Congratulations! You passed!

Grade received 100% **To pass** 100% or higher

Go to next item

To pass this course item, you must receive at 100%, or 1 out of 1 point, by completing the following activity. You can learn more about graded and practice items in the course overview.

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

OR

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

Diagram template
PPTX File

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

After you've completed your research on Wireshark and tcpdump, fill out the template and include at least two features for each tool. These could be related to the tool's capabilities, the type of analysis they perform, contrasting features, user interfaces, usage scenarios, and any other notable distinctions. Then, include three similarities between tcpdump and Wireshark.

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

1. Did you complete this activity? **1 / 1 point**

- (•) Yes
- ( ) No

Correct
Thank you for completing this activity! Understanding the features, capabilities, and limitations of different network protocol analyzers will help you choose and use the appropriate tool to effectively analyze network traffic and respond to security incidents. Go to the next course item to compare your work to a completed exemplar.