Design of Secure Computer Systems

Lab 10

LDAP

This lab will illustrate the use of LDAP to authenticate users of Linux systems.

Name: Rakshita Mathur

Lab Report-10 LDAP
St#300215340

1. Explore

On the LDAP server, display the LDAP directory content using: **ldapsearch -x | less** and observe the entries in the directory

```
# 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
dc: example

# admin, example.com
dn: cn=admin,dc=example,dc=com
objectClass: simpleSecurityObject
objectClass: organizationalRole
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
:
```

```
mike@client:~$ ssh mike@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)? 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:
You are required to change your password immediately (administrator enforced)
Creating directory '/home/mike'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.15.0-20-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.

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:~$
```

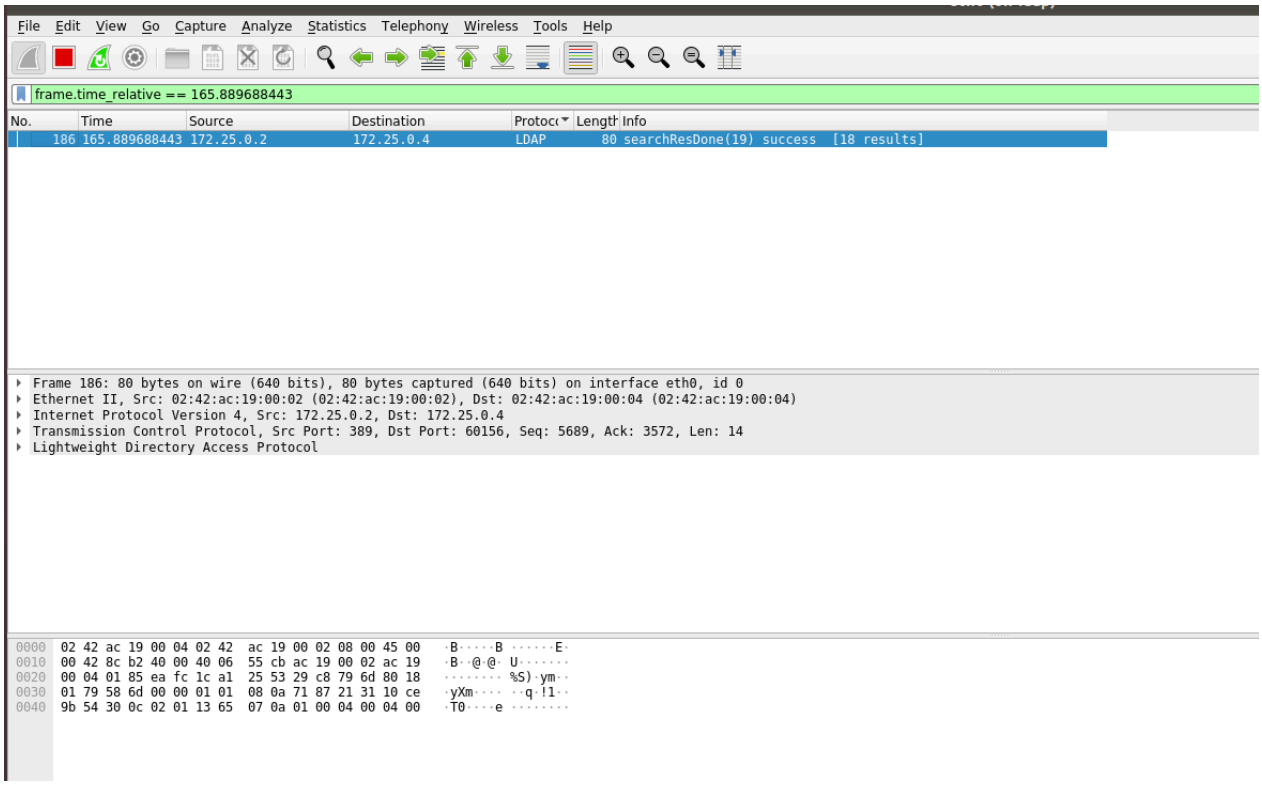
```
mike@client:~$ ssh mike@server1
mike@server1's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Fri Nov 26 17:44:06 2021 from 172.25.0.3
mike@server1:~$
```

```
mike@server1:~$ id
uid=1501(mike) gid=1500(projx) groups=1500(projx)
mike@server1:~$ cat etc/password
cat: etc/password: No such file or directory
mike@server1:~$ id
uid=1501(mike) gid=1500(projx) groups=1500(projx)
mike@server1:~$ cat etc/passwd
cat: etc/passwd: No such file or directory
mike@server1:~$ id
uid=1501(mike) gid=1500(projx) groups=1500(projx)
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
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/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/nologin
admin:x:1000:1000::/home/admin:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mike@server1:~$
```

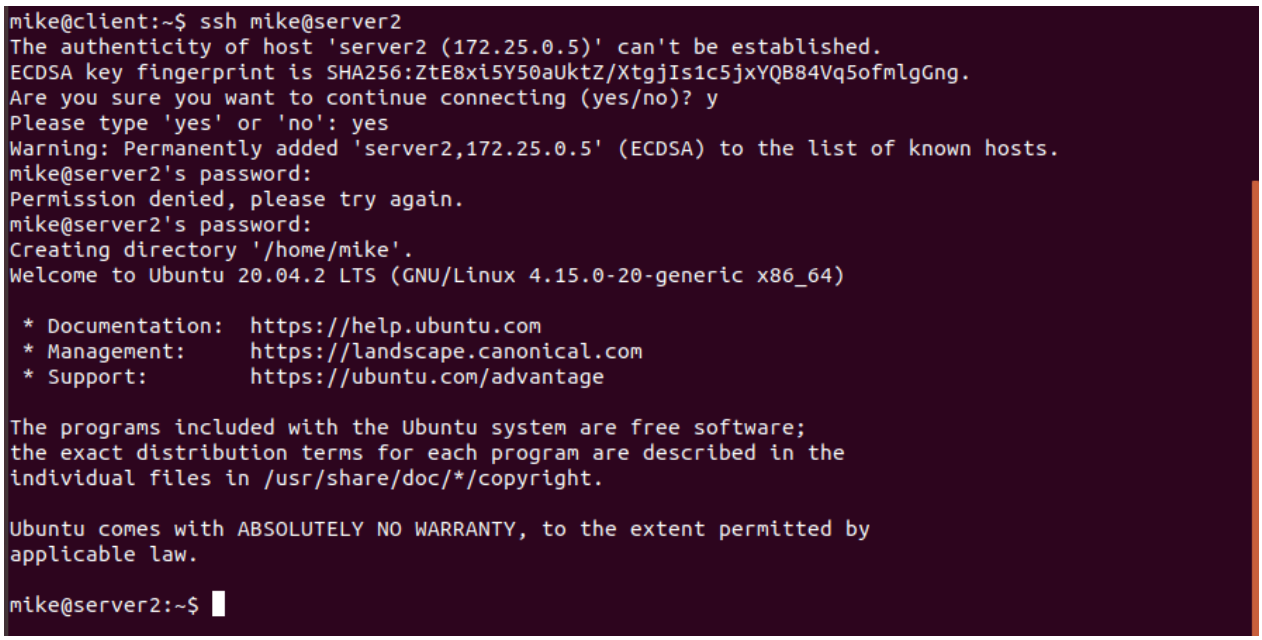
2 View protocol traffic

We apply the filter and save the specified packed as password.pcapng



3. Use the mike credentials to access another server

We used the same password for server 2 as well.



4 Add an LDAP user

```
admin@ldap:~$ ls
[1]+  Done                    wireshark
mike.ldif  password.pcapng  projx.ldif
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
```

```
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:~$ admin@ldap:~$ ldappasswd -s mary123 -W -D "cn=admin,dc=example,dc=com" \
> > -x "uid=mary,ou=users,dc=example,dc=com"
-bash: admin@ldap:~$: command not found
admin@ldap:~$ ldappasswd -s mary123 -W -D "cn=admin,dc=example,dc=com" > -x "uid=mary,ou=users,dc=ex
ample,dc=com"
Enter LDAP Password:
```

SSH marry from mike

```
mike@client:~$ 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)? 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 (administrator enforced)
Creating directory '/home/mary'.
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.15.0-20-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.

WARNING: Your password has expired.
You must change your password now and login again!
Enter login(LDAP) password:
```

```
mike@client:~$ ssh mary@server1
mary@server1's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Thu Nov 25 21:40:24 2021 from 172.25.0.3
groups: cannot find name for group ID 1600
```

Similarly we can ssh marry server 2. Hence same as mike we have made mary.