cd## 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:

1A. tar -xvvf ~/TarDocs.tar\

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

2A. tar -cvvWf Javaless\_Docs.tar --exclude=./Documents/Java. /TarDocs\ then hit enter and then hit enter again

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

3A. tar -tvvf Javaless\_Docs.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:

BONUS:

#### Critical Analysis Question

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

---

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

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

1A. crontab -e

1B. 0 6 \* \* 3 sudo tar -czf /auth\_backup.tgz /var/log/auth.log

### Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:

1A. mkdir -p ~/backups/{ freemem , diskuse , openlist , freedisk }

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

    ```bash

    #!/bin/bash

    # Logs free memory to ~/backups/freemem/free\_mem.txt

    free -h > ~/backups/freemem/free\_mem.txt

    # Logs Disk usage to ~/backups/diskuse/dick\_usage.txt

    df -h > ~/backups/diskuse/dick\_usage.txt

    # Logs Open files to ~/backups/openlist/open\_list.txt

    lsof > ~/backups/openlist/open\_list.txt

    # Logs Free disk space to ~/backups/freedisk/free\_disk.txt

    df -h > ~/backups/freedisk/free\_disk.txt

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

3A. chmod +x system.sh

\*\*Optional\*\*

- Commands to test the script and confirm its execution:

\*\*Bonus\*\*

- Command to copy `system` to system-wcron directory:

BONUS: 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:

    ```bash

# see "man logrotate" for details

# rotate log files weekly

weekly

# use the syslog group by default, since this is the owning group

# of /var/log/syslog.

su root syslog

# keep 4 weeks worth of backlogs

rotate 7

# create new (empty) log files after rotating old ones

notifyempty

# uncomment this if you want your log files compressed

delaycompress

# packages drop log rotation information into this directory

include /etc/logrotate.d

# no packages own wtmp, or btmp -- we'll rotate them here

/var/log/wtmp {

    missingok

    monthly

    create 0664 root utmp

    rotate 1

}

/var/log/btmp {

    missingok

    monthly

    create 0660 root utmp

    rotate 1

}

# system-specific logs may be configured here

### Bonus: Check for Policy and File Violations

1. Command to verify `auditd` is active:

1A. systemctl status auditd.service

2. Command to set number of retained logs and maximum log file size:

    - Add the edits made to the configuration file below:

    ```bash

    [Your solution edits here]

    ```

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

    [Your solution edits here]

    ```

4. Command to restart `auditd`:

4A. service auditd restart

5. Command to list all `auditd` rules:

5A. auditctl -l

6. Command to produce an audit report:

6A. aureport -k

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

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

8A. auditctl -w /var/log/cron -k shadow-file -p rwxa

9. Command to verify `auditd` rules:

9A. auditctl -l

---