Cybersecurity

Operations and Incident Response

4.1.4 Packet Capture and Replay Tools

What are 3 commonly used packet capture and replay tools?

Overview
Given a scenario, the student will use the appropriate tool to assess organizational security.

Grade Level(s)
10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

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).

Teacher Notes:

CompTIA SY0-601 Security+ Objectives

Objective 4.1

- Given a scenario, use the appropriate tool to assess organizational security.
    - Packet capture and replay
        - Tcpreplay
        - Tcpdump
        - Wireshark

Packet Capture and Replay Tools

The ***tcpdump*** tool is a packet analyzer. tcpdump analyzes packets on a network based on a set of criteria known as filters. Filters could be for a set protocol: "http only," "udp only," "icmp only," or it could be for a set host, or for packets going/coming from a certain port. tcpdump can record packets and write them to a file if desired. If file output is not enabled, the results will be displayed to the screen. This tool is a great passive network scanner.

Wireshark is the same type of tool as tcpdump; it analyzes any and all traffic that goes over a network. Similar to tcpdump, Wireshark also uses filters so that the user can sort through all the packets to look for certain ones. The difference between tcpdump and Wireshark is that tcpdump is a command in a Terminal while Wireshark has a GUI. This makes Wireshark easier to use for most beginners because of the graphical interface.

The ***tcpreplay*** command is similar to tcpdump and Wireshark where it captures network traffic; however, it also replays, or retransmits the commands as well. This can be very powerful for malicious actors as they can replay authentication packets, allowing a malicious user to log into a system. tcpreplay can also be used to modify packets, thus a user can capture packets, edit or modify certain packets before replaying them on the network. Companies might use tcpreplay to test security devices to see if they are vulnerable to certain types of attacks.