Network Security Challenge 02 - Hard

This challenge is hosted at `netsec.net.in.tum.de:arbitrary_but_fixed_ephemeral_port`. This means that, before you can solve the actual challenge, you'll have to find it's port! Finding the port is not part of the challenge itself, so only submit the solution to the actual challenge part. We recommend using a tool like *nmap* to find the port.

> The department has an active portscanning protection. Block times are 1h+. Please use lxhalle.in.tum.de to send requests and/or be "polite" with your request load! For example, use the `-max-rate` flag of nmap. Otherwise you might block your whole student dorm etc.
> IMPORTANT: please **DO NOT** upload your port scanning tool here, only the script which interacts with the challenge itself.

After you found the port, the actual challenge begins. This time, the server has chosen a random password and does not reveal it to you. However, you get to know that the password is `PasswordXX`, where `X` is a digit. For example, `Password00`, `Password12`, or `Password99` are valid passwords.

The server expects you to send your login credentials, after you connected. This is how the server sets them up:

```
credentials = "root,Password"+str(random).zfill(2)
```

After entering your credentials, you will have to survive an inverse Turing test to prove that a machine is running the protocol. Or do you really want to do this manually?

> Exercise 2–2 is hosted at `netsec.net.in.tum.de` at some ephemeral port.
> As you might have noticed, the ports of the other challenges are usually 2000X, where X is the challenge number. This is not the case for this challenge, so leave the challenges with the expected port numbers alone.
> 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.