Cryptography and PKI

Exercise 1: Calculate One-way Hashes using HashCalc

Lab Scenario

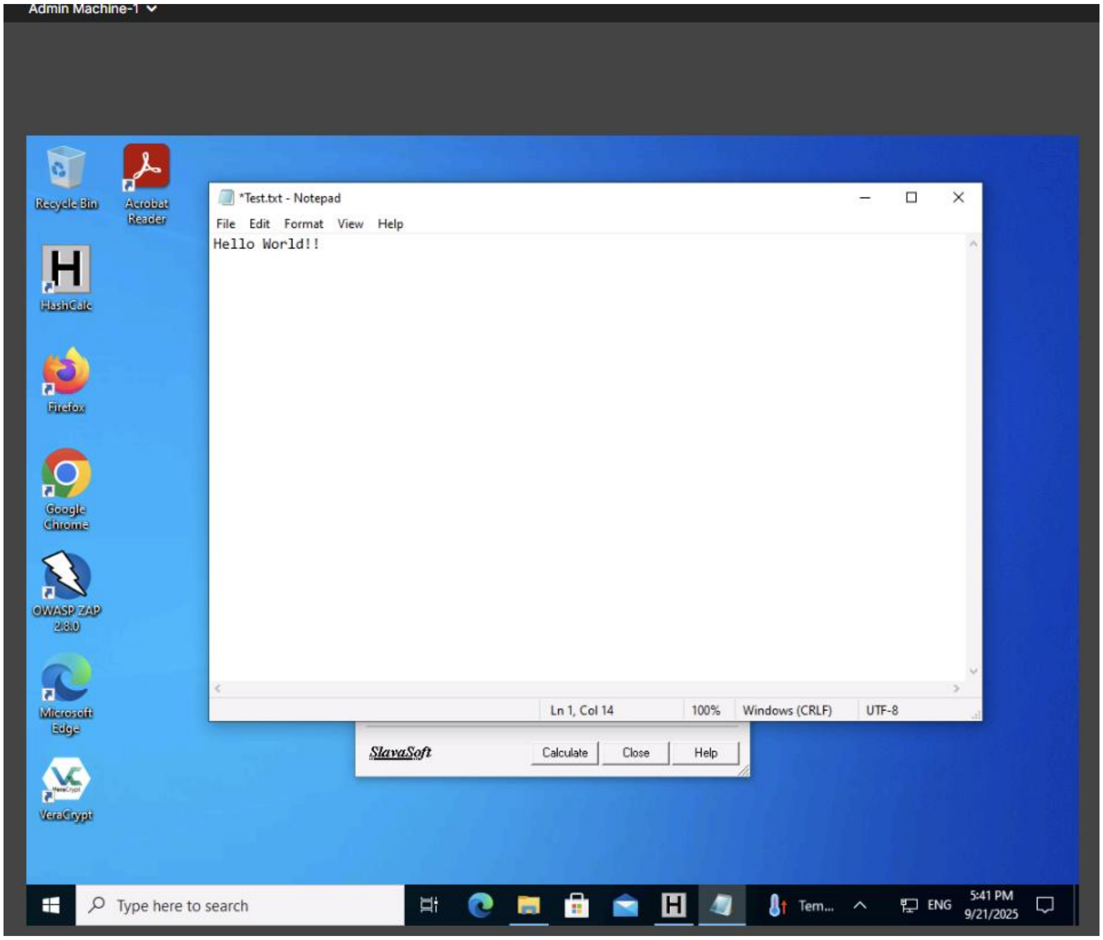
Message digests are also called one-way hash functions because they cannot be reversed.

Lab Objectives

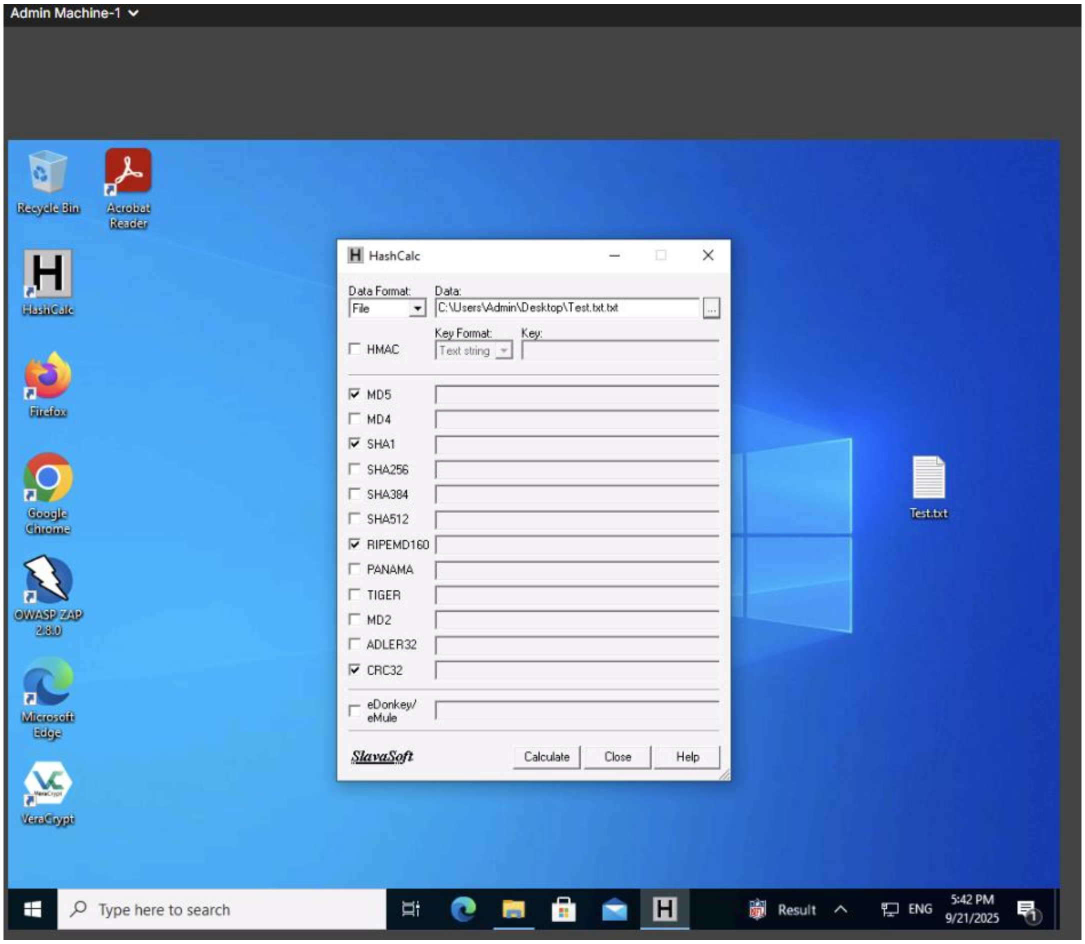
This lab demonstrates how to calculate one-way hashes using HashCalc for checking the integrity of a file by comparing hash values.

Overview of One-way Hash

Message digest (one-way hash) functions distill the information contained in a file (small or large) into a single fixed-length number, typically between 128 and 256 bits.



```
Hello World!!
```



HashCalc

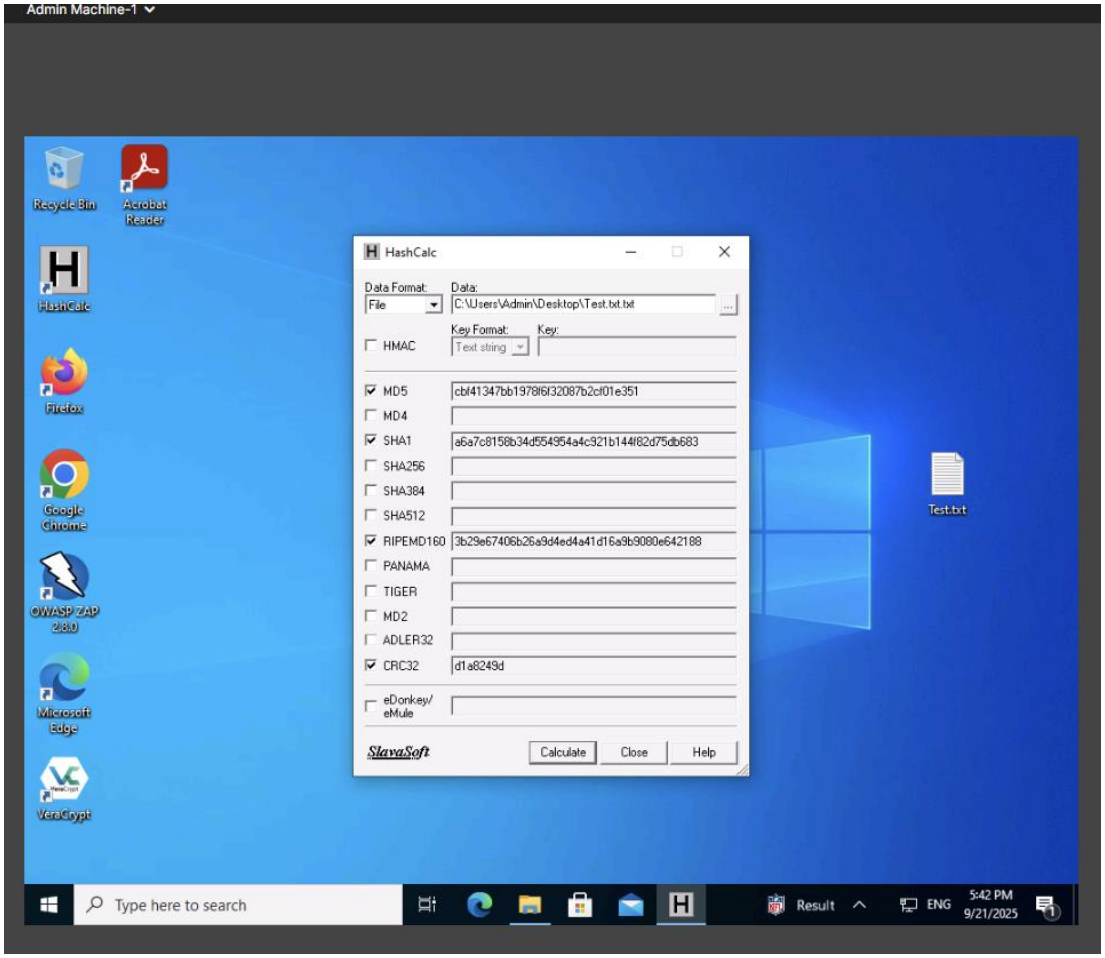
Data Format: File

Data: C:\Users\Admin\Desktop\Test.txt.txt

□ HMAC Key Format: Text string Key:

☑ MD5
□ MD4
☑ SHA1
□ SHA256
□ SHA384
□ SHA512
☑ RIPEMD160
□ PANAMA
□ TIGER
□ MD2
□ ADLER32
☑ CRC32

□ eDonkey/ eMule



HashCalc

Data Format: File

Data: C:\Users\Admin\Desktop\Test.txt.txt

□ HMAC Key Format: Text string Key:

☑ MD5 cbf41347bb1978f6f32087b2cf01e351

□ MD4

☑ SHA1 a6a7c8158b34d554954a4c921b144f82d75db683

□ SHA256

□ SHA384

□ SHA512

☑ RIPEMD160 3b29e67406b26a9d4ed4a41d16a9b9080e642188

□ PANAMA

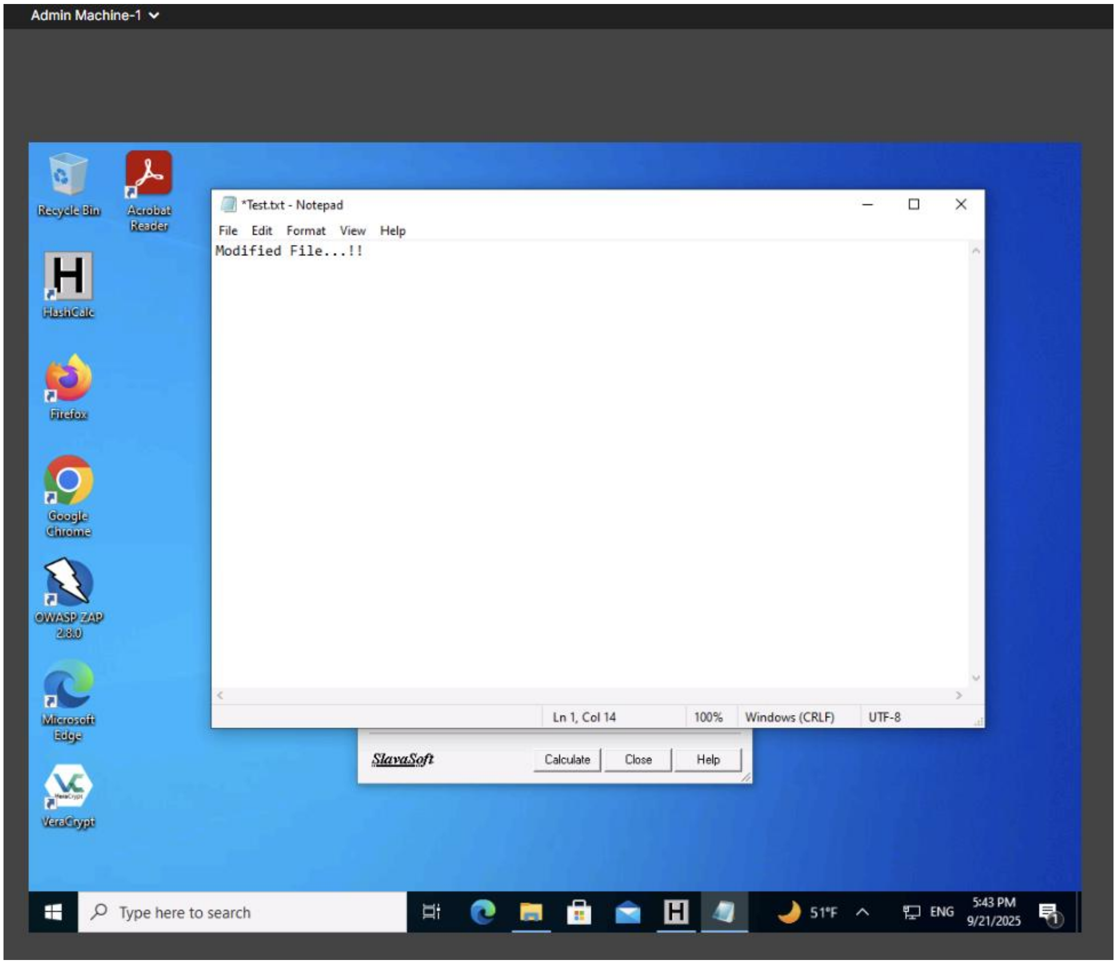
□ TIGER

□ MD2

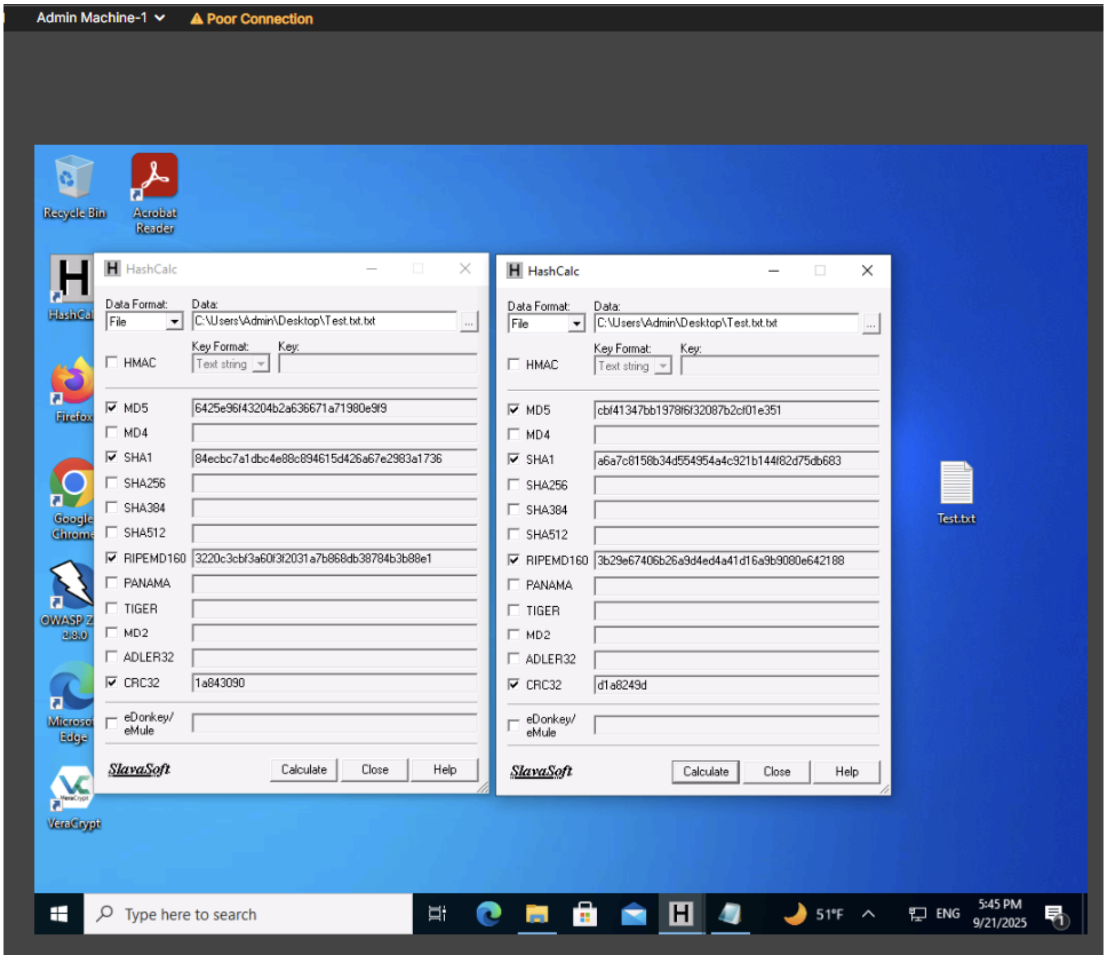
□ ADLER32

☑ CRC32 d1a8249d

□ eDonkey/ eMule



```
Modified File...!!
```



HashCalc

Data Format: File
Data: C:\Users\Admin\Desktop\Test.txt.txt
□ HMAC Key Format: Text string Key:
☑ MD5 6425e96f43204b2a636671a71980e9f9
□ MD4
☑ SHA1 84ecbc7a1dbc4e88c894615d426a67e2983a1736
□ SHA256
□ SHA384
□ SHA512
☑ RIPEMD160 3220c3cbf3a60f3f2031a7b868db38784b3b88e1
□ PANAMA
□ TIGER
□ MD2
□ ADLER32
☑ CRC32 1a843090
□ eDonkey/ eMule

HashCalc

Data Format: File
Data: C:\Users\Admin\Desktop\Test.txt.txt
□ HMAC Key Format: Text string Key:
☑ MD5 cbf41347bb1978f6f32087b2cf01e351
□ MD4
☑ SHA1 a6a7c8158b34d554954a4c921b144f82d75db683
□ SHA256
□ SHA384
□ SHA512
☑ RIPEMD160 3b29e67406b26a9d4ed4a41d16a9b9080e642188
□ PANAMA
□ TIGER
□ MD2
□ ADLER32
☑ CRC32 d1a8249d
□ eDonkey/ eMule

Exercise 2: Calculate MD5 Hashes using HashMyFiles

Lab Scenario

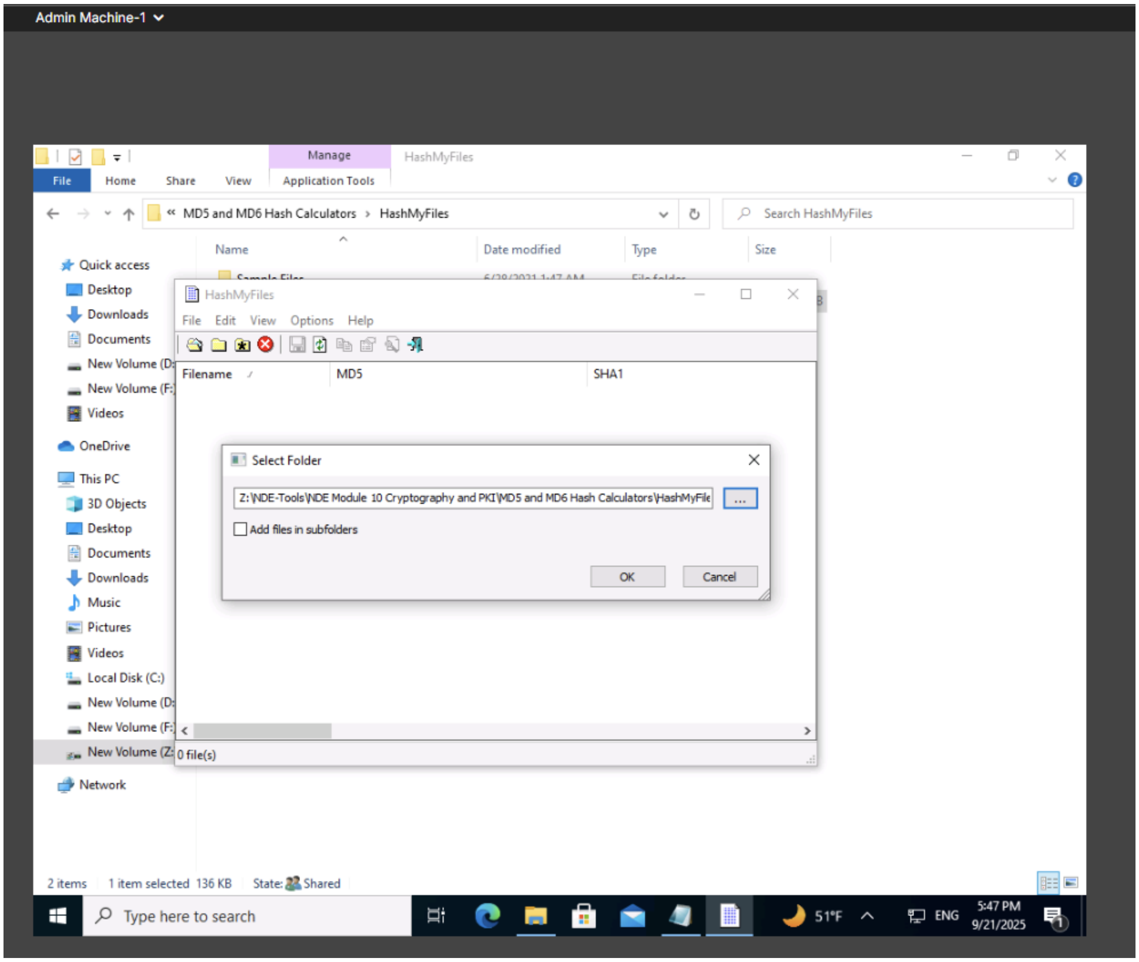
MD5 is a message digest algorithm used in digital signature applications to compress a document securely before the system signs it with a private key.

Lab Objectives

This lab demonstrates how to calculate the MD5 hashes of a given file using HashMyFiles.

Overview of MD5 Hashes

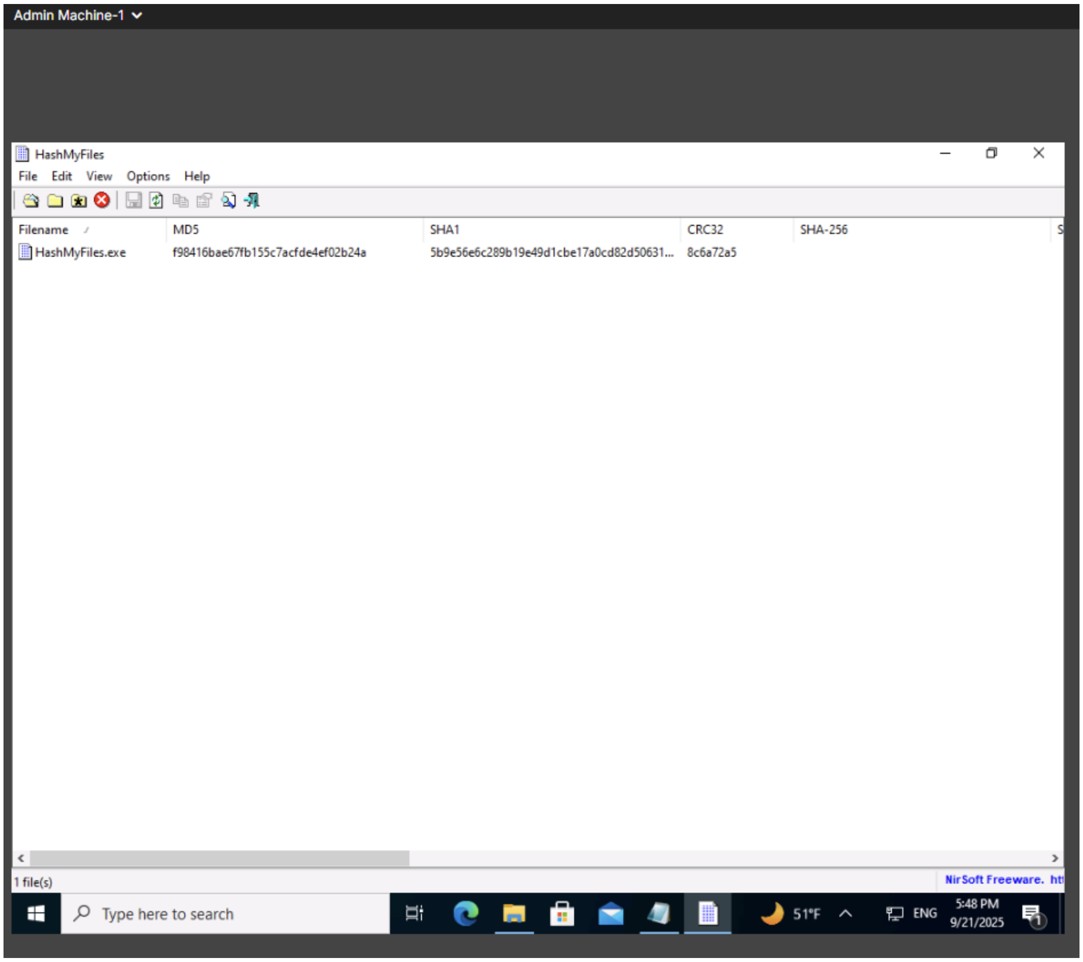
MD5 is a widely used cryptographic hash function that takes a message of arbitrary length as input and outputs a 128-bit (16-byte) fingerprint or message digest of the input. MD5 can be used in a wide variety of cryptographic applications and is useful for digital signature applications, file integrity checking, and storing passwords. However, MD5 is not collision resistant; therefore, it is better to use the latest algorithms, such as MD6, SHA-2, and SHA-3.



Select Folder

Z:\NDE-Tools\NDE Module 10 Cryptography and PKI\MD5 and MD6 Hash Calculators\HashMyFile

□ Add files in subfolders



Filename	MD5	SHA1	CRC32	SHA-256	S
HashMyFiles.exe	f98416bae67fb155c7acfde4ef02b24a	5b9e56e6c289b19e49d1cbe17a0cd82d50631...	8c6a72a5		

Exercise 3: Create a Self-signed Certificate

Lab Scenario

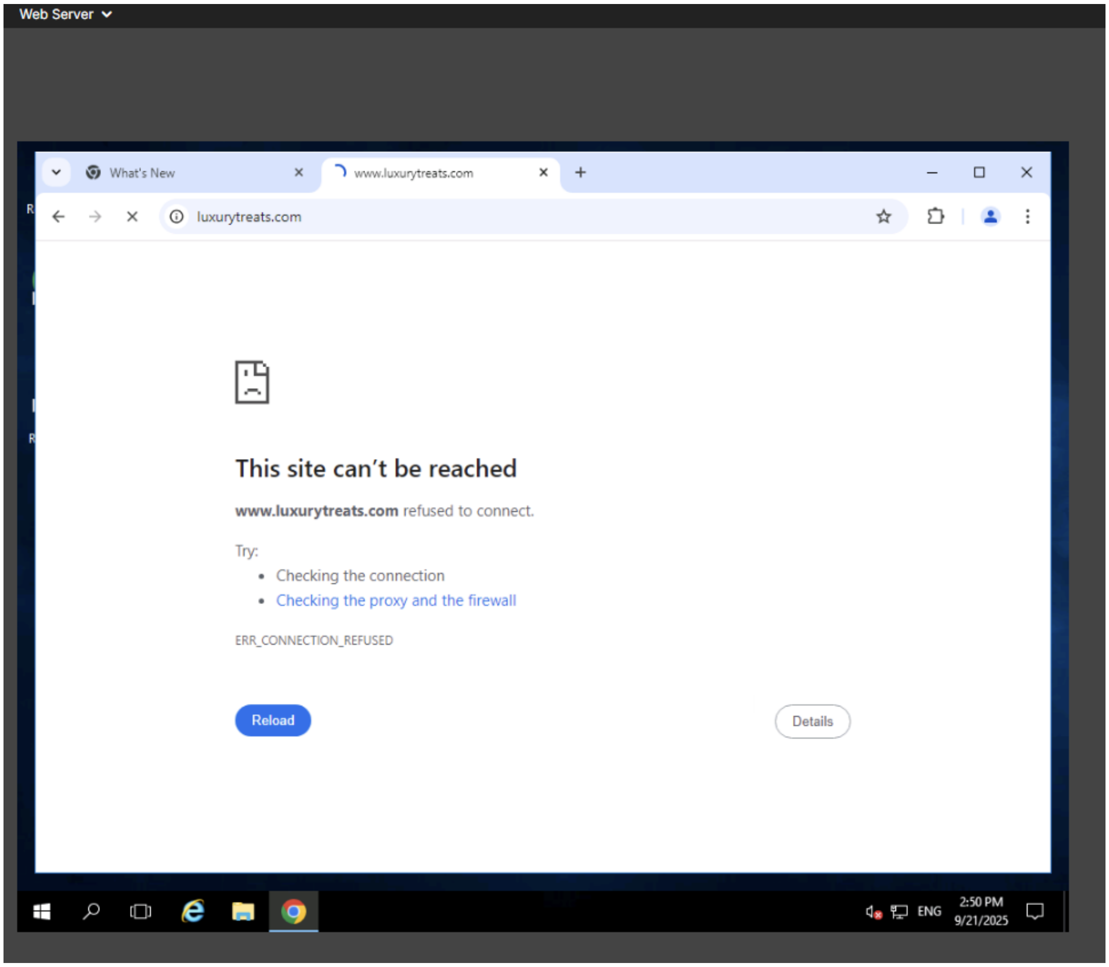
Self-signed certificates are widely used for testing servers.

Lab Objectives

As a network defender, you must know how to create 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.

Overview of Self-signed Certificate

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.



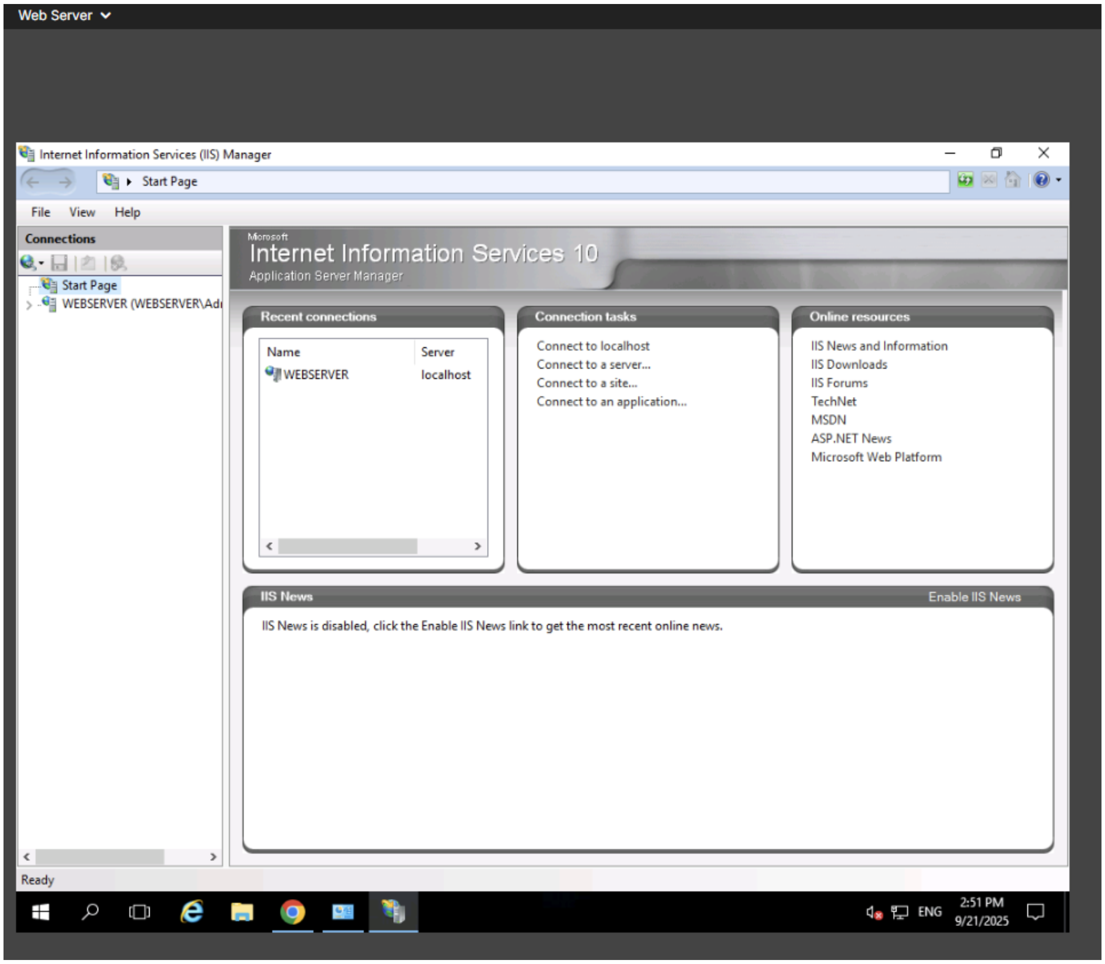
This site can’t be reached

www.luxurytreats.com refused to connect.

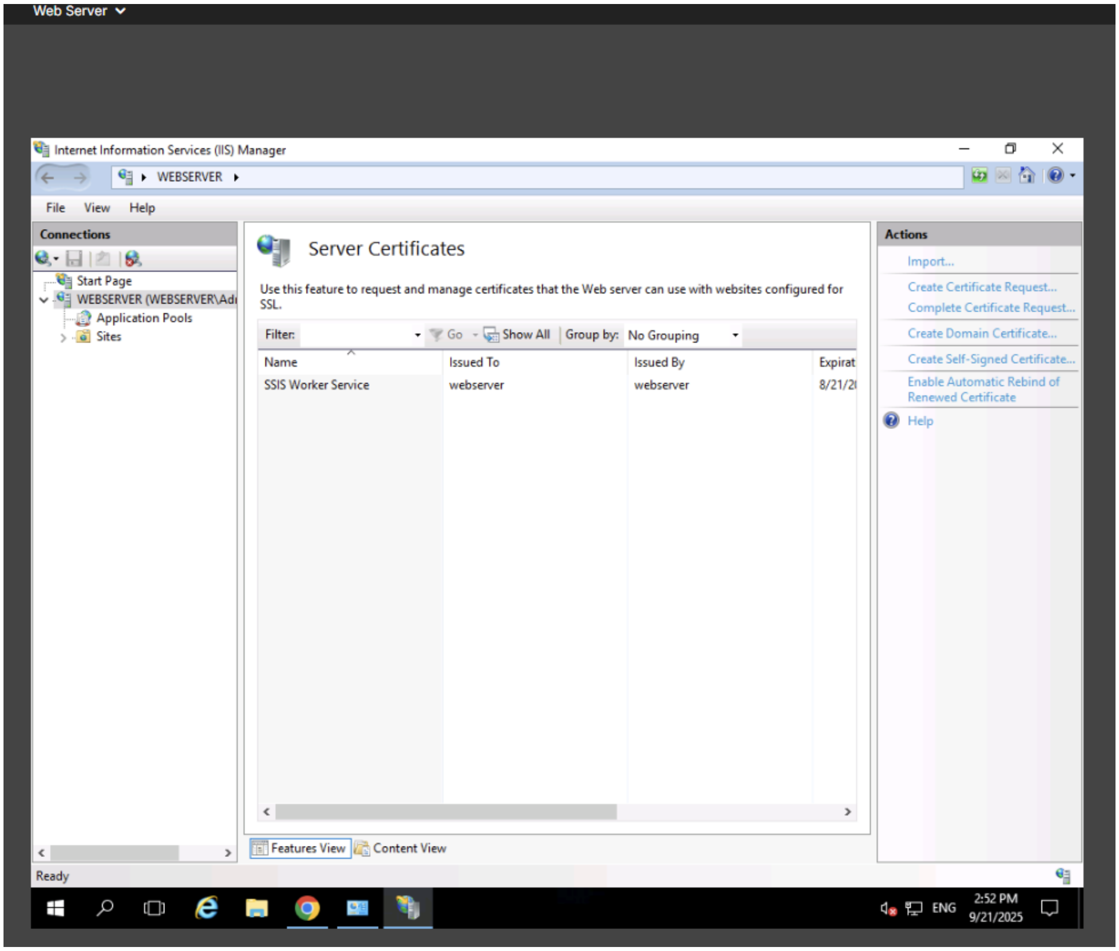
Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED



IIS News is disabled, click the Enable IIS News link to get the most recent online news.



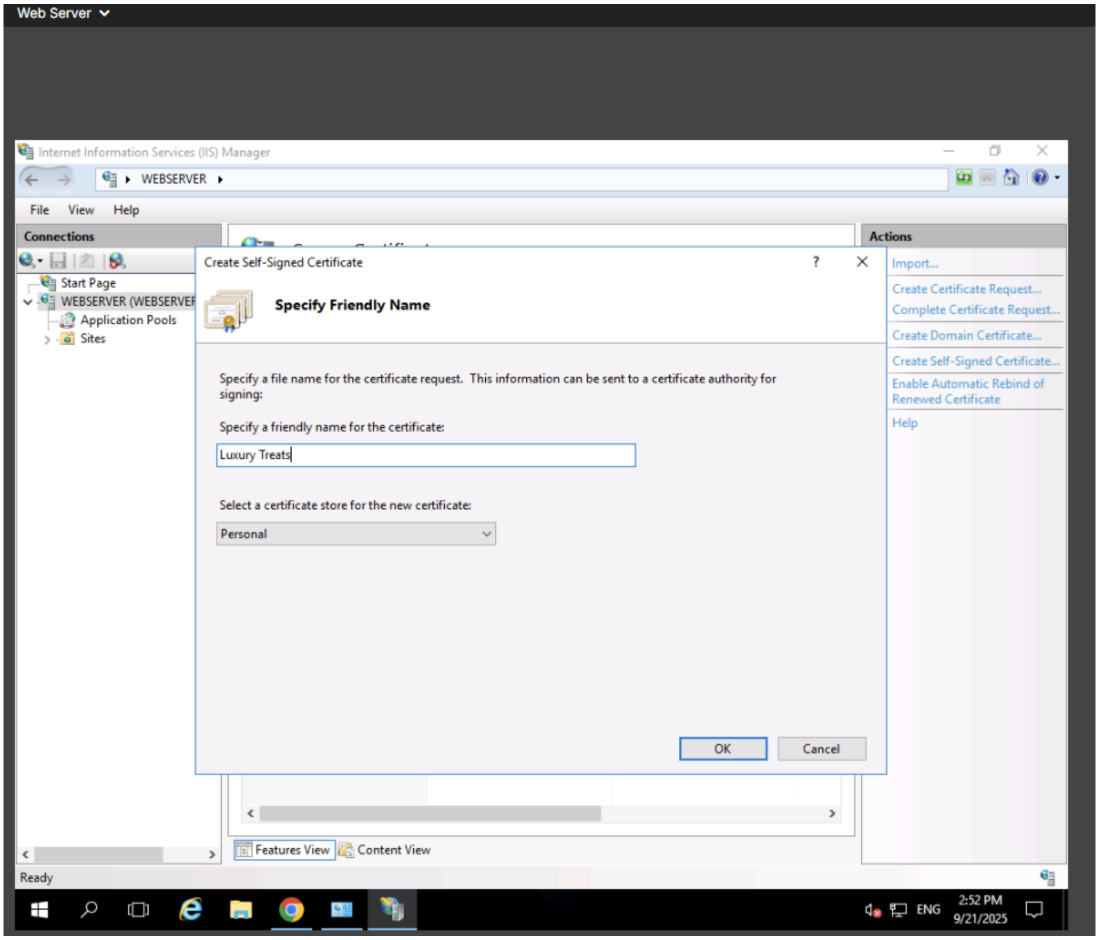
Web Server
Internet Information Services (IIS) Manager
WEBSERVER
File
View
Help
Connections
Start Page
WEBSERVER (WEBSERVER\Ad
Application Pools
Sites
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help
Features View
Content View
Ready
ENG
2:52 PM
9/21/2025

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
SSIS Worker Service	webserver	webserver	8/21/2


Web Server
Internet Information Services (IIS) Manager
WEBSERVER
File
View
Help
Connections
Start Page
WEBSERVER (WEBSERVER
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
ENG
2:52 PM
9/21/2025

Create Self-Signed Certificate

Specify Friendly Name

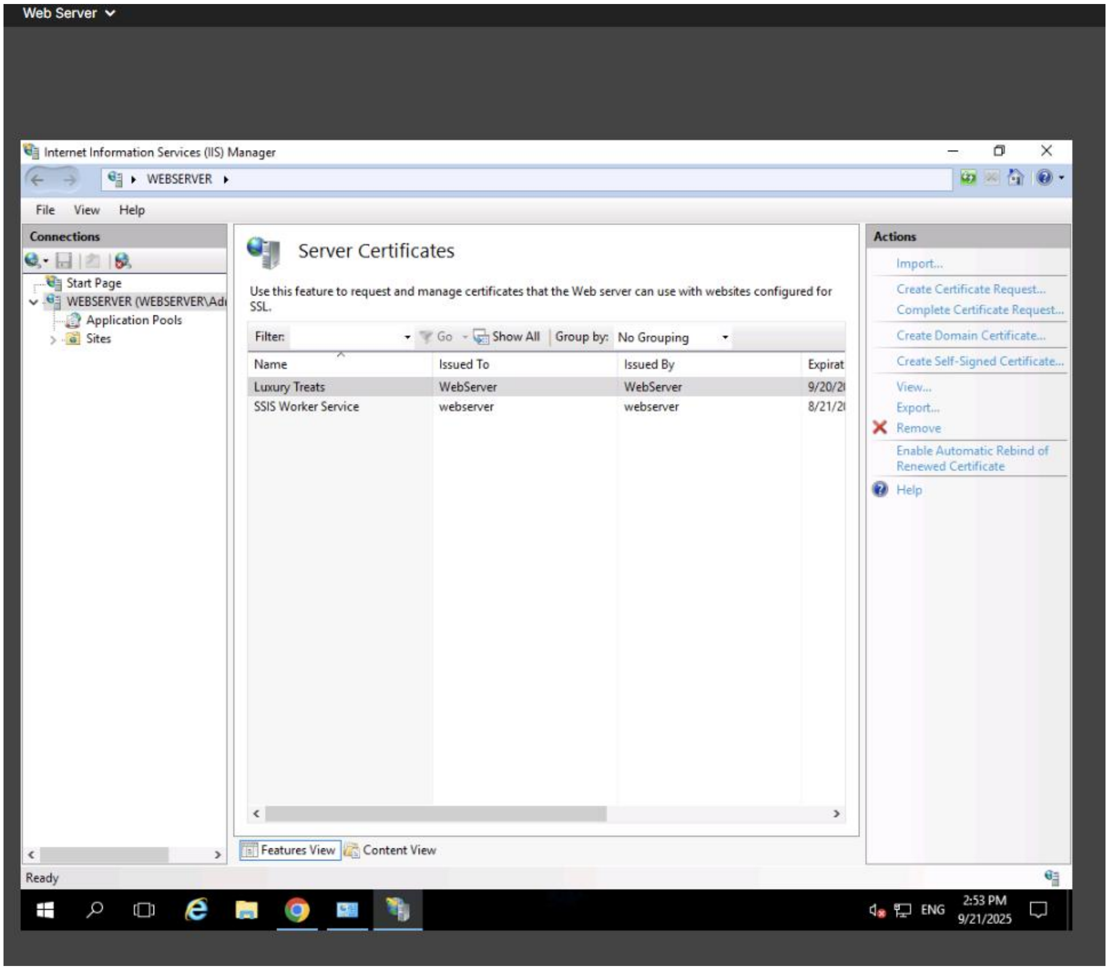
Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:

Specify a friendly name for the certificate:

Luxury Treats

Select a certificate store for the new certificate:

Personal

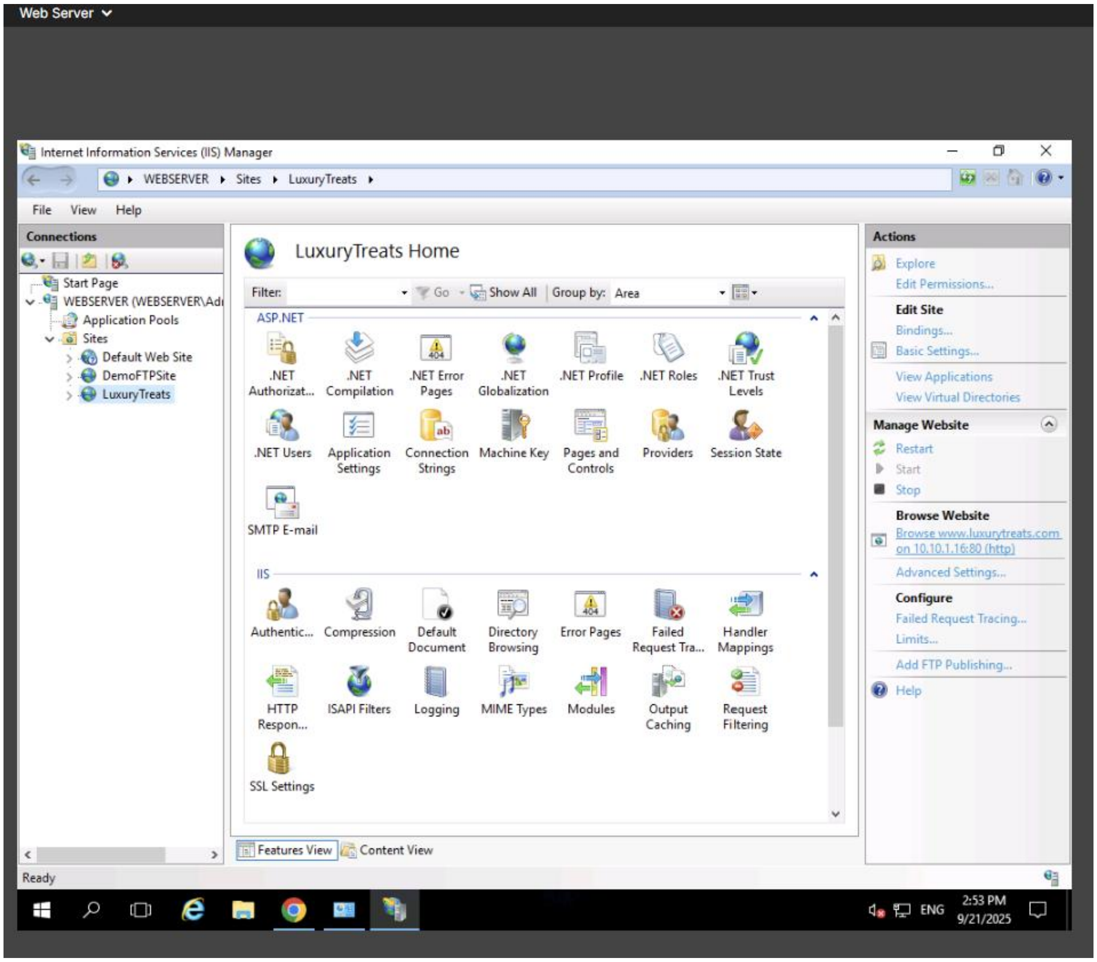

Web Server
Internet Information Services (IIS) Manager
WEBSERVER
File
View
Help
Connections
Start Page
WEBSERVER (WEBSERVER\Adı
Application Pools
Sites
Features View
Content View
Ready
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
View...
Export...
Remove
Enable Automatic Rebind of Renewed Certificate
Help
ENG
2:53 PM
9/21/2025

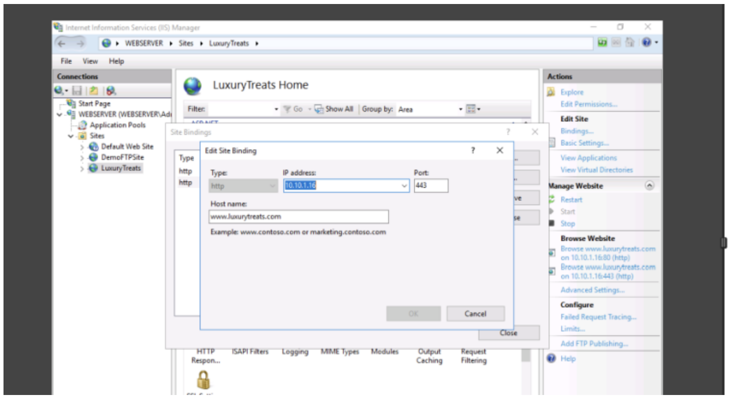
Server Certificates

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
Luxury Treats	WebServer	WebServer	9/20/2(
SSIS Worker Service	webserver	webserver	8/21/2(




Internet Information Services (IIS) Manager
WEBSERVER ▸ Sites ▸ LuxuryTreats ▸
LuxuryTreats Home
Site Bindings
Edit Site Binding
OK
Cancel
Close
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
Manage Website
Browse Website
Browse www.luxurytreats.com on 10.10.1.16:80 (http)
Browse www.luxurytreats.com on 10.10.1.16:443 (http)

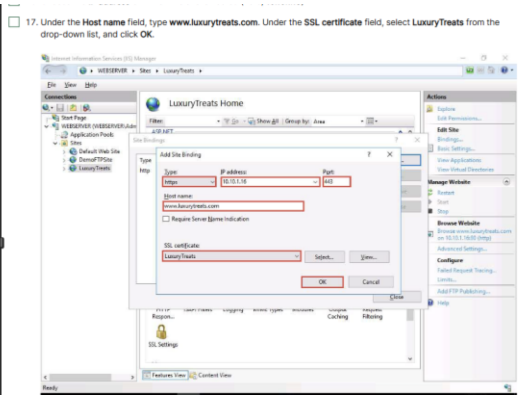
Type: http

IP address: 10.10.1.16

Port: 443

Host name: www.luxurytreats.com

Example: www.contoso.com or marketing.contoso.com



□ 17. Under the **Host name** field, type **www.luxurytreats.com**. Under the **SSL certificate** field, select **LuxuryTreats** from the drop-down list, and click **OK**.

Type: https

IP address: 10.10.1.16

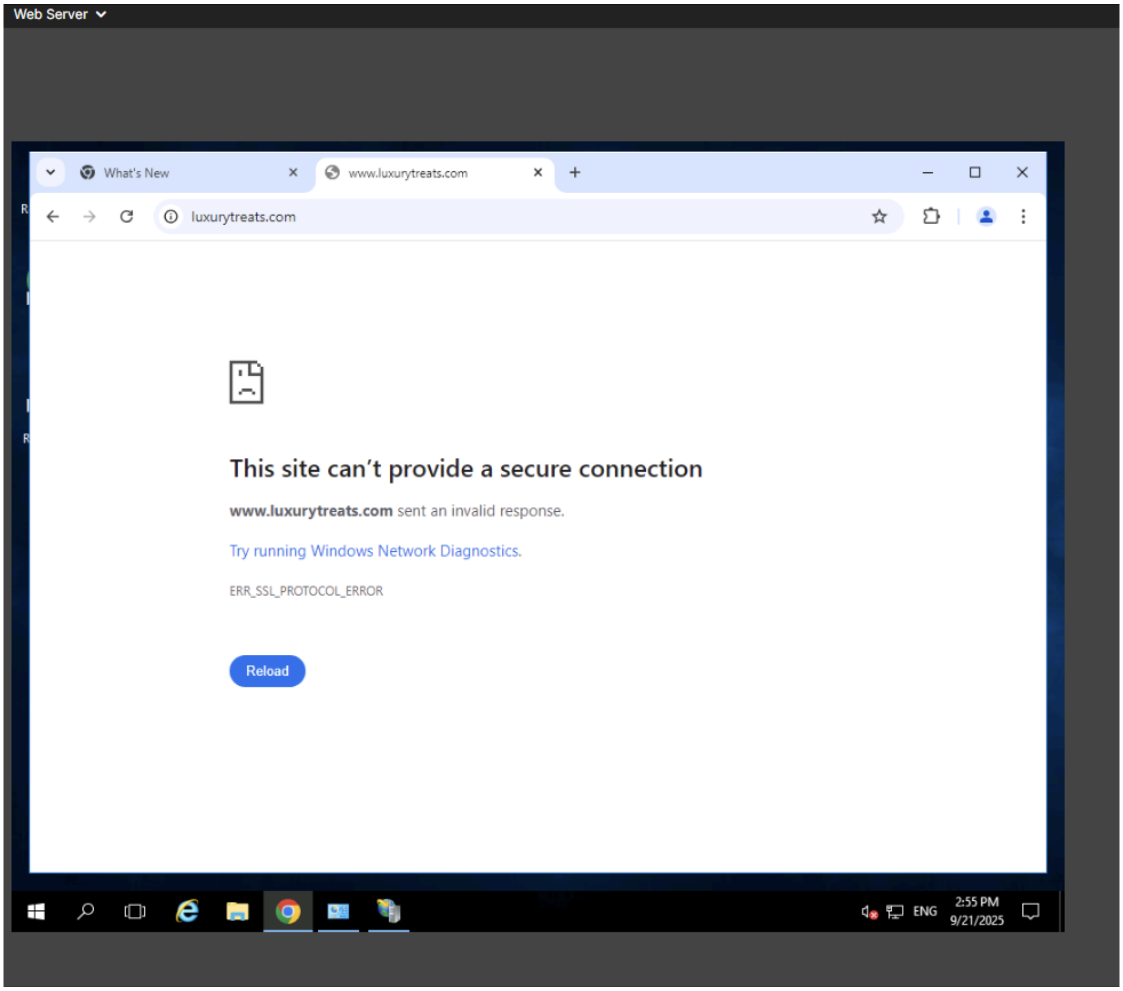
Port: 443

Host name: www.luxurytreats.com

□ Require Server Name Indication

SSL certificate: LuxuryTreats

No option for SSL Certificate



This site can't provide a secure connection

www.luxurytreats.com sent an invalid response.

Try running Windows Network Diagnostics.

ERR_SSL_PROTOCOL_ERROR

Lab Summary: Cryptography and PKI

Exercise 1: Calculate One-way Hashes using HashCalc

This lab demonstrated how to calculate one-way hashes (message digests) using **HashCalc**. By generating multiple hash values (MD5, SHA-1, SHA-256, etc.) for a file, integrity could be checked by comparing the calculated value against a known reference. This reinforced the role of one-way hashes in verifying that files have not been tampered with.

Exercise 2: Calculate MD5 Hashes using HashMyFiles

This exercise used **HashMyFiles** to calculate MD5 values of a given file. The output showed how MD5 generates a 128-bit digest that can be used in digital signature applications and integrity checking. While the lab successfully demonstrated MD5, it also highlighted MD5's weaknesses, specifically its lack of collision resistance, and reinforced why stronger algorithms such as SHA-2 or SHA-3 are recommended in production environments.

Exercise 3: Create a Self-signed Certificate

This lab was designed to demonstrate how to generate and apply a self-signed certificate in IIS to secure a test website (www.luxurytreats.com). The steps were followed up to the point of binding the SSL certificate to the site. However, the certificate did not appear as an option in the **SSL Certificate** drop-down menu. Because of this, the HTTPS binding could not be completed, and the site could not be tested in a browser with SSL enabled.

Outcome

- Exercises 1 and 2 were completed successfully, demonstrating hash calculation tools.
- Exercise 3 was **incomplete** due to the SSL certificate not being available as an option in the lab environment.

Reflection

This module provided practical exposure to cryptographic fundamentals: one-way hashing for file integrity, MD5 hashing, and the creation of SSL certificates. The hashing labs were completed without issue, while the certificate lab was blocked by a lab environment limitation. The absence of an error message made troubleshooting difficult, as a beginner, it was not clear where the issue occurred until the final outcome failed. This underscored the importance of both error feedback in training environments and familiarity with alternative tools for generating and testing self-signed certificates.