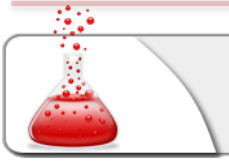
eLearnSecurity
Forging security professionals

HTTP AND HTTPS TRAFFIC SNIFFING



PRELIMINARY SKILLS | SECTION 1 MODULE 1 | LAB #1

LAB

1. Description

In this lab you will intercept some traffic with *Wireshark*, a common sniffer tool. Then you will analyze the capture to discover authentication credentials.

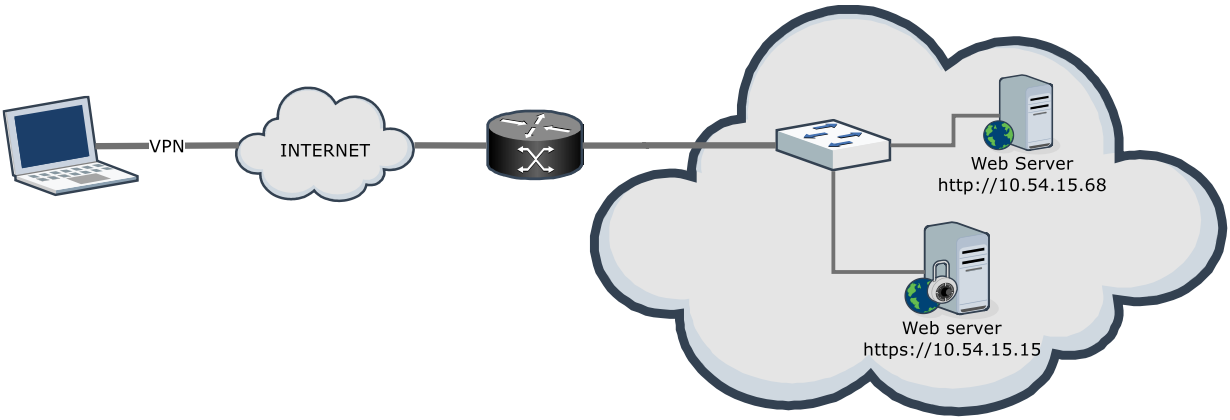
You will learn how sniffers and network protocols work in the *Networking* module. This exercise will help you understand the fundamental difference between a **clear-text and a cryptographic protocol.**

Use this manual to connect to Hera Lab for the first time:
https://members.elearnsecurity.com/lab/manual

2. Lab Environment

In this lab you are connected to a network with two web servers.

- One server provides access to a restricted area on a clear-text protocol: HTTP. After connecting to the lab, you can reach it on http://10.54.15.68
- The other provides access to a restricted area on an encrypted protocol: HTTPS After connecting to the lab, you can reach it on https://10.54.15.15



The credentials for both restricted areas are:

- Username: **elsstudent**
- Password: **testpassword**

3. Goals

- Capture an authentication attempt over HTTP with Wireshark
- Recover the credentials sent over the clear-text protocol by analyzing the network traffic
- Capture an authentication attempt over HTTPs with Wireshark
- Trying to recover the credentials sent over HTTPS. Is it possible?

4. Tools

The best tools for this lab are:

- Wireshark
- A web browser

SOLUTIONS

Please go ahead **ONLY** if you have **COMPLETED** the lab or you are stuck! Checking the solutions before actually trying the concepts and techniques you studied in the course, will dramatically reduce the benefits of a hands-on lab!

[This page intentionally left blank]

5. Solution Steps

5.1. Connect to the VPN and Start Wireshark

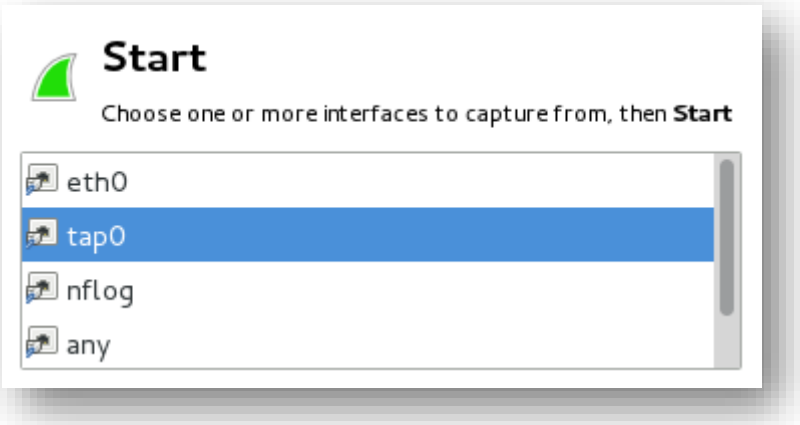
Please refer to this manual on how to connect to the lab:

https://members.elearnsecurity.com/lab/manual

After starting the lab and downloading the OpenVPN files from your members area, you can start the VPN.

```
Tue Feb 24 12:13:18 2015 [admin] Peer Connection Initiated with [AF_INET]74.50.1
24.84:33498
Tue Feb 24 12:13:20 2015 TUN/TAP device tap0 opened
Tue Feb 24 12:13:20 2015 do_ifconfig, tt->ipv6=0, tt->did_ifconfig_ipv6_setup=0
Tue Feb 24 12:13:20 2015 /sbin/ifconfig tap0 10.54.15.100 netmask 255.255.255.0
mtu 1500 broadcast 10.54.15.255
Tue Feb 24 12:13:20 2015 Initialization Sequence Completed
```

Then you can start Wireshark on the OpenVPN network interface (TAP).

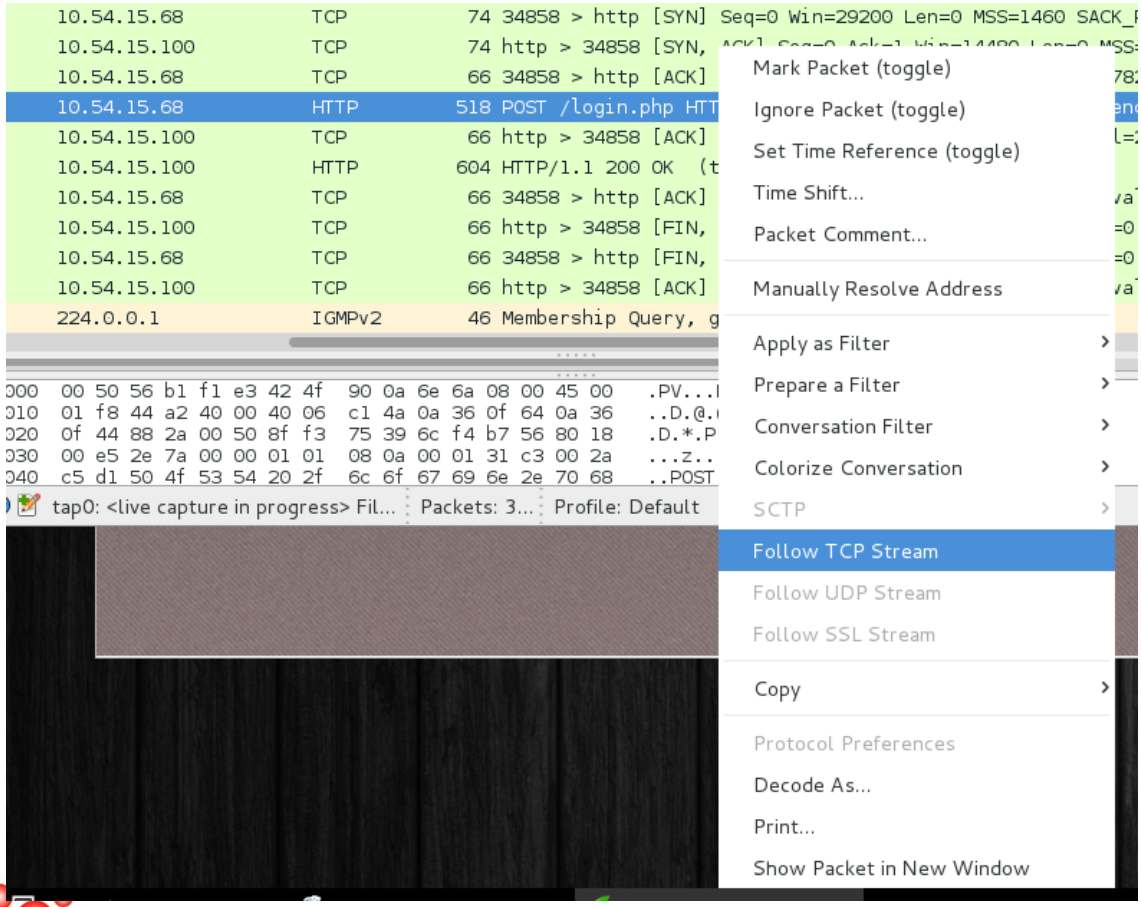


5.2. Capture and Analyze an HTTP Login Session

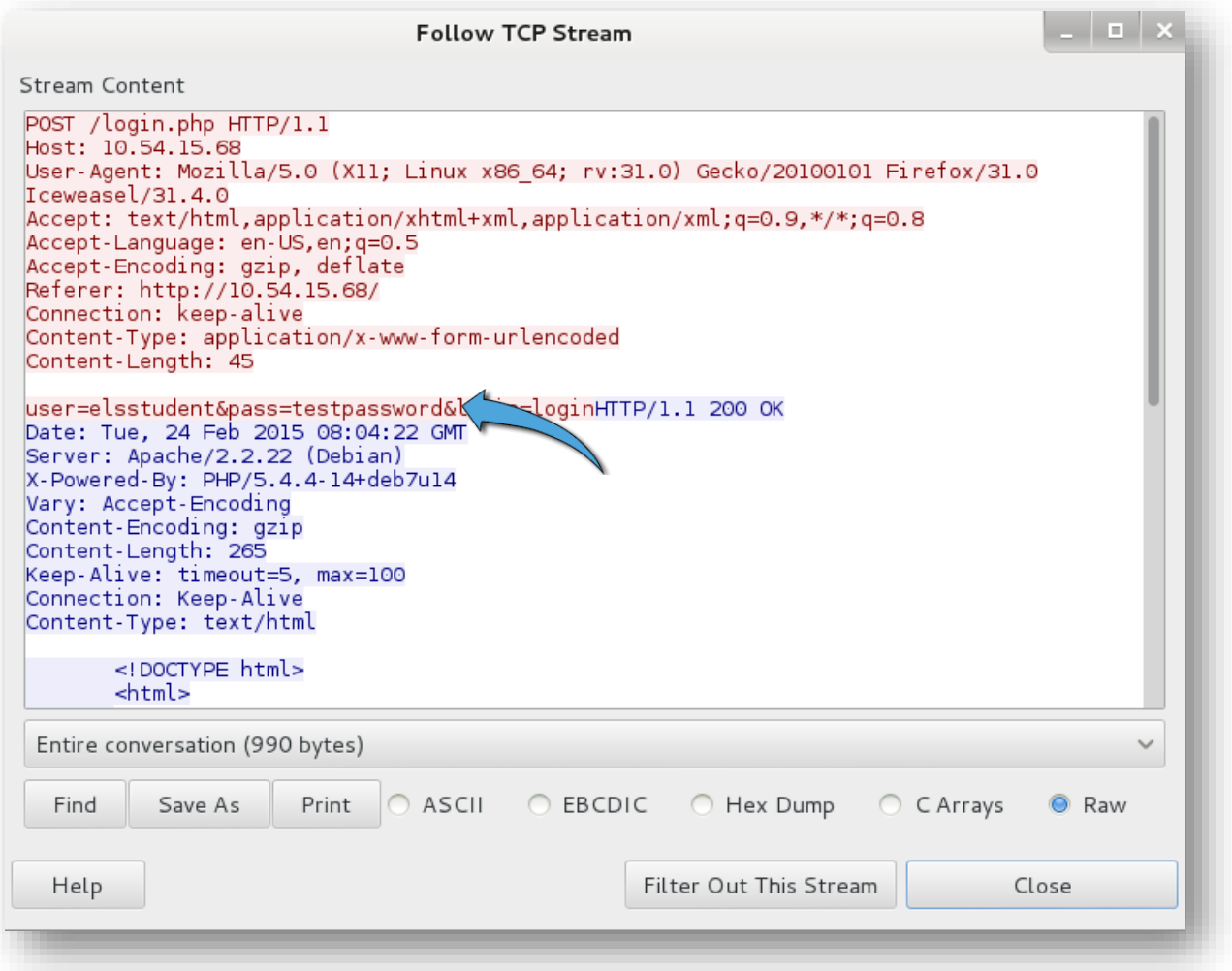
While Wireshark is running, open the browser. Then point it to http://10.54.15.68 and login. Wireshark will capture the traffic.

Then you can run the "Follow TCP Stream" command on the POST HTTP packet. You will see how HTTP works in the *Web Applications* module.

To run the "Follow TCP Stream" command, you have to right-click on the POST packet, and then click on "Follow TCP Stream".



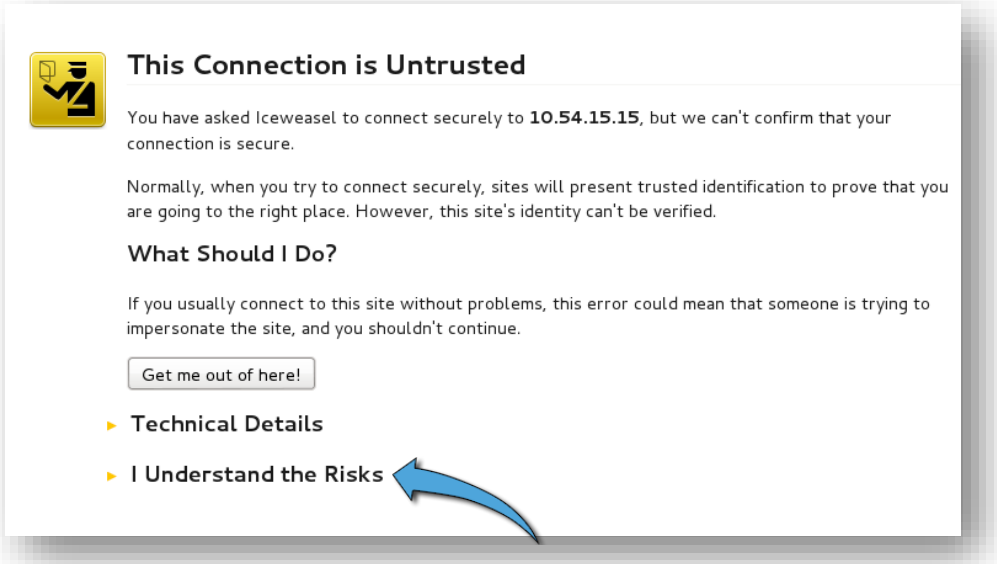
A window similar to the one in the image below will open. Please note that you can easily read the login credentials!

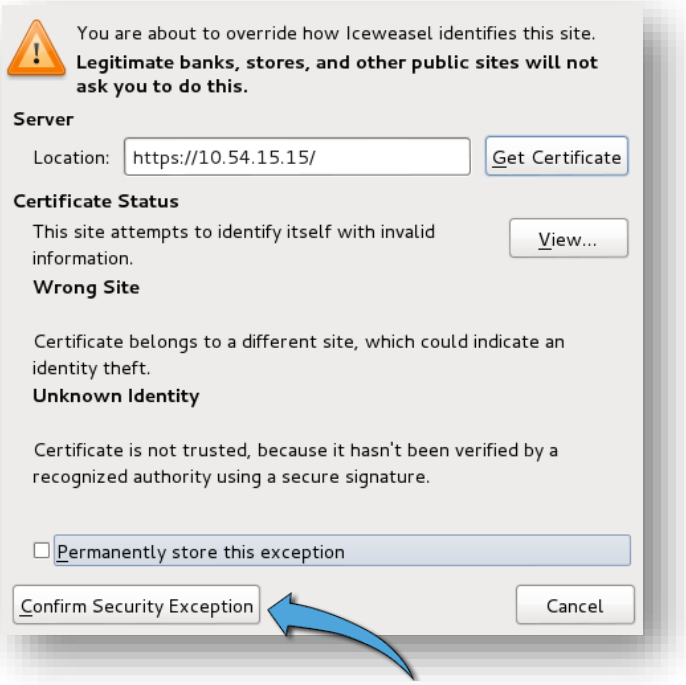


5.3. Capture and Analyze an HTTPS Login Session

Perform the same steps of the previous task on the login page at https://10.54.15.15.

Since the HTTPS server in the lab is private, you have to add a temporary exception to the browser:





After opening the login page, restart the capture in Wireshark and login.

After logging in, you can right-click on any packet to run the “Follow TCP Stream” command.

The results will be unreadable, because of the encryption made by HTTPS.