Lab #4 – Assessment Worksheet

Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you performed all five phases of ethical hacking: reconnaissance (using Zenmap GUI for Nmap), scanning (using OpenVAS), enumeration (exploring the vulnerabilities identified by OpenVAS), compromise (attack and exploit the known vulnerabilities) using the Metasploit Framework application), and conducted post-attack activities by recommending specific countermeasures for remediating the vulnerabilities and eliminating the possible exploits.

Lab Assessment Questions & Answers

1. What are the five steps of ethical hacking?

2. During the reconnaissance step of the attack, what open ports were discovered by Zenmap? What services were running on those ports?

3. What step in the hacking attack process uses Zenmap?

4. What step in the hacking attack process identifies known vulnerabilities?

5. During the vulnerability scan, you identified a vulnerable service in the Linux victim system. What was the name of the vulnerable service?

6. If you are a member of a security penetration testing team, and you identify vulnerabilities and exploits, should you obtain written permission from the owners prior to compromising and exploiting the known vulnerability?