What is Https

- HTTPS is an encrypted version of HTTP

Here's how https works including certificate signing

1. Public Key Infrastructure (PKI): HTTPS relies on PKI, which uses key pairs (private, public) and digital certifactes to secure communicateions
2. Digital Certifactes:
    1. Certificate Authority (CA): A trusted third party to issue digital certifacates.
    2. Certificate: Contains the public key, owner idenity and CA's digital certificate
3. Certificate Signing:
    1. When a website wants an SSL/TLS certificate, it generates a public private key pair and sends public key along with its identity to CA
    2. CA verifies identies and signs the certifacte using its private key, embedding the signature with in the certiface

4. HTTPS Handshake:
    1. When a user connects to a website, browser requests the site's certificate
    2. Browser checks the certificate's validity (expired, revocation, CA Trust)
    3. If valid, the browser extracts public key from certificate
5. Session Key Establishment
    1. Browser generates a symmetric session key for encryption
    2. This session key is encrypted with public key and sent to the server
    3. only the server can decrypt this as it has the private key
6. Secure Communication:
    1. Both Browser and server use symmetric session key for fast and secure communication
    2. Symmetric encryption ensure data exchange is confidential and integrity protected

Try Viewing the Steps for below

- Setting up SSL Certificate on IIS
- Setting up SSL Certificate on Apache Server
- Setting up SSL Certificate on Nginx
- use this article Refer Here

Connecting to windows servers

- When connecting to server we generally have two broader options
    - connectivity for command line access
        - WinRM
        - SSH
    - connectivity for GUI access:
        - mstsc (Remote Desktop Connections)

Connecting to Linux servers

- When connecting to server we generally have two broader options
    - connectivity for command line access
        - SSH
    - connectivity for GUI access:
        - VNC

SSH (Secure Shell)

- SSH supports two types of authentication
    - password
    - key based authentication

How SSH Password authentication works

- Connection initiation: The client start an SSH session with the server using the ssh command

```
ssh username@ipaddress
```

- Password prompt: The server prompts the client for the users password
- Password Transmission: The client sends the password to the server (over encrypted channel)
- Authentication:
    - The server verifies the password and if it is correct the access is granted and session is established.