Activity: Research network protocol analyzers

i probably legally cant give you anything coz its an activity
but here is the gist

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.

theres a venn diagram

just make a similarities chart lol

if you cant figure it out heres a chat gpt answer to the question

GPT ANSWER

Lord Naruzkurai,

Both TCPdump and Wireshark are network analysis tools, but they serve different needs & operate in different contexts. Below are some of the similarities they share:

Packet Capturing:

1. **Core Functionality**: Both TCPdump and Wireshark can capture packets traveling over a network.
2. **Libpcap**: They both use the libpcap library for packet capturing, which makes them highly compatible in terms of the data they can capture.

3. **Filters**: Both offer a filtering mechanism for capturing specific types of packets.

Protocols:

1. **Protocol Support**: Both support a wide range of protocols like TCP, UDP, HTTP, FTP, etc.
2. **Packet Decoding**: Each can decode packets into a more human-readable form, although Wireshark offers a more GUI-driven approach.

Platforms:

1. **Cross-Platform**: Both are available for multiple platforms. TCPdump is primarily used in UNIX-like systems, while Wireshark is available for Windows, macOS, & various Linux distributions, including those you're familiar with such as Ubuntu, Arch, and RHEL9.

Analysis:

1. **Offline Analysis**: Both can save packet data to a file (usually in pcap format) for later analysis.
2. **Deep Inspection**: Both provide a way to look deep into packets to examine header & payload data.

Flexibility:

1. **Command-Line & GUI**: Both tools offer command-line options. While TCPdump is primarily a command-line tool, Wireshark also provides tshark, its own command-line interface.
2. **Scripting**: Both can be scripted & automated to some extent, useful for CyberSec tasks and ethical hacking.

Real-Time & Post-Capture:

1. **Real-Time Analysis**: Both allow real-time packet analysis, although Wireshark offers more detail in an easier-to-read format.
2. **Post-Capture Filters**: Both allow filtering packets after they have been captured.

Revision #1
Created 13 September 2023 14:18:42 by naruzkurai
Updated 1 November 2023 01:10:46 by naruzkurai