LDAP

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.

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”

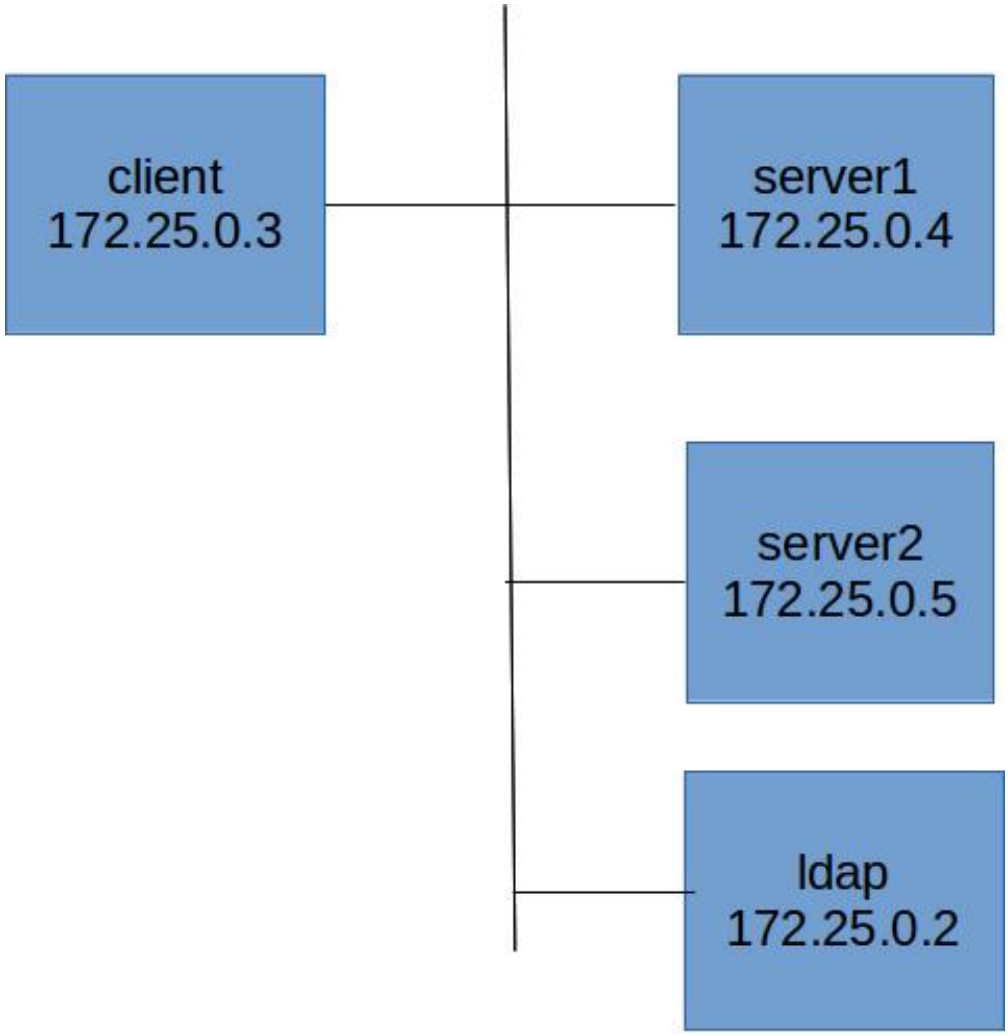

Figure 1: Network topology for the LDAP lab

4 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?

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`

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.

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,
```

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.

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.