# Lab 11

## 2. Implementing a simple HTTP-based messaging service

By running both the server and client, I was able to see the POST request of the client with its JSON object, along with his login credentials.

## 3. ARP Spoofing

By using ettercap, I was able to do ARP poisoning, which allows me to do packet sniffing between 10.0.1.50 and 10.0.1.20. From Wireshark, I was able to obtain the HTTP basic auth username and password, which is `admin` and `l4sT_L4b` respectively. The secret payload is a JSON Object containing all the messages received by the server from POST requests, with username as key.

## TLS and HTTPS

After switching to HTTPS, I can no longer obtain useful information from Wireshark as the sniffed packets are now encrypted.