

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.

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

© Anushka Sinha | github.com/rikusmiles/