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

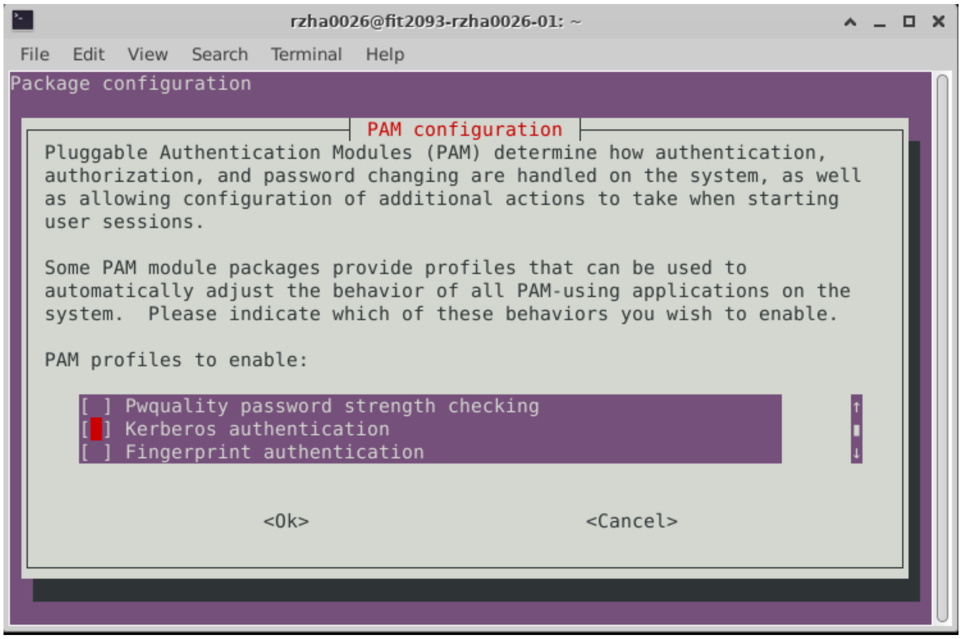
Table 1: User manipulation and access control commands

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:

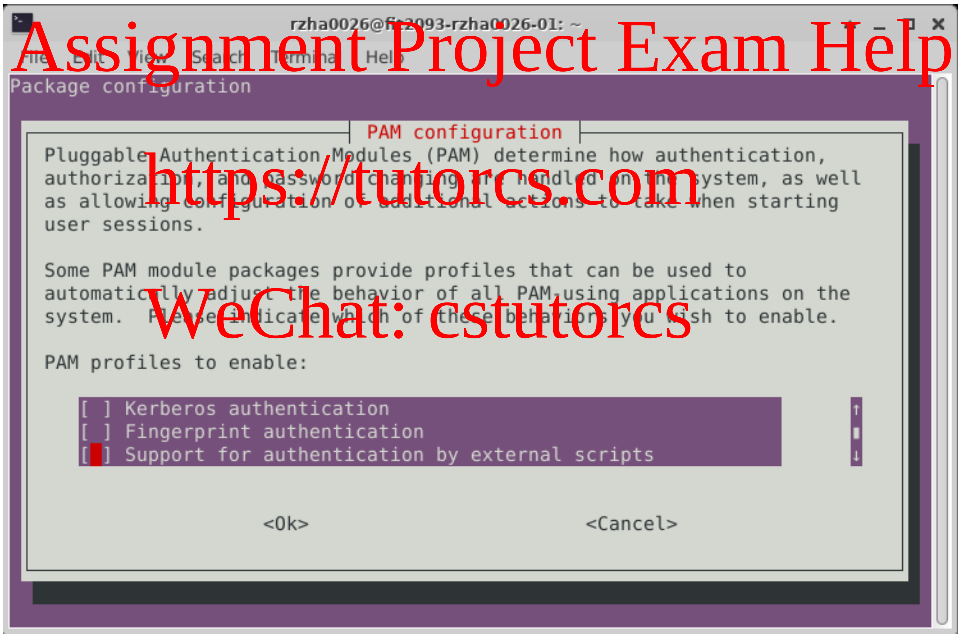
   - Pwquality password strength checking
   - Kerberos authentication
   - Support for authentication by external scripts

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



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>
```

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.

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.