**﻿**LINUX COMMANDS: WK 4 Linux Systems Administration

Command to inspect permissions: ﻿**ls -l shadow**

Command to set permissions (if needed): ﻿**sudo chmod 600 shadow**

Command to inspect permissions: ﻿**ls -l gshadow**

Command to set permissions (if needed): **sudo chmod 600 gshadow**

Command to inspect permissions: **ls -l group**

Command to set permissions (if needed): **sudo chmod 644 group**

Command to inspect permissions: **ls -l passwd**

Command to set permissions (if needed): **sudo chmod 644 passwd**

Command to add each user account (include all five users): **sudo adduser sam**

Command to add admin to the sudo group: **sudo usermod -G sudo admin**

Command to add group: ﻿**sudo addgroup engineers**

Command to add users to engineers group (include all four users):

**sudo usermod -aG engineers sam**

**sudo usermod -G engineers joe**

Command to create the shared folder: ﻿**sudo mkdir /home/engineers**

Command to change ownership of engineer's shared folder to engineer group:

**sudo chown sysadmin:engineers /home/engineers**

Command to install Lynis: ﻿**sudo apt install lynis**

Command to see documentation and instructions: **man lynis; sudo lynis show help**

Command to run an audit: **sudo lynis audit system**

LINUX COMMANDS: WK 5 Archiving and Logging Data

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

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=Java ~/Projects/TarDocs/Documents/**

Command to ensure Java/ is not in the new Javaless\_Docs.tar archive: **tar tvf Javaless\_Docs.tar | grep Java**

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 czvf logs\_backup\_sun.tar.gz --listed-incremental=logs\_backup.snar --level=0 /var/log**

**sudo tar czvf logs\_backup\_mon.tar.gz --listed-incremental=logs\_backup.snar /var/log**

**sudo tar czvf logs\_backup\_tues.tar.gz --listed-incremental=logs\_backup.snar /var/log**

**etc**

Critical Analysis Question

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

**These options are used for completely different (opposing) commands.  The -x option is used to ‘extract’ a tar file whereas the -c option is used to ‘create’ a tar file.**

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 /var/log/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 below:

**﻿#!/bin/bash**

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

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

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

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

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

**sudo chmod +x system.sh**

**Optional**

* Commands to test the script and confirm its execution:

**sudo ./system.sh**

**cat ~/backups/freemem/free\_mem.txt**

**﻿cat ~/backups/diskuse/disk\_usage.txt**

**﻿cat ~/backups/openlist/open\_list.txt**

**﻿cat ~/backups/freedisk/free\_disk.txt**

**Bonus**

* 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 {**

**missingok**

**weekly**

**rotate 7**

**notifempty**

**compress**

**delaycompress**

**endscript**

**}**

Bonus: Check for Policy and File Violations

1. Command to verify auditd is active:

**systemctl status auditd**

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

﻿**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:

﻿**-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:

**sudo systemctl restart auditd**

1. Command to list all auditd rules:

**sudo auditctl -l**

1. Command to produce an audit report (**for all user authentications**):

﻿**sudo aureport -au**

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

**sudo aureport -m**

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

﻿**sudo auditctl -w /var/log/cron**

1. 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 (**NB homework instructions specify since the current system boot):**

﻿**sudo journalctl -p 3 -b**

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

﻿ **﻿sudo journalctl -u systemd-journald -b**

1. Command 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 output to /home/sysadmin/Priority\_High.txt:

﻿**sudo journalctl -p 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:

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

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.