# Kenneth Mead CSI-3670-14117.202110

# Lab 4 LDAP

**Questions**

1. (10 points) Note that the user id and group ids are quite high. Why would this be the case?

To remove the possibility of group id’s and user id’s overlapping each other.

1. (10 points) [From lab] (ldapsearch + subSchemaEntry). Describe what the subSchemaEntry is doing to our ldapsearch

SubSchemaEntry returns what subschema each object belongs to. A schema is, put lightly, the overall layout/plan of the data.

1. (10 points) What is LDAP and how does it compare to Active Directory? (you may reuse your exam answer)

LDAP is the industry standard protocol used to manage directory information services. To elaborate, LDAP provides the details on the technique that should be used but does not provide an actual directory service.

Active Directory is an actual directory service provided by Microsoft. It manages user authentication, directory access per user, assigns and enforces security policies, and can manage installation/updating of software.

Their difference is that LDAP does not actually provide a directory service, it simply provides the tools to get the job done. On the other hand, Active Directory puts LDAP to use and provides the actual directory service.

1. (10 points) What’s the difference between a DC and an OU in LDAP? What is their purpose?

DC’s represents the top of the ldap tree. OU’s represent simple containers to hold other objects.

1. (10 points) What is a Distinguished Name? (you may reuse your exam answer)

An objects entire path back to the domain component. Similar to a folders absolute path.

1. (20 points) Assume we are running an LDAP server for the class. What changes would need to be made to each *client machine* in order for them to authenticate with the LDAP server over a local login? You don’t need to provide exact details, but describe the technologies needed. This will require Googling, FYI.

* Install openldap-clients
* Run authconfig-tui.
* Setup the server IP address and base DN

1. (10 points extra credit) Modify the script above to create a new user from the command line. Copy the old script and rename your new script to be user\_add.sh. It should accept a single user and password combination as follows (so, no need to loop anymore):

$ sudo bash user\_add.sh username password

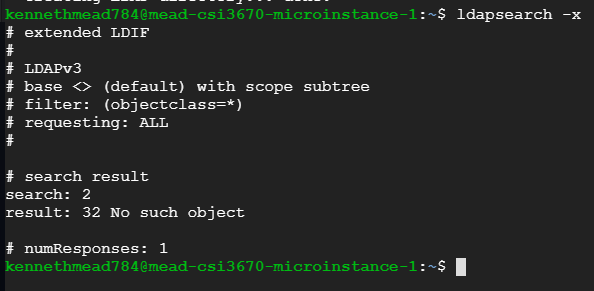
Run this and demonstrate that the user has been successfully added (either via LAM or an ldapsearch query).

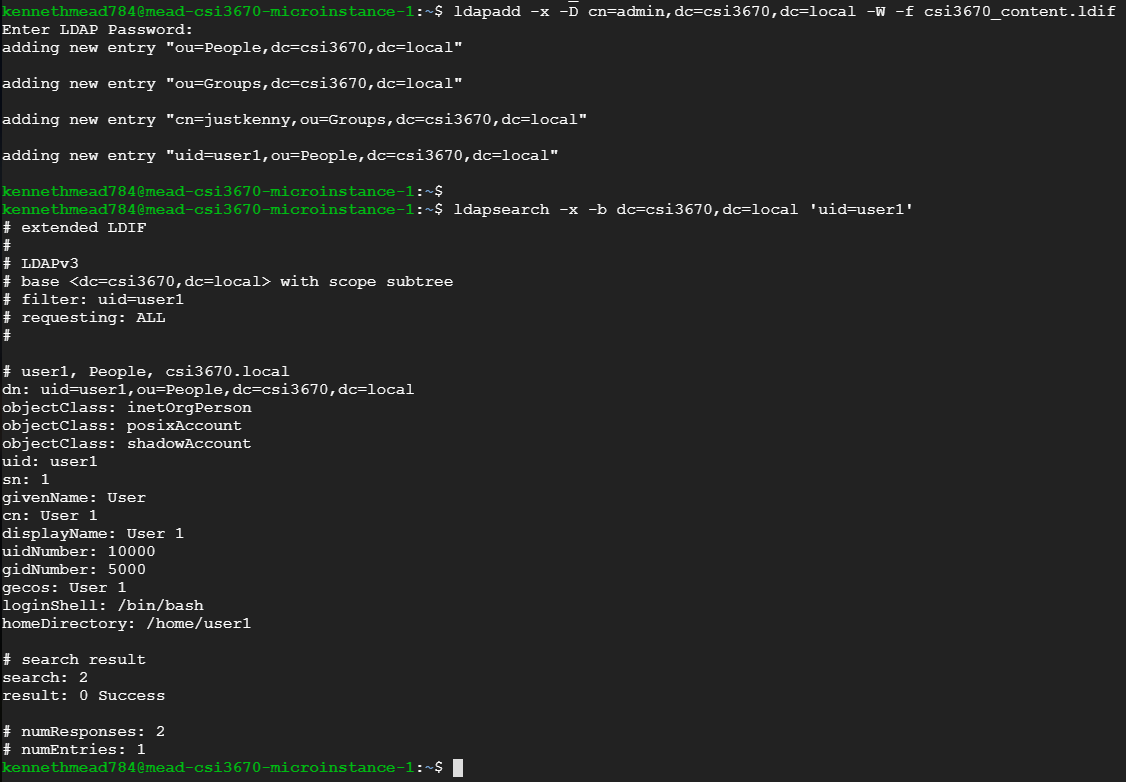
1. (30 points total, 5 per screenshot) Ensure you’ve taken all six required screenshots and put them at the end of this document.

1. Zip up this report, your script(s) and any other materials and submit to Moodle. You may copy/paste your script inside this Word document as well, just make sure that it copies correctly to avoid losing bonus points.

All other content is located in the zip file

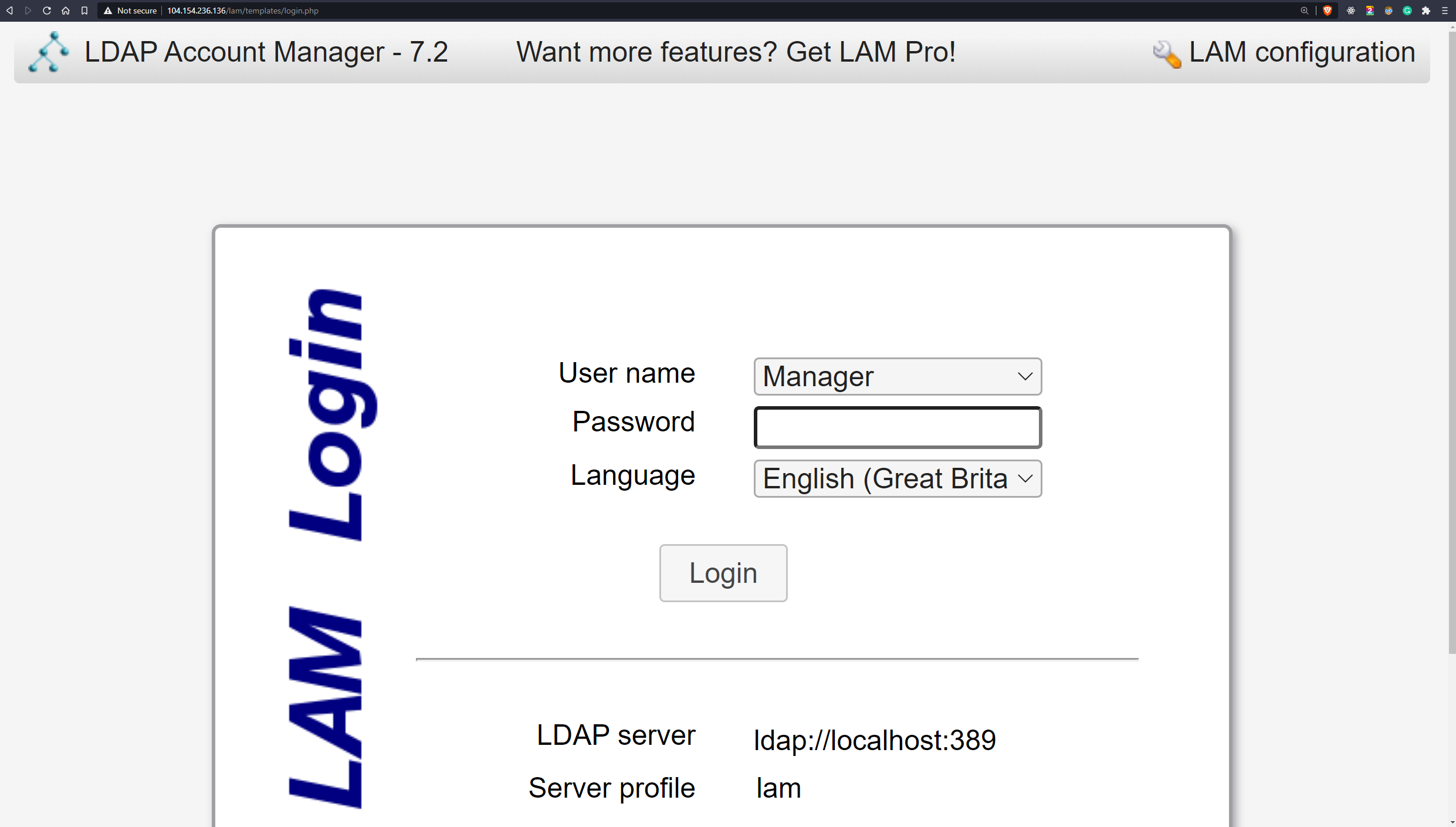
**Screenshots**



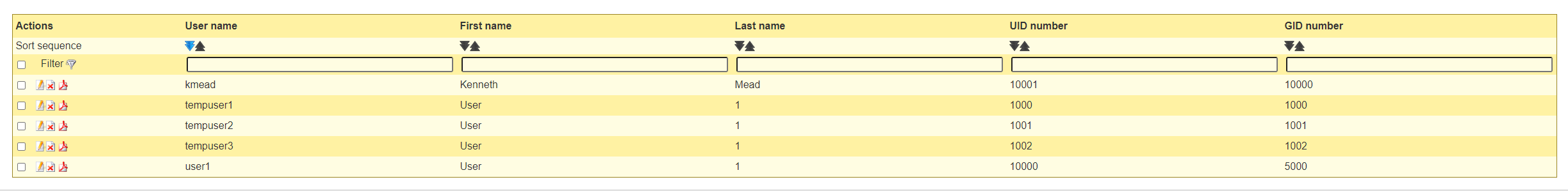


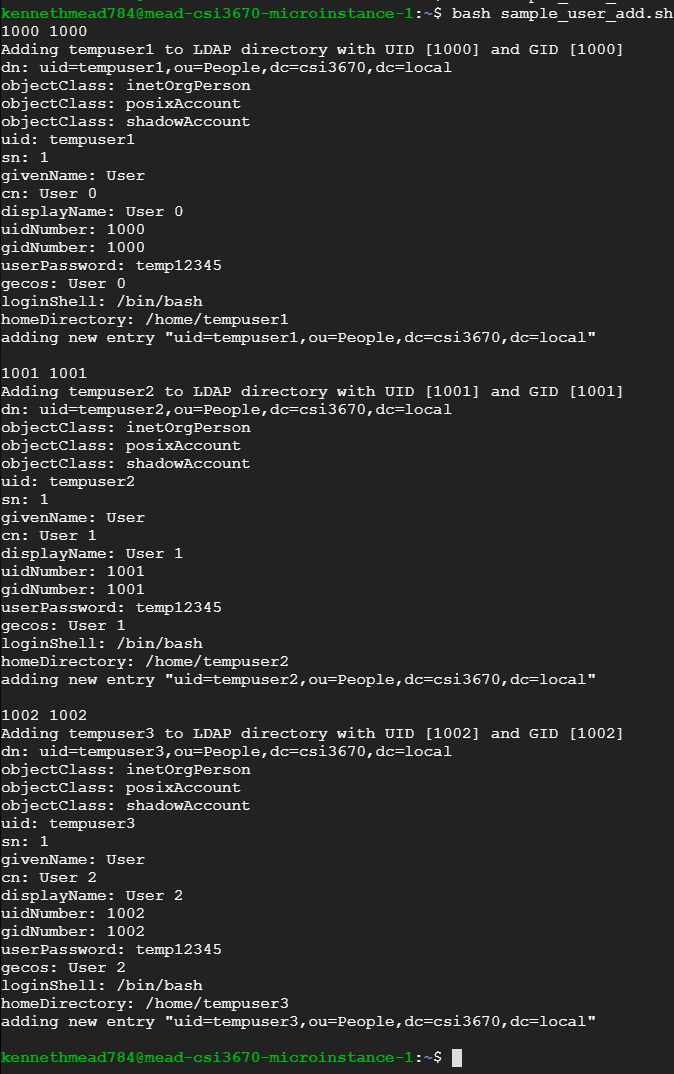
I have a higher resolution monitor, so here is a close-up of my IP

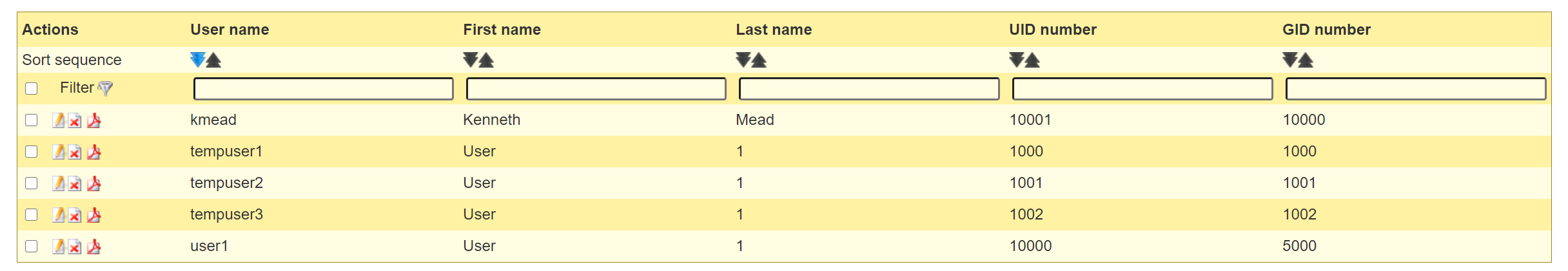




Forgot to take this screenshot at the time needed, so it has the tempusers as well







**Scripts**

#!/bin/bash

users=( "tempuser1" "tempuser2" "tempuser3" )

userpw="temp12345"

ldif\_file="/tmp/bulk\_user.ldif"

dn="cn=admin,dc=csi3670,dc=local"

adminpw="password"   ### REPLACE THIS WITH YOUR ADMIN PASSWORD

i=0

for user in "${users[@]}"; do

  touch $ldif\_file

  uid=$(( $i + 1000 ))

  gid=$(( $i + 1000 ))

  echo $uid $gid

  echo "Adding $user to LDAP directory with UID [$uid] and GID [$gid]"

  echo "dn: uid=$user,ou=People,dc=csi3670,dc=local" >> $ldif\_file

  echo "objectClass: inetOrgPerson" >> $ldif\_file

  echo "objectClass: posixAccount" >> $ldif\_file

  echo "objectClass: shadowAccount" >> $ldif\_file

  echo "uid: $user" >> $ldif\_file

  echo "sn: 1" >> $ldif\_file

  echo "givenName: User" >> $ldif\_file

  echo "cn: User $i" >> $ldif\_file

  echo "displayName: User $i" >> $ldif\_file

  echo "uidNumber: $uid" >> $ldif\_file

  echo "gidNumber: $gid" >> $ldif\_file

  echo "userPassword: $userpw" >> $ldif\_file

  echo "gecos: User $i" >> $ldif\_file

  echo "loginShell: /bin/bash" >> $ldif\_file

  echo "homeDirectory: /home/$user" >> $ldif\_file

  cat $ldif\_file

  # Add user

  ldapadd -x -D $dn -w $adminpw -a -f $ldif\_file

  # Clean up

  rm $ldif\_file

  i=$(( $i + 1 ))

done

**ldif file**

dn: ou=People,dc=csi3670,dc=local

objectClass: organizationalUnit

ou: People

dn: ou=Groups,dc=csi3670,dc=local

objectClass: organizationalUnit

ou: Groups

dn: cn=justkenny,ou=Groups,dc=csi3670,dc=local

objectClass: posixGroup

cn: justkenny

gidNumber: 5000

dn: uid=user1,ou=People,dc=csi3670,dc=local

objectClass: inetOrgPerson

objectClass: posixAccount

objectClass: shadowAccount

uid: user1

sn: 1

givenName: User

cn: User 1

displayName: User 1

uidNumber: 10000

gidNumber: 5000

userPassword: Temp12345

gecos: User 1

loginShell: /bin/bash

homeDirectory: /home/user1