Research network protocol analyzer

In this activity, you'll focus on the two network protocol analyzers: Wireshark and tcpdump. Your goal is to gain a basic understanding of the Wireshark and tcpdump, how they work, and what their features are.

As you've learned, a **network protocol analyzer (packet sniffer)** is a tool designed to capture and analyze data traffic within a network. Network protocol analyzers help security analysts examine and understand the network traffic flows.

Be sure to complete this activity before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

Scenario

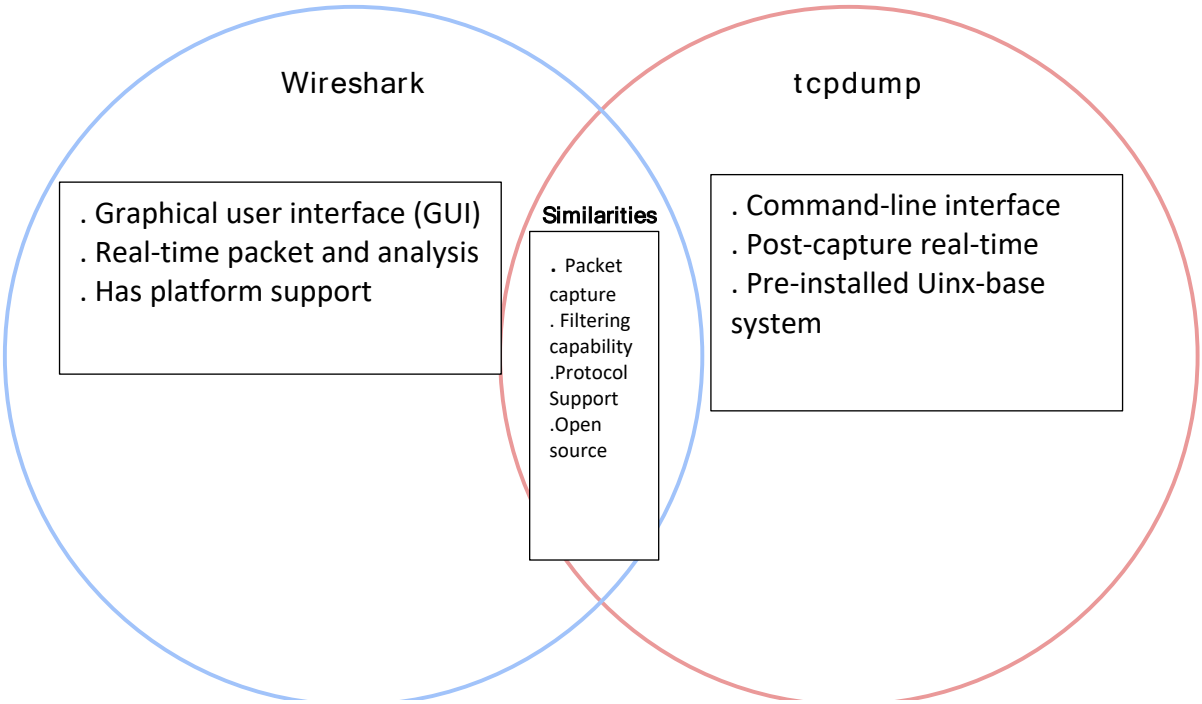
Review the following scenario. Then complete the step-by-step instructions.

In your role as a cybersecurity analyst, you have been asked to research the differences and similarities between Wireshark and tcpdump and create a chart that outlines your findings.

Step-By-Step Instructions

Follow the instructions and answer the question to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

Step 1: Access the template



Step 2: Conduct online research

To begin, conduct online research to learn more about tcpdump and Wireshark. You can begin by using the official Wireshark documentation and tcpdump documentation:

- tcpdump - Resources and documentation
- Wireshark - Official user guide

You can also perform an internet search to find resources that explain how these tools work. Try searching for information using these terms:

- *Wireshark features and functionalities*
- *tcpdump features and functionalities*
- *comparison between tcpdump and Wireshark*

Be sure to critically evaluate the search results and select reliable and authoritative sources such as official documentation, reputable cybersecurity websites, or technical forums that provide accurate and factual information about the tools.

Explore these resources to gather information on tcpdump and Wireshark and focus on understanding the different features and functionalities that each tool has.

Consider these questions to help you compare the two tools:

- What software or equipment is required to access and use the tool? Is the tool open-source or proprietary?
- What type of user interface or layout does the tool use?

- How do security analysts typically use the tool? What are the recommended usage scenarios for each tool?
- How does the tool handle capturing, analyzing, and filtering network traffic?
- Are there any limitations or considerations for using this tool?

Step 3: Fill in the diagram

Pro Tip: Save the template

Finally, be sure to save a blank copy of the template you used to complete this activity. You can use it for further practice or in your professional projects. These templates will help you work through your thought processes and demonstrate your experience to potential employers.

What to Include in Your Response

Be sure to address the following elements in your completed activity:

- **At least 2 differences** between Wireshark and tcpdump
- **At least 3 similarities** between Wireshark and tcpdump

Three differences between Wireshark and tcpdump:

. User Interface:

Wireshark: It has a graphical user interface (GUI) that provides a user-friendly environment. Users can visually inspect captured packets and apply various filters through a graphical interface.

tcpdump: It operates from the command line and lacks a graphical interface. Users interact with the tool using commands, making it more suitable for users comfortable with a command-line environment.

. Real-Time Analysis:

Wireshark: It allows real-time packet capture and analysis. Users can see and analyze network traffic as it happens.

tcpdump: While it can capture packets in real time, the analysis is typically done post-capture. Users may need to capture data first and then analyze it using other tools or review the captured data manually.

. Platform Support:

Wireshark: It provides a more extensive range of platform support, including Windows, macOS, and various Linux distributions. The GUI makes it accessible to users across different operating systems.

tcpdump: It is primarily a command-line tool and is often found pre-installed on Unix-based systems. While it can be used on Windows with tools like WinDump, it is more native to Unix environments.

Four similarities between Wireshark and tcpdump:

. Packet capture:
Both Wireshark and tcpdump are network protocol analyzers designed for capturing and analyzing packets in a network.

. Filtering Capabilities:
Both tools offer powerful filtering capabilities to focus on specific types of traffic. Filters can be based on protocols, IP addresses, ports, and other criteria.

. Protocol Support:
Wireshark and tcpdump support a wide range of network protocols, making them versatile for analyzing diverse network environments.

. Open Source:
Both Wireshark and tcpdump are open-source tools, meaning their source code is freely available to the public. This fosters a collaborative development environment and allows users to modify the tools to suit their needs.
Remember to verify the details through the official documentation and other reliable sources to ensure accuracy in your response.