Lab2

Joseph Potapenko

October 2025

1. Why can't you just change the port with scapy? TCP keeps track of connection state (sequence numbers, ACKs, checksums), so just changing a packet's port will break the connection and the other party's machine will drop or reset it.

2. What type of proxy did you create? A transparent/intercepting proxy — it redirects client traffic to your program without the client knowing.

3. Why don't scapy-created packets get remapped to 8080? The iptables rule skips packets from the root user, so packets your sniffer sends aren't sent back to 8080.

4. What would be needed to handle HTTPS (443)? You'd have to act as a fake server with a trusted certificate so you can decrypt and re-encrypt traffic - which requires the other party to trust your certificate.