Lab #10 – Assessment Worksheet

Securing the Network with an Intrusion Detection System (IDS)

Course Name and Number: ____

Student Name: ____

Instructor Name: ____

Lab Due Date: ____

Overview

In this lab, you configured Snort, an open source intrusion prevention and detection system, on the TargetSnort virtual machine, and the Web-based IDS monitoring tool called Snorby. You also used the OpenVAS scanning tool to scan the TargetSnort virtual machine to test the Snort configuration and see exactly what circumstances trigger an IDS alert.

Lab Assessment Questions & Answers

1. What is the difference between an IDS and an IPS?

2. Why is it important to perform a network traffic baseline definition analysis?

3. Why is a port scan detected from the same IP on a subnet an alarming alert to receive from your IDS?

4. If the Snort IDS captures the IP packets off the LAN segment for examination, is this an example of promiscuous mode operation? Are these packets saved or logged?

5. What is the difference between a host-based IDS and a network-based IDS?

6. How can you block attackers, who are performing reconnaissance and probing, with Nmap and OpenVAS port scanning and vulnerability assessment scanning tools?

7. Why is it a good idea to have host-based intrusion detection systems enabled on critical servers and workstations?

8. Where should you implement intrusion prevention systems in your IT infrastructure?