Lab #5 – Assessment Worksheet

Performing Packet Capture and Traffic Analysis

Course Name and Number: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you used common applications to generate traffic and transfer files between the machines in this lab. You captured data using Wireshark and reviewed the captured traffic at the packet level, and then you used NetWitness Investigator, a free tool that provides security practitioners with a means of analyzing a complete packet capture, to review the same traffic at a consolidated level.

Lab Assessment Questions & Answers

1. Why would a network administrator use Wireshark and NetWitness Investigator together?

2. What was the IP address for LanSwitch1?

3. When the 172.16.8.5 IP host responded to the ICMP echo-requests, how many ICMP echo-reply packets were sent back to the vWorkstation?

4. What was the terminal password for LanSwitch 1 and LanSwitch 2?

5. When using SSH to remotely access a Cisco router, can you see the terminal password? Why or why not?

6. What were the Destination IP addresses discovered by the NetWitness Investigator analysis?

7. Are packet-capturing tools like Wireshark less dangerous on switched LANs?