

Lab #7 - Assessment Worksheet

Analyzing Network Traffic to Create a Baseline Definition

Course Name and Number:

Student Name:

Instructor Name:

Lab Due Date:

Lab Assessment Questions & Answers

1. Both Wireshark and NetWitness Investigator can be used for packet captures and analysis. Which tool is preferred for each task, and why?
2. What is the significance of the TCP three-way handshake for applications that utilize TCP as transport protocol?
3. How many different source IP host addresses did you capture in your protocol captures?
4. How many different protocols did your Wireshark capture session have? What function in Wireshark provides you with a breakdown of the different protocol types on the LAN segment?
5. How can you find Wireshark network traffic packet size counts? How and where? Are you able to distinguish how many of each packet size was transmitted on your LAN segment? Why is this important to know?

6. Why is it important to use protocol capture tools and protocol analyzers as an information systems security professional?

7. What are some challenges to baseline analysis?

8. Why would an information systems security practitioner want to see network traffic on both internal and external network traffic?

9. Which transactions in the lab used TCP as a transport protocol? Which used UDP? Which ports were used in the lab?