## **Week 6 Homework Submission File: Advanced Bash - Owning the System**

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

**Step 1: Shadow People**

1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:  
   * Sudo useradd -r sysd
2. Give your secret user a password:  
   * Sudo passwd sysd … 123abc
3. Give your secret user a system UID < 1000:  
   * 998 generated with -r
4. Give your secret user the same GID:  
   * 998 generated with -r
5. Give your secret user full sudo access without the need for a password:  
   * sysd ALL(ALL:ALL) NOPASSWD:ALL
6. Test that sudo access works without your password:  
     
    Sudo -l

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:  
     
   nano /etc/ssh/ssh\_config (.... sshd config file)

Comment Port 22

Add “Port 2222”

Comment AddressFamily any

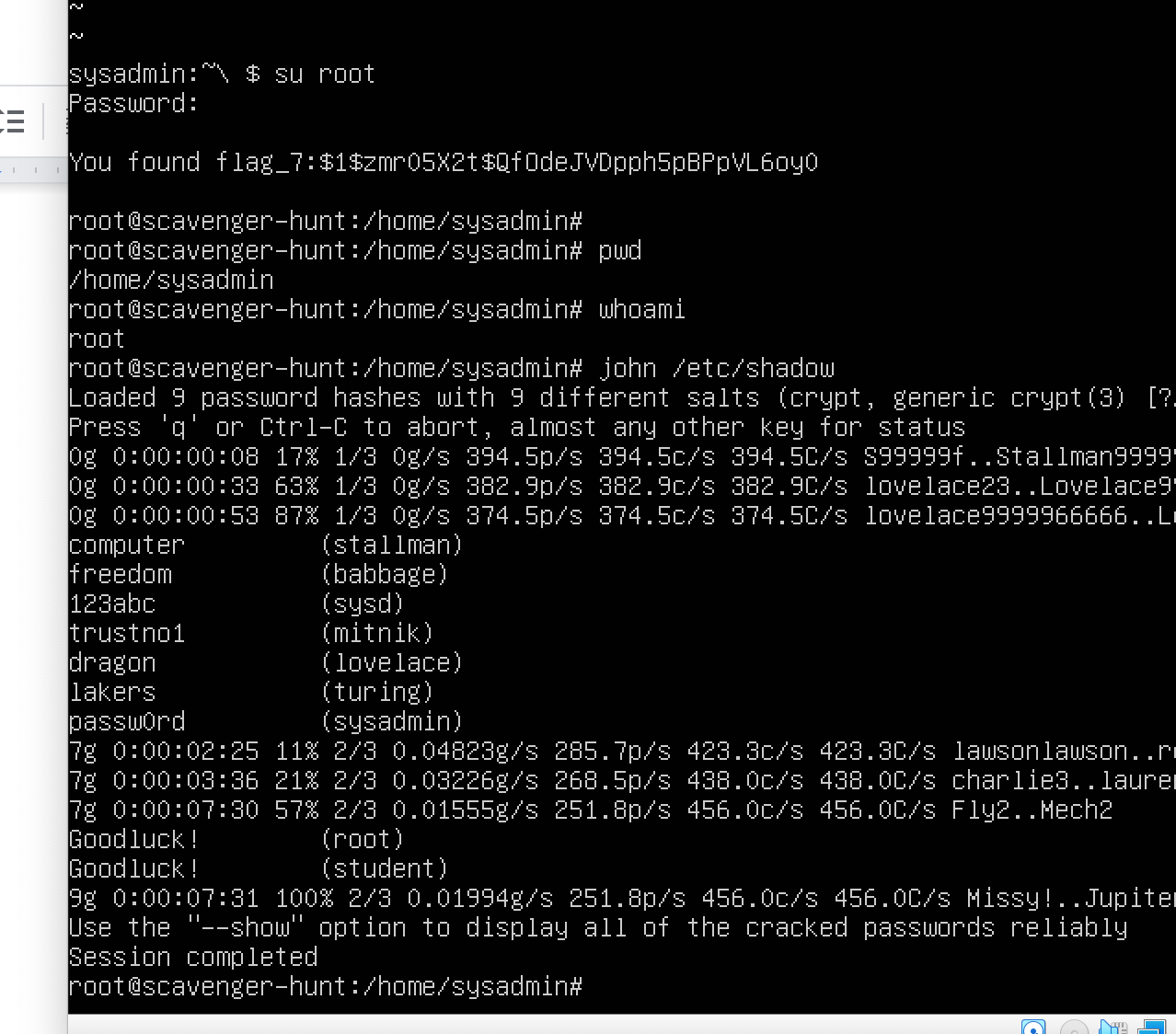
Comment ListenAddress 0.0.0.0

Comment ListenAddress ::

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:  
   * Sudo systemctl restart ssh.service
2. Exit the root account:
   * exit
3. SSH to the target machine using your sysd account and port 2222:
   * Different ip - 192.168.100.105
   * Ssh sysd@192.168.100.105 -p 2222 … from local host (not VM)
   * Password 123abc
   * Welcome screen
4. Use sudo to switch to the root user:  
   * Sudo su sysadmin … switched from $ to sysadmin:sysd\

**Step 4: Crack All the Passwords**

1. SSH back to the system using your sysd account and port 2222:  
   * Ssh sysd@192.168.100.105 -p 2222
2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:
   * John /etc/shadow
   * 

## 

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

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

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

1. Command to **extract** the TarDocs.tar archive to the current directory:  
   tar xvvf TarDcs..tar
2. Command to **create** the Javaless\_Doc.tar archive from the TarDocs/ directory, while excluding the TarDocs/Documents/Java directory:  
   Tar cvvf Javaless\_Docs.tar --exclude=’TarDocs/Documents/Java’ TarDocs/
3. Command to ensure Java/ is not in the new Javaless\_Docs.tar archive:

Tar -tvvf Javaless\_Docs.tar | grep “Java”

**Bonus**

* 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**

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

One is to create and the other is to extract.

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

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

0 6 \* \* 3 tar cvvf /auth\_backup.tgz /var/log/auth.log | gzip -t /auth\_backup.tgz ~/auth\_backup.txt

### **Step 3: Write Basic Bash Scripts**

1. Brace expansion command to create the four subdirectories:

Paste your system.sh script edits below:  
  
 #!/bin/bash

#! /bin/bash

#

#

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

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

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

du -h >> ~/backups/diskuse/diskusage.txt

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

Chmod +x ~/scripts.sh

**Optional**

* Commands to test the script and confirm its execution:

Sudo ./scripts.sh

/backups/freemem/less freemem.txt

**Bonus**

* Command to copy system to system-wide cron directory:

### **Step 4: Perform Various Log Filtering Techniques**

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

Journalctl -p 0..3

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

Journal ctl -b systemd-journald --disk-usage

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

Sudo journalctl --vacuum-files=2

**Bonus**

* Command to filter all log messages with priority levels between zero and two, and save output to /home/sysadmin/Priority\_High.txt:
* Command to automate the last command in a daily cronjob:
* Add the edits made to the crontab file below:  
    
   [Your solution cron edits here]

### **Step 5. Create Priority-Based Log Files**

1. Command to record all mail log messages, except for debug, to /var/log/mail.log:  
   * Add the edits made to the configuration file below:

mail.!debug /var/log/mail.log

**Bonus**

* Command to record all boot log messages, except for info and debug, to /var/log/boot.log:  
  + Add the edits made to the configuration file below:
* [Your solution edits here]

### **Step 6. 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 {

Weekly

Rotate 7

Notifempty

compress

Missingok

}

**# Week 4 Homework Submission File: Linux Systems Administration**

### Step 1: Ensure Permissions on Sensitive Files

1. Permissions on `/etc/shadow` should allow only `root` read and write access.

- Command to inspect permissions: ls -l /etc/passwd

- Command to set permissions (if needed): not needed

2. Permissions on `/etc/gshadow` should allow only `root` read and write access.

- Command to inspect permissions: ls -l /etc/passwd

- Command to set permissions (if needed): not needed

3. Permissions on `/etc/group` should allow `root` read and write access, and allow everyone else read$

- Command to inspect permissions: ls -l /etc/passwd

- Command to set permissions (if needed): not needed

4. Permissions on `/etc/passwd` should allow `root` read and write access, and allow everyone else rea$

- Command to inspect permissions: ls -l /etc/passwd

- Command to set permissions (if needed): not needed

sysadmin@UbuntuDesktop:/etc$ ls -l shadow

-rw------- 1 root shadow 2888 Jul 14 10:16 shadow

sysadmin@UbuntuDesktop:/etc$ ls -l gshadow

-rw------- 1 root shadow 1076 Jul 14 10:16 gshadow

sysadmin@UbuntuDesktop:/etc$ ls -l /etc/group

-rw-r--r-- 1 root root 1303 Jul 14 10:16 /etc/group

sysadmin@UbuntuDesktop:/etc$ ls -l /etc/passwd

-rw-r--r-- 1 root root 3207 Aug 22 11:56 /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): adduser sam, adduser joe, adduser amy$

2. Force users to create 16-character passwords incorporating numbers and symbols.

- Command to edit `pwquality.conf` file: sudo nano pwquality.conf

- Updates to configuration file:

# Minimum acceptable size for the new password (plus one if

# credits are not disabled which is the default). (See pam\_cracklib manual.)

# Cannot be set to lower value than 6.

minlen = 16

3. Force passwords to expire every 90 days.

- Command to to set each new user's password to expire in 90 days (include all five users):

sudo chage -M 90 sam

sudo chage -M 90 joe

sudo chage -M 90 amy

sudo chage -M 90 sara

sudo chage -M 90 admin

4. Ensure that only the `admin` has general sudo access.

- Command to add `admin` to the `sudo` group:

usermod -aG sudo admin

### Step 3: Create User Group and Collaborative Folder

1. Add an `engineers` group to the system.

- Command to add group:

addgroup engineers

2. Add users `sam`, `joe`, `amy`, and `sara` to the managed group.

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

usermod -aG engineers joe

usermod -aG engineers amy

usermod -aG engineers sam

usermod -aG engineers sara

3. Create a shared folder for this group at `/home/engineers`.

- Command to create the shared folder:

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:

chgrp -hR engineers engineers

5. Add the SGID bit and the sticky bit to allow collaboration between engineers in this directory.

- Command to set SGID and sticky bit to shared folder:

sudo chmod g+s,o+t engineers

### Step 4: Lynis Auditing

1. Command to install Lynis:

sudo apt-get install lynis

2. Command to see documentation and instructions:

sudo man lynis

3. Command to run an audit:

lynis audit system

4. Provide a report from the Lynis output on what can be done to harden the system.

- Screenshot of report output:

