

User Guide

In order to run this program:

- Run as root
- Install Python 3.8, Tkinter, Scapy, setproctitle, Crypto, subprocess, watchdog, pyxhook
- Make sure two machines wired in same network

Crypto

Make sure for client.py and server.py, they all have crypto.py in the same directory.

Victim- Server

Run server/victim as:

Python server.py

Each time the responds and result will be show on the console just for debug and analyze.

```
Message Received
Encrypted message: b'IVIVIVIVIVIVIVIV@k\xbd\x0e}D\xa0\xac\xeds!qZ\xab\xec\xdc
J\x9dI\x10\xeba\xba\x11K\xccL\xed\x9f'
AES decrypting
decrypted message: hello"echo echo hello > hi.sh
process title: hello
command: echo echo hello > hi.sh
No output
encoded output: b"IVIVIVIVIVIVIVIV\x1c'pR\xfa\n\xd5\xa8F[Ax\x00\xed\x96m\t\x9
6\xd5?\x96Z.\x08\xbcu\xec!3o\xf9\xaa\xfa.0\xcaa?\xa4\x16\xde\x9e\xa8\x85\xa2\
x85a0\xa0\xf7"
Packet sent
```

Attacker- Client

Put the victim/server machine IP address in the Destination IP field

Destination IP	<input type="text" value="10.0.0.33"/>
----------------	--

Put the attacker/client machine IP address in the Source IP field

Source IP	<input type="text" value="10.0.0.123"/>
-----------	---

Put the camouflaged title name in the Process Title field

Process Title	<input type="text" value="hello"/>
---------------	------------------------------------

Put the commands to executed in the victim machine in the Commands to send field

Commands to send	<input type="text" value="ifconfig"/>
------------------	---------------------------------------

Choose protocol, enter UDP or TCP

Protocol(UDP or TCP)

Then click Send Command button to send command

The Result will be showed in the dark gray area

Also, result will be showed in the console

File Monitoring

10.0.0.33

Put the attacker/client machine IP address in the Source IP field

10.0.0.123

Put the camouflaged title name in the Process Title field

Process Title

Put the commands to executed in the victim machine in the Commands to send field

Commands to send

Choose protocol, enter UDP or TCP

Protocol(UDP or TCP)

Enter file name

Watch File Name

Click Send button on the right side



The result will show on the console or in the local directory.

```
Monitoring
sent packet: b'E\x00\x00T\x00\
\x00P\x02 \x00\xf0\xd5\x00\x00
a\xc1\xdd\x1c\x1d\xf6 '
□
```

Keylogger

Put the victim/server machine IP address in the Destination IP field

Destination IP

Put the attacker/client machine IP address in the Source IP field

Source IP

Put the camouflaged title name in the Process Title field

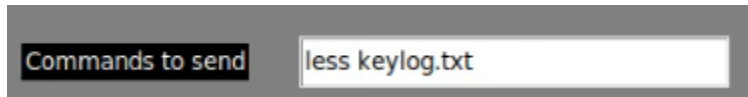
Process Title

Choose protocol, enter UDP or TCP

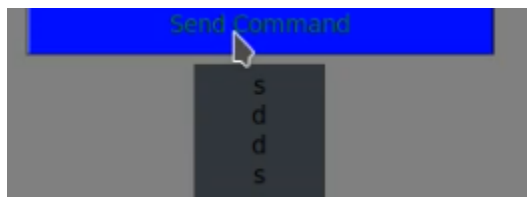
A screenshot of a web application interface. On the left, there is a label "Protocol(UDP or TCP)" in a black box. To its right is a white text input field containing the text "tcp".

Method 1

Type less command in the command field

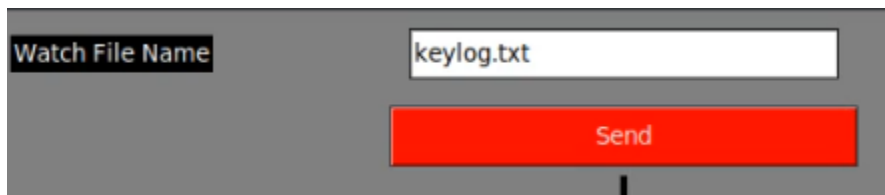
A screenshot of a web application interface. On the left, there is a label "Commands to send" in a black box. To its right is a white text input field containing the text "less keylog.txt".

The result will be shown on the application



Method 2

Type keylog.txt in the watch file name field. Then it will download keylogger file from the victim machine to the local directory.

A screenshot of a web application interface. On the left, there is a label "Watch File Name" in a black box. To its right is a white text input field containing the text "keylog.txt". Below the input field is a red button labeled "Send".