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_Doc.tar --exclude=TarDocs/Documents/Java ~/Projects
```

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

```
tar -tvf Javaless_Doc.tar | grep “Documents/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`?

-x extracts the tar file and -c creates a new backup so that would defeat the purpose

Step 2: Create, Manage, and Automate Cron Jobs

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

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

Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:

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

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

```
#!/bin/bash

free -h > ~/backups/freemem/free_mem.txt
df -h > ~/backups/diskuse/disk_usage.txt
lsof -h > ~/backups/openlist/open_list.txt
df -h > ~/backups/freedisk/free_disk.txt
```

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

```
sudo chmod 777 system.sh
```

Optional

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

```
Cd backups/freemem/free_mem.txt
Cd backups/diskuse/disk_usage.txt
Cd backups/openlist/open_list.txt
Cd 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 {weekly rotate 7 notifempty delaycompress}
```

Bonus: Check for Policy and File Violations

1. Command to verify `auditd` is active:

```
systemclt status auditd
```

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

```
sudo nano /etc/audit/auditd
```

Add the edits made to the configuration file:

```
Max_log_files = 35
Num_logs = 7
```

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

4. Command to restart `auditd`:

```
sudo systemctl restart auditd
```

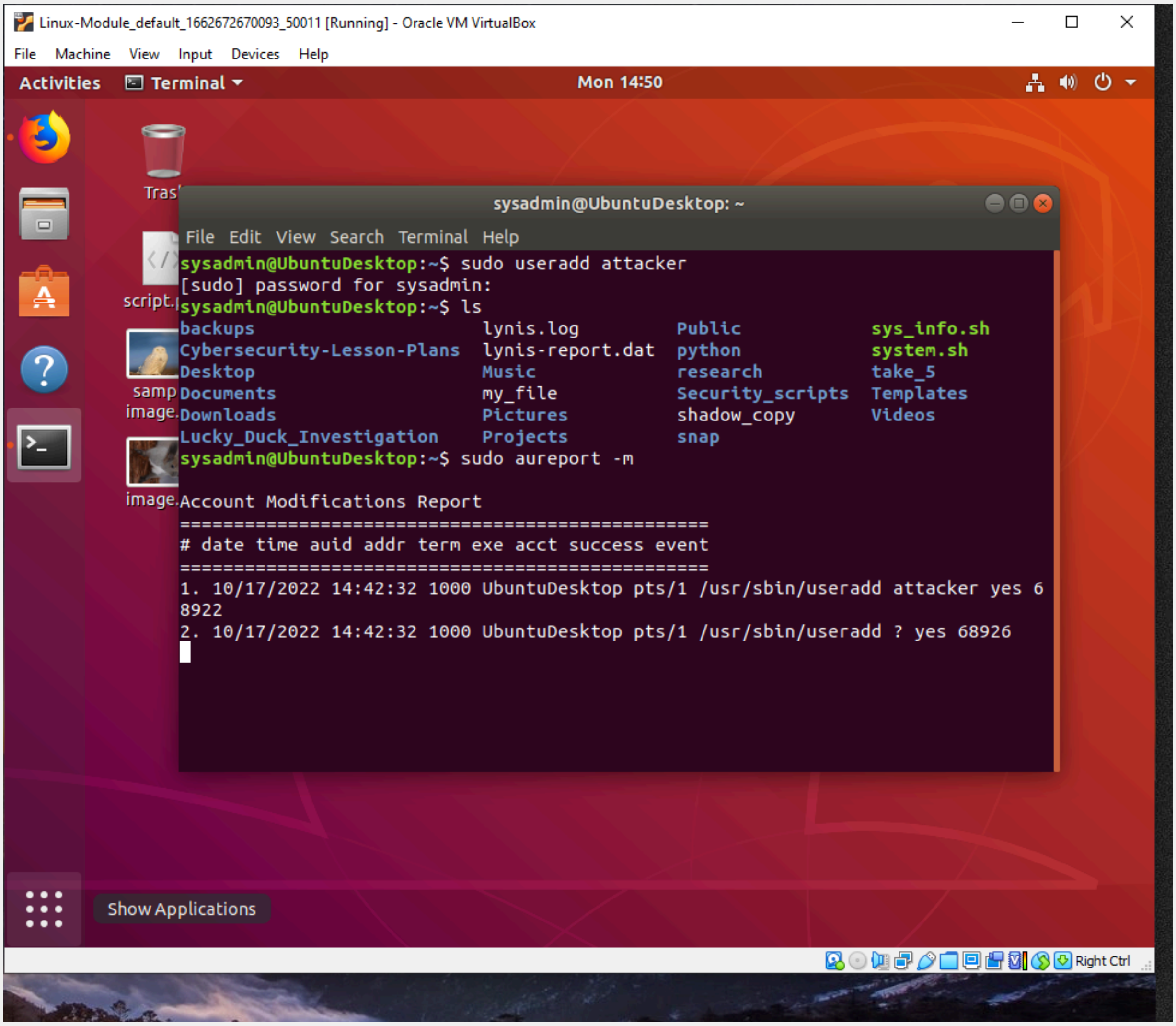
5. Command to list all `auditd` rules:

```
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:


Linux-Module_default_1662672670093_50011 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Mon 14:50
Tras
script.
samp
image.
image.
sysadmin@UbuntuDesktop: ~
File Edit View Search Terminal Help
Show Applications
Right Ctrl

```
sysadmin@UbuntuDesktop:~$ sudo useradd attacker
[sudo] password for sysadmin:
sysadmin@UbuntuDesktop:~$ ls
backups                     lynis.log         Public            sys_info.sh
Cybersecurity-Lesson-Plans  lynis-report.dat  python            system.sh
Desktop                     Music             research          take_5
Documents                   my_file           Security_scripts  Templates
Downloads                   Pictures          shadow_copy       Videos
Lucky_Duck_Investigation    Projects          snap
sysadmin@UbuntuDesktop:~$ sudo aureport -m

Account Modifications Report
=================================================
# date time auid addr term exe acct success event
=================================================
1. 10/17/2022 14:42:32 1000 UbuntuDesktop pts/1 /usr/sbin/useradd attacker yes 6
8922
2. 10/17/2022 14:42:32 1000 UbuntuDesktop pts/1 /usr/sbin/useradd ? yes 68926
```

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 -p emerg..err
```

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

```
df -h
```

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

```
sudo journalctl --vacuum-time=2d
```

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 -priority=(0,1,2) > /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 5 * * 1 sudo journalctl -priority=(0,1,2) >
/home/sysadmin/Priority_High.txt
```