User Guide

In order to run this program:

- Run as root
- Install Python 3.8, Tkinter, Scapy, setprotitle, Crypto, subprocess
- Make sure two machines wired in same network, or port 8505 and 8000 are open on both machines

Crypto

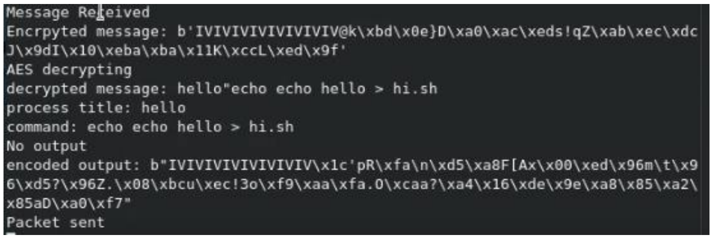
Make sure for client.py and server.py, they all have crypto.py in the same directory.

Victim- Server

Run server/victim as:

Python server.py

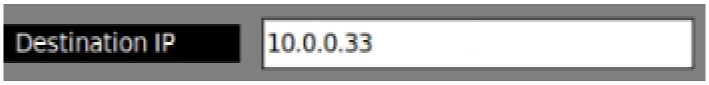
Each time the responds and result will be show on the console just for debug and analyze.



```
Message Received
Encrpyted 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\
x85aD\xa0\xf7"
Packet sent
```

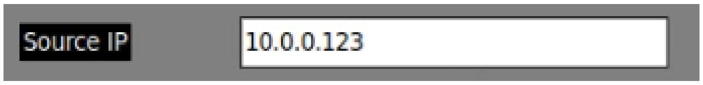
Attacker- Client

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



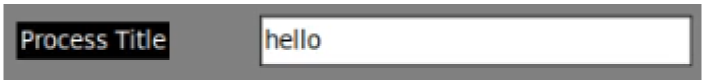
Destination IP 10.0.0.33

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



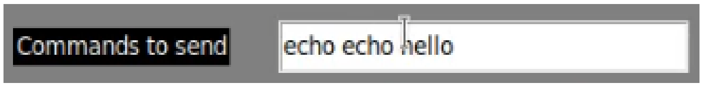
Source IP 10.0.0.123

Put the camouflaged title name in the Process Title field



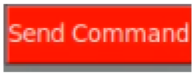
Process Title hello

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

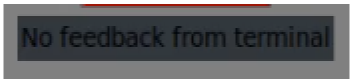


Commands to send echo echo hello

Then click Send Command button to send command

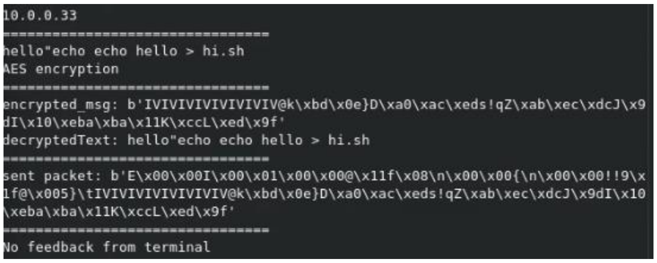


The Result will be showed in the dark gray area



No feedback from terminal

Also, result will be showed in the console



```
10.0.0.33
================================
hello"echo echo hello > hi.sh
AES encryption
================================
encrypted_msg: b'IVIVIVIVIVIVIVIV@k\xbd\x0e}D\xa0\xac\xeds!qZ\xab\xec\xdcJ\x9
dI\x10\xeba\xba\x11K\xccL\xed\x9f'
decryptedText: hello"echo echo hello > hi.sh
================================
sent packet: b'E\x00\x00I\x00\x01\x00\x00@\x11f\x08\n\x00\x00{\n\x00\x00!!9\x
1f@\x005}\tIVIVIVIVIVIVIVIV@k\xbd\x0e}D\xa0\xac\xeds!qZ\xab\xec\xdcJ\x9dI\x10
\xeba\xba\x11K\xccL\xed\x9f'
================================
No feedback from terminal
```