HW 5 – Ivanderick Uy

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

1. Command to **extract** the TarDocs.tar archive to the current directory:

sudo tar xvvf TarDocs.tar -C ~/Projects/

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='TarDocs/Documents/Java' TarDocs

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

sudo tar tvf Javaless\_Docs.tar

Bonus

sudo tar cvvWf logs\_backup\_tar.gz --listed-incremental=snapshot.file.snar --level=0 /var/log

**Critical Analysis Question**

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

Well -x is to extract the files within the tar file and -c is to archive the files in a directory into a tar file, so they would be opposite commands.

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

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

0 18 \* \* 3 tar cvf auth\_backup.tgz ~/var/logs/auth.log

sudo gzip auth.log

**Step 3: Write Basic Bash Scripts**

1. Brace expansion command to create the four subdirectories:

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

1. Paste your system.sh script edits below:
2. #!/bin/bash

sudo cat /proc/meminfo | grep MemFree >> ~/backups/freemem/free\_mem.txt

sudo du >> ~/backups/diskuse/disk\_usage.txt

sudo lsof >> ~/backup/openlist/open\_list.txt

sudo df -h >> ~/backup/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:

sudo ./system.sh

**Bonus**

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

access cron directory: sudo nano /etc/crontab

0 0 \* \* 1 root ~/system.sh

**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.

/var/log/auth.log {

weekly

rotate 7

delaycompress

nocompress

missingok

}

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

1. Command to verify auditd is active:

systemctl is-enabled auditd