```bash

#!/bin/bash

free -h > ~/backup/freemen/free\_mem.txt

du -h > ~/bacakups/diskuse/disk\_use.txt

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

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

```bash

[ GNU nano 2.9.3 /etc/logrotate.conf Modified

# see "man logrotate" for details

# rotate log files weekly

weekly

# use the syslog group by default, since this is the owning group

# of /var/log/syslog.

su root syslog

# keep 7 most reccent logs

Retain 7 most recent logs

# create new (empty) log files after rotating old ones

create

# uncomment this if you want your log files compressed

compress

# packages drop log rotation information into this directory

include /var/log/auth.log

# see "man logrotate" for details

# no packages own wtmp, or btmp -- we'll rotate them here

/var/log/wtmp {

missingok

monthly

create 0664 root utmp

rotate 1

}

/var/log/btmp {

missingok

monthly create 0660 root utmp

rotate 1

}

# system-specific logs may be configured here

/var/log/auth.log {

missingok

weekly

Do not rotate empty logs

Delay Compresion

Skip error messages from logs and continue to next log

1. Permissions on /etc/shadow should allow only root read and write access.
   * Command to inspect permissions: ﻿ls -l shadow
   * Command to set permissions (if needed): ﻿sudo chmod 600 /etc/shadow
2. Permissions on /etc/gshadow should allow only root read and write access.
   * Command to inspect permissions: ﻿ls -l gshadow
   * Command to set permissions (if needed): ﻿sudo chmod 600 /etc/gshadow
3. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.
   * Command to inspect permissions: ﻿ls -l group
   * Command to set permissions (if needed): ﻿sudo chmod 644 /etc/group
4. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.
   * Command to inspect permissions: ﻿ls -l passwd
   * Command to set permissions (if needed): sudo chmod 644 /etc/passwd

**Step 2: Create User Accounts**

1. Add user accounts for sam, joe, amy, sara, and admin.
   * Command to add each user account (include all five users):
   * sudo useradd sam
   * ﻿sudo useradd joe
   * ﻿sudo useradd amy
   * ﻿sudo useradd sara
   * ﻿sudo useradd admin
2. Ensure that only the admin has general sudo access.
   * Command to add admin to the sudo group: ﻿﻿sudo usermod -g sudo admin

**Step 3: Create User Group and Collaborative Folders**

1. Add an engineers group to the system.
   * Command to add group: ﻿sudo groupadd engineers
2. Add users sam, joe, amy, and sara to the managed group.
   * Command to add users to engineers group (include all four users):
   * ﻿﻿sudo usermod -g engineers sam
   * ﻿﻿sudo usermod -g engineers joe
   * ﻿﻿sudo usermod -g engineers amy
   * sudo usermod -g engineers sara
3. Create a shared folder for this group at /home/engineers.
   * Command to create the shared folder: ﻿sudo mkdir /home/engineers
4. Change ownership on the new engineers' shared folder to the engineers group.
   * Command to change ownership of engineer's shared folder to engineer group: ﻿
   * sudo chown :engineers /home/engineers

**Step 4: Lynis Auditing**

1. Command to install Lynis: ﻿sudo apt-get install lynis
2. Command to see documentation and instructions: man lynis
3. Command to run an audit: ﻿sudo lynis audit system
4. Provide a report from the Lynis output on what can be done to harden the system.

**Step 1: Shadow People**

1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:

* sudo adduser sysd -no-create-home

1. Give your secret user a password:

* Sudo passwd sysd

1. Give your secret user a system UID < 1000:

sudo usermod -u 900 sysd

1. Give your secret user the same GID:

usermod -u sudo sysd

1. Give your secret user full sudo access without the need for a password:

this is not needed

# Full privillage granted user

sysd ALL=(ALL:ALL) NOPASSWD:ALL

1. Test that sudo access works without your password:

sudo apt-get update

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file: sudo nano /etc/ssh/sshd\_config

# possible, but leave them commented. Uncommented options override the

# default value.

#Port 22

Port 2222

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:

sudo systemctl restart ssh

1. Exit the root account:
   * Logout

SSH to the target machine using your sysd account and port 2222:

ssh sysa@192.168.6.105 -p 2222

1. Use sudo to switch to the root user:

sudo su –

**Step 4: Crack All the Passwords**

1. SSH back to the system using your sysd account and port 2222:

ssh sysd@192.168.6.105 -p 2222

1. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:

Sudo su