4. Подключитесь FTP-клиентом в пассивном режиме и попробуйте обнаружить логин и пароль с помощью tcpdump.

Параметр "-D" или "--list-interfaces" можно использовать для перечисления всех доступных интерфейсов.

```
Ubuntu 20.04.5 LTS
boris@HP-Z:~$ tcpdump -D
1.eth0 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dummy0 [none]
8.tunl0 [none]
9.sit0 [none]
10.bond0 [none]
boris@HP-Z:~$
```

Обычно основной сетевой интерфейс системы указан в первой позиции, т.е. это «eth0».

Также существует псевдоустройство с именем «any», которое можно использовать для захвата на всех интерфейсах. Однако при использовании «любого» интерфейса tcpdump не сможет установить «неразборчивый режим» или promiscuous mode.

Можно использовать номер интерфейса (или имя) с ключом -i, чтобы слушать конкретный интерфейс.

Параметр -A отображает содержимое пакета в текстовой форме ascii, которая доступна для поиска с помощью grep.

Tcpdump должен работать с привилегиями root, чтобы захватывать пакеты на сетевых интерфейсах, поэтому нужно использовать sudo.

Результат:

```
boris@HP-Z:~$ sudo tcpdump -A port ftp -i eth0 | grep PASS
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
01:55:18.929617 IP 172.28.24.31.48540 > ec2-44-241-66-173.us-west-2.compute.amazonaws.com.ftp: F
lags [P.], seq 12:25, ack 35, win 502, options [nop,nop,TS val 234679129 ecr 1987694290], length
 13: FTP: PASS 123456
...Yvy..PASS 123456
01:55:23.024900 IP ec2-44-241-66-173.us-west-2.compute.amazonaws.com.ftp > 172.28.24.31.48540: F
lags [P.], seq 57:95, ack 31, win 210, options [nop,nop,TS val 1987701784 ecr 234683024], length
 38: FTP: 530 Please login with USER and PASS.
vy......530 Please login with USER and PASS.
```