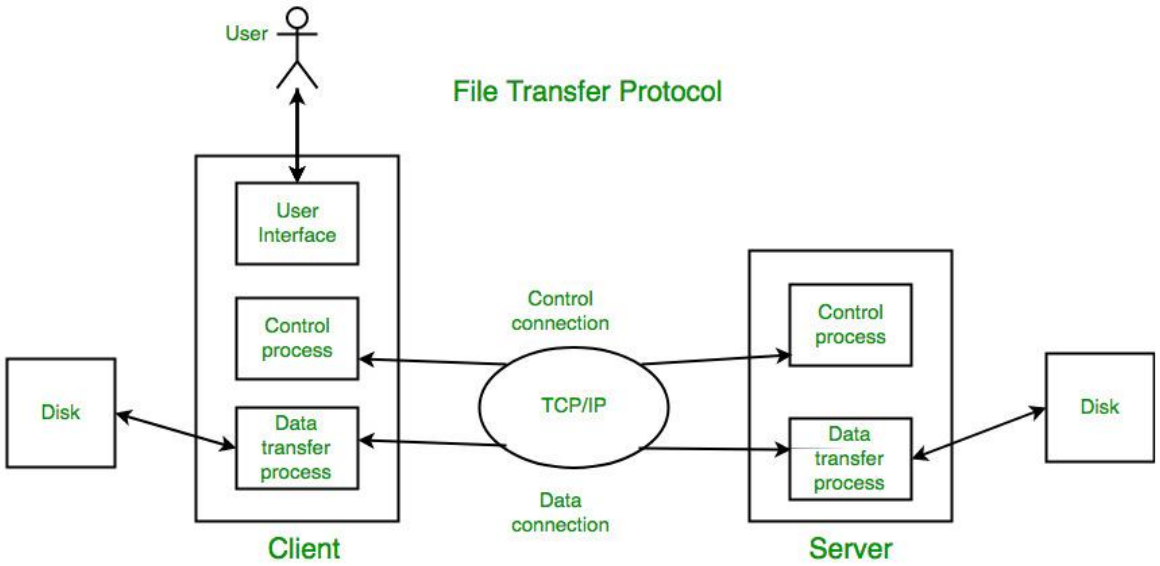
Day 24

Exploitation Analyst

FTP Protocol:



How FTP protocol works?

Scenario 1

Machine 1 wants to share the file to other machines, for it machine 1 will upload tis file on the ftp server and other machines then download the files from there.

Scenario 2:

Machine 1 wants to share the file to other machines, for it machine 1 tries to become itself as a server.

In details:

1. Client Initiates Connection

The user runs an FTP client (like ftp, FileZilla, WinSCP, or browser) and connects to the server using:

- **Server IP / Hostname**
- **Port 21** (default control port)

2. Authentication

The server responds with a greeting/banner.

- The client sends **username** and **password**.
- Server checks credentials.
    - If successful, access is granted.
    - Some servers allow **anonymous login** (username: anonymous).

3. Command Channel Opens (Control)

All commands like:

- LIST (view files)
- CWD (change directory)
- RETR (download)
- STOR (upload)

...are sent over the **control connection** (still on port 21).

4. Data Channel Opens (File Transfer)

When a file transfer begins:

- A **new data connection** is opened.
- The **mode** determines who initiates this:
  - **Active Mode** → server connects back to client on port >1023.
  - **Passive Mode** → client connects to a random port on server (more firewall-friendly).

5. File Transfer Happens

- Actual file content (not commands) is sent over the **data connection**.
- After the transfer, the data connection closes.
- Control connection remains open for further commands.

6. Session Ends

- The client sends a QUIT command.
- Server closes the control connection.

--The End--