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:

```
Sudo tar xvf TarDocs.tar
```

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

```
sudo tar cvf Javaless_Docs.tar --exclude="TarDocs/Documents/Java" TarDocs
```

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

```
Tar -tvf Javaless_Docs.tar | grep Java
```

Bonus

4. 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 --listed-incremental=snapshot.file -cvzf logs_backup.tar.gz
/var/log
```

Critical Analysis Question

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

```
-c creates files and -x extracts files, you would not be able to run them
both 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 -zcfP 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 ~/backups/{freemem,diskuse,openlist,freedisk}
```

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

```
#!/bin/bash

free -h > ~/backups/freemem/free_mem.txt

du -h > ~/backups/diskuse/disk_usage.txt

lsof > ~/backups/openlist/open_list.txt

df -h > ~/backups/freedisk/free_disk.txt
```

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

```
Chmod +x system.sh
```

Optional

4. Commands to test the script and confirm its execution:

```
Sudo ./system.sh

cat ~/backups/freemem/free_mem.txt
cat ~/backups/diskuse/disk_usage.txt
cat ~/backups/openlist/open_list.txt
cat ~/backups/freedisk/free_disk.txt
```

Bonus

5. 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`.

   a. Add your config file edits:

```
/var/log/auth.log {
        rotate 7
        weekly
        notifempty
        delaycompress
```

```
        compress
        2> /dev/null
        endscript
}
```

Bonus: Check for Policy and File Violations

1. Command to verify `auditd` is active:

```
Systemctl is-enabled auditd
```

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

```
Sudo nano /etc/audit/audditd.conf
```

    Add the edits made to the configuration file:

```
num_logs = 7
Max_log_file = 35
```

3. Command using `auditd` to set rules for `/etc/shadow`, `/etc/passwd`, and `/var/log/auth.log`:

```
Sudo nano /etc/audit/rules.d/audit.rules
```

    Add the edits made to the `rules` file below:

```
-w /etc/passwd -p wra -k userpass_audit
-w /etc/shadow -p wra -k hashpass_audit
-w /var/log/auth.log -p wra -k authlog_audit
```

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 auditctl -w /var/log/cron
```

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:

```
sudo journalctl -b -p emerg..err
```

2. Command to check the disk usage of the system journal unit since the most recent boot:

```
sudo journalctl -b -u systemd-journald | less
```

3. Command to remove all archived journal files except the most recent two:

```
Sudo journalctl --vacuum-file=2
```

4. Command to filter all log messages with priority levels between zero and two, and save output to `/home/sysadmin/Priority_High.txt`:

```
sudo journalctl -p 0..2 > /home/sysadmin/Priority_High.txt
```

5. Command to automate the last command in a daily cron job. Add the edits made to the crontab file below:

```
0 22 * * 1-7 journalctl -p crit >> ~/home/sysadmin/Priority_High.txt
```