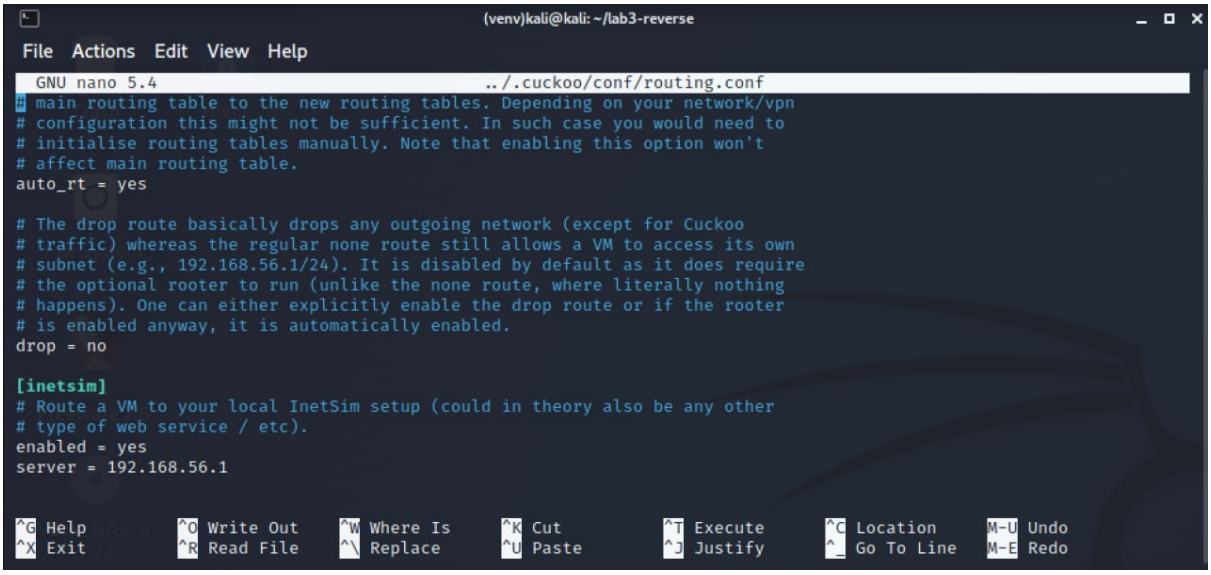
Лабораторна робота №5
Аналіз мережевих комунікацій

Виконав:
Студент 3 курсу ФТІ
групи ФІ-92
Поночевний Назар Юрійович
Варіант 6

Мета роботи
Отримати навички аналізу мережевих комунікацій ШПЗ.

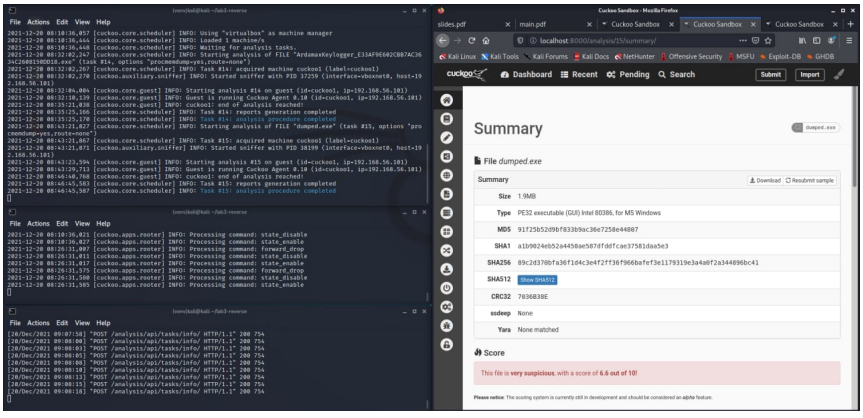
Завдання 1:
Додайте INetSim у Cuckoo Sandbox з розділу 3.3.1. Проаналізуйте 3-5 зразків з theZoo;

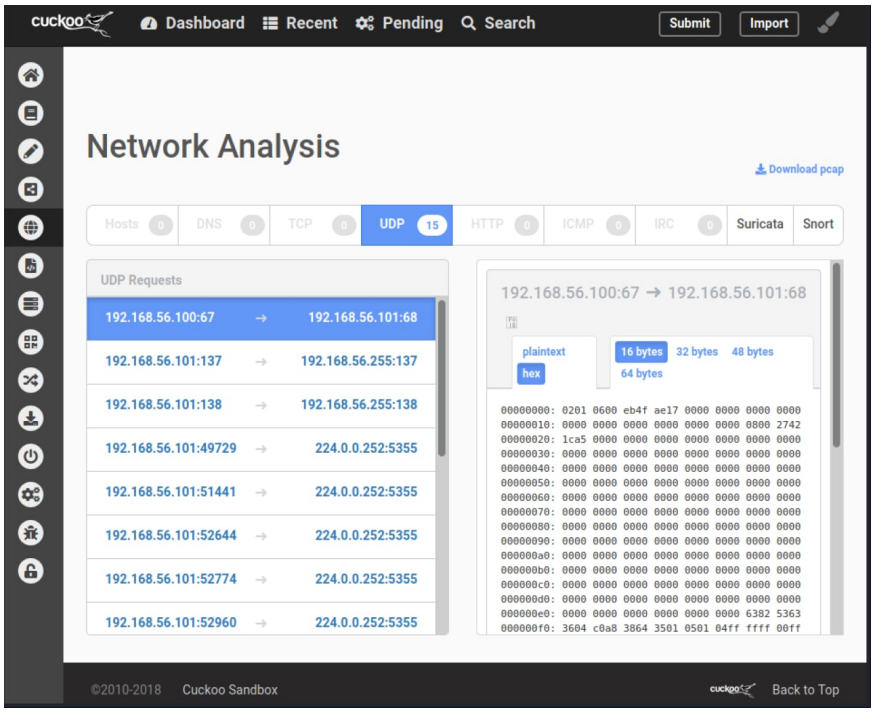
Спочатку під'єднати INetSim до Cuckoo:



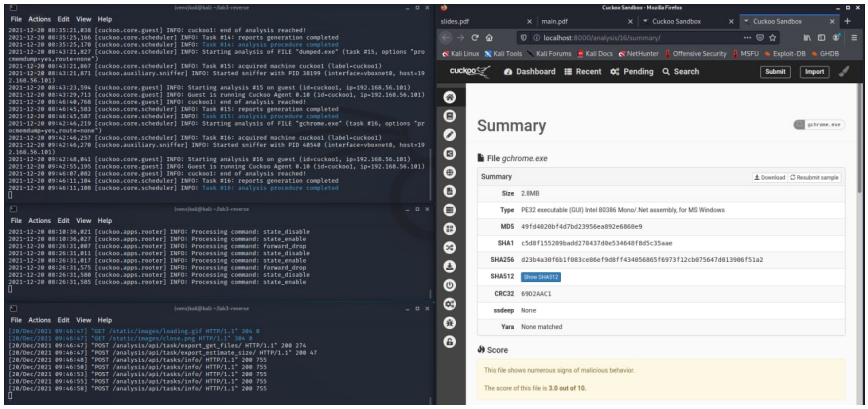
Тепер проаналізуємо зразки:

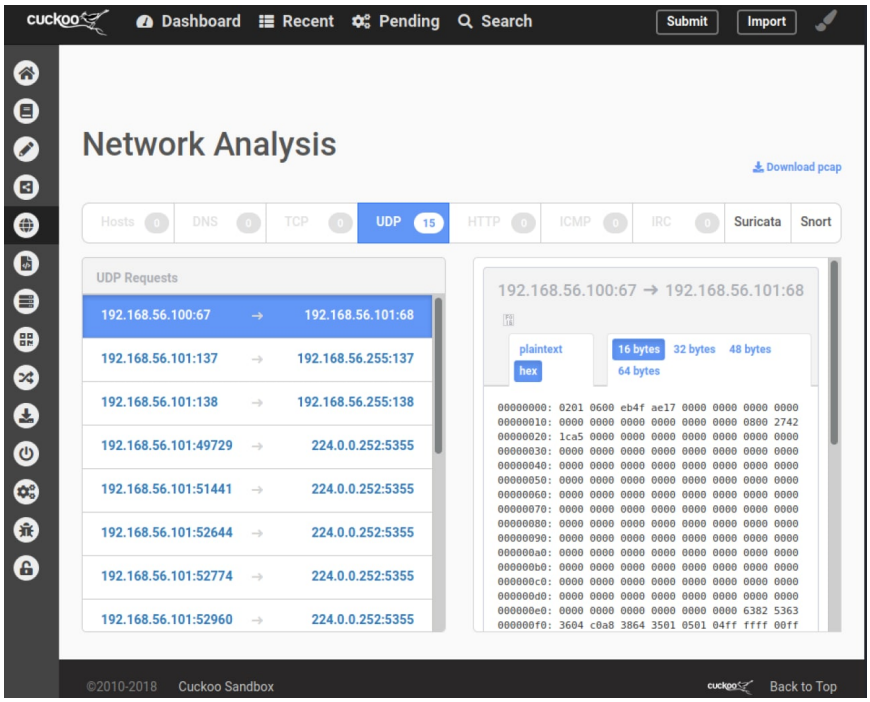
1) Kelihos



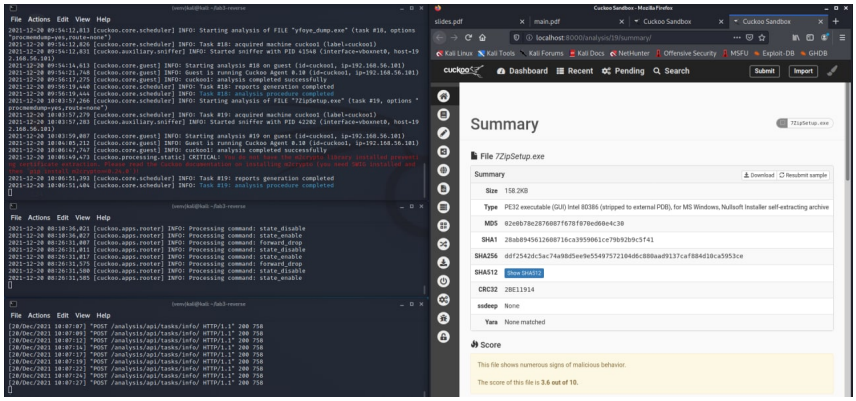

cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
Network Analysis
Download pcap
Hosts 0
DNS 0
TCP 0
UDP 15
HTTP 0
ICMP 0
IRC 0
Suricata
Snort
UDP Requests
192.168.56.100:67 → 192.168.56.101:68
192.168.56.101:137 → 192.168.56.255:137
192.168.56.101:138 → 192.168.56.255:138
192.168.56.101:49729 → 224.0.0.252:5355
192.168.56.101:51441 → 224.0.0.252:5355
192.168.56.101:52644 → 224.0.0.252:5355
192.168.56.101:52774 → 224.0.0.252:5355
192.168.56.101:52960 → 224.0.0.252:5355
192.168.56.100:67 → 192.168.56.101:68
plaintext
hex
16 bytes
32 bytes
48 bytes
64 bytes
00000000: 0201 0600 eb4f ae17 0000 0000 0000 0000
00000010: 0000 0000 0000 0000 0000 0000 0800 2742
00000020: 1ca5 0000 0000 0000 0000 0000 0000 0000
00000030: 0000 0000 0000 0000 0000 0000 0000 0000
00000040: 0000 0000 0000 0000 0000 0000 0000 0000
00000050: 0000 0000 0000 0000 0000 0000 0000 0000
00000060: 0000 0000 0000 0000 0000 0000 0000 0000
00000070: 0000 0000 0000 0000 0000 0000 0000 0000
00000080: 0000 0000 0000 0000 0000 0000 0000 0000
00000090: 0000 0000 0000 0000 0000 0000 0000 0000
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000
000000e0: 0000 0000 0000 0000 0000 0000 6382 5363
000000f0: 3604 c0a8 3864 3501 0501 04ff ffff 00ff
©2010-2018 Cuckoo Sandbox
Back to Top

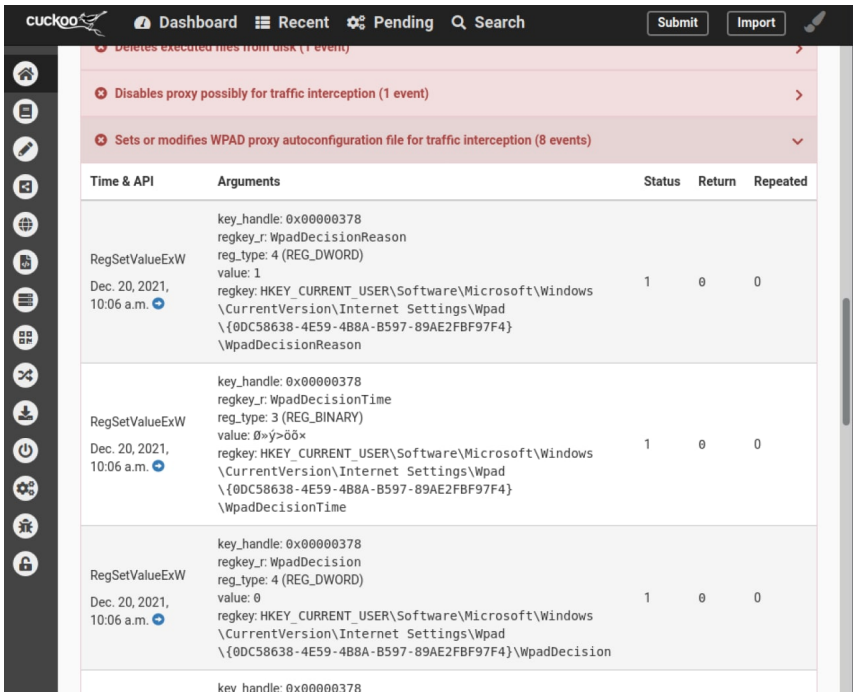
2) Proteus


Summary
File gchrome.exe
Size 2.8MB
Type PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
MD5 49fd4020bf4d7bd23956ea892e6860e9
SHA1 c5d8f155209bad627843fd0e534648f8d5c35aae
SHA256 d23b4a30f6b1f083ce86ef9d8ff4340586865f6973f12cb075647d013906f51a2
SHA512
CRC32 69D2AAC1
ssdeep None
Yara None matched
Score
This file shows numerous signs of malicious behavior.
The score of this file is 3.0 out of 10.


cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
Network Analysis
Download pcap
Hosts 0
DNS 0
TCP 0
UDP 15
HTTP 0
ICMP 0
IRC 0
Suricata
Snort
UDP Requests
192.168.56.100:67 → 192.168.56.101:68
192.168.56.101:137 → 192.168.56.255:137
192.168.56.101:138 → 192.168.56.255:138
192.168.56.101:49729 → 224.0.0.252:5355
192.168.56.101:51441 → 224.0.0.252:5355
192.168.56.101:52644 → 224.0.0.252:5355
192.168.56.101:52774 → 224.0.0.252:5355
192.168.56.101:52960 → 224.0.0.252:5355
192.168.56.100:67 → 192.168.56.101:68
plaintext
hex
16 bytes
32 bytes
48 bytes
64 bytes
00000000: 0201 0600 eb4f ae17 0000 0000 0000 0000
00000010: 0000 0000 0000 0000 0000 0000 0800 2742
00000020: 1ca5 0000 0000 0000 0000 0000 0000 0000
00000030: 0000 0000 0000 0000 0000 0000 0000 0000
00000040: 0000 0000 0000 0000 0000 0000 0000 0000
00000050: 0000 0000 0000 0000 0000 0000 0000 0000
00000060: 0000 0000 0000 0000 0000 0000 0000 0000
00000070: 0000 0000 0000 0000 0000 0000 0000 0000
00000080: 0000 0000 0000 0000 0000 0000 0000 0000
00000090: 0000 0000 0000 0000 0000 0000 0000 0000
000000a0: 0000 0000 0000 0000 0000 0000 0000 0000
000000b0: 0000 0000 0000 0000 0000 0000 0000 0000
000000c0: 0000 0000 0000 0000 0000 0000 0000 0000
000000d0: 0000 0000 0000 0000 0000 0000 0000 0000
000000e0: 0000 0000 0000 0000 0000 0000 6382 5363
000000f0: 3604 c0a8 3864 3501 0501 04ff ffff 00ff
©2010-2018 Cuckoo Sandbox
Back to Top

3) Somoto


Summary
File 7ZipSetup.exe
Score



Завдання 2:

Розгорніть OpenVPN за допомогою openvpn-install [102], робота за протоколом TCP. На стороні клієнта встановіть з'єднання з OpenVPN сервером через HTTP проксі. Проксі можна отримати за допомогою fetch-some-proxies [103] або онлайн сервісів;

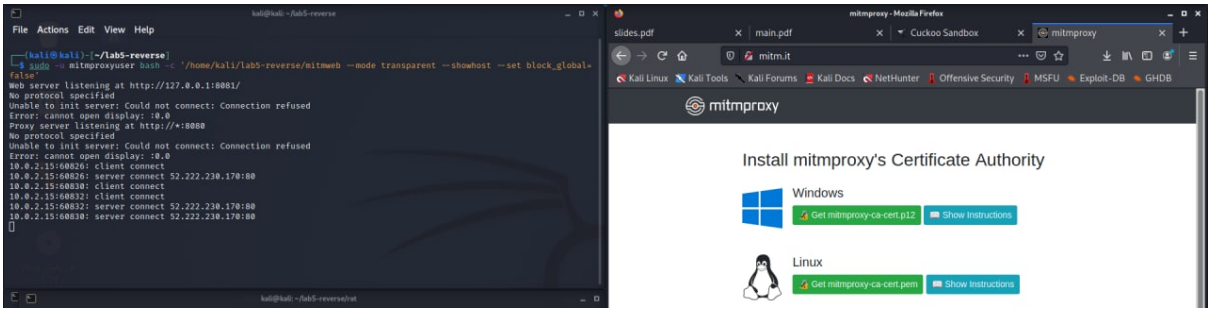
```
Select an option [1-2]: 1

Note: using Easy-RSA configuration from: /etc/openvpn/easy-rsa/vars
Using SSL: openssl OpenSSL 1.1.1l  24 Aug 2021
Generating an EC private key
writing new private key to '/etc/openvpn/easy-rsa/pki/easy-rsa-45100.GM9d1j/tmp.YBJJV5'
-----
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-45100.GM9d1j/tmp.U8q1Z1
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :ASN.1 12:'kali-vpn'
Certificate is to be certified until Mar 24 15:50:28 2024 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Client kali-vpn added.

The configuration file has been written to /home/kali/kali-vpn.ovpn.
Download the .ovpn file and import it in your OpenVPN client.

┌──(kali㉿kali)-[~/lab4-reverse]
└─$
```

```
┌──(kali㉿kali)-[~/lab5-reverse/fetch-some-proxies]
└─$ sudo python fetch.py
+-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-+
|f||e||t||c||h||s||o||m||e||p||r||o||x||i||e||s| ← v3.2.3
+-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-++-+

[i] initial testing ...
[i] retrieving list of proxies ...
[i] testing 2005 proxies (20 threads) ...

socks4://82.103.118.42:1099      # latency: 2.05 sec; country: Bulgaria; anonymity: elite (high)
socks4://188.163.170.130:35578   # latency: 1.21 sec; country: Ukraine; anonymity: elite (high)
http://152.136.39.231:80         # latency: 9.85 sec; country: China; anonymity: elite (high)
socks4://1.220.145.45:4145       # latency: 1.71 sec; country: South Korea; anonymity: elite (high)
http://131.255.239.38:3128       # latency: 1.81 sec; country: Brazil; anonymity: elite (high)
socks4://45.65.65.18:4145        # latency: 1.02 sec; country: Spain; anonymity: elite (high)
http://218.104.169.78:80         # latency: 1.53 sec; country: China; anonymity: elite (high)
http://200.17.137.40:3128        # latency: 2.25 sec; country: Brazil; anonymity: elite (high)
http://169.57.157.148:8123       # latency: 1.53 sec; country: United States; anonymity: elite (high)
http://183.220.195.170:80        # latency: 2.97 sec; country: China; anonymity: elite (high)
http://169.57.157.148:8123       # latency: 1.25 sec; country: United States; anonymity: elite (high)
```

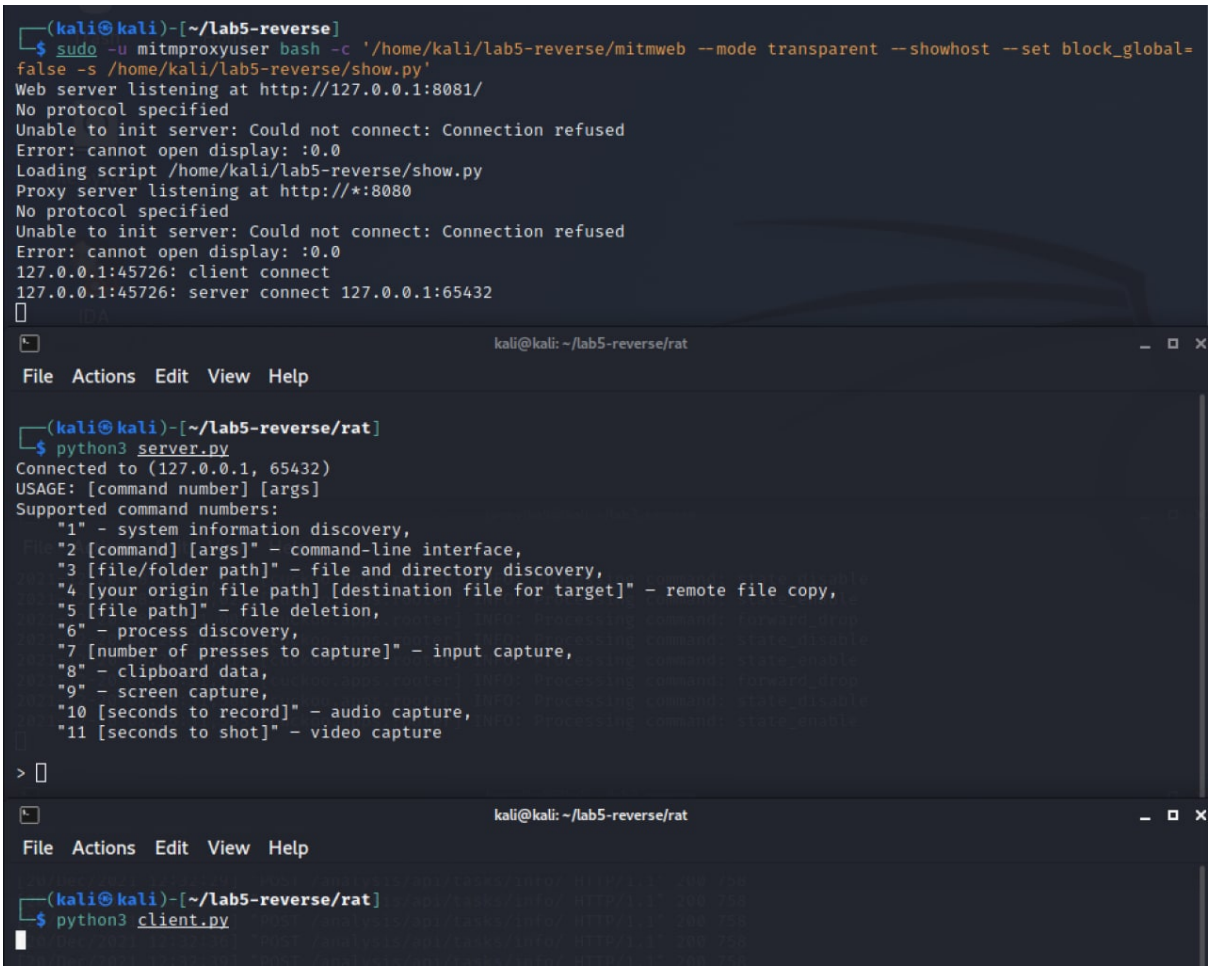
```
┌──(root💀kali)-[/home/kali/lab5-reverse]
└─# openvpn --config /home/kali/kali-vpn.ovpn --http-proxy 89.109.7.67 443                    1 ×
2021-12-20 11:27:46 Unrecognized option or missing or extra parameter(s) in /home/kali/kali-vpn.ovpn:18: block-outsi
de-dns (2.5.1)
2021-12-20 11:27:46 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEA
D] built on May 14 2021
2021-12-20 11:27:46 library versions: OpenSSL 1.1.1l  24 Aug 2021, LZO 2.10
2021-12-20 11:27:46 Outgoing Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
2021-12-20 11:27:46 Outgoing Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
2021-12-20 11:27:46 Incoming Control Channel Encryption: Cipher 'AES-256-CTR' initialized with 256 bit key
2021-12-20 11:27:46 Incoming Control Channel Encryption: Using 256 bit message hash 'SHA256' for HMAC authentication
2021-12-20 11:27:46 TCP/UDP: Preserving recently used remote address: [AF_INET]89.109.7.67:443
2021-12-20 11:27:46 Socket Buffers: R=[131072→131072] S=[16384→16384]
2021-12-20 11:27:46 Attempting to establish TCP connection with [AF_INET]89.109.7.67:443 [nonblock]
2021-12-20 11:27:46 TCP connection established with [AF_INET]89.109.7.67:443
2021-12-20 11:27:46 Send to HTTP proxy: 'CONNECT 5.181.248.224:1194 HTTP/1.0'
2021-12-20 11:27:46 Send to HTTP proxy: 'Host: 5.181.248.224'
```

Завдання 3:

Додайте сертифікат CA mitmproxy у список довірених на клієнті (розділ 5.3.4). Проаналізуйте трафік Вашого зразку з лабораторної роботи 4;




```
┌──(kali㉿kali)-[/tmp/mozilla_kali0]
└─$ sudo mv mitmproxy-ca-cert.pem /usr/local/share/ca-certificates/mitmproxy.crt

┌──(kali㉿kali)-[/tmp/mozilla_kali0]
└─$ sudo update-ca-certificates
Updating certificates in /etc/ssl/certs ...
1 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d ...

Adding debian:mitmproxy.pem
done.
done.
```


┌──(kali㉿kali)-[~/lab5-reverse]
└─$ sudo -u mitmproxyuser bash -c '/home/kali/lab5-reverse/mitmweb --mode transparent --showhost --set block_global=false -s /home/kali/lab5-reverse/show.py'
Web server listening at http://127.0.0.1:8081/
No protocol specified
Unable to init server: Could not connect: Connection refused
Error: cannot open display: :0.0
Loading script /home/kali/lab5-reverse/show.py
Proxy server listening at http://*:8080
No protocol specified
Unable to init server: Could not connect: Connection refused
Error: cannot open display: :0.0
127.0.0.1:45726: client connect
127.0.0.1:45726: server connect 127.0.0.1:65432

kali@kali: ~/lab5-reverse/rat
File Actions Edit View Help
┌──(kali㉿kali)-[~/lab5-reverse/rat]
└─$ python3 server.py
Connected to (127.0.0.1, 65432)
USAGE: [command number] [args]
Supported command numbers:
"1" - system information discovery,
"2 [command] [args]" - command-line interface,
"3 [file/folder path]" - file and directory discovery,
"4 [your origin file path] [destination file for target]" - remote file copy,
"5 [file path]" - file deletion,
"6" - process discovery,
"7 [number of presses to capture]" - input capture,
"8" - clipboard data,
"9" - screen capture,
"10 [seconds to record]" - audio capture,
"11 [seconds to shot]" - video capture
>

kali@kali: ~/lab5-reverse/rat
File Actions Edit View Help
┌──(kali㉿kali)-[~/lab5-reverse/rat]
└─$ python3 client.py