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

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

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

· tar -xvvf TarDocs.tar

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

· ﻿tar -cvvWf Javaless\_Docs.tar --exclude Documents/Java TarDocs

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

· ﻿tar -tvf Javaless\_Docs.tar | grep -i Java

**Critical Analysis Question**

* Why wouldn't you use the options -x and -c at the same with tar?
* The -x option is used to extract files from an achieve while the -c option is used to create a new archive. It would not make sense to use both operations at the same time with tar.

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

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

· Crontab -e

· #This cron job will back up auth.log to auth\_backup.tgz every Wednesday at 6am.

· 0 6 \* \* 3 tar czvf 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 output to a free\_mem.txt file

· free -h | awk ‘{print $1, $4}’ > ~/backups/freemem/freemem.log

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

· df -h | awk ‘{print $1, $3}’ > ~/backups/diskuse/diskuse.log

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

· losf > ~/backups/openlist/openlist.log

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

· df -h | awk ‘{print $1, $4}’ > ~/backups/freedisk/freedisk.log

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

· chmod +x system.sh

**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

notifempty

missingok

compress

delaycompress

endscript

}

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

1. Command to verify auditd is active:

· systemctl status auditd.service

1. Command to set number of retained logs and maximum log file size:
   * Add the edits made to the configuration file below:

· sudo nano /etc/audit/auditd.conf

· num\_logs = 7

· max\_log\_file = 35



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:

· sudo nano /etc/audit/rules.d/audit.rules

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

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

· -w /etc/passwd -p rwa -k authlog\_audit

1. Command to restart auditd:

· sudo systemctl restart auditd

1. Command to list all auditd rules: ﻿sudo auditctl -l
2. Command to produce an audit report: sudo aureport
3. Create a user with sudo useradd attacker and produce an audit report that lists account modifications:

· sudo adduser criminal

· sudo aureport -m

1. Command to use auditd to watch /var/log/cron:

· auditctl -w /var/log/cron

1. Command to verify auditd rules:

· auditctl -l