Intro to Linux

1.5.3 - Network Monitoring

CYBER.ORG
THE ACADEMIC INITIATIVE OF THE CYBER INNOVATION CENTER

Network Monitoring

- Involves various tools and utilities to analyze and troubleshoot network-related issues
- **`tcpdump`** captures and displays network traffic on a specific network interface
  - Useful for monitoring network packets in real-time
  - Captures and filters packets based on source/destination IPs, ports, or protocols

Network Monitoring cont'd

- Wireshark is a network protocol analyzer via GUI
- **`tshark`** is the command-line counterpart to Wireshark
  - Provide detailed insights into network traffic by capturing and analyzing packets and can filter and dissect network packets for troubleshooting and monitoring
- **`netstat`** displays network-related information
  - Includes active network connections, routing tables, and interface statistics

Traceroute, Ping, and mtr

- **`traceroute`** traces the route taken by packets from a computer to a destination host
  - Shows each hop along the path and the round-trip times
- **`ping`** can be used to test the reachability of a host on a network, measuring the round-trip time for packets to that host and back
- **`mtr`** (My TraceRoute) combines ping and traceroute
  - Continuously sends ICMP packets to a destination while displaying the round-trip times and tracing the route