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

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

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

* tar -xf TarDocs.tar

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

* tar --exclude=TarDocs/Documents/Java -cf Javaless\_Docs.tar TarDocs

1. Command to ensure Java/ is not in the new Javaless\_Docs.tar archive:

* tar -tf Javaless\_Docs.tar | grep -i java

**Bonus**

1. 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 -czf logs\_backup.tar.gz --listed-incremental=snapshot.file --level=0 /var/log

#### **Critical Analysis Question**

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

* Because they perform opposite operations. tar -x extracts an archive, while tar -c creates an archive.

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

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

* 0 6 \* \* 3 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 -p ~/backups/{freemem,diskuse,openlist,freedisk}

1. Paste your system.sh script edits below:

* #!/bin/bash

# Free memory

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

# Disk usage.

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

# List open files

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

# Free disk space

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

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

* chmod +x ./system.sh

**Optional**

1. Commands to test the script and confirm its execution:

* cd ~/backup
* cat freemem/free\_mem.txt
* cat diskuse/disk\_usage.txt
* cat openlist/open\_list.txt
* cat freedisk/free\_disk.txt

**Bonus**

1. 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 the 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
8. Command to use auditd to watch /var/log/cron:
   * sudo auditctl -w /var/log/cron
9. 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 0..3

1. Command to check the disk usage of the system journal unit since the most recent boot:

* journalctl -b -u systemd-journald --disk-usage

1. Comand to remove all archived journal files except the most recent two:

* sudo journalctl --vacuum-files=2

1. Command to filter all log messages with priority levels between zero and two, and save the output to /home/sysadmin/Priority\_High.txt:

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

1. Command to automate the last command in a daily cronjob. Add the edits made to the crontab file below: