IT 3850 Computer System Administration  
Spring 2022

**Laboratory # 9 - SSL/TLS**

*Dr. Ronny Bazan (Contact: bazanantequerar@umsystem.edu)*



1. **Objectives**

Configure a self-signed certificate for the Apache webserver.

1. **Material Required**

A RHEL Linux VM and Microsoft Windows 10 VM.

1. **Activity**
2. Go through the SSL/TLS Module slides and videos available on Canvas.
3. Configure your server0 network by using the 3rd subnet of 192.168.100.0/27. Assign the IP 192.168.100.65 with mask 255.255.255.224 to your NIC connected to the vSwitch VMnet2 or ‘Private to my Mac’ (for MacOS users). You can use your previous RHEL VM that is already configured with these network values, with your DNS and Web servers already configured.
4. Make sure you can access the website by typing [**www**.infotc3850.com](http://www.infotc3850.com)
5. **Review Questions**

**\*Important\*. For each question where you are required for a screenshot, include the screenshot that clearly demonstrates you completed that step successfully.** Include any commands you executed for each step as well, if applicable**. All the screenshots for this lab and future labs must include your pawprint in the command prompt or have other information visible that identifies you (i.e. type/draw your pawprint).** This is to ensure that you are submitting your own work.

Answer the following questions and perform the following tasks. Construct your report in a document to submit on Canvas. Make sure to read the directions and the rubric carefully!

1. Configure a self-signed certificate for your web server:
   1. Use an RSA of 2048 bits, the *infotc3850.key* name for the key and the *infotc3850.crt* name for the certificate. Show the command you executed. Text

      Description automatically generated
   2. Display the generated key and certificate using a long list (use the **ls -l** command).

Text

Description automatically generated with medium confidence

1. Open up a web browser in the local system (RHEL) and demonstrate that you are able to access the web site using the HTTPS protocol by going to https://www.infotc3850.com. Show clearly that the web browser was opened in RHEL.

Graphical user interface, application

Description automatically generated

1. Open up a web browser in a remote system (MS Windows 10) and demonstrate that you are able to access the web site using the HTTPS protocol by going to https://www.infotc3850.com. Show clearly that the web browser was opened in MS Windows. Note. You might see ‘certificate error’ next to the padlock, this is expected since we are using self-signed certificates.

A screenshot of a computer

Description automatically generated

IT 3850 Computer System Administration  
Spring 2021

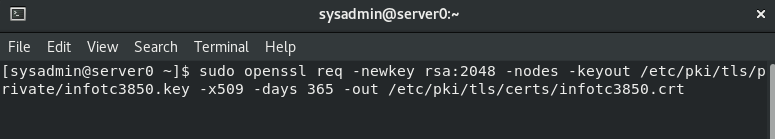
**Laboratory # 9 - SSL/TLS**

*Dr. Ronny Bazan (Contact: bazanantequerar@umsystem.edu)*

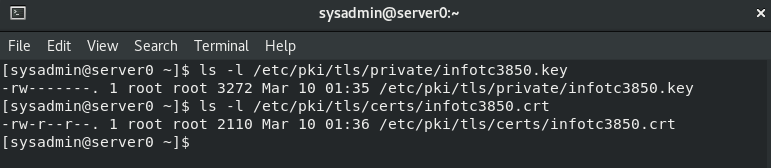
1. **Rubric**

|  |  |  |
| --- | --- | --- |
| **Question** | **Criteria** | **Points** |
| 1a | 20 points for the correct openssl command with all options included. | 20 |
| 1b | 5 points for showing each file x2 | 10 |
| 2 | 40 points for showing the web site on RHEL. | 40 |
| 3 | 30 points for showing the web site on Windows. | 30 |
| **Total** |  | **/100** |

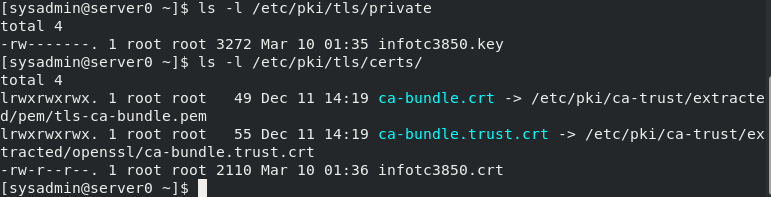
1. **Correct answers**
2. Configure a self-signed certificate
   1. Use an RSA of 2048 bits, the *infotc3850.key* name for the key and the *infotc3850.crt* name for the certificate. Show the command you executed.



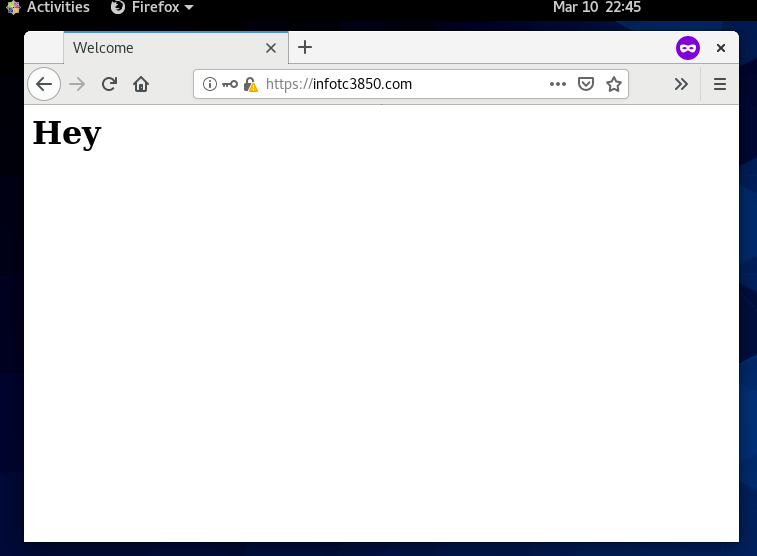
* 1. Display the generated key and certificate using a long list (use the **ls -l** command).



OR



1. Open up a web browser in the local system (RHEL) and demonstrate that you are able to access the web site using the HTTPS protocol. Show clearly that the web browser was opened in RHEL.



1. Open up a web browser in a remote system (MS Windows 10) and demonstrate that you are able to access the web site using the HTTPS protocol. Show clearly that the web browser was opened in MS Windows. Note. You might see ‘certificate error’ next to the padlock, this is expected since we are using self-signed certificates.

