Lab #7 - Assessment Worksheet

Analyzing Network Traffic to Create a Baseline Definition

Course Name and Number: IT NET 280 - Ethical Hacking

Student Name: Connor Morrissy

Instructor Name: Darnell Payne

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?
   Wireshark is better suited for protocol capture because there is no limit on the size of the capture file while NetWitness has a 1GB limit. NetWitness also provides a more detailed protocol analysis, which makes it more suitable for packet analysis.

2. What is the significance of the TCP three-way handshake for applications that utilize TCP as transport protocol?
   It ensures the devices can communicate before sending packets.

3. How many different source IP host addresses did you capture in your protocol captures?
   8

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?
   10 protocols.The Statistics > Protocol Hierarchy function in Wireshark shows a breakdown of protocol types on the LAN.

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?
   To find packet size counts in Wireshark, go to Statistics > Packet Length > Packet Length w/filter window. Yes, you can look at the Packet Length and Count columns to find packet counts and sizes. This can be used to determine what a usual load on the network looks like.

6. Why is it important to use protocol capture tools and protocol analyzers as an information systems security professional?
   So you can monitor protocol and packet traffic that are on the LAN, and also any traffic trying to get into the LAN. This is important to make sure company and security policy is being followed and that the network is not compromised or faulty.

7. What are some challenges to baseline analysis?
   Simplifying the data for better analysis, dealing with large packet-capture files, and working with mulitple tools to monitor and analyze the network.

8. Why would an information systems security practitioner want to see network traffic on both internal and external network traffic?
   Monitoring outside network traffic allows you to see who and what is trying to get into your network. Monitoring internal traffic lets you see which hosts might be compromised and what IP addresses internal employees are accessing.

9. Which transactions in the lab used TCP as a transport protocol? Which used UDP? Which ports were used in the lab?
   TCP: Putty for ssh and ssh sessions
   UDP: TFTP for the tftpd64 application
   Ports used: 21, 22, 23, 69, 80, 138, 54598, 9711, 309, and 56680