## Week 5 Homework Submission File: Archiving and Logging Data

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:
   * sudo tar -xf TarDocs.tar
2. Command to **create** the Javaless\_Doc.tar archive from the TarDocs/ directory, while excluding the TarDocs/Documents/Java directory:
   * tar -cvvWf Javaless\_Doc.tar --exclude=TarDocs/Docucuments/Java ./TarDocs
3. Command to ensure Java/ is not in the new Javaless\_Docs.tar archive:
   * tar -tf Javaless\_Docs.tar | grep -i 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 cvvzf ./logs\_backup.tar.gz --listed-incremental=snapshot.snar --level=0 /var/log #### Critical Analysis Question

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

* You would not use -x and -c together in a tar command because the -c flag is used to create a .tar file; the -x command is used to extract a .tar file

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

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

### Step 3: Write Basic Bash Scripts

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

* #!/bin/bash  
    
   free > ~/backups/freemem/free\_mem.txt  
   df > ~/backups/diskuse/disk\_usage.txt  
   lsof > ~/backups/openlist/open\_list.txt  
   df > ~/backups/freedisk/free\_disk.txt

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

**Optional**

Commands to test the script and confirm its execution:

- `./system.sh`

**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 {  
    weekly  
    rotate 7  
    notifempty  
    delaycompress  
    missingok  
    }

### 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
3. 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
4. Command to restart auditd:
   * sudo systemctl restart auditd
5. Command to list all auditd rules:
   * sudo auditctl -l
6. Command to produce an audit report:
   * sudo aureport -au
7. Create a user with sudo useradd attacker and produce an audit report that lists account modifications:

* sudo aureport -m  
  48. 07/25/2021 14:39:36 1000 UbuntuDesktop pts/0 /usr/sbin/useradd attacker yes 12496

1. Command to use auditd to watch /var/log/cron:
   * sudo auditctl -w /var/log/cron -p wra -k cron\_watch
2. 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:
   * sudo journalctl -b -0 -p 1
2. Command to check the disk usage of the system journal unit since the most recent boot:
   * sudo journalctl -b -0 --disk-usage
3. Comand to remove all archived journal files except the most recent two:
   * sudo journalctl --vacuum-file=2
4. Command to filter all log messages with priority levels between zero and two, and save output to /home/sysadmin/Priority\_High.txt:
   * sudo journalctl -b -0 -p 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:

* sudo crontab -e -u sysadmin  
    
  @daily sudo journalctl -b -0 -p 2 > /home/sysadmin/Priority\_High.txt

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.