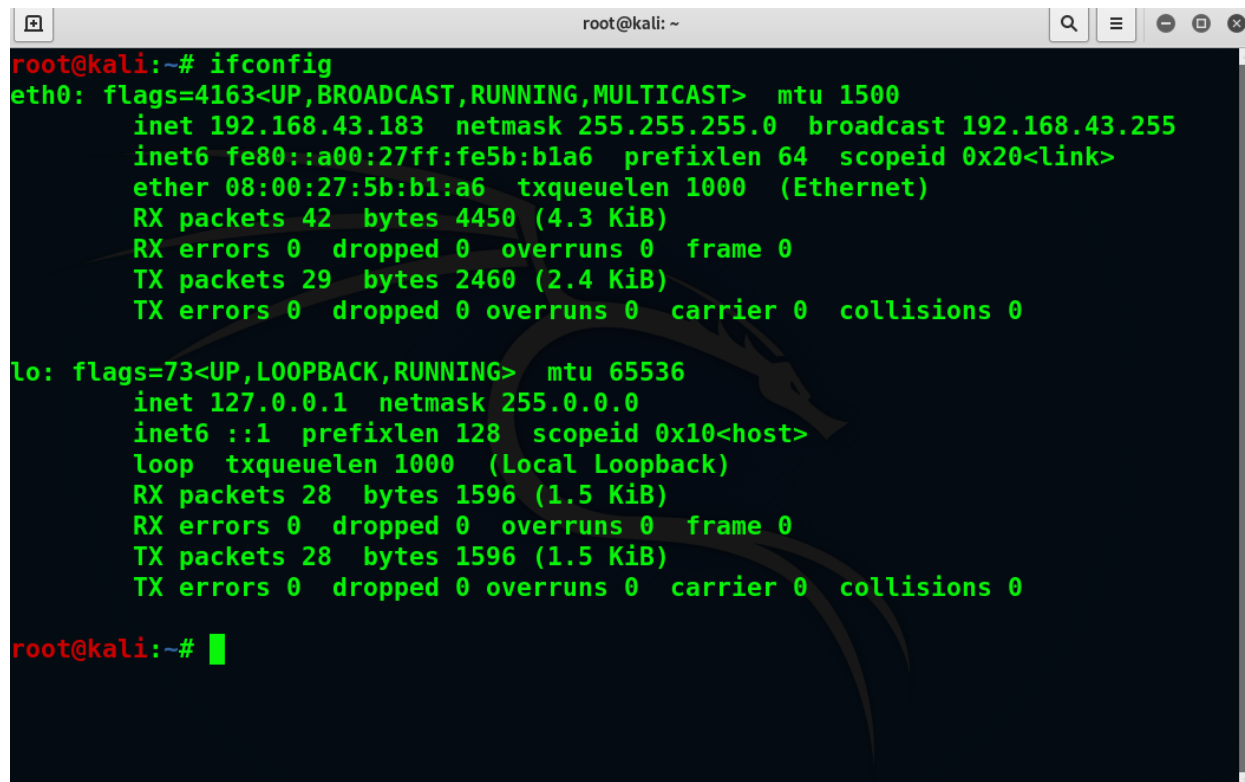


Scanning with Nmap

(target : Kali Linux, Windows 10)

1. Kali Linux scan results :

a) Lets check what is the IP address of our machine with command “ifconfig”.

A terminal window titled 'root@kali: ~' showing the output of the 'ifconfig' command. The output displays details for the 'eth0' (Ethernet) and 'lo' (Local Loopback) interfaces, including their flags, MTU, IP addresses, netmasks, broadcast addresses, and various statistics like RX/TX packets, bytes, errors, and collisions. The 'eth0' interface has an IP of 192.168.43.183, and the 'lo' interface has an IP of 127.0.0.1.

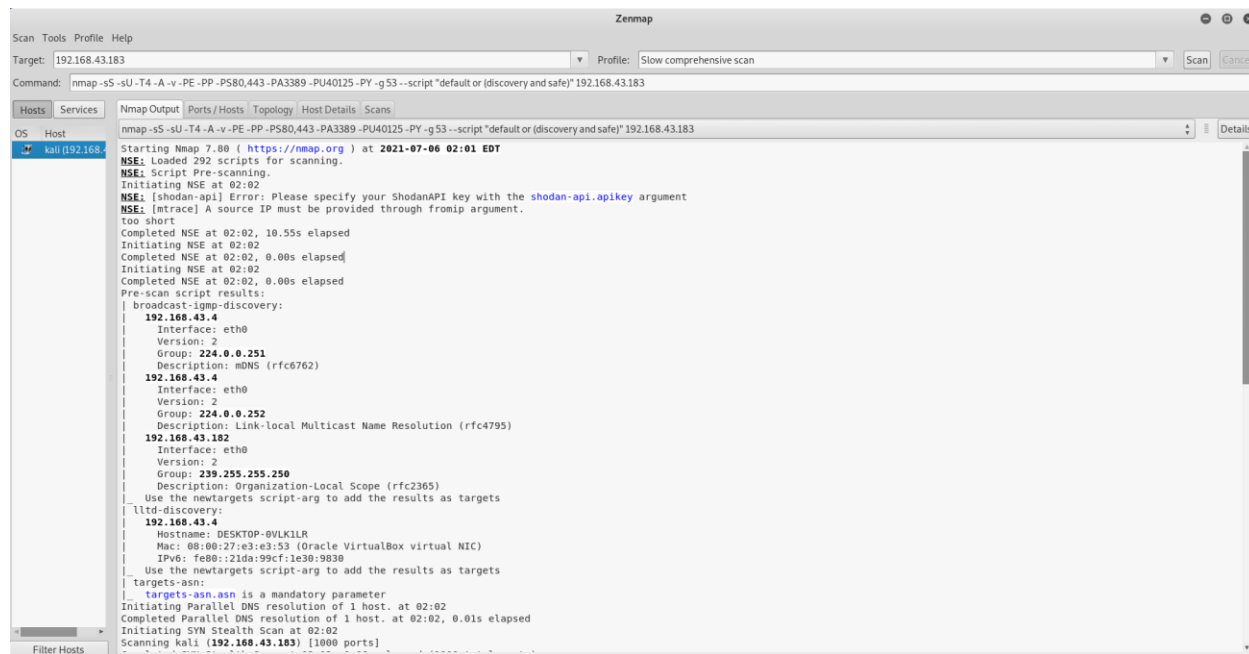
```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.43.183  netmask 255.255.255.0  broadcast 192.168.43.255
    inet6 fe80::a00:27ff:fe5b:b1a6  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:5b:b1:a6  txqueuelen 1000  (Ethernet)
    RX packets 42  bytes 4450 (4.3 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 29  bytes 2460 (2.4 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 28  bytes 1596 (1.5 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 28  bytes 1596 (1.5 KiB)
    TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

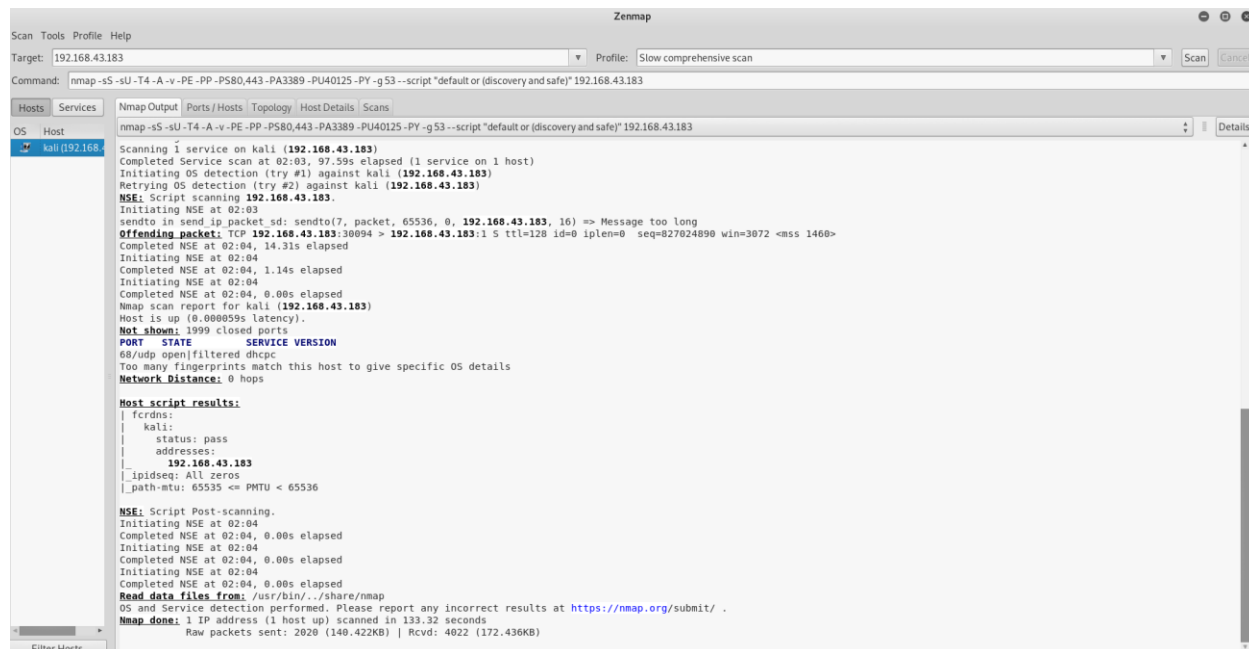
root@kali:~#
```

b) Download & Install the Nmap.

c) Open Nmap and insert IP address of kali linux in target section with slow comprehensive scan profile.



d) Check for the open ports.



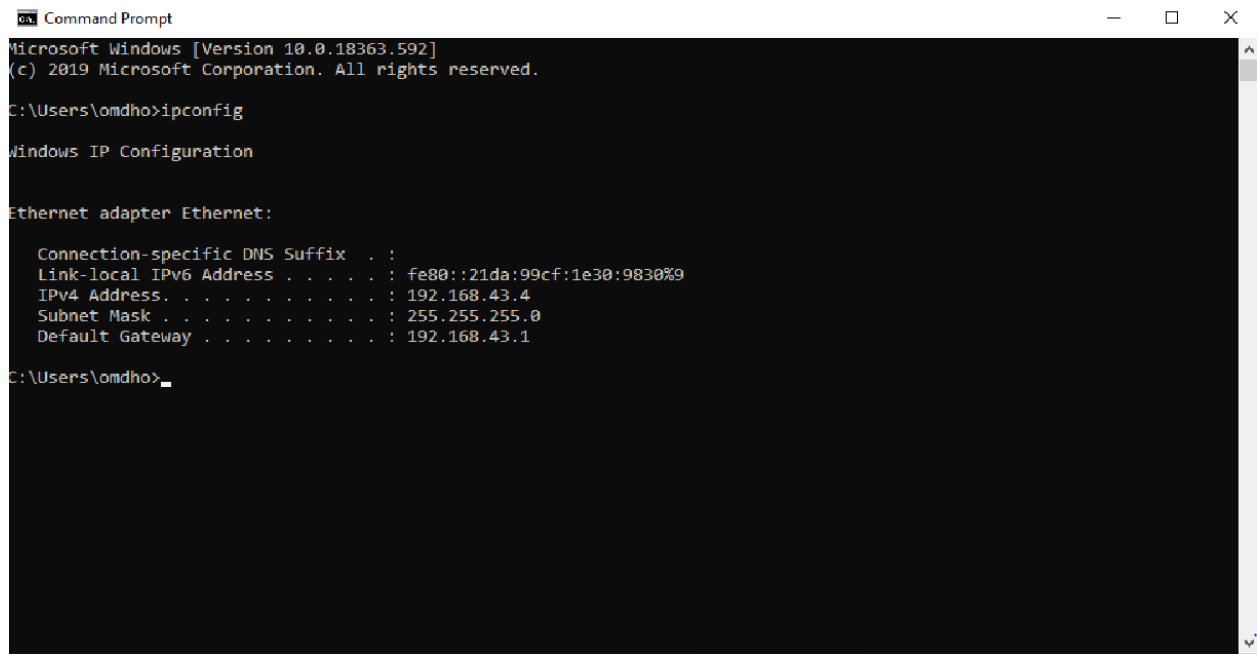
e) Following are the open ports of the kali linux.

f) Here, we get port no. 68/udp port which is in open state and running the dhcpc services.

The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol networks for automatically assigning IP addresses and other communication parameters to device connected to the network using a client-server architecture.

2. Windows 10 scan results :

a) Lets chek the IP address of the windows 10 machine with
command “ipconfig”.

A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The text inside shows the Windows version and copyright information, followed by the command "ipconfig" being executed. The output displays the IP configuration for the Ethernet adapter, including the IPv4 address 192.168.43.4 and the default gateway 192.168.43.1.

```
Microsoft Windows [Version 10.0.18363.592]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\omdho>ipconfig

Windows IP Configuration

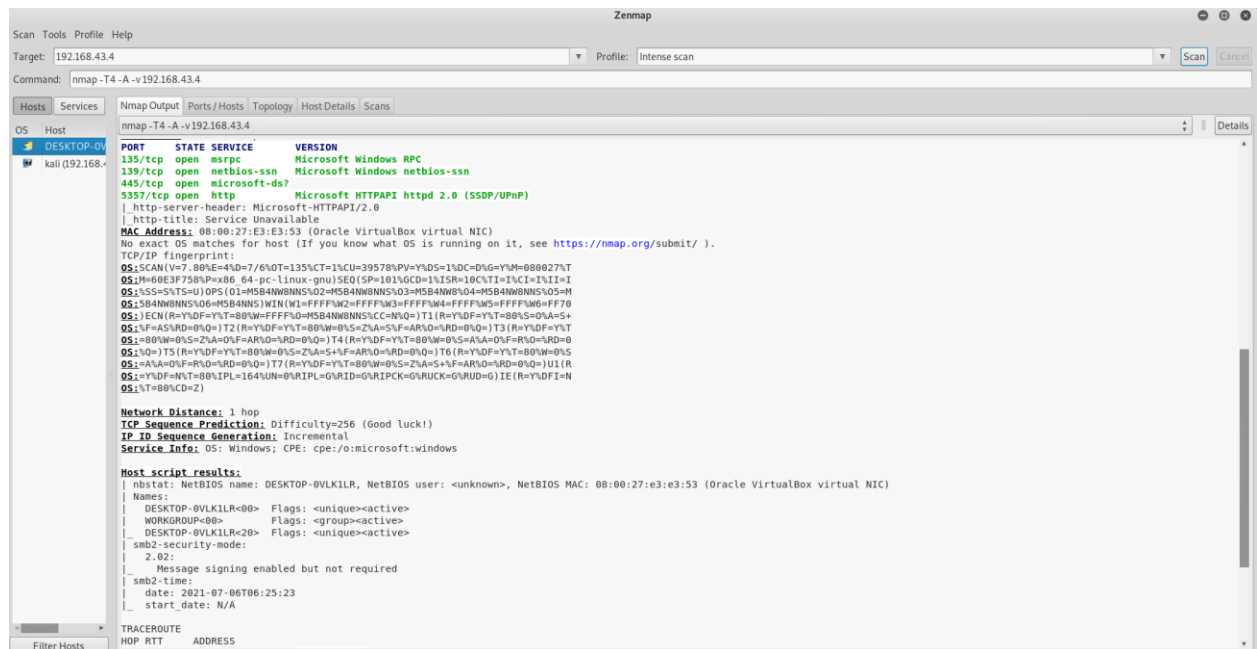
Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::21da:99cf:1e30:9830%9
    IPv4 Address. . . . . : 192.168.43.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.43.1

C:\Users\omdho>
```

b) Open Nmap and insert IP address of windows 10 in target
section intense scan profile.

c) Let check the open ports and running services on that.



d) Here we found the 4 open ports :

135/tcp running Microsoft Windows RPC service.

135/tcp running netbios-ssn service.

445/tcp running Microsoft-ds?

5357/tcp runs http (httpd 2.0) service.

