Basic Vulnerability Assessment On A Virtual Machine

Project Overview:

- In this project, the intern will learn and apply basic cybersecurity concepts by conducting a vulnerability assessment on a given Virtual Machine (VM) or network.
- The intern will use industry-standard tools such as Nmap and Nessus to identify potential vulnerabilities.
- After identifying these vulnerabilities, the intern will analyze the findings and generate a comprehensive report summarizing the findings, including recommendations for mitigating the identified risks.

Project Objectives:

1.Understand Vulnerability Assessment:

- Learn the fundamentals of vulnerability assessments, including the purpose and importance in cybersecurity.
  - Gain knowledge of various types of vulnerabilities(e.g.)misconfiguratio, outdated software, weak password.

2. Hands-on Experience with Security Tools:

1. Install and configure Nmap and Nessus on the provided VM.

2. Use Nmap to perform network scanning and enumeration.

3. Use Nessus to conduct a more in-depth vulnerability scan.

4. Understand the output of both tools and how to interpret the results.

3. Identify and Analyze Vulnerabilities:

1. Identify vulnerabilities within the target VM or network based on the scan results.

2.Analyze the severity of each vulnerability and its potential impact on the system.

4.Report Generation and Documentation:

1.Generate a detailed report summarizing the vulnerabilities identified.

2.Provide recommendations for mitigating each identified vulnerability.

3.Include a brief overview of the tools used and the methodology followed.

5.Presentation of Findings:

1. Present the findings and recommendations to a supervisor or a small team.

2.Explain the steps taken during the assessment and justify the mitigation strategies proposed.

Project Deliverables:

1.Vulnerability Assessment Report:

1. A comprehensive report detailing the vulnerabilities identified, their severity, and recommended mitigations.

2.Sections of the report should include:

- Executive Summary
- Methodology
- Tools Used (Nmap, Nessus)
- Detailed Findings (including screenshots)
- Recommendations for Mitigation

- Conclusion

2.Presentation:

- A PowerPoint or similar presentation summarizing the findings and recommendations.

- The presentation should be concise, clear, and aimed at a non-technical audience.

3. Technical Documentation:

- Documentation of the steps followed during the assessment, including installation and configuration of the tools.

Skills Required:

- Basic understanding of networking concepts (IP addresses, ports, protocols).

- Familiarity with Linux/Windows command line interfaces.

- Basic knowledge of cybersecurity concepts.

Learning Outcomes:

- Gain hands-on experience in vulnerability assessment.

- Develop analytical skills by interpreting scan results and assessing the impact of vulnerabilities.

- Enhance communication skills by preparing technical documentation and delivering presentations.

Duration:

- 4-6 weeks, depending on the intern's familiarity with the tools and the depth of the assessment required.

Mentorship and Support:

- The intern will be assigned a mentor who will provide guidance throughout the project, including initial setup, troubleshooting, and review of the final deliverables.

Tools and Resources:

- Virtual Machine (pre-configured with vulnerable software/services).
- Access to Nmap and Nessus (free version).
- Documentation and tutorials for Nmap and Nessus.

Evaluation Criteria:

- Completeness and accuracy of the vulnerability assessment.
- Quality and clarity of the report and presentation.
- Ability to provide actionable and effective mitigation strategies.
- Proactive problem-solving and troubleshooting throughout the project.

1. Executive Summary

- This report outlines the results of a basic vulnerability assessment conducted on a designated Virtual Machine (VM).
- The assessment was performed using Nmap and Nessus, two widely recognized tools in the field of cybersecurity.
- The purpose of this project was to identify potential vulnerabilities within the VM, assess their severity, and propose mitigation strategies to address the risks.

2. Project Overview

Objective:

- To conduct a vulnerability assessment on a VM using Nmap and Nessus, identify potential security risks, and recommend appropriate mitigation measures.

Tools Used:

Nmap:

- A network scanning tool used for discovering hosts and services on a computer network by sending packets and analyzing the responses.

Nessus:

- A vulnerability scanning tool used to identify security vulnerabilities on a system.

3. Methodology

The vulnerability assessment was conducted in several stages:

1.Network Scanning with Nmap:

- Purpose:
  To identify open ports, running services, and potential vulnerabilities on the target VM.
- Process:
  Conducted a network scan using Nmap to identify active services and open ports.
- Used different scan types such as TCP SYN scan and Service Version Detection.
- A list of open ports, identified services, and potential security issues.

2. Vulnerability Scanning with Nessus:

- Purpose: To perform an in-depth scan of the VM to detect known vulnerabilities.
- Process:

Installed and configured Nessus to scan the VM.

- Conducted a full system scan to identify vulnerabilities, including outdated software, weak passwords, and misconfigurations.
- Output:A detailed list of vulnerabilities categorized by severity (High, Medium, Low).

3. Analysis:

- Reviewed the scan results from both Nmap and Nessus.
- Prioritized vulnerabilities based on their potential impact on the system and the ease of exploitation.

4. Report Generation:

- Compiled the findings into a comprehensive report, detailing each vulnerability, its potential impact, and recommended mitigation strategies.

4. Findings

The following vulnerabilities were identified during the assessment:

1. Open Ports and Unsecured Services:

- **Finding:** Several open ports were identified, including ports used by services that were either outdated or configured insecurely.
- **Impact:**Open ports can be exploited by attackers to gain unauthorized access to the system.

- **Recommendation:**Close unnecessary ports and secure the services running on open ports by updating them to the latest versions and applying proper configurations.

2.Outdated Software:

- **Finding:** Several software applications running on the VM were found to be outdated, with known vulnerabilities.

- **Impact:** Outdated software can be a significant security risk, as attackers can exploit known vulnerabilities to compromise the system.

- **Recommendation:** Regularly update software to the latest versions to ensure that security patches are applied.

3. Weak Passwords:

- **Finding:** The Nessus scan revealed that some user accounts on the VM were using weak passwords.

- **Impact:** Weak passwords make it easier for attackers to gain unauthorized access through brute-force attacks.

- **Recommendation:** Implement strong password policies, requiring the use of complex passwords and regular password changes.

4. Misconfigurations:

- **Finding:** Certain services were found to be misconfigured, such as SSH allowing root login.

- **Impact:** Misconfigurations can lead to unauthorized access or escalation of privileges.

- **Recommendation:** Review and correct misconfigurations, such as disabling root login via SSH and restricting access to critical services.

5. Recommendations for Mitigation

Based on the findings, the following mitigation strategies are recommended:

1. Close Unnecessary Ports:

- Disable or block any open ports that are not required for the VM's operation.

2. Regular Software Updates:

- Implement a patch management process to ensure that all software is kept up to date.

3.Enforce Strong Password Policies:

- Require complex passwords and enable multi-factor authentication (MFA) where possible.

4. Review and Correct Configurations:

- Regularly review system configurations and apply best practices for securing services.

5. Continuous Monitoring:

- Implement continuous monitoring and regular vulnerability assessments to identify and mitigate new vulnerabilities as they arise.

Program :

```
Nmap scan report for 192.168.1.10

Host is up (0.0010s latency).

Not shown: 995 closed ports

PORT     STATE  SERVICE       VERSION

22/tcp   open   ssh          OpenSSH 7.4 (protocol 2.0)

80/tcp   open   http         Apache httpd 2.4.6 ((CentOS) PHP/7.2.24)

443/tcp  open   ssl/https

3306/tcp open   mysql        MySQL 5.7.29

3389/tcp open   ms-wbt-server Microsoft Terminal Services
```

6. Conclusion:

- The vulnerability assessment revealed several areas where the security of the VM could be improved.

- By addressing the identified vulnerabilities through the recommended mitigation strategies, the overall security posture of the system can be significantly enhanced.

- Continuous monitoring and regular assessments are essential to maintaining a secure environment.

7. Appendices:

Appendix A: Nmap Scan Results

Appendix B: Nessus Vulnerability Report

Appendix C: Configuration Files and Documentation

8. References:

Nmap Documentation: https://nmap.org/book/man.html

Nessus User Guide: https://www.tenable.com/products/nessus

OWASP Top Ten Security Risks: https://owasp.org/www-project-top-ten/

CONCLUSION:

- This report provides a clear and concise overview of the vulnerabilities identified in the VM, along with actionable recommendations for improving the system's security.
- The assessment demonstrates a practical understanding of basic cybersecurity principles and the use of industry-standard tools.