

CSI4139 LAB 7 Report

Name: Iyanu Aketepe

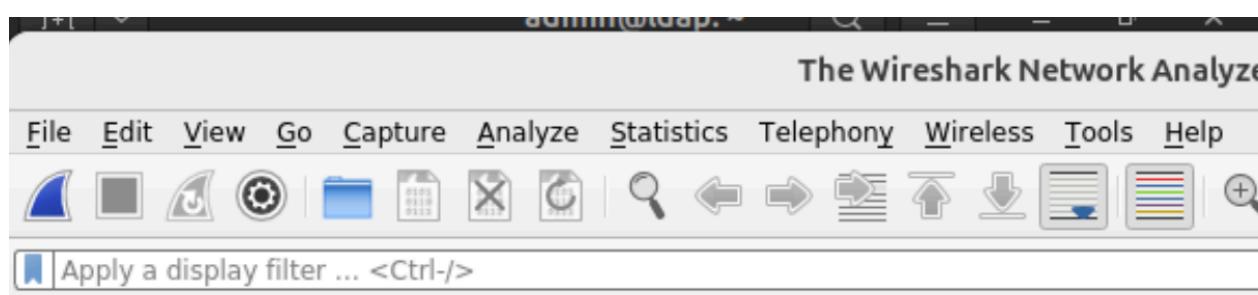
Student No: 300170701

4.1

```
admin@ldap:~$ ldapsearch -x | less
# extended LDIF
#
# LDAPv3
# base <dc=example,dc=com> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# example.com
dn: dc=example,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: example
:■
```

```
admin@ldap:~$ wireshark &
[1] 589
admin@ldap:~$ ■
```

```
mike@client:~$ ssh mike@server1
The authenticity of host 'server1 (172.25.0.4)' can't be
established.
ECDSA key fingerprint is SHA256:ZtE8xi5Y50aUktZ/XtgjIs1c5
jxYQB84Vq5ofmlgGng.
Are you sure you want to continue connecting (yes/no)?
```



Welcome to Wireshark

Capture

...using this filter: Enter a capture filter ...

eth0

Loopback: lo

any

bluetooth-monitor

nflog

nfqueue

Cisco remote capture: ciscodump

```
mike@client:~$ ssh mike@server1
The authenticity of host 'server1 (172.25.0.4)' can't be
established.
ECDSA key fingerprint is SHA256:ZtE8xi5Y50aUktZ/XtgjIs1c5
jxYQB84Vq5ofmlgGng.
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) t
o the list of known hosts.
dispatch_protocol_error: type 7 seq 3
dispatch_protocol_error: Connection to 172.25.0.4 port 22
: Broken pipe
```

```
mike@client:~$ sudo ssh mike@server1
The authenticity of host 'server1 (172.25.0.4)' can't be
established.
ECDSA key fingerprint is SHA256:ZtE8xi5Y50aUktZ/XtgjIs1c5
jxYQB84Vq5ofmlgGng.
Are you sure you want to continue connecting (yes/no)? ye
s
Warning: Permanently added 'server1,172.25.0.4' (ECDSA) t
o the list of known hosts.
mike@server1's password:
You are required to change your password immediately (adm
inistrator enforced)
Creating directory '/home/mike'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 6.8.0-35-generic
x86_64)
```

```
WARNING: Your password has expired.  
You must change your password now and login again!  
Enter login(LDAP) password:  
New password:  
Passwords must differ  
New password:  
Re-enter new password:  
LDAP password information changed for mike  
passwd: password updated successfully  
Connection to server1 closed.  
mike@client:~$ sudo ssh mike@server1  
mike@server1's password:  
Permission denied, please try again.  
mike@server1's password:  
Permission denied, please try again.  
mike@server1's password:  
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 6.8.0-35-generic  
x86_64)  
  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/advantage  
Last login: Thu Oct 31 20:38:29 2024 from 172.25.0.3  
mike@server1:~$ █
```

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

```
mike@server1:/etc$ cat 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
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
```

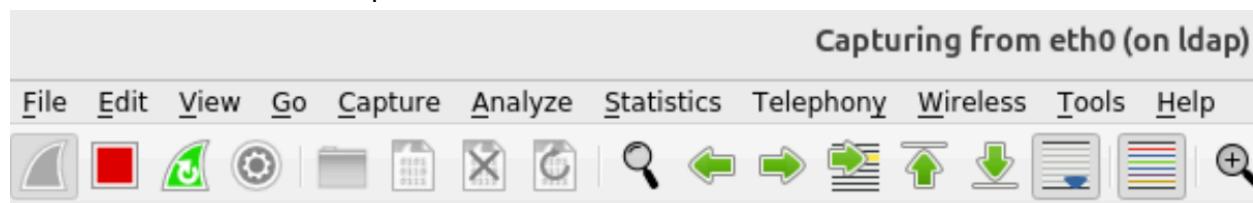
```

systemd-network:x:102:103:systemd Network Management,,,:/
/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/system
d:/usr/sbin/nologin
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin
syslog:x:105:106::/home/syslog:/usr/sbin/nologin
tcpdump:x:106:108::/nonexistent:/usr/sbin/nologin
sshd:x:107:65534::/run/sshd:/usr/sbin/nologin
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/no
login
admin:x:1000:1000::/home/admin:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbi
n/nologin
mike@osboxes1: /etc$ █

```

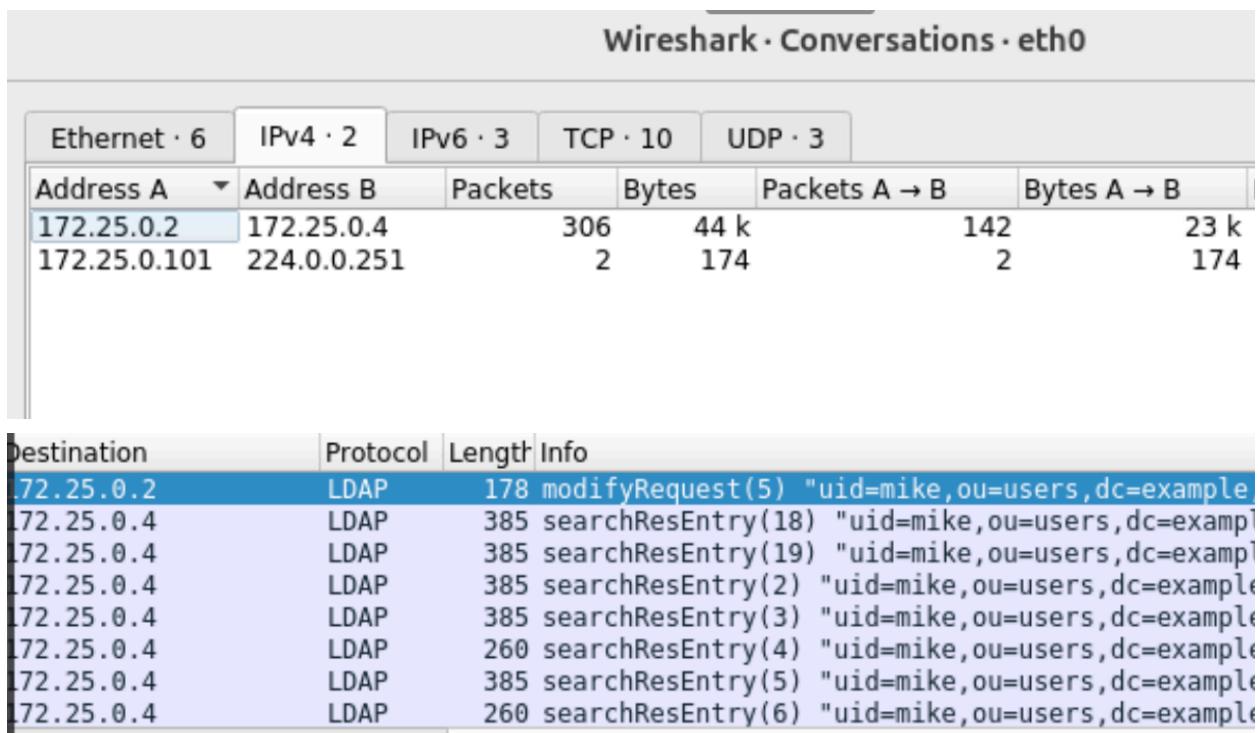
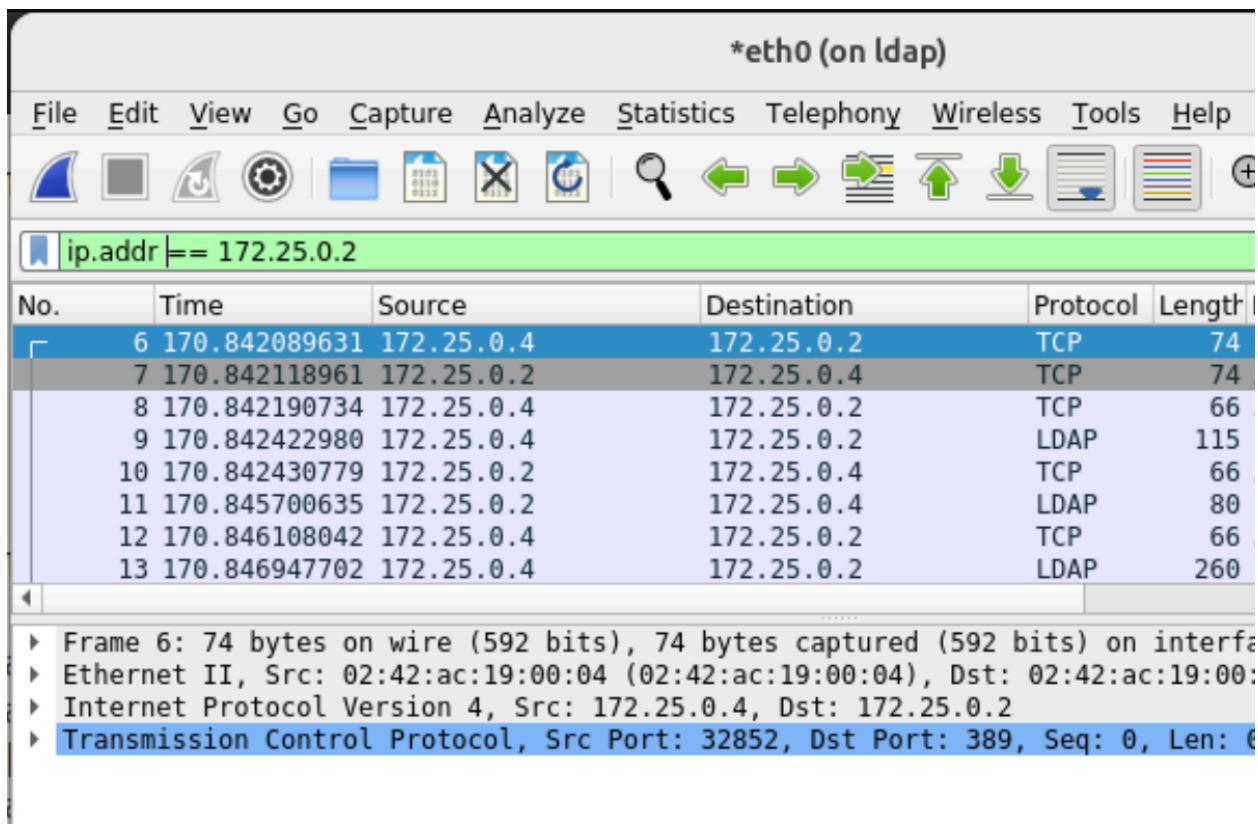
Yes, there are entries in the passwd file

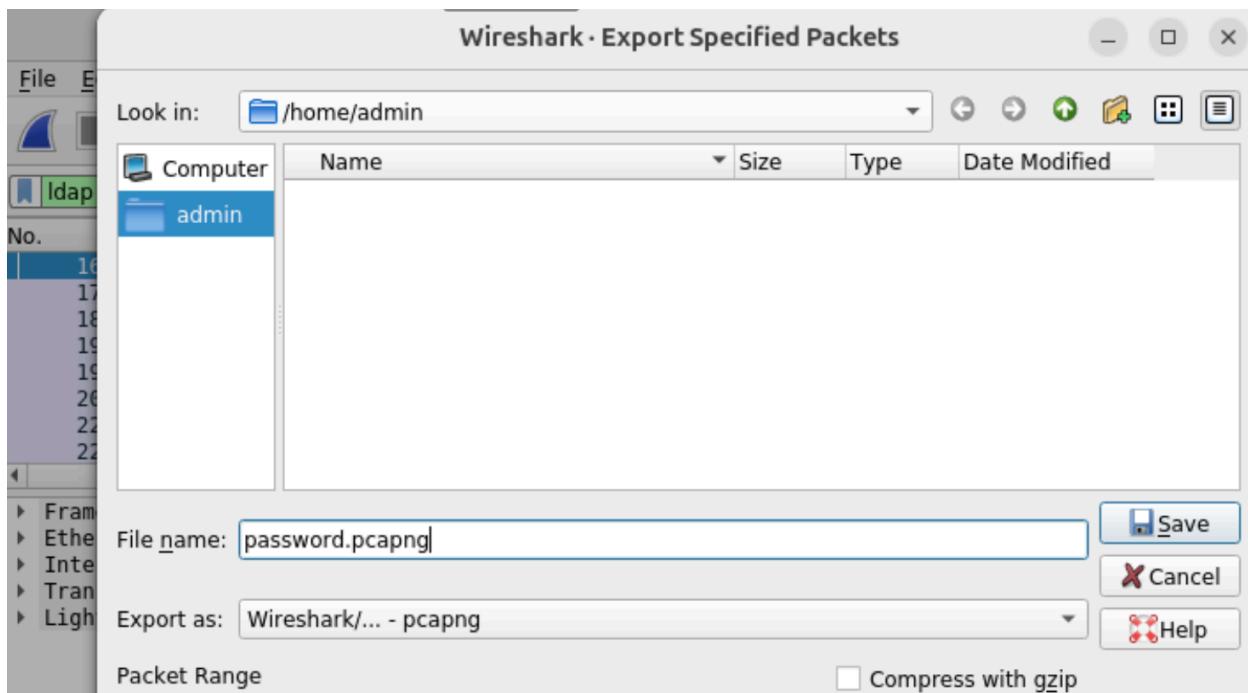
Capturing from eth0 (on ldap)



The screenshot shows the Wireshark interface with the title "Capturing from eth0 (on ldap)". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, search, and navigation. A search bar contains the placeholder "Apply a display filter ... <Ctrl-/>". The main window displays a table of network captures:

No.	Time	Source	Destination	Protocol	Length	In
308	478.460174516	172.25.0.4	172.25.0.2	TCP	66	4
309	478.467014358	172.25.0.4	172.25.0.2	TCP	66	4
310	478.467172928	172.25.0.2	172.25.0.4	TCP	66	3
311	478.467230797	172.25.0.4	172.25.0.2	TCP	66	4
312	483.764535260	02:42:ac:19:00:02	02:42:ac:19:00:04	ARP	42	W
313	483.764735901	02:42:ac:19:00:04	02:42:ac:19:00:02	ARP	42	W
314	483.764759337	02:42:ac:19:00:02	02:42:ac:19:00:04	ARP	42	1
315	483.764764239	02:42:ac:19:00:04	02:42:ac:19:00:02	ARP	42	1
316	565.029009237	172.25.0.101	224.0.0.251	MDNS	87	S
317	575.244209035	fe80::42:3fff:fe57::	ff02::fb	MDNS	107	S
318	575.907316414	fe80::ecc3:a0ff:fed::	ff02::fb	MDNS	107	S
319	632.754182028	fe80::ecc3:a0ff:fed::	ff02::2	ICMPv6	70	R





4.3

```
mike@client:~$ ssh mike@server2
```

```
mike@client:~$ ssh mike@server2

The authenticity of host 'server2 (172.25.0.5)' can't be
established.
ECDSA key fingerprint is SHA256:ZtE8xi5Y50aUktZ/XtgjIs1c5
jxYQB84Vq5ofmlgGng.
Are you sure you want to continue connecting (yes/no)? ye
s
Warning: Permanently added 'server2,172.25.0.5' (ECDSA) t
o the list of known hosts.
mike@server2's password:
Permission denied, please try again.
mike@server2's password:
Creating directory '/home/mike'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 6.8.0-35-generic
x86_64)
```

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

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

The password I used to log in was the same as the new password I created for mike's server1 account

4.4

```
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
```

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

```
GNU nano 4.8                               qa.ldif
dn: cn=qa,ou=groups,dc=example,dc=com
objectClass: top
objectClass: posixGroup
gidNumber: 1501
```

```
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:~$
```

GNU nano 4.8	mary.ldif	Modified
dn: uid=mary,ou=users,dc=example,dc=com		
objectClass: top		
objectClass: account		
objectClass: posixAccount		
objectClass: shadowAccount		
cn: mary		
uid: mary		
uidNumber: 16859		
gidNumber: 100		
homeDirectory: /home/mary		
loginShell: /bin/bash		

```
homeDirectory: /home/mary
loginShell: /bin/bash
gecos: mary
userPassword: {crypt}x
shadowLastChange: 0
shadowMax: 0
shadowWarning: 0
```

```
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 password123 -W -D "cn=admin,d  
c=example,dc=com" -x "uid=mary,ou=users,dc=example,dc=com  
"  
Enter LDAP Password:  
admin@ldap:~$ █
```

```
mary@server1's password:  
You are required to change your password immediately (ad  
ministrator enforced)  
Creating directory '/home/mary'.  
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 6.8.0-35-generic  
x86_64)
```

```
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 mary  
passwd: password updated successfully  
Connection to server1 closed.  
mike@client:~$ █
```

```
mike@client:~$ ssh mary@server1
mary@server1's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 6.8.0-35-generic
x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Thu Oct 31 21:51:38 2024 from 172.25.0.3
mary@server1:~$
```

```
mike@client:~$ ssh mary@server2
mary@server2's password:
Creating directory '/home/mary'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 6.8.0-35-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.
```

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:~\$ █