Network Security Challenge 08 - Easy

A customer of Nolan Nets is complaining that their web services don't work because Nolan keeps issuing invalid certificates for them. Since Nolan keeps insisting that there is nothing wrong with them, they want a real experts opinion. They sent you address and port of their server where they send you certificates and ask you to tell them if there's something wrong with them.

Your task is to connect to the server port, receive the PEM-encoded certificates, parse them and validate them. Inside the zipfile from the scoreboard you can also find the certificate of Nolan's Certificate Authority, which you are supposed to trust. Check if the certificate you receive is signed by Nolan's CA and if it is otherwise valid. Lucky for you, the server tells you if you are wrong.

> Exercise 8–1 is hosted at `netsec.net.in.tum.de` at port 20108.
> We recommend connecting to the server using `netcat (man nc)` first.
> It is advisable to have a Linux system at hand for the challenges. Our servers and clients are written in python.