Read tcpdump logs

A **network protocol analyzer**, sometimes called a packet sniffer or a packet analyzer, is a tool designed to capture and analyze data traffic within a network. They are commonly used as investigative tools to monitor networks and identify suspicious activity. There are a wide variety of network protocol analyzers available, but some of the most common analyzers include:

- SolarWinds NetFlow Traffic Analyzer
- ManageEngine OpManager
- Azure Network Watcher
- Wireshark
- tcpdump

This reading will focus exclusively on tcpdump, though you can apply what you learn here to many of the other network protocol analyzers you'll use as a cybersecurity analyst to defend against any network intrusions. In an upcoming activity, you'll review a tcpdump data traffic log and identify a DoS attack to practice these skills.

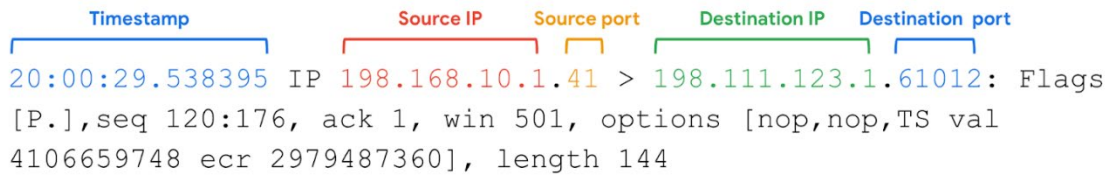
tcpdump

tcpdump is a command-line network protocol analyzer. It is popular, lightweight–meaning it uses little memory and has a low CPU usage–and uses the open-source libpcap library. tcpdump is text based, meaning all commands in tcpdump are executed in the terminal. It can also be installed on other Unix-based operating systems, such as macOS®. It is preinstalled on many Linux distributions.

tcpdump provides a brief packet analysis and converts key information about network traffic into formats easily read by humans. It prints information about each packet directly into your terminal. tcpdump also displays the source IP address, destination IP addresses, and the port numbers being used in the communications.

Interpreting output

tcpdump prints the output of the command as the sniffed packets in the command line, and optionally to a log file, after a command is executed. The output of a packet capture contains many pieces of important information about the network traffic.



Some information you receive from a packet capture includes:

- **Timestamp**: The output begins with the timestamp, formatted as hours, minutes, seconds, and fractions of a second.
- **Source IP**: The packet's origin is provided by its source IP address.
- **Source port**: This port number is where the packet originated.
- **Destination IP**: The destination IP address is where the packet is being transmitted to.

- **Destination port**: This port number is where the packet is being transmitted to.

Note: By default, tcpdump will attempt to resolve host addresses to hostnames. It'll also replace port numbers with commonly associated services that use these ports.

Common uses

tcpdump and other network protocol analyzers are commonly used to capture and view network communications and to collect statistics about the network, such as troubleshooting network performance issues. They can also be used to:

- Establish a baseline for network traffic patterns and network utilization metrics.
- Detect and identify malicious traffic
- Create customized alerts to send the right notifications when network issues or security threats arise.
- Locate unauthorized instant messaging (IM), traffic, or wireless access points.

However, attackers can also use network protocol analyzers maliciously to gain information about a specific network. For example, attackers can capture data packets that contain sensitive information, such as account usernames and passwords. As a cybersecurity analyst, It’s important to understand the purpose and uses of network protocol analyzers.

Key takeaways

Network protocol analyzers, like tcpdump, are common tools that can be used to monitor network traffic patterns and investigate suspicious activity. tcpdump is a command-line network protocol analyzer that is compatible with Linux/Unix and macOS®. When you run a tcpdump command, the tool will output packet routing information, like the timestamp, source IP address and port number, and the destination IP address and port number. Unfortunately, attackers can also use network protocol analyzers to capture data packets that contain sensitive information, such as account usernames and passwords.