Lab #5: Identify Threats & Vulnerabilities in an IT Infrastructure

Course Name: Risk Management in Information Systems (IAA202)
Student Name: Nguyễn Trần Vinh – SE160258
Instructor Name: Mai Hoàng Đỉnh
Lab Due Date: 18/2/2023

Part A: How to Identify Risks, Threats & Vulnerabilities in an IT Infrastructure Using ZeNmap GUI (Nmap) & Nessus® Reports

Learning Objectives and Outcomes

Upon completing this lab, students will be able to:

- Review a ZeNmap GUI (Nmap) network discovery and port scanning report and a Nessus® software vulnerability report from a risk management perspective
- Identify hosts, operating systems, services, applications, and open ports on devices from the ZeNmap GUI (Nmap) scan report from a risk management perspective
- Identify critical, major, and minor software vulnerabilities from the Nessus® vulnerability assessment scan report
- Assess the exploit potential of the identified software vulnerabilities by conducting a high-level risk impact by visiting the Common Vulnerabilities & Exposures (CVE) online listing of software vulnerabilities at http://cve.mitre.org/
- Craft an executive summary prioritizing the identified critical and major threats and vulnerabilities and their risk impact on the IT organization

Overview

One of the most important first steps to risk management and implementing a security strategy is to identify all resources and hosts within the IT infrastructure. Once you identify the workstations and servers, you now must then find the threats and vulnerabilities found on these workstations and servers. Servers that support mission critical applications require security operations and management procedures to ensure C-I-A throughout. Servers that house customer privacy data or intellectual property require additional security controls to ensure the C-I-A of that data. This lab requires the students to identify threats and vulnerabilities found within the Workstation, LAN, and Systems/Applications Domains.

Lab Assessment Questions

1. What are the differences between ZeNmap GUI (Nmap) and Nessus?

Nmap	Nessus
Nmap is used for host detection and it is a port discovery tool so that it discovers active hosts on the network, also detects the version of the database system running on our server and operating system too.	Whereas, Nessus is the first vulnerability scanner used to discover the weakness of the system.

As Nmap is a port scanner that discovers the active host by network scanning once it is done Nmap gathers information about the open ports.	Whereas, Nessus is known for a vulnerability scanner which scans ports like Nmap and looks only for the specific weakness of the system against a known host.
Nmap is a better performing network that discovering an IP network infrastructure.	Whereas, Nessus is better performing software which refers to check the inability of the system.
Nmap can protect your system network from intruders.	Nessus does not actively prevent attacks, it is only a tool that checks weaknesses and helps to find the issue.
The available platform for Nmap is Windows and Unix variants operating systems.	Nessus is supported on the platform of Windows, Linux, Mac, Unix.
Nmap is a standard security tool that protects from cyber attacks.	Whereas, Nessus is not a complete security solution but only has a small part of a good security strategy.
Many free operating systems come with Nmap packages, they may not be installed we need to upgrade that with the latest version.	Nessus is typically installed on servers and runs as a web-based application.
Nmap can be used to monitor a single host as well as a vast network.	The Nessus having scans that allow users to specify which machines they want to scanned.
Nmap is open-source; it has a scripting engine that allows users to create complex Nmap scripts. The list of Nmap scripts founded on Nmap's site.	Plugins are used to determine the vulnerability is present on a specified machine. There are 34000 plugins available in Nessus.
Nmap is free to download under GPL.	It is not free for a long time and the cost of Nessus depends on who is using it. If you are using it for home then it has a "home feed" subscription and professional having other subscription plans at different prices.
Nmap can be used by hackers to get access to the uncontrolled part of the system. Hackers are not the only people who use the software platform.	Whereas Nessus is a security scanning tool that remotely scans a computer and if any malicious hackers use it to gain access to the network system the system gets alert.

2. Which scanning application is better for performing a network discovery reconnaissance probing ofan IP network infrastructure?
Answer: Nmap.

3. Which scanning application is better for performing a software vulnerability assessment withsuggested remediation steps?
Answer: Nessus.

4. How many total scripts (i.e., test scans) does the Intense Scan using ZenMap GUI perform?
Answer: There are 36 scripts loaded for scanning.

5. From the ZenMap GUI pdf report page 6, what ports and services are enabled on the Cisco SecurityAppliance device?
Answer: Port 443 and ssl/http service are enabled on the Cisco Security Appliance device.

6. What is the source IP address of the Cisco Security Appli-ance device (refer to page 6 of the pdfreport)?
Answer: The IP address is 172.30.0.1

7. How many IP hosts were identified in the Nessus® vulnerability scan? List them.
Answer: 7 IP hosts, include:

- 172.16.20.1
- 172.17.20.1
- 172.18.20.1
- 172.19.20.1
- 172.20.20.1
- 172.30.0.10
- 172.30.0.66

8. While Nessus provides suggestions for remediation steps, what else does Nessus provide that can helpyou assess the risk impact of the identified software vulnerability?
Answer: Beside remediation steps, Nessus also provides devices and software on the network that is not authorized or indicate a network compromise.

9. Are open ports necessarily a risk? Why or why not?
Answer: Of course, open ports are a risk, because the attacker can use these ports to exploit the vulnerabilities such as using Trojan to make a screenshot and then send a screenshot back to the attacker.

10. When you identify the known software vulnerability, where can you go to assess the risk impact of thesoftware vulnerability?
Answer: Common Vulnerability Scoring System (CVSS).

11. If Nessus provides a pointer in the vulnerability assessment scan report to look up CVE-2009-3555 when using the CVE search listing, specify what this CVE is, what the potential exploits are, and assess the severity of the vulnerability.
Answer: CVE is a list of information security vulnerabilities and exposures that provides common names for publicity of known problems. CVE also helps to share data across separate vulnerability capabilities easily.

12. Explain how the CVE search listing can be a tool for security practitioners and a tool for hackers.
Answer: The CVE search listing can be a useful tool for both security practitioners and hackers since it helps practitioners and hackers know what programs they can use and what they cannot to secure or hack the systems.

13. What must an IT organization do to ensure that software updates and security patches areimplemented timely?
Answer: An IT organization should establish a patch management plan which evaluates the criticality and applicability of the software patch.

14. What would you define in a vulnerability management policy for an organization?
Answer: A vulnerability management policy should have defined timelines for how long an administrator has to address vulnerability on a system.

15. Which tool should be used first if performing an ethical hacking penetration test and why?
Answer: Nmap is the one that should be used when performing an ethical hacking penetration test. Because it is a powerful port scanner and auditing utility. Besides that it is an open source application and can run on many different operating systems such as Windows, Linux, Mac OS.