Lab #2 – Assessment Worksheet

Performing a Vulnerability Assessment

Course Name and Number: IA 5010

Student Name: Yifan Zhang

Instructor Name: Themis Papageorge

Lab Due Date: 24/09/2015

Overview

In this lab, you used Nmap commands within the Zenmap application to scan the virtual network and identify the devices on the network and the operating systems and services running on them. You also used OpenVAS to conduct a vulnerability assessment and record the high risk vulnerabilities identified by the tool. Finally, you used the information you gathered from the report to discover mitigations for those risks and make mitigation recommendations based on your findings.

Lab Assessment Questions & Answers

1. What is Zenmap typically used for? How is it related to Nmap? Describe a scenario in which you would use this type of application.

   Zenmap typically used in assess vulnerability of a system. It is the user friendly graphic interface of Nmap which encapsulates many Nmap commands. Usually, we apply this software at the scanning and vulnerability phase of hacking process, paticularly in scanning part. It always used with OpenVAS together.

2. Which application can be used to perform a vulnerability assessment scan in the reconnaissance phase of the ethical hacking process?

   openVAS is used to perform a vulnerability scan work.

3. What must you obtain before you begin the ethical hacking process or penetration test on a live production network, even before performing the reconnaissance step?

   Before we start our ethical hacking, we need to be authorized by our client first which means that we need to be allowed to enter their system legally. At the same time we need to sign up some documents like (SLA) which defines the scop and responsibility of his hacking activity.

4. What is a CVE listing? Who hosts and who sponsors the CVE database listing Web site?

   CVE means Common Vulnerability Exposures and CVE listing is the lists of those vulnerabilities that are open to public. The host is the Mitre Corporation and the two sponsors are Department of Homeland Security and the the U.S. National Cyber Security Division.

5. Can Zenmap detect which operating systems are present on IP servers and workstations? Which option includes that scan?

   Zenmap could detect the operating systems. Nmap -sV can be used to judge which OS it is through judging which services it is available and Nmap -O can be used to guess what kind of OS probably is but less accuracy than option -sV.

6. How can you limit the breadth and scope of a vulnerability scan?

   For openVAS, we can import an .txt file which contains the particular hosts' IP that we want to scan and also we can specify the scan intensity. For Zenmap, we can use "--exclude" option of nmap to exempt those IP hosts that we don't want to scan. Also, we can choose different intensity to scan such as ping scan etc.

7. Once a vulnerability has been identified by OpenVAS, where would you check for more information regarding the identified vulnerability, exploits, and any risk mitigation solution?

   If a vulnerability was found by OpenVAS, we can go to National Vulnerability Database Https://web.nvd.nist.gov/view/vuln/search) and search the case number of this vulnerability(CVE number). Besides, in OpenVAS's report we also could find references which contains more information about the CVE

8. What is the major difference between Zenmap and OpenVAS?

   Zenmap help us to know about the overall network environment because it offers us rich and powerful scripts to monitor things like ports/hosts, operating systems, protocols etc. However, OpenVAS provide us with a powerful analytical abilities on assessment of vulnerabilities within the existing network.

9. Why do you need to run both tools like Zenmap and OpenVAS to complete the reconnaissance phase of the ethical hacking process?

   Firstly we need use Zenmap to see some potential weakness of the existing network systems. For instance, we need to know that which port/hosts are open to attackers and which kind of services runs and what operation system probably is used. Then, we use OpenVAS to scan these IP address which could tell us what kind of vulnerability that the attackers could exploit and how to mitigate the vulnerability etc.