LESSON NOTES

Intro to Linux

System Management

1.5.3 Network Monitoring

Lesson Overview:

Students will:

- Understand the utilities used for monitoring and managing networks

Guiding Question: How can a network be monitored and managed?

Suggested Grade Levels: 9 - 12

Technology Needed: None

CompTIA Linux+ XK0-005 Objective:

1.5 - Given a scenario, use the appropriate networking tools or configuration files

- Network monitoring
  - tcpdump
  - wireshark/tshark
  - netstat
  - traceroute
  - ping
  - mtr

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Network Monitoring

Network monitoring involves various tools and utilities to analyze and troubleshoot network-related issues. CompTIA stresses tcpdump, wireshark/tshark, netstat, traceroute, ping, and mtr.

The command-line packet analyzer **`tcpdump`** captures and displays network traffic on a specific network interface. This is useful for monitoring network packets in real-time. **`tcpdump`** can be used with various options to capture and filter packets based on specific criteria like source/destination IPs, ports, or protocols.

Wireshark is a network protocol analyzer via GUI (graphical user interface), while **`tshark`** is its command-line counterpart. Both provide detailed insights into network traffic by capturing and analyzing packets and can filter and dissect network packets for troubleshooting and monitoring.

The command-line utility **`netstat`** displays network-related information, including active network connections, routing tables, and interface statistics. Running **`netstat`** with various options provides information about network connections, routing, and statistics. This is useful for monitoring network connections and checking for open ports.

The command-line utility **`traceroute`** traces the route (hence the name) taken by packets from a computer to a destination host. This shows each hop along the path and the round-trip times. Using the destination hostname or IP address with **`traceroute`** shows the path and latency of packets as they travel through routers and switches to reach the destination. (Please note, **`traceroute`** does not work on many cyber ranges including the CYBER.ORG Range because network traffic is filtered)

A simple command-line tool called **`ping`** is used to test the reachability of a host on a network and measure the round-trip time for packets to travel to that host and back. Using **`ping IP`** where IP is the destination IP address or hostname will send ICMP echo requests and display the response time. This is useful for checking network connectivity and latency.

Combining both **`ping`** and **`traceroute`** is the utility **`mtr`** (My TraceRoute). This continuously sends ICMP packets to a destination while displaying the round-trip times and tracing the route, providing ongoing network performance metrics. Similarly, **`mtr IP`** where IP is the same as above starts a continuous trace route and ping monitoring session, which can help identify network issues over time.

These network monitoring tools are essential for diagnosing network problems, analyzing traffic, and ensuring network performance and reliability. The appropriate tool needed for network monitoring tasks depends on the user's specific needs and preferences.