Cybersecurity

Module 5 Challenge Submission File

Archiving and Logging Data

Make a copy of this document to work in, and then for each step, add the solution command below the prompt. Save and submit this completed file as your Challenge deliverable.

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

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

```
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='Java' -cvvf Javaless_Docs.tar ~/Projects
```

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

```
tar tvf Javaless_Docs.tar | grep -i Java/
```

Critical Analysis Question

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

The -x is to extract files from an archive, while the -c is to create a tar file backup. You cannot extract and create at the same time, otherwise you will be undoing your work.

Step 2: Create, Manage, and Automate Cron Jobs

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

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

Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:

```
mkdir ~/backups/{freemem,diskuse,openlist,freedisk}ls
```

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

```
#!/bin/bash

# prints the amount of free memory on the system and saves it to
free.mem.txt
free -h | grep -i ‘free\|mem’ | awk ‘{print $1, “   ” $4}’ | sed -e
‘s/shared/free/g’ -e ‘s/total/     /g’ >> ~/backups/freemem/free_mem.txt

# prints disk usage and saves it to disk_usage.txt
du -h >> ~/backups/diskuse/disk_usage.txt

# lists all open files and saves it to open_list.txt
lsof >> ~/backups/openlist/open_list.txt

# prints file system diskspace statistics and saves it to free_disk.txt
df -h >> ~/backups/freedisk/free_disk.txt
```

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

```
sudo chmod +x system.sh
```

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`.

   a. Add your config file edits:

```
/var/log/auth.log {
weekly
rotate 7
notifempty
Delaycompress
Missingok
}
```