# CSY2085 – Server Administration and Security

## Workshop 2 - Windows Server Roles

STUDENT NAME: Muhammad Raza

STUDENT NUMBER: 21624838

## Task 1 - Run Windows Client

**Question: What is your IP address of your Windows client?**

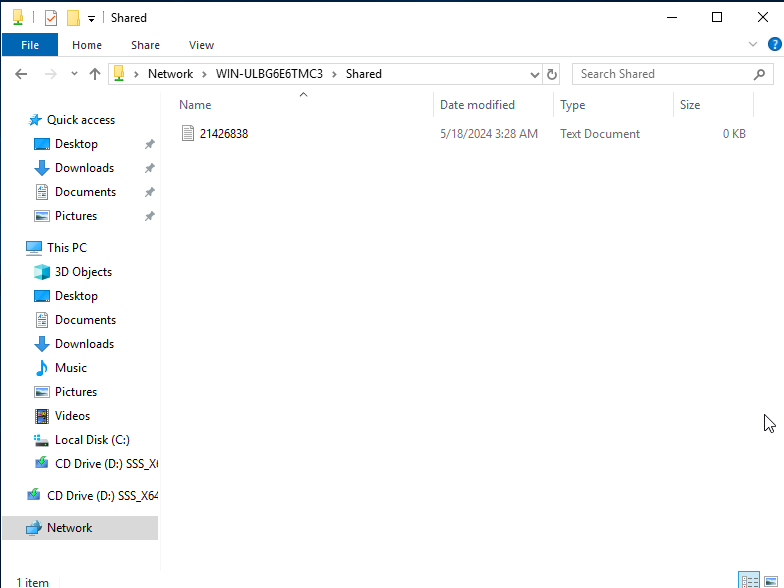
10.0.2.15

## Task 2 - Configuring the Windows File Server

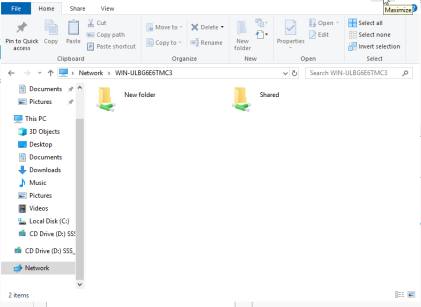
**Question : What is your Windows Server IP address?**

**192.168.56.1**

## Task 3 - Connecting to the File Server

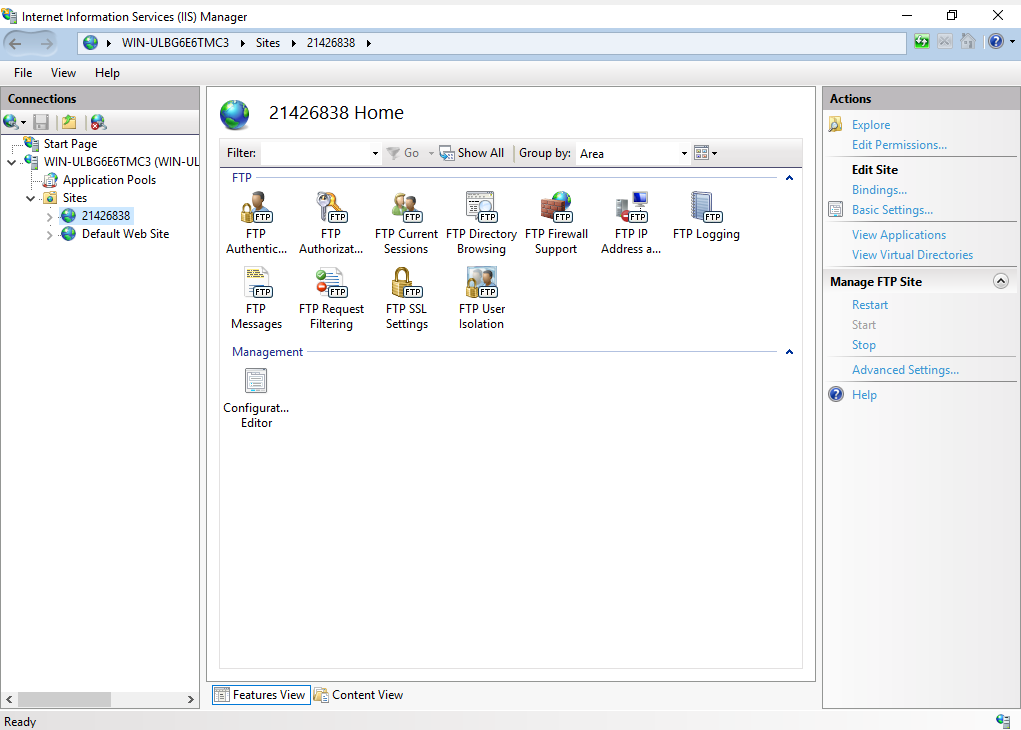
1. Open up the “Shared” folder on the server and create a new text file with your Student ID:  
   

## Task 4 - Create another shared folder

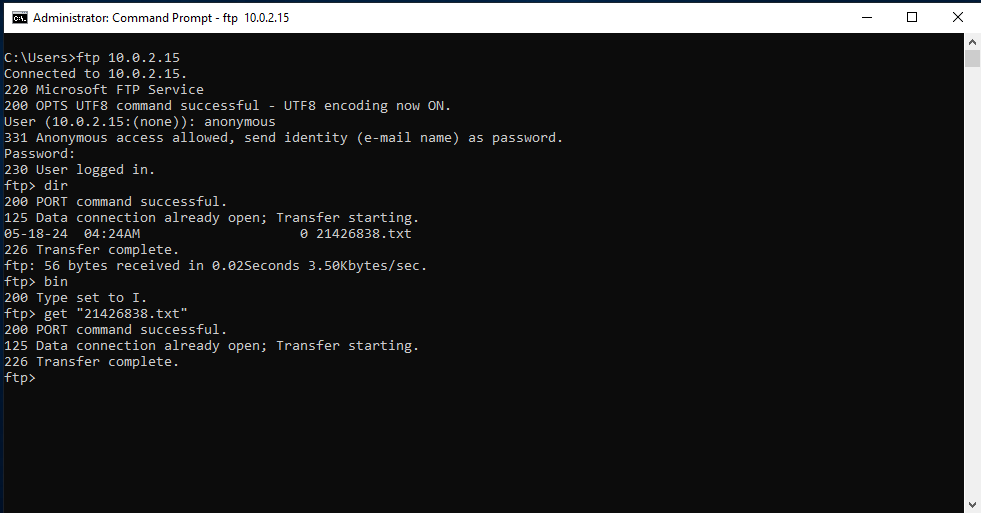
1. Capture and paste the screen like that in Task 3.  
     
   

# Part 2 - Windows Server as an FTP Server

## Task 1 - Installing the FTP Server Service

****

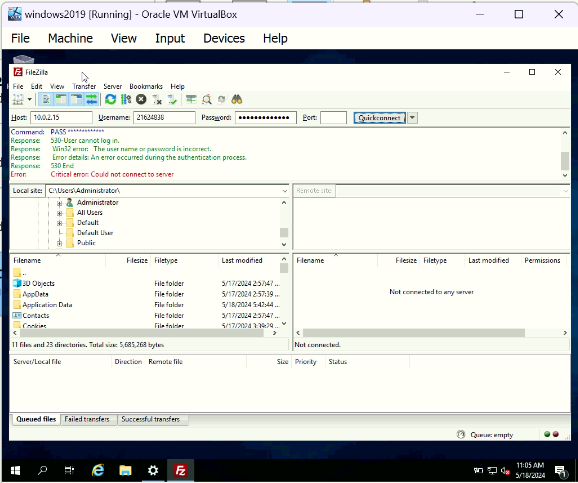
1. Take a screenshot of your Command Prompt, showing the Transfer Complete.

****

1. Task 2 - Configuring the FTP Server for authenticated user logins  
   Now try to log into your FTP server using the username name of “anonymous” as in the first exercise.

**When you attempt to log into your FTP server using the username "anonymous" after configuring it for authenticated user logins, the login attempt is rejected. The server does not permit anonymous access in this configuration and will provide an error message like "530 Login incorrect." Only authenticated users with valid credentials can log in.**

## Now screen capture the Command Prompt screen and paste it below: **ftp 2**

1. Task 3 - Installing and configuring a Graphical FTP Client  
     
   

**Task 4**

1. Do research into FTP Service trying to identify any challenges with this service and how they can be overcome. Max 500 words

**Challenges with FTP Service and How to Overcome Them**

**1. Security Issues**

FTP, being an older protocol, has inherent security vulnerabilities, primarily due to its lack of encryption. Data, including login credentials, is transmitted in plaintext, making it susceptible to interception by attackers.

**Solution:**

**Use Secure Versions:** Transition to secure variants like FTPS (FTP Secure) or SFTP (SSH File Transfer Protocol). FTPS adds a layer of SSL/TLS encryption, while SFTP uses SSH to encrypt data, providing a higher level of security.

**Implement Strong Authentication:** Use strong, unique passwords and consider multi-factor authentication (MFA) to enhance login security.

**2. Lack of Data Integrity**

FTP does not natively support data integrity verification. Files can become corrupted during transfer without any indication to the user.

**Solution:**

**Enable Checksum Verification:** Implement checksum verification (e.g., MD5, SHA-256) to ensure data integrity. This can be done manually or through additional software that automates checksum calculation and verification.

**3. Passive Mode Issues**

FTP’s active mode can be problematic with firewalls and NAT (Network Address Translation) because it requires the server to initiate a connection back to the client. Passive mode solves this but can still face issues with certain network configurations.

**Solution:**

**Configure Firewall Rules:** Ensure firewalls are configured to allow the necessary range of ports for passive mode. This often involves setting a fixed range of ports on the FTP server and opening those ports on the firewall.

**Use Passive Mode Consistently:** Configure clients and servers to default to passive mode to avoid connectivity issues.

**4. Complex Configuration and Management**

FTP servers can be challenging to configure and manage, particularly for users without advanced technical skills. This includes setting up user permissions, managing data directories, and configuring secure connections.

**Solution:**

**Use Managed FTP Services:** Opt for managed FTP services or cloud-based solutions that handle configuration and management, reducing the burden on in-house IT staff.

**Leverage User-Friendly Tools:** Use graphical user interface (GUI) tools for server configuration and management. These tools often simplify complex tasks through a more intuitive interface.

**5. Limited Logging and Monitoring**

FTP servers may not provide detailed logging and monitoring by default, making it difficult to track access and detect unauthorized activities.

**Solution:**

**Enable Detailed Logging:** Configure the FTP server to enable detailed logging of all activities, including successful and failed login attempts, file transfers, and changes.

**Implement Monitoring Solutions:** Use monitoring tools to keep an eye on FTP server activity in real time. Alerts can be set up for suspicious activities or potential security breaches.

**6. Scalability Issues**

Traditional FTP servers may struggle with scalability, particularly under high loads or with large numbers of simultaneous connections.

**Solution:**

**Load Balancing:** Implement load balancing solutions to distribute traffic across multiple servers, ensuring that no single server becomes a bottleneck.

**Cloud-Based Solutions:** Consider cloud-based FTP solutions that offer scalable resources and can handle varying loads more efficiently.

**7. Compatibility Issues**

Different FTP clients and servers may have compatibility issues, particularly with proprietary extensions or differing interpretations of the FTP standard.

**Solution:**

**Use Standard-Compliant Software:** Ensure both the FTP server and clients strictly adhere to FTP standards. Avoid proprietary extensions unless necessary and ensure that any custom features are well-documented and understood by all parties.

By addressing these challenges with the suggested solutions, FTP can remain a viable file transfer protocol, balancing its long-standing reliability with modern security and usability enhancements.