Network Programming – Project
ZT-FTP (Zero Trust File Transfer Protocol)

Group Members:

Rahf Abukhas - RHF0227287@ju.edu.jo
Yaqeen Fandi - YQY0213471@ju.edu.jo

Project Overview

This project implements a **Zero Trust File Transfer Protocol (ZT-FTP)** using Java sockets.
The system consists of a **client** and a **multi-threaded server** that supports secure authentication, session-based access control, and file operations with role-based permissions.

Implemented Features
Authentication

- Username and password authentication using users.txt, format (Username:Password:Role)
- Role-based access control:
    - normal user
    - super user
- Session key generation using UUID
- Maximum authentication attempts limit (connection terminated after multiple failures)

Session Security

- Every command requires a valid session key
- Connection terminated after multiple invalid session key attempts

File Operations

- **LIST**
    - Normal user: lists files in own directory
    - Super user: lists all users' files
- **UPLOAD**
    - Upload files from client to server
- **DOWNLOAD**
    - Download files from server to client

- **DELETE**
  - o Available only for super users
- **Logging**
  - o All major actions are logged in logs/server.log

Zero Trust Principles Applied

- Authentication before any operation
- Session key validation for every request
- Least privilege (normal users restricted to own directory)
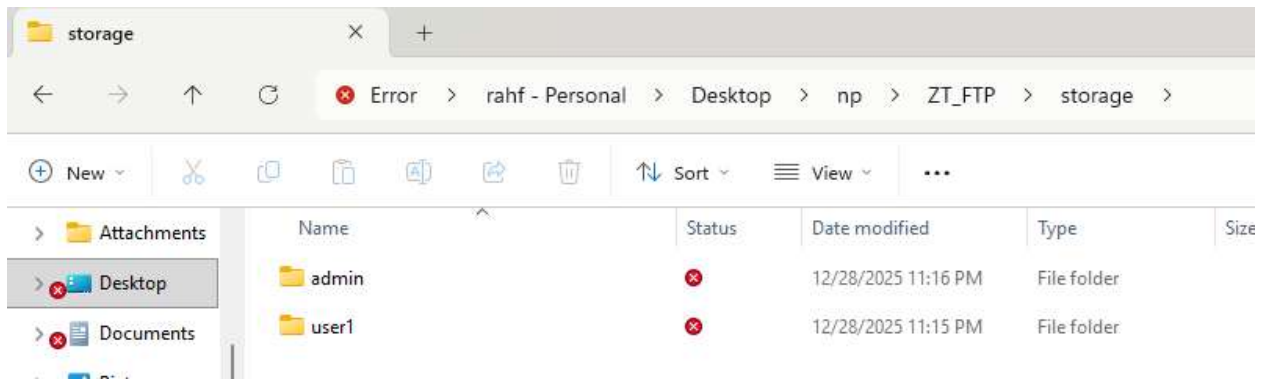
Directory Structure

ZT_FTP/

The files will be uploaded should be her behind the src

Uesers.txt file:
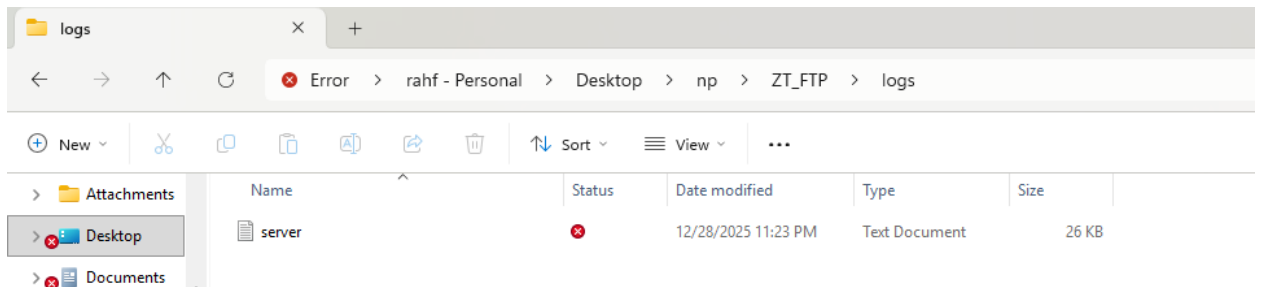
```
user1:pass1:normal
admin:adminpass:super
```

Storage Folder:

Logs file:

How to Run

1.Run the main

Output: ZT-FTP Server running on port 5000

2.Run the Client

How to Use the Client

- Enter username and password
- Upon successful login, a session key is generated
- Choose a number from the menu:

1) LIST
2) UPLOAD
Just write the file name (e.g., file.txt)
3) DOWNLOAD
Just write the file name (e.g., file.txt)
4) DELETE (super only)
To delete the admin files: write the file name (e.g., file.txt)
To delete other users' files: write the full path (e.g., user1/file.txt)
5) bye

Notes

- The server automatically terminates the connection after multiple failed authentication attempts
- Logs are stored in logs/server.log.
- The project demonstrates Zero Trust concepts at the application level.

References (Java File Handling & Utilities)

Java Basics & Core Concepts

W3Schools – Java Tutorial :https://www.w3schools.com/java/default.asp

File Handling in Java

W3Schools – Java Files (Create, Read, Write): https://www.w3schools.com/java/java_files.asp

W3Schools – Java File Delete Example : https://www.w3schools.com/java/java_files_delete.asp

Oracle Java 8 API – java.io.File : https://docs.oracle.com/javase/8/docs/api/java/io/File.html

Unique Identifiers (Session Keys)

Oracle Java 8 API – java.util.UUID : https://docs.oracle.com/javase/8/docs/api/java/util/UUID.html