Challenge Description

Your task is to examine the logs or packet capture, identify which account was **compromised**, and determine the password used during the successful login.

Submit your answer as: `csd{username_password}`

Attachments: ftpchal.pcap

How to Identify a Successful FTP Login in Packet Captures

When analyzing FTP traffic, authentication is easy to inspect because FTP transmits usernames and passwords in **plaintext**. Understanding the sequence of server response codes allows you to quickly determine whether a login attempt succeeded or failed.

These are the key codes involved in authentication:

Code	Meaning
220	Service ready — the server greets the client
331	Username accepted — password required
230	**Login successful** (authentication succeeded)
530	Login incorrect (authentication failed)

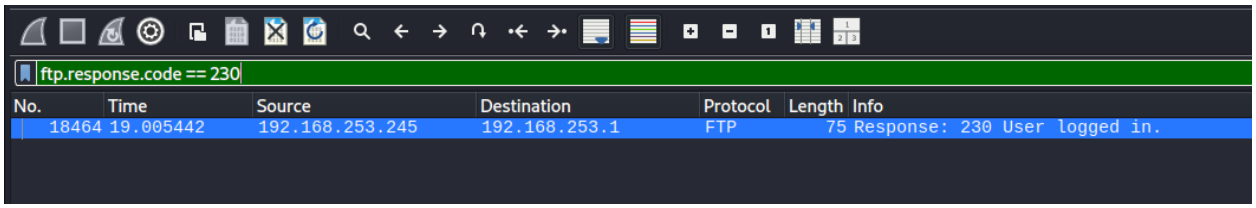
A normal FTP authentication exchange looks like this:

```
Client → [Connects to FTP server]
Server → 220 Service ready

Client → USER <username>
Server → 331 Username OK, need password

Client → PASS <password>
Server → 230 Login successful ← SUCCESS
OR
Server → 530 Login incorrect ← FAILURE
```

How to Determine the Compromised Account

1. **Locate the server replies with code 230**
   This indicates a successful login.

After opening the ftpchal.pcap file
We first successful response can be seen at packet 18464



2. **Check the packets immediately before the 230**