COSC 3364 – Principles of Cybersecurity
Lab 06
Discretionary Access Control

Groups

What Are Groups Used For?

- Being a member of a group allows special access to system resources

- Group membership can also be used to prevent access to system resources

Primary and Secondary Groups

- *Primary group*: Main group user belongs to

- *Secondary groups*: Other groups that user belongs to

Getting a User's Group Information

- Use the `id` command to see what groups a user belongs to

  - Interpreting the results:

    - uid=1002(student): User ID and user name

    - gid=1002(student): Primary user group ID and group name

    - groups=1002(student,60(games),1001(ocs): Secondary group IDs and group names

- Use the group command to list all the groups the user is a member of

  - The primary group is always listed first

Making Changes to Groups

- Change group ownership of a file to another group: `chgrp`

  - Example: `chgrp games sample.txt`

Modifying Group Information

- /etc/passwd

  - Defines the user's primary group membership

  - Uses the GID of the group

- /etc/group

  - Stores information about each group, including group name, GID, and secondary user membership

- /etc/gshadow

❑ Stores additional information about the group, including group administrators and the group password
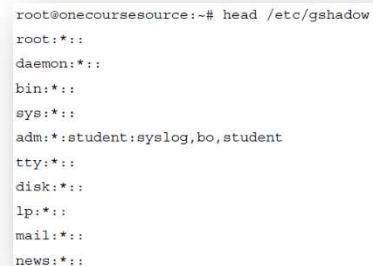
Special Groups

- Have GID values under 1000

- root: system administrator only

- adm: users who can access files related to system monitoring such as log files

- lp, tty, mail, cdrom: used by the OS for background processes to access files

- sudo (super user do): used with the sudo command

User Private Groups

- Each user has his or her own private group

- This group is usually their primary group

The /etc/gshadow File

- Contains group information

- Viewable only by the root user

- Each line describes one group

- Each line is separated into fields of data using : as the field separator

```
root@onecoursesource:~# head /etc/gshadow
root:*::
daemon:*::
bin:*::
sys:*::
adm:*:student:syslog,bo,student
tty:*::
disk:*::
lp:*::
mail:*::
news:*::
```

Creating and Modifying Groups

- Creating groups

  ❑ groupadd command

  ❑ Example: groupadd -g 5000 payroll

  ❑ The -g option assigns the GID to the group (in this case 5000)

- Modifying groups

  ❑ groupmod command

  ❑ Example: groupmod -n payables payroll to change the name of the group from payables to payroll

Deleting Groups

- Use the groupdel command

- First, search the filesystem for all files owned by the group and change their ownerships to another group
- If this step isn't taken, the files owned by the deleted group end up just being owned by the GID of the group, which makes the group permission worthless

Adding Users to Groups

- Use the `usermod` command with the `-G` option
  - ❑ Example: `usermod -G adm student`
  - ❑ Warning: this option will override existing group membership
- To add a user to a group while keeping the current group membership, add the `-a` option
  - ❑ Example: `usermod -G adm -a student`

Group Administrators

- To allow a user to manage a group, add them as a group administrator with the `-A` option of the `gpasswd` command
  - ❑ Example: `gpasswd -A student games`
- Then the user can add users to the group with the `-a` option
  - ❑ Example: `gpasswd -a bo games`
- To remove a user, use the `-d` option
  - ❑ Example: `gpasswd -d bo games`

Users

Importance of User Accounts

- Granting system access
- Securing files and directories
- Security processes
- Additional privileges
- Additional authentication

User Account Information Storage

- Local user account information
  - ❑ /etc/passwd: primary account data

- /etc/shadow: passwords and related data

- /etc/group: group account data

- /etc/gshadow: group account data

- User accounts can also be provided by network servers

The /etc/passwd File

- Despite its name, doesn't contain password information

- This file is not usually manually modified; commands such as `useradd`, `userdel`, and `usermod` change its contents

- Each line describes one group

- Each line contains fields of data with a `:` as a field separator

- Example line: `root:x:0:0:root:/root:/bin/bash`

- Example line: `root:x:0:0:root:/root:/bin/bash`

  - root is the user name

  - x is the password placeholder

  - 0 represents the UID

  - 0 represents the user's primary group

  - root is a comment field

  - /root is the user's home directory

  - /bin/bash is the user's login shell

Special User Accounts

- Default accounts, typically with UID values under 1000

- Some default accounts are daemon accounts, used by daemon-based software

- Other accounts provide features to the OS, such as the nobody account

- Some accounts are created when you add new software

- Administrators should be aware of default accounts and their security features or threats

Default User Account Examples

- root: The system administrator account

- syslog: used by the system logging daemon to access files

- **lp**: one of many users (including mysql, mail, postfix, and dovecot) used by the OS to provide access to specific files by daemons

- **bind**: used by the software that provides DNS functions

The /etc/shadow File

- Contains password data

- Viewable only by the root user

- Each line describes one user's account's password information

- Each line is separated into fields with a **:** as a field separator
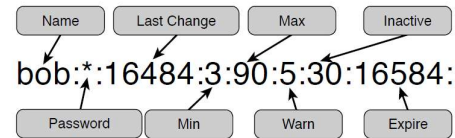
Managing User

- Creating users

  - ❑ Use the `useradd` command

  - ❑ Example: `useradd timmy`

  - ❑ `-u` option can assign a UID to the user

  - ❑ New user's account is locked by default

- **Setting the account password**

  - ❑ Use the `passwd` command

  - ❑ Example: `passwd timmy`

  - ❑ You are prompted to enter the new password

Modifying Users

- Use the `usermod` command

- Use options to specify the change to make

-m	Change the min days field.
-M	Change the max days field.
-d	Change the "date since last password change" field (YYYY-MM-DD format).
-I	Change the inactive field.
-E	Change the expiration date field (YYYY-MM-DD format).
-W	Change the warning days field.

Restricted Shell Accounts

- Add the -s option to the `useradd` command and provide an argument of /bin/rbash

  Example: `useradd -m -s /bin/rbash limited`

- Properties of restricted accounts

  - ❑ Cannot change directories with the `cd` command

  - ❑ Cannot change the values of these variables: SHELL, PATH, ENV, and BASH_ENV

  - ❑ Cannot run any command that have a pathname that starts with the **/** character

❑ Cannot redirect output to a file

Using su

■ Switches to another user account

❑ Example: `su - student`

■ Opens a new shell in which the identity has been switched

■ The `-` option enables you to switch as if you were logging in directly, so that the user's initialization files are executed

■ To use su you must be the root user or you must have the password for the account being switched to

■ Use the exit command to close the shell

Using sudo

■ Executes specific tasks as another user without actually switching to that account

❑ Example: `sudo apt-get install joe`

■ Access is configured in /etc/sudoers

■ /etc/sudoers should not be modified directly; use the `visudo` command

Pluggable Authentication Modules (PAM)

■ Set of libraries that is called by authentication-based software

■ Features

❑ Can limit access by time or date

❑ Can limit system resource utilization after the user logs in

❑ Can be applied to specific login commands

❑ Can create additional log entries for specific login events

■ Primary configuration file, /etc/pam.conf, is rarely used

■ Each authentication-based program has a separate configuration file under the /etc/pam.d directory

Category	Description
account	Used to verify that a user account has the rights to use a service. This could include checking if a user can log in via the network or at a specific time of day.
auth	Used to authenticate (that is, verify) that the user is who they claim to be, normally by having the user provide a password for the account that they are attempting to use.
password	Used to update authentication methods, such as providing a new password for an account.
session	Used to perform actions prior to and after a service has been provided to a user. For example, this could be used to limit a user account access.
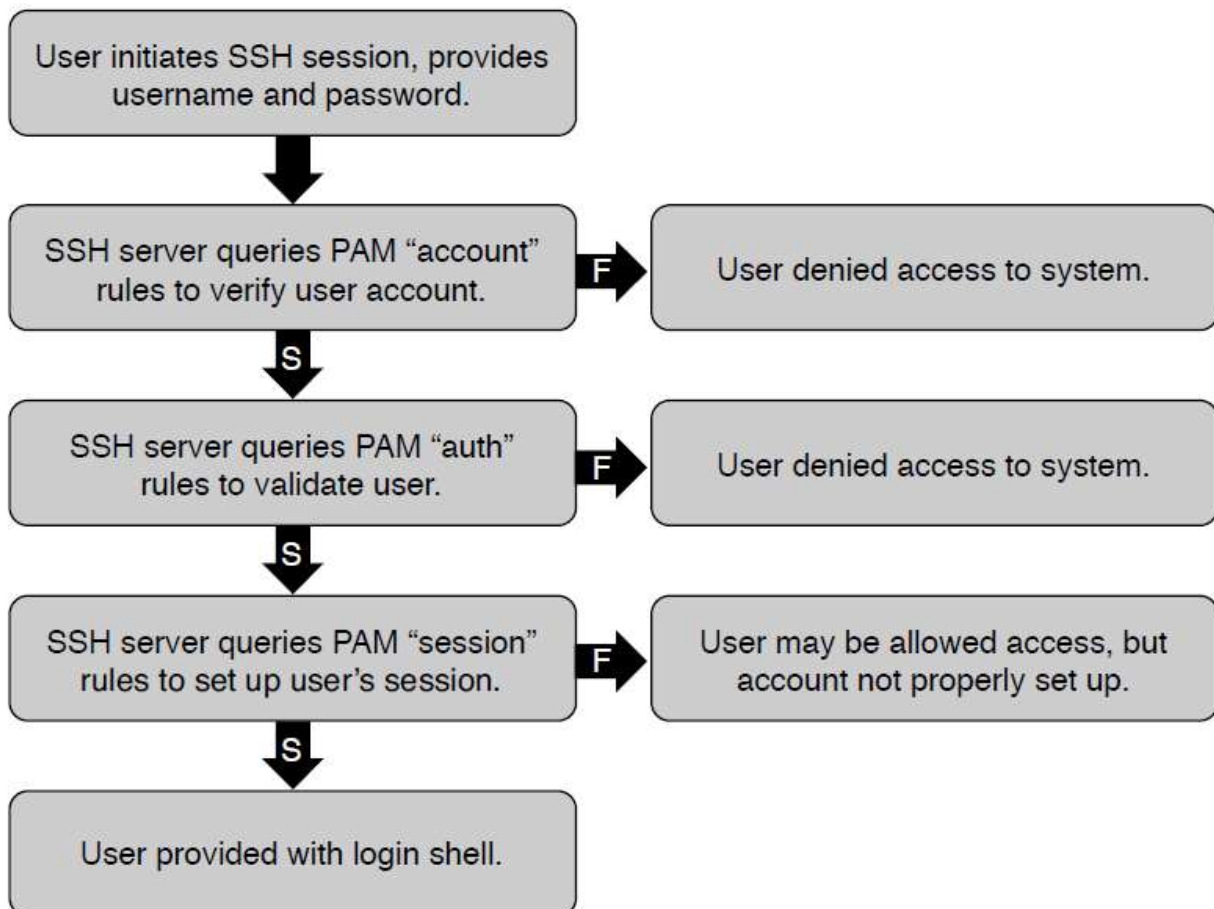
Control	Description
requisite	If the corresponding module returns a "failure," the rest of the category's modules are not executed and the category returns an overall result of "failure."
required	If the corresponding module returns a "failure," the overall result of the category will be "failure." However, additional modules will be executed (their return values are not used for the overall return value of the category).
sufficient	If the corresponding module returns a "success," the overall result of the category will be "success," without any additional modules executed. If, however, a previous module returned "failure" when a "required" control was specified, then this result is ignored.
optional	The outcome of the corresponding module is not relevant unless it is the only module for the service. Typically this value is used for performing an action during the authentication process that does not have to be tested for success or failure.

Module	Description
pam_access	Used for "location-based" access control
pam_cracklib	Used to modify password policies
pam_deny	Always returns a "failure" result
pam_env	Used to set environment variables
pam_mkhomedir	Used to create home directories
pam_nologin	Used to determine if a user's login shell is **/etc/nologin**
pam_tally	Used to count login attempts
pam_time	Used for "time-based" access control
pam_timestamp	Used to control access based on last login
pam_unix	Used for standard user authentication

Tasks

Provide screenshots where * is indicated.

1. **Explore Group and User Information:**
   a. Display default user's information*

   ```
   labuser1@ML-RefVm-535928:~/Documents$ id
   uid=1000(labuser1) gid=1000(labuser1) groups=1000(labuser1),4(adm),20(dialout),24(cdro
   m),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),119(netdev),120(lxd)
   labuser1@ML-RefVm-535928:~/Documents$
   ```

   b. Display contents of passw

   ```
   labuser1@ML-RefVm-535928:/$ 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:/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
   systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
   systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
   messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
   systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nolo
   gin
   syslog:x:104:111::/home/syslog:/usr/sbin/nologin
   _apt:x:105:65534::/nonexistent:/usr/sbin/nologin
   tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
   uuidd:x:107:113::/run/uuidd:/usr/sbin/nologin
   tcpdump:x:108:114::/nonexistent:/usr/sbin/nologin
   sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
   pollinate:x:110:1::/var/cache/pollinate:/bin/false
   landscape:x:111:116::/var/lib/landscape:/usr/sbin/nologin
   fwupd-refresh:x:112:117:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
   _chrony:x:113:122:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin
   labuser1:x:1000:1000:Ubuntu:/home/labuser1:/bin/bash
   lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
   rtkit:x:114:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
   usbmux:x:115:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
   avahi:x:116:124:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
   saned:x:117:126::/var/lib/saned:/usr/sbin/nologin
   colord:x:118:127:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
   pulse:x:119:128:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
   xrdp:x:120:131::/run/xrdp:/usr/sbin/nologin
   labuser1@ML-RefVm-535928:/$
   ```

   c. Display contents of shadow*

```
labuser1@ML-RefVm-535928:/etc$ sudo cat shadow
[sudo] password for labuser1:
root:*:19371:0:99999:7:::
daemon:*:19371:0:99999:7:::
bin:*:19371:0:99999:7:::
sys:*:19371:0:99999:7:::
sync:*:19371:0:99999:7:::
games:*:19371:0:99999:7:::
man:*:19371:0:99999:7:::
lp:*:19371:0:99999:7:::
mail:*:19371:0:99999:7:::
news:*:19371:0:99999:7:::
uucp:*:19371:0:99999:7:::
proxy:*:19371:0:99999:7:::
www-data:*:19371:0:99999:7:::
backup:*:19371:0:99999:7:::
list:*:19371:0:99999:7:::
irc:*:19371:0:99999:7:::
gnats:*:19371:0:99999:7:::
nobody:*:19371:0:99999:7:::
systemd-network:*:19371:0:99999:7:::
systemd-resolve:*:19371:0:99999:7:::
messagebus:*:19371:0:99999:7:::
systemd-timesync:*:19371:0:99999:7:::
syslog:*:19371:0:99999:7:::
_apt:*:19371:0:99999:7:::
tss:*:19371:0:99999:7:::
uuidd:*:19371:0:99999:7:::
tcpdump:*:19371:0:99999:7:::
sshd:*:19371:0:99999:7:::
pollinate:*:19371:0:99999:7:::
landscape:*:19371:0:99999:7:::
fwupd-refresh:*:19371:0:99999:7:::
_chrony:*:19371:0:99999:7:::
labuser1:$6$O1NamDP7vt$kZCDz2OEAOGzB32zlMeHiRNZpjUMEcjT4OWglWt.gWW6Vmc5g/2HQ4smErY/Feg
25GD8icnAOqhHPTrW099ME.:19998:0:99999:7:::
lxd:!:19380:::::::
rtkit:*:19380:0:99999:7:::
usbmux:*:19380:0:99999:7:::
avahi:*:19380:0:99999:7:::
saned:*:19380:0:99999:7:::
colord:*:19380:0:99999:7:::
pulse:*:19380:0:99999:7:::
xrdp:!:19380:0:99999:7:::
labuser1@ML-RefVm-535928:/etc$
```

d. Display contents of group*

```
systemd-network:x:102:        news:x:9:
systemd-resolve:x:103:        uucp:x:10:
crontab:x:104:                man:x:12:
messagebus:x:105:             proxy:x:13:
systemd-timesync:x:106:       kmem:x:15:
input:x:107:                  dialout:x:20:labuser1
sgx:x:108:                    fax:x:21:
kvm:x:109:                    voice:x:22:
render:x:110:                 cdrom:x:24:labuser1
syslog:x:111:                 floppy:x:25:labuser1
tss:x:112:                    tape:x:26:
uuidd:x:113:                  sudo:x:27:labuser1
tcpdump:x:114:                audio:x:29:labuser1,pulse    syslog:x:111:
_ssh:x:115:                   dip:x:30:labuser1           tss:x:112:
landscape:x:116:              www-data:x:33:              uuidd:x:113:
fwupd-refresh:x:117:          backup:x:34:                tcpdump:x:114:
admin:x:118:                  operator:x:37:              _ssh:x:115:
netdev:x:119:labuser1         list:x:38:                  landscape:x:116:
lxd:x:120:labuser1            irc:x:39:                   fwupd-refresh:x:117:
sgx_prv:x:121:                src:x:40:                   admin:x:118:
_chrony:x:122:                gnats:x:41:                 netdev:x:119:labuser1
labuser1:x:1000:              shadow:x:42:                lxd:x:120:labuser1
rtkit:x:123:                  utmp:x:43:                  sgx_prv:x:121:
avahi:x:124:                  video:x:44:labuser1         _chrony:x:122:
scanner:x:125:saned           sasl:x:45:                  labuser1:x:1000:
saned:x:126:                  plugdev:x:46:labuser1       rtkit:x:123:
colord:x:127:                 staff:x:50:                 avahi:x:124:
pulse:x:128:                  games:x:60:                 scanner:x:125:saned
pulse-access:x:129:           users:x:100:                saned:x:126:
ssl-cert:x:130:xrdp           nogroup:x:65534:            colord:x:127:
xrdp:x:131:                   systemd-journal:x:101:      pulse:x:128:
root:x:0:                     systemd-network:x:102:      pulse-access:x:129:
daemon:x:1:                   systemd-resolve:x:103:      ssl-cert:x:130:
bin:x:2:                      crontab:x:104:              xrdp:x:131:
sys:x:3:                      messagebus:x:105:
adm:x:4:syslog,labuser1       systemd-timesync:x:106:
tty:x:5:                      input:x:107:
disk:x:6:                     sgx:x:108:
lp:x:7:                       kvm:x:109:
mail:x:8:                     render:x:110:
```

e. Display contents of gshadow*

```
labuser1@ML-RefVm-535928:/etc$ sudo cat gshadow
root:*::
daemon:*::
bin:*::
sys:*::
adm:*::syslog,labuser1
tty:*::
disk:*::
lp:*::
mail:*::
news:*::
uucp:*::
man:*::
proxy:*::
kmem:*::
dialout:*::labuser1
fax:*::
voice:*::
cdrom:*::labuser1
floppy:*::labuser1
tape:*::
sudo:*::labuser1
audio:*::labuser1,pulse
dip:*::labuser1
www-data:*::
backup:*::
operator:*::
list:*::
irc:*::
src:*::
gnats:*::
shadow:*::
utmp:*::
video:*::labuser1
sasl:*::
plugdev:*::labuser1
staff:*::
games:*::
users:*::
nogroup:*::
systemd-journal:!::
systemd-network:!::
systemd-resolve:!::
```

```
systemd-resolve:!::
crontab:!::
messagebus:!::
systemd-timesync:!::
input:!::
sgx:!::
kvm:!::
render:!::
syslog:!::
tss:!::
uuidd:!::
tcpdump:!::
_ssh:!::
landscape:!::
fwupd-refresh:!::
admin:!::
netdev:!::labuser1
lxd:!::labuser1
sgx_prv:!::
_chrony:!::
labuser1:!::
rtkit:!::
avahi:!::
scanner:!::saned
saned:!::
colord:!::
pulse:!::
pulse-access:!::
ssl-cert:!::xrdp
xrdp:!::
labuser1@ML-RefVm-535928:/etc$
```

2. **Alice:**
   a. Create user named **alice** with an ID of 222

```
labuser1@ML-RefVm-535928:/$ sudo adduser --uid 222 alice
Adding user `alice' ...
Adding new group `alice' (222) ...
Adding new user `alice' (222) with group `alice' ...
Creating home directory `/home/alice' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for alice
Enter the new value, or press ENTER for the default
        Full Name []: Alice
        Room Number []: 2
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

b. Set the password of the user account to 'alice'

```
labuser1@ML-RefVm-535928:/$ sudo passwd alice
New password:
BAD PASSWORD: it is based on a dictionary word
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: it is based on a dictionary word
Retype new password:
passwd: password updated successfully
labuser1@ML-RefVm-535928:/$
```

c. Determine the primary group of **alice***

```
labuser1@ML-RefVm-535928:/$ id alice
uid=222(alice) gid=222(alice) groups=222(alice)
labuser1@ML-RefVm-535928:/$
```

d. What is the primary group ID of **alice's** primary group? How was this generated?

```
gid=222(alice)
```
, we decided it when we created the user.

e. Switch to user account **alice**
f. Attempt to create group **analysts**
g. Attempt to create group **analysts** as super user*

```
labuser1@ML-RefVm-535928:/$ su -- alice
Password:
alice@ML-RefVm-535928:/$ groupadd analysts
groupadd: Permission denied.
groupadd: cannot lock /etc/group; try again later.
alice@ML-RefVm-535928:/$ sudo groupadd analysts
[sudo] password for alice:
alice is not in the sudoers file.  This incident will be reported.
alice@ML-RefVm-535928:/$
```

h. Return to default user
i. Display the end of `/var/log/auth.log`
j. Locate incident report*

```
alice@ML-RefVm-535928:/$ exit
exit
labuser1@ML-RefVm-535928:/$ sudo tail /var/log/auth.log
Oct  2 21:57:05 ML-RefVm-535928 sudo: pam_unix(sudo:session): session opened for user
root(uid=0) by (uid=1000)
Oct  2 21:57:18 ML-RefVm-535928 passwd[1667]: pam_cracklib(passwd:chauthtok): pam_get_
authtok_verify returned error: Failed preliminary check by password service
Oct  2 21:57:26 ML-RefVm-535928 passwd[1667]: pam_unix(passwd:chauthtok): password cha
nged for alice
Oct  2 21:57:26 ML-RefVm-535928 sudo: pam_unix(sudo:session): session closed for user
root
Oct  2 22:00:00 ML-RefVm-535928 su: (to alice) labuser1 on pts/0
Oct  2 22:00:00 ML-RefVm-535928 su: pam_unix(su:session): session opened for user alic
e(uid=222) by (uid=1000)
Oct  2 22:01:08 ML-RefVm-535928 sudo:    alice : user NOT in sudoers ; TTY=pts/0 ; PWD
=/ ; USER=root ; COMMAND=/usr/sbin/groupadd analysts
Oct  2 22:02:01 ML-RefVm-535928 su: pam_unix(su:session): session closed for user alic
e
Oct  2 22:02:16 ML-RefVm-535928 sudo: labuser1 : TTY=pts/0 ; PWD=/ ; USER=root ; COMMA
ND=/usr/bin/tail /var/log/auth.log
Oct  2 22:02:16 ML-RefVm-535928 sudo: pam_unix(sudo:session): session opened for user
root(uid=0) by (uid=1000)
labuser1@ML-RefVm-535928:/$ sudo grep -i 'failed' /var/log/auth.log
Oct  2 17:41:08 ML-RefVm-535928 systemd-logind[649]: Failed to restore VT, ignoring: B
ad file descriptor
Oct  2 21:57:18 ML-RefVm-535928 passwd[1667]: pam_cracklib(passwd:chauthtok): pam_get_
authtok_verify returned error: Failed preliminary check by password service
Oct  2 22:02:54 ML-RefVm-535928 sudo: labuser1 : TTY=pts/0 ; PWD=/ ; USER=root ; COMMA
ND=/usr/bin/grep -i failed /var/log/auth.log
labuser1@ML-RefVm-535928:/$
```

3. **Analysts and Agents:**
   a. Create group **analysts** with an ID of 2222
   b. Create group **agents** with an ID of 3333
   c. Add **alice** to group **analysts**
   d. Display group information for **alice***

```
labuser1@ML-RefVm-535928:/$ sudo groupadd --gid 2222 analysts
labuser1@ML-RefVm-535928:/$ sudo groupadd --gid 3333 agents
labuser1@ML-RefVm-535928:/$ sudo usermod -aG analysts alice
labuser1@ML-RefVm-535928:/$ id alice
uid=222(alice) gid=222(alice) groups=222(alice),2222(analysts)
labuser1@ML-RefVm-535928:/$
```

e. Delete user account **alice**
f. Create user account **alice** with an ID of 222 while adding account to **analysts**
g. Display group information for **alice***

```
labuser1@ML-RefVm-535928:/$ sudo deluser --remove-home alice
Looking for files to backup/remove ...
Removing files ...
Removing user `alice' ...
Warning: group `alice' has no more members.
Done.
labuser1@ML-RefVm-535928:/$ sudo adduser --uid 222 --gid 2222 alice
Adding user `alice' ...
Adding new user `alice' (222) with group `analysts' ...
Creating home directory `/home/alice' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: it is based on a dictionary word
Retype new password:
passwd: password updated successfully
Changing the user information for alice
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
labuser1@ML-RefVm-535928:/$ id alice
uid=222(alice) gid=2222(analysts) groups=2222(analysts)
labuser1@ML-RefVm-535928:/$
```

h. What is the primary group of ID of **alice's** primary group? How was this generated?
i. Switch to user account **alice**
j. Attempt to set **alice** as group administrator of **agents***

```
labuser1@ML-RefVm-535928:/$ id alice
uid=222(alice) gid=2222(analysts) groups=2222(analysts)
labuser1@ML-RefVm-535928:/$ su - alice
Password:
alice@ML-RefVm-535928:~$ sudo usermod -aG agents alice
[sudo] password for alice:
alice is not in the sudoers file.  This incident will be reported.
alice@ML-RefVm-535928:~$
```

k. Return to default user
l. Set **alice** as group administrator of **agents**

```
labuser1@ML-RefVm-535928:~/Desktop$ sudo gpasswd -A alice agents
labuser1@ML-RefVm-535928:~/Desktop$ █
```

4. Bob:

a. Create user named **bob** with an ID of 333
b. Set the password of the user account to 'bob'
c. Add **bob** to group **analysts** and set as group administrator
d. Add **bob** to group **agents**
e. Display contents of group*

```
labuser1@ML-RefVm-535928:/$ sudo adduser --uid 333 bob
Adding user `bob' ...
Adding new group `bob' (333) ...
Adding new user `bob' (333) with group `bob' ...
Creating home directory `/home/bob' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: it is WAY too short
BAD PASSWORD: is a palindrome
Retype new password:
passwd: password updated successfully
Changing the user information for bob
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
labuser1@ML-RefVm-535928:/$ sudo usermod -aG analysts bob
labuser1@ML-RefVm-535928:/$ sudo usermod -aG agents bob
labuser1@ML-RefVm-535928:/$ cat /etc/group*
root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog,labuser1
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
```

```
labuser1@ML-RefVm-535928:~/Desktop$ sudo gpasswd -A bob analysts
labuser1@ML-RefVm-535928:~/Desktop$
```

```
ssl-cert:x:130:xrdp
xrdp:x:131:
analysts:x:2222:bob
agents:x:3333:alice
bob:x:333:
labuser1@ML-RefVm-535928:/$ ▌
```

f. Open `/etc/pam.d/common-password` as super user

g. Update password policy to a minimum length of 8 and must contain an uppercase letter, lowercase letter, and a digit* (https://linux.die.net/man/8/pam_cracklib)

```
# here are the per-package modules (the "Primary" block)
minlen=8 ucredit=-1 lcredit=-1 dcredit=-1 difok=3
password        [success=1 default=ignore]      pam_unix.so obscure sha512 use
# here's the fallback if no module succeeds
```

h. Switch to user account **bob**

i. Attempt to set the password of the user account to '`wtpwniwn`'

j. Set the password of the user account to '`Wtpw0912`'*

```
labuser1@ML-RefVm-535928:~/Desktop$ sudo nano /etc/pam.d/common-password
labuser1@ML-RefVm-535928:~/Desktop$ su - bob
Password:
bob@ML-RefVm-535928:~$ passwd
Changing password for bob.
Current password:
New password:
BAD PASSWORD: is too simple
New password:
Retype new password:
passwd: password updated successfully
bob@ML-RefVm-535928:~$
```

k. Return to default user

```
bob@ML-RefVm-535928:~$ exit
logout
labuser1@ML-RefVm-535928:~/Desktop$
```

5. **Carol:**
   a. Create user named **carol** with an ID of 444
   b. Set the password of the user account to 'carol'

```
labuser1@ML-RefVm-535928:~/Desktop$ sudo adduser --uid 444 carol
Adding user `carol' ...
Adding new group `carol' (444) ...
Adding new user `carol' (444) with group `carol' ...
Creating home directory `/home/carol' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
Retype new password:
passwd: password updated successfully
Changing the user information for carol
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
labuser1@ML-RefVm-535928:~/Desktop$
```

   c. Switch to user account **alice**
   d. Delete **bob** from group **agents**
   e. Attempt to add **carol** to group **analysts**
   f. Add **carol** to group **agents***

```
labuser1@ML-RefVm-535928:~/Desktop$ su - alice
Password:
alice@ML-RefVm-535928:~$ sudo deluser bob agents
[sudo] password for alice:
Removing user `bob' from group `agents' ...
Done.
alice@ML-RefVm-535928:~$ usermod -aG analysts carol
usermod: Permission denied.
usermod: cannot lock /etc/passwd; try again later.
alice@ML-RefVm-535928:~$ sudo usermod -aG agents carol
alice@ML-RefVm-535928:~$
```

   g. Return to default user
   h. Display contents of passwd*

```
colord:x:118:127:colord colour management da
pulse:x:119:128:PulseAudio daemon,,,:/run/pu
xrdp:x:120:131::/run/xrdp:/usr/sbin/nologin
alice:x:222:2222:,,,:/home/alice:/bin/bash
bob:x:333:333:,,,:/home/bob:/bin/bash
carol:x:444:444::/home/carol:/bin/bash
labuser1@ML-RefVm-535928:~/Desktop$
```

i. Display contents of group*

```
analysts:x:2222:bob,carol
agents:x:3333:alice
bob:x:333:
carol:x:444:
labuser1@ML-RefVm-535928:~/Desktop$
```

```
labuser1@ML-RefVm-535928:~/Desktop$ sudo gpasswd -d carol analysts
Removing user carol from group analysts
labuser1@ML-RefVm-535928:~/Desktop$ sudo usermod -aG agents bob
```

```
analysts:x:2222:bob,carol
agents:x:3333:alice,carol,bob
bob:x:333:
carol:x:444:
labuser1@ML-RefVm-535928:~/Desktop$
```

For some reason didn't remove carol from analysts.