## 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 directory: **tar  -xzvf TarDocs.tar /home/Projects**

2. Command to **create** the `Javaless_Docs.tar` archive from the `TarDocs/` directory, while excluding the `TarDocs/Documents/Java` directory: **tar -cvvWf Javaless_Docs.tar epscript/ > Javaless_Docs.txt, or tar -czvf Javaless_Docs.tar TarDocs/ --exclude=TarDocs/Documents/Java**

3. Command to ensure `Java/` is not in the new `Javaless_Docs.tar` archive: **tar tvvf Javaless_Doc.tar | less, ls -l ~/Projects/TarDocs/Documents/**

**Bonus**
- Command to create an incremental archive called `logs_backup_tar.gz` with only changed files to `snapshot.file` for the `/var/log` directory: **tar cvvWf logs_backup_tar.gz –listed-incremental=epscript_backup.snar –level=0 lods_backup_tar.gz -C snapshot.file /var/log**

#### Critical Analysis Question

- Why wouldn't you use the options `-x` and `-c` at the same with `tar`? **The -x tar command is used to extract an archive and  -c is used to create one.**

---

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

1. Cron job for backing up the `/var/log/auth.log` file: **0 23 * * 5 tar cvf ~/var/log/auth.log_backup.tar.gz ~/var/log/auth.log**

---

### Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:  **mkdir -p Main/{Sub1,Sub2, Sub3, Sub4} or mkdir -p Main/”Sub”{1..4}”.sh**

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

```bash
#!/bin/bash
```

mkdir -p Main/{Sub1,Sub2, Sub3, Sub4}
```

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

**Optional**
- Commands to test the script and confirm its execution: ./system.sh

**Bonus**
- Command to copy `system` to system-wide cron directory: cp ~/etc/system >>

---

### 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:

   ```bash
  /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: s**ystemctl status auditd**

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:

   ```bash
num_logs = 10
max_log_file = 50
  ```

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:
  ```

  ```bash
  sudo nano /etc/audit/rules.d/auit.rules
-w /etc/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` rules: 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 useradd attacker, sudo aureport -m

8. Command to use `auditd` to watch `/var/log/cron`: sudo aureport -au, sudo -k

9. Command to verify `auditd` rules: sudo auditctl -l

---

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

1. Command to return `journalctl` messages with priorities from emergency to error: journalctl -p 3

1. Command to check the disk usage of the system journal unit since the most recent boot: journalctl –disk-usage, journalctl -b

1. Command to remove all archived journal files except the most recent two: sudo journlctl --vacuum-time=2

1. Comand to remove all archived journal files except the most recent two: `/home/sysadmin/Priority_High.txt`: sudo journlctl –vacum-time=-p{0..2}

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

  ```bash
  [Your solution cron edits here]
  ```

---