**Week 5 Homework Submission File: Archiving and Logging Data**

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

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:

Tar -xvf TarDocs.tar

1. Command to **create** the Javaless\_Doc.tar archive from the TarDocs/ directory, while excluding the TarDocs/Documents/Java directory:

tar cvf Javaless\_Docs.tar Google-Maps-Hacks/ Design-Patterns/ Music-Sheets/ c++interviewquestions.pdf/ IntelliJIDEA\_ReferenceCard.pdf/

1. Command to ensure Java/ is not in the new Javaless\_Docs.tar archive:

tar tf Javaless\_Docs.tar | grep -i Java

**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 cvf logs\_backup.tar.gz --listed-incremental=logs\_backup.snar --level=0 /var/log

**Critical Analysis Question**

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

-x is to extract a tar file and the -c is to create a file. You cannot extract a file unless it is made first and the product would be what you were trying to archive with tar prior to you doing anything with the information.

**Step 2: Create, Manage, and Automate Cron Jobs**

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

**\* 6 \* \* 3 tar cvf auth\_backup.tar /var/log/auth.log >/dev/null 2>&1**

**Step 3: Write Basic Bash Scripts**

1. Brace expansion command to create the four subdirectories:

mkdir {freemem,diskuse,openlist,freedisk}

1. Paste your system.sh script edits below:

#!/bin/bash

free -h >> ~/backups/freemem/free\_mem.txt

ls -lh >> ~/backups/diskuse/disk\_usage.txt

lsof >> ~/backups/openlist/open\_list.txt

df -h >> ~/backups/freedisk/free\_disk.txt

1. Command to make the system.sh script executable:

sudo chmod -x system.sh

**Optional**

* Commands to test the script and confirm its execution:

cat disk\_usage.txt

cat free\_disk.txt

cat free\_mem.txt

cat open\_list.txt

**Bonus**

* Command to copy system to system-wide cron directory:

**\* 4 \* \* 0 system.sh >/dev/null 2>&1**

**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:

[/var/log/auth.log {

weekly

rotate 7

notifempty

delaycompress

missingok

endscript

}]

**Bonus: Check for Policy and File Violations**

1. Command to verify auditd is active:

systemctl status auditd

1. Command to set number of retained logs and maximum log file size:
   * Add the edits made to the configuration file below:

[max\_log\_file = 35

num\_logs = 7]

1. 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:

[-w /etc/shadow -p wra -hashpass\_audit shadow

-w /etc/passwd -p wra -userpass\_audit passwd

-w /var/log/auth.log -p wra -authlog\_audit]

1. Command to restart auditd:

sudo systemctl restart auditd

1. Command to list all auditd rules:

sudo auditctl -l

1. Command to produce an audit report:

sudo aureport -au

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

1. 12/10/2021 08:30:37 1001 ubuntu-vm pts/0 /usr/sbin/useradd attacker yes 203

2. 12/10/2021 08:30:37 1001 ubuntu-vm pts/0 /usr/sbin/useradd ? yes 204

1. Command to use auditd to watch /var/log/cron:

-w /var/log/cron

1. Command to verify auditd rules:

auditctl –l

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

1. Command to return journalctl messages with priorities from emergency to error:
2. Command to check the disk usage of the system journal unit since the most recent boot:
3. Command to remove all archived journal files except the most recent two:
4. Command to filter all log messages with priority levels between zero and two, and save output to /home/sysadmin/Priority\_High.txt:
5. Command to automate the last command in a daily cronjob. Add the edits made to the crontab file below:

[Your solution cron edits here]