

## Cybersecurity Guided Notes (ANSWER KEY)

# Lesson 4.1.4 - Packet Capture and Replay Tools

1. What is the function of a tcpdump tool?

It analyzes the packets being sent and received over a network.

2. What are filters as used in a tcpdump operation?

Filters are the set of criteria guiding the tcpdump process of analyzing packets

3. What are the common definitive types of filters applied in a tcpdump?

The types include protocol filters, host filters, and port filters

4. What happens when the file output function for a tcpdump is not enabled?

The results of the operation will only be displayed on the computer screen

5. What are the key differences between Wireshark and tcpdump?

Wireshark is a GUI user environment while tcpdump is used in a CLI environment

6. If a user wishes to run a network analysis on a Google Chromebook using both Wireshark and tcpdump, how would they go about it?

To use Wireshark, the user will download and install the executable setup file and then run it to perform a network analysis. For tcpdump, the user will use Chrome Shell, which is the command line for Chrome OS, to run the tcpdump command..

7. How is tcpreplay different from tcpdump?

In addition to capturing network traffic, tcpreplay also retransmits commands

8. In what way can tcpreplay be a useful or malicious tool?

Because it can retransmit commands, the tool can be used to replay authentication packets which can either allow a malicious user to gain access into a system or help a security professional to test a system's vulnerability to certain network attacks. Also, it allows the user to edit or modify packets.

9. How might tcpreplay compromise network security?

An attacker may modify packets so that they are directed to a different destination than the one intended or to the target system..