Machine Reconnaissance

Introduction

This report documents a penetration testing process aimed at identifying and analyzing vulnerabilities present in a vulnerable virtual machine. The exercise involved evaluating open ports and running services to uncover potential security gaps that could be exploited. This analysis is crucial for understanding the impact these vulnerabilities may have on the system's security and the overall integrity of the organization.

Objective

The objective of this exercise is to demonstrate the knowledge acquired in the module, where we learned how to conduct a comprehensive scan of a vulnerable machine. By evaluating the open ports and services, we aim to develop an in-depth analysis of how the discovered vulnerabilities can affect security in a corporate environment.

Scope

Each vulnerability identified will be explained in a clear and understandable manner, with the goal of raising awareness about security risks and making the findings accessible to both technical and non-technical audiences.

Tools and Techniques Used

For the execution of these tests, two virtual machines were used: one attacking machine (Kali Linux) and one vulnerable machine (Metasploitable 2). Basic and advanced port scans were conducted using the Nmap tool, which enabled the identification of open ports and the software versions running on them. Based on this information, vulnerabilities that could be exploited were identified and analyzed.

Vulnerabilities

- **Port**: 21/tcp, **Service**: ftp, **Version**: vsftpd 2.3.4, **ID CVE**: CVE-2011-2523
  Explication: Downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp
  Severity: V4.0: (not available), V3.1: 9.8 CRITICAL, V2.0: 10.0 HIGH
- **Port**: 22/tcp, **Service**: ssh, **Version**: OpenSSH 4.7p1, **ID CVE**: CVE-2008-5161
  Explication: Error handling in the SSH protocol when using a block cipher algorithm in Cipher Block Chaining (CBC) mode makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext.
  Severity: V4.0: (not available), V3.x: (not available), V2.0: 2.6 LOW

- **Port**: 53/tcp, **Service**: domain, **Version**: ISC BIND 9.4.2, **ID CVE**: CVE-2008-4163
  Explication: Unspecified vulnerability in ISC BIND 9.4.2 allows remote attackers to cause a denial of service (UDP client handler termination) via unknown vectors.
  Severity: V4.0: (not available), V3.x: (not available), V2.0: 7.8 HIGH
- **Port**: 53/tcp, **Service**: domain, **Version**: ISC BIND 9.4.2, **ID CVE**: CVE-2008-0122
  Explication: Off-by-one error in the inet_network function in libbind in ISC BIND allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via crafted input that triggers memory corruption.
  Severity: V4.0: (not available), V3.x: (not available), V2.0: 10.0 HIGH
- **Port**: 80/tcp, **Service**: http, **Version**: Apache httpd 2.2.8, **ID CVE**: CVE-2010-1452
  Explication: The mod_cache and mod_dav modules in the Apache HTTP Server allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.
  Severity: V4.0: (not available), V3.x: (not available), V2.0: 5.0 MEDIUM
- **Port**: 80/tcp, **Service**: http, **Version**: Apache httpd 2.2.8, **ID CVE**: CVE-2011-3192
  Explication: The byterange filter in the Apache HTTP Server allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges.
  Severity: V4.0: (not available), V3.x: (not available), V2.0: 7.8 HIGH
- **Port**: 80/tcp, **Service**: http, **Version**: Apache httpd 2.2.8, **ID CVE**: CVE-2009-1891
  Explication: The mod_deflate module in Apache compresses large files even after the associated network connection is closed, allowing remote attackers to cause a denial of service (CPU consumption).
  Severity: V4.0: (not available), V3.x: (not available), V2.0: 7.1 HIGH
- **Port**: 111/tcp, **Service**: rpcbind, **Version**: 2 (RPC #100000), **ID CVE**: CVE-2003-1070
  Explication: Unknown vulnerability in rpcbind for Solaris allows remote attackers to cause a denial of service (rpcbind crash).
  Severity: V4.0: (not available), V3.x: (not available), V2.0: 5.0 MEDIUM
- **Port**: 139/tcp, **Service**: netbios-ssn, **Version**: Samba smbd 3.X - 4.X, **ID CVE**: CVE-2007-2447
  Explication: Samba has a command injection vulnerability that allows remote attackers to execute arbitrary commands via a crafted packet.
  Severity: V4.0: 9.8 CRITICAL, V3.x: 9.0 CRITICAL, V2.0: 7.5 HIGH
- **Port**: 512/tcp, **Service**: exec, **ID CVE**: N/A
  Explication: No specific vulnerability found, but running the exec service is generally considered a security risk as it can be used for remote command

execution.
Severity: V4.0: N/A, V3.x: N/A, V2.0: N/A

- **Port**: 513/tcp, **Service**: login, **ID CVE**: N/A
  Explication: The login service is commonly used for remote login and is inherently risky if left unsecured. There are no specific vulnerabilities associated, but the service itself can be an attack vector.
  Severity: V4.0: N/A, V3.x: N/A, V2.0: N/A
- **Port**: 514/tcp, **Service**: shell, **ID CVE**: N/A
  Explication: Running the rsh (remote shell) service is highly insecure due to lack of encryption. It is vulnerable to man-in-the-middle attacks.
  Severity: V4.0: N/A, V3.x: N/A, V2.0: N/A
- **Port**: 1099/tcp, **Service**: java-rmi, **Version**: GNU Classpath grmiregistry, **ID CVE**: CVE-2011-3556
  Explication: Java RMI registry can allow remote attackers to execute arbitrary code or access sensitive information through deserialization attacks.
  Severity: V4.0: 9.8 CRITICAL, V3.x: 9.0 CRITICAL, V2.0: 7.5 HIGH
- **Port**: 1524/tcp, **Service**: bindshell, **Version**: Metasploitable root shell,**ID CVE**: N/A
  Explication: A known backdoor installed on the Metasploitable machine, allowing root access to remote attackers.
  Severity: V4.0: N/A, V3.x: N/A, V2.0: N/A (Backdoor)
- **Port**: 2049/tcp, **Service**: nfs, **Version**: 2-4 (RPC #100003), **ID CVE**: CVE-2018-16871
  Explication: NFS shares can be vulnerable to unauthorized access if not configured properly, allowing attackers to mount shared directories and access sensitive files.
  Severity: V4.0: 7.5 HIGH, V3.x: 6.5 MEDIUM, V2.0: 5.0 MEDIUM
- **Port**: 2121/tcp, **Service**: ccproxy-ftp, **ID CVE**: N/A
  Explication: No specific vulnerability found. However, exposing FTP services is inherently risky due to unencrypted data transfer, which could expose login credentials.
  Severity: V4.0: N/A, V3.x: N/A, V2.0: N/A
- **Port**: 3306/tcp, **Service**: mysql, **ID CVE**: CVE-2012-2122
  Explication: MySQL authentication bypass vulnerability that allows remote attackers to authenticate without a valid password.
  Severity: V4.0: 7.5 HIGH, V3.x: 7.0 HIGH, V2.0: 5.0 MEDIUM
- **Port**: 3632/tcp, **Service**: distccd, **Version**: distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)), **ID CVE**: CVE-2004-2687
  Explication: Remote code execution vulnerability in the distccd service that allows remote attackers to execute arbitrary commands.
  Severity: V4.0: 10.0 CRITICAL, V3.x: 9.0 CRITICAL, V2.0: 7.5 HIGH
- **Port**: 5432/tcp, **Service**: postgresql, **Version**: PostgreSQL DB 8.3.0 - 8.3.7, **ID CVE**: CVE-2007-0555
  Explication: PostgreSQL has an input validation flaw that allows privilege

escalation, potentially allowing attackers to execute arbitrary SQL code.
Severity: V4.0: 8.5 HIGH, V3.x: 7.8 HIGH, V2.0: 6.5 MEDIUM

- **Port**: 5900/tcp, **Service**: vnc, **Version**: VNC (protocol 3.3), **ID CVE**: CVE-2011-2523
  Explication: VNC allows attackers to bypass authentication and access remote desktops.
  Severity: V4.0: 7.5 HIGH, V3.x: 7.8 HIGH, V2.0: 5.0 MEDIUM
- **Port**: 6000/tcp, **Service**: X11, **ID CVE**: CVE-1999-0526
  Explication: X11 service is exposed and can allow remote attackers to access the graphical display system without authentication.
  Severity: V4.0: 9.8 CRITICAL, V3.x: 9.0 CRITICAL, V2.0: 7.5 HIGH
- **Port**: 6667/tcp, **Service**: irc, **Version**: UnrealIRCd, **ID CVE**: CVE-2010-2075
  Explication: Backdoor in UnrealIRCd 3.2.8.1 allows remote attackers to execute arbitrary commands.
  Severity: V4.0: 10.0 CRITICAL, V3.x: 9.8 CRITICAL, V2.0: 7.5 HIGH
- **Port**: 8009/tcp, **Service**: ajp13, **Version**: Apache Jserv (Protocol v1.3), **ID CVE**: CVE-2020-1938
  Explication: AJP connector in Apache Tomcat is vulnerable to file inclusion attacks, allowing attackers to read arbitrary files on the server.
  Severity: V4.0: 7.5 HIGH, V3.x: 8.1 HIGH, V2.0: 6.5 MEDIUM

Impact Analysis

The impact of the vulnerabilities found during the scanning process is significant, as many of them allow remote code execution, unauthorized access, or denial of service (DoS). These security breaches could be exploited by external attackers, threatening the confidentiality, integrity, and availability of the organization’s data.

For instance, the vulnerabilities found in the Samba and Apache services exposed on ports 139, 445, and 80 are particularly critical. Remote code execution and command injection can give attackers full control over the system, enabling malware or ransomware propagation, exfiltration of sensitive data, or unauthorized access to critical resources.

Additionally, services like **rpcbind**, **nfs**, and **vnc** are vulnerable to denial of service attacks and exposure of sensitive information, which can compromise the network's operational integrity.

Vulnerabilities in key services such as MySQL and PostgreSQL represent major risks for databases, which could be exploited to manipulate data or disrupt the integrity of transactions, directly impacting business operations.

Mitigation

To enhance the security of our network, it is crucial to verify and address each of the vulnerabilities outlined in the previous section. The mitigation process should prioritize those vulnerabilities classified as critical, as they pose the highest risk to the company.

Apply Updates and Patches: It is essential to keep services and operating systems up to date with the latest versions. Services such as Apache, Samba, and MySQL should be upgraded to versions that are no longer vulnerable to remote code execution or command injection attacks.

Restrict Access: To minimize the risk of exploitation, it is recommended to apply access control lists (ACLs) to limit which IP addresses can interact with critical services like NFS, MySQL, and PostgreSQL. Additionally, network segmentation can reduce the exposure of sensitive services to external attackers.

Disable Unnecessary Services: Services like **exec**, **login**, and **rsh** should be disabled if not needed, as they present significant risks due to their lack of encryption and vulnerability to man-in-the-middle attacks.

Secure Configuration of Services: Network services such as **Samba** and **Apache** should be properly configured to ensure that file permissions and access policies are appropriate. Disabling unnecessary features like **Directory Indexing** in Apache and restricting access to phpMyAdmin are good security practices.

Continuous Monitoring: Implement real-time monitoring tools to detect suspicious activity or attempts to exploit vulnerabilities, which is key to maintaining proactive security. Services like VNC and RPC should be continuously monitored.