**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:

sudo tar -cvf Javaless\_Docs.tar --exclude /home/sysadmin/Projects/TarDocs/Documents/Java /home/sysadmin/Projects/TarDocs/Documents

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

tar --list -f Javaless\_Docs.tar | grep 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:

**Critical Analysis Question**

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

You wouldn’t use them at the same time because one command (-x) extracts the tar file’s contents, while the other (-c) creates it. This is not something you should do 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 sudo /home/sysadmin/Projects/auth\_backup.sh

Text

Description automatically generated

**Step 3: Write Basic Bash Scripts**

1. Brace expansion command to create the four subdirectories:

sudo mkdir /home/backups && sudo mkdir /home/backups/{freemem,diskuse,openlist,freedisk}

1. #!/bin/bash

[Your solution script contents here]

Text

Description automatically generated

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

Sudo chmod +x system.sh

**Optional**

* Commands to test the script and confirm its execution:

sudo ./system.sh

cat /home/backups/diskuse/disk\_usage.txt

**Bonus**

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

sudo cp system.sh /etc/cron.weekly/system

**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

rotation 7

notifempty

delaycompress

missingok

}

**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:

sudo nano /etc/audit/auditd.conf

* + 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:

[Your solution edits here]

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:

aureport –au

1. Create a user with sudo useradd attacker and produce an audit report that lists account modifications:
2. 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:

sudo journalctl -b -1 -p "emerg".."err"

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

sudo journalctl -b -u systemd -journald

1. Comand to remove all archived journal files except the most recent two:

journalctl --vacuum-time=2

1. 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

1. Command to automate the last command in a daily cronjob. Add the edits made to the crontab file below:

sudo cp /home/sysadmin/Priority\_High.sh /etc/cron.daily

#!/bin/bash @daily journalctl -p 0..2 >> /home/sysadmin/Priority\_High.txt