Step 1: Create, Extract, Compress, and Manage tar Backup Archives

Command to extract the TarDocs.tar archive to the current directory: tar -xvf ../Downloads/TarDocs

Command to create the Javaless\_Doc.tar archive from the TarDocs/ directory, while excluding the TarDocs/Documents/Java directory: tar cvs Javaless\_Docs.tar --exclude “Java” ~/Projects/TarDocs/Documents

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

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 with tar? Because when you create a file you can simply exclude the information you do not need, instead of extracting the whole file and moving it first to only remove it later. Also there is no need to specify that you are creating a new file from the extracted information because it would need to go somewhere new anyway.

Step 2: Create, Manage, and Automate Cron Jobs

Cron job for backing up the /var/log/auth.log file:tar -zcf /var/log/auth\_backup.tgz /var/log/auth.log

Step 3: Write Basic Bash Scripts

Brace expansion command to create the four subdirectories: mkdir -p ~/backups/{freemem,diskuse,openlist,freedisk}

Paste your system.sh script edits below:

#!/bin/bash

Mkdir -p ~/backups/{freemem,diskuse,openlist,freedisk}

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

Du -h > ~/backups/diskuse/disk\_usage.txt

Lsof -h > ~/backups/openlist/open\_list.txt

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

Command to make the system.sh script executable:chmod +x system.sh

Optional

Commands to test the script and confirm its execution:bash system.sh (then moved to directory diskuse and ran ‘less disk\_usage.txt’)

Bonus

Command to copy system to system-wide cron directory:

Step 4. Manage Log File Sizes

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 {

Missingok

Weekly

Delaycompress

Notifempty

Rotate7

}

Bonus: Check for Policy and File Violations

Command to verify auditd is active: sudo logrotate -vf /etc/logrotate.conf

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

Add the edits made to the configuration file below:

[Your solution edits here]

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]

Command to restart auditd:

Command to list all auditd rules:

Command to produce an audit report:

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

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

Command to verify auditd rules:

Bonus (Research Activity): Perform Various Log Filtering Techniques

Command to return journalctl messages with priorities from emergency to error:

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

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

Command to filter all log messages with priority levels between zero and two, and save output to /home/sysadmin/Priority\_High.txt:

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