## 

## **Todd Peralta**

## **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:

$ tar -xvf TarDocs.tar -C ~/Projects

1. Command to **create** the Javaless\_Doc.tar archive from the TarDocs/ directory, while excluding the TarDocs/Documents/Java directory:

$ tar cvvf Javaless\_Docs.tar --exclude="TarDocs/Documents/Java" TarDocs/

1. Command to ensure Java/ is not in the new Javaless\_Docs.tar archive:  
     
   $ tar tvvf Javaless\_Docs.tar | grep "Java"

#### **Critical Analysis Question**

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

You wouldn't want to extract and create at the same time.

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

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

$crontab -e

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:

$ mkdir -p Backups/{freemem,diskspace,openlist,freedisk}

Paste your system.sh script edits below:

#!/bin/bash

#2.1 Print out free memory

free -h > ~/Projects/TarDocs/Backups/freemem/freemem.txt

#2.2 Print out disk usage

du -h > ~/Projects/TarDocs/Backups/freedisk/diskspace.txt

#2.3 List all open files and save it.

lsof > ~/Projects/TarDocs/Backups/openlist/openlist.txt

#2.4 Print file system disk space statistics and save it to

df -h > ~/Projects/TarDocs/Backups/diskspace/diskspace.txt

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

**Optional**

* Commands to test the script and confirm its execution:

It worked by creating .txt files into the 4 sundirectories.

### **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

#compress

missingok

create}

### 

### 

### **I will come back to Bonus when I have more time on the weekend. :)**

### 

### 

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

1. Command to verify auditd is active:
2. Command to set number of retained logs and maximum log file size:  
   * Add the edits made to the configuration file below:
3. [Your solution edits here]
4. 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:
5. [Your solution edits here]
6. Command to restart auditd:
7. Command to list all auditd rules:
8. Command to produce an audit report:
9. Create a user with sudo useradd attacker and produce an audit report that lists account modifications:
10. Command to use auditd to watch /var/log/cron:
11. Command to verify auditd rules:

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

1. Command to return journalctl messages with priorities from emergency to error:
2. Command to check the disk usage of the system journal unit since the most recent boot:
3. Comand to remove all archived journal files except the most recent two:
4. Command to filter all log messages with priority levels between zero and two, and save output to /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: