CYB102 Project 1

(🔗 Instructions Page)

👤 Student Name: Weicong Xie
✉️ Student Email: Weicongx.wx@gmail.com

Reflection (Required)

🤔 **Reflection Question #1:** If I had to **explain "what are .pcap files" in 3 emojis,** they would be… (Feel free to put other comments about your experience in this unit here, too!)

📡💾🔍

🧠**Reflection Question #2:** How does Wireshark help us to analyze network traffic?

It tells us the type of info being sent and tells us the source and destination.

📣 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

Required Challenges (Required)

Item #1: The bad apple's IP address:

10.6.1.104

Item #2: The subject lines of three different phishing emails:

1. I can destroy everything! - 12345678
2. You got owned! - jigabu
3. Your ife about to get ruined! - computercomputer

Item #3: An explanation of how you went about finding the bad apple from just the .pcap files: (Please be specific about what filters/searches you used!)

I opened A.pcap, searched: smtp.data.fragment, it seemed normal.

I opened B.pcap, searched: smtp.data.fragment, it seemed normal.

I opened C.pcap, searched: smtp.data.fragment, BOOM! I see a bunch of suspicious emails coming from the same IP address.

I opened D.pcap just to make sure, searched: smtp.data.fragment, it seemed normal.

Stretch Challenge (Optional)

Item #1: Three screenshots of three different .eml files showing the content of phishing emails you identified:

[Insert Screenshot Here]
[Insert Screenshot Here]
[Insert Screenshot Here]

Notes (Optional):

Submission Checklist

👉*Check off each of the features you have completed.* ***You will only be graded on the features you check off.***

Required Challenges

- ☑ ~~Item #1~~
- ☑ ~~Item #2~~
- ☑ ~~Item #3~~

Stretch Challenge

- ☐ Item #1