Week 5 Homework Submission File: Archiving and Logging Data

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

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

1. Command to **extract** the `TarDocs.tar` archive to the current director:

   After moving the TarDocs.tar files from the download to /hone/sysadmin/Projects

   ```
   cd /home/sysadmin/Projects
   ```

   ```
   tar xvvf TarDocs.tar
   ```

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

```
tar --exclude='./folder' --exclude='./upload/folder2' -cvf /backup/filename.tar
```

   ```
   tar -cvvWf Javaless_Doc.tar --exclude=Java ~/Projects/TarDocs/Documents
   ```

3. Command to ensure `Java/` is not in the new `Javaless_Docs.tar` archive:

   ```
   tar -tvf /TarDocs/Javaless_Doc.tar   | grep -i Java
   ```

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_backup.snar –level=0 /var/log/
  ```

Critical Analysis Question

- Why wouldn't you use the options `-x` and `-c` at the same with `tar`?

  ```
  -c is used for archiving, and -x is for restoration, doing archiving and
  restoring at the same time is a conflict.
  ```

Step 2: Create, Manage, and Automate Cron Jobs

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

   0 6 * * 3 tar -czf /var/log/auth_backup.tgz /var/log/auth.log

---

Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:
2.

   https://developmentality.wordpress.com/2010/04/11/advanced-mkdir-and-brace-expansion-fun/

   mkdir -p /backups/{freemem,diskuse,openlist,freedisk}

3. Paste your `system.sh` script edits below:

   ```
   #!/bin/bash

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

   df -h >  ~/backups/freeduse/disk_usage.txt

   lsof  >  ~/backups/openfiles/open_list.txt

   df -kh >  ~/backups/freedisk/free_disk.txt
   ```

4. Command to make the `system.sh` script executable:

Sudo chmod 755 system.sh

Optional

- Commands to test the script and confirm its execution:

sudo sh system.sh or ./system.sh

Bonus

- Command to copy `system.sh` to system-wide cron directory:

sudo cp system.sh /var/spool/cron/crontabs/

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:

```
# backs up authentication messages to the /var/log/auth.log
/var/log/auth.log {
    rotate 180
    daily
    notifempty
    compress
    delaycompress
    endscript
}
```

Bonus: Check for Policy and File Violations

1. Command to verify `auditd` is active:

   systemctl status auditd

2. Command to set number of retained logs and maximum log file size:
   - Add the edits made to the configuration file below:

     sudo nano /etc/audit/auditd.conf

```
#
# 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 = 35
num_logs = 7
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
```

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

```
-w /et/shadow -p wa -k shadow
-w /etc/passwd -p wa -k passwd
```

4. Command to restart `auditd`:

sudo systemctl restart auditd

5. Command to list all `auditd` rule:

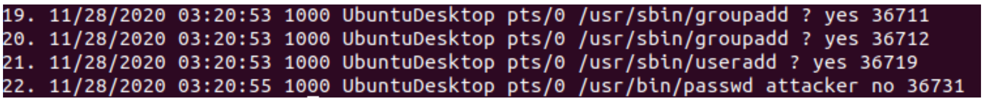
   sudo auditctl -l

6. Command to produce an audit report:

   sudo aureport -au

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

   sudo aureport -m



```
19. 11/28/2020 03:20:53 1000 UbuntuDesktop pts/0 /usr/sbin/groupadd ? yes 36711
20. 11/28/2020 03:20:53 1000 UbuntuDesktop pts/0 /usr/sbin/groupadd ? yes 36712
21. 11/28/2020 03:20:53 1000 UbuntuDesktop pts/0 /usr/sbin/useradd ? yes 36719
22. 11/28/2020 03:20:55 1000 UbuntuDesktop pts/0 /usr/bin/passwd attacker no 36731
```

8. Command to use `auditd` to watch `/var/log/cron`:

   sudo auditctl -w /var/log/cron

Command to verify `auditd` rules:

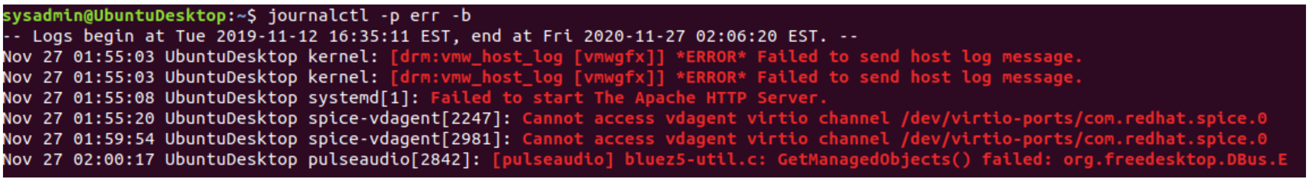
su auditctl -l

Bonus (Research Activity): Perform Various Log Filtering Techniques

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

   https://www.digitalocean.com/community/tutorials/how-to-use-journalctl-to-view-and-manipulate-systemd-logs#:~:text=By%20Priority&text=You%20can%20use%20journalctl%20to,filter%20out%20lower%20priority%20messages.&text=This%20will%20show%20you%20all%20messages%20marked%20as%20error%2C%20critical,the%20standard%20syslog%20message%20levels.

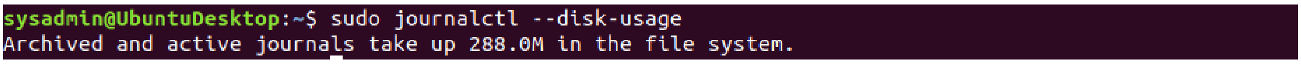
   journalctl -p err -b



```
sysadmin@UbuntuDesktop:~$ journalctl -p err -b
-- Logs begin at Tue 2019-11-12 16:35:11 EST, end at Fri 2020-11-27 02:06:20 EST. --
Nov 27 01:55:03 UbuntuDesktop kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log message.
Nov 27 01:55:03 UbuntuDesktop kernel: [drm:vmw_host_log [vmwgfx]] *ERROR* Failed to send host log message.
Nov 27 01:55:08 UbuntuDesktop systemd[1]: Failed to start The Apache HTTP Server.
Nov 27 01:55:20 UbuntuDesktop spice-vdagent[2247]: Cannot access vdagent virtio channel /dev/virtio-ports/com.redhat.spice.0
Nov 27 01:59:54 UbuntuDesktop spice-vdagent[2981]: Cannot access vdagent virtio channel /dev/virtio-ports/com.redhat.spice.0
Nov 27 02:00:17 UbuntuDesktop pulseaudio[2842]: [pulseaudio] bluez5-util.c: GetManagedObjects() failed: org.freedesktop.DBus.E
```

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

   sudo journalctl --disk-usage



```
sysadmin@UbuntuDesktop:~$ sudo journalctl --disk-usage
Archived and active journals take up 288.0M in the file system.
```

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

   journalctl --vacuum-files=2

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

   https://www.golinuxcloud.com/view-logs-using-journalctl-filter-journald/

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

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

```
0 0 * * * journalctl -p "0".."2" > /home/sysadmin/Priority_High.txt
```