

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

Môn: HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX
BÁO CÁO BÀI THỰC HÀNH
Tìm hiểu về dịch vụ xác thực LDAP

Họ và tên sinh viên: Lê Anh Tuấn

Mã số sinh viên: B21DCAT205

Họ và tên giảng viên: TS. Đinh Trường Duy

Hà Nội 11 năm 2023

1. GIỚI THIỆU BÀI THỰC HÀNH

1.1 Mục đích

- Bài thực hành này minh họa việc sử dụng LDAP để xác thực người dùng trên hệ thống Linux, sao cho nhiều máy tính chia sẻ một kho thông tin người dùng và nhóm duy nhất, bao gồm cả mật khẩu xác thực người dùng. Chiến lược này cho phép người dùng và quản trị viên quản lý một tập hợp thông tin đăng nhập duy nhất có thể được sử dụng để truy cập vào nhiều máy tính.

1.2 Yêu cầu

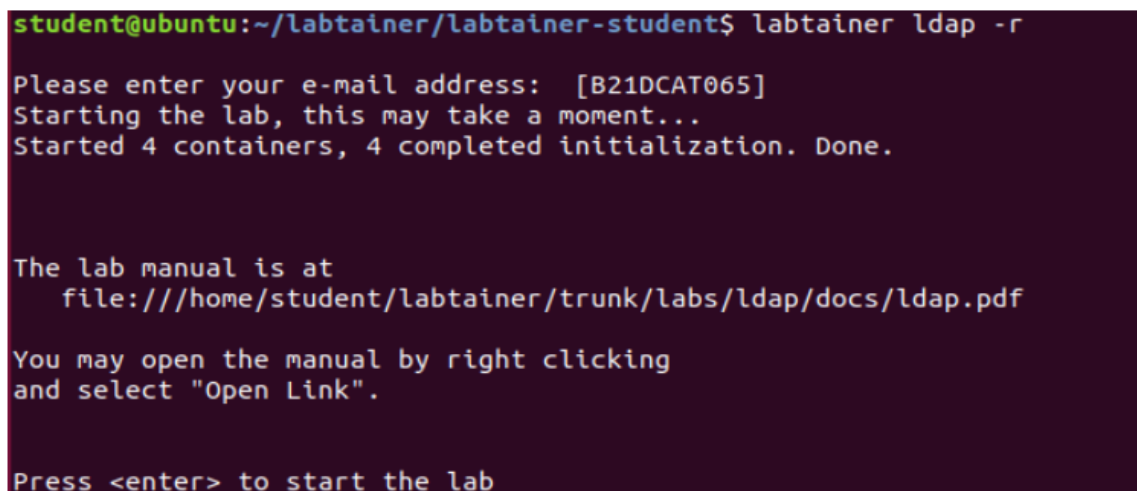
- Nắm được kiến thức về các kiến thức cơ bản của người dùng, nhóm và xác thực trong Linux, ví dụ như các tệp `/etc/passwd` và `/etc/shadow`. Ngoài ra, cần có kiến thức cơ bản về việc sử dụng Lightweight Directory Access Protocol (LDAP).

2 NỘI DUNG THỰC HÀNH

Chuẩn bị lab

Khởi động lab:

```
labtainer -r ldap
```



```
student@ubuntu:~/labtainer/labtainer-student$ labtainer ldap -r
Please enter your e-mail address: [B21DCAT065]
Starting the lab, this may take a moment...
Started 4 containers, 4 completed initialization. Done.

The lab manual is at
  file:///home/student/labtainer/trunk/labs/ldap/docs/ldap.pdf

You may open the manual by right clicking
and select "Open Link".

Press <enter> to start the lab
```

Chúng ta có 3 Terminal hiện ra, 1 là `admin@ldap`, 2 là `mike@client`, 3 là `admin@server1` và `admin@server2` cùng chung 1 terminal.

Nhiệm vụ 1: Tìm hiểu

Trước tiên ta sử dụng lệnh `ldapsearch -x | less` trên `admin@ldap` để xem thông tin thư mục ldap, bao gồm thông tin các user, các group trong miền `example.com`. Lưu ý mục “mike” và “projx” vì nhiệm vụ sau sẽ sử dụng đến

```
admin@ldap: ~
File Edit View Search Terminal Help
cn: admin
description: LDAP administrator

# users, example.com
dn: ou=users,dc=example,dc=com
objectClass: organizationalUnit
ou: users

# groups, example.com
dn: ou=groups,dc=example,dc=com
objectClass: organizationalUnit
ou: groups

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

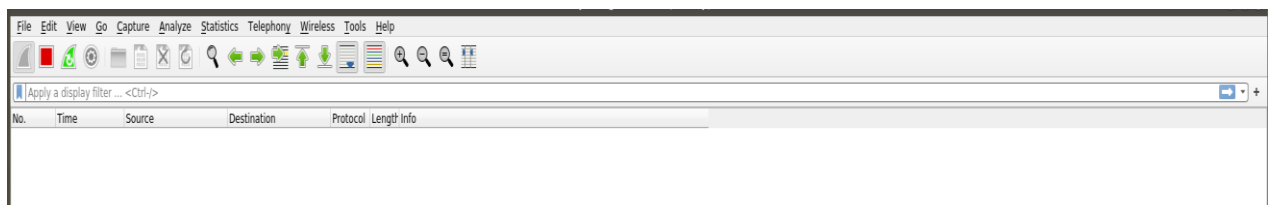
# mike, users, example.com
dn: uid=mike,ou=users,dc=example,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: mike
uid: mike
uidNumber: 1501
gidNumber: 1500
homeDirectory: /home/mike
loginShell: /bin/bash
gecos: mike
shadowLastChange: 0
shadowMax: 0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

# search result
search: 2
result: 0 Success

# numResponses: 7
# numEntries: 6
(END)
```

Khởi động **wireshark** trên **admin@ldap** và chọn bộ lọc thiết bị **eth0**:

wireshark &



Chọn thiết bị **eth0**. Từ máy tính **client**, kết nối SSH đến **server1** với người dùng "mike", mật khẩu là **password123**

```
ssh mike@server1
```

Vì sử dụng ssh để kết nối nên Server sẽ sử dụng key để mã hóa mật khẩu, từ đó chúng ta có thể thấy trên wireshark các gói tin chúng ta bắt được

```
mike@client: ~
File Edit View Search Terminal Help
mike@client:~$ ssh mike@server1
The authenticity of host 'server1 (172.25.0.4)' can't be established.
ECDSA key fingerprint is SHA256:ZtE8xi5Y50aUktZ/XtgjIs1c5jxYQ8B4VqSofmlgGng.
Are you sure you want to continue connecting (yes/no)? Y
Please type 'yes' or 'no': yes
Warning: Permanently added 'server1,172.25.0.4' (ECDSA) to the list of known hosts.
mike@server1's password:
Permission denied, please try again.
mike@server1's password:
packet write_wait: Connection to 172.25.0.4 port 22: Broken pipe
mike@client:~$ ssh mike@server1
mike@server1's password:
You are required to change your password immediately (administrator enforced)
Creating directory '/home/mike'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.18.0-15-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
```

Capturing from eth0 (on ldap)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	02:42:ac:19:00:03	Broadcast	ARP	42	Who has 172.25.0.4? Tell 172.25.0.3
2	10.937734477	172.25.0.4	172.25.0.2	TCP	74	49516 → 389 [SYN] Seq=0 Win=29200 Len=0 M
3	10.938761397	172.25.0.2	172.25.0.4	TCP	74	389 → 49516 [SYN, ACK] Seq=0 Ack=1 Win=28
4	10.939087545	172.25.0.4	172.25.0.2	TCP	66	49516 → 389 [ACK] Seq=1 Ack=1 Win=29312 L
5	10.940189011	172.25.0.4	172.25.0.2	LDAP	115	bindRequest(1) "cn=admin,dc=example,dc=com"
6	10.940597678	172.25.0.2	172.25.0.4	TCP	66	389 → 49516 [ACK] Seq=1 Ack=50 Win=29056
7	10.940598131	172.25.0.2	172.25.0.4	LDAP	98	bindResponse(1) success

Hệ thống yêu cầu ta đổi mật khẩu do mật khẩu cũ đã hết hạn, ta đổi mật khẩu thành **tuant123**, các tiến trình vẫn được bắt trong phần **wireshark**

```
WARNING: Your password has expired.
You must change your password now and login again!
Enter login(LDAP) password:
LDAP Password incorrect: try again
Enter login(LDAP) password:
New password:
Re-enter new password:
LDAP password information changed for mike
passwd: password updated successfully
Connection to server1 closed.
mike@client:~$
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
239	578.091783567	172.25.0.4	172.25.0.2	TCP	66	49532 → 389 [FIN, ACK] Seq=638 Ack=1005 Win=32512 Len=0 TSval=...
240	578.091822290	172.25.0.2	172.25.0.4	TCP	66	389 → 49532 [FIN, ACK] Seq=1005 Ack=639 Win=32256 Len=0 TSval=...
241	578.091836473	172.25.0.4	172.25.0.2	TCP	66	49532 → 389 [ACK] Seq=639 Ack=1006 Win=32512 Len=0 TSval=3435...
242	578.092583879	172.25.0.4	172.25.0.2	LDAP	260	searchRequest(18) "dc=example,dc=com" wholeSubtree
243	578.101955160	172.25.0.2	172.25.0.4	LDAP	385	searchResEntry(18) "uid=mike,ou=users,dc=example,dc=com"
244	578.102036352	172.25.0.2	172.25.0.4	LDAP	80	searchResDone(18) success [18 results]
245	578.102059863	172.25.0.4	172.25.0.2	TCP	66	49524 → 389 [ACK] Seq=3378 Ack=5370 Win=47488 Len=0 TSval=343...
246	578.103079958	172.25.0.4	172.25.0.2	LDAP	260	searchRequest(19) "dc=example,dc=com" wholeSubtree
247	578.103251789	172.25.0.2	172.25.0.4	LDAP	385	searchResEntry(19) "uid=mike,ou=users,dc=example,dc=com"
248	578.103290178	172.25.0.2	172.25.0.4	LDAP	80	searchResDone(19) success [18 results]
249	578.103309628	172.25.0.4	172.25.0.2	TCP	66	49524 → 389 [ACK] Seq=3572 Ack=5703 Win=48512 Len=0 TSval=343...
250	578.104582551	172.25.0.4	172.25.0.2	TCP	66	49524 → 389 [FIN, ACK] Seq=3572 Ack=5703 Win=48512 Len=0 TSva...
251	578.105488924	172.25.0.2	172.25.0.4	TCP	66	389 → 49524 [FIN, ACK] Seq=5703 Ack=3573 Win=48256 Len=0 TSva...
252	578.105546185	172.25.0.4	172.25.0.2	TCP	66	49524 → 389 [ACK] Seq=3573 Ack=5704 Win=48512 Len=0 TSval=343...

▶ Frame 242: 260 bytes on wire (2080 bits), 260 bytes captured (2080 bits) on interface eth0, id 0
 ▶ Ethernet II, Src: 02:42:ac:19:00:04 (02:42:ac:19:00:04), Dst: 02:42:ac:19:00:02 (02:42:ac:19:00:02)
 ▶ Internet Protocol Version 4, Src: 172.25.0.4, Dst: 172.25.0.2
 ▶ Transmission Control Protocol, Src Port: 49524, Dst Port: 389, Seq: 3184, Ack: 5037, Len: 194
 ▶ Lightweight Directory Access Protocol

Đăng nhập lại với mật khẩu mới, ta đã vào được **server1** với tài khoản “mike”

```
mike@client:~$ ssh mike@server1
mike@server1's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.18.0-15-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Last login: Sat Nov 18 06:02:23 2023 from 172.25.0.3
mike@server1:~$
```

Dùng lệnh **id** để kiểm tra **userID** và **groupID** của “mike”

```
mike@server1:~$ id
uid=1501(mike) gid=1500(projx) groups=1500(projx)
```

Từ đây biết được id của mike là 1501 và group của mike là projx với id là 1500 đúng như khi ta dùng lệnh **ldapsearch** tại **admin@ldap**.

Ta dùng lệnh `cat /etc/passwd` để kiểm tra người dùng và nhóm

```
mike@server1:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:101:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
```

Nhiệm vụ 2: Xem lưu lượng giao thức

Ta thấy rằng hiện đang có root, admin là đang login.

Tiếp đây chúng ta sẽ đăng nhập vào user “mike” ở server2 luôn với câu lệnh **ssh mike@server2** và mật khẩu là **tuan123**

```
mike@server1:~$ ssh mike@server2
The authenticity of host 'server2 (172.25.0.5)' can't be established.
ECDSA key fingerprint is SHA256:ZtE8xi5Y50aUktZ/XtgjIs1c5jxYQB84Vq5ofmlgGng.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server2,172.25.0.5' (ECDSA) to the list of known hosts.
mike@server2's password:
Creating directory '/home/mike'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.18.0-15-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.

mike@server2:~$
```

Tiếp theo ta sẽ tìm gói tin đã thay đổi mật khẩu của “mike” .

Với giao thức truyền tin là ldap, ta sử dụng filter ldap để lọc các giao thức này ra. Follow và chọn tcp stream, ta nhận được các thông tin trông có phần giống với khi ta

dùng lệnh **ldapsearch** ban đầu => wireshark đã bắt toàn bộ thông tin khi chúng ta đăng nhập vào máy chủ ldap



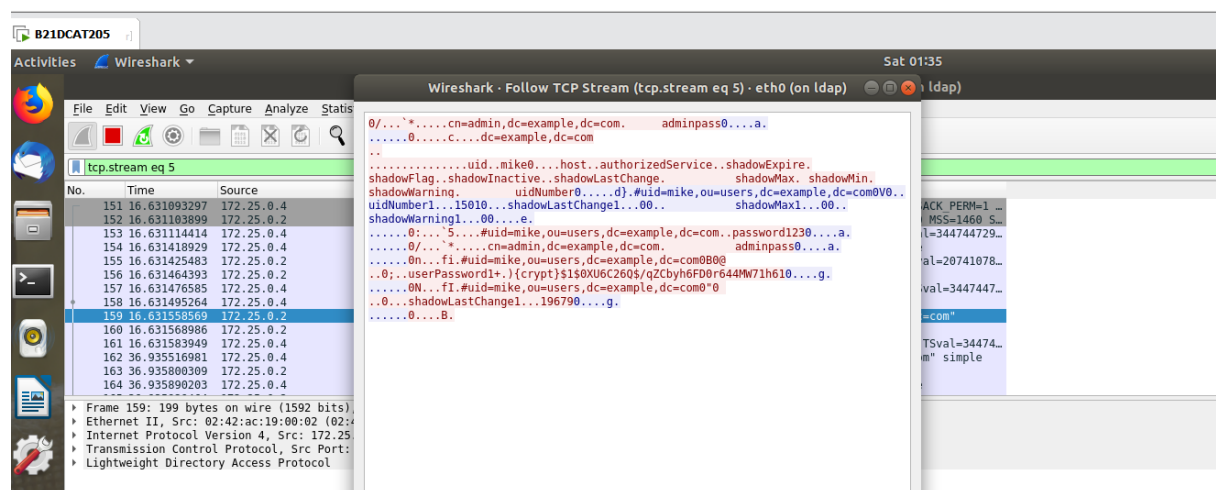
Về dữ liệu trong ldap thì thông tin trong ldap sẽ lưu trữ ở các file .ldif trong đó sẽ chứa thông tin về người dùng, mật khẩu (mã hóa) **userID** và **groupID** của người dùng cũng như group đó

Và nếu như userPassword của 1 user nào đó được đổi thì định dạng đổi sẽ có dạng

userPassword: {crypt}x

Vậy nên trong wireshark ta sẽ tìm gói tin có định dạng trên => gói tin đó chính là gói tin đổi mật khẩu người dùng "mike"

Chọn **File => Export Specified Packets => Selected Packets only** => lưu tên file là **password.pcapng**



Nhiệm vụ 3: Sử dụng tài khoản mike để truy cập máy chủ còn lại

Thoát khỏi phiên SSH đến server1 bằng cách nhập lệnh "exit". Sau đó, SSH đến server2 bằng cách nhập lệnh "ssh mike@server2". Mật khẩu bạn mong đợi sử dụng để xác thực đến server2 là mật khẩu mới mà bạn đã thay đổi trên server1. Sau khi đăng nhập vào server2, thoát khỏi phiên SSH đó bằng cách nhập lệnh "exit".

Nhiệm vụ 4: Thêm một người dùng LDAP

Chuyển đến cửa sổ terminal ảo LDAP và sử dụng lệnh ls để xem danh sách thư mục.

```
admin@ldap:~$ ls
mike.ldif  password.pcapng  projx.ldif
```

Xem tệp có tên mike.ldif, tệp này được sử dụng để định nghĩa người dùng có tên "mike". Sau đó, xem tệp projx.ldif. Lệnh LDAP được sử dụng để thêm mục đã định nghĩa trong tệp mike.ldif là:

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

Với -x là định nghĩa bình thường; -W là mật khẩu admin sẽ được ẩn; -D là chỉ định admin (mật khẩu admin là adminpass).

```
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)
```

Sau đó có thể cấp cho người dùng mật khẩu mặc định (mật khẩu ban đầu) với câu lệnh:

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

```
admin@ldap:~$ ldappasswd -s password123 -W -D "cn=admin,dc=example,dc=com" -x "uid=mike,ou=users,dc=example,dc=com"
Enter LDAP Password:
admin@ldap:~$
```

Ta thử tạo một nhóm mới có tên “qa” và 1 người dùng mới có tên “mary”, gán mary vào nhóm qa. Trong admin ldap tạo 2 file .ldif mới có tên mary.ldif và qa.ldif bằng câu lệnh:

```
vi mary.ldif và vi qa.ldif
```



```

admin@ldap: ~
File Edit View Search Terminal Help
dn: uid=mary,ou=users,dc=example,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: mary
uid: mary
uidNumber: 1510
gidNumber: 1510
homeDirectory: /home/mary
loginShell: /bin/bash
gecos: mary
shadowMax: 0
shadowWarning: 0
shadowLastChange: 19621

```

```

admin@ldap: ~
File Edit View Search Terminal Help
dn: cn=qa,ou=groups,dc=example,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 1510
cn: qa

```

Sau đó ấn **ESC** và **:wq** để lưu file và thoát khỏi phần soạn thảo Sử dụng các lệnh ldapadd cho 2 file .ldif trên và lệnh ldappasswd cho người dùng “mary”

```

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:~$ 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:~$ ldappasswd -s password123 -W -D "cn=admin, dc=example, dc=com" -x "uid=mary, ou=users,dc=example ,dc=com"
Enter LDAP Password:

```

Đã hoàn thành tạo người dùng “mary” và nhóm “qa”.

Dùng `ldapsearch -x` để kiểm tra xem người dùng và nhóm đã được thêm vào ldap chưa


```
# mary, users, example.com
dn: uid=mary,ou=users,dc=example,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: mary
uid: mary
uidNumber: 1510
gidNumber: 1510
homeDirectory: /home/mary
loginShell: /bin/bash
gecos: mary
shadowMax: 0
shadowWarning: 0
shadowLastChange: 19621

# qa, groups, example.com
dn: cn=qa,ou=groups,dc=example,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 1510
cn: qa

# search result
search: 2
result: 0 Success

# numResponses: 9
# numEntries: 8
admin@ldap:~$
```

Đã thêm thành công.

```
admin@ldap:~$ ssh mary@server1
The authenticity of host 'server1 (172.25.0.4)' can't be established.
ECDSA key fingerprint is SHA256:ZtE8xi5Y50aUktZ/XtgjIs1c5jxYQB84Vq5ofmlgGng.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server1,172.25.0.4' (ECDSA) to the list of known hosts.
mary@server1's password:
You are required to change your password immediately (password expired)
Creating directory '/home/mary'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.18.0-15-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.
```

Thử đăng nhập vào server1 và server2 của ldap với người dùng “mary” mật khẩu “password123” thì server sẽ yêu cầu đổi lại mật khẩu, tôi đổi thành “tuan123”

```

admin@ldap:~$ ssh mary@server2
The authenticity of host 'server2 (172.25.0.5)' can't be established.
ECDSA key fingerprint is SHA256:ZtE8xi5Y50aUktZ/XtgjIs1c5jxYQB84Vq5ofmlgGng.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'server2,172.25.0.5' (ECDSA) to the list of known hosts.
mary@server2's password:
Permission denied, please try again.
mary@server2's password:
Creating directory '/home/mary'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.18.0-15-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:~$

```

Nhiệm vụ 5: Mã hóa dữ liệu truyền LDAP

Ta sử dụng sudo su để vào chương trình root sau đó dùng lệnh nano để chỉnh sửa file /etc/ldap.conf và file /etc/ldap/ldap.conf của server1 và server2

```

admin@server1:~$ sudo su
root@server1:/home/admin# nano /etc/ldap.conf
root@server1:/home/admin# nano /etc/ldap/ldap.conf
root@server1:/home/admin#

```

Chỉnh sửa tệp /etc/ldap.conf và thay đổi dòng sau: **uri ldap://ldap** thành **uri ldaps://ldap** và xóa dấu chú thích khỏi dòng: **#ssl on** sẽ trở thành: **ssl on**

# Another way to specify your LDAP server is to provide an uri ldaps://ldap	# Netscape SDK LDAPS ssl on
--	--------------------------------

Sau đó, chỉnh sửa tệp /etc/ldap/ldap.conf (lưu ý thư mục khác biệt!) và thêm dòng này vào cuối tệp: **TLS_REQCERT allow**

```

root@server1: /home/admin
File Edit View Search Terminal Tabs Help
root@server1: /home/admin x admin@server2: ~
GNU nano 4.8 /etc/ldap/ldap.conf Modified
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.

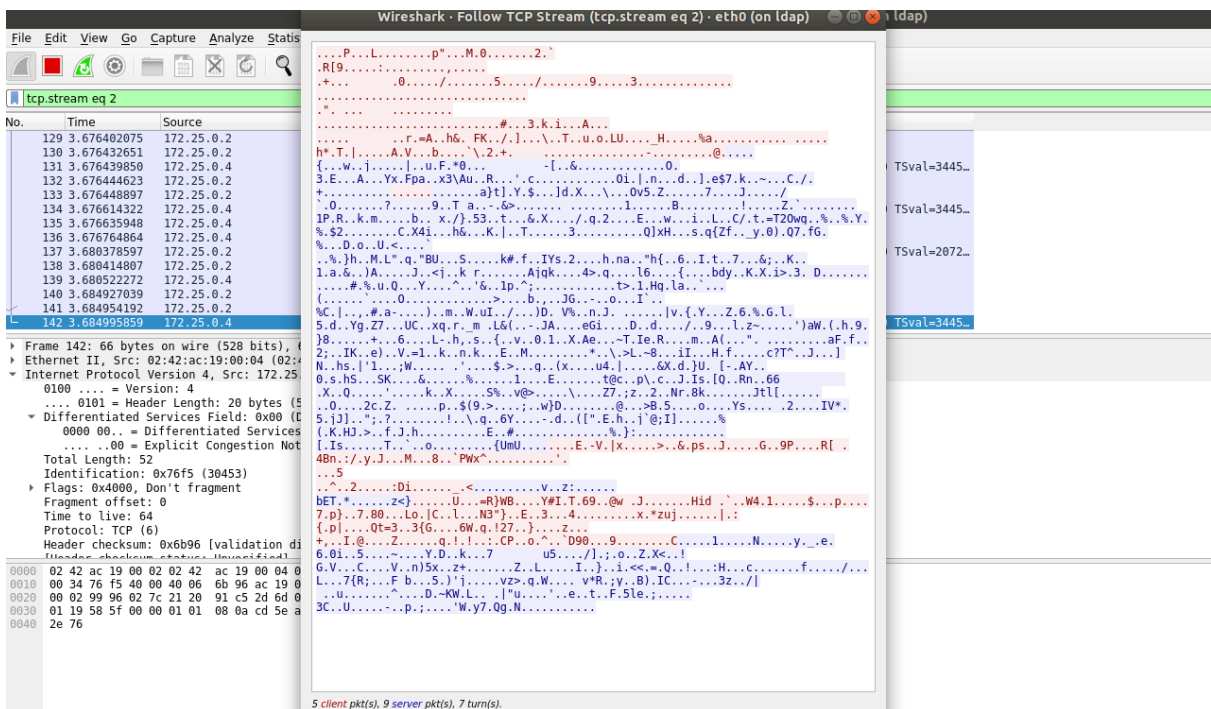
#BASE dc=example,dc=com
#URI ldap://ldap.example.com ldap://ldap-master.example.com:666

#SIZELIMIT 12
#TIMELIMIT 15
#DEREF never

# TLS certificates (needed for GnuTLS)
TLS_CACERT /etc/ssl/certs/ca-certificates.crt
TLS_REQCERT allow

```

Thử connect lại bằng tài khoản mike ta thấy thông tin đã được mã hóa.



Checkwork bài làm

```

student@ubuntu:~/labtainer/labtainer-student$ checkwork ldap
Results stored in directory: /home/student/labtainer_xfer/ldap
Labname ldap

Student      | correct_pcap | mike_server1 | mike_server2 | mary_server1 | mary_server2 |
=====|=====|=====|=====|=====|=====|
B210CAT205   | Y            | Y            | Y            | Y            | Y            |

What is automatically assessed for this lab:
mike_server1, mike_server2, mary_server1, mary_server2, pcap_strings, pcap_pass: user initiated session on the server
correct_pcap: strings extracted from pcap < 15 lines and userPassword in strings

```

Kết quả nộp bài

ID	Thời gian	Bài tập	Kết quả
15080	2023-11-18 18:59:04	Tìm hiểu về dịch vụ xác thực LDAP	4/5 (WA)

