

# 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
<b>220</b>	Service ready — the server greets the client
<b>331</b>	Username accepted — password required
<b>230</b>	<b>Login successful</b> (authentication succeeded)
<b>530</b>	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

No.	Time	Source	Destination	Protocol	Length	Info
18464	19.005442	192.168.253.245	192.168.253.1	FTP	75	Response: 230 User logged in.

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

18460	19.003967	192.168.253.245	192.168.253.1	FTP	81	Response: 220 Microsoft FTP Service
18461	19.004623	192.168.253.1	192.168.253.245	FTP	66	Request: USER Elf67
18462	19.004671	192.168.253.245	192.168.253.1	FTP	77	Response: 331 Password required
18463	19.005130	192.168.253.1	192.168.253.245	FTP	69	Request: PASS snowball
18464	19.005442	192.168.253.245	192.168.253.1	FTP	75	Response: 230 User logged in.