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

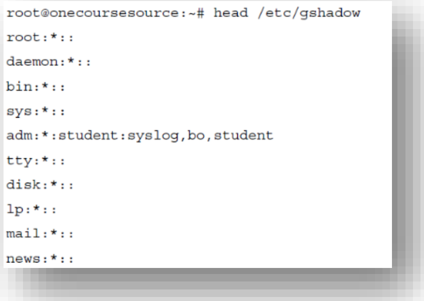
- Have GID values under 1000
- root: system administrator only
- adm: users who can access files related to system monitoring such as log files
- lp, tty, mail, cdrom: used by the OS for background processes to access files
- sudo (super user do): used with the `sudo` command

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

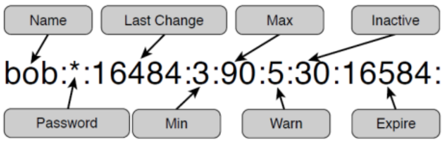
- Default accounts, typically with UID values under 1000
- Some default accounts are daemon accounts, used by daemon-based software
- Other accounts provide features to the OS, such as the nobody account
- Some accounts are created when you add new software
- Administrators should be aware of default 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

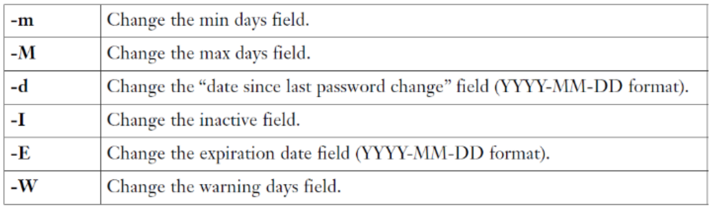


- Contains password data
- Viewable only by the root user
- Each line describes one user's account's password information
- Each line is separated into fields with a **:** as a field separator

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



-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.

- Use the `usermod` command
- Use options to specify the change to make

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

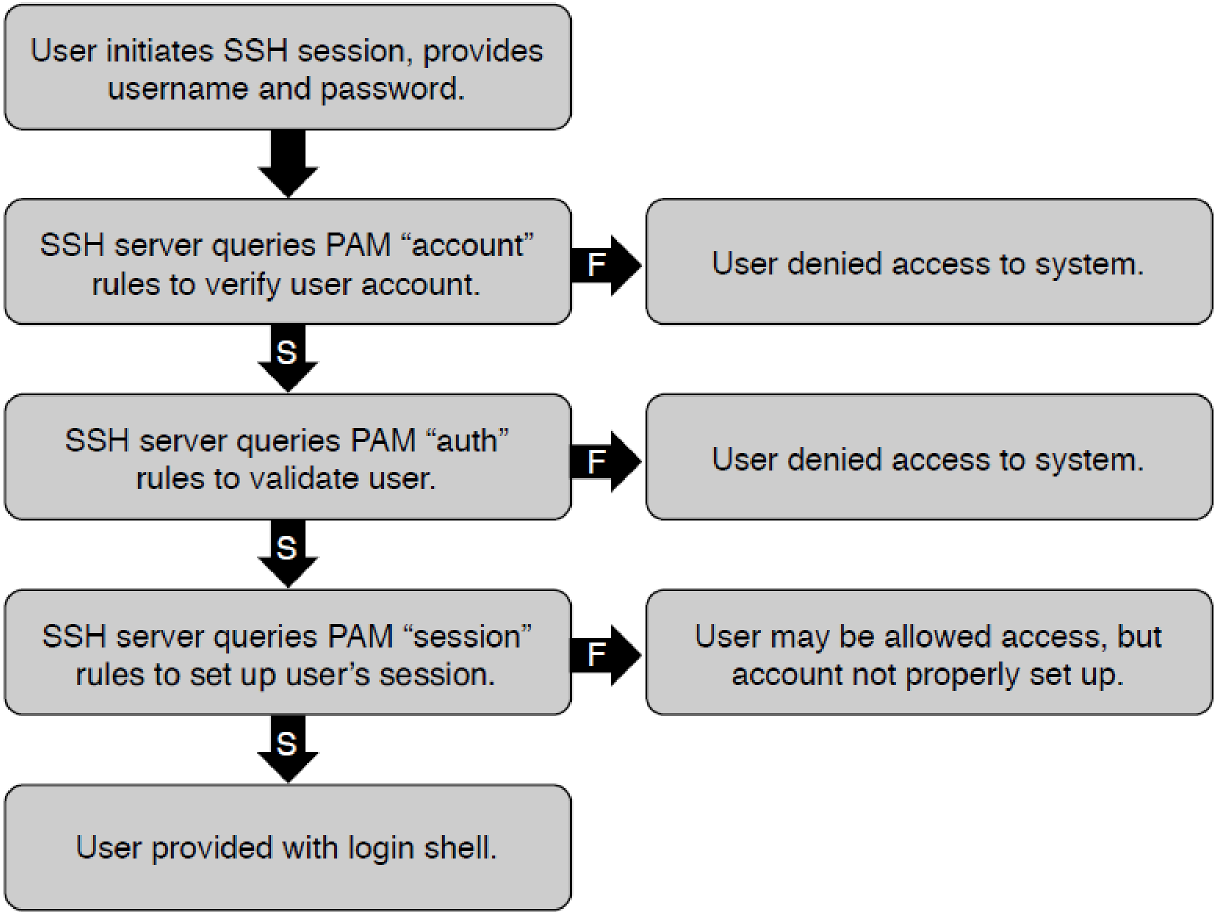
Using sudo

- ■ 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.


User initiates SSH session, provides username and password.
SSH server queries PAM “account” rules to verify user account.
F
User denied access to system.
S
SSH server queries PAM “auth” rules to validate user.
F
User denied access to system.
S
SSH server queries PAM “session” rules to set up user’s session.
F
User may be allowed access, but account not properly set up.
S
User provided with login shell.

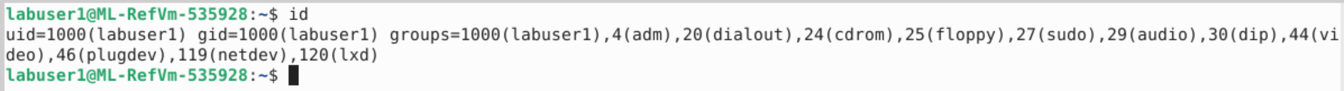
Control	Description
requisite	If the corresponding module returns a "failure," the rest of the category's modules are not executed and the category returns an overall result of "failure."
required	If the corresponding module returns a "failure," the overall result of the category will be "failure." However, 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

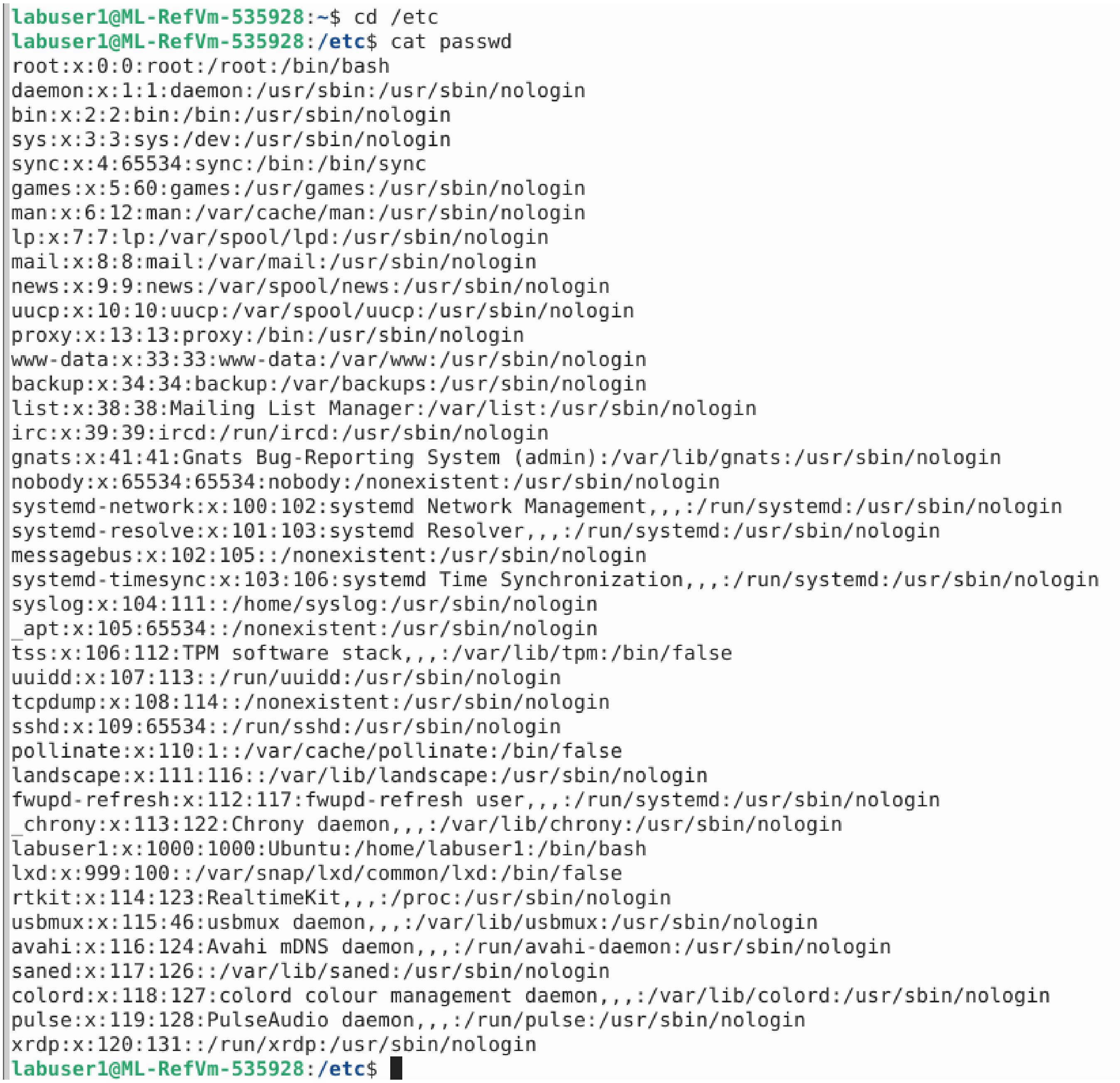
Provide screenshots where * is indicated.

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



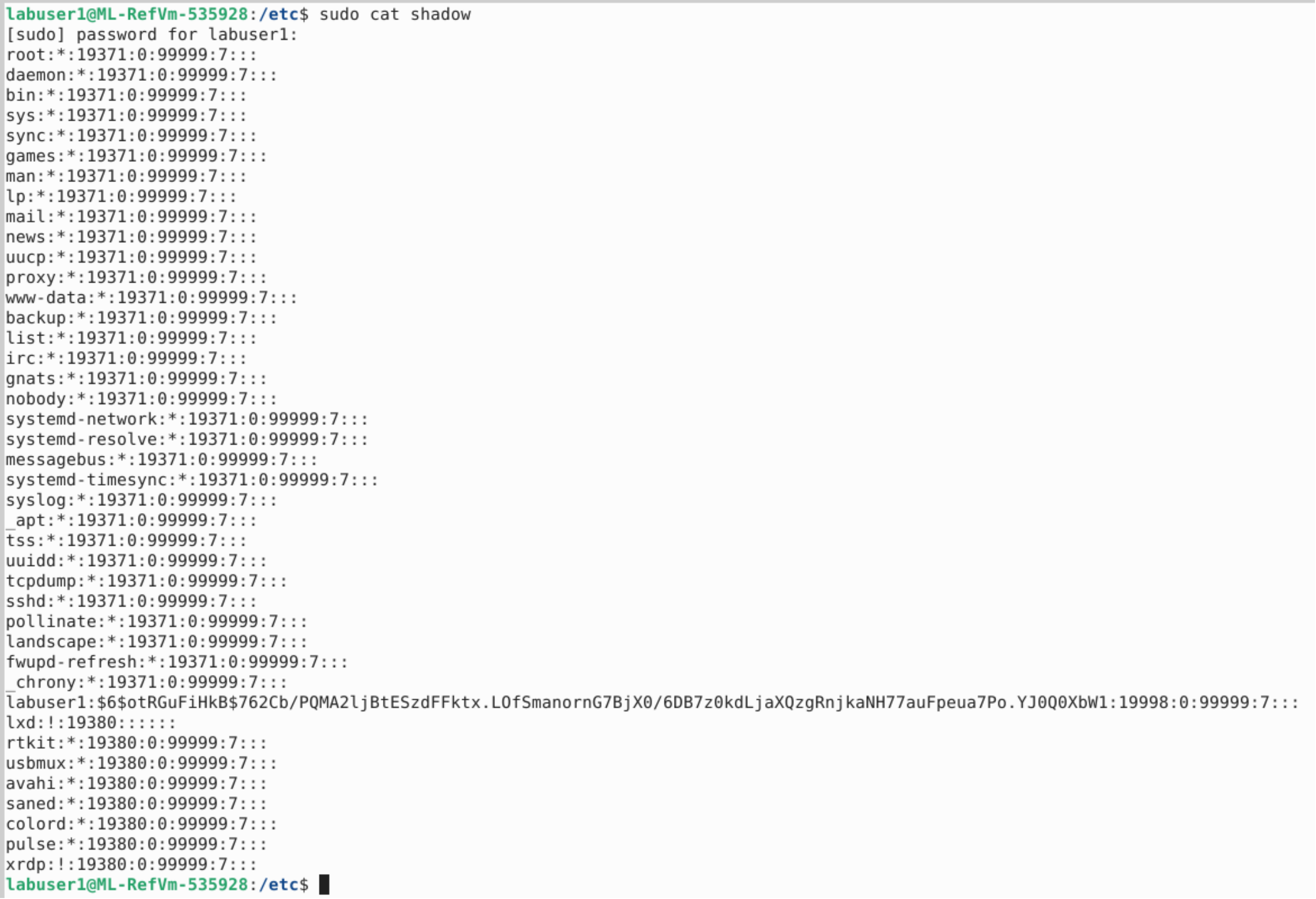
```
labuser1@ML-RefVm-535928:~$ id
uid=1000(labuser1) gid=1000(labuser1) groups=1000(labuser1),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(vi
deo),46(plugdev),119(netdev),120(lxd)
labuser1@ML-RefVm-535928:~$
```

    b. Display contents of passwd*



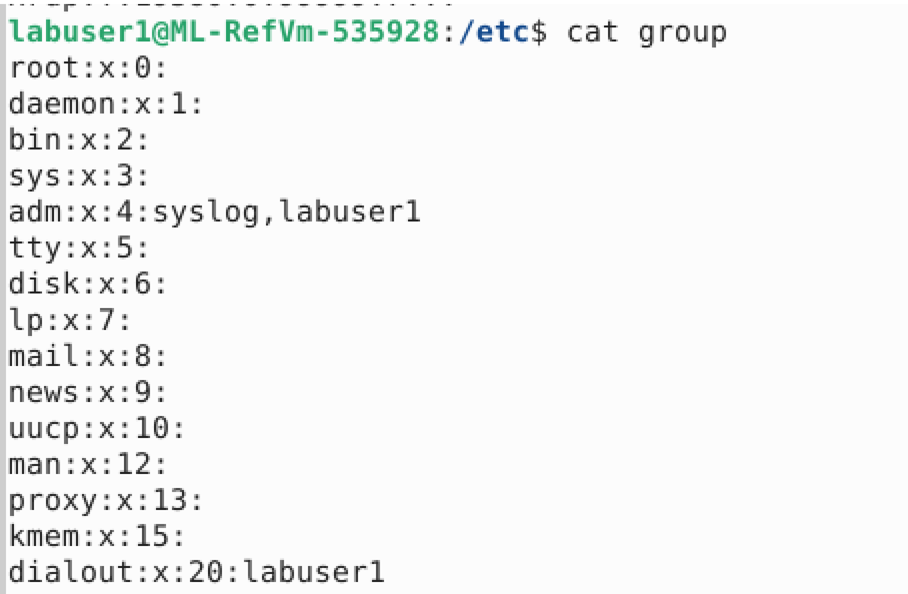
```
labuser1@ML-RefVm-535928:~$ cd /etc
labuser1@ML-RefVm-535928:/etc$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
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:/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/nologin
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:/etc$
```

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:$6$otRGuFiHkB$762Cb/PQMA2ljBtESzdFFktx.LOfSmanornG7BjX0/6DB7z0kdLjaXQzgRnjkaNH77auFpeua7Po.YJ0Q0XbW1:19998:0:99999:7:::
lxd:!:19380::::::
rtkit:*:19380:0:99999:7:::
usbmux:*:19380:0:99999:7:::
avahi:*:19380:0:99999:7:::
saned:*:19380:0:99999:7:::
colord:*:19380:0:99999:7:::
pulse:*:19380:0:99999:7:::
xrdp:!:19380:0:99999:7:::
labuser1@ML-RefVm-535928:/etc$ █
```

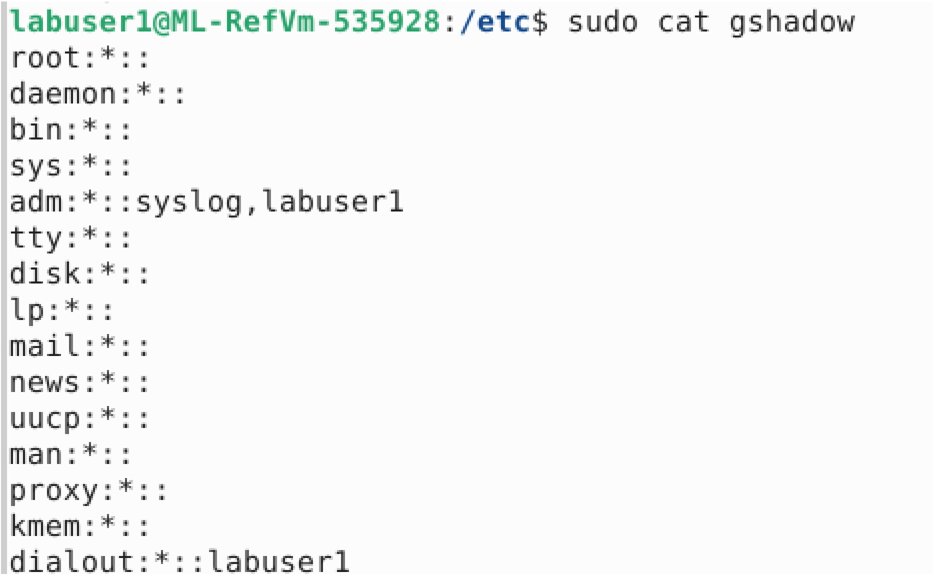
d. Display contents of group*



```
labuser1@ML-RefVm-535928:/etc$ cat 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:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:labuser1
```

I couldn’t fit all of it in the screenshot.

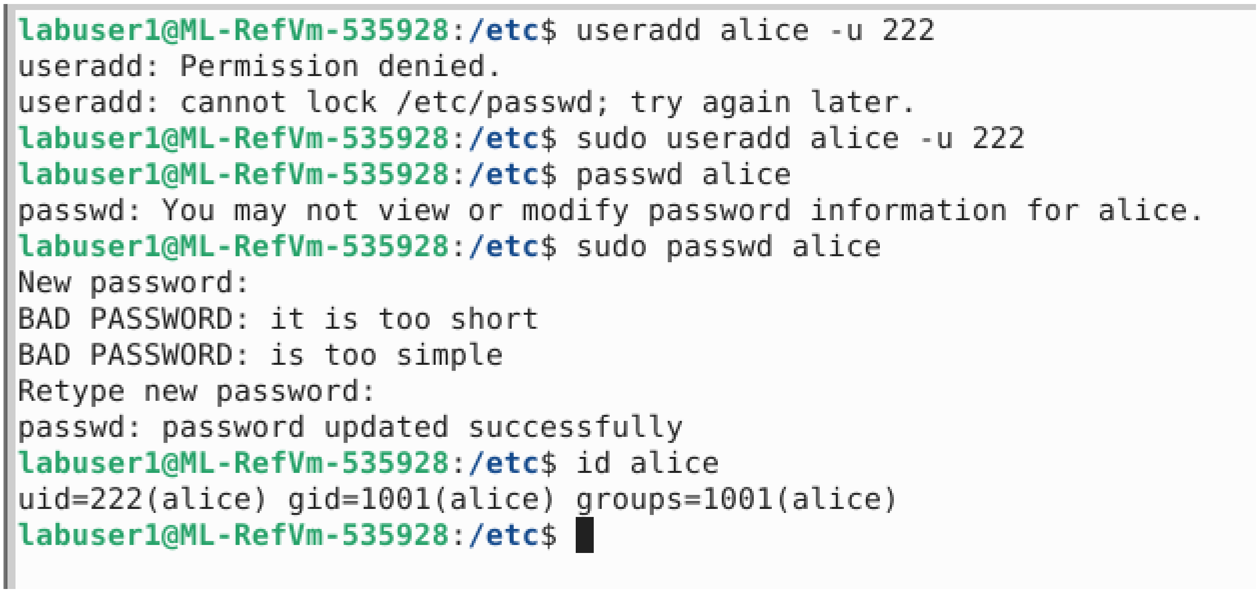
e. Display contents of gshadow*



```
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
```

I couldn't fit all of it in the screenshot.

2. **Alice:**
   a. Create user named **alice** with an ID of 222
   b. Set the password of the user account to '`alice`'
   c. Determine the primary group of **alice***



```
labuser1@ML-RefVm-535928:/etc$ useradd alice -u 222
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
labuser1@ML-RefVm-535928:/etc$ sudo useradd alice -u 222
labuser1@ML-RefVm-535928:/etc$ passwd alice
passwd: You may not view or modify password information for alice.
labuser1@ML-RefVm-535928:/etc$ sudo passwd alice
New password:
BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
Retype new password:
passwd: password updated successfully
labuser1@ML-RefVm-535928:/etc$ id alice
uid=222(alice) gid=1001(alice) groups=1001(alice)
labuser1@ML-RefVm-535928:/etc$ █
```

The primary group is alice.

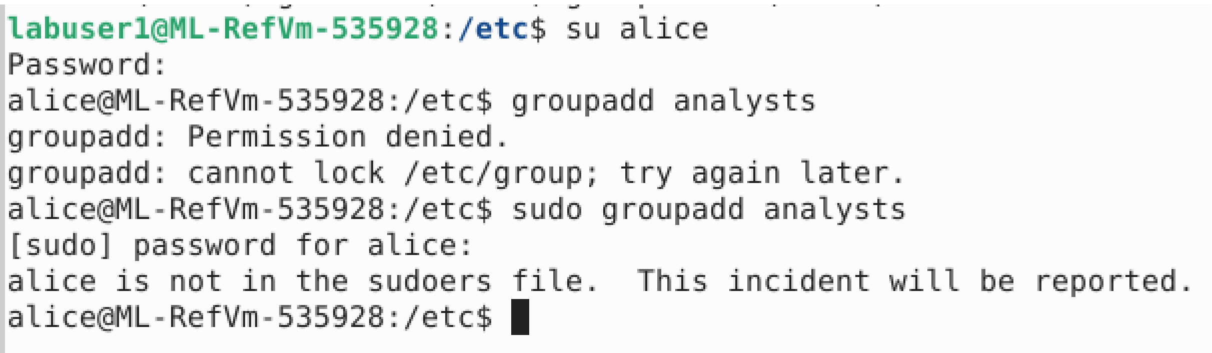
   d. What is the primary group ID of **alice's** primary group? How was this generated?

The primary group ID is 1001. This is generated when the user is created and is incremented from the highest group id.

   e. Switch to user account **alice**

f. Attempt to create group **analysts**

g. Attempt to create group **analysts** as super user*

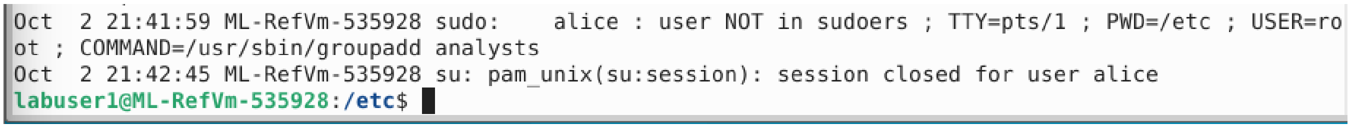


```
labuser1@ML-RefVm-535928:/etc$ su alice
Password:
alice@ML-RefVm-535928:/etc$ groupadd analysts
groupadd: Permission denied.
groupadd: cannot lock /etc/group; try again later.
alice@ML-RefVm-535928:/etc$ sudo groupadd analysts
[sudo] password for alice:
alice is not in the sudoers file.  This incident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

h. Return to default user

i. Display the end of `/var/log/auth.log`

j. Locate incident report*



```
Oct  2 21:41:59 ML-RefVm-535928 sudo:    alice : user NOT in sudoers ; TTY=pts/1 ; PWD=/etc ; USER=ro
ot ; COMMAND=/usr/sbin/groupadd analysts
Oct  2 21:42:45 ML-RefVm-535928 su: pam_unix(su:session): session closed for user alice
labuser1@ML-RefVm-535928:/etc$ █
```

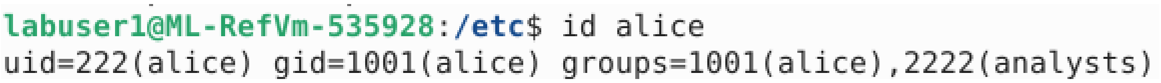
3. Analysts and Agents:

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***

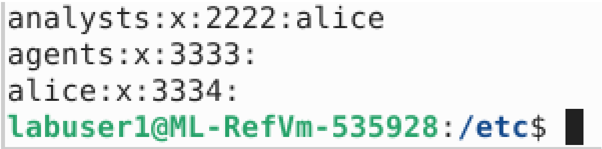


```
labuser1@ML-RefVm-535928:/etc$ id alice
uid=222(alice) gid=1001(alice) groups=1001(alice),2222(analysts)
```

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***



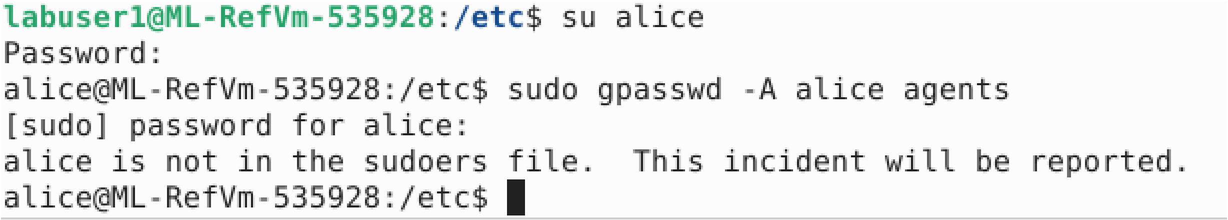
```
analysts:x:2222:alice
agents:x:3333:
alice:x:3334:
labuser1@ML-RefVm-535928:/etc$ █
```

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

4. The primary group ID is 3334. This is generated when the user is created and is incremented from the highest group id.

a. Switch to user account **alice**

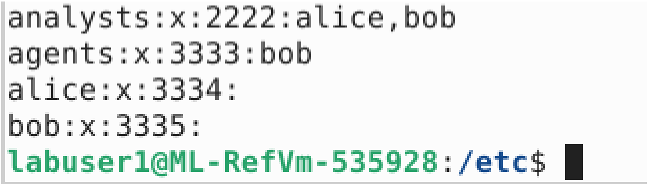
b. Attempt to set **alice** as group administrator of **agents***



```
labuser1@ML-RefVm-535928:/etc$ su alice
Password:
alice@ML-RefVm-535928:/etc$ sudo gpasswd -A alice agents
[sudo] password for alice:
alice is not in the sudoers file.  This incident will be reported.
alice@ML-RefVm-535928:/etc$ 
```

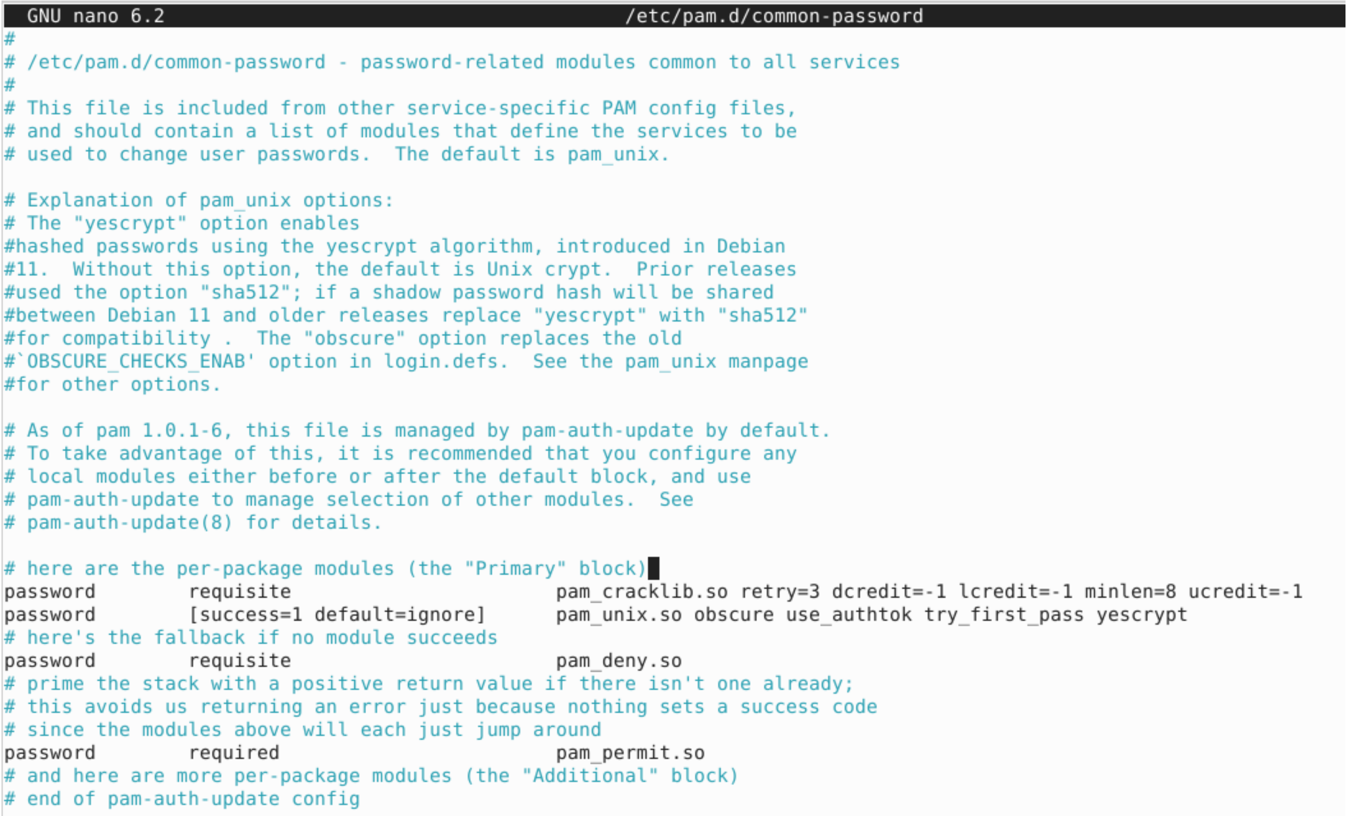
c. Return to default user
d. Set **alice** as group administrator of **agents**

5. **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*



```
analysts:x:2222:alice,bob
agents:x:3333:bob
alice:x:3334:
bob:x:3335:
labuser1@ML-RefVm-535928:/etc$ 
```

   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)

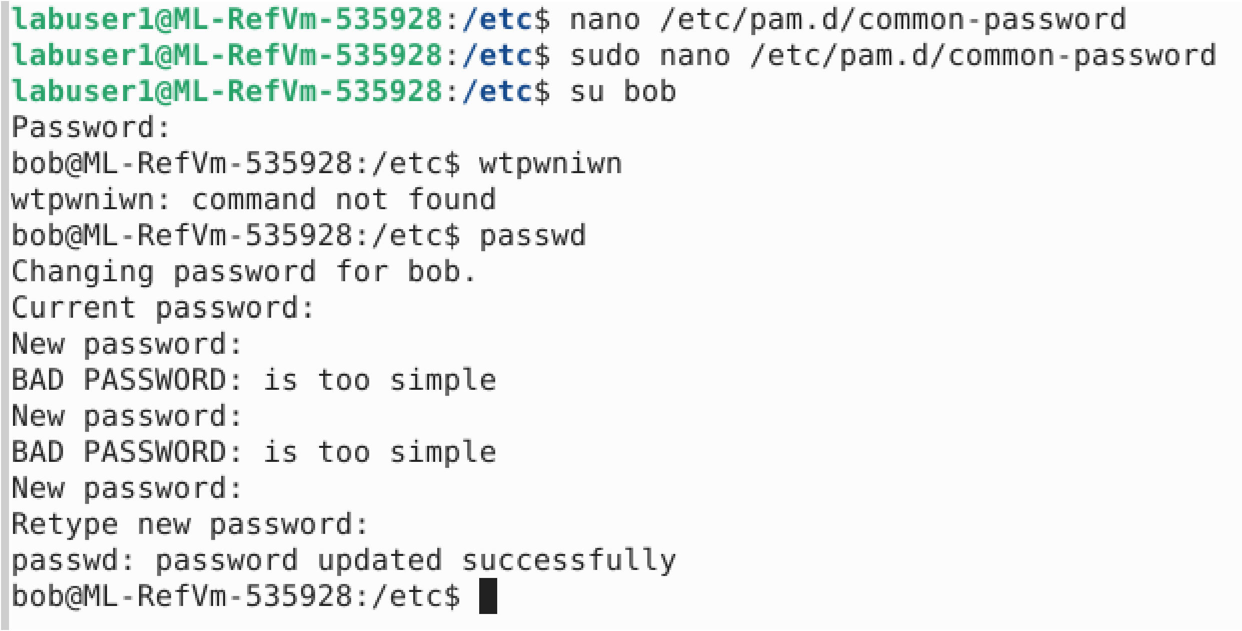


```
  GNU nano 6.2                                    /etc/pam.d/common-password
#
# /etc/pam.d/common-password - password-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of modules that define the services to be
# used to change user passwords.  The default is pam_unix.

# Explanation of pam_unix options:
# The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11.  Without this option, the default is Unix crypt.  Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility .  The "obscure" option replaces the old
#`OBSCURE_CHECKS_ENAB' option in login.defs.  See the pam_unix manpage
#for other options.

# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password        requisite                       pam_cracklib.so retry=3 dcredit=-1 lcredit=-1 minlen=8 ucredit=-1
password        [success=1 default=ignore]      pam_unix.so obscure use_authtok try_first_pass yescrypt
# here's the fallback if no module succeeds
password        requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password        required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
# end of pam-auth-update config
```

h. Switch to user account **bob**

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

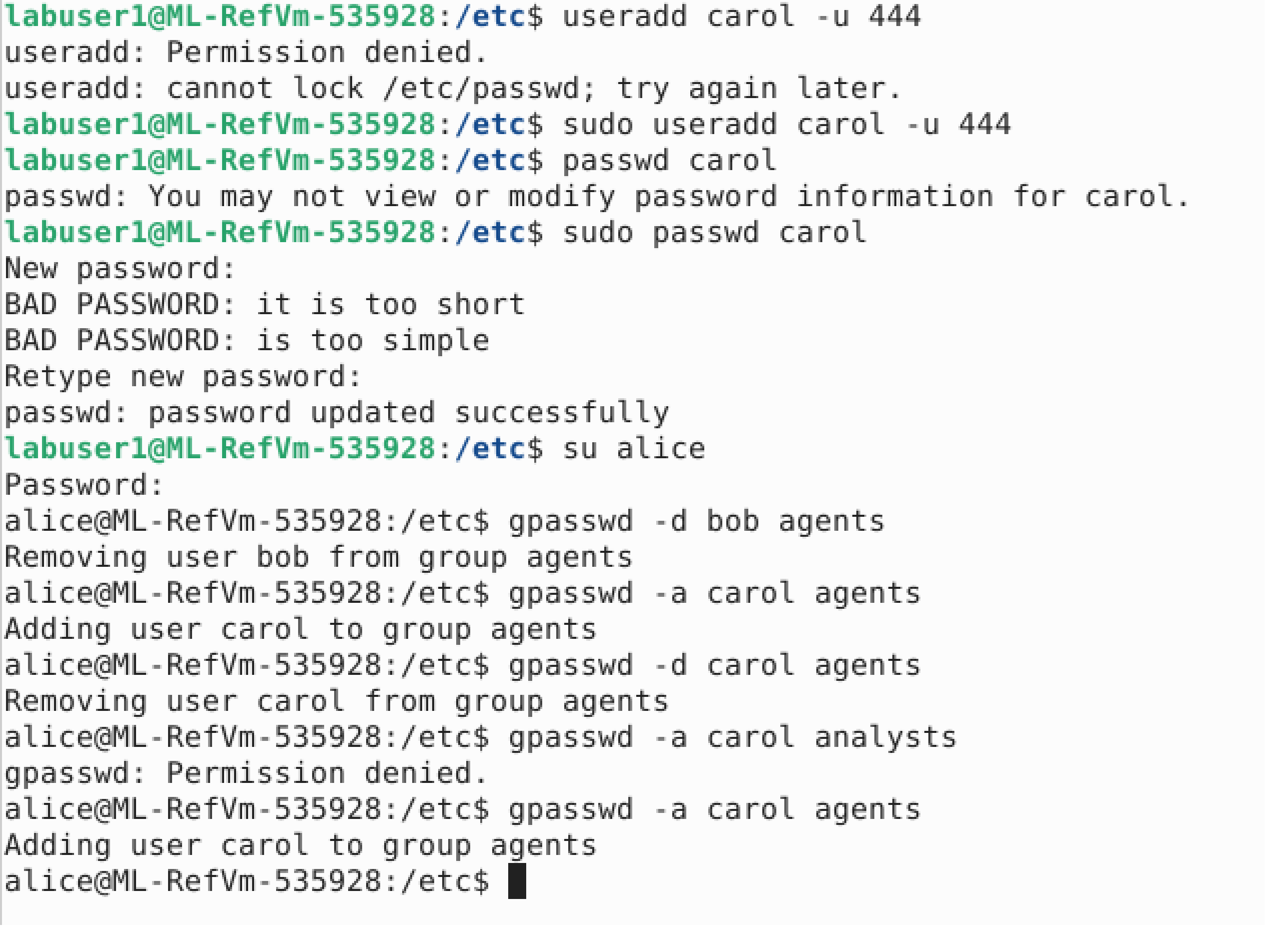
j. Set the password of the user account to ‘`Wtpw0912`’*



```
labuser1@ML-RefVm-535928:/etc$ nano /etc/pam.d/common-password
labuser1@ML-RefVm-535928:/etc$ sudo nano /etc/pam.d/common-password
labuser1@ML-RefVm-535928:/etc$ su bob
Password:
bob@ML-RefVm-535928:/etc$ wtpwniwn
wtpwniwn: command not found
bob@ML-RefVm-535928:/etc$ passwd
Changing password for bob.
Current password:
New password:
BAD PASSWORD: is too simple
New password:
BAD PASSWORD: is too simple
New password:
Retype new password:
passwd: password updated successfully
bob@ML-RefVm-535928:/etc$ 
```

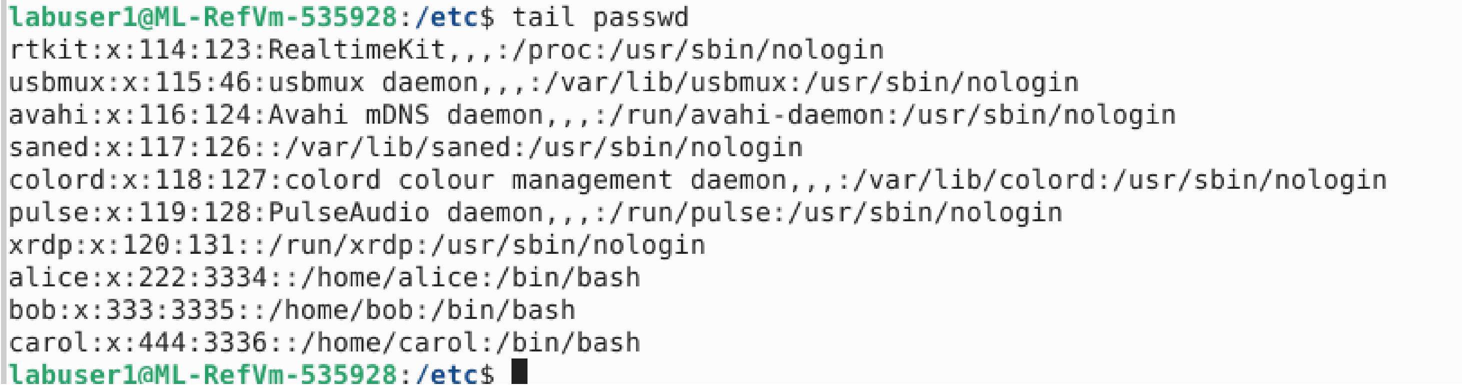
k. Return to default user

6. **Carol:**
    a. Create user named **carol** with an ID of 444
    b. Set the password of the user account to ‘`carol`’
    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***



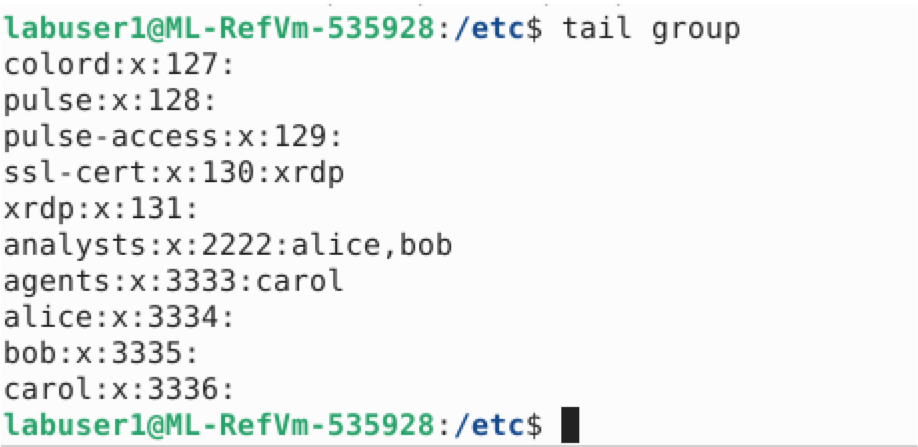
```
labuser1@ML-RefVm-535928:/etc$ useradd carol -u 444
useradd: Permission denied.
useradd: cannot lock /etc/passwd; try again later.
labuser1@ML-RefVm-535928:/etc$ sudo useradd carol -u 444
labuser1@ML-RefVm-535928:/etc$ passwd carol
passwd: You may not view or modify password information for carol.
labuser1@ML-RefVm-535928:/etc$ sudo passwd carol
New password:
BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
Retype new password:
passwd: password updated successfully
labuser1@ML-RefVm-535928:/etc$ su alice
Password:
alice@ML-RefVm-535928:/etc$ gpasswd -d bob agents
Removing user bob from group agents
alice@ML-RefVm-535928:/etc$ gpasswd -a carol agents
Adding user carol to group agents
alice@ML-RefVm-535928:/etc$ gpasswd -d carol agents
Removing user carol from group agents
alice@ML-RefVm-535928:/etc$ gpasswd -a carol analysts
gpasswd: Permission denied.
alice@ML-RefVm-535928:/etc$ gpasswd -a carol agents
Adding user carol to group agents
alice@ML-RefVm-535928:/etc$ 
```

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



```
labuser1@ML-RefVm-535928:/etc$ tail passwd
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
alice:x:222:3334::/home/alice:/bin/bash
bob:x:333:3335::/home/bob:/bin/bash
carol:x:444:3336::/home/carol:/bin/bash
labuser1@ML-RefVm-535928:/etc$ 
```

i. Display contents of group*



```
labuser1@ML-RefVm-535928:/etc$ tail group
colord:x:127:
pulse:x:128:
pulse-access:x:129:
ssl-cert:x:130:xrdp
xrdp:x:131:
analysts:x:2222:alice,bob
agents:x:3333:carol
alice:x:3334:
bob:x:3335:
carol:x:3336:
labuser1@ML-RefVm-535928:/etc$
```