Assessment Worksheet

Performing Reconnaissance and Probing Using Common Tools

Course and Section:

Student Name:

Lab Due Date:

Overview

In this lab, you explored the common tools available in the virtual lab environment. You used Wireshark to capture and analyze network traffic and OpenVAS to scan the network. You reviewed a sample collection of data using NetWitness Investigator, connected to a remote Windows machine, and explored two file transfer applications, FileZilla and Tftpd64. You used PuTTY to connect to a Linux machine and ran several Cisco commands to display statistics for the network interfaces. Finally, you used Zenmap to perform a scan of the network and created a network topology chart.

Lab Assessment Questions & Answers

- Name at least five applications and tools used in the lab.
  - Wireshark
  - Command Prompt
  - NetWitness Investigator
  - OpenVas
  - Windows Remote Desktop
  - tftpd64
  - PuTTY
- What is promiscuous mode?
  - Promiscuous mode captures a wider variety of packets within the same LAN. In essence, non-promscuous only captures packets destined to and from your workstation, while promiscuous sniffs the network as a whole.
- How does Wireshark differ from NetWitness Investigator?

    - Wireshark is a much lower-level view of network traffic, but NetWitness provides a more clear overall picture that is easily comparable between it and an older scan. The instructions note that this is important for detecting problems that have arisen.

- Why is it important to select the student interface in the Wireshark?
    - The student interface shows less data, while the public interface shows a large amount of TCP packets, and would be a burden to use for this assignment.

- What is the command line syntax for running an Intense Scan with Zenmap on a target subnet of 172.30.0.0/24?
    - nmap - T4 -A -v 172.30.0.0/24

- Name at least five different scans that may be performed with Zenmap.
    - Intense Scan
    - Intense Scan plus UDP
    - Intense Scan, all TCP ports
    - Intense Scan, no ping
    - Ping Scan

- How many different tests (i.e., scripts) did your Intense Scan perform?
    - 110 scripts

- Based on your interpretation of the Intense Scan, describe the purpose/results of each tests script performed during the report.
    - The intense scan intially checks for open ports, and checks network devices for open ports as well. Ater that it checks for services, and attempts to identify the operating system on each device. Finally, for each device it attempts to identify the services for each port on a given host.

- How many total IP hosts did Zenmap find on the network?
    - 5, including localhost