Penetration Testing and Vulnerability Assessment Report

Overview: The procedures used to perform a vulnerability assessment and penetration test on the Metasploitable 2 virtual machine (the target computer) are described in this paper. The evaluation included downloading and setting up Metasploitable 2, then installing and configuring Nessus on Kali Linux to do vulnerability scanning. The report provides information on the susceptible services, possible exploits, and suggested mitigations with an emphasis on high threat vulnerabilities found during the examination.

Methodology:

1. **Metasploitable 2 Installation:**
    - Downloaded Metasploitable 2 from the provided link.
    - Installed the VM on the testing environment.
2. **Nessus Setup:**
    - Installed Nessus on Kali Linux.
    - Configured Nessus for vulnerability scanning.
3. **Vulnerability Scanning:**
    - Conducted a vulnerability scan on the Metasploitable 2 VM using Nessus.

High-Threat Vulnerability Findings:
Several high-risk vulnerabilities on the target system were found by the scan. Three weaknesses were chosen to be examined in further detail:

1. **Vulnerable Service 1: SSH (CVE-2007-2791)**
    - **Description:** Because of CVE-2007-2791, the Secure Shell (SSH) service may permit unwanted access to the system.
    - **Exploit:** By using ineffective encryption techniques or launching brute force attacks against SSH credentials, an attacker may be able to take advantage of this vulnerability.
    - **Mitigation:** Key-based authentication should be used, strict password regulations should be followed, and SSH should be updated to the most recent version in order to mitigate this issue.
2. **Vulnerable Service 2: MySQL Database (CVE-2007-3782)**
    - **Description:** Due to the vulnerability of the MySQL Database service to CVE-2007-3782, private information may be accessed without authorization.
    - **Exploit:** Exploiting this vulnerability may involve SQL injection attacks, enabling attackers to manipulate or extract data from the database. By using SQL injection attacks to take advantage of this vulnerability, attackers might be able to change or remove data from the database.
    - **Mitigation:** Update to the most recent version of MySQL, apply input validation to stop SQL injection, and limit database user access.
3. **Vulnerable Service 3: Microsoft Windows SMB (CVE-2007-6753)**
    - **Description:** Due to the Microsoft Windows SMB vulnerability to CVE-2007-6753, remote attackers can escalate privileges on the victim system, cause denial of service, expose sensitive data, and execute arbitrary code.

- **Exploit:** By using malicious SMB packets, this vulnerability enables remote attackers to run any code.
- **Mitigation:** Use firewalls to filter SMB traffic, limit access to trusted networks, and apply the most recent security upgrades for Windows SMB.

CVE Investigation:

1. **CVEs related to SSH (CVE-2007-2791):**
   - **NVD Investigation:**
     - Examined the NVD record for the particular CVE linked to SSH.
     - Gathered details on the vulnerability, including the severity score, affected versions, description, and any patches or workarounds that are available.
   - **ExploitDB Investigation:**
     - Searched ExploitDB for exploits linked to SSH.
     - Investigated pertinent exploits in order to comprehend the assaults' nature and their consequences.
2. **CVEs related to MySQL Database (CVE-2007-3782):**
   - **NVD Investigation:**
     - Examined the NVD record for the CVE connected to MySQL.
     - Gathered information on the vulnerability, including its description, severity rating, impacted MySQL versions, and any suggested fixes.
   - **ExploitDB Investigation:**
     - Searched ExploitDB for vulnerabilities pertaining to MySQL.
     - Examined pertinent exploits to comprehend possible attack scenarios and any defenses that could be in place.
3. **CVEs related to Microsoft Windows SMB (CVE-2007-6753):**
   - **NVD Investigation:**
     - Investigated the Windows SMB-related CVE's NVD entry.
     - Retrieved details on the vulnerability's severity, impacted Windows versions, description, and any available fixes.
   - **ExploitDB Investigation:**
     - Searched ExploitDB for vulnerabilities pertaining to Windows SMB.
     - Examined pertinent exploits to learn about potential attacks that target SMB vulnerabilities and any countermeasures that may be available.

Overall Analysis:

1. **SSH:**
   - ✓ Evaluated the risk of exploitation and the seriousness of the SSH-related CVE.
   - ✓ Created mitigating techniques, such as upgrading SSH software and putting robust authentication in place.
2. **MySQL Database:**
   - ✓ Evaluated the effect and severity of the MySQL-related CVE.
   - ✓ developed mitigating strategies, including as protecting database setups and patching MySQL instances.

3. **Microsoft Windows SMB:**
    - ✓ Examined the Windows SMB-related CVE to ascertain its seriousness and its dangers.
    - ✓ Implemented mitigating strategies, such as updating Windows and setting up firewalls to restrict SMB access.

Conclusion: Critical vulnerabilities in the Metasploitable 2 virtual machine were found by the penetration test and vulnerability assessment. Insights into possible dangers and suggested mitigations are provided by the thorough examination of high-threat vulnerabilities. To keep a network environment secure, regular security upgrades, appropriate setup, and attentive monitoring are necessary. It is advised to conduct regular evaluations and ongoing monitoring in order to stay ahead of changing security risks. Potential vulnerabilities, exploits, and mitigation techniques were revealed by the thorough examination of CVEs linked to Microsoft Windows SMB, MySQL Database, and SSH. Systems that make use of these services must be protected against known dangers with the use of this information.

Recommendations:

- Update and patch vulnerable services on a regular basis.
- Put robust authentication and access control measures in place.
- To recognize and counter new risks, and periodically evaluate vulnerabilities.

Acknowledgments: To the creators of Nessus, Metasploitable, and the National Vulnerability Database, extend our special gratitude for their fantastic contributions to cybersecurity.