**Activity Overview**



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**

To use the template for this course item, click the link and select *Use Template*.

Link to template:[Diagram template](https://docs.google.com/presentation/d/1ouKZ4YVI9IKrIEGEz5A-A2fwcKsLYxZRqtOT1d9D-Lc/template/preview?usp=sharing&resourcekey=0-5nQZnN18beQMlTyXERtt0A)

OR

If you don’t have a Google account, you can download the template directly from the following attachment.

[Diagram template](https://d3c33hcgiwev3.cloudfront.net/3DAgXUPIS7GOQrGQx8Zpng_37a4405bb78c48b0b9269a90b6c730f1_Diagram-template.pptx?Expires=1722729600&Signature=AvaHBICsqlftaLQm76CetbTk472CgjmEGCcYxiwd3R1XoAqaQ4fPJZUeu810jqeb09SxjhBwmH1AinsBhCKiV21sV6tiN-GjxjfUqxmT2NF1WEQfS-xMTQryyx3a2~4zYsZaauGGBA3K0uvhhwsm-oKIOEpkLn7bLiEbtfoM8zs_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[PPTX File](https://d3c33hcgiwev3.cloudfront.net/3DAgXUPIS7GOQrGQx8Zpng_37a4405bb78c48b0b9269a90b6c730f1_Diagram-template.pptx?Expires=1722729600&Signature=AvaHBICsqlftaLQm76CetbTk472CgjmEGCcYxiwd3R1XoAqaQ4fPJZUeu810jqeb09SxjhBwmH1AinsBhCKiV21sV6tiN-GjxjfUqxmT2NF1WEQfS-xMTQryyx3a2~4zYsZaauGGBA3K0uvhhwsm-oKIOEpkLn7bLiEbtfoM8zs_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

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](https://www.tcpdump.org/index.html#documentation)
* [Wireshark - Official user guide](https://www.wireshark.org/docs/wsug_html/)

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?