Network Security Challenge 02 - Easy

The government still follows the advice of Nolan Nets II. He now came to the great conclusion that the Linux kernel is evil, since it is open source and anyone can see the source code. How can something be secure if everyone knows how it works?? He did not stop there, he thinks any protocol used on any network, especially the Internet, has to implemented by the user themselves. That way, the code remains secret and by that, secure. So, secret intel is now hosted on a TCP server which you can only connect to if you implement your own TCP handshake. The catch here is that the first packet, the SYN packet, already has to have the TCP cookie as the SEQ number. Ask Nolan why that is important. Your task is to implement this modified TCP handshake and obtain the secret!

Exercise 2 - easy is hosted at `netsec.net.in.tum.de` at port 20102.
For this challenge, connecting via *netcat* will not work. The template and the solution use Python Scapy. Please look at the Scapy demo on how to use the library: `https://scapy.readthedocs.io/en/latest/index.html`
Important: You need root on a Linux machine to solve this challenge!
Also important: When you implement "your own TCP", the Linux kernel might try to intervene. Here is how to keep it from doing that: `https://stackoverflow.com/questions/9058052/unwanted-rst-tcp-packet-with-scapy`. This fix IS NOT necessary for the autograder, please do not implement it in your submitted script.
Also important: Please replace the interface name in the template with your Internet-facing interface. Before submitting your solution, please replace the interface with `enX0` to make it work inside the docker container.
Also important: Some magic firewall (which we cannot control) sits between the NetSec VM and the Internet. It imposes some very strict rules on how the TCP handshake has to work. Firstly, the ACK of the second packet (from the server) and the third packet (second to the server) have to be equal to the SEQ number of the previous message (as opposed to our slides and the RFC where the ACK number is SEQ + 1). Otherwise, implement the TCP flags according to the standard. If you don't receive an answer from the NetSec VM, it was dropped by the firewall. You will receive the solution flag in the third packet.
General advice: It is advisable to have a Linux system at hand for the challenges. Our servers and clients are written in Python.