CIS 458: Systems Security
Week02 Assignment: Networking Essentials for System Security and Qualitative Risk Assessment
Point Value: 15 Pts, late submission policy (20%/day for up-to 5 days)
Due Date: 9/14/2022 by 11:59PM EST
Submission format: The following reports to be submitted on BB using the assignment link of **"Submit Week02 Assignment Here":**

(1) Entire assignment solution in PDF format and created/submitted by (1st Group Member)
(2) Entire assignment solution in PDF format and created/submitted by (2nd Group Member)
(3) Agreed-Upon assignment solution for **Part I and Part II ONLY** and **(2) screenshots for Part III**

Note: Missing an individual's submission leads to receive **NO** credit for the individual's assignment.

Learning Objectives
In this lab, you'll:

- Practice with the essential networking concepts,
- Investigate several network attack scenarios,
- Perform a Qualitative Risk Assessment using PILAR Risk Management Tool.

What to turn in?

- Answer to the following questions as well as screenshots as directed.
- In your report, organize and answer the questions by labeling each section with the same headings listed in the assignment. In each section, list the question in BOLD first then list its answer second in non-bold format
- Note that the assignment report will be returned ungraded if it is submitted without complying with the above-mentioned requirements. 25% penalty will be applied for the re-submitted corrected version provided that it is resubmitted within the time frame allocated by the instructor; otherwise no credit will be given to the submitted work.

Part I: Working with Essential Networking Concepts (6Pts)

Working with HTTP Protocol
HTTP uses several methods to send web requests including GET and POST. POST method is used to allow users to upload an HTML form to send sensitive information such as password, Wireshark can reveal this info.

1. Open the **HTTP_FORM.pcap** file and filter the traffic to locate the password value.
   Q-1: What is the password info that you found? How did you find it? And why is Wireshark able to see it?
2. Open the **download.pcap** file in Wireshark and calculate the network throughput/(download data rate) for transmitting a file using HTTP protocol in this trace.
   Q-2: What is the file download's network throughput in Mbps?

Working with TCP Protocol
The Wireshark's IO graph tool is used to check client and server interaction data for a meaningful analysis. The Wireshark IO graph can help to measure the throughput (the rate is packet-per-tick), where each tick is one second. In this case, we will see how to make use of the IO graph.

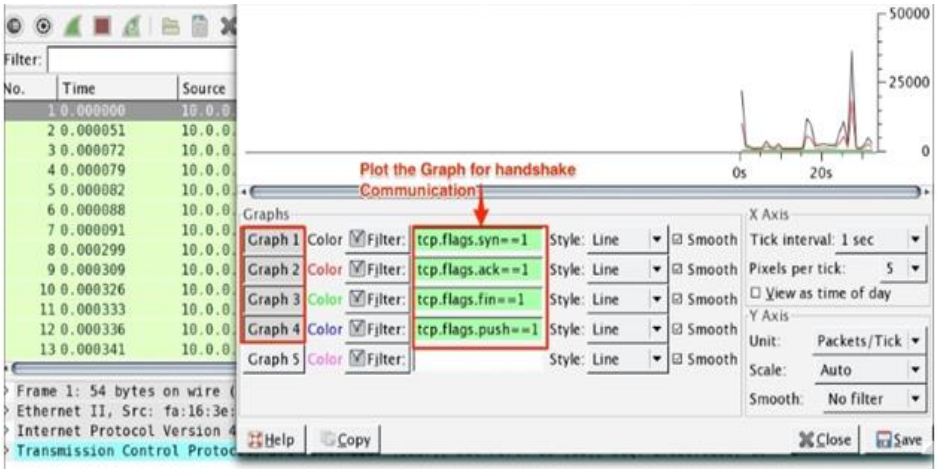
1. Open the file **http_01.pcap** in Wireshark and follow the given steps:
   - Click on **Statistics** | **IO graph**.
   - The **IO graph** dialog box will appear. In the **IO graph** dialog box try to find the spike and click on it.
   - When you click on the graph (the high area), Wireshark will automatically show the corresponding packet in the Packet List pane. Go back to the **IO graph** dialog box.
   - Apply this filter to the generated graph **tcp.analysis.duplicate_ack**
     Q:3 What is the outcome of this filter and how it is useful in troubleshooting network performance? Attach a screenshot for the graph generated showing the filter is applied to the graph.
2. Open the **RST-01.pcap** file in the Wireshark:
   Q-4: In this trace, investigate the RST TCP packet and explain why the RST packet has been set after SYN-ACK instead of ACK?
   Q-5: In what circumstances RST packet must be sent?
3. Open the **RST-02.pcap** file in Wireshark:
   Q-6: Investigate the RST TCP packet and explain why RST has been set after the SYN packet?

Part II: Network Attacks Scenarios **(4 Pts)**

There are various attack techniques that exploit how the network protocols are working. In this section, we will analyze several types of attacks by capturing traffic from live networks that happened to be under attack. Then, we will use Wireshark to make sense of this traffic and identify what type of attacks we are dealing with.

Scenario #1:

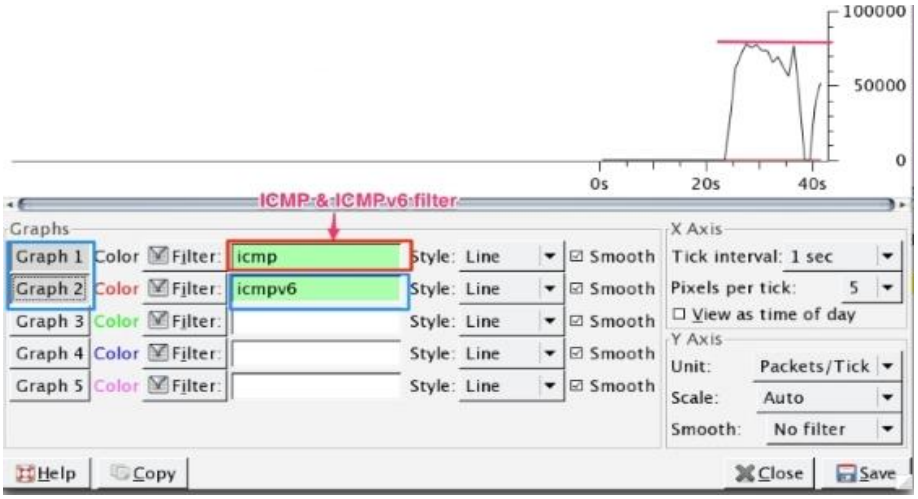
In this scenario, the network security team captured a real time traffic from a network under attack. Then, the Wireshark I/O graph tool was used to visualize the TCP handshake traffic for further analysis as shown below:



Q-1: Based on the graph shown above, what type of attack does the network suffer from? And why? What OSI Layer does this attack belong to? and why. Explain how can we defend our network against this attack?

Scenario #2:

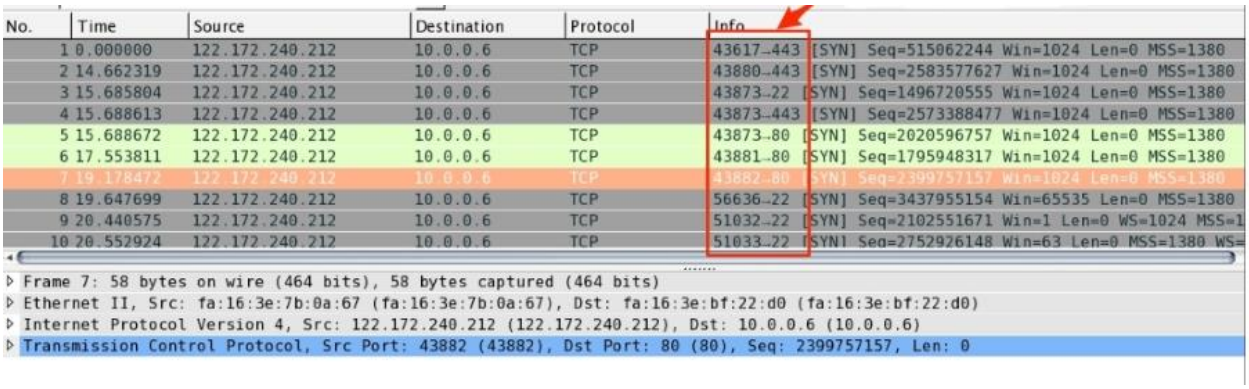
In this scenario, the network security team captured a real time traffic from a network under attack. Then, the Wireshark I/O graph tool was used to visualize the network traffic for further analysis as shown below:



Q-2: Based on the graph shown above, what type of attack does the network suffer from? And why? What OSI Layer does this attack belong to? and why. Explain how can we defend our network against this attack?

Scenario #3:

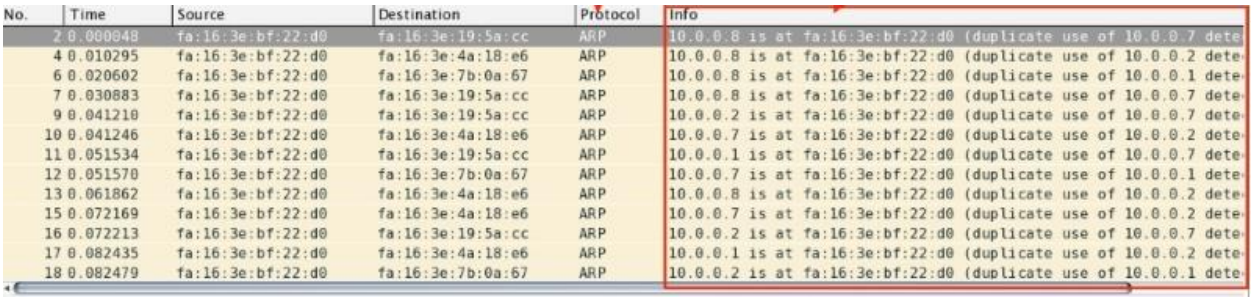
In this scenario, the network security team captured a real time traffic from a network under attack. Then, the Wireshark I/O graph tool was used to visualize the network traffic for further analysis as shown below:



Q-3: Based on the graph shown above, what type of attack does the network suffer from? And why? What OSI Layer does this attack belong to? and why. Explain how can we defend our network against this attack?

Scenario #4:

In this scenario, the network security team captured a real time traffic from a network under attack. Then, the Wireshark I/O graph tool was used to visualize the network traffic for further analysis as shown below:



Q-4: Based on the graph shown above, what type of attack does the network suffer from? And why? What OSI Layer does this attack belong to? and why. Explain how can we defend our network against this attack?

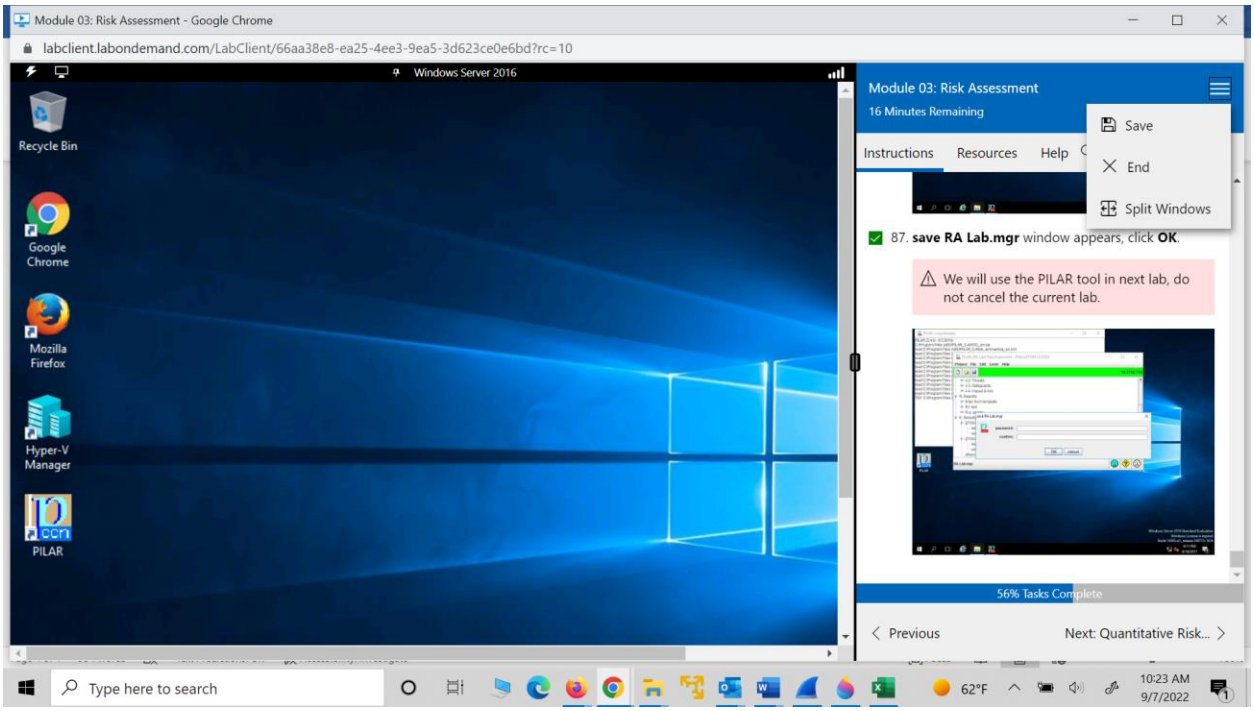
Part III: Qualitative risk assessment **(5Pts)**

Qualitative risk assessment is the process of using non-numerical based methods to identify and analyze the risk event and its impact if and when it occurs. It works on relative or descriptive measures to analyze the probability of the risk occurring.

1. Login into your iLabs account here:
   https://eccouncil.learnondemand.net/Organization/5922
2. Complete the Qualitative risk assessment part **(steps 1-87)** only. Here is the link to launch your assignment:
   https://eccouncil.learnondemand.net/Lab/23254
   Q-1: submit a screenshot that shows that you completed these steps. Ensure that the screenshot shows the date and timestamp of completion.

Notes:

- You can save your work and complete it later if you wish.
- Make sure to save your work before closing the lab assignment by going to the top right conner menu and select save. Screenshot below shows this info.
- The lab duration is listed in the system and can be extended twice for 15 minutes each.


Module 03: Risk Assessment - Google Chrome
labclient.labondemand.com/LabClient/66aa38e8-ea25-4ee3-9ea5-3d623ce0e6bd?rc=10
Windows Server 2016
Recycle Bin
Google Chrome
Mozilla Firefox
Hyper-V Manager
PILAR
Module 03: Risk Assessment
16 Minutes Remaining
Save
End
Split Windows
Instructions
Resources
Help
87. save RA Lab.mgr window appears, click OK.
We will use the PILAR tool in next lab, do not cancel the current lab.
56% Tasks Complete
Previous
Next: Quantitative Risk...
Type here to search
62°F
10:23 AM
9/7/2022