Lab 2: Create a Self-signed Certificate

Lab Scenario

As a professional ethical hacker and penetration tester, you must possess a proper knowledge of creating this certificate as it validates the public key contained within the certificate belonging to the person, company, server, or other entity mentioned. The labs in this exercise demonstrate the creation of a self-signed certificate.

Lab Objectives

- Create and use self-signed certificates

Overview of Self-signed Certificate

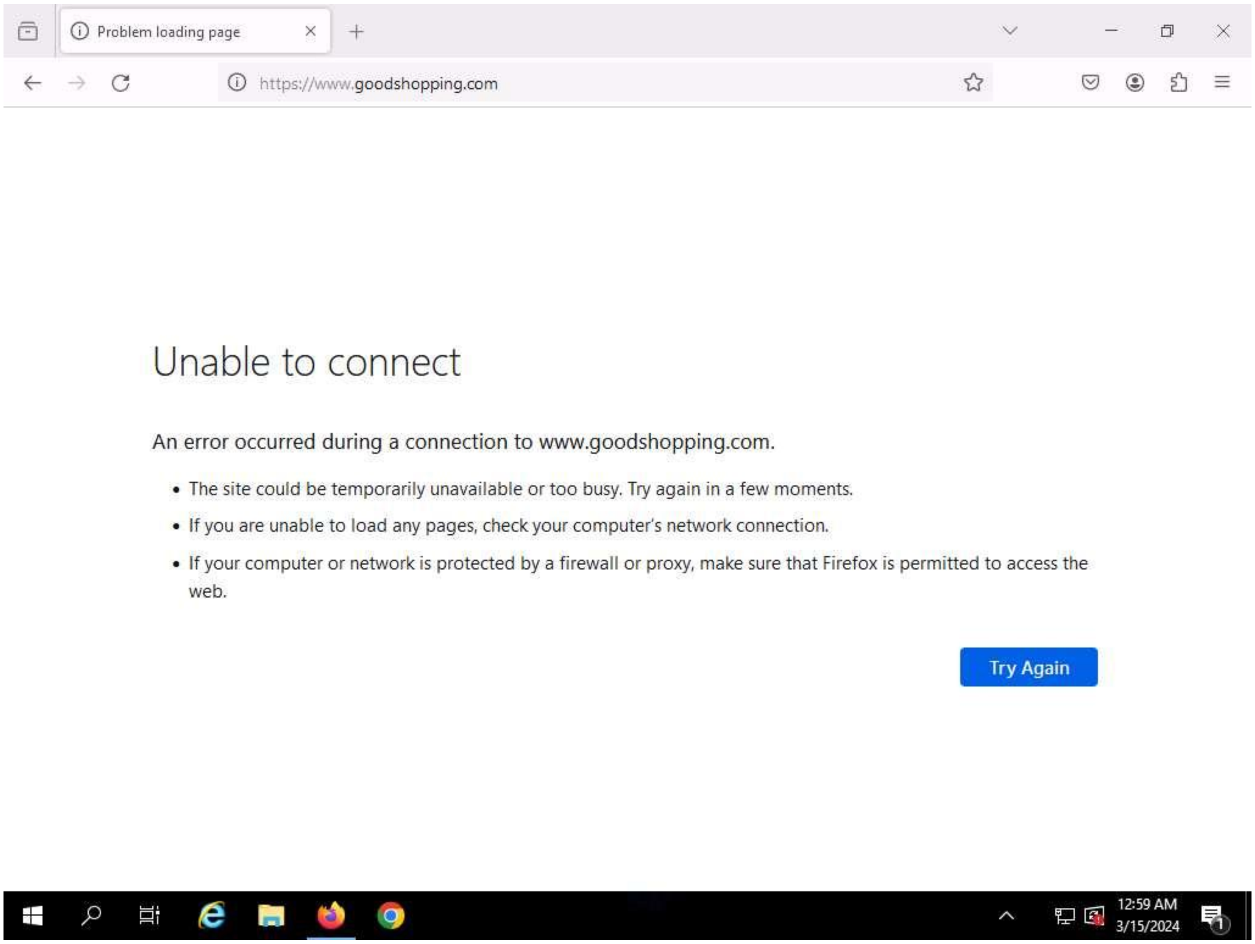
In cryptography and computer security, a self-signed certificate is an identity certificate signed by the same entity whose identity it verifies. However, the term is unrelated to the identity of the person or organization that actually performs the signing procedure.

Task 1: Create and Use Self-signed Certificates

Self-signed certificates are widely used for testing servers. In self-signed certificates, a user creates a pair of public and private keys using a certificate creation tool such as Adobe Acrobat Reader, Java's keytool, Apple's Keychain, etc. and signs the document with the public key. The recipient requests the private key from the sender in order to verify the certificate. However, certificate verification rarely occurs due to the necessity of disclosing the private key: this makes self-signed certificates useful only in a self-controlled testing environment.

Here, we will create a self-signed certificate in Windows Server 2019.

1. Click on Windows Server 2019 to switch to the **Windows Server 2019**. Click Ctrl+Alt+Delete to activate the machine and login with **Administrator**/**Pa$$w0rd**.
2. Before you start this task, you will need to check with your local sites whether they include a self-signed certificate.
3. Launch any web browser, and go to **https://www.goodshopping.com** (here, we are using **Mozilla Firefox**).
4. As you are using an https channel to browse the website, it displays a page stating that **Unable to connect**.
5. As the site does not have a self-signed certificate, it displays a error message, as shown in the screenshot. Close the web browser.

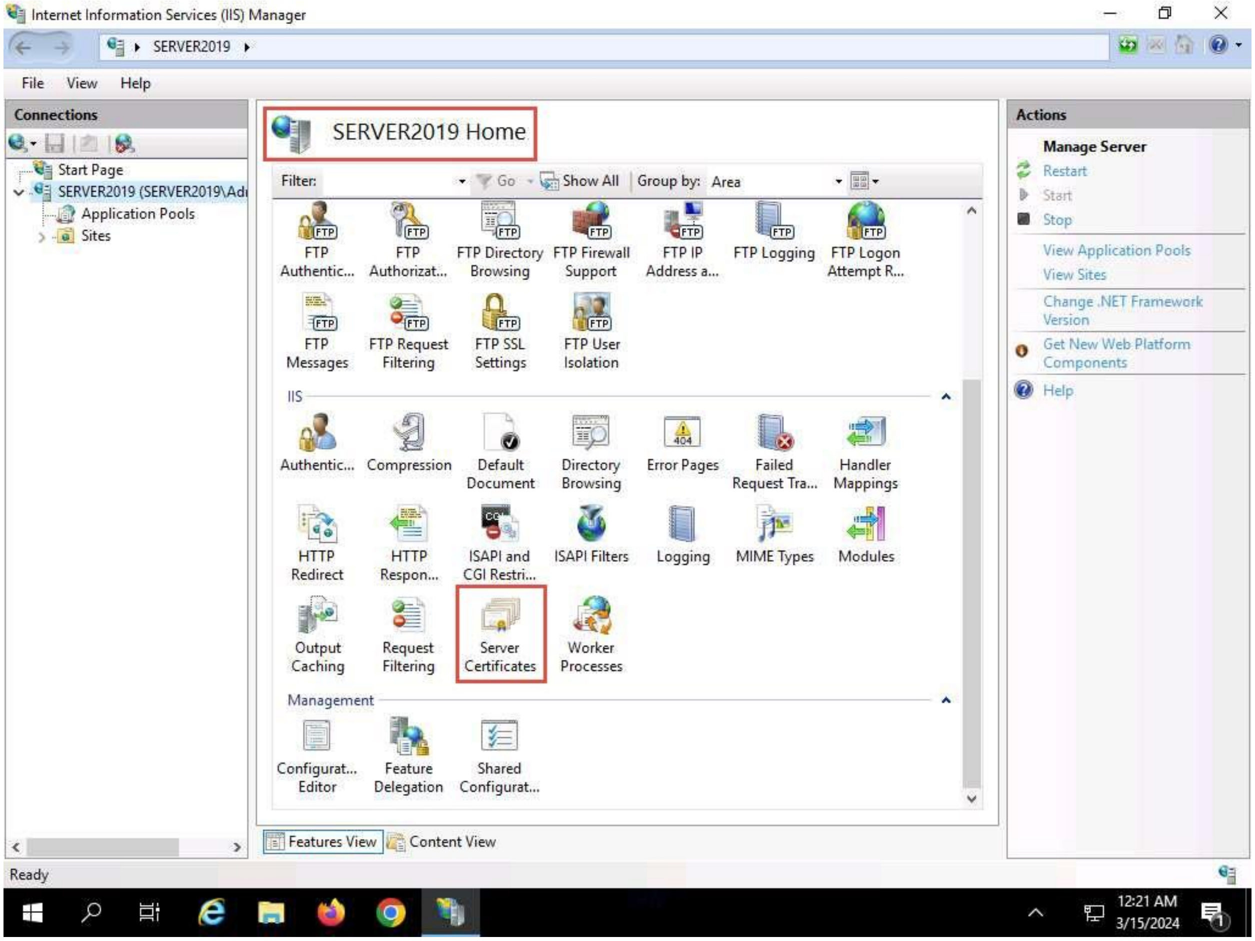


Unable to connect

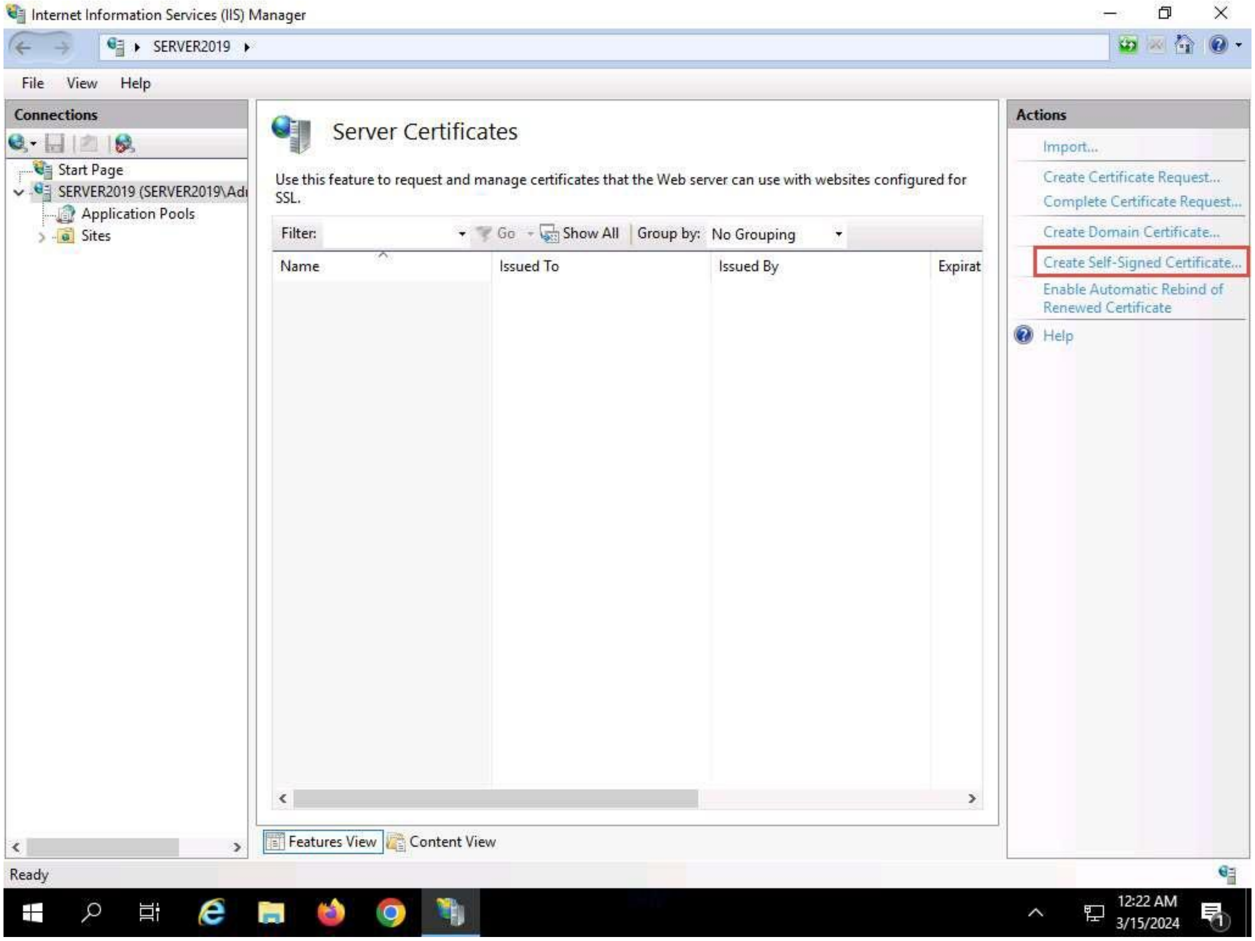
An error occurred during a connection to www.goodshopping.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

6. Click the **Type here to search** icon present in the bottom-left of **Desktop** and type **iis**. Select **Internet Information Services (IIS) Manager** from the results.
7. The **Internet Information Services (IIS) Manager** window appears; click the machine name (**SERVER2019 (SERVER2019\Administrator**)) under the **Connections** section from the left-hand pane.
8. In **SERVER2019 Home**, double-click **Server Certificates** in the **IIS** section.

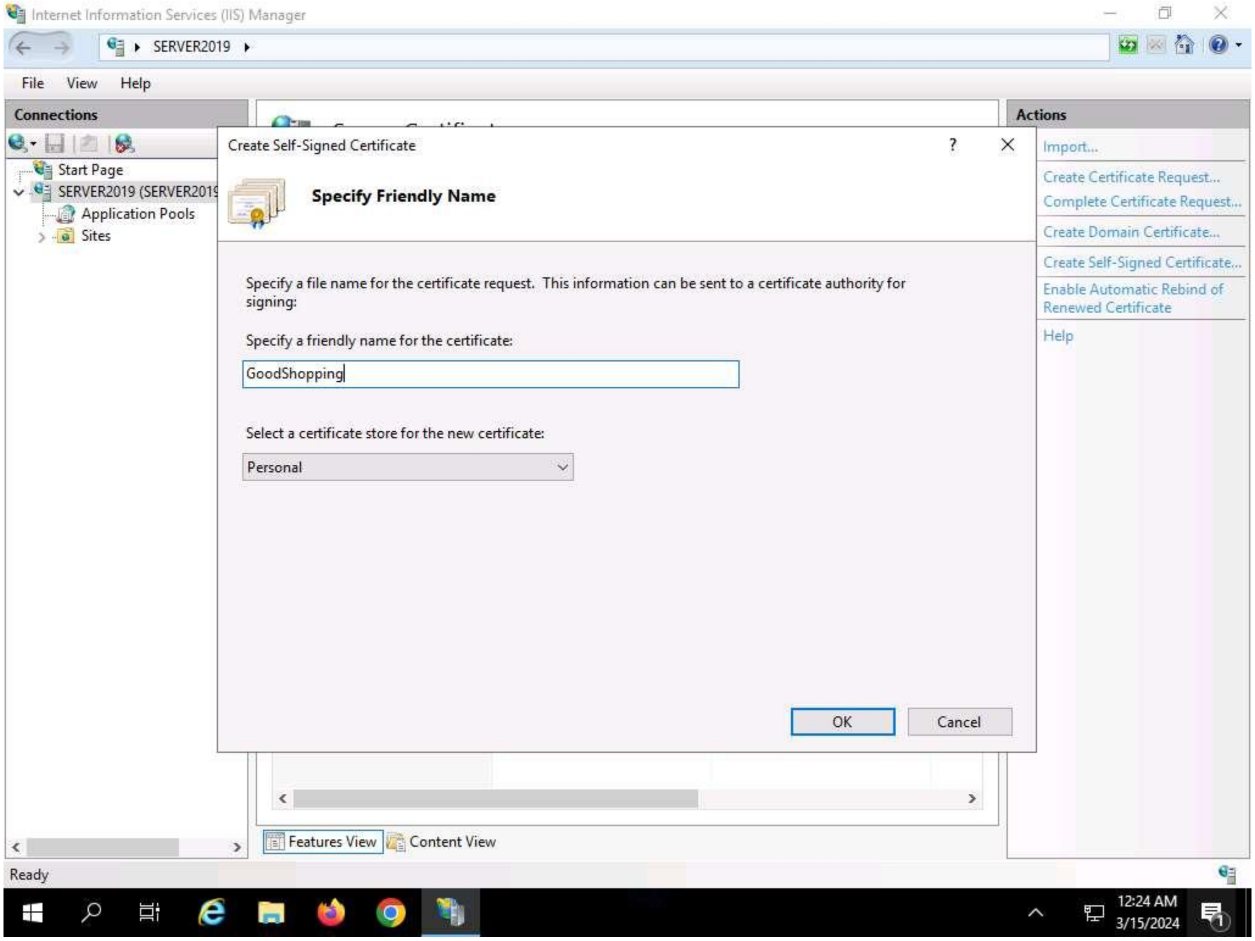


9. The **Server Certificates** wizard appears; click **Create Self-Signed Certificate...** from the right-hand pane in the **Actions** section.


Internet Information Services (IIS) Manager
SERVER2019
File
View
Help
Connections
Start Page
SERVER2019 (SERVER2019\Adı
Application Pools
Sites
Server Certificates
Filter:
Go
Show All
Group by:
No Grouping
Name
Issued To
Issued By
Expirat
Features View
Content View
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Ready
12:22 AM
3/15/2024

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

10. The **Create Self-Signed Certificate** window appears; type **GoodShopping** in the **Specify a friendly name for the certificate** field. Ensure that the **Personal** option is selected in the **Select a certificate store for the new certificate** field; then, click **OK**.



Internet Information Services (IIS) Manager
SERVER2019
File
View
Help
Connections
Start Page
SERVER2019 (SERVER2019
Application Pools
Sites
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready
12:24 AM
3/15/2024

Create Self-Signed Certificate

Specify Friendly Name

Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

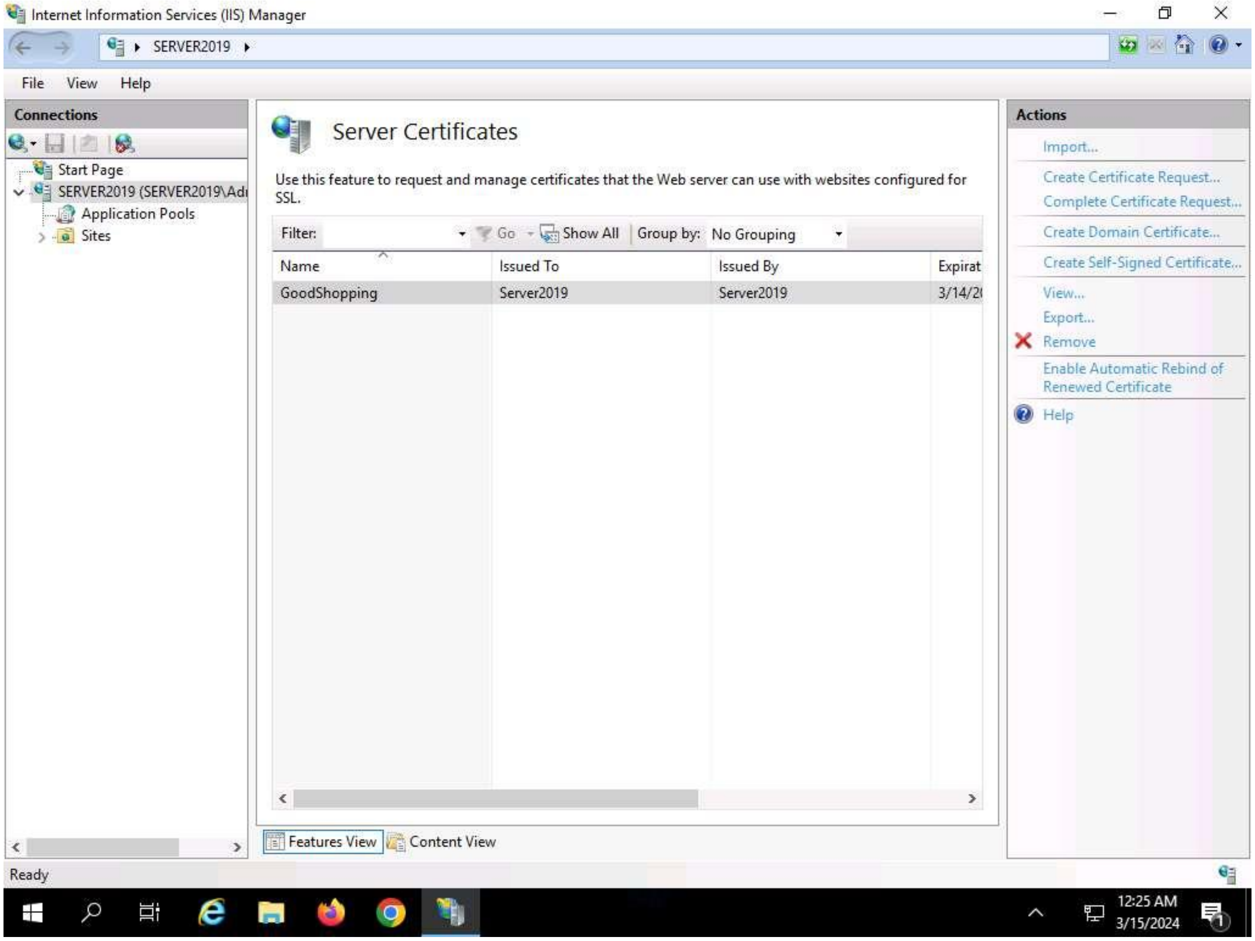
Specify a friendly name for the certificate:

GoodShopping

Select a certificate store for the new certificate:

Personal

11. A newly created self-signed certificate will be displayed in the **Server Certificates** pane, as shown in the screenshot.


Internet Information Services (IIS) Manager
SERVER2019
File
View
Help
Connections
Start Page
SERVER2019 (SERVER2019\Adı
Application Pools
Sites
Features View
Content View
Ready
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
12:25 AM
3/15/2024

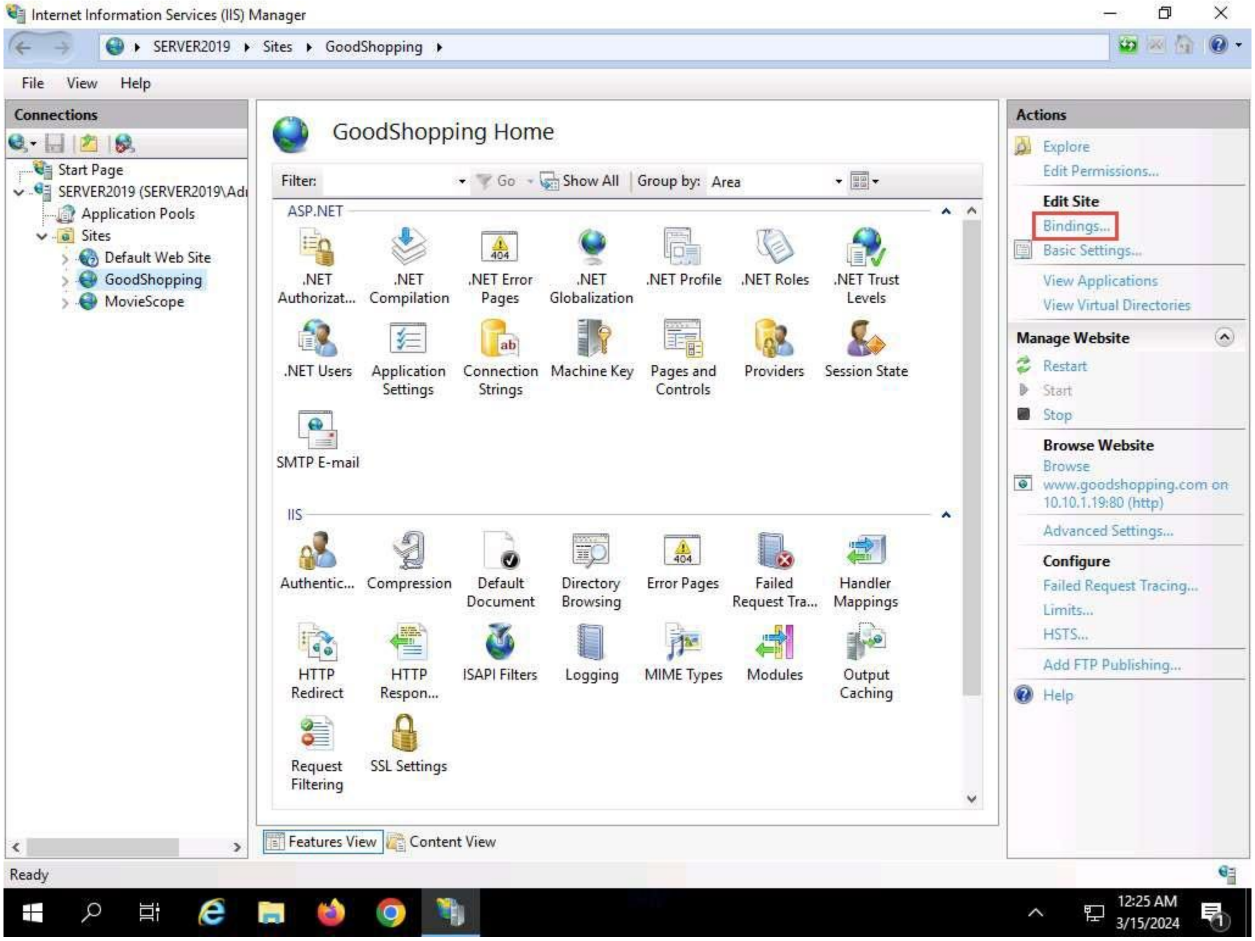
Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

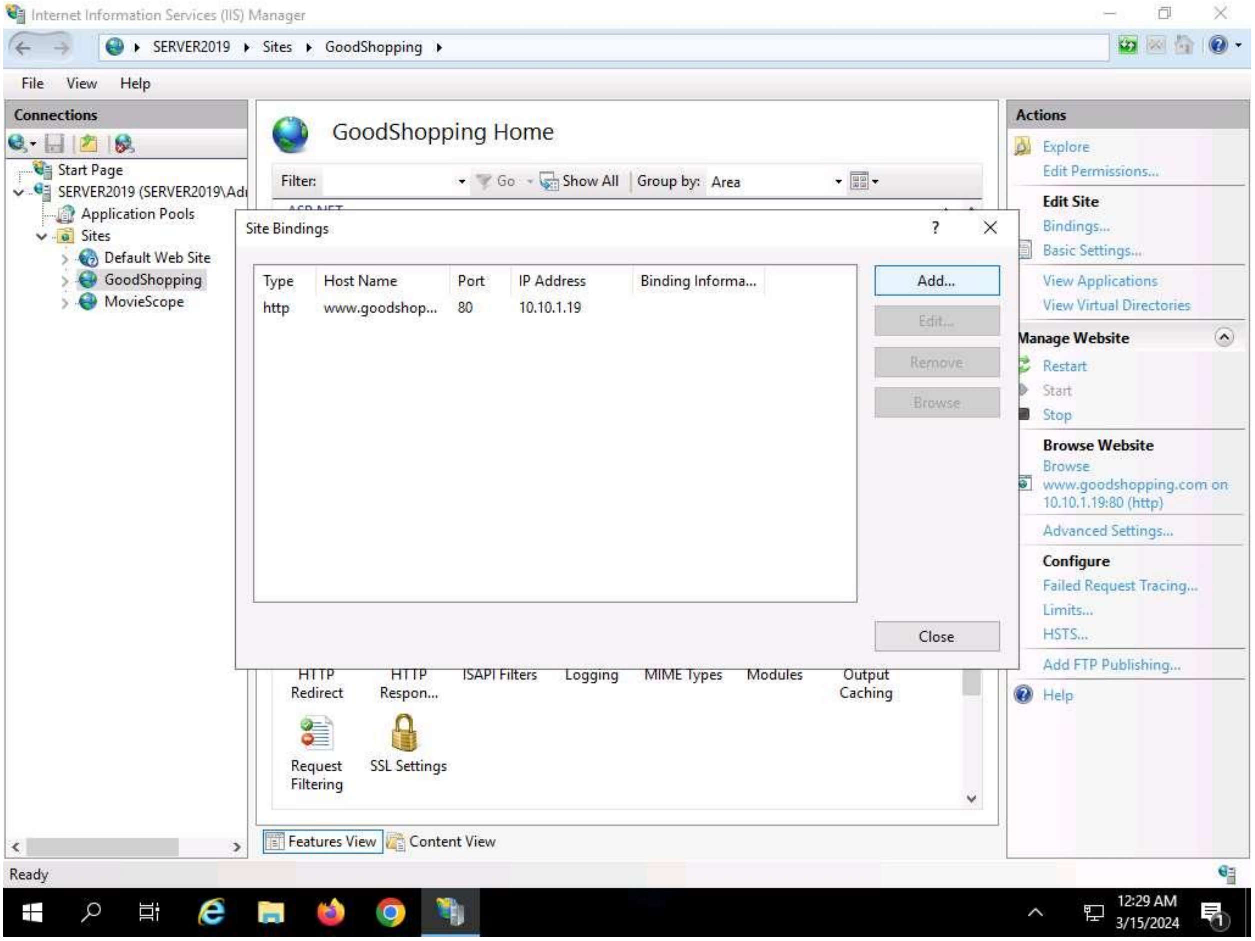
Filter: Go Show All Group by: No Grouping

Name	Issued To	Issued By	Expirat
GoodShopping	Server2019	Server2019	3/14/2(

12. Expand the **Sites** node from the left-hand pane, and select **GoodShopping** from the available sites. Click **Bindings…** from the right-hand pane in the **Actions** section.



13. The **Site Bindings** window appears; click **Add…**.

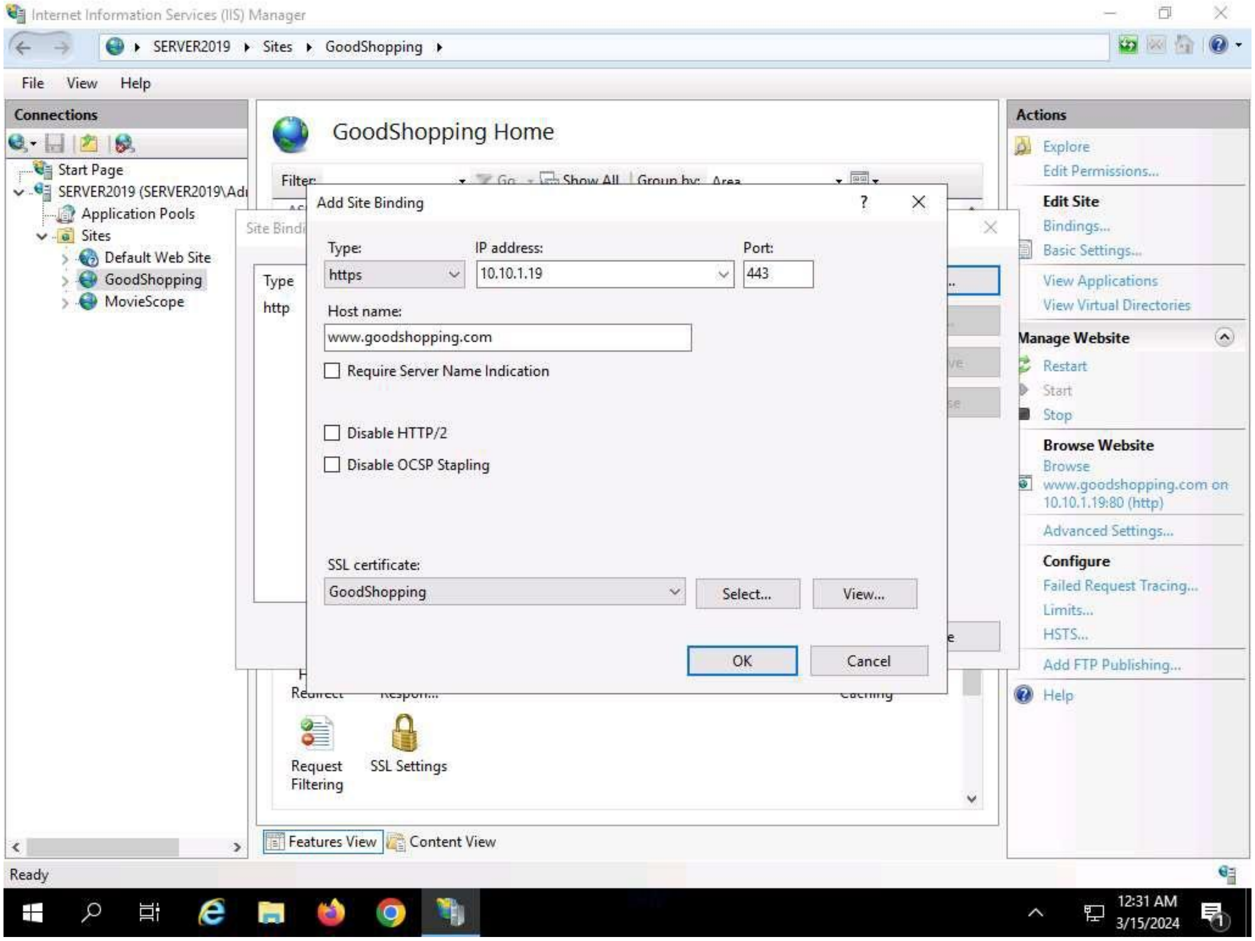


Type	Host Name	Port	IP Address	Binding Informa...
http	www.goodshop...	80	10.10.1.19	

14. The **Add Site Binding** window appears; choose **https** from the **Type** field drop-down list. Once you choose the https type, the port number in the **Port** field automatically changes to **443** (the channel on which HTTPS runs).

15. Choose the **IP address** on which the site is hosted (here, **10.10.1.19**).

16. Under the **Host name** field, type **www.goodshopping.com**. Under the **SSL certificate** field, select **GoodShopping** from the drop-down list, and click **OK**.



Add Site Binding

Type: https

IP address: 10.10.1.19

Port: 443

Host name: www.goodshopping.com

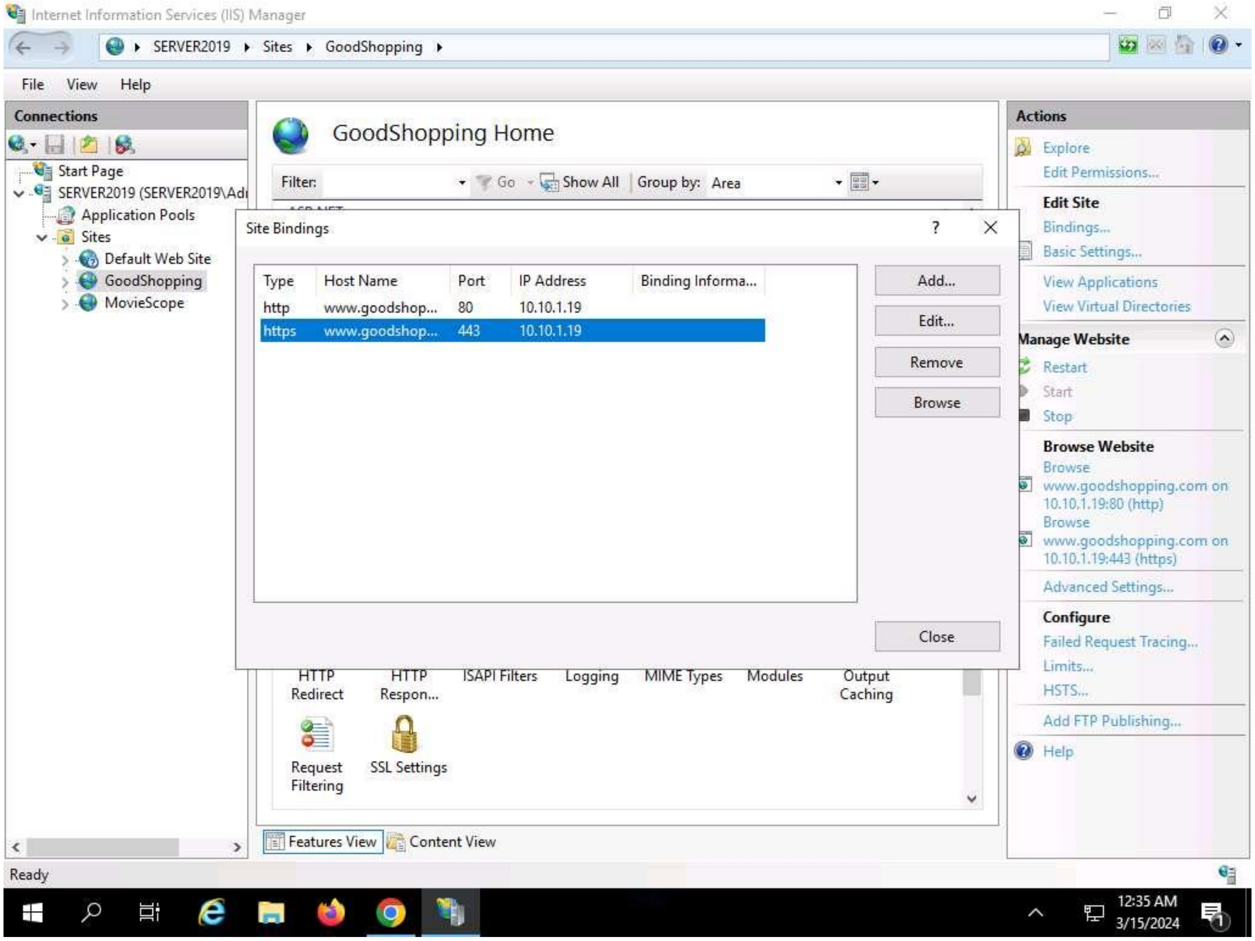
□ Require Server Name Indication

□ Disable HTTP/2

□ Disable OCSP Stapling

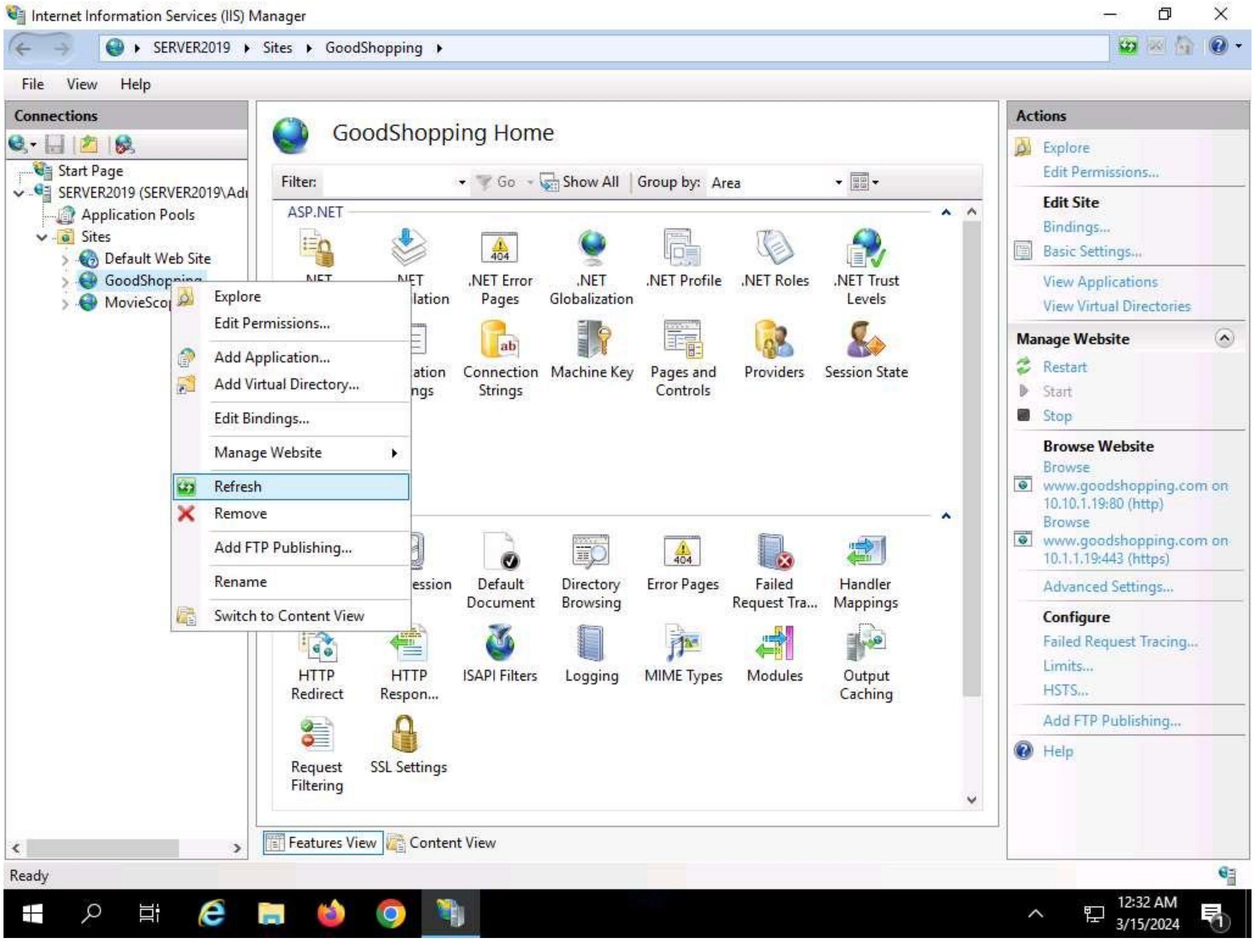
SSL certificate: GoodShopping

17. The newly created SSL certificate is added to the **Site Bindings** window; then, click **Close**.



Type	Host Name	Port	IP Address	Binding Informa...
http	www.goodshop...	80	10.10.1.19	
https	www.goodshop...	443	10.10.1.19	

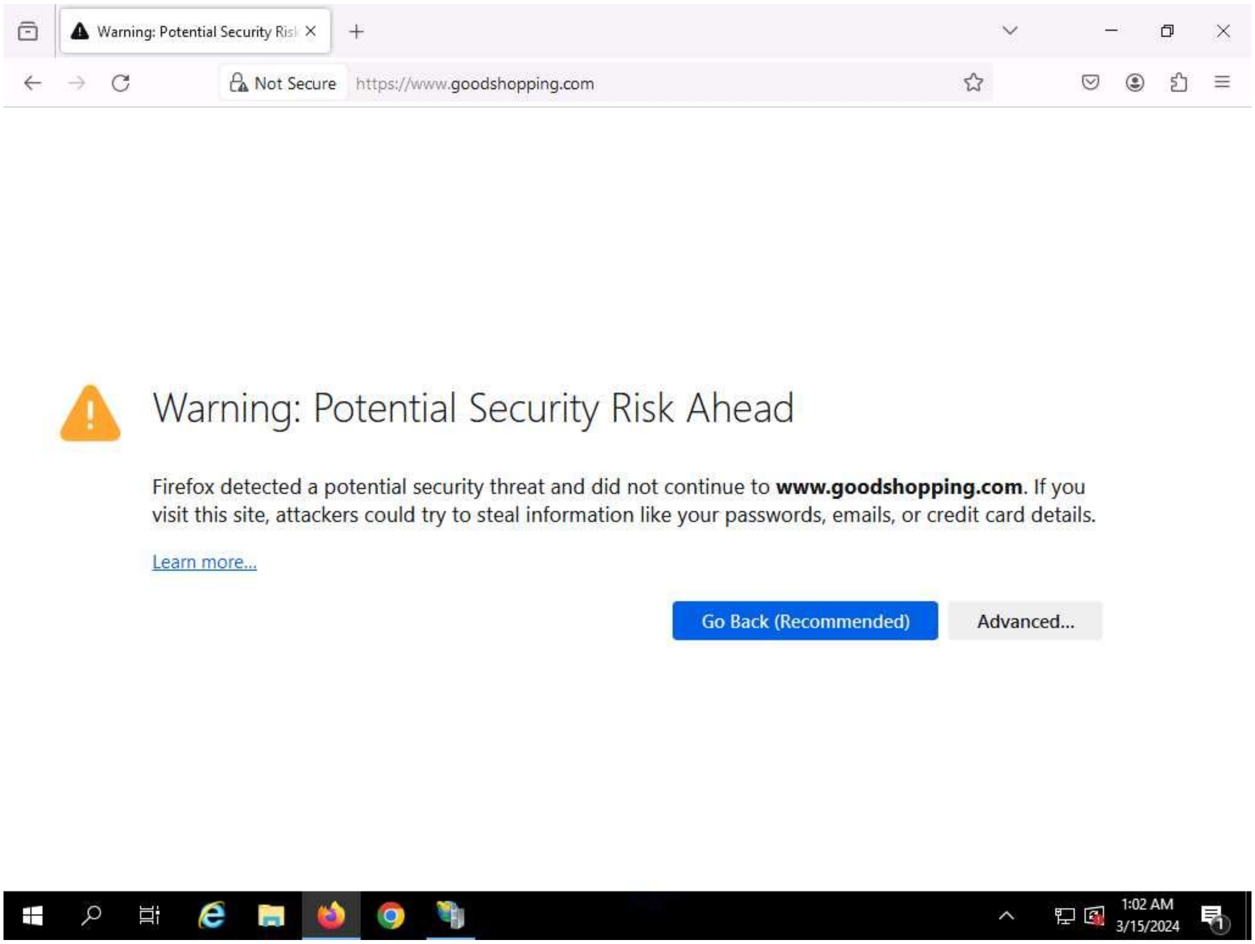
18. Now, right-click the name of the site for which you have created the self-signed certificate (here, **GoodShopping**) and click **Refresh** from the context menu.



19. Minimize the **Internet Information Services (IIS) Manager** window.

20. Open the **Mozilla Firefox** browser and go to **https://www.goodshopping.com**.

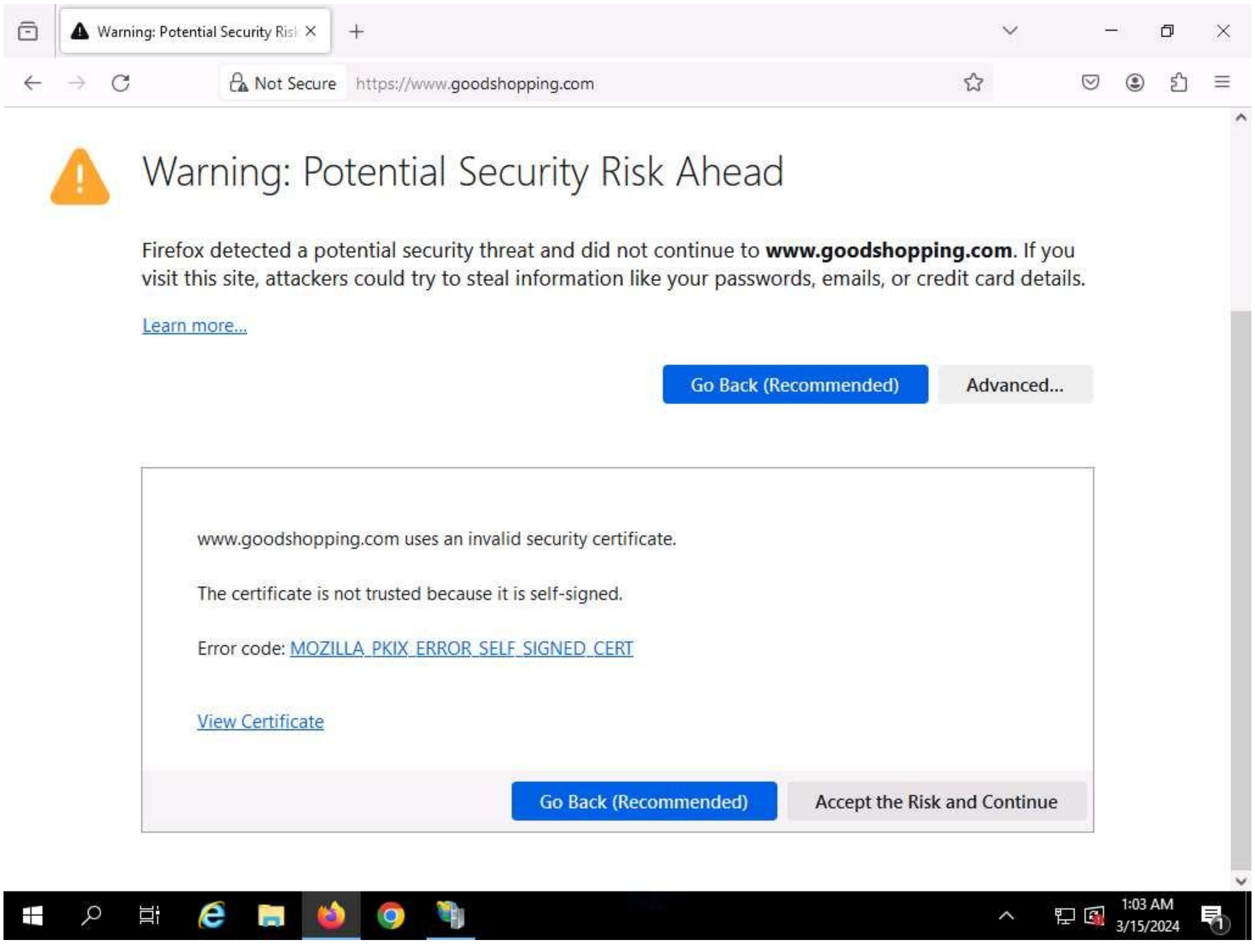
21. The **Warning:Potential Security Risk Ahead** message appears, click **Advanced…** to proceed.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **www.goodshopping.com**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

22. Click **Accept the Risk and Continue**.



Warning: Potential Security Risk
Not Secure
https://www.goodshopping.com
1:03 AM
3/15/2024

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **www.goodshopping.com**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more...

Go Back (Recommended) Advanced...

www.goodshopping.com uses an invalid security certificate.

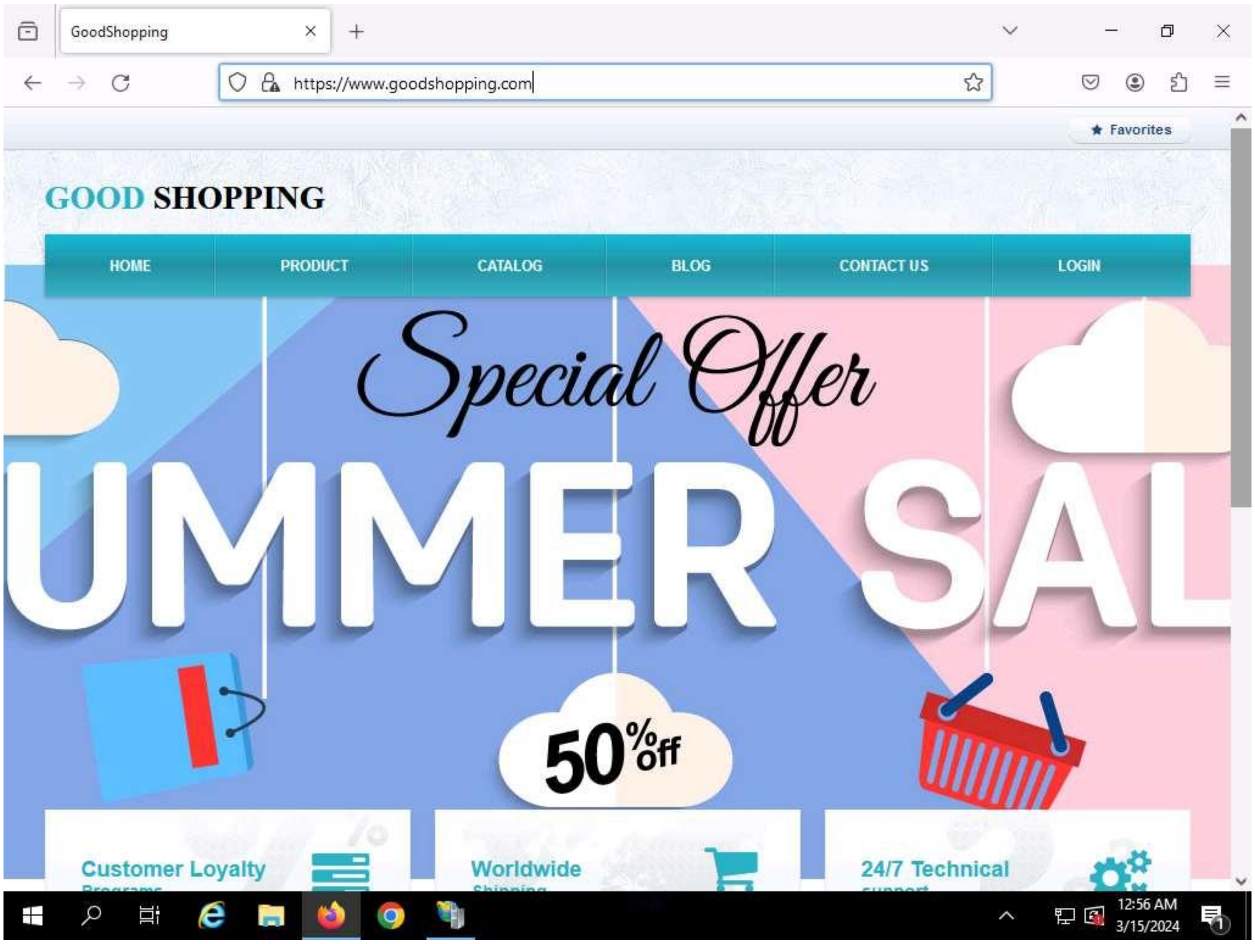
The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

View Certificate

Go Back (Recommended) Accept the Risk and Continue

23. Now you can see **Goodshopping webpage** with **ssl certificate** assigned to it, as shown in the screenshot.



24. This concludes the demonstration of creating and using a self-signed certificate.

25. Close all open windows and document all the acquired information.

Question 20.2.1.1

Create and use a self-signed certificate for the website www.goodshopping.com hosted on the machine at 10.10.1.19. Write the port number on which HTTPS is running in this task.