LABORATOIRE VII – CEG 4399

CEG 4399- Design of Secure Computer Sys.

Université d'Ottawa

Professeur : Amir H. Razavi

Noms et numéros des étudiants :
Gbegbe Decaho Jacques 300094197

Date de soumission: 07 November 2024

LDAP

Introduction

1 Overview

This lab illustrates the use of LDAP to authenticate users of Linux systems, such that multiple computers share a single repository of user and group information, including the passwords that authenticate users. This strategy allows users and administrators to manage a single set of credentials that can then be used to access multiple computers.

1.1 Background

The student is expect to have separately learned about the basic elements of Linux users, groups and authentication, e.g., the /etc/passwd and /etc/shadow files. The student is also expected to have a basic knowledge of the use of Lightweight Directory Access Protocol (LDAP).

The student is expected to have some familiarity with the Linux command line, the basics of the file system, and the ability to locate and edit a file. And some experience with the Wireshark tool is expected (e.g., the wireshark-intro lab).

2 Lab Environment

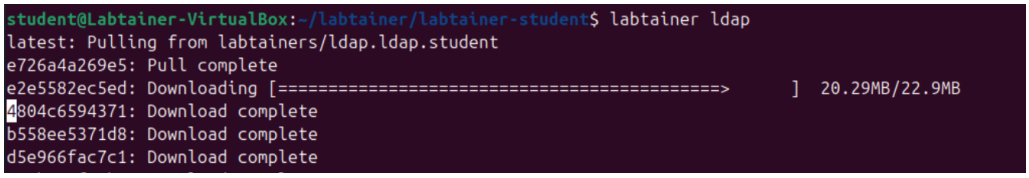
This lab runs in the Labtainer framework, available at http://my.nps.edu/web/c3o/labtainers. That site includes links to a pre-built virtual machine that has Labtainers installed, however Labtainers can be run on any Linux host that supports Docker containers.

From your labtainer-student directory start the lab using:

```
labtainer ldap
```

A link to this lab manual will be displayed.

We loaded the "**ldap**" labtainer into the virtualbox in order to launch our working environment.



3 Network Configuration

This lab includes a client computer, two servers and an ldap server shown in Figure 1. When the lab starts, you will get one virtual terminal connected to the client, and one connected to the ldap server.

The host names of each component are per the diagram. The /etc/hosts files allow use of these host names instead of explicit ip addresses.

The two Linux servers have been configured to use the ldap server to authenticate users. The ldap server has been initially configured with a single user whose ID is "mike".

The ldap server is configured for the "example.com" domain, with an ldap administrator of "admin" whose password is "adminpass"

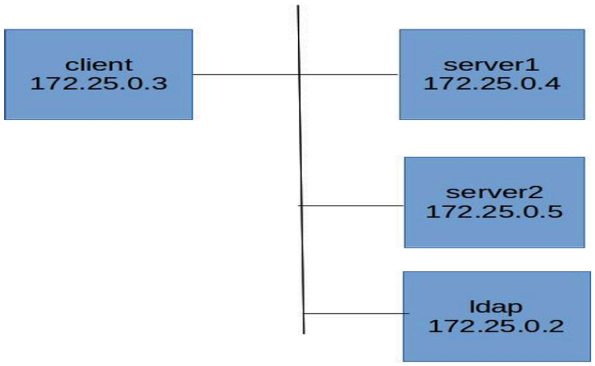


Figure 1: Network topology for the LDAP lab

The different identifiers and passwords defined by default are:

- **mike: password123**
- **admin: adminpass**

1. Lab Tasks

4.1 Explore

On the ldap server, display the ldap directory content using:

```
ldapsearch -x | less
```

and observe the entries in the directory. Note entry for "mike" and "projx".
Start wireshark on the ldap component so that you can observe the protocol traffic.

```
wireshark &
```

Select the `eth0` device. From the "client" computer, ssh to server1 as user "mike":

```
ssh mike@server1
```

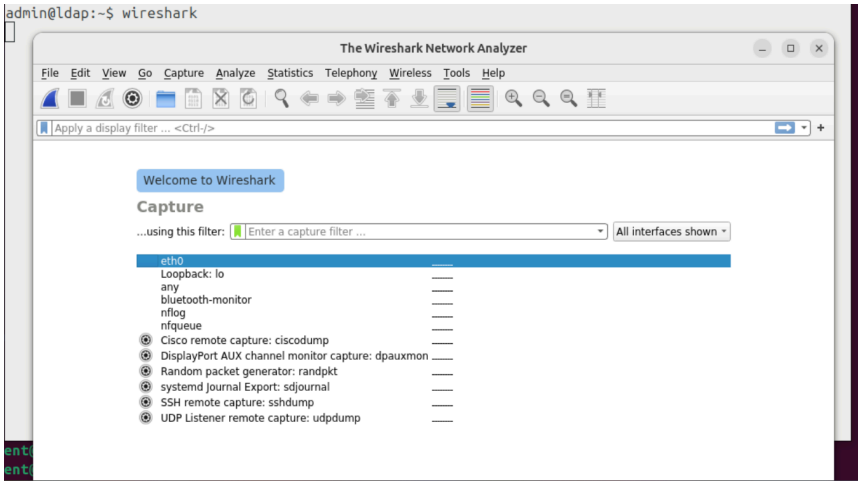
The initial password for "mike" is "password123". The system will require that your change this password and then you will need to ssh again into server1. Change the password to whatever you like, but remember it. Use `ssh` again to login to server1 as mike, providing your new password. Use the `id` command to view your user ID and group. Then, view the /etc/passwd file. Do you see entries for your user or group?

After running the command **"ldapsearch -x | less"**, we observed and captured the parts in the directory content showing the details of **"projx"** and **"mike"**.

```
# projx, groups, example.com
dn: cn=projx,ou=groups,dc=example,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 1500
cn: projx
```

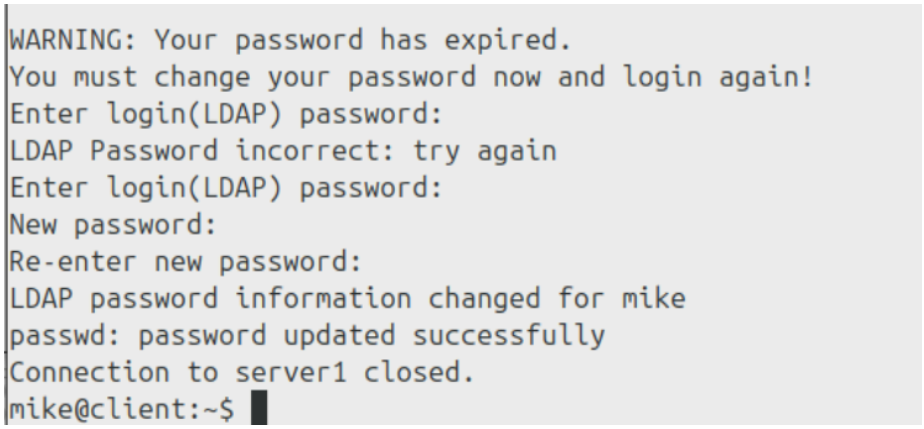
```
# mike, users, example.com
dn: uid=mike,ou=users,dc=example,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: mike
uid: mike
uidNumber: 1501
gidNumber: 1500
homeDirectory: /home/mike
loginShell: /bin/bash
gecos: mike
shadowLastChange: 0
shadowMax: 0
shadowWarning: 0
```

Then we connected to the **wireshark** from the console of **"admin@ldap"**.

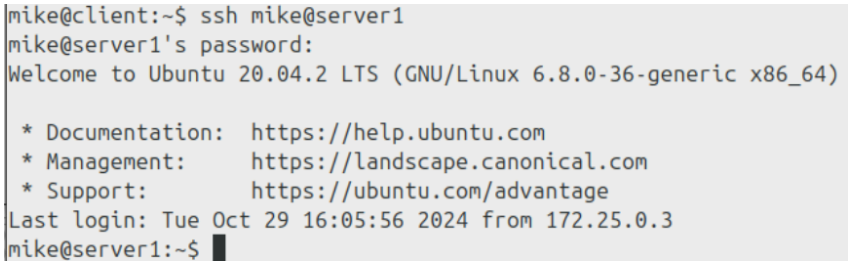


In the **"mike@client"** window, we executed the command **"ssh mike@server1"** in order to connect **"mike"** to server 1. Above, we entered the password **"password123"** in order to validate the authorization to connect to the server.

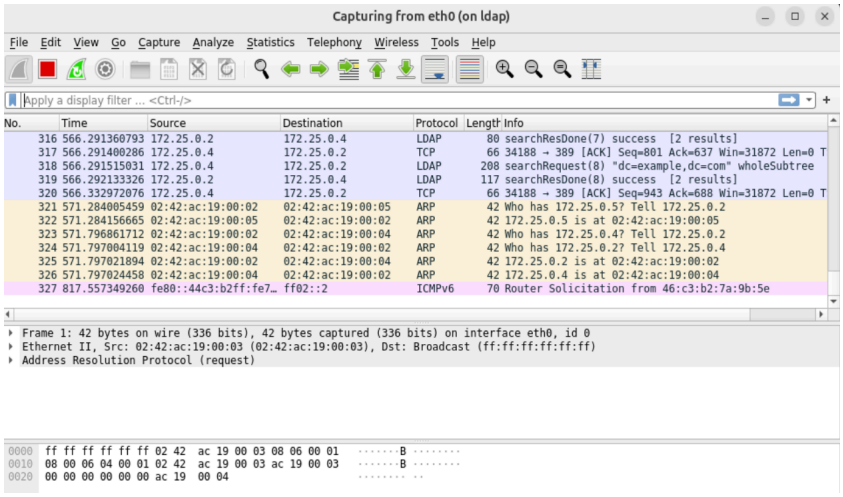
Above we see that **"mike"** is finally logged in to **server 1**.
At the bottom we see a warning asking **"mike"** to change the password because it is old.



Above, we have changed the password of **“mike”** to “**mike123**”.
We have checked the values of the account of “**mike**” present in the directory. As shown in the screen below.



Now in order to verify that everything is "**OK**" we reconnected to **server 1** as "**mike**".

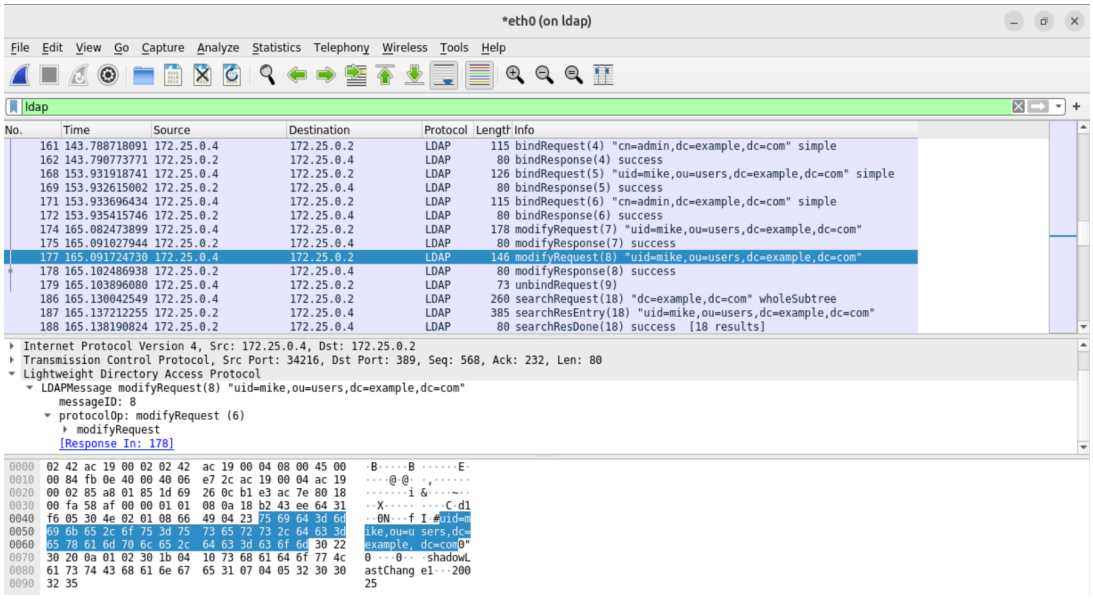


In **wireshark**, we observe the **different threads active** on the **network**.

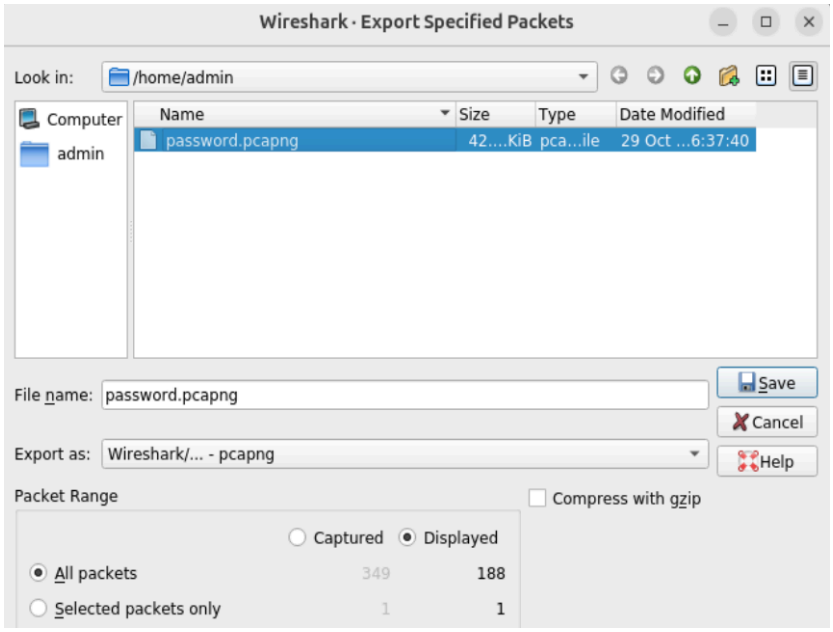
4.2 View protocol traffic

Go to the wireshark window, and stop capturing packets (e.g., the red stop button). Enter a display filter of "ldap", i.e., near the top where it says "Apply a display filter...". Review the LDAP traffic. Which components are exchanging packets? Locate the packet that changed mike's password and use `File / Export Specified Packets` to save that packet in a file named `password.pcapng`

We applied a filter to the wireshark to identify only the threads linked to the "**ldap**".



We have identified the "**ldap**" thread that was responsible for changing the password in the wireshark.



We saved this thread on the virtual machine with the name "**password.pcapng**"

```
mike@server2:~$ exit
logout
Connection to server2 closed.
mike@server1:~$
```

Then we terminated the "**mike**" connection on **server 2**.
Then we reconnected to **server 1** with the command **"ssh mike@server1**"

4.3 Use the mike credentials to access another server

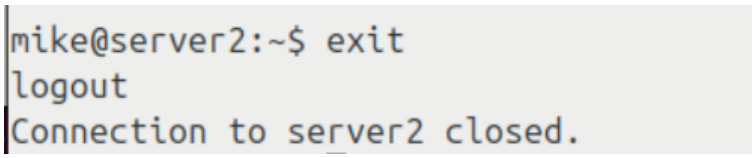
Exit your ssh session from server1. Then ssh to server2:

```
ssh mike@server2
```

What password do you expect to use to authenticate to server2? After logging into server2, exit that ssh session.

The expected password is the one established at the base **"adminpass**".

After which we broke the connection with server 1 and logged into server 2 to verify that we have access to **server 2.**



Then we terminated the connection on **server 2**.

4.4 Add an LDAP user

Go to the ldap virtual terminal and use `ls` to see a directory listing. View the file named `mike.ldif`, it was used to define the user named "mike". Then view the projx.ldif file. The LDAP command that was used to add the entry defined in mike.ldif is:

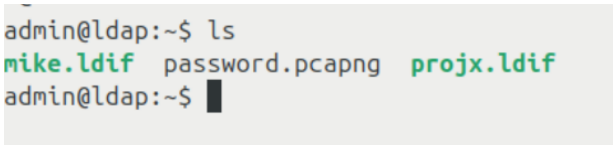
```
ldapadd -x -W -D "cn=admin,dc=example,dc=com" -f mike.ldif
```

Note how the `-D` option names the administrator on whose behalf the LDAP addition is to be made. Use `man ldapadd` to learn more about the syntax of that command. The initial password for the mike user was created with this command:

```
ldappasswd -s password123 -W -D "cn=admin,dc=example,dc=com" \
   -x "uid=mike,ou=users,dc=example,dc=com"
```

Create ldif files to define a new group named "qa" and a new user having an ID of "mary". Assign mary to the qa group. Take care to adjust the uidNumber and gidNumber values. Use the ldapadd command to add the new group and the new user. Use the ldappasswd command to assign an initial password to mary. Again, the password for the LDAP administrator is "adminpass".

Then go to the client computer and test your ability to ssh as mary to both server1 and server2.



We checked the files present in the **ldap folder**.

```
admin@ldap:~$ cat mike.ldif
dn: uid=mike,ou=users,dc=example,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: mike
uid: mike
uidNumber: 1501
gidNumber: 1500
homeDirectory: /home/mike
loginShell: /bin/bash
gecos: mike
userPassword: {crypt}x
shadowLastChange: 0
shadowMax: 0
shadowWarning: 0
```

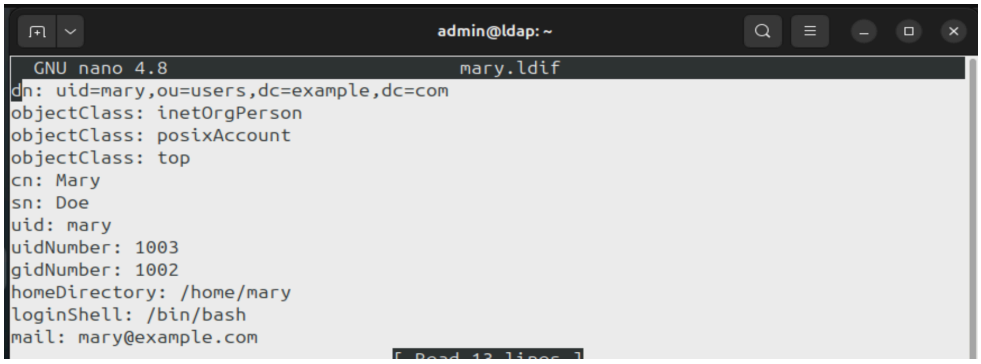
Above we have displayed the components of the "**mike.ldif**" file with the "**cat**" command.

```
admin@ldap:~$ cat projx.ldif
dn: cn=projx,ou=groups,dc=example,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 1500
admin@ldap:~$
```

Above, we have displayed the components of the "**projx.ldif**" file with the "**cat**" command.

```
admin@ldap:~$ ldapadd -x -W -D "cn=admin,dc=example,dc=com" -f mike.ldif
Enter LDAP Password:
adding new entry "uid=mike,ou=users,dc=example,dc=com"
ldap_add: Already exists (68)
```

In the "**admin@ldap**" window, using the command "**ldapadd -x -W -D "cn=admin,dc=example,dc=com" -f mike.ldif"**, we defined mike as an administrator and specified the file to import containing his information.



With "**nano**" we verified that the information was correct by adding it to the file.

Similarly, we checked and added the information in the group file "**qa.ldif**".

```
admin@ldap:~$ nano qa.ldif
admin@ldap:~$ nano mary.ldif
admin@ldap:~$ ldapadd -x -W -D "cn=admin,dc=example,dc=com" -f qa.ldif
Enter LDAP Password:
adding new entry "cn=qa,ou=groups,dc=example,dc=com"

admin@ldap:~$ ldapadd -x -W -D "cn=admin,dc=example,dc=com" -f mary.ldif
Enter LDAP Password:
adding new entry "uid=mary,ou=users,dc=example,dc=com"

admin@ldap:~$ ldappasswd -s "mary123" -W -D "cn=admin,dc=example,dc=com" -x "uid=mary,ou=users,dc=ex
ample,dc=com"
Enter LDAP Password:
admin@ldap:~$
```

We created and defined a new admin "**mary**" and added her using the "**mary.ldif**" file containing her information.
We then changed the password of "**mary**" in the file to that of "**mary123**"

```
mike@server1:~$ ssh mary@server1
mary@server1's password:
Creating directory '/home/mary'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 6.8.0-36-generic x86_64)

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

mary@server1:~$
```

We then managed to connect it to **server 1**

```
mary@server1:~$ exit
logout
Connection to server1 closed.
```

We have terminated his connection to this server.

```
mike@server1:~$ ssh mary@server2
mary@server2's password:
Creating directory '/home/mary'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 6.8.0-36-generic x86_64)

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

mary@server2:~$
```

We then managed to connect it to **server 2**.

```
mary@server2:~$ exit
logout
Connection to server2 closed.
```

We have terminated his connection to this server.

5 Submission

After finishing the lab, go to the terminal on your Linux system that was used to start the lab and type:

```
stoplab
```

When you stop the lab, the system will display a path to the zipped lab results on your Linux system. Provide that file to your instructor, e.g., via the Sakai site.

We finally stopped the labtainer with the "**stoplab**" command.

```
student@Labtainer-VirtualBox:~/labtainer/labtainer-student$ stoplab
Results stored in directory: /home/student/labtainer_xfer/ldap
student@Labtainer-VirtualBox:~/labtainer/labtainer-student$
```