Due: Jan 28, 2020 11:59pm
You need to turn in a detailed written lab report (in PDF) that documents your findings, including required code (if any), screenshots, explanation of questions that we ask in this assignment. You need to finish your written lab report independently. Copying and sharing solutions are not allowed. Submit your lab report through Canvas.

HW1: HTTP Wireshark, Trace Decode, and Apache Web Server

1 Lab Task 1

1.1 Install Wireshark

Wireshark is a very important tool to learn network protocols; you can sniff every package that is going through the LAN. You can get Wireshark from http://www.wireshark.org.

1.2 Trace HTTP (screenshots, 15 points)

Use Wireshark to collect the HTTP request message when a web browser sends a request to the web server www.example.com, and collect the HTTP response message from the web server to web browser. Document the screenshots of captured HTTP messages by Wireshark.

1.3 Trace Decode (7*5 points)

Based on the collected HTTP messages, answer the following questions:

1. What is the full URL of the object requested by the web browser? (include both the server name and document path)
2. What version of HTTP is the browser using for this request? What version of HTTP is the web server using for the response?
3. Is this HTTP connection persistent or non-persistent?
4. What kind of web browser sent this request? Why does the server (potentially) need to know this information?
5. What operating system was the web browser running on?
6. What kind of web server answered the request?
7. Did the server successfully produce the requested document? What type of document did the server say it is?

2 Lab Task 2

2.1 Deploy Two Virtual Machines (screenshots, 20 points)

We need to deploy two virtual machines (SEEDUbuntu16.04 VM) on one physical machine (e.g., your laptop). You can download SEEDUbuntu16.04 VM from https://seedsecuritylabs.org/lab_env.html. We put these two VMs on the same network. For the VMnetwork setting, if you are using VirtualBox, please use "NAT Network" as the network adapter for each VM. If you are using Vmware, the default "NAT" setting is good enough. One IP address is set to 192.168.0.10, and the other one is 192.168.0.100. You need to make sure these two VMs are connected (you can use the $ping$ tool to test the connectivity)

2.2 Apache Web Server (screenshots and answers, 30 points)

Apache HTTP server is the most popular web server on the Internet. Your task in this problem is to run an Apache HTTP server on one of the SEEDUbuntu16.04 VMs, and answer the following questions. The Apache HTTP server is pre-built on SEEDUbuntu16.04 VM (so you do not need to install it). Please make sure that you start the server, i.e., the web server runs.

Please answer the following questions.

1. (10 points) Which port number is your Apache web server listening at?
2. (10 points) If you open your browser and enter https://localhost:XXXX, what do you see? You need to replace XXXX with your port number. Based on your observation above, does this default server configuration support HTTPS protocol? HTTPS is the secure version of HTTP protocol.
3. (10 points) Suppose the VM where the web server is running is VM A, and the other one is VM B. Find out the IP address of your VM A where the web server is running. Then access your web server by typing http://<ipaddress>:<portnumber> in the address bar of VM B. (You need to replace the ip address and the port number with the IP address and port number of yours.) Can you find out the access log on VM A showing the entries of VM B's http request?