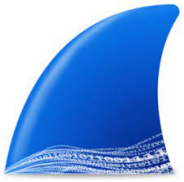

Activity: Analyzing a PCAP file for Signs of Network Attack

Analyzing a PCAP (Packet Capture) file can provide invaluable insight into network behavior and potential attacks. Here's an activity to guide you:

1. **Open the PCAP file in Wireshark**
    - Launch Wireshark.
    - Click on `File` in the menu, then `Open`, and navigate to your PCAP file. Click `Open` to load it.
2. **Explore the Packet List Pane**
    - This pane displays all the packets in the PCAP file in chronological order.
    - Review the Source, Destination, Protocol, and Info columns to get an overview of the network communication. Look for any patterns or anomalies.
3. **Use Display Filters**
    - Display filters help you to narrow down the packet view.
    - For instance, if you want to see only DNS traffic, enter `dns` in the display filter bar and press Enter.
4. **Look for Malicious Traffic**
    - Look for multiple SYN packets without corresponding ACK packets, which could indicate a SYN flood attack.
    - Look for a large number of packets sent to or received from a specific IP address or set of IP addresses, which might indicate a DDoS attack.
    - Use `http.request` or `http.response` filters to view HTTP requests and responses. Look for suspicious GET requests or status codes (like multiple 401 Unauthorised responses, indicating brute-force attacks).
5. **Inspect Packet Details**
    - Click on a packet to select it. The Packet Details pane will show the selected packet's layered structure.
    - Expanding the layers will show more detail. For example, in a TCP packet, you can see the source and destination ports, sequence numbers, and flags.
6. **Follow TCP/UDP/HTTP Streams**
    - Right-click on a packet and select `Follow` > `TCP Stream` (or UDP, HTTP as appropriate).

- This brings up a dialogue showing the complete conversation between the client and server. This can be useful to see the content of a session and identify anomalies.

7. **Use Statistics Tools**
    - Wireshark has many built-in tools to analyze traffic. For instance, `Statistics > Conversations` shows the communication between different pairs of endpoints.
    - `Statistics > Endpoints` shows all unique network endpoints. A large amount of traffic to/from a single endpoint could suggest an attack.
    - `Statistics > Protocol Hierarchy` shows what protocols are being used and how much of the traffic each one takes up.
8. **Save Your Analysis**
    - You can save filtered packet views for future reference or to share with others. Just set your filter, then click `File > Save As` and ensure the `Displayed` option is selected.