**Laboratory Exercise D1 – Sniffing**

Due Date: 9/23/2022

Points Possible: Number of points out of total course points or recommended percent of the course grade.

**1. Overview**

For this lesson, students will use the Cyber Range: Kali Linux with Metasploitable (2020.09) environment to sniff traffic using Wireshark and Nmap.

**2. Resources required**

This exercise requires a Kali Linux VM running in the Cyber Range.

**3. Initial Setup**

For this exercise, you will log in to your Cyber Range account and select the Kali Linux with Metasploitable (2020.09) environment, then click “start” to start your environment and “join” to get to your Linux desktop login. Log in using these credentials:

Username: **student**

Password: **student**

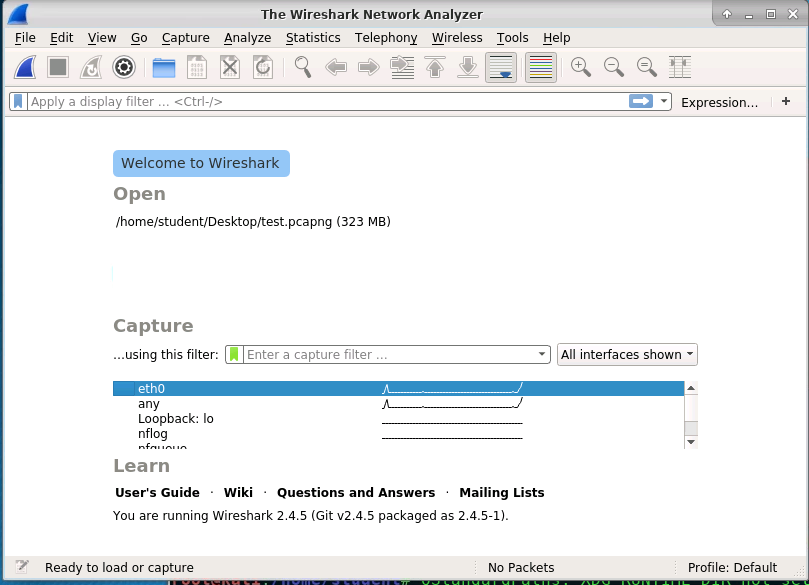
**4. Tasks**

**Task 1: Setting up Wireshark**

Complete the following:

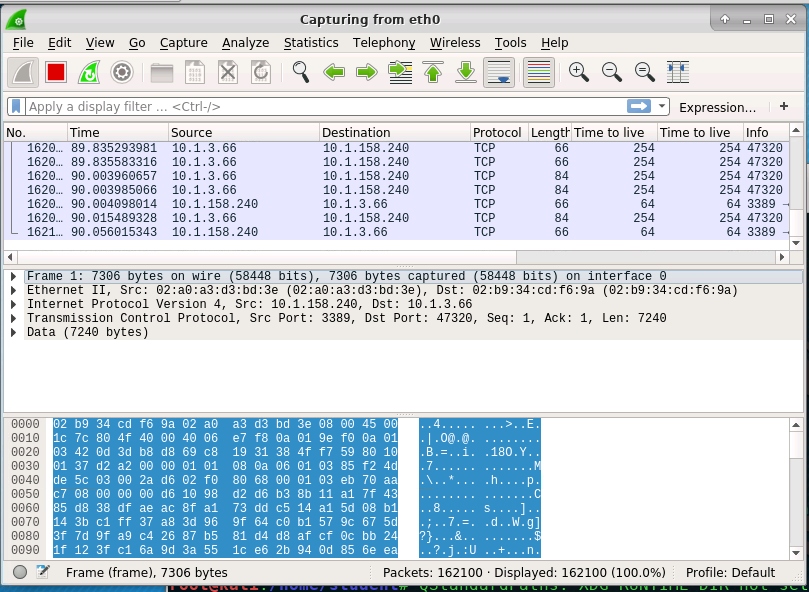
1. Open up a terminal and type sudo wireshark & and then hit enter. You may get a popup error. Disregard this error and click on OK to continue.
2. Choose the eth0 interface and double click on it. See the image below.

|  |
| --- |
| Graphical user interface, application  Description automatically generated |



Wireshark will begin capturing packets.

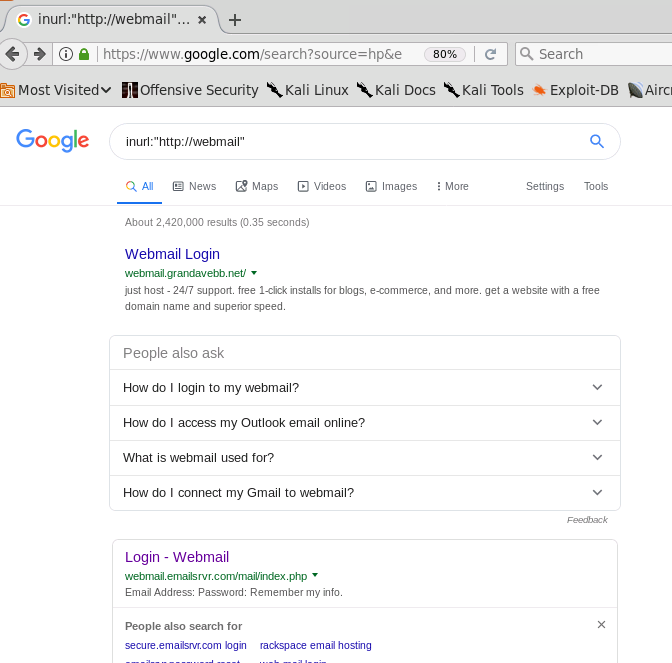
|  |
| --- |
| Graphical user interface, application  Description automatically generated |



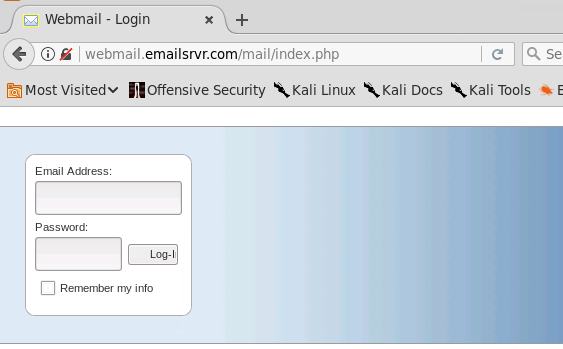
Stop Wireshark by clicking the red square and then open a browser.

**Task 2: Finding an insecure website**

1. In a Google search box, type inurl:"<http://webmail>"



1. Sites are fixing this vulnerability daily so what you see in the screenshots will be different. Choose any website with a http login page. Your site will vary, but the process is the same. In my case, the website is http://webmail.emailsrvr.com



1. Return to Wireshark and hit the shark fin to start capturing packets. Do not save the previous capture.
2. Return to the Browser and make up an email and password (**DO NOT USE A REAL ONE**)and click login.
3. Now return to Wireshark and stop the capture.

|  |
| --- |
| Graphical user interface, application  Description automatically generated |

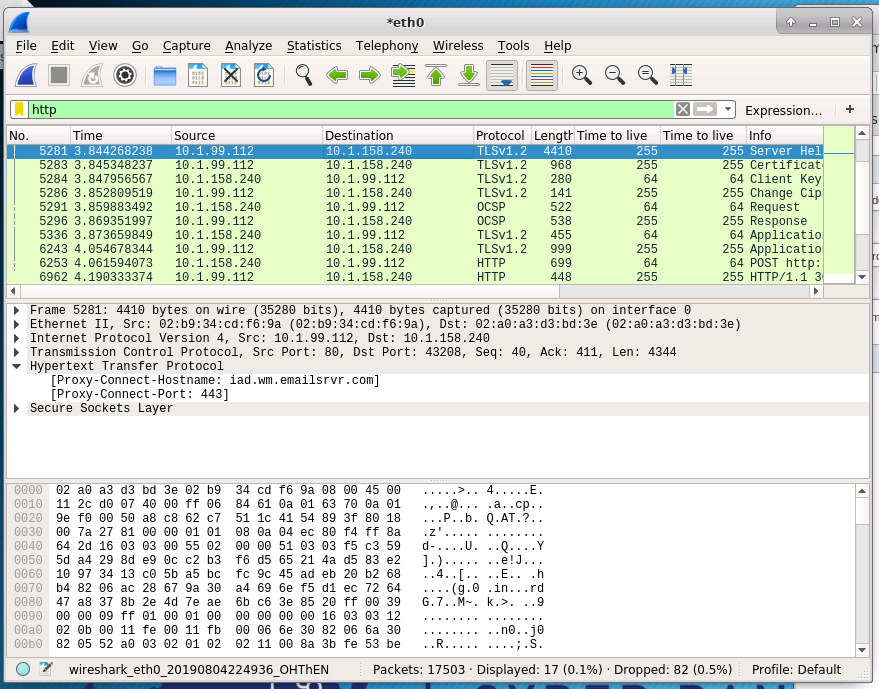
**Task 3: Sniffing the HTTP protocol using Wireshark**

Wireshark is a great network utility and packet sniffer. Anything that is not encrypted across the network, Wireshark will capture in clear text.

Complete the following:

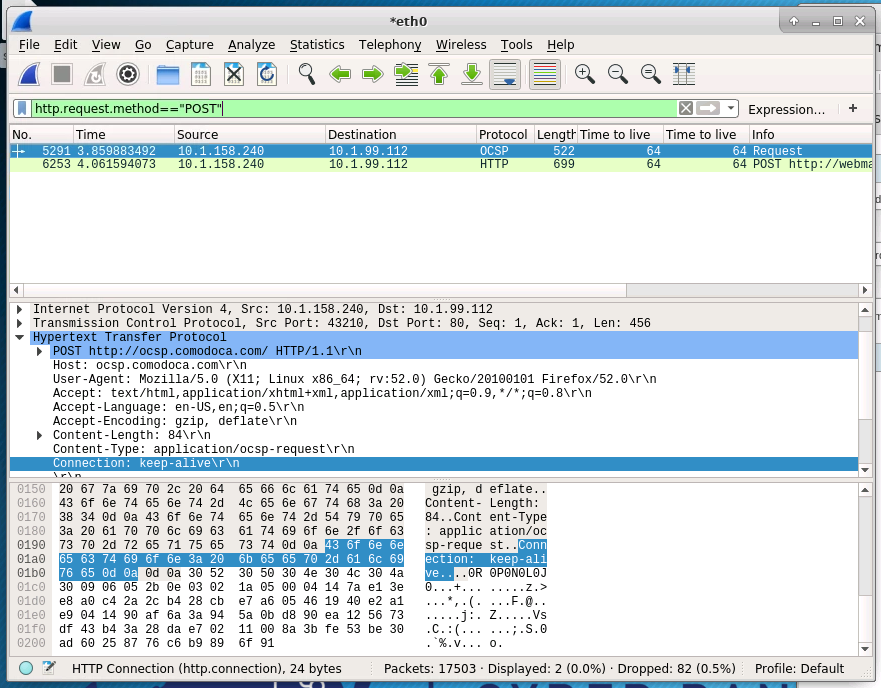
1. Type **http** in the Wireshark Filter box and press enter**.** This will list all the HTTP packets that were captured.

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |



1. In most cases, this is still too much to sift through. Wireshark has a very powerful filtering system. We can filter only POST requests which will show all login attempts. To do this, type http.request.method=="POST" and press enter.

|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |



1. Now we are down to two packets! Examine them and see if you can find the username and password.



**As you can see** the packet show clear text username and password. This is why having a HTTPS site when logging in to a webserver is very important. Hackers can compromise webservers, or be on the internal network and harvest credentials. Properly secured sites should have https, TLS 1.3 and an updated SSL certificate.

**Task 4: Checking the Certificate in Firefox**

It is a good idea to pay attention to the left-hand side of the browser when completing tasks online. Here the browser will let you know about any security issues.

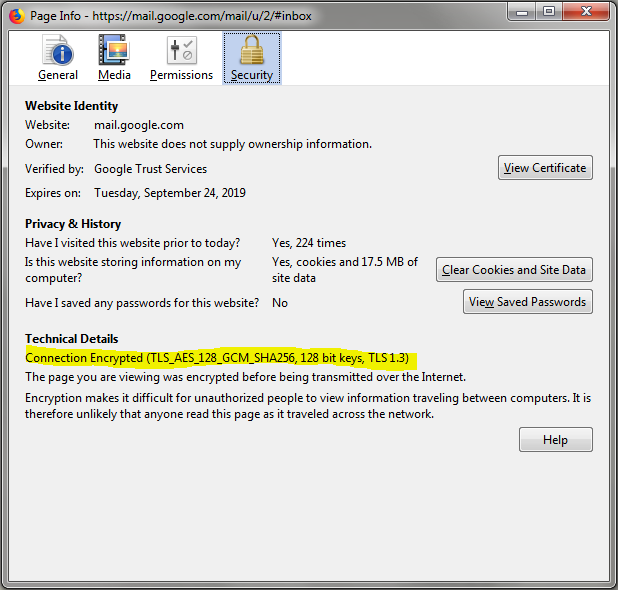


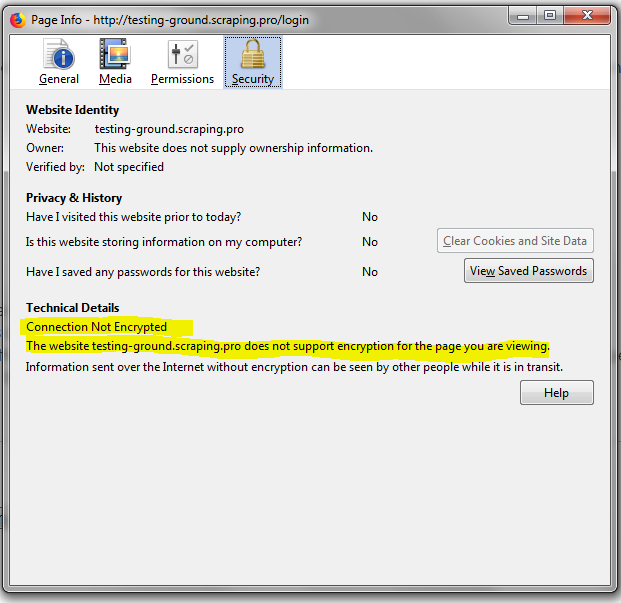


To view the certificate is very similar in every browser. Using our Google search from Task 2, find another insecure site and view the connection. Click the notice next to the URL. Choose connection>more information. Then choose Security.

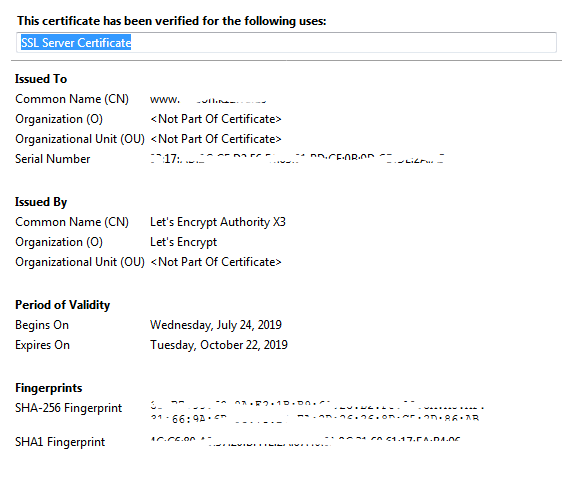
Here you can view the certificate if there is one. Open a new tab and visit your school’s website. Follow the same process only this time view the certificate. Also, notice the difference before viewing the certificate. It should look similar to the screenshots below.

|  |
| --- |
| A screenshot of a computer  Description automatically generated |





Click View Certificate to view the certificate.



Never log into a site that is not encrypted. This is a sure way to have your credentials stolen. If the site is one you must log into, send the administrator a message letting them know that the server is insecure.

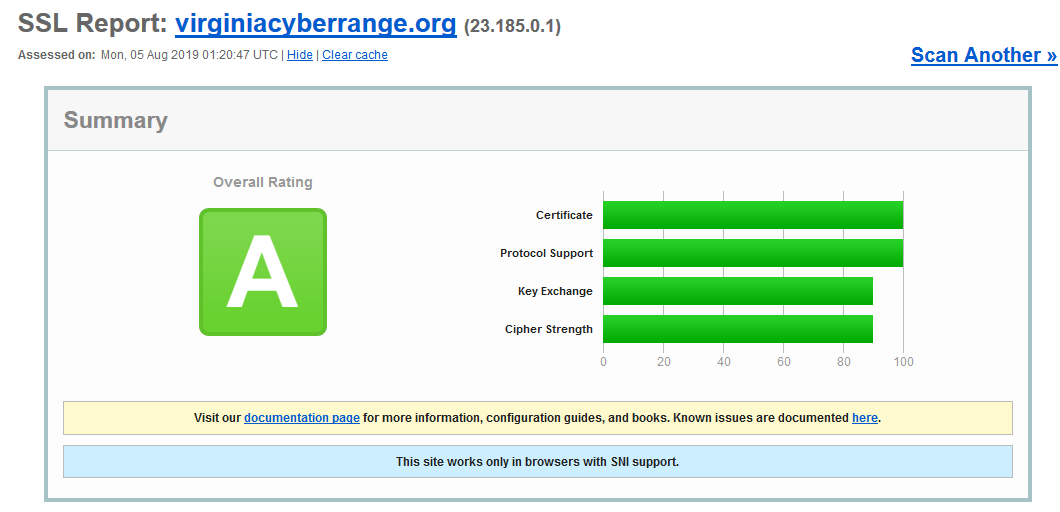
**Task 5: Using SSL labs to scan a server**

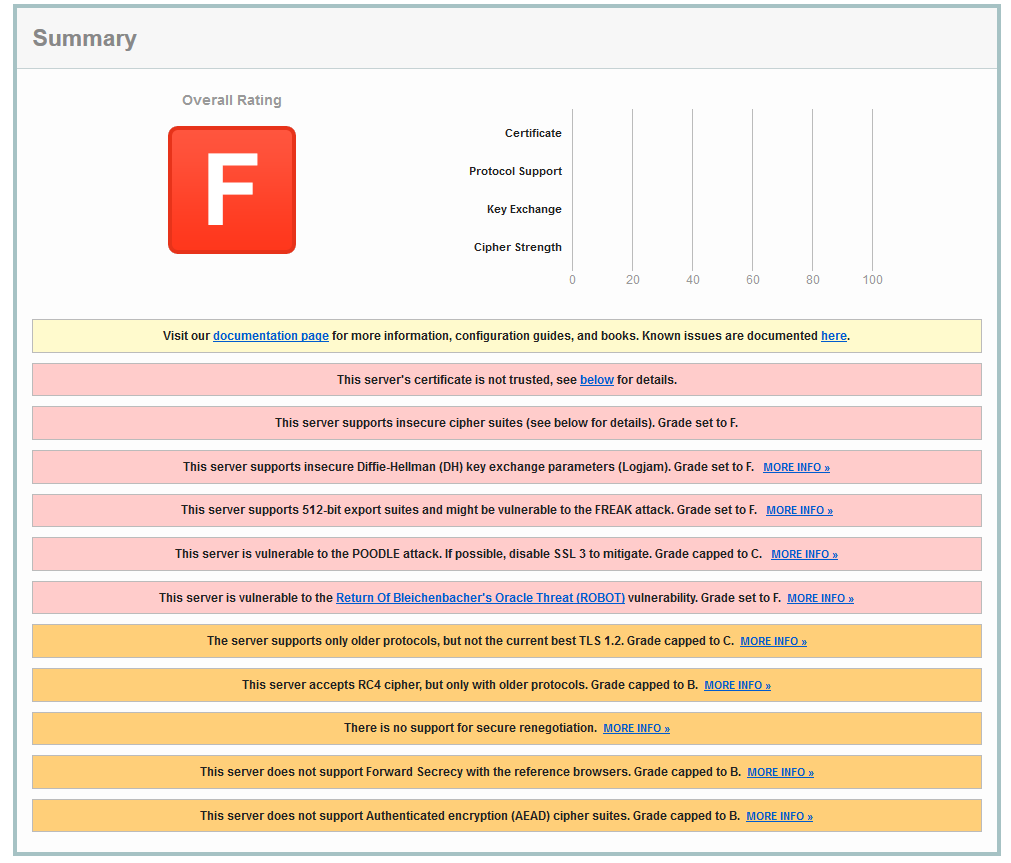
An important mitigation to prevent sniffing is encryption. Ethical Hackers will test for SSL TLS encryption. Besides the browser providing feedback, the server can be scanned from the web using: <https://www.ssllabs.com/ssltest/index.html>

Complete the following:

1. Visit the site above and in the scan box type: virginiacyberrange.org and hit Submit.
2. Wait; it may take some time.
3. Review the results. See results on following page for virginiacyberrange.org.
4. Scan an insecure website, wait, and view the results. See example results for an insecure website on following page.

|  |
| --- |
| A screenshot of a computer  Description automatically generated |





The insecure site clearly has major issues. For a Certified Ethical Hacker (CEH), this information is useful for further testing and reporting.