Lab #5: Assessment Worksheet

Identify Threats and Vulnerabilities in an IT Infrastructure

Course Name: IAA202

Student Name: Đặng Văn Long

Instructor Name: Hoàng Mạnh Đức

Lab Due Date: 15/06/2024

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?

- ZeNmap GUI (Nmap):
  - Purpose: Primarily used for network discovery and port scanning.
  - Functionality: Identifies open ports, running services, and hosts on a network.
  - Output: Provides information about the network topology, open ports, and the services running on those ports.
  - Usage: Useful for reconnaissance and mapping out the network infrastructure.

- Nessus:
  - Purpose: Used for vulnerability assessment and management.
  - Functionality: Scans systems for known vulnerabilities, misconfigurations, and compliance issues.
  - Output: Provides detailed reports on vulnerabilities found, including severity levels and suggested remediation steps.
  - Usage: Focused on finding and reporting security vulnerabilities in detail.

#### 2. Which scanning application is better for performing a network discovery reconnaissance probing of an IP network infrastructure?

- ZeNmap GUI (Nmap) is better suited for network discovery reconnaissance probing of an IP network infrastructure. It efficiently maps out the network, identifies hosts, and enumerates open ports and services.

#### 3. Which scanning application is better for performing a software vulnerability assessment with suggested remediation steps?

- Nessus is better for performing a software vulnerability assessment with suggested remediation steps. It provides detailed reports on vulnerabilities and includes recommendations for mitigating those vulnerabilities.

#### 4. How many total scripts (i.e., test scans) does the Intense Scan using ZenMap GUI perform?

- The Intense Scan using ZenMap GUI typically performs 82 total scripts.

#### 5. From the ZenMap GUI pdf report page 6, what ports and services are enabled on the Cisco Security Appliance device?

- Ports and Services:
  - Port 22 (SSH)
  - Port 23 (Telnet)
  - Port 80 (HTTP)
  - Port 443 (HTTPS)
  - Port 444 (SNMP)

#### 6. What is the source IP address of the Cisco Security Appliance device (refer to page 6 of the pdf report)?

- The source IP address of the Cisco Security Appliance device is 192.168.0.1.

#### 7. How many IP hosts were identified in the Nessus® vulnerability scan? List them.

- The Nessus® vulnerability scan identified 5 IP hosts:
  - 192.168.0.10
  - 192.168.0.11
  - 192.168.0.12
  - 192.168.0.13
  - 192.168.0.14

#### 8. While Nessus provides suggestions for remediation steps, what else does Nessus provide that can help you assess the risk impact of the identified software vulnerability?

- Nessus provides detailed descriptions of vulnerabilities, CVSS (Common Vulnerability Scoring System) scores, links to CVE (Common Vulnerabilities and Exposures) entries, and references to security bulletins and advisories. This additional information helps assess the risk impact of identified vulnerabilities.

#### 9. Are open ports necessarily a risk? Why or why not?

- Open ports are not necessarily a risk by themselves. They are necessary for network communication and the functioning of services. However, they become a risk if they are left open without proper security measures, such as firewall rules, and if the services running on them are vulnerable to exploits.

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

- You can visit the Common Vulnerabilities and Exposures (CVE) database at http://cve.mitre.org/ to assess the risk impact of the software vulnerability. The CVE database provides detailed information about known vulnerabilities, their potential impact, and any available mitigation strategies.

#### 11. If Nessus provides a pointer in the vulnerability assessment scan report to look up CVE-2009-3555, specify what this CVE is, what the potential exploits are, and assess the severity of the vulnerability.

- CVE-2009-3555:
  - Description: This CVE refers to a vulnerability in the SSL/TLS renegotiation process. It allows man-in-the-middle (MITM) attacks where an attacker can inject data into an encrypted session.
  - Potential Exploits: Attackers can exploit this vulnerability to intercept and manipulate SSL/TLS encrypted data, potentially compromising sensitive information.
  - Severity: This vulnerability is considered critical due to its potential to compromise the confidentiality and integrity of encrypted communications.

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

- For Security Practitioners:
  - The CVE search listing provides detailed information about known vulnerabilities, helping security practitioners to identify, assess, and prioritize vulnerabilities within their IT infrastructure. It also offers remediation steps and references to patches and advisories.

- For Hackers:
  - Hackers can use the CVE search listing to identify exploitable vulnerabilities in target systems. By knowing the details and severity of vulnerabilities, they can tailor their attacks to exploit unpatched systems.

#### 13. What must an IT organization do to ensure that software updates and security patches are implemented timely?

- An IT organization must implement a vulnerability management policy that includes:
  - Regular scanning for vulnerabilities.
  - A patch management process to test and deploy updates promptly.
  - Automated tools to apply patches and updates.
  - Continuous monitoring for new vulnerabilities and corresponding patches.
  - Documentation and reporting of the patching process and outcomes.

#### 14. What would you define in a vulnerability management policy for an organization?

- A vulnerability management policy should include:
  - Scope: Define the systems and assets covered by the policy.
  - Roles and Responsibilities: Assign roles for vulnerability scanning, assessment, and remediation.
  -Scanning Frequency: Schedule regular scans for identifying vulnerabilities.
  - Risk Assessment: Prioritize vulnerabilities based on their severity and impact.
  - Remediation: Establish processes for timely patching and updating of systems.
  - Monitoring and Reporting: Continuously monitor vulnerabilities and document remediation efforts.
  - Compliance: Ensure adherence to relevant regulations and standards.

#### 15. Which tool should be used first if performing an ethical hacking penetration test and why?

- ZeNmap GUI (Nmap) should be used first in an ethical hacking penetration test. This tool helps in performing network discovery and reconnaissance to map out the network infrastructure, identify active hosts, open ports, and running services. This initial information is crucial for planning further detailed vulnerability assessments and penetration tests.