Implementing a Secure Network Design

(CompTIA Security + SY – 601)

Objectives:

- To analyze potential indicators associated with network attacks
- To implement secure network designs

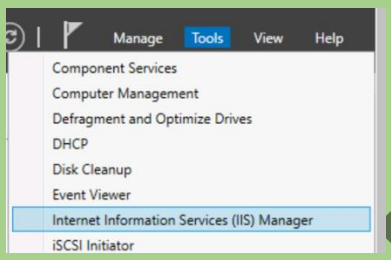
Resources:

- DHCP Security settings
- Internal Windows webserver
- Kali Virtual Machine (PT-1 Kali)

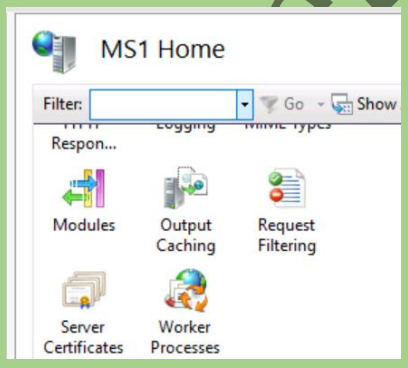
Instructions:

Request Server Certificate

- Select the **MS1 VM** and sign-in
- In server Manager, select **Tools > Internet Information Services (IIS) Manager**

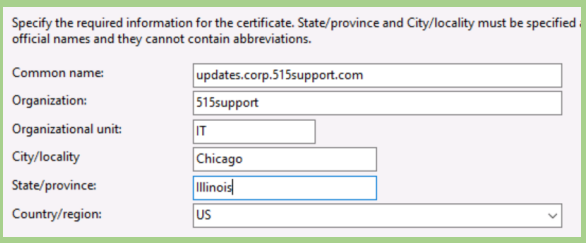


- In the connections pane, select the MS1 server icon. In the Home pane, open the **Server Certificates** applet

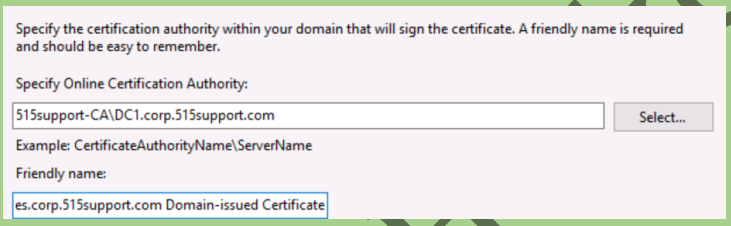


- In the Action pane, select **Create Domain Certificate**

- Complete the Create Certificate wizard with the following responses:

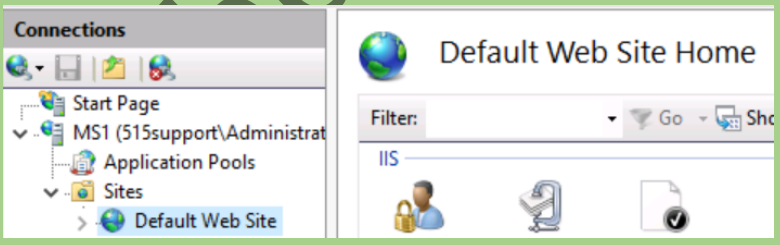


- Select **Next**
- On the Online Certification Authority page, select the **Select** button, the select 515support-CA and select **OK**
- In the Friendly name box type: updates.corp515support.com Domain-issued Certificate and then select **Finish**

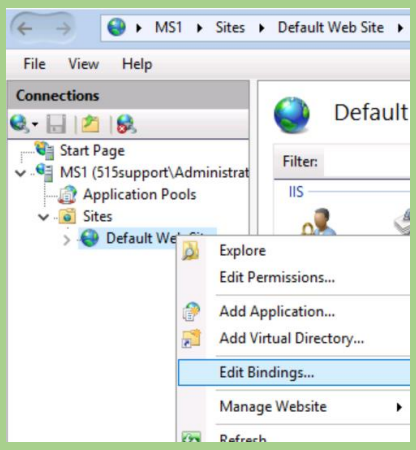


Configure HTTPS

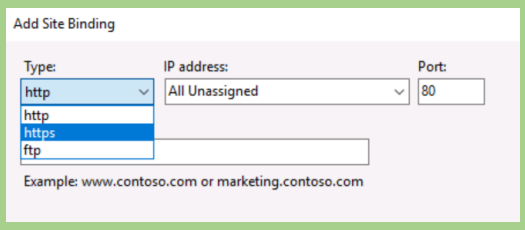
- In the IIS Manager, expand the **Sites** node on the server to show the **Default Web Site node**



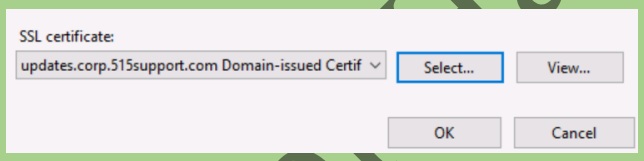
- Right-click Default Web Site and select **Edit Bindings**



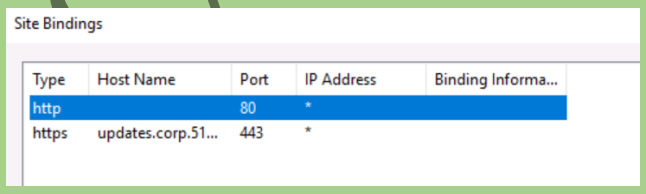
- Select the **Add** button
- In the Add Site Binding dialog box, from the Type drop-down list, select **https**



- In the Host name box, type: **updates.corp.515support.com**
- From the SSL certificate drop-down list, select **updates.corp.515support.com Domain-issued certificate**



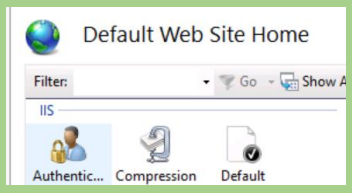
- Select OK
- In the Site Bindings dialog box, select HTTP, and then select Remove to delete HTTP, and then select **Remove** to delete HTTP from the list. Select **Yes** when prompted to confirm the removal



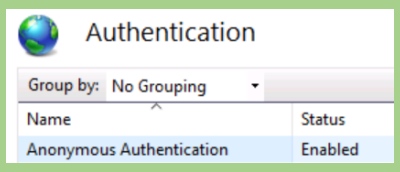
- Select **Close**

Configure authentication policy

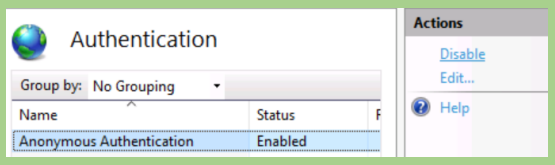
- In IIS Manager, select the **Default Web Site** node



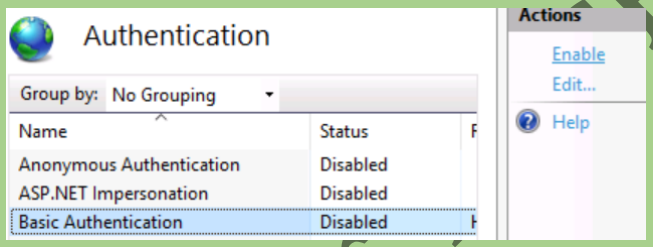
- In the Home pane, open the **Authentication** applet



- Select **Anonymous Authentication** them in the Action pane, select **Disable**

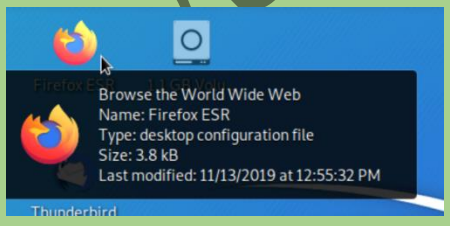


- Select **Basic Authentication**, them in the Actions pane, select **Enable**

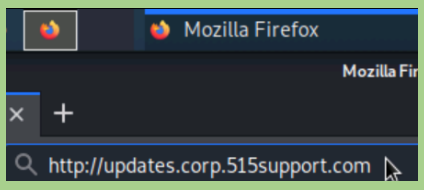


Test Web Credentials

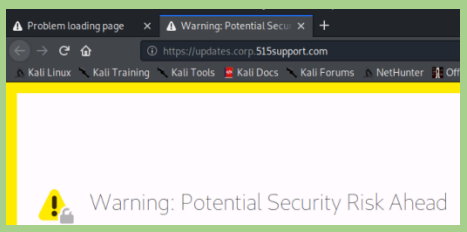
- Sign-in to the **PT1-Kali** VM
- From the menu at the top of the Kali Linux screen, select **Firefox ESR**



- Attempt the web connection by using http://updates.corp.515support.com

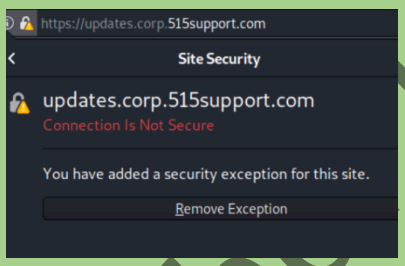


- You will receive a *Warning: Potential Security Risk Ahead* message, select **Advanced**, then **Accept the Risk and continue**



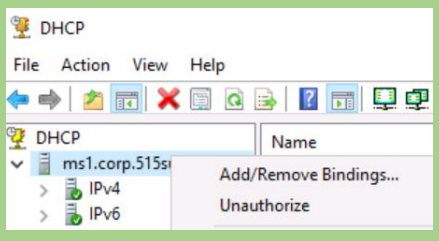
- When prompted by the **Authentication Required** dialog box, enter the 515support\Administrator and Pa$$w0rd credentials

- If prompted to save the login by Firefox, select **Never for this Site**
- After the connection is complete, select the browser padlock icon to confirm that you are viewing the page over a secure connection

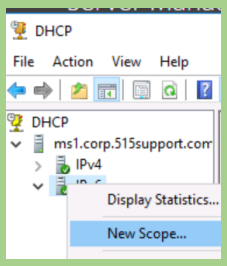


DHCP Security

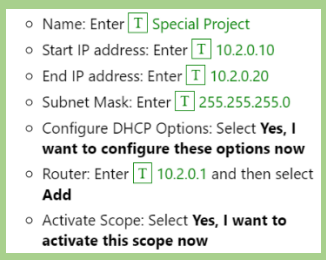
- Switch to the **MS1** VM
- In the Server Manager, select Tools and then select DHCP to open the **DHCP** management console select the **ms1.corp.515support.com** server icon, and then right-click it



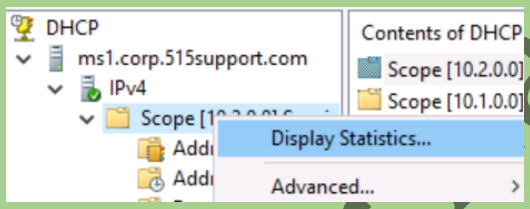
- Select **IPv4** and then right-click it and select **New Scope**…



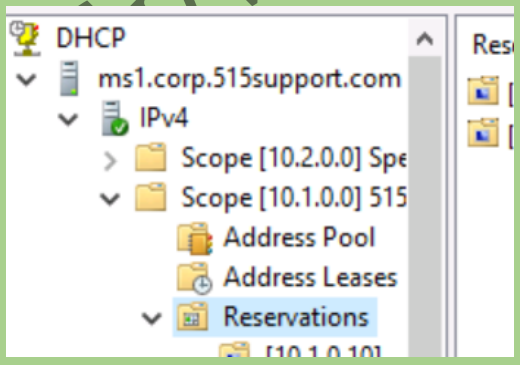
- To create a scope for the new R&D segment, use the following responses in the wizard (accept the default settings for any value not specified below). Choose **Next** in each window



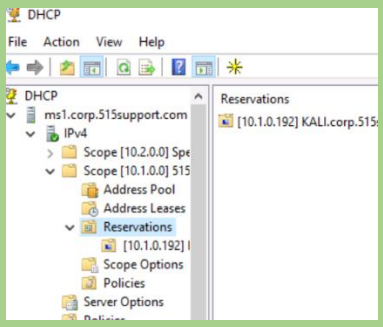
- Select **Finish** to complete the wizard
- Select the **Scope [10.2.0.0] Special Project Scope** node, and then right-click it and select **Display Statistics**



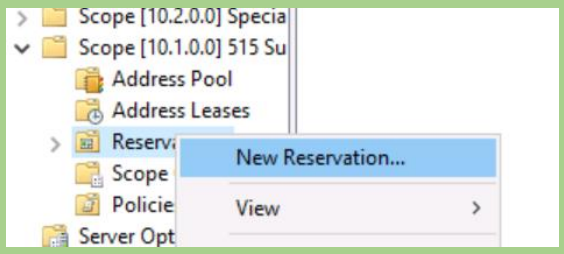
- Close the Statistics box
- Expand the Scope **[10.1.0.10] 515 Support Scope**, and then select the **Reservations** node
- Select the **10.1.0.10** reservation. In the left-hand pane, right-click 10.1.0.10 and select **Properties**. Copy value from the **MAC address** box and then click **Cancel**



- Delete the LX1 (CentOS) reservation from the 515 SupportScope

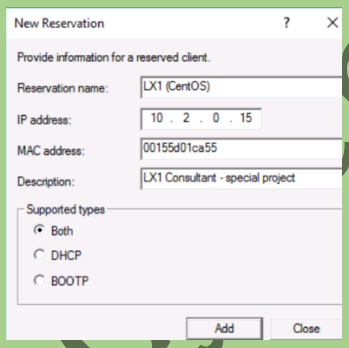


- Select the **Reservations** node in the **Special Project** scope



- Right-click the **Reservations** node, and then select **New Reservation**
- In the **New Reservation** box, enter the following information

- Reservation Name: LX1 (CentOS)
- IP address: 10.2.0.15
- MAC address: *Paste from the clipboard or Notepad document*
- Description: LX1 Consultant - special project



- Select **Add** and then **Close** the New Reservation box
- Select the **Filters** node under the **IPv4** node
- Select the **Allow** node, and then right-click it and select **New Filter**
- Paste in the MAC address value you copied above, and then enter **LX1 consultation computer** in the **Description** field
- Right-click **IPv4** and select **Properties**
- Select the Filters tab and then check the box

Observations:

- Successfully created and applied a domain certificate
- HTTPS binding was configured correctly, ensuring secure web access
- Authentication policies were effectively set up, enhancing security
- Verified secure web access from Kali VM
- DHCP scope, reservations, and filters were configured as instructed

Results:

- Secure network design was implemented through certificate management, HTTPS configuration, and authentication policies.
- DHCP settings were properly configured to enhance network security.

Conclusion:

The lab demonstrated effective implementation of a secure network design, focusing on certificate management, HTTPS configuration, and DHCP security settings. These measures collectively ensure a robust and secure network environment.

Future Work:

- Automate the certificate management process.
- Implement advanced authentication methods like multi-factor authentication (MFA).
- Explore network segmentation and advanced firewall configurations for enhanced security