1. Start a TryHackMe Room and Get Machine IP

hint: https://www.youtube.com/watch?v=IpjifLzyX8Q

- Go to the assigned room (e.g., https://tryhackme.com/room/networkservices)
- Scroll to Task related to ftp and click the green 'Start Machine' button
- Wait 30–60 seconds
- The machine's IP address will appear at the top of the task (e.g., 10.10.27.237)

2. Use FTP to Connect to the Machine

- In terminal, type:
  gftp 10.10.27.237 (this works fine on mac)
- When prompted:
  Username: anonymous
  Password: (press Enter)
- After logging in, use commands:
  ls
  get PUBLIC_NOTICE.txt
  bye

3. Monitor the Session Using Wireshark

- Launch Wireshark
- Capture on interface: tun0 (the VPN tunnel)
- Use filter: ftp || tcp.port == 21
- Re-run FTP commands to see the traffic live
- Right-click → Follow TCP Stream to view full session
- Look for USER, PASS, LIST, RETR, PORT commands

4. Common Student Questions & Answers

Q: I installed OpenVPN but terminal says `command not found`?
A: You likely installed the GUI version. Either use Tunnelblick (GUI) or install via Homebrew: brew install openvpn

Q: How do I know the VPN is working?
A: After running `sudo openvpn config.ovpn`, look for `Initialization Sequence Completed`. Then try: ping 10.10.xx.xx where 10.10.xx.xx is targets IP

Q: Why can't I connect to the FTP machine?
A: Wait at least 60 seconds after clicking 'Start Machine'. If `ftp` says 'Connection refused',

try restarting the machine from the TryHackMe interface.

Q: What if I don’t see anything in Wireshark?
A: Make sure you're capturing on the `tun0` or similar interface. You can check in Capture->Options. Also, start Wireshark capture before logging into FTP.

5. Wrapping Up

- Use Wireshark to capture and screenshot login and file access traffic
- Use the public file `PUBLIC_NOTICE.txt` to demonstrate file exfiltration
- Document all findings in your lab report
- Use the TryHackMe room to complete and answer all tasks related to FTP