Week 5 Homework Submission File: Archiving and Logging Data

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

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:
sudo tar -xvf TarDocs.tar
2. Command to **create** the `Javaless_Doc.tar` archive from the `TarDocs/` direc
tory, while excluding the `TarDocs/Documents/Java` directory:
sudo tar cvvWf Javaless_Docs.tar --
exclude "TarDocs/Documents/Java" TarDocs/Documents

3. Command to ensure `Java/` is not in the new `Javaless_Docs.tar` archive:
sudo tar -xvvf 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 cvvWF logs_backup_tar.gz --listed-incremental=test_backup.snar --
level=0 /var/log/snapshot.file

/var/log/usr.snar
Critical Analysis Question

- Why wouldn't you use the options `-x` and `-c` at the same with `tar`?
-x Reads files from the archive and writes them into the active file system.
-c Creates a new archive; therefor -x cannot read from an archive (-
c) that has not been created

Step 2: Create, Manage, and Automate Cron Jobs

1. Cron job for backing up the `/var/log/auth.log` file:
0 06 * * 3 tar -zcf /auth_backup.tgz /var/log/auth.log

Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:
mkdir backup {freemem,diskuse,openlist,freedisk}

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

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

# INSTRUCTIONS: Edit the following placeholder command and output filepaths
# For example: cpu_usage_tool > ~/backups/cpuuse/cpu_usage.txt
# The cpu_usage_tool is the command and ~/backups/cpuuse/cpu_usage.txt is the fil
epath
# In the above example, the `cpu_usage_tool` command will output CPU usage inform
ation into a `cpu_usage.txt$
# Do not forget to use the -
h option for free memory, disk usage, and free disk space

# Free memory output to a free_mem.txt f
echo "Free Memory $(free -h)" > ~/backups/freemem/free_mem.txt

# Disk usage output to a disk_usage.txt file
echo "Disk Usage $(du -h)" > ~/backups/diskuse/disk_usage.txt

# List open files to a open_list.txt file
echo "OpenFiles $(lsof -l)" > ~/backups/openlist/open_list.txt

# Free disk space to a free_disk.txt file
echo "Free Disk $(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 ./system.sh
Bonus
- Command to copy `system` to system-wide cron directory:
Xcopy /E var/spool/cron > /etc/cron ????

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 7
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:
nano auditd.conf

    - Add the edits made to the configuration file below:

    ```bash
    [#
# 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
]
```

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
## 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
syst]
```

4. Command to restart `auditd`:
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 criminal
sudo less audit.log

8. Command to use `auditd` to watch `/var/log/cron`:
-w /var/log/cron -p wa -k cron

9. Command to verify `auditd` rules:
sudo useradd criminal then check audit.log

---

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

1. Command to return `journalctl` messages with priorities from emergency to erro
r:
Priority=3
1. Command to check the disk usage of the system journal unit since the most rece
nt boot:
journalctl --disk-usage
1. Comand to remove all archived journal files except the most recent two:
sudo journalctl --vacuum-files=2

1. Command to filter all log messages with priority levels between zero and two,
and save output to `/home/sysadmin/Priority_High.txt`:
journalctl --priority=0..2 > /home/sysadmin/Priority_High.txt
1. Command to automate the last command in a daily cronjob. Add the edits made to
 the crontab file below:
crontab -e (to add to cron job)
    ```bash
    [# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
0 18 * * * mv ~/Downloads/doctors*.docx /usr/share/doctors
0 18 * * * mv ~/Downloads/patients*.txt /usr/share/patients
0 18 * * * mv ~/Downloads/treatments*.pdf /usr/share/treatments
0 06 * * 3 tar -zcf /auth_backup.tgz /var/log/auth.log
0 00 * * 7 journalctl --priority=0..2 > /home/sysadmin/Priority_High.txt

    ```

```