CS 406 : Cryptography and Network Security Spring 2024

Bonus Lab — Taste of Reality

Instructor: Manoj Prabhakaran *Lab TA:* Nilabha Saha

Note: In these challenges, you will use a tool called `netcat` to connect to a quizzing server. Copy the command in the "connection info" part of the challenge description and paste it on your terminal and execute the same to connect to the quizzing server. The quizzing server compares your answer with the expected answer after converting all your characters to lowercase and stripping any spaces.

If you are having trouble connecting to the server, there is a `questions.txt` file attached with each problem. If there are k questions, the flag **cs406{ans1_ans2_..._ansk}** will also be accepted. Please note there should be no spaces in the flag, and all challenges' flag-checking for this lab is case-insensitive (for this type of flag).

Challenge 1: Certificates Galore

SSH to the cs406 user on the indus server by executing

```
ssh cs406@indus.cse.iitb.ac.in
```

The password for the same can be found in the Moodle announcements for Lab 4.
You can inspect several certificates stored on the server in `/etc/ssl/certs`. You could use `openssl x509` to inspect the certificates (with the appropriate options). Use it to answer the questions asked on the quizzing server.

Challenge 2: DNSSEC

You can read a high-level overview of the DNSSEC technology here. Use Wireshark (which you can also install using `sudo apt install wireshark` on a Linux system) to open the given `.pcap` file and investigate the packets. Answer the questions asked on the quizzing server.

Challenge 3: Transport Layer Security

You can find an excellent illustrated guide of the TLS1.3 protocol at The Illustrated TLS 1.3 Connection.
Use the `.pcapng` file associated with this challenge and observe how the protocol is being followed by inspecting the packets in Wireshark. You have also been given the pre-master secret, you may refer to this to understand how to incorporate the same in Wireshark.
Answer the questions asked on the quizzing server.