**USTH-BS3 – Web Security -Lab 05: Securing web servers (about 1.5 hour)  
  
1. Purpose**: To apply measures to enhance the security of the Microsoft IIS web servers

**2. Pre-Requirements**:

+ Students know how to install Windows OS on a machine

+ Students know how to install Microsoft IIS web servers on Windows machines

**3. Lab Content**:

3.1 Prepare a Windows machine (can be Windows 8, Windows 10, or Windows 2008/2012 servers)

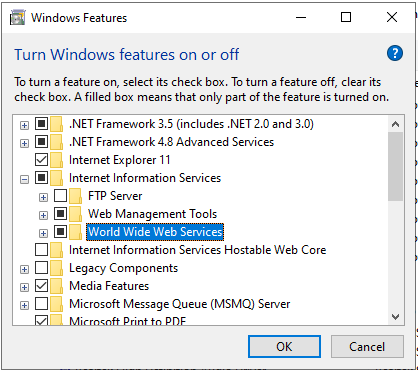
+ Install Windows (Windows 2008/2012 servers preferred) on a virtual machine if you do not have one

+ Make sure that the Windows copy is updated.

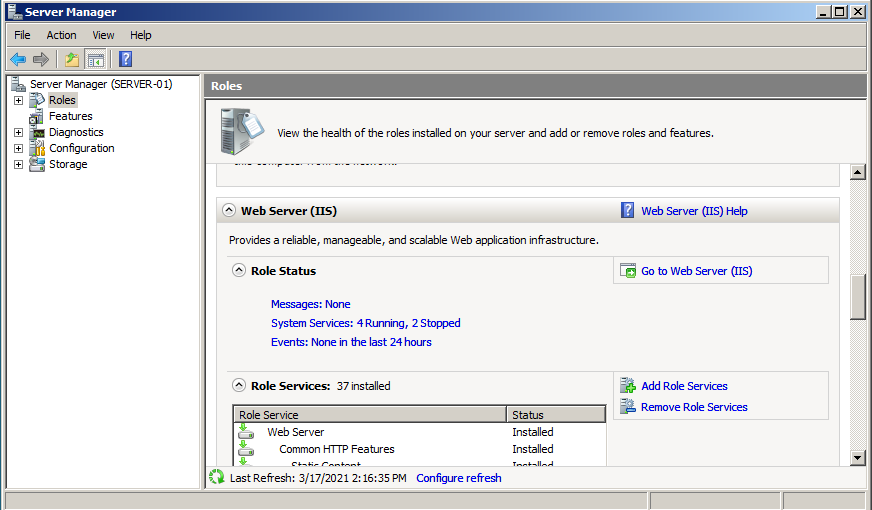
3.2 Install Microsoft IIS web server and make sure IIS is working

+ Check if Microsoft IIS is installed on the machine:

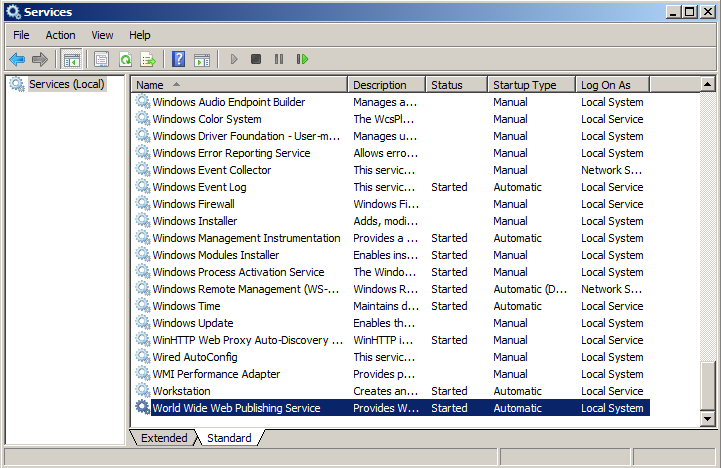
- On Windows 8, Windows 10: Open Control Panel / Programs and Features, then click at function “Turn Windows Features on or off”, check for World Wide Web Services



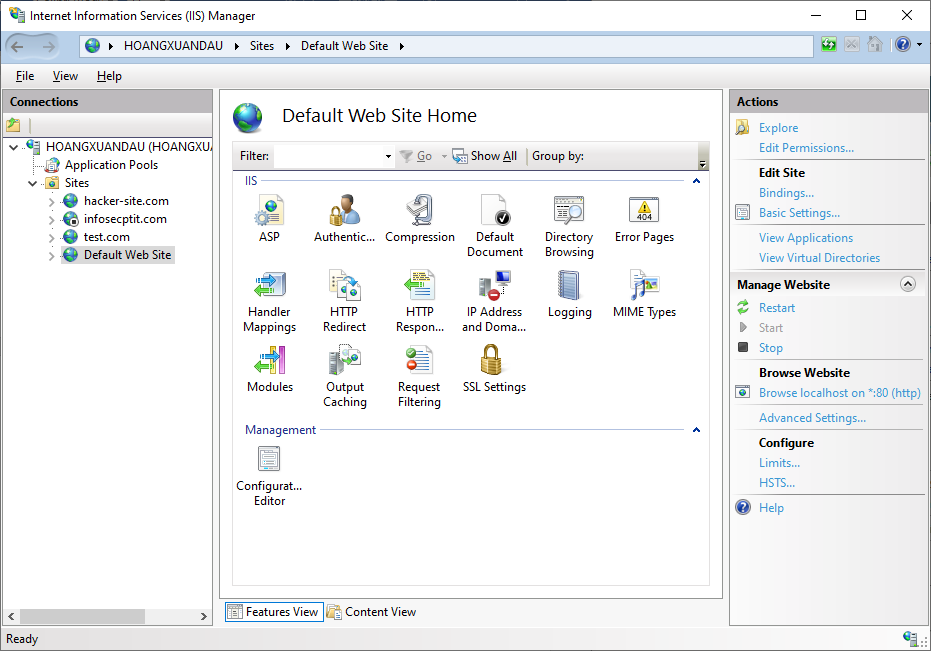
- On Windows server, click at Start / Administrative Tools / Server Manager, Open Roles on the left menu:



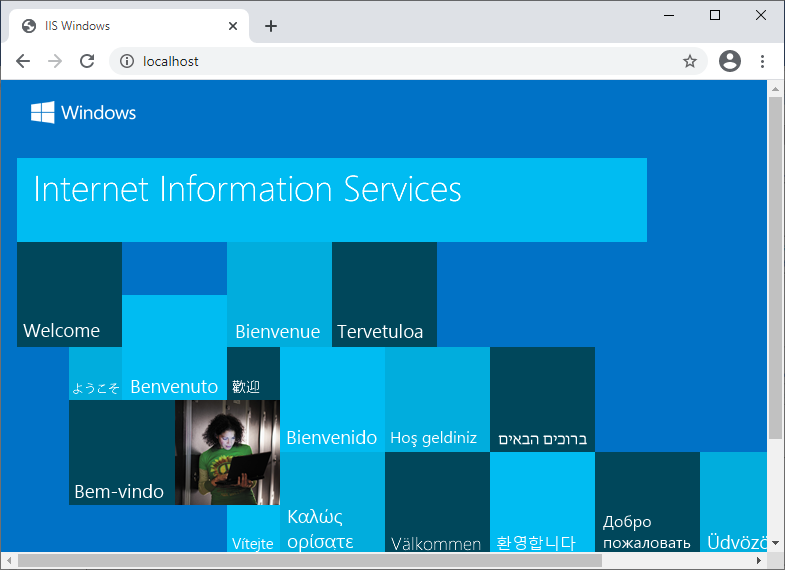
+ Install Microsoft IIS if not installed on the machine: Open Services manager and check for “World Wide Web Publishing Service”



+ Check if IIS is working with the default website:



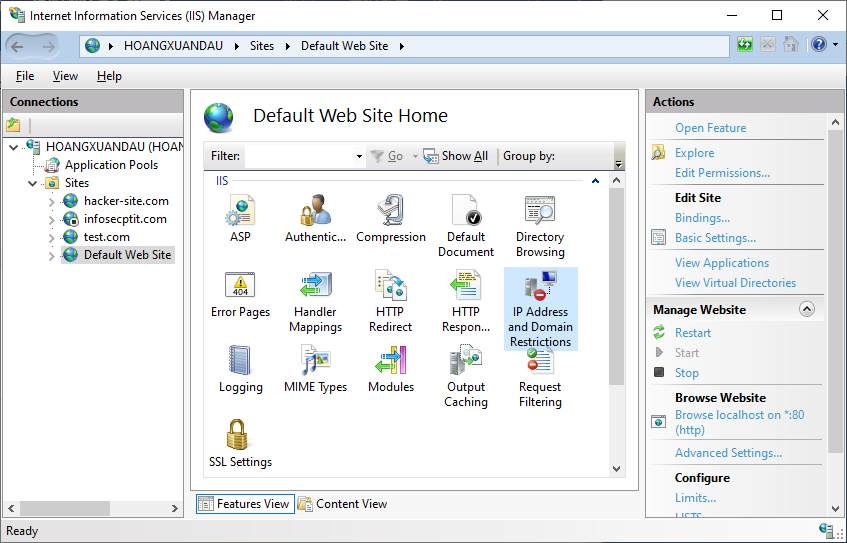
Microsoft IIS Manager

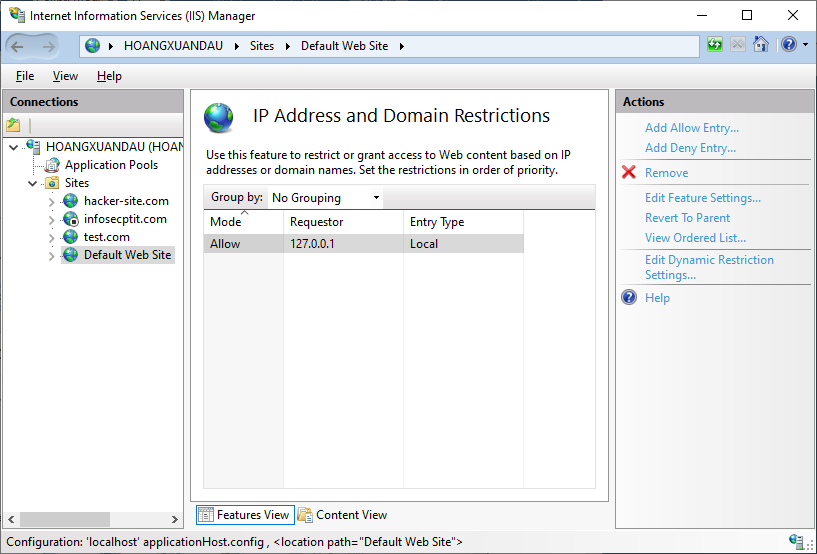


Microsoft IIS default website

3.3 Restrict accesses to IIS using IP and domains: This is used when we need to restrict the accesses to a website or web folder from specific IPs or domains.

+ Open the Microsoft IIS Manager, then navigate to the website or web folder that need to add a restriction:



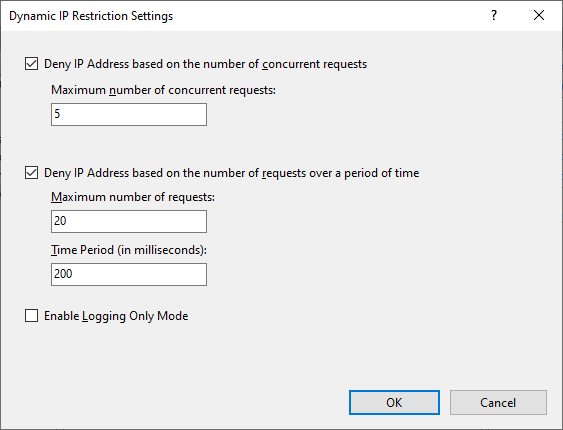


IP Address and Domain Restrictions

- Add Allow Entry: To add an IP address or a range of IPs that can access the site or folder

- Add Deny Entry: To add an IP address or a range of IPs that are forbidden to access the site or folder

- Edit Dynamic Restriction Settings: Enable and change the settings for dynamic Restriction to the accesses to the site or folder



3.4 To do tasks for students (with screenshots taken)

1. Have Microsoft IIS installed

2. Have Microsoft IIS working with default website

3. Enable an allow IP and access the default website from web browser

4. Enable a deny IP and access the default website from web browser

5. Enable Dynamic Restriction Settings for the website and use hping3 to send large amount of request to the website and view the results (hping3 is available in Kali Linux or you can get it from <http://www.hping.org/download.html>).

Ex: send SYN flood to < target> with random source IPs:

hping3 <target> -q -d 120 -S -p 80 --flood --rand-source

**USTH-BS3 – Web Security -Lab 06: Scan websites for vulnerabilities (about 1.5 hour)  
  
1. Purpose**: Using Acunetix web vulnerability or OWASP ZAP scanner to scan websites for vulnerabilities

**2. Pre-Requirements**:

+ Students knew the common types of vulnerabilities on websites and web applications

**3. Lab Content**:

3.1. Download and install Acunetix web vulnerability/ OWASP ZAP scanner

+ Information about Acunetix web vulnerability scanner can be found at <https://www.acunetix.com/vulnerability-scanner/>

+ Get OWASP ZAP at: https://www.zaproxy.org/download/

+ Install on your machine if you do not have one ready.

3.2. Use scanner to scan at least 5 websites (you can select 5 other websites):

+ <https://usth.edu.vn>

+ <http://dantri.com.vn>

+ <https://huonglieuminhkien.com>

+ <https://vietnamnet.vn>

+ https://www.vietcombank.com.vn

3.3. Analyze the scanned reports.