# Week 5 Homework Submission File: Archiving and Logging Data

---

## Step 1: Create, Extract, Compress, and Manage tar Backup Archives

1. Command to **extract** the TarDocs.tar archive to the current directory: I downloaded the tar file with wget command and moved to the project file.

   **wget "https://drive.google.com/uc?id=1fRjFS1vOdS7yfKJgpJxR02_UxeT_ql_u&export=download"**

   **mv TarDocs.tar ~/Projects**

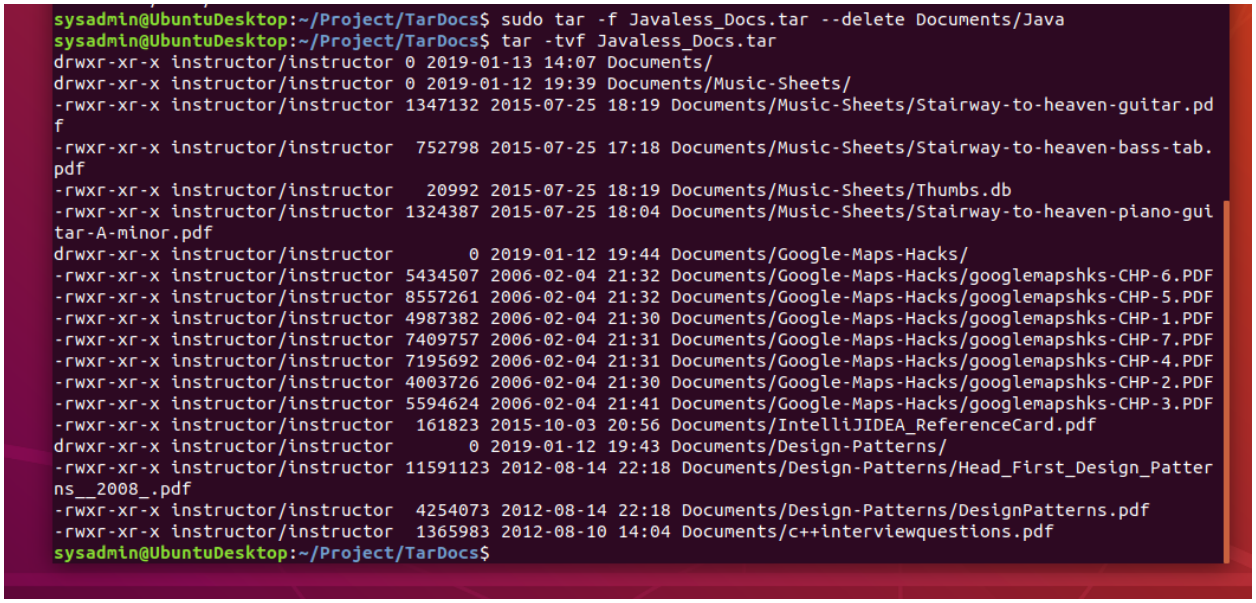
   **sudo tar xvf TarDocs.tar**

2. Command to **create** the Javaless_Doc.tar archive from the TarDocs/ directory, while excluding the TarDocs/Documents/Java directory:

   **sudo tar cvf Javaless_Docs.tar --exclude=’Java/*’ Documents**

3. Command to ensure Java/ is not in the new Javaless_Docs.tar archive: **sudo tar -f Javaless_Docs.tar --delete Documents?Java**

   **tar -tvf Javaless_Docs.tar**




**Bonus**

- Command to create an incremental archive called logs_backup_tar.gz with only changed files to snapshot.file for the /var/log directory: **sudo tar -cvzf logs_backup.tar.gz --listed-incremental=snapshot.file --level=0 /var/log**

**Critical Analysis Question**

- Why wouldn't you use the options -x and -c at the same with tar?
- **-x is an option for that tar command which relates to extract or untar an archive**
- **-c is another option creates the archive**

  **We can not use both -x and -c commands in a single tar command. But we can use -x and -C (uppercase C) to create a file**

## Step 2: Create, Manage, and Automate Cron Jobs

1. Cron job for backing up the /var/log/auth.log file:

```
#!/bin/bash

#Creating this script to create, manage and automate cron task.  Details of this script will be stored
#in the location var /log/auth_backup.tgz folder
#Craeting a copy  of the auth.log and moving it into auth_backyp.tgz folder
sudo cp -vp /var/log/auth.log /var/log/auth_backup.tgz/

#creating an archive of the file
sudo tar cvvWf auth_backup.tar auth.log

#Creating the zip file
sudo tar cvzf auth_backup.tgz auth_backup.tar
```

**Testing the script:**

```
sysadmin@UbuntuDesktop:/var/log/auth_backup.tgz$ sh ./auth_backup.sh
'/var/log/auth.log' -> '/var/log/auth_backup.tgz/auth.log'
-rw-r----- syslog/adm    52544 2020-11-27 20:08 auth.log
Verify -rw-r----- syslog/adm    52544 2020-11-27 20:08 auth.log
auth_backup.tar
sysadmin@UbuntuDesktop:/var/log/auth_backup.tgz$
```

**Checking if tar files are created**

```
sysadmin@UbuntuDesktop:/var/log/auth_backup.tgz$ ls -l
total 124
-rw-r--r-- 1 root   root   446 Nov 27 20:07 auth_backup.sh
-rw-r--r-- 1 root   root 61440 Nov 27 20:08 auth_backup.tar
-rw-r--r-- 1 root   root  5288 Nov 27 20:08 auth_backup.tgz
-rw-r----- 1 syslog adm  52544 Nov 27 20:08 auth.log
```

**setting crontab to 02:00am every saturday**

**0 02 * * 6 /var/log/auth_backup.tgz/auth_backup.sh**

```
sysadmin@UbuntuDesktop:/var/log/auth_backup.tgz$ ls -l
total 124
-rwxr-xr-x 1 root   root   446 Nov 27 20:07 auth_backup.sh
-rw-r--r-- 1 root   root 61440 Nov 27 20:08 auth_backup.tar
-rw-r--r-- 1 root   root  5288 Nov 27 20:08 auth_backup.tgz
-rw-r----- 1 syslog adm  52544 Nov 27 20:08 auth.log
```

## Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:
   **sudo mkdir backups/{freemem,diskuse,openlist,freedisk}**

   **or**

   **mkdir backups**

   **cd backups**

   **Mkdir freemem diskuse openlis freedisk**

```
sysadmin@UbuntuDesktop:~/backups$ ls
diskuse  freedisk  freemem  openlist
```

2. Paste your system.sh script edits below:

   **#!/bin/bash**

   **free -h > ~/backups/freemem/free_mem.txt**

   **du -h > ~/backups/diskuse/disk_usage.txt**

   **lsof > ~/backups/openlist/open_list.txt**

   **df -h > ~/backups/freedisk/free_disk.txt**

3. Command to make the system.sh script executable: **chmod +x system.sh**

**Optional**

- Commands to test the script and confirm its execution: **sudo ./sysmtem.sh**

```
sysadmin@UbuntuDesktop:~$ sudo ./system.sh
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
sysadmin@UbuntuDesktop:~$
```

**Bonus**

- Command to copy system to system-wide cron directory: **sudo cp system.sh /etc/cron.weekly**

```
sysadmin@UbuntuDesktop:~$ sudo cp system.sh /etc/cron.weekly
sysadmin@UbuntuDesktop:~$ ls /etc/cron.weekly
0anacron  backup.sh  lynis.system.sh  man-db  system.sh  update-notifier-common  update.sh
sysadmin@UbuntuDesktop:~$
```

---

## Step 4. Manage Log File Sizes

1. Run sudo nano /etc/logrotate.conf to edit the logrotate configuration file.

   Configure a log rotation scheme that backs up authentication messages to the /var/log/auth.log.

   - Add your config file edits below:
   - 

```
/var/log/wtmp {
    missingok
    monthly
    create 0664 root utmp
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0660 root utmp
    rotate 1
}
```

2. [Your logrotate scheme edits here]

```
28
29 /var/log/btmp {
30     missingok
31     monthly
32     create 0660 root utmp
33     rotate 1
34 }
35
36 /var/log/auth.log {
37     missingok
38     weekly
39     notifempty
40     rotate 7
41     compress
42     delaycompress
43 }
```

---

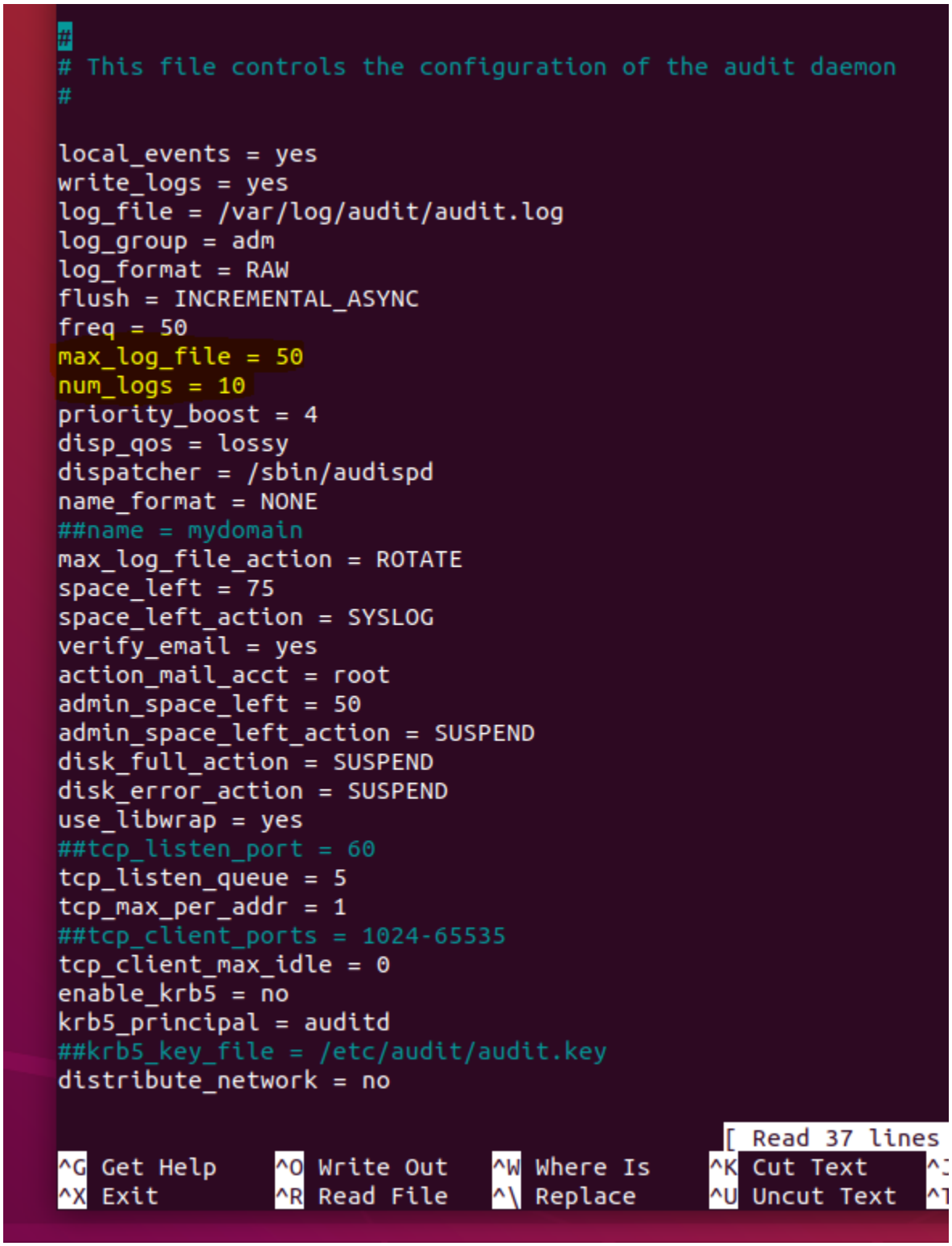
## Bonus: Check for Policy and File Violations

1. Command to verify auditd is active: **sudo systemctl status auditd.service**

```
sysadmin@UbuntuDesktop:/$ sudo systemctl status auditd.service
● auditd.service - Security Auditing Service
   Loaded: loaded (/lib/systemd/system/auditd.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2020-11-26 18:47:59 EST; 24h ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
 Main PID: 654 (auditd)
    Tasks: 2 (limit: 4915)
   CGroup: /system.slice/auditd.service
           └─654 /sbin/auditd

Nov 26 18:47:59 UbuntuDesktop augenrules[658]: backlog_wait_time 15000
Nov 26 18:47:59 UbuntuDesktop augenrules[658]: enabled 1
Nov 26 18:47:59 UbuntuDesktop augenrules[658]: failure 1
Nov 26 18:47:59 UbuntuDesktop augenrules[658]: pid 654
Nov 26 18:47:59 UbuntuDesktop augenrules[658]: rate_limit 0
Nov 26 18:47:59 UbuntuDesktop augenrules[658]: backlog_limit 8192
Nov 26 18:47:59 UbuntuDesktop augenrules[658]: lost 0
Nov 26 18:47:59 UbuntuDesktop augenrules[658]: backlog 0
Nov 26 18:47:59 UbuntuDesktop augenrules[658]: backlog_wait_time 0
Nov 26 18:47:59 UbuntuDesktop systemd[1]: Started Security Auditing Service.
sysadmin@UbuntuDesktop:/$
```

2. Command to set number of retained logs and maximum log file size: **sudo nano /etc/audit/auditd.conf**
    - Add the edits made to the configuration file below:


#
# This file controls the configuration of the audit daemon
#
local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 50
num_logs = 10
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
distribute_network = no
[ Read 37 lines
^G Get Help
^O Write Out
^W Where Is
^K Cut Text
^X Exit
^R Read File
^\ Replace
^U Uncut Text

3. Command using auditd to set rules for /etc/shadow, /etc/passwd and /var/log/auth.log: **sudo nano /etc/audit/rules.d/audit/rules**
    - Add the edits made to the rules file below:

```
## First rule - delete all
-D


## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 0

## Set failure mode to syslog
-f 1


 -w /etc/shadow -p wra -k hashpass_audit
 -w /etc/passwd -p wra -k userpass_audit
 -w /var/log/auth.log -p wra -k authlog_audit
```

4. Command to restart auditd: **sudo systemctl restart auditd.service**

5. Command to list all auditd rules: **sudo auditctl -l**

```
sysadmin@UbuntuDesktop:/$ sudo auditctl -l
-w /etc/shadow -p rwa -k hashpass_audit
-w /etc/passwd -p rwa -k userpass_audit
-w /var/log/auth.log -p rwa -k authlog_audit
sysadmin@UbuntuDesktop:/$
```

6. Command to produce an audit report: **sudo aureport -m**

```
sysadmin@UbuntuDesktop:/$ sudo aureport -m

Account Modifications Report
============================================
# date time auid addr term exe acct success event
============================================
1. 11/24/2020 21:14:46 -1 ? ? /usr/sbin/useradd vboxadd no 238
2. 11/24/2020 21:14:46 -1 ? ? /usr/sbin/useradd vboxadd no 239
3. 11/24/2020 21:14:46 -1 ? ? /usr/sbin/useradd vboxadd no 240
4. 11/24/2020 21:14:46 -1 ? ? /usr/sbin/useradd vboxadd no 241
5. 11/24/2020 21:23:12 -1 ? ? /usr/sbin/useradd vboxadd no 222
6. 11/24/2020 21:23:12 -1 ? ? /usr/sbin/useradd vboxadd no 223
7. 11/24/2020 21:23:12 -1 ? ? /usr/sbin/useradd vboxadd no 224
8. 11/24/2020 21:23:12 -1 ? ? /usr/sbin/useradd vboxadd no 225
9. 11/26/2020 18:48:25 -1 ? ? /usr/sbin/useradd vboxadd no 235
10. 11/26/2020 18:48:25 -1 ? ? /usr/sbin/useradd vboxadd no 236
11. 11/26/2020 18:48:25 -1 ? ? /usr/sbin/useradd vboxadd no 237
12. 11/26/2020 18:48:25 -1 ? ? /usr/sbin/useradd vboxadd no 238
sysadmin@UbuntuDesktop:/$
```

7. Create a user with sudo useradd attacker and produce an audit report that lists account modifications:

```
sysadmin@UbuntuDesktop:/$ sudo adduser attacker
Adding user `attacker' ...
Adding new group `attacker' (1023) ...
Adding new user `attacker' (1020) with group `attacker' ...
The home directory `/home/attacker' already exists.  Not copying from `/etc/skel'.
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for attacker
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
sysadmin@UbuntuDesktop:/$ su attacker
Password:
attacker@UbuntuDesktop:/$ whoami
attacker
attacker@UbuntuDesktop:/$
```

```
sysadmin@UbuntuDesktop:/$ sudo aureport -au

Authentication Report
============================================
# date time acct host term exe success event
============================================
1. 11/24/2020 21:14:47 gdm UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 245
2. 11/24/2020 21:16:55 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 272
3. 11/24/2020 21:17:21 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 293
4. 11/24/2020 21:23:12 gdm UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 229
5. 11/24/2020 21:23:29 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 254
6. 11/24/2020 21:45:25 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 272
7. 11/24/2020 21:59:22 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 275
8. 11/24/2020 22:00:55 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 278
9. 11/24/2020 22:29:42 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 324
10. 11/24/2020 22:39:28 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 327
11. 11/24/2020 22:39:38 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 330
12. 11/24/2020 22:49:07 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 342
13. 11/24/2020 23:42:55 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 379
14. 11/25/2020 00:15:01 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 406
15. 11/25/2020 00:15:54 sysadmin ? /dev/pts/0 /usr/bin/sudo no 409
16. 11/25/2020 00:15:56 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 410
17. 11/26/2020 18:48:26 gdm UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 242
18. 11/26/2020 18:49:46 sysadmin UbuntuDesktop /dev/tty1 /usr/lib/gdm3/gdm-session-worker yes 269
19. 11/26/2020 18:50:10 sysadmin ? /dev/pts/0 /usr/bin/sudo yes 284
20. 11/27/2020 16:53:05 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker no 968
21. 11/27/2020 16:53:09 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 970
22. 11/27/2020 18:50:35 sysadmin UbuntuDesktop /dev/tty2 /usr/lib/gdm3/gdm-session-worker yes 1035
23. 11/27/2020 18:51:46 sysadmin ? /dev/pts/3 /usr/bin/sudo yes 1038
24. 11/27/2020 19:37:28 root UbuntuDesktop pts/3 /usr/bin/chfn yes 70440
25. 11/27/2020 19:37:41 attacker ? /dev/pts/3 /bin/su no 70472
26. 11/27/2020 19:37:55 attacker ? /dev/pts/3 /bin/su no 70479
27. 11/27/2020 19:38:21 root UbuntuDesktop pts/3 /usr/bin/chfn yes 71483
28. 11/27/2020 19:38:30 attacker ? /dev/pts/3 /bin/su yes 71534
29. 11/27/2020 19:39:27 sysadmin ? /dev/pts/3 /bin/su yes 72073
^C
sysadmin@UbuntuDesktop:/$
```

8. Command to use auditd to watch /var/log/cron: **sudo auditctl -w /var/log/cron**

9. Command to verify auditd rules:

```
sysadmin@UbuntuDesktop:/$ sudo auditctl -l
-w /etc/shadow -p rwa -k hashpass_audit
-w /etc/passwd -p rwa -k userpass_audit
-w /var/log/auth.log -p rwa -k authlog_audit
-w /var/log/cron -p rwxa
```

## Bonus (Research Activity): Perform Various Log Filtering Techniques

1. Command to return journalctl messages with priorities from emergency to error:

   **sudo journalctl -p emerg..err -b -0**

2. Command to check the disk usage of the system journal unit since the most recent boot:

   **sudo journalctl -u systemd-journald -b -0 | less**

```
-- Logs begin at Tue 2019-11-12 16:35:11 EST, end at Fri 2020-11-27 19:46:07 EST. --
Nov 26 18:47:52 UbuntuDesktop systemd-journald[268]: Journal started
Nov 26 18:47:52 UbuntuDesktop systemd-journald[268]: Runtime journal (/run/log/journal/e5853fe375964d39b27025
eb6608e969) is 8.0M, max 160.1M, 152.1M free.
Nov 26 18:47:52 UbuntuDesktop systemd-journald[268]: Time spent on flushing to /var is 5.281027s for 503 entr
ies.
Nov 26 18:47:52 UbuntuDesktop systemd-journald[268]: System journal (/var/log/journal/e5853fe375964d39b27025e
b6608e969) is 416.0M, max 3.9G, 3.5G free.
(END)
```

3. Comand to remove all archived journal files except the most recent two:

   **Sudo journalctl --vacuum-time=”5 days”**

4. Command to filter all log messages with priority levels between zero and two, and save output to /home/sysadmin/Priority_High.txt:

```
sysadmin@UbuntuDesktop:/$ sudo journalctl -p 0..2 >> /home/sysadmin/Priority_High.txt
sysadmin@UbuntuDesktop:/$ sudo cat /home/sysadmin/Priority_High.txt
-- Logs begin at Sat 2020-11-14 16:33:58 EST, end at Fri 2020-11-27 19:49:24 EST. --
-- No entries --
```

5. Command to automate the last command in a daily cronjob. Add the edits made to the crontab file below:

   **sudo nano journal_filter_priority_0_2.sh**

```
#!/bin/bash

sudo journalctl -p 0..2 >> /home/sysadmin/Priortiy_High.txt
```

```
sysadmin@UbuntuDesktop:/$ sudo chmod +x journal_filter_priority_0_2.sh
sysadmin@UbuntuDesktop:/$ ls
03-instructor  dev              journal_filter_priority_0_2.sh  media  run
03-student     etc              lib                             mnt    sbin
bin            home             lib32                           opt    snap
boot           initrd.img       lib64                           proc   splunk
cdrom          initrd.img.old   lost+found                      root   srv
```

**sudo mv journal_filter_priority_0_2.sh /etc/cron.daily**
**ls -l /etc/cron.daily/**

```
sysadmin@UbuntuDesktop:/$ sudo mv journal_filter_priority_0_2.sh /etc/cron.daily
sysadmin@UbuntuDesktop:/$ ls -l /etc/cron.daily/
total 88
-rwxr-xr-x 1 root root  268 Jul  9  2019 00logwatch
-rwxr-xr-x 1 root root  311 May 29  2017 0anacron
-rwxr-xr-x 1 root root  539 Jul 16  2019 apache2
-rwxr-xr-x 1 root root  376 Nov 20  2017 apport
-rwxr-xr-x 1 root root 1478 Apr 20  2018 apt-compat
-rwxr-xr-x 1 root root  314 Jan 16  2018 aptitude
-rwxr-xr-x 1 root root  355 Dec 29  2017 bsdmainutils
-rwxr-xr-x 1 root root 2189 Jul 24  2017 chkrootkit
-rwxr-xr-x 1 root root  322 Nov 20 00:21 cleanup.sh
-rwxr-xr-x 1 root root  384 Dec 12  2012 cracklib-runtime
-rwxr-xr-x 1 root root 1176 Nov  2  2017 dpkg
lrwxrwxrwx 1 root root   37 Nov 16 21:38 google-chrome -> /opt/google/chrome/cron/google-chrome
-rwxr-xr-x 1 root root   73 Nov 27 19:52 journal_filter_priority_0_2.sh
-rwxr-xr-x 1 root root  372 Aug 21  2017 logrotate
-rwxr-xr-x 1 root root  130 Nov 20 00:19 lynis.partial.sh
-rwxr-xr-x 1 root root 1065 Apr  7  2018 man-db
-rwxr-xr-x 1 root root  538 Mar  1  2018 mlocate
-rwxr-xr-x 1 root root  249 Jan 25  2018 passwd
-rwxr-xr-x 1 root root 3477 Feb 20  2018 popularity-contest
-rwxr-xr-x 1 root root  383 Mar 29  2019 samba
-rwxr-xr-x 1 root root  123 Jan 29  2014 tripwire
-rwxr-xr-x 1 root root  246 Mar 21  2018 ubuntu-advantage-tools
-rwxr-xr-x 1 root root  214 Nov 12  2018 update-notifier-common
```