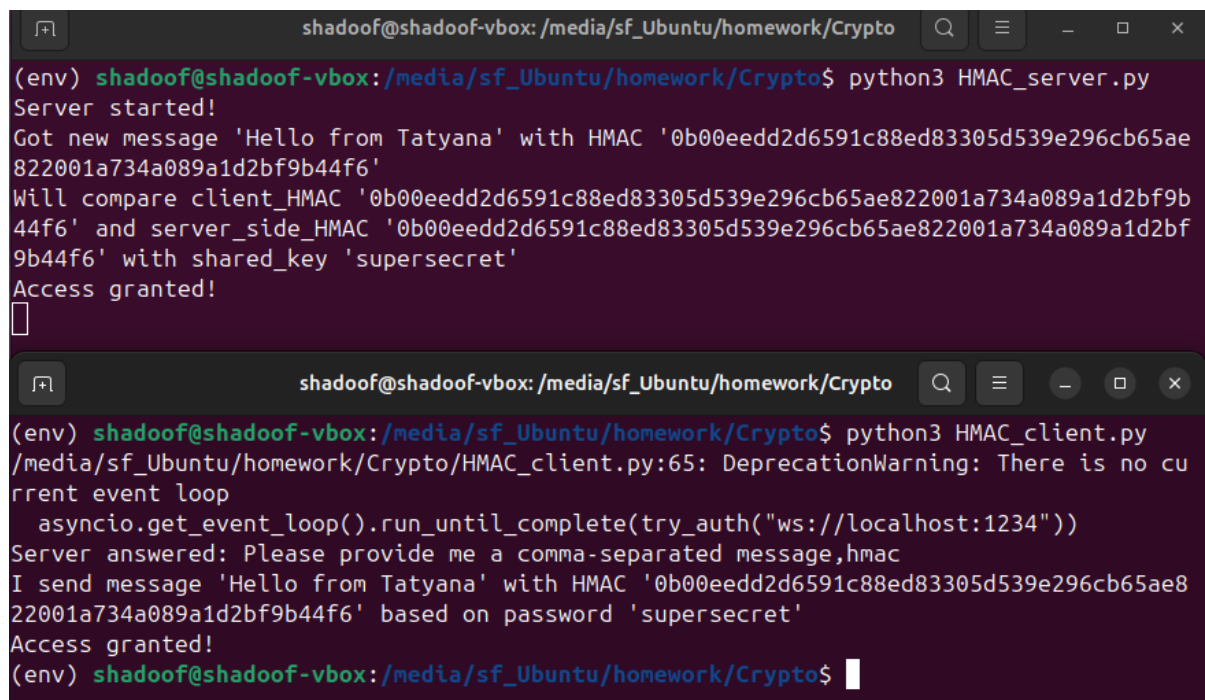


Перед началом проверки работоспособности создадим виртуальное окружение в домашней директории пользователя командой `python3 -m venv /env`. Далее активируем его командой `source env/bin/activate`. И перейдем в папку, в которой расположены все python-файлы к заданиям.

Также в виртуальном окружении выполним установку пакетов `websockets` и `scapy` командой `pip install <название_пакета>`.

Задание 1

Откроем два окна терминала, в одном запустим код сервера HMAC, в другом – клиента HMAC.



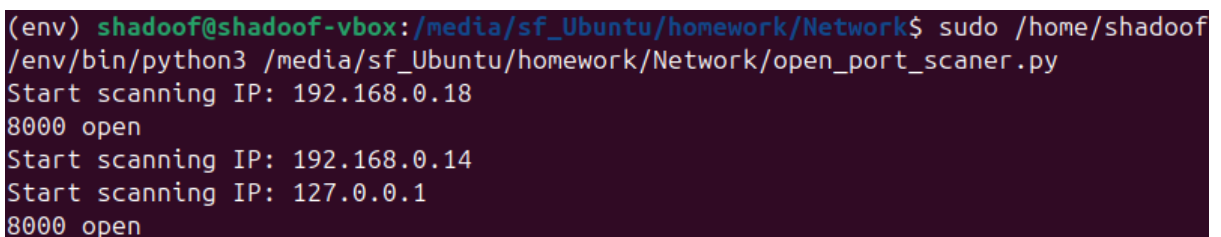
```
shadoof@shadoof-vbox: /media/sf_Ubuntu/homework/Crypto
(env) shadoof@shadoof-vbox: /media/sf_Ubuntu/homework/Crypto$ python3 HMAC_server.py
Server started!
Got new message 'Hello from Tatyana' with HMAC '0b00eedd2d6591c88ed83305d539e296cb65ae822001a734a089a1d2bf9b44f6'
Will compare client_HMAC '0b00eedd2d6591c88ed83305d539e296cb65ae822001a734a089a1d2bf9b44f6' and server_side_HMAC '0b00eedd2d6591c88ed83305d539e296cb65ae822001a734a089a1d2bf9b44f6' with shared_key 'supersecret'
Access granted!
█

shadoof@shadoof-vbox: /media/sf_Ubuntu/homework/Crypto
(env) shadoof@shadoof-vbox: /media/sf_Ubuntu/homework/Crypto$ python3 HMAC_client.py
/media/sf_Ubuntu/homework/Crypto/HMAC_client.py:65: DeprecationWarning: There is no current event loop
  asyncio.get_event_loop().run_until_complete(try_auth("ws://localhost:1234"))
Server answered: Please provide me a comma-separated message,hmac
I send message 'Hello from Tatyana' with HMAC '0b00eedd2d6591c88ed83305d539e296cb65ae822001a734a089a1d2bf9b44f6' based on password 'supersecret'
Access granted!
(env) shadoof@shadoof-vbox: /media/sf_Ubuntu/homework/Crypto$ █
```

Задание 2

Для проверки этого задания я запустила свой веб-сервер на порту 8000 командой `python3 -m http.server 8000`.

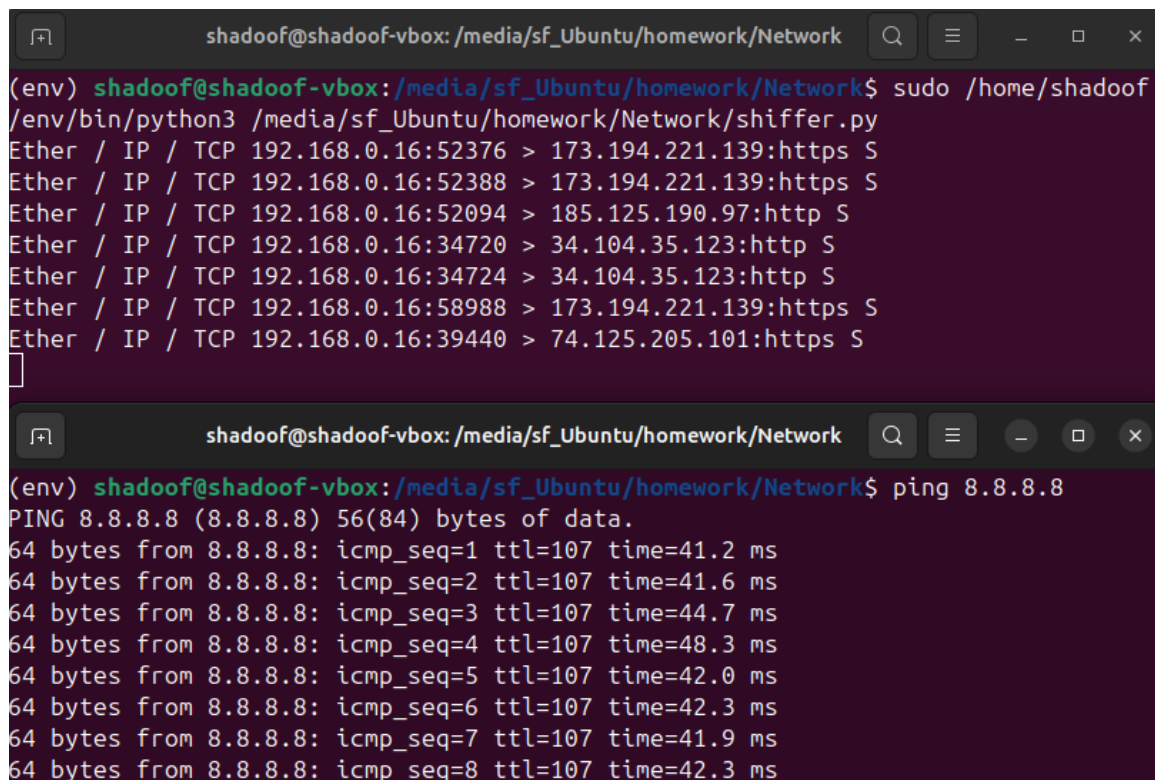
Также для этого задания требуется запускать код от имени суперпользователя, для этого воспользуемся командой `sudo /home/shadoof/env/bin/python3 /media/sf_Ubuntu/homework/Network/open_port_scanner.py`.



```
(env) shadoof@shadoof-vbox: /media/sf_Ubuntu/homework/Network$ sudo /home/shadoof/env/bin/python3 /media/sf_Ubuntu/homework/Network/open_port_scanner.py
Start scanning IP: 192.168.0.18
8000 open
Start scanning IP: 192.168.0.14
Start scanning IP: 127.0.0.1
8000 open
█
```

Задание 3

Запускаем код от имени суперпользователя командой из предыдущего задания. Также запустим браузер, например, google.com, чтобы сгенерировать tcp-пакеты.



The image shows two screenshots of a terminal window. The top screenshot shows the output of a script named 'shiffer.py' running with sudo privileges. The output lists several captured network packets, all of which are TCP SYN packets. The bottom screenshot shows the output of a 'ping' command to 8.8.8.8, which displays ICMP echo request and response details, confirming that only SYN packets are being captured by the sniffer.

```
shadoof@shadoof-vbox: /media/sf_Ubuntu/homework/Network
(env) shadoof@shadoof-vbox:/media/sf_Ubuntu/homework/Network$ sudo /home/shadoof
/env/bin/python3 /media/sf_Ubuntu/homework/Network/shiffer.py
Ether / IP / TCP 192.168.0.16:52376 > 173.194.221.139:https S
Ether / IP / TCP 192.168.0.16:52388 > 173.194.221.139:https S
Ether / IP / TCP 192.168.0.16:52094 > 185.125.190.97:http S
Ether / IP / TCP 192.168.0.16:34720 > 34.104.35.123:http S
Ether / IP / TCP 192.168.0.16:34724 > 34.104.35.123:http S
Ether / IP / TCP 192.168.0.16:58988 > 173.194.221.139:https S
Ether / IP / TCP 192.168.0.16:39440 > 74.125.205.101:https S

```

```
shadoof@shadoof-vbox: /media/sf_Ubuntu/homework/Network
(env) shadoof@shadoof-vbox:/media/sf_Ubuntu/homework/Network$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=107 time=41.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=107 time=41.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=107 time=44.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=107 time=48.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=107 time=42.0 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=107 time=42.3 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=107 time=41.9 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=107 time=42.3 ms

```

Как видим, сниффер перехватывает только пакеты SYN. Чтобы убедиться, что другие пакеты не перехватываются, я запустила ping.