| Cybersecurity |
| --- |
| Module 5 Challenge Submission File |

## Archiving and Logging Data

Make a copy of this document to work in, and then for each step, add the solution command below the prompt. Save and submit this completed file as your Challenge deliverable.

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

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

| tar xvvf tar\_docs.tar |
| --- |

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

| tar -cvf ~/Projects/Javaless\_Docs.tar --exclude=TarDocs/Documents/Java TarDocs/Documents/ |
| --- |

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

| tar -tf ~/Projects/Javaless\_Docs.tar | grep Java |
| --- |

#### Optional

1. Command to create an incremental archive called logs\_backup.tar.gz with only changed files to snapshot.file for the /var/log directory:

|  |
| --- |

#### Critical Analysis Question

1. Why wouldn't you use the options -x and -c 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:

| 0 6 \* \* 3 tar -cvzf /path/to/auth\_backup.tgz /var/log/auth.log |
| --- |

### Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:

| sudo mkdir -p /backups/{freemem,diskuse,openlist,freedisk} |
| --- |

1. Paste your system.sh script edits:

|  |
| --- |

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

| chmod +x system.sh |
| --- |

#### Optional

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

| I first used sudo nano system.sh  Disk usage and free disk had the same and open files was too big to fit  Than ran these commands  # Free memory output to a free\_mem.txt file  echo -e "Free memory available" && free -h > /home/sysadmin/backups/freemem/free\_mem.txt    # Disk usage output to a disk\_usage.txt file  echo -e "Disk space used" && df -h >> /home/sysadmin/backups/diskuse/disk\_usage.txt    # List open files to a open\_list.txt file  echo -e "Open files" && lsof > /home/sysadmin/backups/openlist/open\_list.txt  # Free disk space to a free\_disk.txt file  echo -e "Free disk space" && df -h > /home/sysadmin/backups/freedisk/free\_disk.txt |
| --- |

#### 

1. Command to copy system to system-wide cron directory:

| [Enter answer here] |
| --- |

### 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.

* 1. Add your config file edits:

| /var/log/auth.log{  Weekly  Rotate 7  Notifempty  Delaycompress  Missingok |
| --- |
| } |

### Optional Additional Challenge: Check for Policy and File Violations

1. Command to verify `auditd` is active:

| [Enter answer here] |
| --- |

1. Command to set number of retained logs and maximum log file size:

| [Enter answer here] |
| --- |

Add the edits made to the configuration file:

| [Enter answer here] |
| --- |

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

| [Enter answer here] |
| --- |

Add the edits made to the rules file below:

| [Enter answer here] |
| --- |

1. Command to restart auditd:

| [Enter answer here] |
| --- |

1. Command to list all auditd rules:

| [Enter answer here] |
| --- |

1. Command to produce an audit report:

| [Enter answer here] |
| --- |

1. Create a user with sudo useradd attacker and produce an audit report that lists account modifications:

| [Enter answer here] |
| --- |

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

| [Enter answer here] |
| --- |

1. Command to verify auditd rules:

| [Enter answer here] |
| --- |

#### 

### Optional (Research Activity): Perform Various Log Filtering Techniques

1. Command to return journalctl messages with priorities from emergency to error:

| [Enter answer here] |
| --- |

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

| [Enter answer here] |
| --- |

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

| [Enter answer here] |
| --- |

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

| [Enter answer here] |
| --- |

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

| [Your solution cron edits here] |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.