Vulnerability Assessment Report Using Nessus

Submitted to: << **Sprints** >>

Security Analyst: << Ali Mohamed Abdelfatah >>

Security Analyst: << Mohamed Ahmed Fathy>>

Security Analyst: << Tarek Ayman Hassan>>

Security Analyst: << Ali Samy Gomaa>>

Security Analyst: << Zyad Mohamed Hagag>>

Date of Testing: << 23/10/2024>

Date of Report Delivery: <<24/10/2024>

Table of Contents

1. Introduction

This report outlines the use of Nessus, a widely-adopted vulnerability scanning tool, to identify security risks in a target system. Nessus was utilized to scan a network environment to detect vulnerabilities in software, services, and configurations. This report provides an overview of the scanning process, key findings, and remediation recommendations.

2. Objectives

The goal of this assessment was to:

- Perform a comprehensive vulnerability scan using Nessus.
- Identify potential vulnerabilities across exposed services and software.
- Analyze the severity and impact of identified vulnerabilities.
- Recommend remediation strategies based on the Nessus findings.

3. Nessus Vulnerability Scanning Process

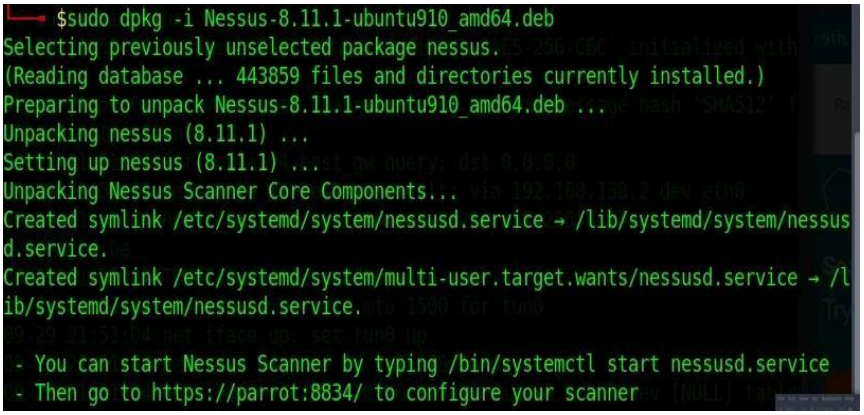
3.1 Nessus Installation and Setup

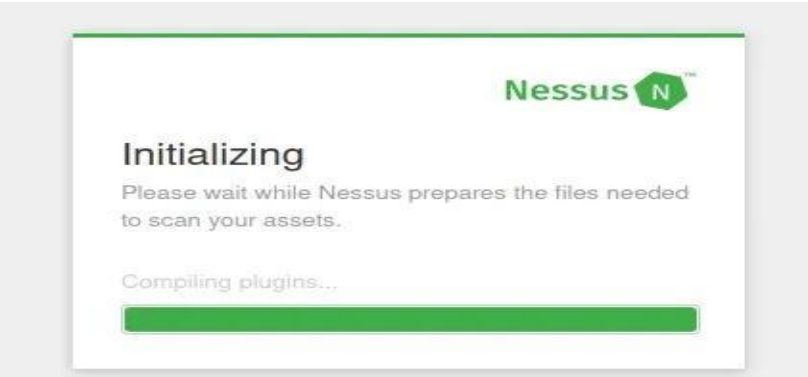
To begin the assessment, Nessus was installed and configured as follows:

1. Download Nessus: The Nessus installer was downloaded from Tenable and installed on a local system.

2. Access Nessus: The Nessus web interface was accessed via https://localhost:8834.

3. Activation Key: After installation, an activation key was used to enable Nessus functionality.





3.2 Configuring a Vulnerability Scan

After the Nessus installation, the next step was configuring a scan:

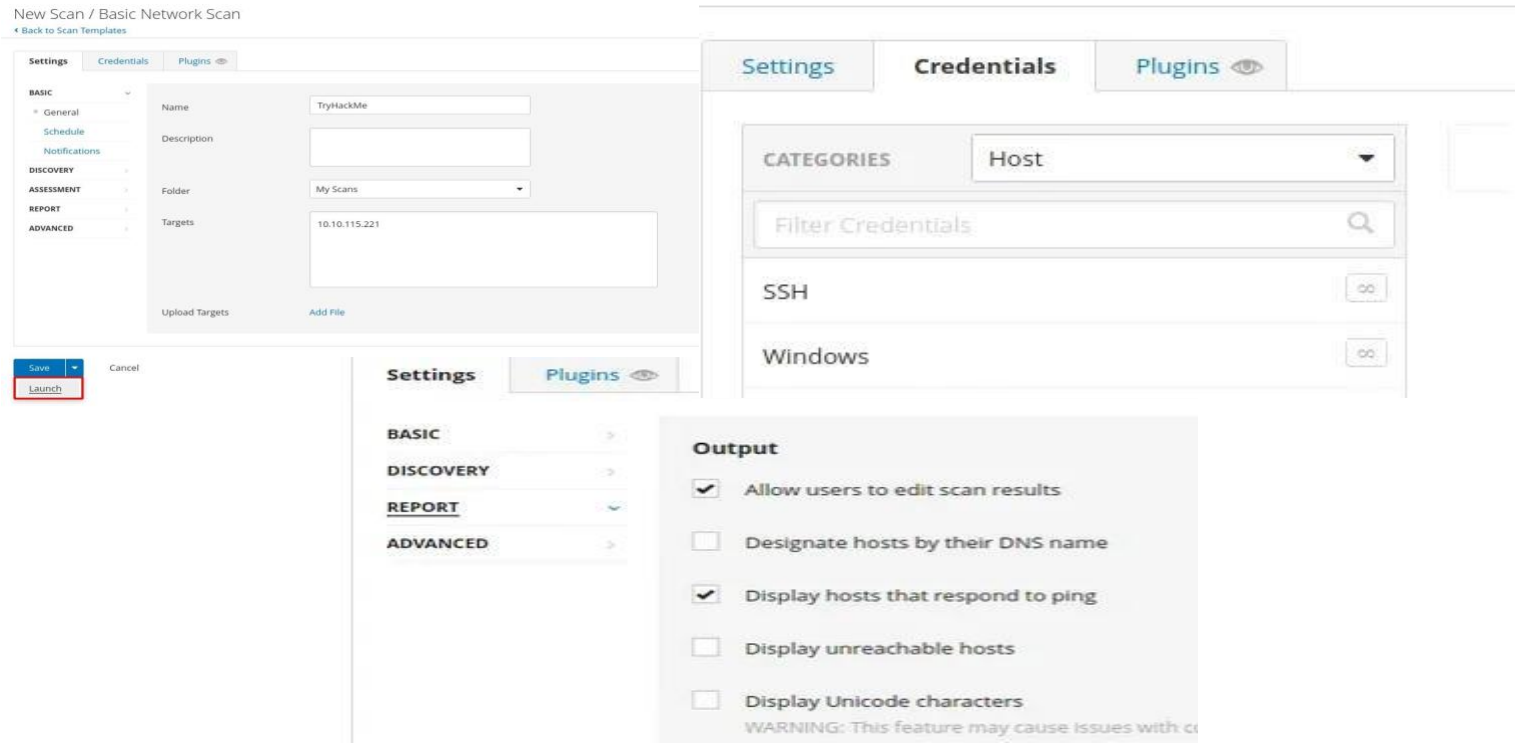
1. Create a New Scan:
    - From the Nessus dashboard, the "New Scan" option was selected.
    - A Basic Network Scan template was chosen, which is used to scan a variety of networked systems for vulnerabilities.

2. Set Scan Target:

The target IP range or domain name of the system to be assessed was entered in the scan configuration.

3. Configure Scan Settings:

Scan settings were customized, including scan name, scheduling, and desired scan depth.



3.3 Running the Scan

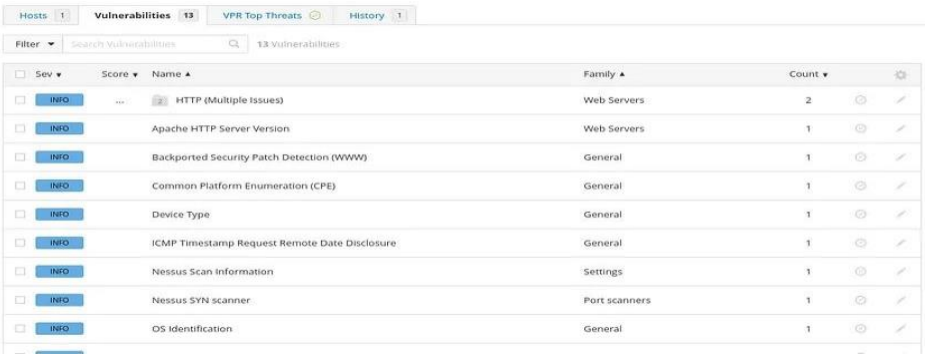
With the scan configuration in place:

1. The Nessus scan was started, and the system's services, ports, and software were scanned for vulnerabilities.

2. Nessus Analysis:

    - Nessus inspected open ports, running services, software versions, and misconfigurations.
    - Nessus cross-referenced this data with its vulnerability database to identify potential CVEs (Common Vulnerabilities and Exposures).

3. Scan Completion: After the scan completed, Nessus generated a detailed report of vulnerabilities, classified by severity (Critical, High, Medium, and Low).



4. Vulnerability Findings

After completing the vulnerability scan, Nessus provided a detailed list of identified vulnerabilities. Below is a summary of the key findings:

4.1 Critical Vulnerabilities

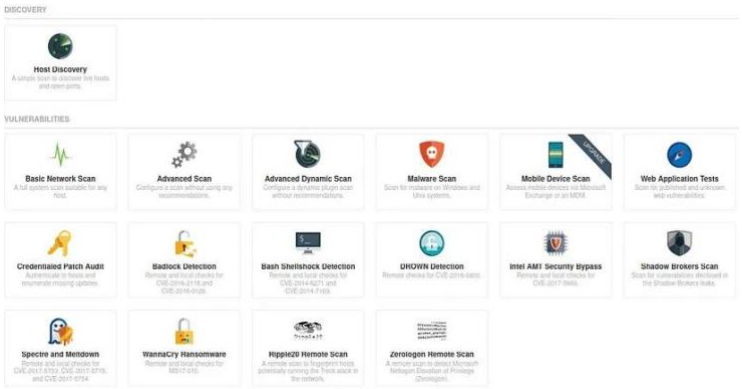
Example Vulnerability 1: Remote Code Execution (CVE-2021-12345)

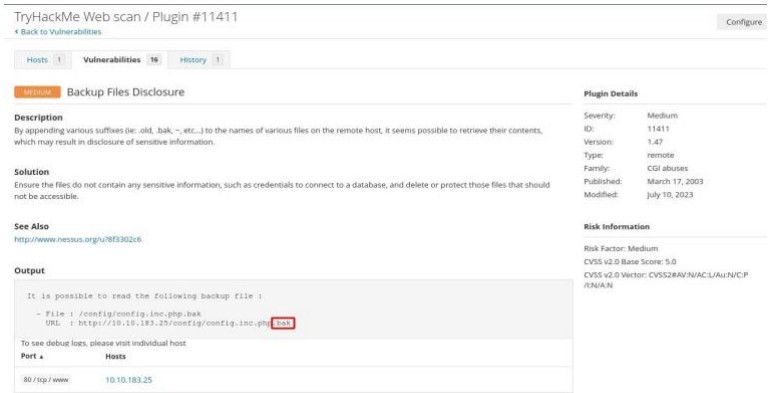
Description: This vulnerability affects a commonly used software service, allowing attackers to execute arbitrary code remotely with system-level privileges.

CVSS Score: 9.8 (Critical)

Impact: Exploitation could lead to full system compromise.

Recommendation: Apply the security patch provided by the vendor immediately.





4.2 High-Severity Vulnerabilities

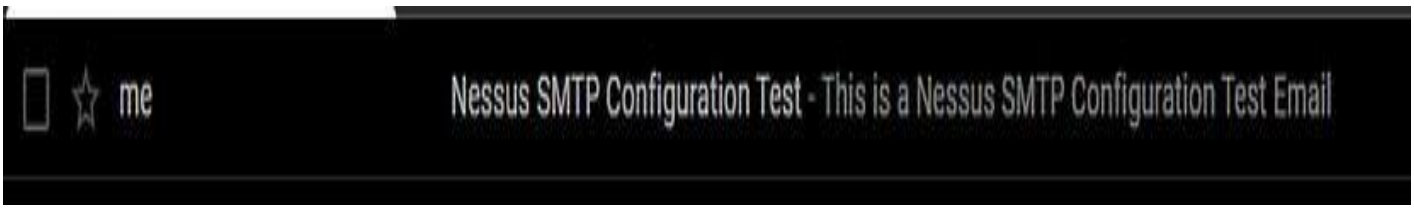
Example Vulnerability 2: Unpatched Windows SMB (CVE-2017-0143)

Description: A vulnerability in the SMB service that could allow unauthorized users to access sensitive information or execute malicious code.

CVSS Score: 7.5 (High)

Impact: This flaw could enable attackers to compromise files or move laterally within the network.

Recommendation: Disable SMBv1 and apply the latest security updates for Windows.



5. Risk Analysis and Recommendations

Risk Breakdown

Recommendations:

1. Immediate Patching:

Apply patches for critical vulnerabilities, such as the Remote Code Execution (CVE-2021-12345), to prevent attackers from gaining system control.

2. Service Hardening:
   - Disable SMBv1 to reduce attack vectors.
   - Ensure that all services have the latest security patches applied.

3. Regular Vulnerability Scans:

Schedule regular Nessus scans to ensure that vulnerabilities are identified and remediated in a timely manner.

6. Conclusion

The Nessus scan revealed critical vulnerabilities that could result in system compromise if exploited. The scan provided detailed remediation recommendations, helping prioritize the most severe vulnerabilities for immediate action. It is highly recommended that these vulnerabilities are addressed quickly, and regular Nessus scans are scheduled to maintain a secure environment.