1. Create 3 groups

```
group1:x:1001:
group2:x:1002:
Group3:x:1003:
```

2. Create 15 users

```
user1:x:1001:1004::/home/user1:/bin/sh
user2:x:1002:1005::/home/user2:/bin/sh
user3:x:1003:1006::/home/user3:/bin/sh
user4:x:1004:1007::/home/user4:/bin/sh
user5:x:1005:1008::/home/user5:/bin/sh
user6:x:1006:1009::/home/user6:/bin/sh
user7:x:1007:1010::/home/user7:/bin/sh
user8:x:1008:1011::/home/user8:/bin/sh
user9:x:1009:1012::/home/user9:/bin/sh
user10:x:1010:1013::/home/user10:/bin/sh
user11:x:1011:1014::/home/user11:/bin/sh
user12:x:1012:1015::/home/user12:/bin/sh
user13:x:1013:1016::/home/user13:/bin/sh
user14:x:1014:1017::/home/user14:/bin/sh
user15:x:1015:1018::/home/user15:/bin/sh
```

3. Assign the 15 users across the 3 groups

```
group1:x:1001:user1,user2,user3,user4,user5
group2:x:1002:user6,user7,user8,user9,user10
group3:x:1003:user11,user12,user13,user14,user15
```

4. Write a script that searches through the /var/log directory and filters out the word “packets” from an Ubuntu instance.

```
#!/bin/bash

# "A script that searches through the /var/log directory and filters out the
# word “packets” from an Ubuntu instance."

grep -r  “packets” /var/log
```

```
ubuntu@ip-172-31-22-212:~$ sudo ./packets.sh
grep: /var/log/journal/95e93e2fac0c4f76a198c17e9c885a8e/user-1000.journal: binary
file matches
/var/log/auth.log:Jul 16 10:01:19 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ;
PWD=/var/log ; USER=root ; COMMAND=/usr/bin/grep -r “packets”
/var/log/auth.log:Jul 16 10:03:50 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ;
PWD=/var ; USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
/var/log/auth.log:Jul 16 10:04:52 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ; PWD=/
; USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
/var/log/auth.log:Jul 16 10:17:53 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ;
PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
/var/log/auth.log:Jul 16 10:25:00 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ;
PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
ubuntu@ip-172-31-22-212:~$ vi packets.sh
ubuntu@ip-172-31-22-212:~$ sudo find /var/log/ -type f -exec grep -l 'packets' {} \;
-print
/var/log/journal/95e93e2fac0c4f76a198c17e9c885a8e/user-1000.journal
/var/log/journal/95e93e2fac0c4f76a198c17e9c885a8e/user-1000.journal
/var/log/auth.log
/var/log/auth.log
ubuntu@ip-172-31-22-212:~$ ./packets.sh
grep: /var/log/chrony: Permission denied
grep: /var/log/journal/95e93e2fac0c4f76a198c17e9c885a8e/user-1000.journal: binary
file matches
grep: /var/log/amazon: Permission denied
grep: /var/log/btmp: Permission denied
grep: /var/log/private: Permission denied
/var/log/auth.log:Jul 16 10:01:19 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ;
PWD=/var/log ; USER=root ; COMMAND=/usr/bin/grep -r “packets”
/var/log/auth.log:Jul 16 10:03:50 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ;
PWD=/var ; USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
/var/log/auth.log:Jul 16 10:04:52 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ; PWD=/
; USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
/var/log/auth.log:Jul 16 10:17:53 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ;
PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
/var/log/auth.log:Jul 16 10:25:00 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ;
PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
ubuntu@ip-172-31-22-212:~$ sudo ./packets.sh
grep: /var/log/journal/95e93e2fac0c4f76a198c17e9c885a8e/user-1000.journal: binary
file matches
/var/log/auth.log:Jul 16 10:01:19 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ;
PWD=/var/log ; USER=root ; COMMAND=/usr/bin/grep -r “packets”
/var/log/auth.log:Jul 16 10:03:50 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ;
PWD=/var ; USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
/var/log/auth.log:Jul 16 10:04:52 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ; PWD=/
; USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
/var/log/auth.log:Jul 16 10:17:53 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ;
PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
```

```
/var/log/auth.log:Jul 16 10:25:00 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ;
PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
ubuntu@ip-172-31-22-212:~$ cat /var/log/auth.log | grep -i "packets"
Jul 15 17:27:28 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/1 ; PWD=/home/ubuntu ;
USER=root ; COMMAND=/usr/bin/vim packets.sh
Jul 16 09:55:23 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ; PWD=/var/log ;
USER=root ; COMMAND=/usr/bin/find /var/log/ -type f -exec grep -l packets {} ; -print
Jul 16 10:01:19 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ; PWD=/var/log ;
USER=root ; COMMAND=/usr/bin/grep -r “packets”
Jul 16 10:03:50 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ; PWD=/var ; USER=root ;
COMMAND=/usr/bin/grep -r “packets” /var/log
Jul 16 10:04:52 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ; PWD=/ ; USER=root ;
COMMAND=/usr/bin/grep -r “packets” /var/log
Jul 16 10:17:53 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ;
USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
Jul 16 10:23:09 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ;
USER=root ; COMMAND=./packets.sh
Jul 16 10:25:00 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ;
USER=root ; COMMAND=/usr/bin/grep -r “packets” /var/log
Jul 16 11:31:48 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/1 ; PWD=/home/ubuntu ;
USER=root ; COMMAND=./packets.sh
Jul 16 11:35:57 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/1 ; PWD=/home/ubuntu ;
USER=root ; COMMAND=/usr/bin/find /var/log/ -type f -exec grep -l packets {} ; -print
Jul 16 11:36:53 ip-172-31-22-212 sudo:   ubuntu : TTY=pts/1 ; PWD=/home/ubuntu ;
USER=root ; COMMAND=./packets.sh
ubuntu@ip-172-31-22-212:~$
```