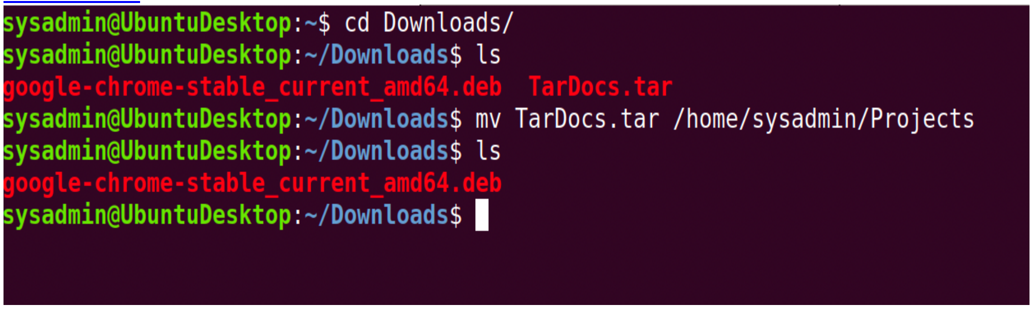
Week 5 Homework: Archiving and Logging Data

Lab Environment

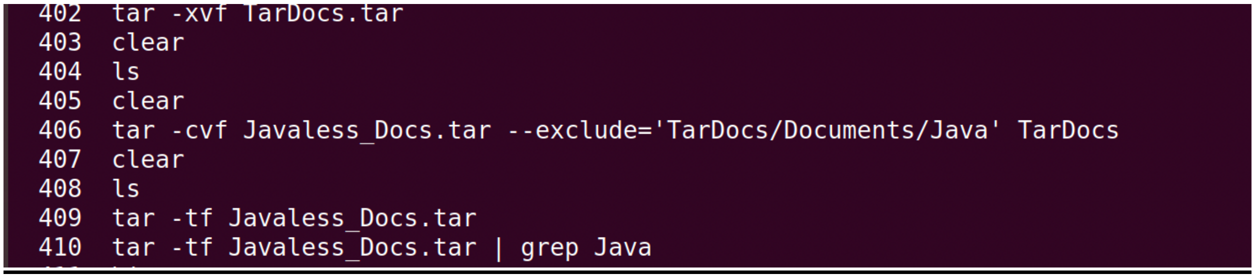
To set up your lab environment with the necessary files, complete the following steps.

- Log into your local virtual machine. Use the following credentials:
  - Username: sysadmin
  - Password: cybersecurity
- Open the terminal within your Ubuntu VM by pressing Ctrl+Alt+T for Windows users or Ctrl+Options+T for Mac users.
  - Alternatively, press Windows+A (Command+A for Mac users), type "Terminal" in the search bar, and select the terminal icon (not the Xfce Terminal icon).
- Create a directory called Projects in your /home/sysadmin/ directory.
- Download the following file (you can either slack it to yourself or use the Firefox browser in your Ubuntu machine), and move it to your ~/Projects directory before you get started:
  - TarDocs.tar



```
sysadmin@UbuntuDesktop:~$ cd Downloads/
sysadmin@UbuntuDesktop:~/Downloads$ ls
google-chrome-stable_current_amd64.deb  TarDocs.tar
sysadmin@UbuntuDesktop:~/Downloads$ mv TarDocs.tar /home/sysadmin/Projects
sysadmin@UbuntuDesktop:~/Downloads$ ls
google-chrome-stable_current_amd64.deb
sysadmin@UbuntuDesktop:~/Downloads$ 
```

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



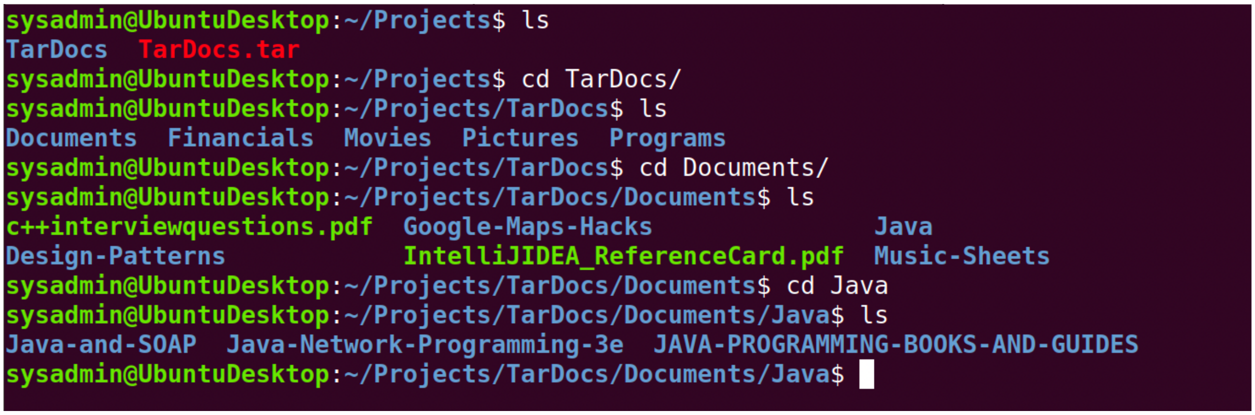
```
  402  tar -xvf TarDocs.tar
  403  clear
  404  ls
  405  clear
  406  tar -cvf Javaless_Docs.tar --exclude='TarDocs/Documents/Java' TarDocs
  407  clear
  408  ls
  409  tar -tf Javaless_Docs.tar
  410  tar -tf Javaless_Docs.tar | grep Java
```

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

   tar -xvf 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



```
sysadmin@UbuntuDesktop:~/Projects$ ls
TarDocs  TarDocs.tar
sysadmin@UbuntuDesktop:~/Projects$ cd TarDocs/
sysadmin@UbuntuDesktop:~/Projects/TarDocs$ ls
Documents  Financials  Movies  Pictures  Programs
sysadmin@UbuntuDesktop:~/Projects/TarDocs$ cd Documents/
sysadmin@UbuntuDesktop:~/Projects/TarDocs/Documents$ ls
c++interviewquestions.pdf  Google-Maps-Hacks              Java
Design-Patterns            IntelliJIDEA_ReferenceCard.pdf  Music-Sheets
sysadmin@UbuntuDesktop:~/Projects/TarDocs/Documents$ cd Java
sysadmin@UbuntuDesktop:~/Projects/TarDocs/Documents/Java$ ls
Java-and-SOAP  Java-Network-Programming-3e  JAVA-PROGRAMMING-BOOKS-AND-GUIDES
sysadmin@UbuntuDesktop:~/Projects/TarDocs/Documents/Java$ 
```

3. Command to ensure Java/ is not in the new Javaless_Docs.tar archive:

   tar -tf Javaless_Docs.tar | Java

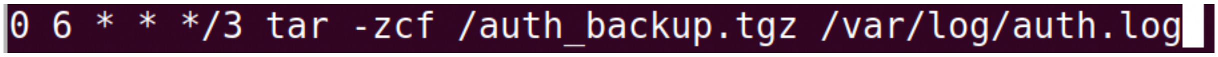
Critical Analysis Question

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

  C is not utilized during the extraction command with tar because we were not ls creating an archive then with the create command with tar because we are not extracting data.

Step 2: Create, Manage, and Automate Cron Jobs

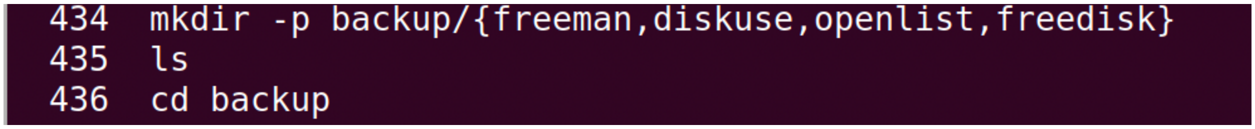
1. Cron job for backing up the /var/log/auth.log file:



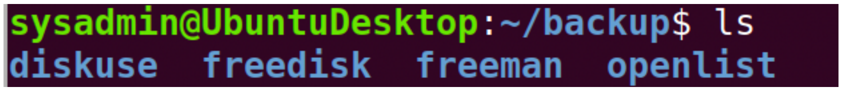
```
0 6 * * */3 tar -zcf /auth_backup.tgz /var/log/auth.log
```

Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:

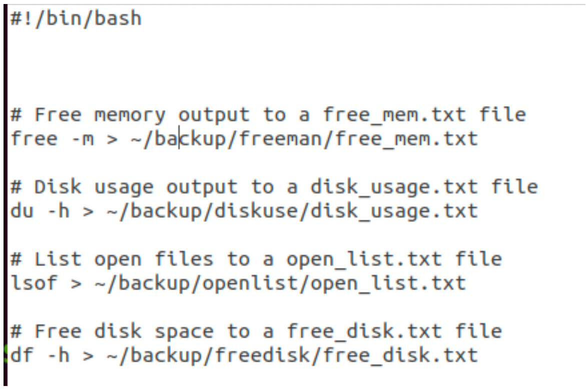


```
  434  mkdir -p backup/{freeman,diskuse,openlist,freedisk}
  435  ls
  436  cd backup
```



```
sysadmin@UbuntuDesktop:~/backup$ ls
diskuse  freedisk  freeman  openlist
```

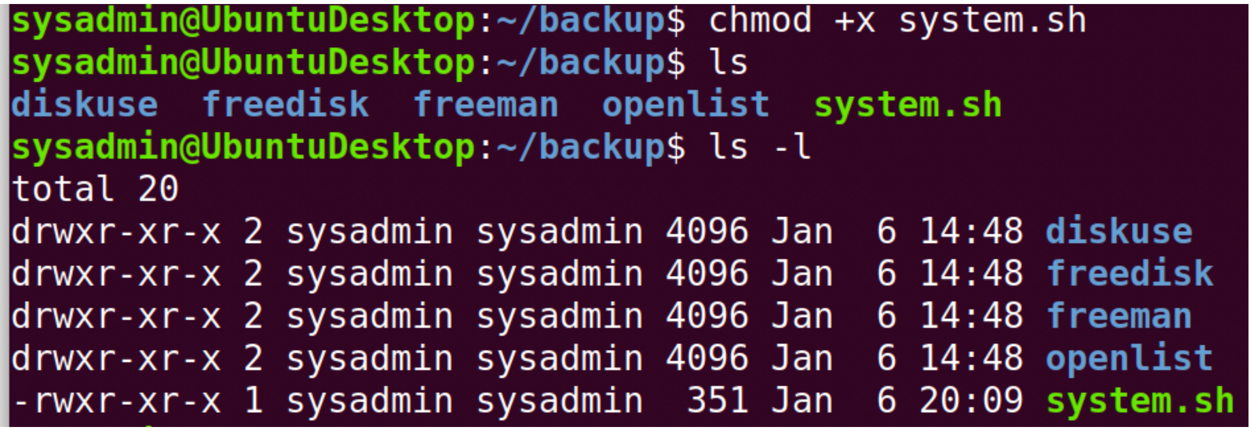
2. Paste your system.sh script edits below:



```
#!/bin/bash


# Free memory output to a free_mem.txt file
free -m > ~/backup/freeman/free_mem.txt

# Disk usage output to a disk_usage.txt file
du -h > ~/backup/diskuse/disk_usage.txt

# List open files to a open_list.txt file
lsof > ~/backup/openlist/open_list.txt

# Free disk space to a free_disk.txt file
df -h > ~/backup/freedisk/free_disk.txt
```

3. #!/bin/bash
   [Your solution script contents here]

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



```
sysadmin@UbuntuDesktop:~/backup$ chmod +x system.sh
sysadmin@UbuntuDesktop:~/backup$ ls
diskuse  freedisk  freeman  openlist  system.sh
sysadmin@UbuntuDesktop:~/backup$ ls -l
total 20
drwxr-xr-x 2 sysadmin sysadmin 4096 Jan  6 14:48 diskuse
drwxr-xr-x 2 sysadmin sysadmin 4096 Jan  6 14:48 freedisk
drwxr-xr-x 2 sysadmin sysadmin 4096 Jan  6 14:48 freeman
drwxr-xr-x 2 sysadmin sysadmin 4096 Jan  6 14:48 openlist
-rwxr-xr-x 1 sysadmin sysadmin  351 Jan  6 20:09 system.sh
```

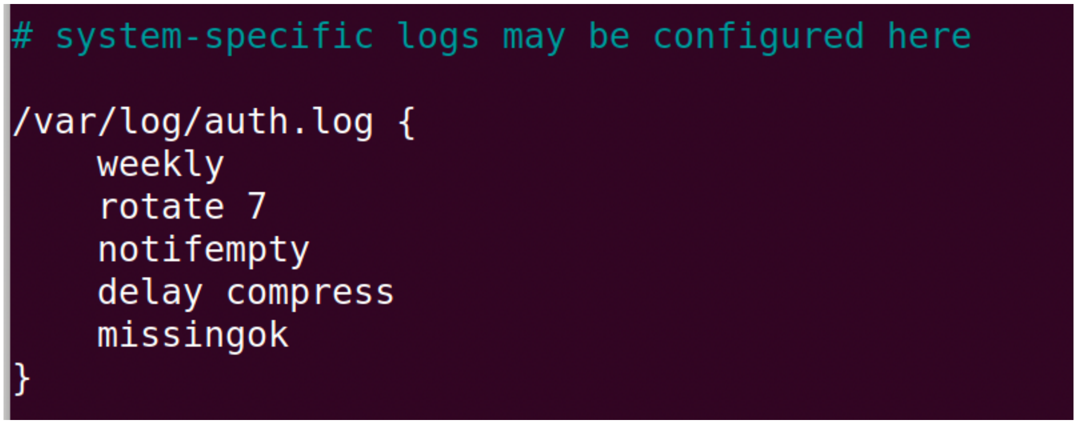
Step 4. Manage Log File Sizes

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.

   ○ Add your config file edits below:

   [Your logrotate scheme edits here]



```
# system-specific logs may be configured here

/var/log/auth.log {
    weekly
    rotate 7
    notifempty
    delay compress
    missingok
}
```