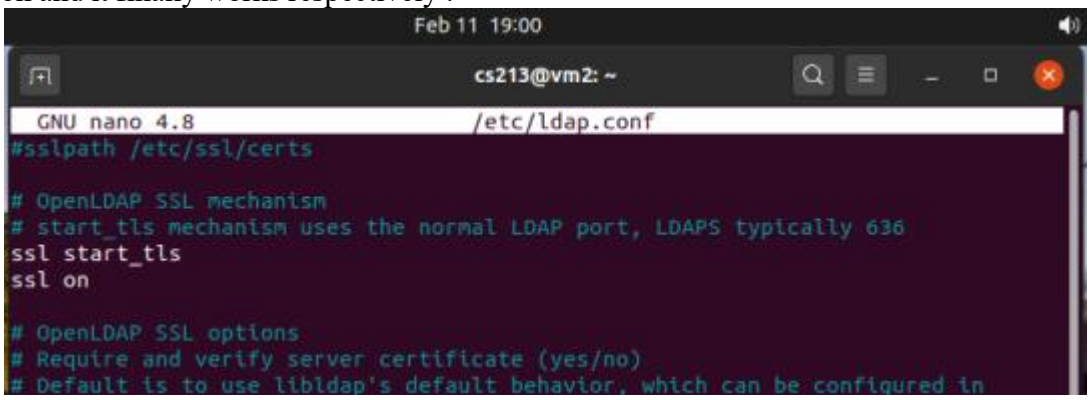
Your screen shot here:

```
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-94-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

     https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.
*** System restart required ***
herrycooly@cosc328:~$
```

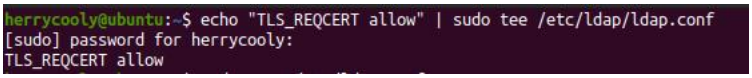
-Now the last step to complete the whole setup with SSL/TLS login connection between client and server without using ssh. Please follow the steps from the web link here:

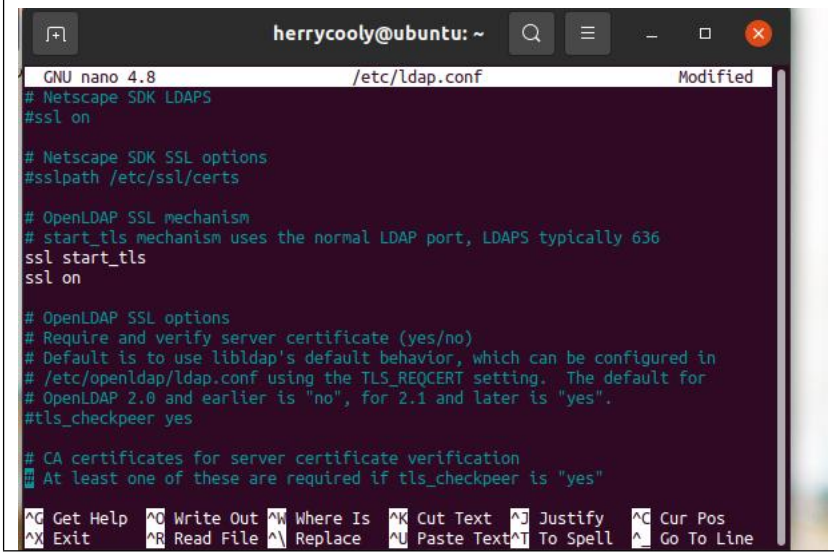
https://computingforgeeks.com/secure-ldap-server-with-ssl-tls-on-ubuntu/

When you edit **/etc/ldap.conf** and complete the steps on VM2 client, take screen shots to show SSL is being turned on and it finally works respectively :



Your two screen shots from VM2 here:





Submitting your work:

Export this Word document with all your answers and screen shots as PDF format, and then submit your PDF file via Lab 5 assignment tab on Moodle by *Friday, March 1, 2024 (midnight).*