| 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:

| sysadmin@UbuntuDesktop:~/Projects$ tar xvvf TarDocs.tar |
| --- |

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

| sysadmin@UbuntuDesktop:~/Projects$ tar cvf Javaless\_Docs.tar --exclude="TarDocs/Documents/Java" TarDocs/ |
| --- |

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

| sysadmin@UbuntuDesktop:~/Projects$ tar tvf 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:

| sysadmin@UbuntuDesktop:~/Projects$ sudo tar --listed-incremental=snapshot.file -cvzf logs\_backup.tar.gz /var/log |
| --- |

#### Critical Analysis Question

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

You wouldn’t use the options ‘-x’ and ‘-c’ at the same time with ‘tar’ because ‘-x’ stands for ‘execute’ while ‘-c’ stands for ‘create’ and you cannot execute anything without it having already been created. In other words, a ‘tar’ file must be created first in order to execute the ‘tar’. So, they must not be used in the same command, but separately to achieve the proper result.

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

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

| sysadmin@UbuntuDesktop:~/Projects$ crontab -e  0 6 \* \* 3 tar -zcvf /auth\_backup.tgz /var/log/auth.log |
| --- |

### Step 3: Write Basic Bash Scripts

1. Brace expansion command to create the four subdirectories:

| sysadmin@UbuntuDesktop:~/Projects$ sudo mkdir -p ~/backups/{freemem,diskuse,openlist,freedisk} |
| --- |

1. Paste your system.sh script edits:

| sysadmin@UbuntuDesktop:~$ nano system.sh  —------------------------------------------------------------  #!/bin/bash  # Free memory output to a free\_mem.txt file  free -h > ~/backups/freemem/free\_mem.txt  # Disk usage output to a disk\_usage.txt file  du -h > ~/backups/diskuse/disk\_usage.txt  # Lists all open files and saves to a open\_list.txt file  ls -h > ~/backups/openlist/open\_list.txt  # System disk space output to a free\_disk.txt file  du -h > ~/backups/freedisk/free\_disk.txt |
| --- |

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

| sysadmin@UbuntuDesktop:~$ sudo chmod +x system.sh |
| --- |

#### 

#### 

#### Optional

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

| sysadmin@UbuntuDesktop:~$ cat ~/backups/freemem/free\_mem.txt  sysadmin@UbuntuDesktop:~$ cat ~/backups/diskuse/disk\_usage.txt  sysadmin@UbuntuDesktop:~$ cat ~/backups/openlist/open\_list.txt  sysadmin@UbuntuDesktop:~$ cat ~/backups/freedisk/free\_disk.txt |
| --- |

#### 

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

| sysadmin@UbuntuDesktop:~$ 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.

* 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:

| sysadmin@UbuntuDesktop:~$ systemctl status auditd |
| --- |

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

| sysadmin@UbuntuDesktop:~$ sudo nano /etc/audit/auditd.conf |
| --- |

Add the edits made to the configuration file:

| max\_log\_file = 35  num\_logs = 7 |
| --- |

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

| sysadmin@UbuntuDesktop:~$ sudo nano /etc/audit/rules.d/audit.rules |
| --- |

Add the edits made to the rules file below:

| ## New rules for shadow and passwd files  -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 |
| --- |

1. Command to restart auditd:

| sysadmin@UbuntuDesktop:~$ sudo systemctl restart auditd |
| --- |

1. Command to list all auditd rules:

| sysadmin@UbuntuDesktop:~$ sudo auditctl -l |
| --- |

1. Command to produce an audit report:

| sysadmin@UbuntuDesktop:~$ aureport -au |
| --- |

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

| sysadmin@UbuntuDesktop:~$ sudo useradd attacker  sysadmin@UbuntuDesktop:~$ sudo aureport -m  19. 05/02/2023 23:19:30 1000 UbuntuDesktop pts/0 /usr/sbin/useradd attacker yes 4853  20. 05/02/2023 23:19:30 1000 UbuntuDesktop pts/0 /usr/sbin/useradd ? yes 4857 |
| --- |

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

| sysadmin@UbuntuDesktop:~$ sudo auditctl -w /var/log/cron |
| --- |

1. Command to verify auditd rules:

| sysadmin@UbuntuDesktop:~$ sudo auditctl -l |
| --- |

#### 

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

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

|  |
| --- |

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

|  |
| --- |

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

|  |
| --- |

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

|  |
| --- |

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

|  |
| --- |

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