Access Control and Password Management

IMPORTANT NOTES: Study lecture materials at least 1 hour and attempt task 3 (Users and Access Control) prior to the lab session. Prepared questions will be discussed in the lab session.

1 Overview

The objective of this lab is to understand the access control and password management in UNIX. Optional worksheet will further explore the techniques that an attackers can use to crack the password in UNIX. In this lab, students are required to create users and groups in UNIX. Unix stores hashes of all its accounts' passwords in a single file i.e. `/etc/passwd` on old systems and `/etc/shadow` on new ones. In the optional worksheet, students can further explore `set-UID` and crack the passwords by a tool called "John the Ripper" to crack the passwords stored in a file. Students will recover passwords using different techniques.

2 Lab Environment

Virtual Machine. Cloud Ubuntu VM.

User Accounts Information. `crack-these.txt` is in the `/srv/fit2093files/fit2093lab/` folder for the lab optional worksheet.

3 Lab Task: Users and Access Control

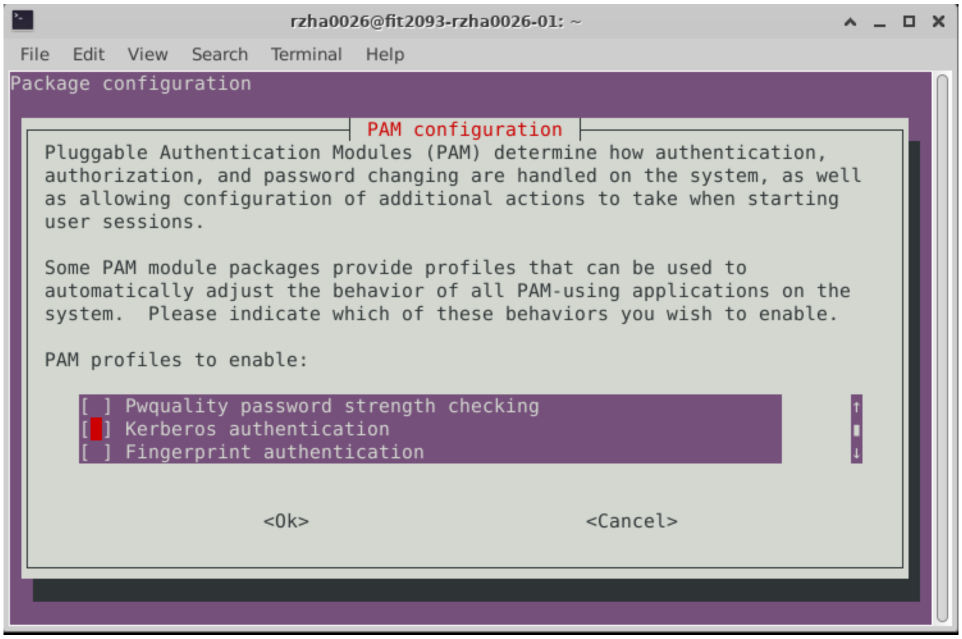
`adduser`	add a user to the system
`addgroup`	add a user group to the system
`usermod`	modify a user account
`su` [username]	change user ID or become superuser
`passwd`	change user password
`chmod`	change file mode bits

Table 1: User manipulation and access control commands

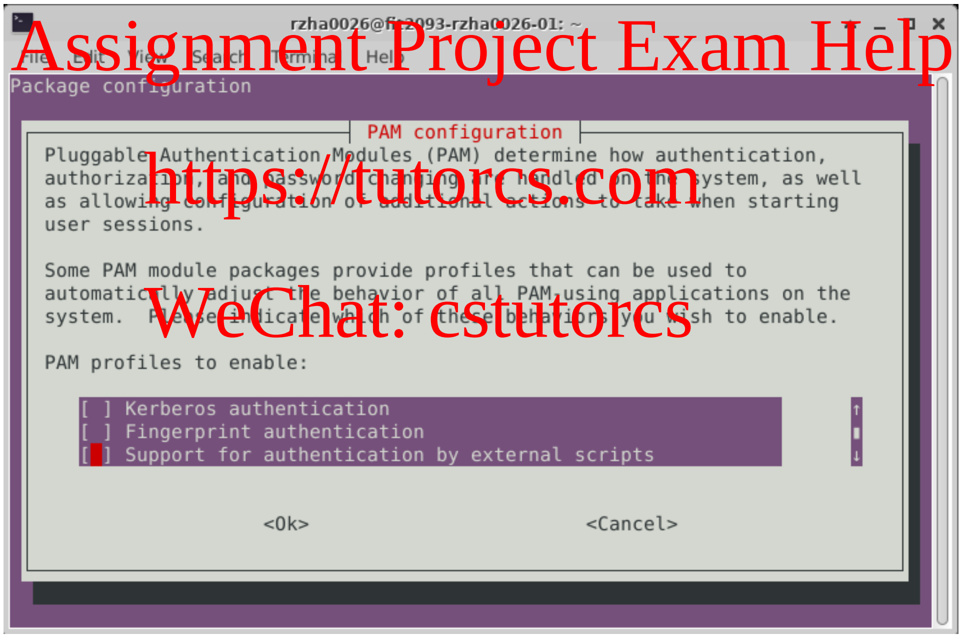
1. Create a new user account for one of your group members and give it a default login password. Add the user to the `sudo` group. Create a new user group named `fitstudents` and add the user to the group. Use the terminal to login to the new user account. Change the password of the user.

   In order to create a new user or change its password, we need to temporarily disable some Pluggable Authentication Modules (PAM) in the cloud VM. Run `sudo pam-auth-update --force` in a terminal and disable the following options:

   - Pwquality password strength checking
   - Kerberos authentication
   - Support for authentication by external scripts


rzha0026@fit2093-rzha0026-01: ~
File Edit View Search Terminal Help

```
Package configuration

                         PAM configuration
 Pluggable Authentication Modules (PAM) determine how authentication,
 authorization, and password changing are handled on the system, as well
 as allowing configuration of additional actions to take when starting
 user sessions.

 Some PAM module packages provide profiles that can be used to
 automatically adjust the behavior of all PAM-using applications on the
 system.  Please indicate which of these behaviors you wish to enable.

 PAM profiles to enable:

    [ ] Pwquality password strength checking
    [ ] Kerberos authentication
    [ ] Fingerprint authentication


              <Ok>                           <Cancel>
```


rzha0026@fit2093-rzha0026-01: ~
File Edit View Search Terminal Help

```
Package configuration

                         PAM configuration
 Pluggable Authentication Modules (PAM) determine how authentication,
 authorization, and password changing are handled on the system, as well
 as allowing configuration of additional actions to take when starting
 user sessions.

 Some PAM module packages provide profiles that can be used to
 automatically adjust the behavior of all PAM-using applications on the
 system.  Please indicate which of these behaviors you wish to enable.

 PAM profiles to enable:

    [ ] Kerberos authentication
    [ ] Fingerprint authentication
    [ ] Support for authentication by external scripts


              <Ok>                           <Cancel>
```

If the Kerberos password is required during any steps in this lab exercise, please re-run the above steps.

Before executing adduser check its manual using `man adduser`. Adding a new user (with username `sierra` and a sudoer):

```
adduser --ingroup sudo sierra
```

You would encounter the following error:

```
adduser: Only root may add a user or group to the system.
```

Use sudo adduser --ingroup sudo sierra to add a new user, you will be asked to enter the password (for fit2093 user):

```
[sudo] password for fit2093:
Adding user `sierra' ...
Adding new user `sierra' (1001) with group `sudo' ...
Creating home directory `/home/sierra' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for sierra
Enter the new value, or press ENTER for the default
Full Name []: Sierra
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
```

To list the current defined groups issue cat /etc/group.

To add a new group run sudo addgroup fitstudents and check the list of groups again using cat /etc/group. Add sierra to fitstudents using sudo adduser sierra fitstudents.

To switch the user from terminal issue su sierra To change the password issue passwd, you will be prompted to enter current password followed by new password (twice):

```
Changing password for sierra.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

2. Avoid other users from listing or writing to the new user's home directory by assigning proper permissions to the user's home directory. However, anyone from the sudo group should be able to access the new user's files if they know the file name and where it is located at. Add your authcate user to the sudo group. Logout and relogin to the cloud VM to make the change of authcate user's group effective, and try this.

   To see the current permissions on home directory of user sierra issue ll or ls -la e.g. ll ~ while logged as sierra or ll /home/sierra, the permission for the folder ./ is for the home directory of the user. The permission for ../ is for the parent directory, what user is the owner of that directory?

```
total 20
drwxr-xr-x 2 sierra sudo 4096 Apr 19 03:59 .
drwxr-xr-x 6 root   root 4096 Apr 19 03:59 ..
-rw-r--r-- 1 sierra sudo  220 Apr 19 03:59 .bash_logout
-rw-r--r-- 1 sierra sudo 3771 Apr 19 03:59 .bashrc
-rw-r--r-- 1 sierra sudo  807 Apr 19 03:59 .profile
```

Change the directory to home directory `cd ~` (for the user `sierra`) Check the current directory using `pwd` command, you should see `/home/sierra`

Create a new file in home directory using `echo "Say the year is the year of the phoenix..." > merwin.txt` and check the permission on the file using `ll ~`

```
total 36
drwxr-xr-x 2 sierra sudo 4096 Apr 19 03:59 .
drwxr-xr-x 6 root   root 4096 Apr 19 03:59 ..
-rw-r--r-- 1 sierra sudo  220 Apr 19 03:59 .bash_logout
-rw-r--r-- 1 sierra sudo 3771 Apr 19 03:59 .bashrc
drwxr-xr-x 4 sierra sudo 4096 Apr 19 04:01 .cache
drwxr-xr-x 4 sierra sudo 4096 Apr 19 04:01 .config
drwxr-xr-x 3 sierra sudo 4096 Apr 19 04:01 .local
-rw-r--r-- 1 sierra sudo   12 Apr 19 04:01 mervin.txt
-rw-r--r-- 1 sierra sudo  807 Apr 19 03:59 .profile
```

Change the permission on home directory issue `chmod 710 /home/sierra`, check the man page of `chmod` command and check the permissions again.

```
total 36
drwx--x--- 5 sierra sudo 4096 Apr 19 04:01 .
drwxr-xr-x 6 root   root 4096 Apr 19 03:59 ..
-rw-r--r-- 1 sierra sudo  220 Apr 19 03:59 .bash_logout
-rw-r--r-- 1 sierra sudo 3771 Apr 19 03:59 .bashrc
drwxr-xr-x 4 sierra sudo 4096 Apr 19 04:01 .cache
drwxr-xr-x 4 sierra sudo 4096 Apr 19 04:01 .config
drwxr-xr-x 3 sierra sudo 4096 Apr 19 04:01 .local
-rw-r--r-- 1 sierra sudo   12 Apr 19 04:01 mervin.txt
-rw-r--r-- 1 sierra sudo  807 Apr 19 03:59 .profile
```

Change the permission on the file so it is only read only for the group using `chmod 740 ~/merwin.txt`, and check the permissions again.

```
drwx--x--- 5 sierra sudo 4096 Apr 19 04:01 .
drwxr-xr-x 6 root   root 4096 Apr 19 03:59 ..
-rw-r--r-- 1 sierra sudo  220 Apr 19 03:59 .bash_logout
-rw-r--r-- 1 sierra sudo 3771 Apr 19 03:59 .bashrc
drwxr-xr-x 4 sierra sudo 4096 Apr 19 04:01 .cache
drwxr-xr-x 4 sierra sudo 4096 Apr 19 04:01 .config
drwxr-xr-x 3 sierra sudo 4096 Apr 19 04:01 .local
-rwxr----- 1 sierra sudo   12 Apr 19 04:01 mervin.txt
-rw-r--r-- 1 sierra sudo  807 Apr 19 03:59 .profile
```

Check the group owner of the newly created file. Switch user back to your authcate user. Run `sudo adduser [authcate] sudo` to add your authcate user to the sudo group. Logout and relogin to the cloud VM. Can you list the content of `/home/sierra`? What if the directory permission was 700 instead of 710, try this.

4 Understanding UNIX password handling

Files shadow and passwd contain user's accounts information, shadow has more restrictive permissions than the passwd file. Run following commands and examine both files, note the permission restrictions and compare the contents of the files. Why do you think shadow file is more restricted than passwd?

```
% ls -l /etc/passwd
% ls -l /etc/shadow
% sudo cat /etc/passwd
% sudo cat /etc/shadow
```

In shadow file, find your user name and hashed password, an example is shown below

```
    ahsan:$6$ViV1fAdR$7J7WsQhS7DpqPqGQQtYqnoLsOm4J0Ixd0WLnU0EN5
jywHCsdhk2qAEgfWdUOso4Hy0VElMsZklDeZlGN3ZG.Q1:16579:0:99999:7:::
```

We are looking for hash of the password, which is second field.

```
    $6$ViV1fAdR$7J7WsQhS7DpqPqGQQtYqnoLsOm4J0Ixd0WLnU0EN5jywHCsdhk2qAEg
fWdUOso4Hy0VElMsZklDeZlGN3ZG
```

1. The first field (numerical number) indicates the type of hashing algorithm used

   $1 = MD5
   $2 = Blowfish
   $2a = eksblowfish
   $5 = SHA-256
   $6 = SHA-512

2. The second field is the salt value

   The salt is used to ensure that users with the same password will most likely not have the same hashed password, and it also strengthen the password.

3. The last field is the hash value of salt + user password

To complete this task: identify number of users in your system (you can add more users with adduser command), what hashing algorithms they are using and what are hashed salt and password values.
To see the defined users we can issue `cat /etc/passwd`, the output may look as follows:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
```

```
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
messagebus:x:102:105::/var/run/dbus:/bin/false
colord:x:103:108:colord colour management daemon,,,:/var/lib/colord:/bin/false
lightdm:x:104:111:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:105:114::/nonexistent:/bin/false
avahi-autoipd:x:106:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:107:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
usbmux:x:108:46:usbmux daemon,,,:/home/usbmux:/bin/false
kernoops:x:109:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:110:119:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:111:122:RealtimeKit,,,:/proc:/bin/false
speech-dispatcher:x:112:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
hplip:x:113:7:HPLIP system user,,,:/var/run/hplip:/bin/false
saned:x:114:123::/home/saned:/bin/false
seed:x:1000:1000:Seed,,,:/home/seed:/bin/bash
mysql:x:115:125:MySQL Server,,,:/nonexistent:/bin/false
bind:x:116:126::/var/cache/bind:/bin/false
snort:x:117:127:Snort IDS:/var/log/snort:/bin/false
ftp:x:118:128:ftp daemon,,,:/srv/ftp:/bin/false
telnetd:x:119:129::/nonexistent:/bin/false
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
sshd:x:120:65534::/var/run/sshd:/usr/sbin/nologin
sierra:x:1001:27:Sierra,,,:/home/sierra:/bin/bash
```

To see the shadow file, `cat /etc/shadow` which will result in an error, hence `sudo cat /etc/shadow` and the output may look as follows:

```
root:$6$012BPz.K$fbPkT6H6Db4/B8cLWbQI1cFjn0R25yqtqrSrFeWfCgybQWWnwR4ks/.rjqyM7Xwh/pDyc5U
1BWOzkWh7T9ZGu.:15933:0:99999:7:::
daemon:*:15749:0:99999:7:::
bin:*:15749:0:99999:7:::
sys:*:15749:0:99999:7:::
sync:*:15749:0:99999:7:::
games:*:15749:0:99999:7:::
man:*:15749:0:99999:7:::
lp:*:15749:0:99999:7:::
mail:*:15749:0:99999:7:::
news:*:15749:0:99999:7:::
uucp:*:15749:0:99999:7:::
proxy:*:15749:0:99999:7:::
www-data:*:15749:0:99999:7:::
backup:*:15749:0:99999:7:::
list:*:15749:0:99999:7:::
irc:*:15749:0:99999:7:::
gnats:*:15749:0:99999:7:::
nobody:*:15749:0:99999:7:::
libuuid:!:15749:0:99999:7:::
syslog:*:15749:0:99999:7:::
messagebus:*:15749:0:99999:7:::
colord:*:15749:0:99999:7:::
```

```
lightdm:*:15749:0:99999:7:::
whoopsie:*:15749:0:99999:7:::
avahi-autoipd:*:15749:0:99999:7:::
avahi:*:15749:0:99999:7:::
usbmux:*:15749:0:99999:7:::
kernoops:*:15749:0:99999:7:::
pulse:*:15749:0:99999:7:::
rtkit:*:15749:0:99999:7:::
speech-dispatcher:!:15749:0:99999:7:::
hplip:*:15749:0:99999:7:::
saned:*:15749:0:99999:7:::
seed:$6$OqXAiWQA$AIjctTUkHMECipE8EiAAJh76YZgrvadHKmWs3hQ3BU8vCC1bSVv4NhGWw2FsZ01Li
Zw0SL6Gc/p8Plw7ShkZR0:15933:0:99999:7:::
mysql:!:15931:0:99999:7:::
bind:*:15931:0:99999:7:::
snort:*:15931:0:99999:7:::
ftp:*:15931:0:99999:7:::
telnetd:*:15931:0:99999:7:::
vboxadd:!:15937::::::
sshd:*:16080:0:99999:7:::
sierra:$6$pHYzCBhY$mDgqcnzd33W6Pea/lOmmaS61W9hbdlC4Dqa9qzFUvTAFxpvnqWfrn9OSRMdoHZ7KAVSu
Ezcr7hjlmXGPBy.uT/:17594:0:99999:7:::
```

For the user we created in previous lab (in this case sierra) the hashing algorithm is SHA-512, we can use the command `mkpasswd` to generate the password as in shadow file. Try `mkpasswd --help` to see the options.

```
Usage: mkpasswd [OPTIONS]... [PASSWORD [SALT]]
Crypts the PASSWORD using crypt(3).

      -m, --method=TYPE     select method TYPE
      -5                    like --method=md5
      -S, --salt=SALT       use the specified SALT
      -R, --rounds=NUMBER   use the specified NUMBER of rounds
      -P, --password-fd=NUM read the password from file descriptor NUM
                            instead of /dev/tty
      -s, --stdin           like --password-fd=0
      -h, --help            display this help and exit
      -V, --version         output version information and exit

If PASSWORD is missing then it is asked interactively.
If no SALT is specified, a random one is generated.
If TYPE is 'help', available methods are printed.
```

To regenerate the password for user sierra we can use `mkpasswd -m sha-512 -S pHYzCBhY` then enter the password you chose for created user when prompted

```
Password:
```

The output (for the password I have used) is as follows:

```
$6$pHYzCBhY$mDgqcnzd33W6Pea/lOmmaS61W9hbdlC4Dqa9qzFUvTAFxpvnqWfrn9OSRMdoHZ7KAVSu
Ezcr7hjlmXGPBy.uT/
```

One of the options provided is the number of rounds (`-R` or `--rounds=NUMBER`) which is used to increase the difficulty level of brute-force or dictionary attack.