Lab #7 – Assessment Worksheet

Analyzing Network Traffic to Create a Baseline Definition

Course Name and Number: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you monitored the traffic on the virtual network, a key step in determining a network baseline. You used TCPdump, a command line packet analyzer, to capture HTTP traffic generated by the Damn Vulnerable Web Application (DVWA). You used Wireshark to capture traffic you generated with the available tools using Telnet, Secure Shell (SSH), File Transfer Protocol (FTP), and Trivial FTP (TFTP) protocols over several machines in the network. Finally, you used NetWitness Investigator as to analyze the captured data.

Lab Assessment Questions & Answers

1. Both Wireshark and NetWitness Investigator can be used for packet capture 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 address did you capture in your protocol capture?

4. How many different protocols did your protocol capture session have? What function in Wireshark provides you with a breakdown of the different protocol types on the LAN segment?

5. How and where can you find Wireshark network traffic packet size counts? Can you distinguish how many of each packet size was transmitted on your LAN segment? Why is this important?

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?