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 -xf TarDocs.tar
```

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

```
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
```

Optional

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`?

   It is a conflict of interest because one command creates the file for the archive and then another command executes the tar.

Step 2: Create, Manage, and Automate Cron Jobs

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

```
0 6 * * 3 tar -czf /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 backup/{freedisk,openlist,diskuse,freemem}
```

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

```
#!/bin/bash

#Free Memory

sudo free -h > /home/sysadmin/projects/backup/freemem/free_mem.txt

#Disk Usage

sudo du -h > /home/sysadmin/projects/backup/diskuse/disk_usage.txt
```

```
#Open List

sudo lsof > /home/sysadmin/projects/backup/openlist/open_list.txt

#Free Disk Space Statistics

df -h > /home/sysadmin/projects/backup/freedisk/free_disk.txt
```

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

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

Optional

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

```
sudo ./system.sh
Or
sudo Sh system.sh
```

5. Command to copy `system` to system-wide cron directory:

```
sudo cp system.sh /etc/cron.d/
```

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:

```
# see "man logrotate" for details

/var/log/auth.log {

# rotate log files weekly
weekly

# use the adm group by default, since this is the owning group
# of /var/log/syslog.
su root adm

# keep 7 weeks worth of backlogs
rotate 7

# create new (empty) log files after rotating old ones
notifempty
missingok
# use date as a suffix of the rotated file
#dateext

# uncomment this if you want your log files compressed
#compress
delaycompress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may be also be configured here.
}
```

Optional Additional Challenge: Check for Policy and File Violations

1. Command to verify `auditd` is active:

```
systemctl status auditd
Or
sudo systemctl is-active auditd
```

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

```
sudo nano /etc/audit/auditd.conf
```

Add the edits made to the configuration file:

```
#
# 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
space_left = 75
space_left_action = SYSLOG
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
```

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

```
sudo nano /etc/audit/audit.rules
```

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

```
## First rule - delete all
-D
-w /etc/shadow -p wa -k hashpass_audit
-w /etc/passwd -p wa -k underpass_audit
-w /var/log/auth.log -p wa -k authlog_audit

## 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
```

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 ausearch -i
```

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

```
sudo useradd attacker
sudo ausearch -k attacker
```

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

```
sudo auditctl -w /var/log/cron -p wa -k watch_cron
```

9. Command to verify `auditd` rules:

```
sudo nano /etc/audit/audit.rules
Or list
sudo auditctl -l
```

Optional (Research Activity): Perform Various Log Filtering Techniques

1. Command to return `journalctl` messages with priorities from emergency to error:

```
sudo journalctl -p emergency..err
```

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

```
sudo journalctl --disk-usage
```

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

```
sudo journalctl --vacuum-files=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 0 * * * journalctl -p 0..2 > /home/sysadmin/Priority_High.txt

I added a new command to have it automate daily at midnight.
```