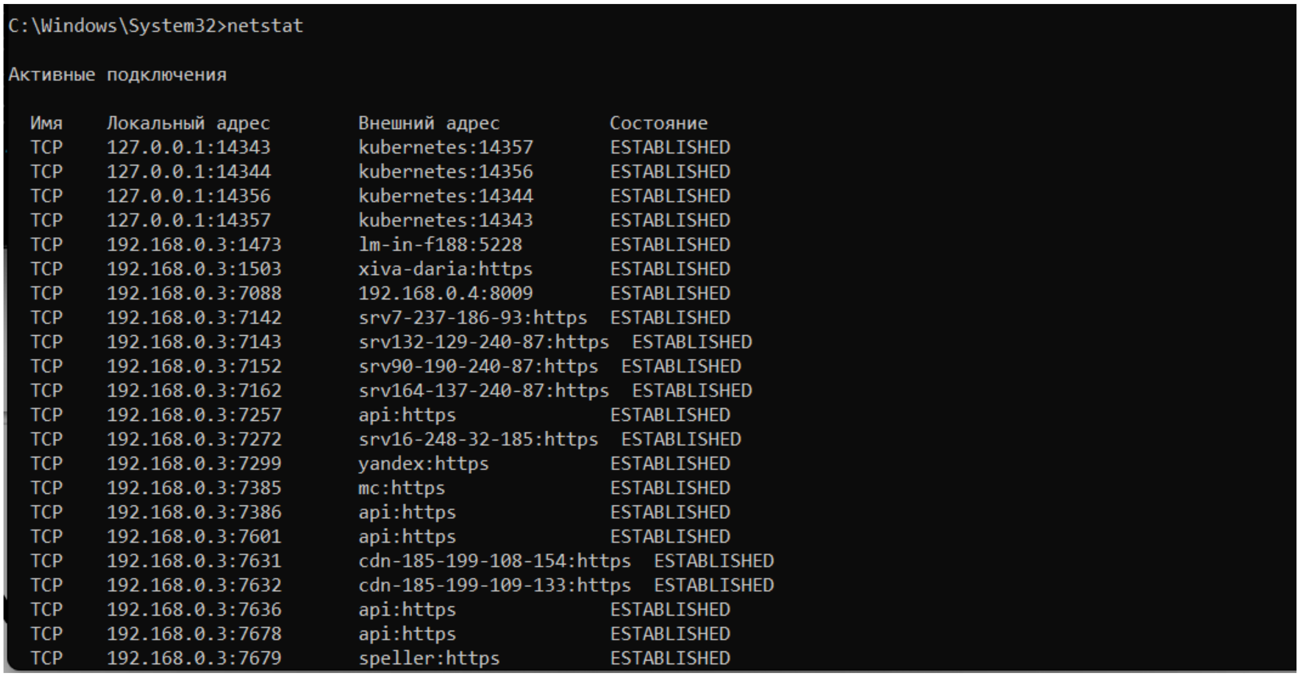
1. netstat:

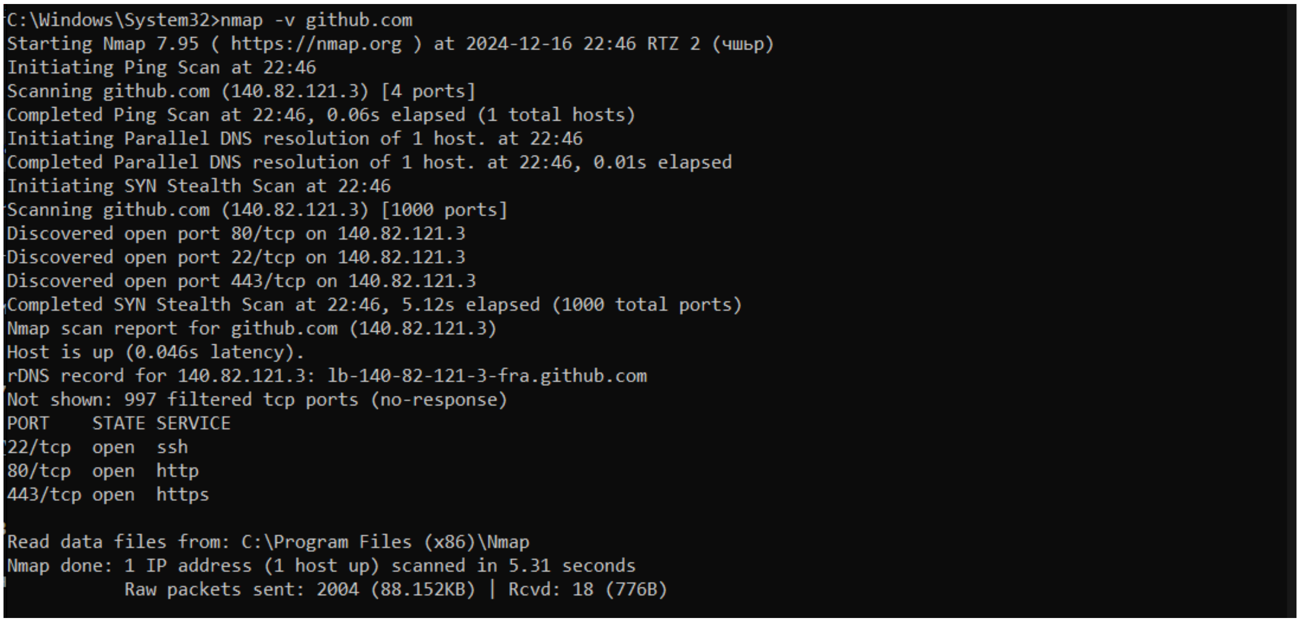


```
C:\Windows\System32>netstat

Активные подключения

  Имя    Локальный адрес        Внешний адрес          Состояние
  TCP    127.0.0.1:14343        kubernetes:14357       ESTABLISHED
  TCP    127.0.0.1:14344        kubernetes:14356       ESTABLISHED
  TCP    127.0.0.1:14356        kubernetes:14344       ESTABLISHED
  TCP    127.0.0.1:14357        kubernetes:14343       ESTABLISHED
  TCP    192.168.0.3:1473       lm-in-f188:5228        ESTABLISHED
  TCP    192.168.0.3:1503       xiva-daria:https       ESTABLISHED
  TCP    192.168.0.3:7088       192.168.0.4:8009       ESTABLISHED
  TCP    192.168.0.3:7142       srv7-237-186-93:https  ESTABLISHED
  TCP    192.168.0.3:7143       srv132-129-240-87:https  ESTABLISHED
  TCP    192.168.0.3:7152       srv90-190-240-87:https  ESTABLISHED
  TCP    192.168.0.3:7162       srv164-137-240-87:https  ESTABLISHED
  TCP    192.168.0.3:7257       api:https              ESTABLISHED
  TCP    192.168.0.3:7272       srv16-248-32-185:https  ESTABLISHED
  TCP    192.168.0.3:7299       yandex:https           ESTABLISHED
  TCP    192.168.0.3:7385       mc:https               ESTABLISHED
  TCP    192.168.0.3:7386       api:https              ESTABLISHED
  TCP    192.168.0.3:7601       api:https              ESTABLISHED
  TCP    192.168.0.3:7631       cdn-185-199-108-154:https  ESTABLISHED
  TCP    192.168.0.3:7632       cdn-185-199-109-133:https  ESTABLISHED
  TCP    192.168.0.3:7636       api:https              ESTABLISHED
  TCP    192.168.0.3:7678       api:https              ESTABLISHED
  TCP    192.168.0.3:7679       speller:https          ESTABLISHED
```

2. nmap



```
C:\Windows\System32>nmap -v github.com
Starting Nmap 7.95 ( https://nmap.org ) at 2024-12-16 22:46 RTZ 2 (чшьр)
Initiating Ping Scan at 22:46
Scanning github.com (140.82.121.3) [4 ports]
Completed Ping Scan at 22:46, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:46
Completed Parallel DNS resolution of 1 host. at 22:46, 0.01s elapsed
Initiating SYN Stealth Scan at 22:46
Scanning github.com (140.82.121.3) [1000 ports]
Discovered open port 80/tcp on 140.82.121.3
Discovered open port 22/tcp on 140.82.121.3
Discovered open port 443/tcp on 140.82.121.3
Completed SYN Stealth Scan at 22:46, 5.12s elapsed (1000 total ports)
Nmap scan report for github.com (140.82.121.3)
Host is up (0.046s latency).
rDNS record for 140.82.121.3: lb-140-82-121-3-fra.github.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 5.31 seconds
           Raw packets sent: 2004 (88.152KB) | Rcvd: 18 (776B)
```

- 22/tcp (ssh): Открыт для удалённого доступа по SSH (предположительно, для администраторов).
- 80/tcp (http): Открыт для стандартного веб-доступа без шифрования.
- 443/tcp (https): Открыт для защищённого веб-доступа через HTTPS.