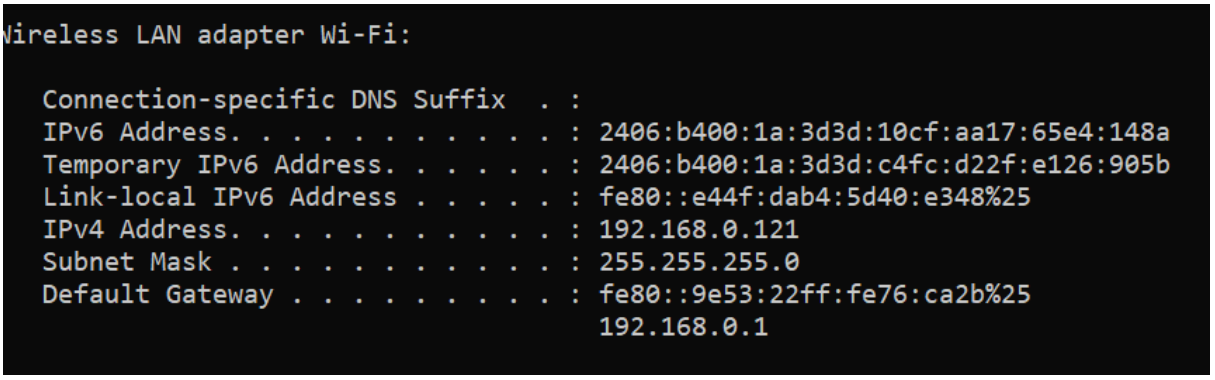
Task 1

On my Windows system, **ipconfig** command gives



My address is 192.168.0.121, as shown here. Since the subnet mask is 255.255.255.0, my local IP range would then be

192.168.0.0 to 192.168.0.24 ~ 256

The last octet (an address has 4 numbers called octets, separated by dots) in the subnet mask is 0, which means, when converted to binary, it is 8 bits of 0s. That means that many 2^8 = 256 addresses are available to host addresses to take up.

Upon running the TCP SYN scan

IP addresses:

1. 192.168.0.1; Open ports:- 21, 80, 139, 445, 1900
2. 192.168.0.112; Open ports:- 445
3. 192.168.0.119; Open ports:- All 1000 scanned are closed

4. 192.168.0.121 (My PC); Open ports:- 135, 139, 445, 1024, 3306

Out of 256 IP addresses, these 4 hosts were scanned using a modified TCP SYN command *to reduce time and ignore DNS resolution (where it was getting stuck)*: **nmap -sn --script broadcast-arp-discovery -n 192.168.0.0/24**

Port services (after browsing & Googling) -

- 21 - FTP, so used for data transfer (File Transfer Protocol)

RISK - transfer is not encrypted

- 80 - HTTP, web traffic

RISK - not encrypted, HTTPS is encrypted

- 135 - Microsoft service to facilitate Windows client-server communication

RISK - vulnerable to Denial of Service (DoS) attacks

- 445 - File sharing & inter-process communication in Windows system processes

RISK - can be exploited if not properly secured (disabling firewall)

- 139 - file & printer sharing

RISK - normally closed, otherwise data from the network could be exposed

- 1024 - Flexible and held in reserve for anything

RISK - not vulnerable in general, can be exploited if open and not careful like in 445

- 3306 - MySQL server, connection for clients & applications (My PC has MySQL, and that is why it showed up in the scan)

RISK - vulnerable if exposed without safeguards, especially to unknown netw

- 1900 - network discovery

RISK - similar to 445 and 1024