Project 3 - Network Forensics

Network forensics is the art of looking at saved network traffic to work out what happened. This is used, for example, when attackers are discovered inside a company's network and investigators want to find out which machines were compromised and what data was exfiltrated (stolen).

Network captures are made in packet capture (.PCAP) files. They contain every packet observed wherever the measurement was made. This could be a machine, switch, or router.

A super useful tool for capturing network traffic and analyzing PCAP files is Wireshark. You can find it at: https://www.wireshark.org/#download with versions for every major OS. You can find tons of tutorials online for how to use Wireshark, like this one: https://www.youtube.com/watch?v=74a8MTkh7Tk

Here is a link to a simple practice problem. The goal in this one is to find the two "flag" strings. You can paste the flags into the boxes on the web-page to check if you got them right. This challenge is what was shown in the lecture introducing this project:

For this project, we have a more complex networking task for you. You will need the PCAP as well as the slides that explain the scenario. If you have trouble downloading either of these in a browser, retry with a command line tool like wget.

Basically, somebody has been anonymously threatening a professor using a spoofed email account, and you are trying to figure out who did it. This challenge was built back before HTTPS was common, so you will be able to directly spy on lots of things that would normally be encrypted today. Here is the list of prime suspects, the students in the victim professor's class.

- Chemistry 109 class list:
  - Teacher: Lily Tuckrige
  - Students:
    - Amy Smith
    - Burt Greedom
    - Tuck Gorge
    - Ava Book
    - Johnny Coach
    - Jeremy Ledvkin
    - Nancy Colburne
    - Tamara Perkins
    - Esther Pringle
    - Asar Misrad
    - Jenny Kant

What to turn in:

Pretend that you work for this fictional university's IT department, and you need to figure out who is sending these threats. Because student disciplinary action is involved, you need to assemble evidence to prove your case. We are expecting a 2-3 page write-up of an accusation with proof to support it. The audience of this report should be non-technical university administrators, so if you use technical terms you should briefly explain what they mean.

Some things this writeup should include are:

- a summary of the first spoofed email incident, how the IT department began watching a particular dorm room, and then what you discover in that PCAP file.
- An accusation against one or more of the students in the class
- Proof that supports your accusation
- An explanation of how you found the proof you included. If you used Wireshark, talk about the filters and tools you used. This explanation will be the main way you show us that you did this project yourself, rather than taking an answer from somebody else. We recommend that it should constitute at least half of the overall report. You may include screenshots to help explain what happened, but please crop them so your report is not simply a pile of images

Graduate Extension:

For grad students, your report must contain the incriminating search engine queries the guilty suspect made. This is not strictly necessary to figure out what happened, but it makes the case stronger and you need to find and include this evidence.