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:
   ```
   Tar -xvf TarDocs.tar -C ~/Projects/
   ```
2. Command to **create** the Javaless_Doc.tar archive from the TarDocs/ directory, while excluding the TarDocs/Documents/Java directory:
   ```
   sudo tar -cvvf Javaless_Doc.tar --exclude "TarDocs/Documents/Java" TarDocs
   ```
3. Command to ensure Java/ is not in the new Javaless_Docs.tar archive:
   ```
   tar -tvf Javaless_Doc.tar | grep "Documents/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 -czvf logs_backup.tar.gz --list-   incremental==snapshot.file/var/log

Critical Analysis Question

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

You can’t extract a file from the archive and create a new archive file at the same time.

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 /auth_backup.tgz /var/log/auth.log
```

Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:
   ```
   Sudo mkdir -p ~/backup/{freeman,diskuse,openlist,freedisk}
   ```

```
#!/bin/bash
#Free memory output to a free_mem.txt file free -h > ~backups/freemem/free_mem.txt #Disk usage output to a
disk_usage.txt file du -h > ~/backups/disuse/disk_usage.txt
# List open files to a open_list.txt file lsof > ~/backups/openlist/open_list.txt # Free command to disk space to a
free_disk.txt file df -h >
~/backups/freedisk/free_disk.txt
```

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

Optional

- Commands to test the script and confirm its execution: sudo ./system.sh cat ~/backups/freedisk/ free_disk.txt

Bonus

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

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/auth.log { Weekly
Rotate 7 Notifempty Delaycompress missingok}
```

2. [Your logrotate scheme edits here]

Bonus: Check for Policy and File Violations

1. Command to verify auditd is active: systemctl status auditd