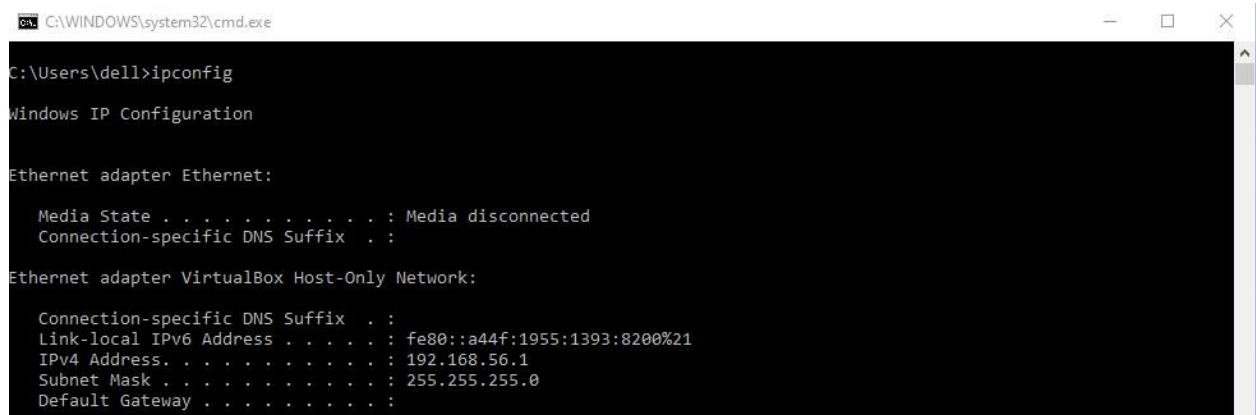


- To Perform nmap scanning on windows 7 and kali-linux,find the open/closed ports with services.

We have to find ip address of the target machine using cmd “ipconfig”.

A screenshot of a Windows Command Prompt window titled "C:\WINDOWS\system32\cmd.exe". The user has entered the command "ipconfig". The output shows the configuration for two network adapters. The first is "Ethernet adapter Ethernet:", which shows "Media State . . . . . : Media disconnected" and "Connection-specific DNS Suffix . : ". The second is "Ethernet adapter VirtualBox Host-Only Network:", which shows "Connection-specific DNS Suffix . : ", "Link-local IPv6 Address . . . . . : fe80::a44f:1955:1393:8200%21", "IPv4 Address. . . . . : 192.168.56.1", "Subnet Mask . . . . . : 255.255.255.0", and "Default Gateway . . . . . : ".

```
C:\WINDOWS\system32\cmd.exe
C:\Users\dell>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

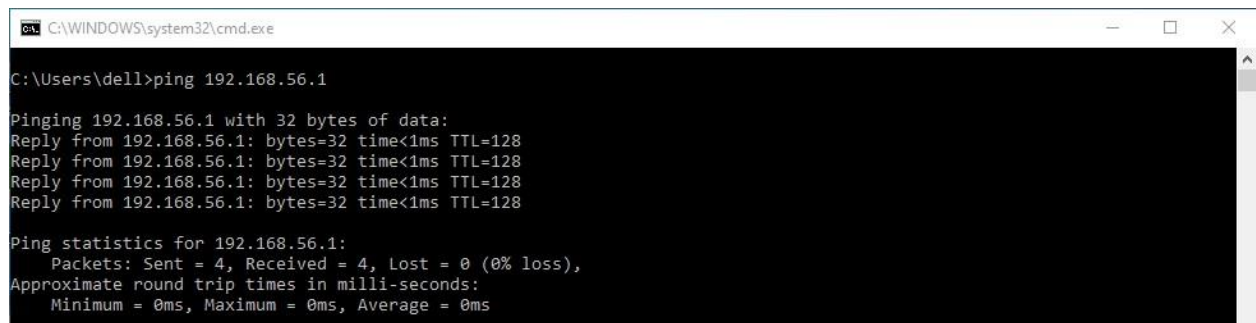
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::a44f:1955:1393:8200%21
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```

We got the ip address of the target machine “192.168.56.1”

Now we will check if the target machine is up,for that we need to use ping command in cmd.

A screenshot of a Windows Command Prompt window titled "C:\WINDOWS\system32\cmd.exe". The user has entered the command "ping 192.168.56.1". The output shows four successful replies from 192.168.56.1, each with 32 bytes of data, a time less than 1ms, and a TTL of 128. Below the replies, it shows ping statistics for 192.168.56.1: "Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)", "Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms".

```
C:\WINDOWS\system32\cmd.exe
C:\Users\dell>ping 192.168.56.1

Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128
Reply from 192.168.56.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

First we are going to use intense scan plus UDP on nmap.

Zenmap

Scan Tools Profile Help

Target: 192.168.56.1 Profile: Intense scan plus UDP Scan Cancel

Command: nmap -sS -sU -T4 -A -v 192.168.56.1

Hosts Services

Service

- http
- isakmp
- llmnr
- microsoft-ds
- mmcc
- msrpc
- nat-t-ike
- netbios-dgm
- netbios-ns
- netbios-ssn
- ntp
- tcpwrapped
- unknown
- upnp
- ws-discovery
- zeroconf

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -sS -sU -T4 -A -v 192.168.56.1

Host is up (0.00073s latency).  
**Not shown:** 1985 closed ports

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	
5357/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

|\_http-server-header: Microsoft-HTTPAPI/2.0  
|\_http-title: Service Unavailable

67/udp open|filtered tcpwrapped  
123/udp open|filtered ntp  
137/udp open|filtered netbios-ns  
138/udp open|filtered netbios-dgm  
500/udp open|filtered isakmp  
1900/udp open|filtered upnp  
3702/udp open|filtered ws-discovery

| wsd-discover:  
| Devices  
| Message id: fe453eba-74e3-4817-9199-a6865b701577  
| Address: http://192.168.56.1:5357/9e9c9859-f24a-44d9-985e-3bb08cbleaa1/  
| Type: Device pub:Computer

4500/udp open|filtered nat-t-ike  
5050/udp open|filtered mmcc  
5353/udp open|filtered zeroconf  
5355/udp open|filtered llmnr

No exact OS matches for host (If you know what OS is running on it, see <https://nmap.org/submit/> ).  
TCP/IP fingerprint:  
OS:SCAN(V=7.91%E=4%D=8/3%OT=135%CT=1%CU=2%PV=Y%DS=0%DC=L%G=Y%  
TM=61090E55%P=  
OS:i686-pc-windows-windows)SEQ(SP=103%GCD=1%ISR=10A%TI=I%CI=I%II=I%SS=S  
%TS=  
OS:U)OPS(O1=MFFD7NNS%O2=MFFD7NNS%O3=MFFD7%O4=MFFD7NNS%O5=MFFD7NNS%

Filter Hosts

## Open/closed and filtered ports(UDP)

Zenmap

Scan Tools Profile Help

Target: 192.168.56.1 Profile: Intense scan plus UDP Scan Cancel

Command: nmap -sS -sU -T4 -A -v 192.168.56.1

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

- 192.168.0.8
- 192.168.56.1

Filter Hosts

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
137	tcp	filtered	netbios-ns	
445	tcp	open	microsoft-ds	
5040	tcp	open	unknown	
5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5700	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664	tcp	open	msrpc	Microsoft Windows RPC
49665	tcp	open	msrpc	Microsoft Windows RPC
49666	tcp	open	msrpc	Microsoft Windows RPC
49667	tcp	open	msrpc	Microsoft Windows RPC
49668	tcp	open	msrpc	Microsoft Windows RPC
49669	tcp	open	msrpc	Microsoft Windows RPC
67	udp	open filtered	tcpwrapped	
123	udp	open filtered	ntp	
137	udp	open filtered	netbios-ns	
500	udp	open filtered	isakmp	
3702	udp	open filtered	ws-discovery	
4500	udp	open filtered	nat-t-ike	
5050	udp	open filtered	mmcc	
5353	udp	open filtered	zeroconf	
5355	udp	open filtered	llmnr	

Now, we are doing TCP scan

The screenshot shows the Zenmap application window. At the top, there's a menu bar with 'Scan', 'Tools', 'Profile', and 'Help'. Below the menu, the 'Target' field is set to '192.168.56.1' and the 'Profile' is 'Intense scan, all TCP ports'. The 'Command' field contains 'nmap -p 1-65535 -T4 -A -v 192.168.56.1'. On the left, there's a 'Services' tab selected, showing a list of services: http, isakmp, llmnr, microsoft-ds, mmcc, msrpc, nat-t-ike, netbios-dgm, netbios-ns, netbios-ssn, ntp, tcpwrapped, unknown, upnp, ws-discovery, and zeroconf. The main area displays the 'Nmap Output' for the command 'nmap -p 1-65535 -T4 -A -v 192.168.56.1'. The output text is as follows:

```
nmap -p 1-65535 -T4 -A -v 192.168.56.1

Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-03 15:12 India
Standard Time
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:12
Completed NSE at 15:12, 0.00s elapsed
Initiating NSE at 15:12
Completed NSE at 15:12, 0.00s elapsed
Initiating NSE at 15:12
Completed NSE at 15:12, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 15:12
Completed Parallel DNS resolution of 1 host. at 15:12, 0.24s elapsed
Initiating SYN Stealth Scan at 15:12
Scanning 192.168.56.1 [65535 ports]
Discovered open port 135/tcp on 192.168.56.1
Discovered open port 445/tcp on 192.168.56.1
Discovered open port 139/tcp on 192.168.56.1
Discovered open port 49669/tcp on 192.168.56.1
Discovered open port 49664/tcp on 192.168.56.1
Discovered open port 49665/tcp on 192.168.56.1
Discovered open port 49668/tcp on 192.168.56.1
Discovered open port 49667/tcp on 192.168.56.1
Discovered open port 5700/tcp on 192.168.56.1
Discovered open port 5040/tcp on 192.168.56.1
Discovered open port 49666/tcp on 192.168.56.1
Discovered open port 5357/tcp on 192.168.56.1
Completed SYN Stealth Scan at 15:13, 19.04s elapsed (65535 total ports)
Initiating Service scan at 15:13
Scanning 12 services on 192.168.56.1
Service scan Timing: About 50.00% done; ETC: 15:14 (0:00:54 remaining)
Completed Service scan at 15:15, 156.09s elapsed (12 services on 1
host)
Initiating OS detection (try #1) against 192.168.56.1
Retrying OS detection (try #2) against 192.168.56.1
Retrying OS detection (try #3) against 192.168.56.1
```

At the bottom of the main area, there's a 'Filter Hosts' button.



## TCP ports

Zenmap

Scan Tools Profile Help

Target: 192.168.56.1 Profile: Intense scan, all TCP ports Scan Cancel

Command: nmap -p 1-65535 -T4 -A -v 192.168.56.1

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

Service

- http
- isakmp
- llmnr
- microsoft-ds
- mmcc
- msrpc
- nat-t-ike
- netbios-dgm
- netbios-ns
- netbios-ssn
- ntp
- tcpwrapped
- unknown
- upnp
- ws-discovery
- zeroconf

Port	Protocol	State	Service	Version
135	tcp	open	msrpc	Microsoft Windows RPC
137	tcp	filtered	netbios-ns	
139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445	tcp	open	microsoft-ds	
5040	tcp	open	unknown	
5357	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPr
5700	tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPr
49664	tcp	open	msrpc	Microsoft Windows RPC
49665	tcp	open	msrpc	Microsoft Windows RPC
49666	tcp	open	msrpc	Microsoft Windows RPC
49667	tcp	open	msrpc	Microsoft Windows RPC
49668	tcp	open	msrpc	Microsoft Windows RPC
49669	tcp	open	msrpc	Microsoft Windows RPC
67	udp	open filtered	tcpwrapped	
123	udp	open filtered	ntp	
137	udp	open filtered	netbios-ns	
138	udp	open filtered	netbios-dgm	
500	udp	open filtered	isakmp	
1900	udp	open filtered	upnp	
3702	udp	open filtered	ws-discovery	
4500	udp	open filtered	nat-t-ike	
5050	udp	open filtered	mmcc	
5353	udp	open filtered	zeroconf	

Filter Hosts

```
iqbal@kali: ~  
File Actions Edit View Help  
  
(iqbal@kali)-[~]  
$ nmap -p-65535 -v -T3 -A 192.168.0.11  
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-17 18:10 IST  
NSE: Loaded 153 scripts for scanning.  
NSE: Script Pre-scanning.  
Initiating NSE at 18:10  
Completed NSE at 18:10, 0.00s elapsed  
Initiating NSE at 18:10  
Completed NSE at 18:10, 0.00s elapsed  
Initiating NSE at 18:10  
Completed NSE at 18:10, 0.00s elapsed  
Initiating Ping Scan at 18:10  
Scanning 192.168.0.11 [2 ports]  
Completed Ping Scan at 18:10, 0.00s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 18:10  
Completed Parallel DNS resolution of 1 host. at 18:10, 0.04s elapsed  
Initiating Connect Scan at 18:10  
Scanning 192.168.0.11 [65535 ports]  
Completed Connect Scan at 18:10, 3.14s elapsed (65535 total ports)  
Initiating Service scan at 18:10  
NSE: Script scanning 192.168.0.11.  
Initiating NSE at 18:10  
Completed NSE at 18:10, 0.01s elapsed  
Initiating NSE at 18:10  
Completed NSE at 18:10, 0.01s elapsed  
Initiating NSE at 18:10  
Completed NSE at 18:10, 0.01s elapsed  
Nmap scan report for 192.168.0.11  
Host is up (0.00016s latency).
```

```
iqbal@kali: ~  
File Actions Edit View Help  
Completed Parallel DNS resolution of 1 host. at 18:10, 0.04s elapsed  
Initiating Connect Scan at 18:10  
Scanning 192.168.0.11 [65535 ports]  
Completed Connect Scan at 18:10, 3.14s elapsed (65535 total ports)  
Initiating Service scan at 18:10  
NSE: Script scanning 192.168.0.11.  
Initiating NSE at 18:10  
Completed NSE at 18:10, 0.01s elapsed  
Initiating NSE at 18:10  
Completed NSE at 18:10, 0.01s elapsed  
Initiating NSE at 18:10  
Completed NSE at 18:10, 0.01s elapsed  
Nmap scan report for 192.168.0.11  
Host is up (0.00016s latency).  
All 65535 scanned ports on 192.168.0.11 are closed  
  
NSE: Script Post-scanning.  
Initiating NSE at 18:10  
Completed NSE at 18:10, 0.00s elapsed  
Initiating NSE at 18:10  
Completed NSE at 18:10, 0.00s elapsed  
Initiating NSE at 18:10  
Completed NSE at 18:10, 0.00s elapsed  
Read data files from: /usr/bin/./share/nmap  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 4.40 seconds  
  
(iqbal@kali)-[~]  
$
```