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=”Java” /home/sysadmin/Projects/TarDocs
3. Command to ensure Java/ is not in the new Javaless\_Docs.tar archive:
   * tar tvvf 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:
  + sudo tar --listed-incremental=snapshot.file.1 -cvzf logs\_backup\_tar.gz /var/log

**Critical Analysis Question**

* Why wouldn't you use the options -x and -c at the same time with tar?
  + Because they have different purposes -x extracts the file while -c creates a file

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

1. Cron job for backing up the /var/log/auth.log file:
   * 0 6 \* \* 3 tar -cvf auth\_backup.tar /var/log/auth.log > /auth\_backup.tgz

**Step 3: Write Basic Bash Scripts**

1. Brace expansion command to create the four subdirectories:
   * sudo mkdir -p ~/backups/{freemem,diskuse,openlist,freedisk}
2. Paste your system.sh script edits below:

#!/bin/bash

# Free memory output to a free\_mem.txt file

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

# Disk usage output to a disk\_usage.txt file

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

# List open files to a open\_list.txt file

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

# Free disk space to a free\_disk.txt file

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

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

**Optional**

* Commands to test the script and confirm its execution:
  + sudo ./system.sh
  + cd ~/backups/diskuse (to navigate to one of the subdirectories in the ~/backups/ directory)
  + ls (to list files in that subdiretory which is disk\_usage.txt)
  + cat disk\_usage.txt (to view the contents)

**Bonus**

* Command to copy system to system-wide cron directory:
  + sudo cp system.sh /etc/cron.weekly

**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 {

rotate 7

weekly

missingok

notifempty

compress

delaycompress

endscript

}

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

1. Command to verify auditd is active:
   * systemctl status auditd
2. 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 -k hashpass\_audit

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

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

1. Command to restart auditd:
   * sudo systemctl restart auditd
2. Command to list all auditd rules:
   * sudo auditctl -l
3. Command to produce an audit report:
   * sudo aureport -au
4. Create a user with sudo useradd attacker and produce an audit report that lists account modifications:
   * sudo aureport -m
5. Command to use auditd to watch /var/log/cron:
   * sudo auditctl -w /var/log/cron
6. Command to verify auditd rules:
   * sudo auditctl -l

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

1. Command to return journalctl messages with priorities from emergency to error:
   * journalctl -b -p "emerg".."err"
2. Command to check the disk usage of the system journal unit since the most recent boot:
   * journalctl --disk-usage -u system-journald
3. Comand to remove all archived journal files except the most recent two:
   * sudo journalctl --vacuum-time=2d
4. Command to filter all log messages with priority levels between zero and two, and save output to /home/sysadmin/Priority\_High.txt:
   * journalctl -p 0..2 > /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:

\* \* \* \* \* journalctl -p 0..2 > /home/sysadmin/Priority\_High.txt