**Week 5 Homework Submission File: Archiving and Logging Data: Henry Bartechko**

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:
   * **sysadmin@UbuntuDesktop:~/Projects$ tar xvf TarDocs.tar**
   * **sysadmin@UbuntuDesktop:~/Projects/TarDocs$ ls**
   * **Documents  Financials  Movies  Pictures  Programs**
2. Command to **create** the Javaless\_Doc.tar archive from the TarDocs/ directory, while excluding the TarDocs/Documents/Java directory:
   * **sysadmin@UbuntuDesktop:~/Projects$ tar -cf Javaless\_Docs.tar --exclude='Java' TarDocs**
3. Command to ensure Java/ is not in the new Javaless\_Docs.tar archive:
   * **sysadmin@UbuntuDesktop:~/Projects$ tar tf 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:
  + **sysadmin@UbuntuDesktop:~/Projects$ sudo tar -cf logs\_backup.tar.gz --listed-incremental=var\_log.snar --level=0 /var/log**
  + **sysadmin@UbuntuDesktop:~/Projects$ ls**
  + **Javaless\_Docs.tar  logs\_backup.tar.gz  TarDocs  TarDocs.tar  var\_log.snar**

**Critical Analysis Question**

* Why wouldn't you use the options -x and -c at the same with tar? **Because -x extracts an existing tar archive file, while -c creates a new tar archive file.**

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

1. Cron job for backing up the /var/log/auth.log file:
   * #Wednesday a backup of var/log/auth.log
   * **0 6 \* \* 3 sudo tar -czf auth\_backup.tgz  var/log/auth.log**

**Step 3: Write Basic Bash Scripts**

1. Brace expansion command to create the four subdirectories:
   * **sysadmin@UbuntuDesktop:~$ mkdir ~/backups**
   * **sysadmin@UbuntuDesktop:~$ mkdir ~/backups/{freemem,diskuse,openlist,freedisk}**
   * **sysadmin@UbuntuDesktop:~/backups$ ls**
   * **diskuse  freedisk  freemem  openlist**
2. Paste your system.sh script edits below:
   * **sysadmin@UbuntuDesktop:/home$ sudo nano system.sh**

**!/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 -h > ~/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:
   * **sysadmin@UbuntuDesktop:/home$ sudo chmod +x system.sh**

**Optional**

* Commands to test the script and confirm its execution:
  + **sysadmin@UbuntuDesktop:/home$ sudo sh system.sh**
  + **sysadmin@UbuntuDesktop:~/backups$ ls ~/backups/freemem**
  + **free\_mem.txt**
  + **sysadmin@UbuntuDesktop:~/backups$ ls ~/backups/diskuse**
  + **disk\_usage.txt**
  + **sysadmin@UbuntuDesktop:~/backups$ ls ~/backups/openlist**
  + **open\_list.txt**
  + **sysadmin@UbuntuDesktop:~/backups$ ls ~/backups/freedisk**
  + **free\_disk.txt**

**Bonus**

* Command to copy system to system-wide cron directory:
* **sysadmin@UbuntuDesktop:/home$ sudo cp ./system.sh /etc/cron.weekly**
* **sysadmin@UbuntuDesktop:/etc/cron.weekly$ ls**
* **0anacron  man-db  system.sh  update-notifier-common**

**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.

·         **sysadmin@UbuntuDesktop:/etc/cron.weekly$ sudo nano /etc/logrotate.conf**

* Add your config file edits below:

#log rotation scheme that backs up authentication messages to the /var/log/auth$

/var/log/auth.log {

     rotate 7

     weekly

     notifempty

     compress

     delaycompress

     nomissingok

     endscript

}

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

1. Command to verify auditd is active:
   * **sysadmin@UbuntuDesktop:/etc/cron.weekly$ systemctl status auditd**
2. Command to set number of retained logs and maximum log file size:
   * **sysadmin@UbuntuDesktop:/etc/cron.weekly$ sudo /etc/audit/auditd.conf**
   * Add the edits made to the configuration file below:

# This file controls the configuration of the audit daemon

#

local\_events = yes

write\_logs = yes

log\_file = /var/log/audit/audit.log

log\_group = adm

log\_format = RAW

flush = INCREMENTAL\_ASYNC

freq = 50

**max\_log\_file = 35**

**num\_logs = 7**

priority\_boost = 4

disp\_qos = lossy

dispatcher = /sbin/audispd

name\_format = NONE

Command using auditd to set rules for /etc/shadow, /etc/passwd and /var/log/auth.log:

**sysadmin@UbuntuDesktop:/etc$ sudo nano /etc/audit/rules.d/audit.rules**

* Add the edits made to the rules file below:

# rules to monitor /etc/shadow, /etc/passwd, /var/log/auth.log

-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: sysadmin@UbuntuDesktop:/etc$ sudo systemctl restart auditd**
2. Command to list all auditd rules: **sysadmin@UbuntuDesktop:/etc$ sudo auditctl -l**

-w /etc/shadow -p rwa -k hashpass\_audit

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

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

-w /usr -p wa -k usr

1. Command to produce an audit report: **sysadmin@UbuntuDesktop:/etc$ sudo aureport -au**
2. Create a user with sudo useradd attacker and produce an audit report that lists account modifications: **sysadmin@UbuntuDesktop:/etc$ sudo aureport -m**
   * **01/11/2021 11:15:19 1000 UbuntuDesktop pts/0 /usr/bin/passwd attacker yes 4289**
3. Command to use auditd to watch /var/log/cron: **-w /var/log/cron -p wra -k cron\_audit**
4. Command to verify auditd rules**: sysadmin@UbuntuDesktop:/etc$ sudo auditctl -l**

-w /etc/shadow -p rwa -k hashpass\_audit

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

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

-w /usr -p wa -k usr

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

1. Command to return journalctl messages with priorities from emergency to error:
   * **sysadmin@UbuntuDesktop:/etc$ journalctl -b -1  -p "emerg".."err"**
2. Command to check the disk usage of the system journal unit since the most recent boot:
   * **sysadmin@UbuntuDesktop:/etc$ journalctl -b -1  --disk-usage**
   * **Archived and active journals take up 280.0M in the file system.**
3. Command to remove all archived journal files except the most recent two:
   * **sysadmin@UbuntuDesktop:/etc$ sudo journalctl --vacuum-files=2**
4. Command to filter all log messages with priority levels between zero and two, and save output to /home/sysadmin/Priority\_High.txt:
   * **sysadmin@UbuntuDesktop:/etc$ journalctl  -p "0".."2" > /home/sysadmin/Priority\_High.txt**
   * **sysadmin@UbuntuDesktop:~$ ls**
   * another\_sys\_info.sh  Cybersecurity-Lesson-Plans  Documents  for\_loops.sh  Pictures       Projects  python research2 Templates
   * backups              Desktop                     Downloads  Music     **Priority\_High.txt**  Public **research  sys\_info.sh  Videos**
5. Command to automate the last command in a daily cronjob. Add the edits made to the crontab file below:
   * **sysadmin@UbuntuDesktop:/etc$ sudo nano Priority\_High.sh**

#!/bin/bash

#automate High\_Priority.txt

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

·         **sysadmin@UbuntuDesktop:/etc$ sudo chmod +x Priority\_High.sh**

·         **sysadmin@UbuntuDesktop:/etc$ ls cron.daily**

**00logwatch  apport      bsdmainutils  dpkg       man-db   popularity-contest  tripwire**

**0anacron apt-compat  chkrootkit        google-chrome  mlocate  Priority\_High.sh ubuntu-advantage-tools** **sysadmin@UbuntuDesktop:/etc$ ls cron.daily**

**00logwatch  apport      bsdmainutils  dpkg       man-db   popularity-contest  tripwire**

**0anacron apt-compat  chkrootkit        google-chrome  mlocate  Priority\_High.sh ubuntu-advantage-tools**

**apache2 aptitude    cracklib-runtime  logrotate  passwd   samba               update-notifier-common**

**apache2 aptitude    cracklib-runtime  logrotate  passwd   samba               update-notifier-common**

6.      Please fill out and submit SubmissionFile.md.