Basic Vulnerability Assessment for a Small Business Network

Table of Contents

1. Executive Summary

This report presents the findings of a vulnerability assessment conducted on a simulated small business IT infrastructure using a Metasploitable 2 server. The assessment aimed to identify security gaps, prioritize risks, and provide mitigation strategies to enhance the overall security posture. The assessment revealed multiple vulnerabilities, with critical and high-risk issues requiring immediate attention.

2. Introduction

- **Purpose**: The purpose of this assessment is to simulate a real-world vulnerability assessment for a small business, identifying potential security risks and providing actionable recommendations.
- **Scope**: The assessment covers the following components of the IT infrastructure:
    - Metasploitable 2 server (acting as the vulnerable small business network).

Methodology: The assessment was conducted using Nessus, a widely used vulnerability scanning tool, to identify vulnerabilities within the Metasploitable 2 environment.

3. Assessment Overview

- **Business Description**: The simulated small business operates a basic IT infrastructure, including web services, databases, and user accounts, represented by the Metasploitable 2 server.

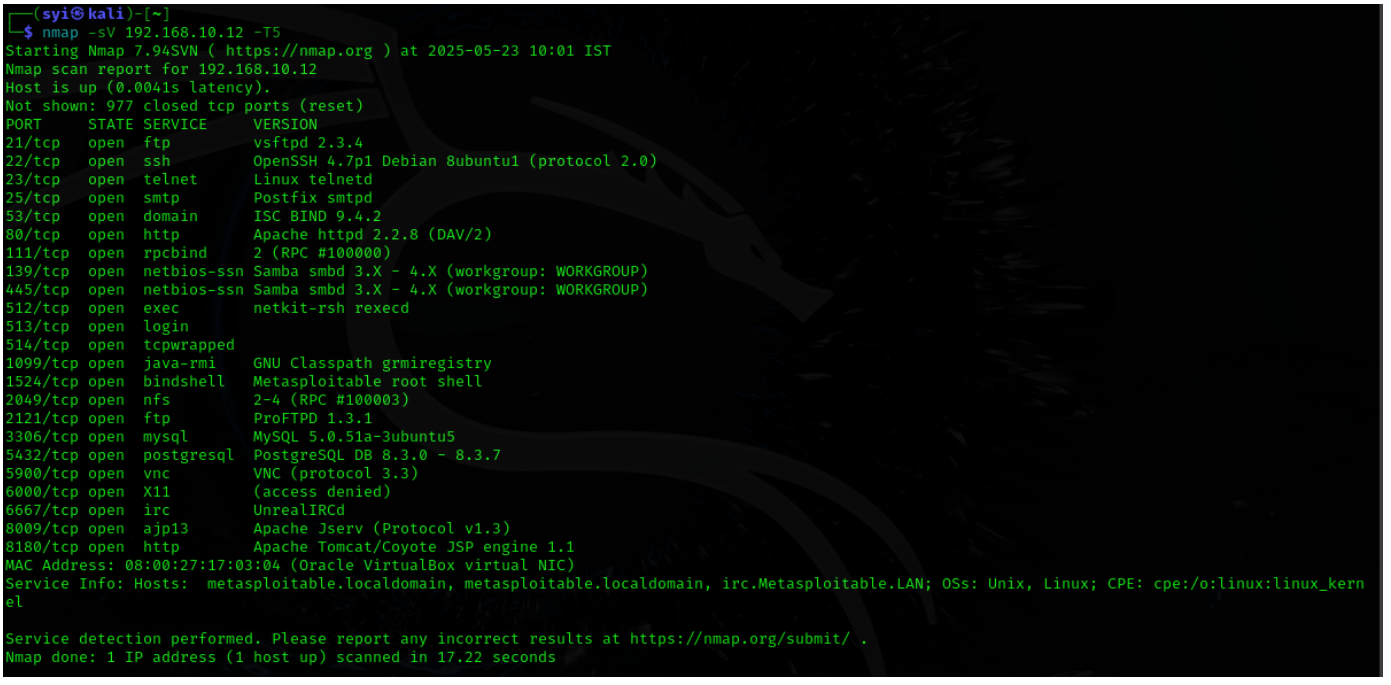
Tools Used: Nessus was utilized to perform the vulnerability scan, providing detailed reports on identified vulnerabilities.

Set up a virtual lab using VirtualBox

- Download and install VirtualBox
- Install Kali Linux as your primary OS for security testing (available from the official Kali website).
- Set up vulnerable machines like Metasploitable (a deliberately insecure Linux machine for testing) and OWASP Juice Shop (a web app with known vulnerabilities).
- Configure the virtual network to ensure the machines can communicate (use a NAT or Host-Only network in VirtualBox).

Conduct network and port scans

- Use Nmap to scan the Metasploitable machine.
- Target : Metasploit(192.168.10.12).



Vulnerabilities

Apache Tomcat SEoL (<= 5.5.x)

Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained

by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0

VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. We can able to login using VNC authentication and a password of 'password'. A remote unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0

NFS Shares World Readable

Synopsis

The remote NFS server exports world-readable shares.

Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP,or IP range).

Solution

Place the appropriate restrictions on all NFS shares.

Risk Factor

Medium

CVSS v3.0 Base Score

7.5

SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

Risk Factor

Medium

CVSS v3.0 Base Score

5.3