CSCI 466- Networks Fall 2024

Wireshark Lab 4 (Network Forensics)

Due Wednesday, November 20th @ 11:59 PM.

Network forensics is the process of analyzing network traffic to identify the source of security incidents or malicious activity. Thousands of cyber crimes happen every day, and there is evidence that can be found in network traffic. In this lab, you will be analyzing the network traffic of an infected machine. You will answer questions and build a timeline to explain the who/when/how/what/why regarding the accident. You will use **Wireshark** and **Zui** to gather evidence and answer questions during your investigation.

Background Information: You, a network forensics investigator, have received an alert from the SOC team (Security Operations Center) that a machine on the enterprise network has been generating suspicious network traffic. The SOC team suspects that malware may have been installed on the machine. They were able to retrieve a recent PCAP file (lab4evidence.pcap) that captured recent network traffic from the (suspected) infected machine.

Tools:

- **Wireshark**: You should already have Wireshark installed on your machine. You can open the evidence PCAP file and analyze traffic
- **ZUI:** Zui is a forensics tool that can extract meaningful events and suspicious events from a PCAP file. You can open a PCAP file, and then enter the "query pool" to look at all the events and search for certain things
  Zui Download link: https://zui.brimdata.io/docs/Installation

Please do not use **NetworkMiner** for this assignment. **NetworkMiner** will reassemble files onto your machine, which may lead to potentially unwanted programs (PUPs) or malware being assembled onto your machine. You can use Wireshark and Zui to answer all the questions for this lab

Evidence: The evidence PCAP file can be downloaded here
https://www.cs.montana.edu/pearsall/classes/fall2024/466/labs/lab4evidence.pcap

You will need to download this file, and open it in Wireshark and Zui.

Load the PCAP file into Wireshark/ZUI, and answer some basic questions before looking for malicious traffic.

1. What is the hash of the evidence PCAP file?
2. What is the IP address of the infected machine? Is this a public or private IP address?
3. What is the MAC address of the infected machine?
4. What is the IP address of the DNS server that is used by the infected machine?

There was a piece of malware that was installed onto the machine. Try to find when and how the malware was installed onto the machine (from the network trace) and answer the following questions:

5. Find the initial piece of malware. Take a screenshot of the malicious packet/event.
    a. What is the filename of the malware?
    b. What is the file extension of the malware?
    c. What is the hash of the malware?
6. Plug the hash value into VirusTotal and take a screenshot. Is the file malicious?
7. What is the "name" associated with this malware?
8. What type of malware is it? (You can google common malware types if you don't know what this question is asking)
9. What IP address did the malware come from? Plug the IP address into VirusTotal and take a screenshot. Is it a malicious IP address?
10. This IP address came from a DNS query. What is the hostname associated with this IP address? Plug the hostname into VirusTotal and take a screenshot.
11. Use a **WHOIS** tool (there are tons of these tools online) to find out who is registered under that IP address and take a screenshot

Next, you will try to find evidence of C2 communication, which is very common behavior in cyber attacks.

12. Is there any evidence of communication with a command and control (C2) server?
13. What is the IP address of the C2 server?
14. Did this IP address come from a DNS query?. What is the hostname associated with that IP address?
15. What types of messages were exchanged with the C2 server?
16. Did the infected machine download any files from the C2 server?

Lastly, answer some additional questions regarding the incident.

17. Are there any other suspicious files you can see from the trace? Do you think they are malicious?
18. Using your answer from question 7, do a little bit of research/chat-gpt into this specific strand of malware. What does this malware typically *do* according to your research? (ie what are the common behaviors for this malware?)
19. Using your answer from question 7, how is this malware typically distributed? (ie how do machines get infected with this malware to begin with?)
20. Using all the evidence you have collected, build a basic timeline with the important events that transpired during the cyber attack. Be sure to include a timestamp for each event.

Submission

Please take your answers and screenshots and place them in a lab report. Submit your lab report as a PDF to the Brightspace submission box.

You are allowed to work with one partner. If you worked with a partner, please write each persons name at the top of the lab report.