Intro to Network Traffic Analysis

Network traffic analysis is the act of monitoring network traffic in order to detect and prevent threats and other possible problems. There are many ways to monitor networks. A common way is to use a packet sniffer such as Wireshark on a host machine. Network traffic analysis is important to any organization because it can help detect suspicious traffic and is a starting point for threat hunting and incident resoponse.

Three Real-World Use Cases

1. Identify possible cyber attacks

2. Monitor employee's traffic for disallowed content

3. Investigating events

Step By Step Guides

How to open a PCAP file with Wireshark

1. Open Wireshark

2. Click file in the menu bar

3. Click open in the dropdown menu

4. Choose the file you would like to open

5. Click Open

How to apply filters in Wireshark

1. In Wireshark click the search bar at the top of the screen

2. Type in whicever protocols, ip addresses, etc you would like to filter

How to export a filtered packet capture in Wireshark

1. Once you have paused the capture on wireshark apply the filter(s) that you want

2. Click File

3. Click Export Specified Packets

Screenshots



