# Windows Unit 4 Lab Guide #1 (4.1 - 4.5)

As you set up different server roles, think about why securing one server is essential for the safety of an entire network and how attackers can use certain vulnerabilities in servers to gain access to the rest of a network.

Commands you might need: we don’t do that here

### 4.1 - Servers Introduction

1. Do you remember your server acronyms? Do you know their purpose?
   1. SMB
   2. FTP
   3. IIS
   4. DNS
   5. AD

### 4.2 - Server Differences

1. Visit the Add Roles and Features window via Server Manager
2. Continue to the roles panel and expand the Web Server (IIS) box
   1. Note that **both** FTP and Web Server (HTTP/WWW) roles fall under this category
3. Visit the Remove Roles and Features window via Server Manager
4. Pro tip: if you accidentally clicked the wrong window (chose Add instead of Remove or vice versa) the starting page of the window has a redirect link to the other window)
5. Check out your IE ESC settings. Are they set properly?

### 4.3 - SMB Server

1. Set up an SMB share
   1. Share a folder of your choice - you can create a new one too, just make sure it has files inside so you know when it has worked properly.
2. Disable insecure SMB versions
3. Explore file permissions for the share
4. Access the shares via File Explorer
   1. Type in “\\127.0.0.1\” followed by your share name
      1. Pro tip: 127.0.0.1 is the loopback address, which basically tells your computer to look at itself for any shares. Useful for networking troubleshooting.
      2. Pro tip: if you only type in “\\127.0.0.1” you can find all non-hidden shares on your computer
   2. Access your hidden C share found at \\127.0.0.1\C$
   3. Access a public anonymous share found at \\live.sysinternals.com\tools
5. Can you access shares via a web browser?

### 4.4 - FTP Server

1. Install the FTP Server role and create an FTP site
   1. What manager can you use to do this?
2. Install FileZilla Server and secure it
   1. Find the settings and look through them
   2. Determine what needs to be changed for FileZilla to be secure
      1. Ask questions if you don’t know what a setting does
   3. Some things you may want to look at:
      1. Custom welcome message
      2. Bounce Attack Protection
      3. Automatic Bans
      4. Users and Passwords
3. While FileZilla Server is running, connect to the server via Filezilla Client
   1. Use IP address 127.0.0.1 to connect to yourself

### 4.5 - HTTP

1. Install the Web Server role
   1. Explore the different types of IIS Servers, and find what services each requires
      1. FTP
      2. HTTP
      3. SMTP
2. Deploy a website using IIS
   1. Google how to do this, it is not too complicated
   2. Ask questions if you get stuck
3. Secure the website
   1. Only authorized users can access
      1. If it is supposed to be anonymously accessible, allow anonymous access
   2. Users shouldn’t be able to directory browse
      1. This is when they can look through the server’s files by changing the URL
      2. They should only be allowed to access files if they give a specific path
4. Logging
5. Open ports for the service