

This PDF Lecture is made by
Abid Biswas, **Ethical Hacker (Purple Teaming)**
(CEH, NSE1, NSE2, NSE3,
ISC²(CC), Google Cyber Security Professional Cert)
BSc in Information and Communication Engineering (ICE) at EWU



Installing a Windows Web Server:

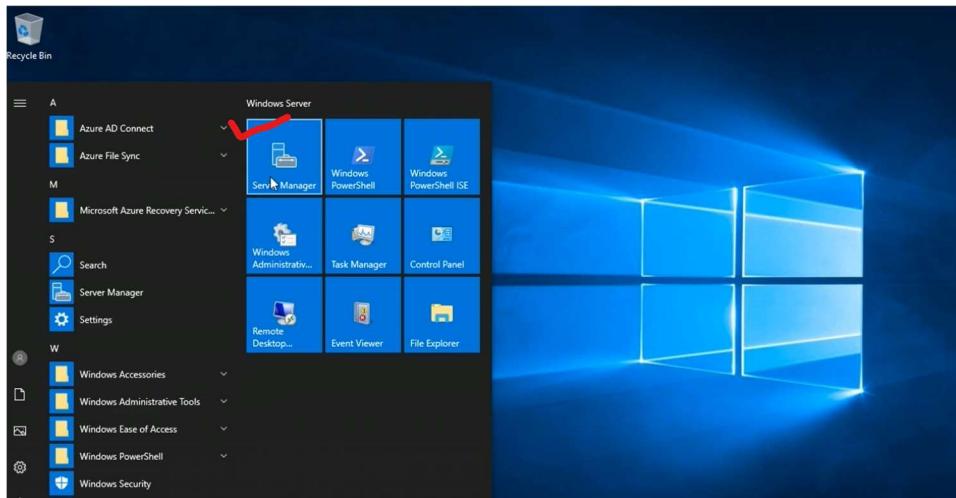
There are many web server stacks that we can run on Windows platform. We will use built-in **IIS (Internet Information Service)**. It is not installed automatically. We will use **Windows Server 2019**.

We will go to PowerShell Prompt and type: **get-windowsfeature *web*** (this means show me any windows components with features that have the web in their name)

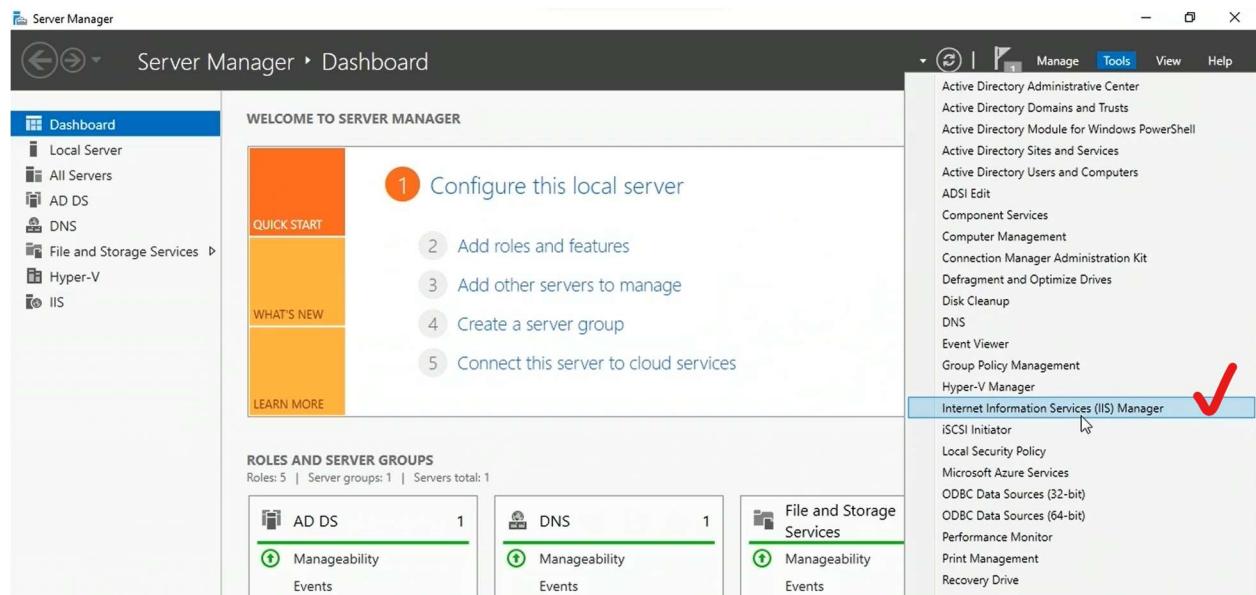
```
Administrator: Windows PowerShell
PS C:\Users\Administrator.WIN-M6CGN1MFJLQ> get-windowsfeature *web*
Display Name                                     Name          Install State
-----[ ] Certificate Enrollment Policy Web Service   ADCS-Enroll-Web-Pol      Available
[ ] Certificate Enrollment Web Service           ADCS-Enroll-Web-Svc      Available
[ ] Certification Authority Web Enrollment       ADCS-Web-Enrollment      Available
[ ] Web Application Proxy                      Web-Application-Proxy    Available
[ ] Remote Desktop Web Access                  RDS-Web-Access          Available
[ ] Web Server (IIS)                           Web-Server              Available
[ ] Web Server
  [ ] Common HTTP Features                   Web-Common-Http        Available
  [ ] Default Document                     Web-Default-Doc        Available
  [ ] Directory Browsing                   Web-Dir-Browsing       Available
  [ ] HTTP Errors                          Web-Http-Errors        Available
  [ ] Static Content                      Web-Static-Content     Available
  [ ] HTTP Redirection                   Web-Http-Redirect      Available
  [ ] WebDAV Publishing                  Web-DAV-Publishing     Available
[ ] Health and Diagnostics                 Web-Health             Available
[ ] HTTP Logging                         Web-Http-Logging       Available
[ ] Custom Logging                      Web-Custom-Logging     Available
[ ] Logging Tools                       Web-Log-Libraries      Available
[ ] ODBC Logging                        Web-ODBC-Logging       Available
[ ] Request Monitor                    Web-Request-Monitor    Available
```

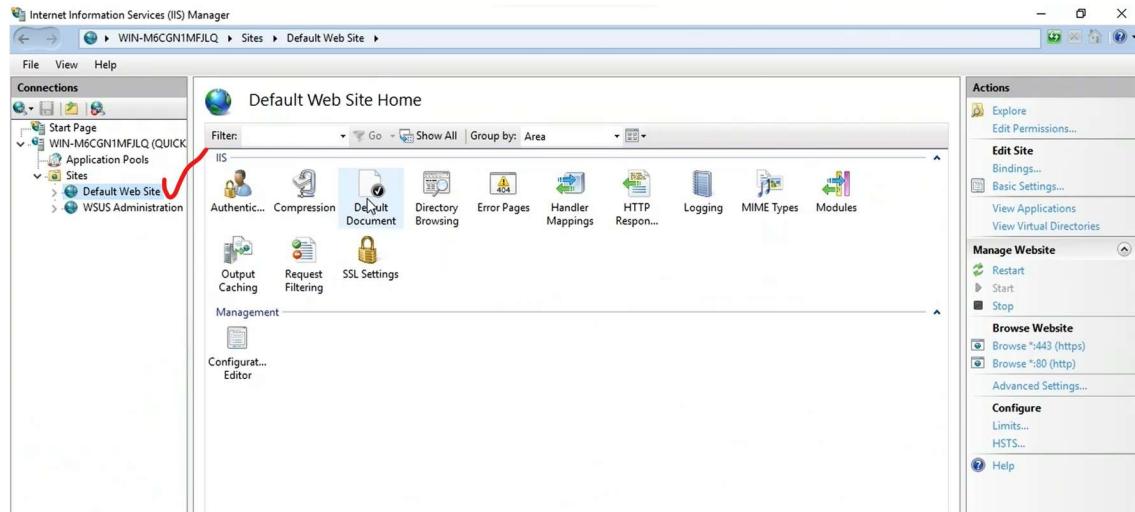
In the Display Name column there is no **x** inside the **[]** web Server (IIS) and that means the server is not installed yet. To install the service, we can use **install-windows feature** or **add-windows feature cmdlets**. We can also use GUI:

Start menu → Server Manager



Add roles and features → next (select role-based or feature-based installation) → select a server in from the server pool → in the bottom we will find IIS and we will select that then we will click next → we will select next, and **Role Services** screen will appear (we will only select HTTP Redirection when we want to check if secure cookies are being used, Windows Authentication will let us use credentials to log in, we should not use FTP server or in other words it transmits everything including signing credentials over the network unless we use a service called secure FTP and it will transmit everything even if we use VPN for tunneling) → next → install → we will then close it and we will see that it appears. We can also find it inside **Windows Administrative Tools** from the start menu





Default Document is when someone visits our website it will first appear. We can click one and we can move up and down to select the priority that which one will pop up first. We can view the default folder c drive → inetpub → wwwroot

Authentication:

Default web site → Authentication → Anonymous Authentication is enabled that means anyone can visit the homepage without any credentials → we will edit it

Directory Browsing → This feature is very important incase of webapp security. We must have strong security and authentication in order to active this feature

Error Pages → We can control the Error Pages details that will pop up depending on the HTTP status code like a 403 error, for example. **A 403 is a forbidden code where something has been requested through the web server but the web server refuses to grant access to it.**

SSL Settings → SSL is outdated protocol, and we should use TLS instead of it. By enabling SSL server side, you need a PKI certificate, and it protects the network connection. But what we're talking about here is setting up an option where clients can also have PKI certificates installed on client devices. And if we choose Require, our web server would have to trust the issuer of those certificates before the client is even allowed to try to authenticate to our web application. So, it's just an additional layer of security for highly secure websites.

If we right click in the Default Web Site we can see Site Bindings too, we can click edit to see the details. I can choose Edit Bindings and notice that we have both a http binding on TCP Port 80 as well as one on 443 https. We could click Edit to see the details. It looks like there's a default SSL certificate already assigned to the server. And if we clicked View, we get a message saying the certificate can't be verified up to a trusted certification authority, so we can see who it was Issued by. In other words, this is a private certificate issued by a private certification authority. This means that when client devices connect to this website over HTTPS, their devices by default will not trust the issuer of the certificate, unless we install it on all of those devices. So, if you could have a public facing web application, you need to make sure that you have a certificate issued by a publicly trusted certification authority. So, at this point, we've now set up a basic default Microsoft Internet Information Services or IIS web server stack.

 This document is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this document, or any portion of it, may result in severe civil and criminal penalties and will be prosecuted to the maximum extent possible under the law.

For permissions to use or reproduce this document or for any questions related to copyright, please contact: abidbiswas2021@gmail.com