Lab #5 Identifying Risks, Threats, and Vulnerabilities in an IT Infrastructure Using Zenmap® GUI (Nmap) and Nessus® Reports

Introduction

Imagine a system administrator learns of a server's vulnerability, and a service patch is available to solve it. Unfortunately, simply applying a patch to a server is not assurance enough that a risk has been mitigated. The system admin has the option of opening the application and verifying that the patch has raised the version number as expected. Still, the admin has no guarantee the vulnerability is closed, at least not until the vulnerability is directly tested. That's what vulnerability scanners are for.

Two vulnerability scanners available to the system administrator are Nmap® and Nessus®, which produce scan reports. The purpose of using Zenmap® GUI (Nmap) and Nessus® reports is to enable you to create network discovery port scanning reports and vulnerability reports. These reports can identify the hosts, operating systems, services, applications, and open ports that are at risk in an organization.

In this lab, you will look at an Nmap® report and a Nessus® report. You will visit the *http://cve.mitre.org* Web site, you will define vulnerability and exposure according to the site, and you will learn how to conduct searches of the Common Vulnerabilities and Exposures (CVE) listing.

Learning Objectives

Upon completing this lab, you will be able to:

- Review a Zenmap® GUI (Nmap) network discovery and port scanning report and a Nessus® software vulnerability report.
- Identify hosts, operating systems, services, applications, and open ports on devices from the Zenmap® GUI (Nmap) scan report.
- Identify critical, major, and minor software vulnerabilities from the Nessus® vulnerability assessment scan report.
- Visit the Common Vulnerabilities and Exposures (CVE) online listing of software vulnerabilities at *http://cve.mitre.org* and learn how to conduct searches on the site.

Hands-On Steps

▶Note:
This is a paper-based lab. To successfully complete the deliverables for this lab, you will need access to Microsoft® Word or another compatible word processor. For some labs, you may also need access to a graphics line drawing application, such as Visio or PowerPoint. Refer to the Preface of this manual for information on creating the lab deliverable files.

1. On your local computer, **create the lab deliverable files**.
2. **Review the Lab Assessment Worksheet**. You will find answers to these questions as you proceed through the lab steps.
3. **Review the Lab 5 Nmap Scan Report** that accompanies this lab.
4. In your Lab Report file, using the Lab 5 Nmap Scan Report, **answer the following questions:**
   - What are the date and timestamp of the Nmap host scan?
   - What is the total number of loaded scripts for scanning?
   - A synchronize packet (SYN) stealth scan discovers all open ports on the targeted host. How many ports are open on the targeted host for the SYN stealth scan at 13:36?
   - Identify hosts, operating systems, services, applications, and open ports on devices from the Zenmap GUI (Nmap) scan report.

Why Nmap Became Popular

Nmap started more than 15 years ago as a simple, command-line tool. Its one purpose—to send crafted packets to a targeted Internet Protocol (IP) address to determine what ports are listening for connections. Knowing what specific ports are listening, the Nmap operator can infer what services are running.

For example, if Transmission Control Protocol (TCP) port 80 is open and listening, it's a safe assumption the target machine is a Web server, running the Hypertext Transfer Protocol (HTTP) service on port 80. Other popular ports such as 21, 25, 137, and 161 mean the services File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Network Basic Input/Output System (NetBIOS), and Simple Network Management Protocol (SNMP) are listening, respectively. This made Nmap very popular with administrators who could then monitor and verify their systems' services.

Nmap also became very popular as an easy tool for reconnaissance. With malicious intent, a person armed with knowing what services were running could research what vulnerabilities to exploit. The fast scanning Nmap made locating the recently discovered exploits called zero-day exploits very efficient.

Over the past 15 years, the features available in Nmap have multiplied several times. The ability to craft packets down to specific flags and options can make troubleshooting—and disrupting—networked devices almost limitless. The people and companies tasked with protecting against hackers must play a game of cat and mouse against the growing set of options in tools such as Nmap. Innovation and open source allows this game to be played indefinitely.

5. **Review** the **Lab 5 Nessus Vulnerability Scan Report** that accompanies this lab.

6. In your Lab Report file, using the **Lab 5 Nessus Vulnerability Scan Report**, **answer** the following questions:

   - How many hosts were scanned?
   - What were the start and end times for each of the scans?
   - How many total vulnerabilities were discovered for each host?
   - How many of the vulnerabilities were critical, major, and minor software vulnerabilities?

▶Note:
Nessus is a powerful vulnerability scanner, with a fast-growing list of available plug-ins. As a vulnerability scanner, the tool scans the networked devices for potential weaknesses and exploitable services. As you see from the lab sample, reporting can be detailed and customized. While still free for personal, home use, Nessus is also available for commercial use with an annual subscription fee.

Nessus can be installed and run fairly easily, but here are a few tips that will produce much more benefit. First, update the plug-ins on install. By default, Nessus will update plug-ins once a day. Another tip is to use Nessus as a compliance tool. While it is by nature a vulnerability tool, one Nessus feature is to load a configuration file (called an audit file by Nessus) and then scan with Nessus to verify compliance against your end devices.

7. On your local computer, **open** a new **Internet browser window**.

8. In the address box of your Internet browser, **type** the URL **http://cve.mitre.org** and **press Enter** to open the Web site.

9. On the Web site, toward the top left of the screen, **click** the **CVE List link**.

10. **Review** the **CVE List Main Page**.

11. In your Lab Report file, **define CVE**.

12. On the right, under **Items of Interest**, **click** the **Terminology link**.

13. **Review** the definitions for **vulnerability** and **exposure**.

14. In your Lab Report file, **define** the terms **vulnerability** and **exposure**.

15. At the top right of the Web site, **click** the **Search link**.

16. In the Search box, **type** the words **Microsoft® XP 2003 Service Pack 1** and **click the Search button**.
17. In your Lab Report file, **describe** some of the results you discover.
18. After viewing the results, **conduct** another search and this time, **type** the words **Cisco ASA 5505 Security +** and **click the Search button**.
19. In your Lab Report file, **describe** some of the search results.

▶Note:
This completes the lab. Close the **Web browser**, if you have not already done so.

Lab #5 - Assessment Worksheet

Identifying Risks, Threats, and Vulnerabilities in an IT Infrastructure Using Zenmap® GUI (Nmap) and Nessus® Reports

Course Name and Number: _____

Student Name: _____

Instructor Name: _____

Lab Due Date: _____

Overview

In this lab, you looked at an Nmap® report and a Nessus® report. You visited the *http://cve.mitre.org* Web site, you defined vulnerability and exposure according to the site, and you learned how to conduct searches of the Common Vulnerabilities and Exposures (CVE) listing.

Lab Assessment Questions & Answers

1. Describe the purpose of a Zenmap® GUI (Nmap) report and Nessus® report?

2. Review the Lab 5 Nmap Scan Report. On page 6, what ports and services are enabled on the Cisco Adaptive Security Appliance device?

3. Review the Lab 5 Nmap Scan Report. On page 6, what is the source IP address of the Cisco Adaptive Security Appliance device?

4. How many IP hosts were identified in the Lab 5 Nessus Vulnerability Scan Report? List them.

5. When you identify a known software vulnerability, where can you go to assess the risk impact of the software vulnerability?

6. Define CVE.

7. Explain how the CVE search listing can be a tool for security practitioners and a tool for hackers.