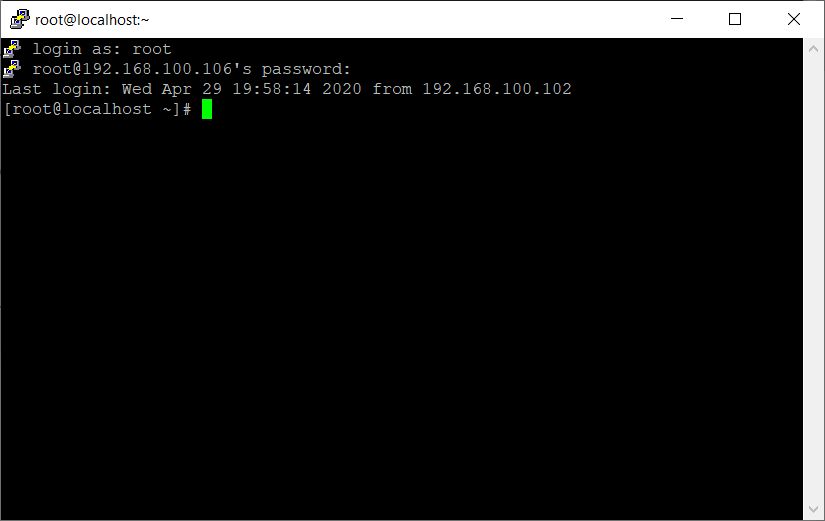
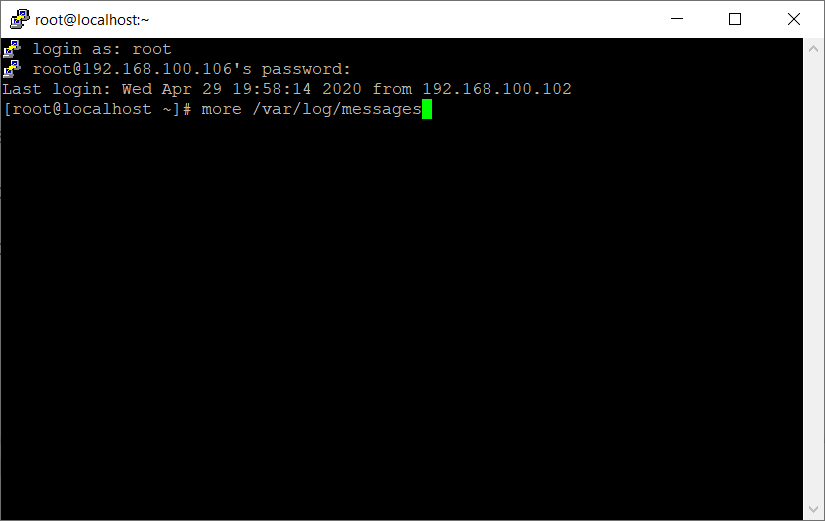
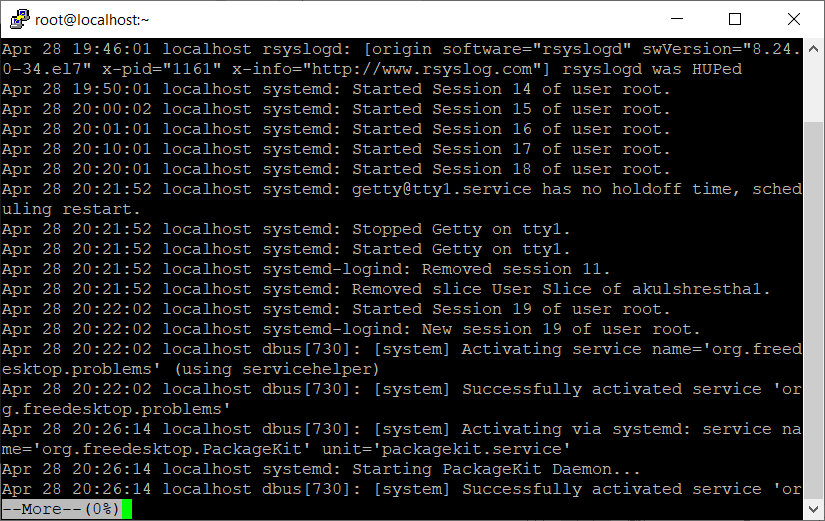
**LOGS**

1) Use putty to login as superuser  
2) Use more command to take a quick look at files/var/log/messages. Use space bar to read more pages and CTRL+C to quit  
**#more /var/log/messages**  
3) List at least 5 names of processes or programs that sent log messages.  
4) Use more command to take a quick look to files/var/log/secure. Use space bar to read more pages and CTRL+C to quit  
#more /var/log/secure  
5) Show some examples where you see changes from commands like su, sudo, ssh, groupadd, chage, useradd, etc.  
6) What can you tell about the messages file and secure file? What is the purpose of them in your opinion?  
7) Use command logger to write an entry on /var/log/messages, and check if you see the entry  
#logger "I love Linux"  
#tail -5 /var/log/messages

**TAR and SCP**  
8) Using putty, open 2 terminal sessions from different Linux VM's (hostname1 and hostname2)  
9) On hostname1, login as superuser  
10) Edit /etc/host file (#vi /etc/hosts)  
11) Add ip and name of hostname2 as the following example:  
      192.168.0.22 hostname2  
       Save and exit  
12) Ping hostname2 ($#ping hostname2)  
       You should see the ip address of hostname2  
       Type CTRL+C to stop ping  
13) Login as a regular user on both hostname1 and hostname2  
14) Check names ($hostname)  
On hostname1:   
15) Create a directorty on the regular user home directory ($mkdir files)  
16) Change directory to the new dir ($cd files)  
17) Create 4 empty files ($touch files a b c d)  
18) Create another file with date data on it ($date > e)  
19) Create a tar file with the content of the directory ($tar -cvf tarfile \*)  
20) List the content of the tarfile ($tar -tvf tarfile)  
21) Check file type ($file tarfile)  
22) Copy tarfile from hostname1 to hostname2 using your regular userid  
      ($scp /tmp/tarfile pszajt@hostname2:/tmp)  
       [pszajt@centos2021 ~]$ scp tarfile pszajt@centos2020:/tmp  
       The authenticity of host 'centos2020 (192.168.0.22)' can't be established.  
       ECDSA key fingerprint is SHA256:DP8Jh0rakyKec83plOOPYzTzY18MVlwNIu3rQK5Tveo.  
       ECDSA key fingerprint is MD5:f1:f1:fb:8a:cd:4c:bc:16:8a:f4:0d:2c:00:08:6f:97.  
       Are you sure you want to continue connecting (yes/no)? yes  
       Warning: Permanently added 'centos2020' (ECDSA) to the list of known hosts.  
       pszajt@centos2020's password:  
       tarfile 100% 10KB 8.0MB/s 00:00  
On hostname2  
23) Change directory to /tmp ($cd /tmp)  
24) Check tarfile ($tar -tvf tarfile)  
25) Extract files ($tar -xvf tarfile)  
26) Check content of file e ($cat e)  
27) Open a Windows prompt (cmd)  
28) Copy the tarfile from the Linux server to your windows laptop  
      (pscp pszajt@192.168.0.33:\home\pszajt\files\tarfile .)  
      type yes if the command asks you: Are you sure you want to continue connecting (yes/no)?  
      and type your regular user password  
29) Copy the tarfile from your windows laptop to your Linux server as tarfile2  
      (pscp tarfile pszajt@192.168.0.33:\home\pszajt\files\tarfile2)  
      type yes if the command asks you: Are you sure you want to continue connecting (yes/no)?  
      and type your regular user password







List at least 5 names of processes or programs that sent log messages.

Chronyd

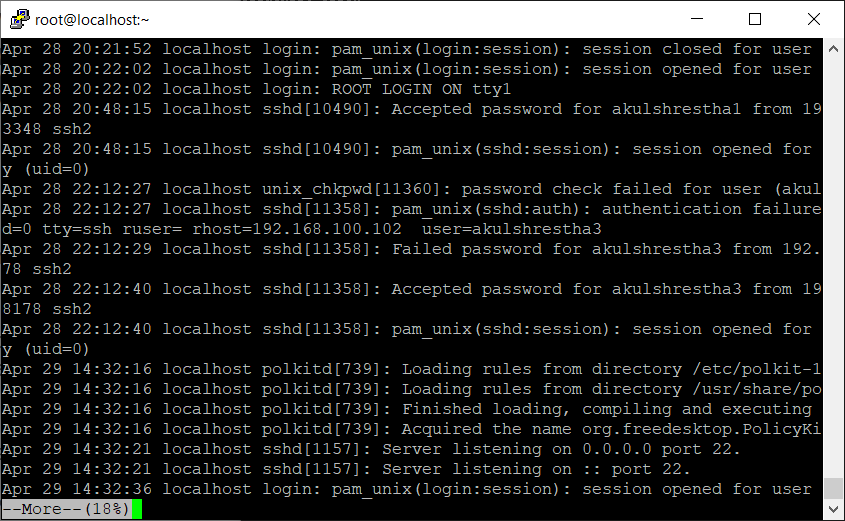
Dbus

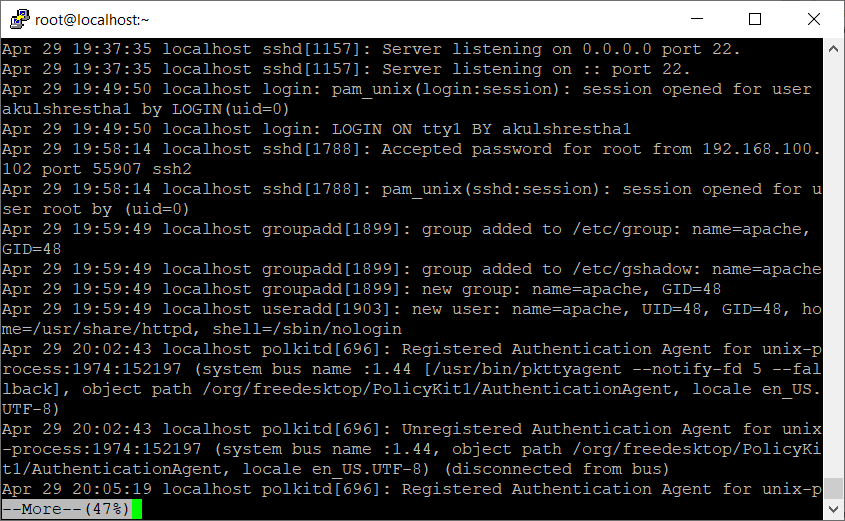
Kernel

Rsyslogd

Journal

Lvm

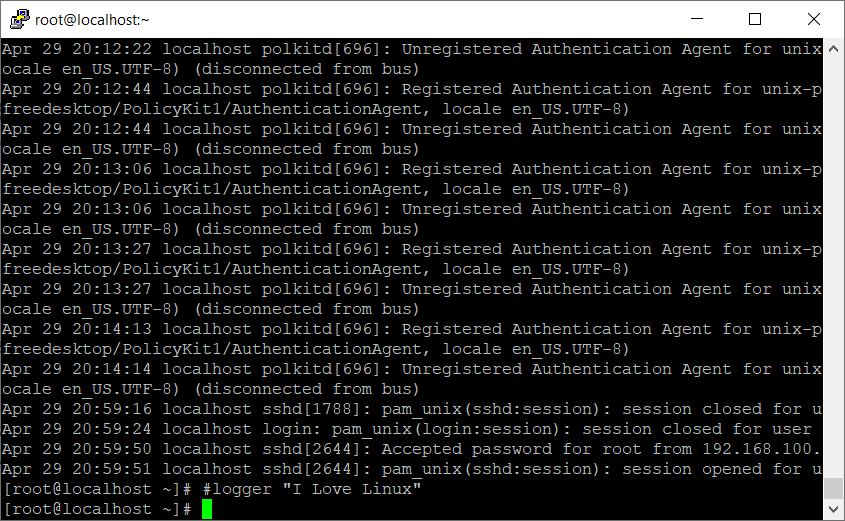


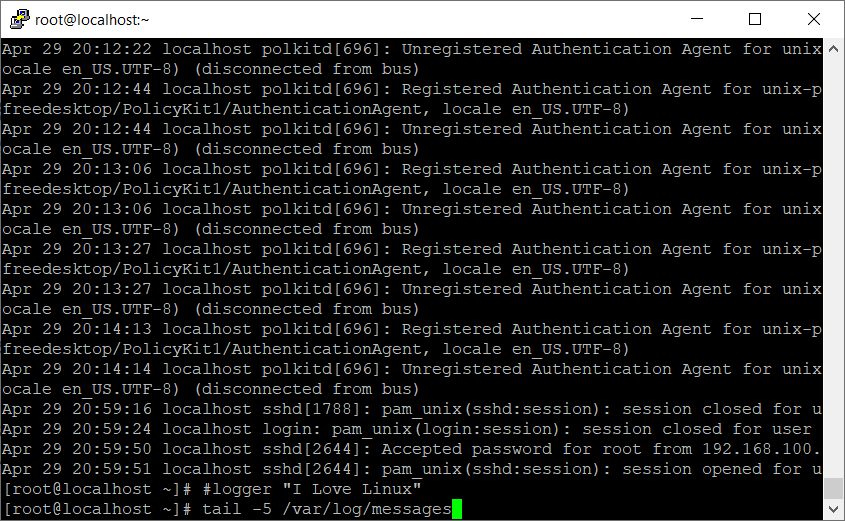


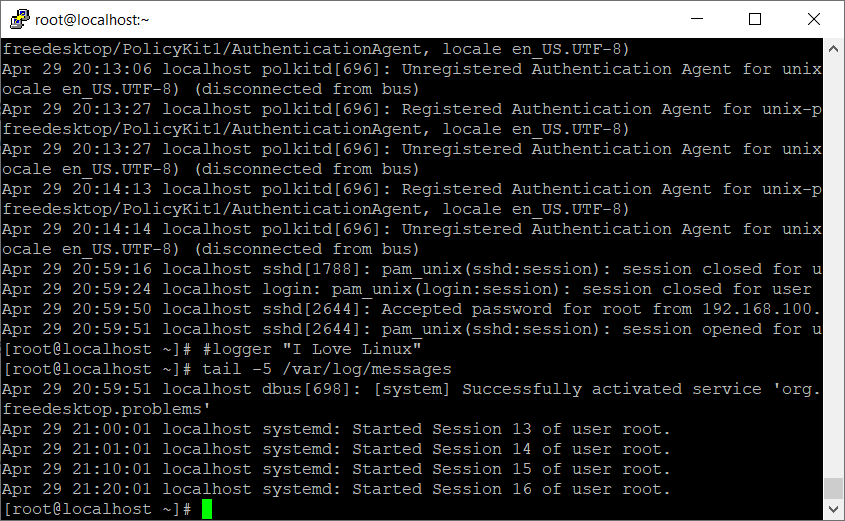
What can you tell about the messages file and secure file? What is the purpose of them in your opinion?

**/var/log/messages** – Contains global system messages, including the messages that are logged during system startup. There are several things that are logged in /var/log/messages including mail, cron, daemon, kern, auth, etc.

**/var/log/secure** – Contains information related to authentication and authorization privileges. For example, sshd logs all the messages here, including unsuccessful login.







Part II

