Module Two Assignment Introduction to Wireshark & Deep Packet Inspection

Grading Criteria

Total Points: 25

☐ **[2.5 points]** Your submission is labeled as "cs460_module01_lab00_[nau_id]_[lastname]_[firstname].pdf." For example, if I were to submit a file, it would be labeled as cs460_module01_lab00_mv668_vigil-hayes_morgan.pdf. **FAILURE TO COMPLY WITH THIS STEP CAN LEAD TO A ZERO GRADE.**

☐ **[2.5 points]** Your submission submitted in **PDF format**. **FAILURE TO COMPLY WITH THIS STEP CAN LEAD TO A ZERO GRADE.**

☐ **[10 points]** Part 1 has an annotated screenshot of your filtered traffic capture from Wireshark.

- ☐ [4 points] Screenshot is legible
- ☐ [3 points] There is a correct coded market next to the incoming/downlink packets
- ☐ [3 points] There is a correct coded marker next to the outgoing/uplink packets

☐ **[10 points]** Part 2 has correctly annotated screenshots of your filtered traffic capture from Wireshark (can use the same capture as used in Part 1)

- ☐ [2.5 points] There is a screenshot with a GREEN rectangle drawn around the payload portion of one of the incoming packets
- ☐ [2.5 points] There is a screenshot with a RED rectangle drawn around the payload portion of one of the outgoing packets
- ☐ [5 points] What are some things you think a malicious actor could learn from a packet capture collected using a tool like Wireshark?

Note that if you need any help with figuring out Wireshark, you can look to the resources linked at the end of this lab, seek help on the #module02 channel on the class Slack, or attend Office Hours.

Part 1: Capture Traffic

Hint: This lab is much easier if you close all other applications and other browser tabs and windows, e.g., do not have Slack open AND five different browser windows simultaneously because it will make it harder to discern which packets are supposed to be from the target web server.

Open Wireshark and start capturing packets on your Internet-facing network interface.

Open a browser and open this link:

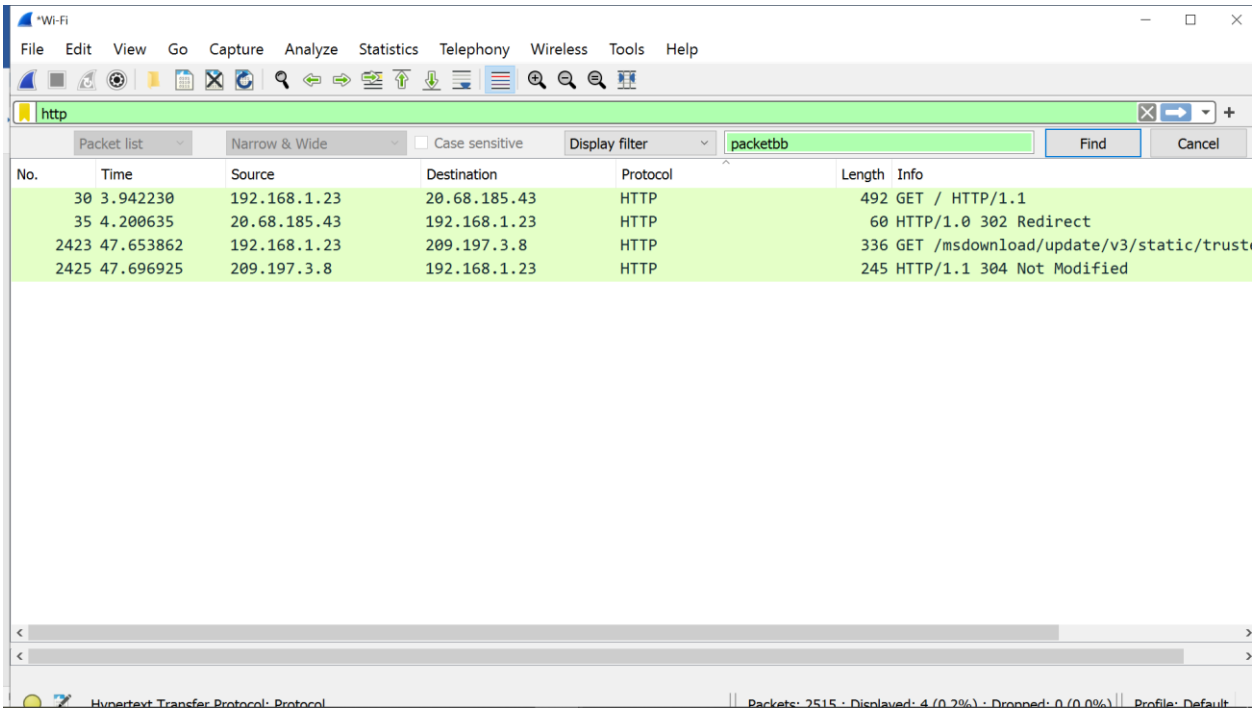
http://h2020.myspecies.info/

Pay attention to Wireshark. Take note of which IP address represents your address and which one represents the website server's address.

After the page has loaded in your browser, stop the capture in Wireshark.

Filter the packet capture so that you only see packets exchanged between your device and the web server. Take a screenshot that captures as many packets as you can and paste it below:

[SCREENSHOT GOES HERE]



Next, you will annotate your screenshot (which will hopefully help with Part 2).

Place a color-coded marker (e.g., a dot, a smiley face emoji) next to all packets that represent uplink traffic. *Make sure that you use the same marker for all uplink packets.*

Place a *different* color-coded marker (e.g., a star, an angry face emoji) next to all packets that represent downlink traffic. *Make sure that you use the same marker for all downlink packets.*

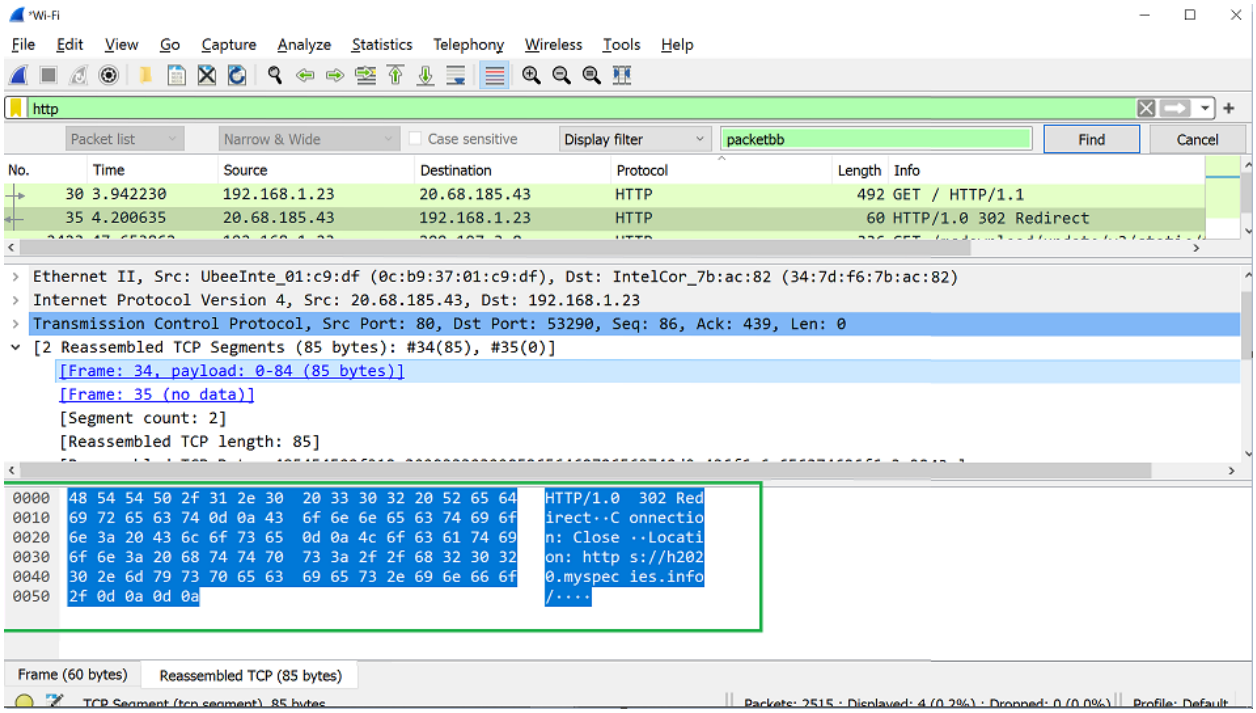
Part 2: Digging into Packets

For this part, you will be using the capture you have opened in Wireshark from Part 1.

Identify one of the HTTP packets that your browser sent to the web server. Use Wireshark to highlight the payload of the packet and take a screenshot and paste it below.

[SCREENSHOT GOES HERE]

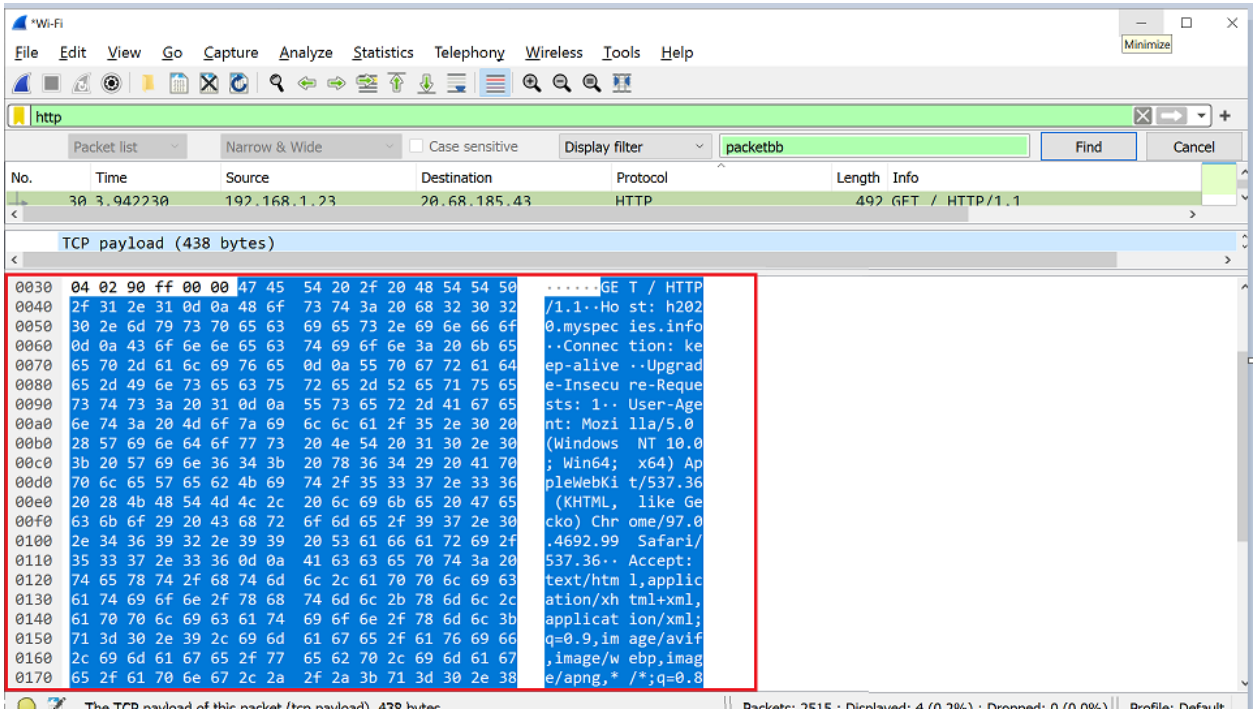
Payload portion of one of the incoming packets



Identify one of the HTTPs packets that the web server sent to your browser. Use Wireshark to highlight the payload of the packet and take a screenshot and paste it below.

[SCREENSHOT GOES HERE]

payload portion of one of the outgoing packets



Take some time to reflect on what you have learned so far in this class and what you observed doing the "deep packet inspection" exercise above. Write 1-2 paragraphs (~150 words) on how a malicious attacker might use a passive packet capturing tool like Wireshark to violate the CIA+authenticity+accountability pentagon we have discussed in class.

There are different types of network attacks aimed at three pillars of Network Security confidentiality, Integrity and availability

Attack against confidentiality:

Packet Capturing (Packet Sniffing): Packet Capturing (Packet Sniffing) is a type of network attack where the attacker capture the data packets (typically Ethernet frames) in travel. Once the data is captured, the

attacker can read the sensitive data like passwords or card numbers, if the network traffic is not encrypted. The most widely used packet capture software is Wireshark.

Phishing and Pharming: Phishing is an attempt to hack sensitive information (usually financial information like bank userid/password credit card details etc.), by sending unsolicited emails with fake URLs. Pharming is another network attack aimed at redirecting the traffic of one website to another website.

Attack against Integrity:

Salami attacks: Salami attacks are a series of minor data security attacks that together result in a larger attack. For example, deducting a very small amount or money from a bank account which is not noticeable. But when the deduct very small amounts from large number of accounts, it become a huge amount.

Data diddling attacks: Data diddling is an illegal or unauthorized data alteration. Changing data before or as it is input into a computer or output. Example: Account executives can change the employee time sheet information of employees before entering to the HR payroll application.

Attack against Availability:

DoS (Denial of Service attacks): DOS Attack is a type of attack to a network server with large number or service requests with it cannot handle. DoS (Denial of Service Attack) can causes the server to crash the server and legitimate users are denied the service.

DDoS (Distributed Denial of Service attacks): Distributed Denial of Service attack (DDoS) is a type of DoS attack, originating from many attacking computers from different geographical regions.

Resources

https://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/#:~:text=Sample%20Captures&text=The%20wiki%20contains%20a%20page,downloaded%20file%20to%20open%20one.&text=You%20can%20also%20save%20your,to%20save%20your%20captured%20packets.

https://www.wireshark.org/docs/wsug_html_chunked/ChapterWork.html