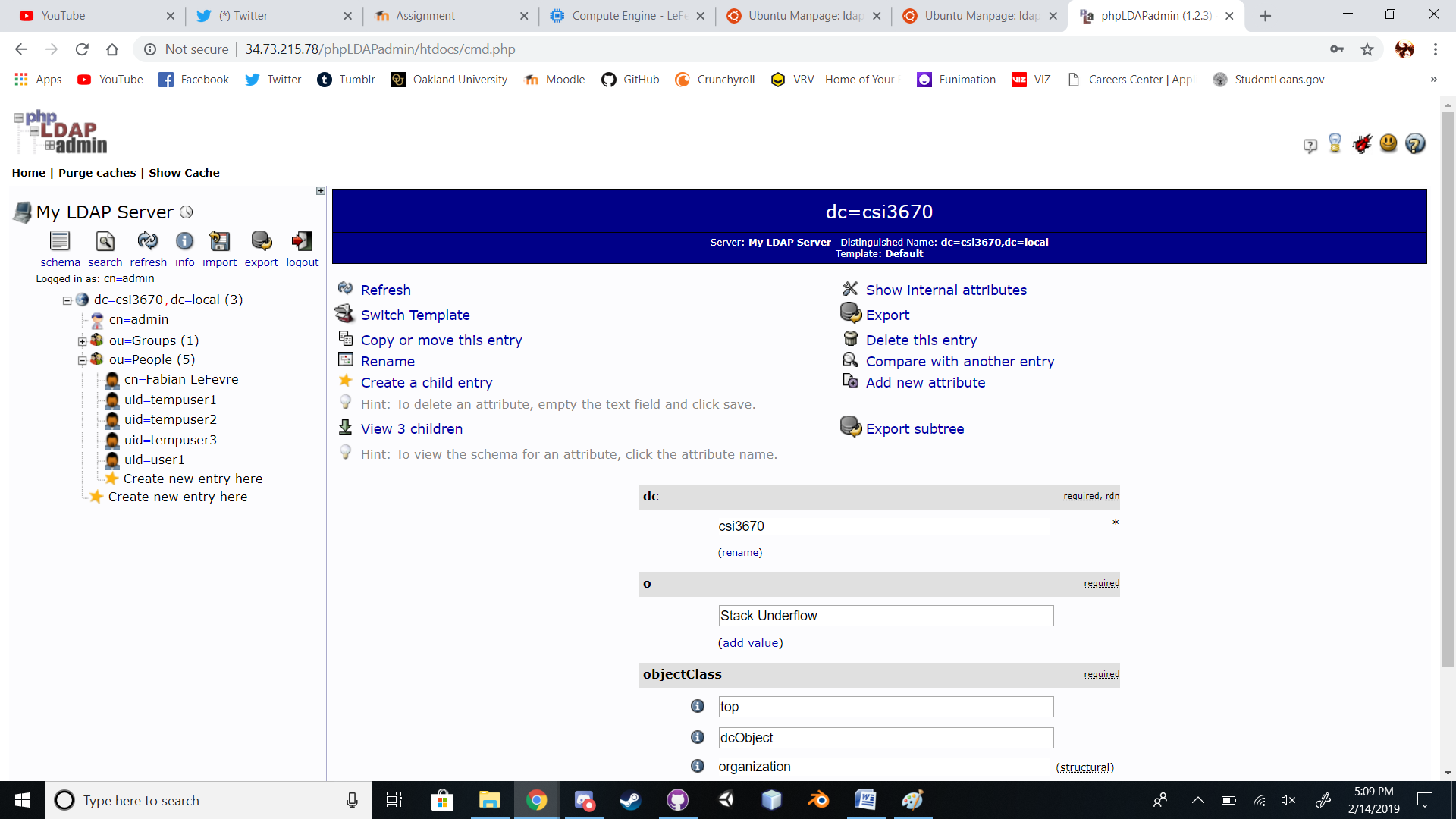
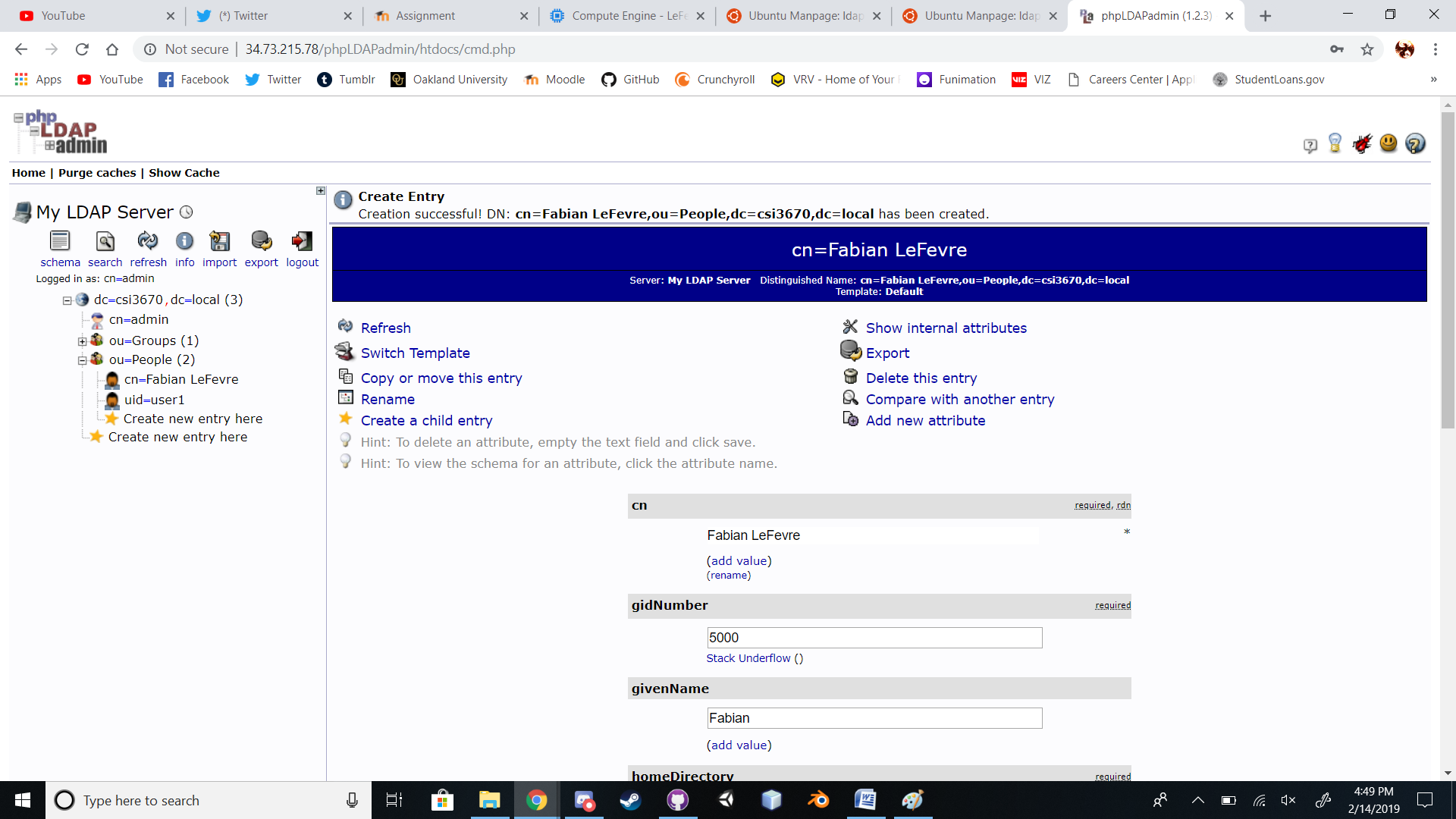
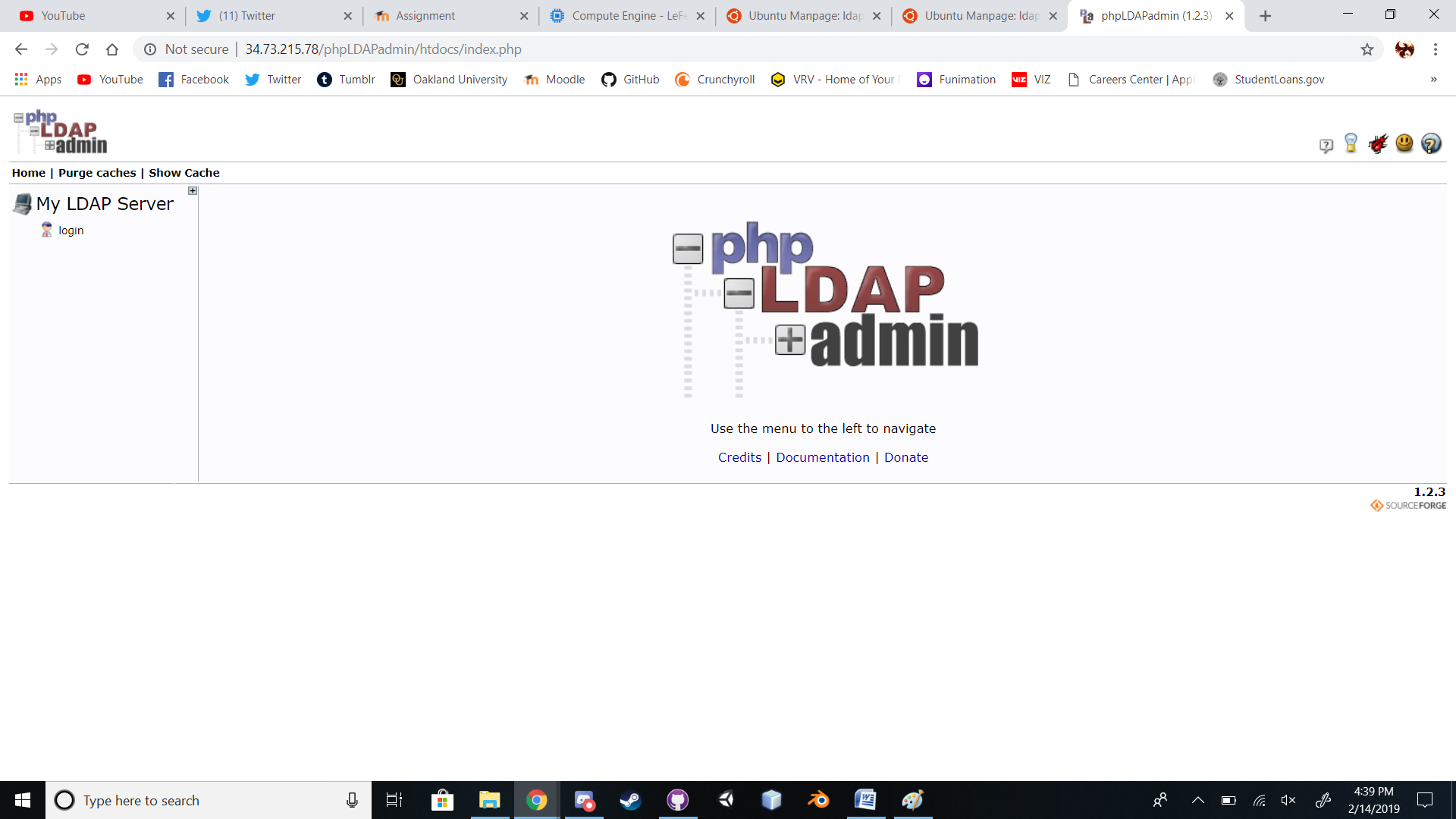
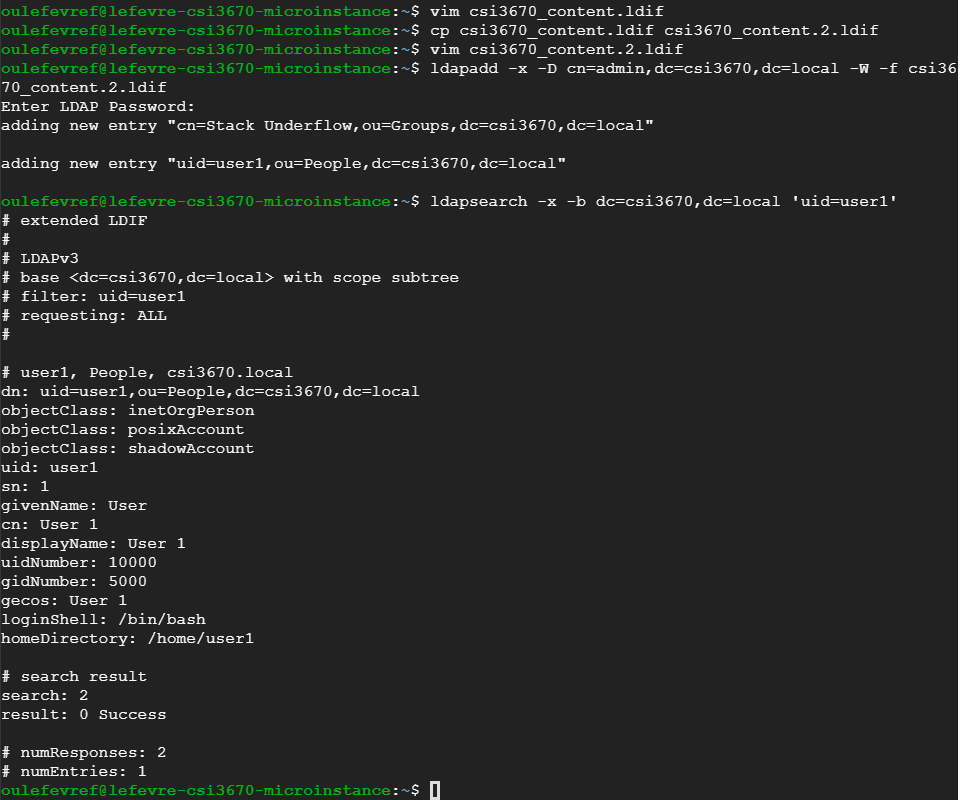
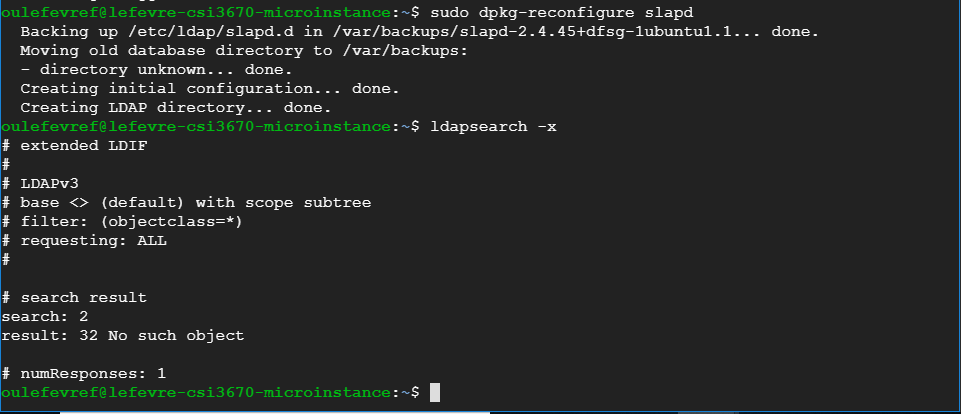
**Name: Fabian LeFevre**

**Homework**

1. Ensure you’ve taken all required screenshots and put them where requested throughout the lab manual.



**2) Bash fun with LDAP!**

Create a bash script. Call it sample\_user\_add.sh

#!/bin/bash

# Comment block similar to the script from Part 1

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

userpw="temp12345"

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

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

adminpw="temp12345"

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 AD19ad19 -a -f $ldif\_file

# Clean up

rm $ldif\_file

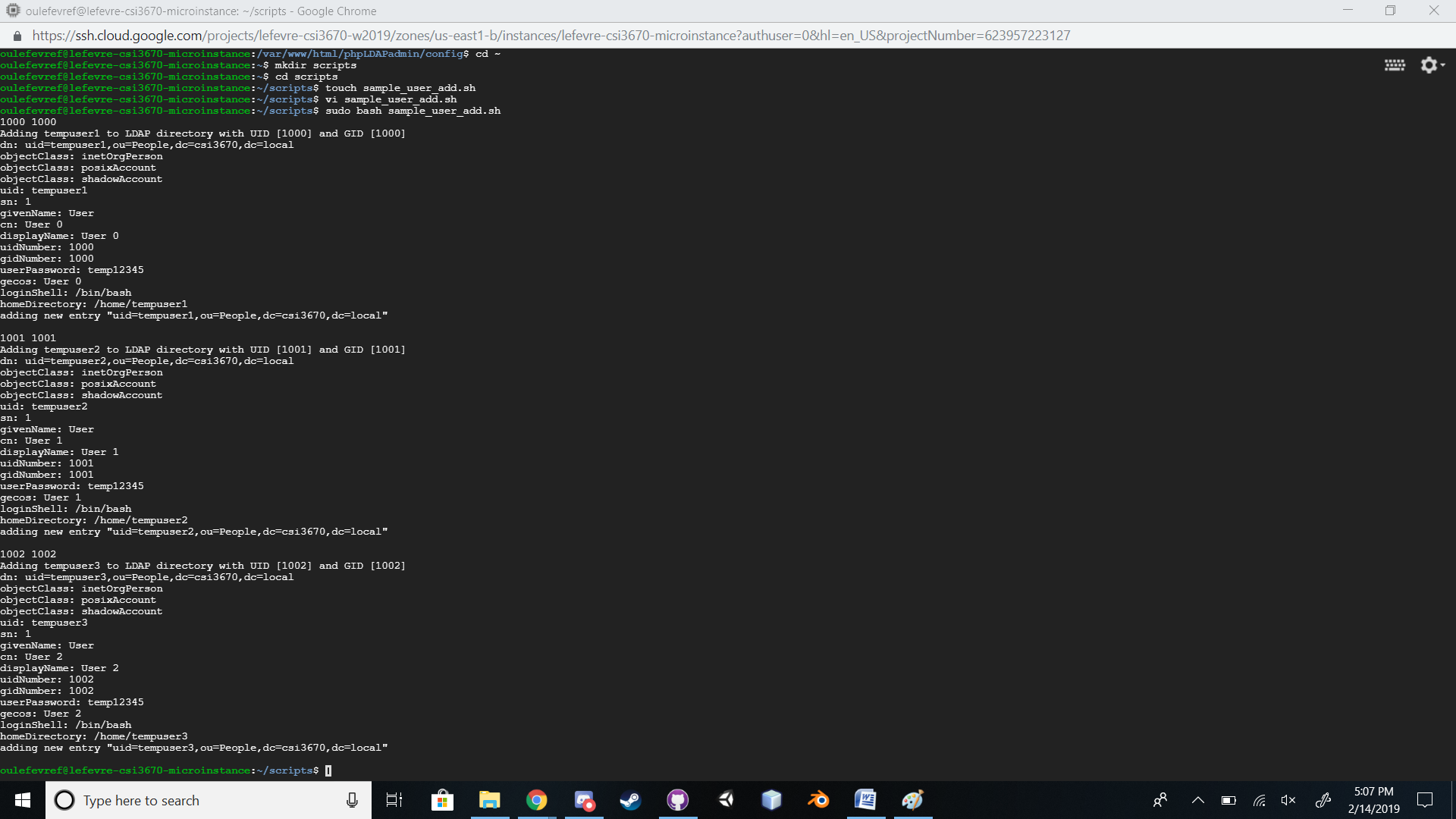
i=$(( $i + 1 ))

done

Run it with bash (don’t run it with sh):

$ sudo bash sample\_user\_add.sh

**Take a screenshot or copy/paste the results here:**



1. [From lab] Note that the user id and group ids are quite high. Why would this be the case?

**uidNumber: 10000**

**gidNumber: 5000**

1. [From lab] Run the following command. In Q3, describe what it does.

**$ ldapsearch -x -b dc=csi3670,dc=local subschemaSubentry**

**(This is correct)**

**Goes through to locate and describe the way the current domain tree is currently configured from passed parameters.**

1. What is LDAP and how does it compare to Active Directory?

**LDAP is an application protocol for querying directory services. LDAP Ssores information in regards to users/groups in a central location. Acts as a database using special attributes and optimizations for reading directory information.**

**LDAP, as stated before, mainly acts as a protocol for directory service queries. Doesn’t have any Windows requirements and has no concept of domains or the functionality of single-sign on. LDAP has to have user/group policies defined in order to be used.**

**AD mainly serves as a directory services database and is built on top of LDAP. In order to use AD, the system will need to have a Microsoft domain controller available. AD also utilizes single-sign on for Windows users. AD is also managed through Group Policy.**

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

**DC is the Domain Component and OU is the Organizational Unit. DC refers to the domain name in the LDAP tree. OU refers to the object within the LDAP tree under the DC.**

**DC’s purpose is to specify the domain to be queried. OU’s purpose is to specify a user or group within the queried DC. Both DC and OU act as a unique identifier field for a d istinguished name.**

1. What is a Distinguished Name?

**A Distinguished Name works like an absolute path in a directory. Each portion of it acts as directional instructions to query the LDAP tree through. In this case, the DN is listed in reverse and ends on the root distinction rather than starting with the root.**

**EX DN: uid = john, ou=person, dc=sys, dc=com**

1. 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.

**The client machine will need to install LDAP packages and configure them through the installation prompts (EX: libnss-ldap, libpam-ldap, ldap-utils). Will then need to adjust system config files (EX: /etc/ldap.conf, sudo auth-client-config –t nss –p lac\_ldap, sudo pam-auth-update, sudo vi /etc/pam.d/common-session <- session required pam\_mkhomdire.so skel=/etc/skel umask=077). Should be able to authenticate client machines through the LDAP server after taking these steps**

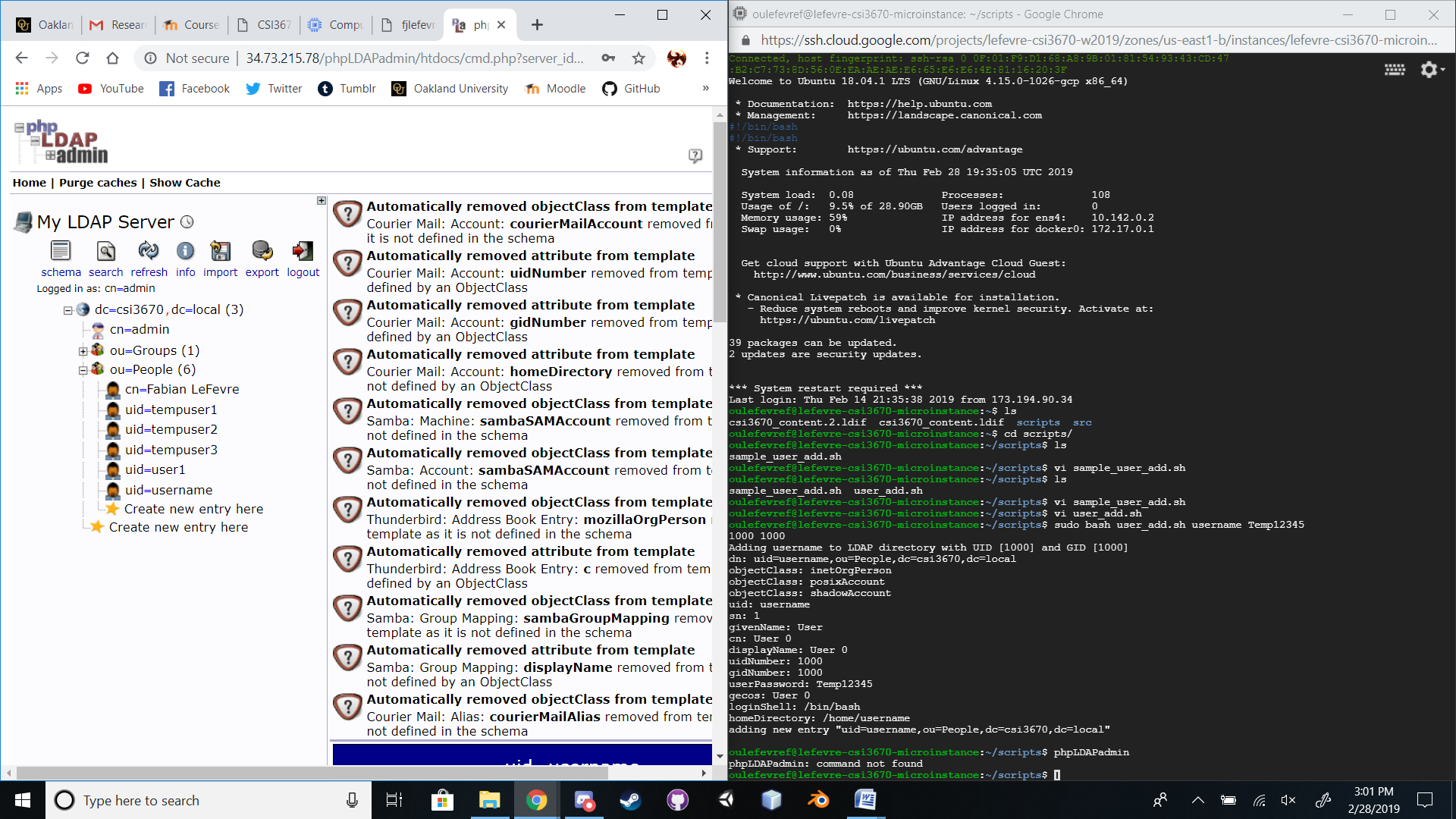
**SOURCE:** [**https://www.tecmint.com/configure-ldap-client-to-connect-external-authentication/**](https://www.tecmint.com/configure-ldap-client-to-connect-external-authentication/)

1. Modify the script above to create a new user from the command line. Call it 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 phpLDAPadmin or an ldapsearch query).

* 1. *For extra credit, make your arguments intelligent and read any number of user/password combinations.*



1. Zip up this report, your script(s) and any other materialsand submit to Moodle