**Certificate**

* Login to IIS server with admin privileges and open mmc
* Click File and select Add/Remove Snap-in
* Select Certificates and click Add
* Select Computer Account and click next
* Select Local Computer and click Finish, then click OK
* Close the snap-ins window, then double click Certificates
* Right click Personal, All Tasks, Advanced Operations, Create Custom Request
* Click Next, then select proceed without enrollment policy and click next
* For template select Legacy key, and for request format select PKCS #10, then click next
* Expand the details section for custom request, then click properties
* Type a friendly name for your certificate and a description
* Select the subject tab and select common name from the drop down menu for subject name
* In the value box, enter your fully qualified domain name, then click add
* Also enter information for the Organization, OU, Locality, State, and Country fields
* For alternative name, select DNS in the drop down menu and enter your fully qualified domain name in the value box, then click add
* Select the Private Key tab and for CSP select Microsoft RSA SChannel
* In Key Options set the key siza to be 2048 and check Make private key exportable
* In Key Type select Exchange
* Double check that settings are correct, then click OK
* Click next, then choose where to save the request
* Select Base64 as the file format, then click Finish
* Open the certificate request with notepad and copy the contents
* Open a web browser and enter the ip of the server running your CA, followed by /certsrv/
* Log in using your admin credentials
* Click request a certificate and then click advanced certificate request
* Paste the certificate request in the text box
* Under Certificate Template select Web Server from the drop down menu
* Click submit, then click download certificate
* Go back to IIS manager and click Complete Certificate Request
* Enter the file path of the certificate you downloaded
* Enter the friendly name and select Web Hosting from the drop down menu, then click OK
* In the left pane of IIS manager, open Sites and select Default Web Site
* In the right pane click bindings and click Add
* For type select https and select the IP address of the server
* For ssl certificate select the certificate for the web server and click ok

**Testssl**

* Install testssl from the following github page <https://github.com/drwetter/testssl.sh>
* Run Powershell as administrator and run the following command to install Windows Subsystem for Linux Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Windows-Subsystem-Linux
* Download a Linux distro from the following link <https://docs.microsoft.com/en-us/windows/wsl/install-manual>
* Extract the distro .apx packages contents in powershell using the following commands Rename-Item .\Ubuntu.appx .\Ubuntu.zip
* Expand-Archive .\Ubuntu.zip .\Ubuntu
* Run the distro .exe file in the unzipped directory and create a user account
* In file explorer, transfer the testssl folder to the rootfs/home/username directory in the linux directory
* Switch to the root user in the linux subsystem and cd into the testssl directory
* Make the testssl.sh file executable by running chmod +x testssl.sh
* Run the script by typing bash testssl.sh followed by the hostname of your IIS server
* If the certificate was created correctly, Trust (hostname) should say Ok via SAN

**TLS GPO**

* Login to Netop VM and open Group Policy Management
* Create a new GPO, right click it and click edit
* Navigate to Computer Configuration, Preferences, Windows Settings, Registry
* Right click the white pane in the registry menu and click new, registry item
* Click the Action drop down menu and select Create
* For Hive select HKEY\_LOCAL\_MACHINE
* In key path type SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server
* In Value Name type DisabledByDefault
* For Value Type select REG\_DWORD
* For Value Data type 1, then select Hexadecimal, then click OK
* Create a second registry item and repeat the same steps, but replace TLS 1.0 with TLS 1.1 in the key path type
* Link the GPO to the OU containing the IIS Server
* Run testssl.sh on the IIS Server
* TLS 1 and TLS 1.1 should show up as not offered