**TASK 1: SCAN LOCAL NETWORK FOR OPEN PORTS**

To scan local network, we need IP address or its Network address. For windows,

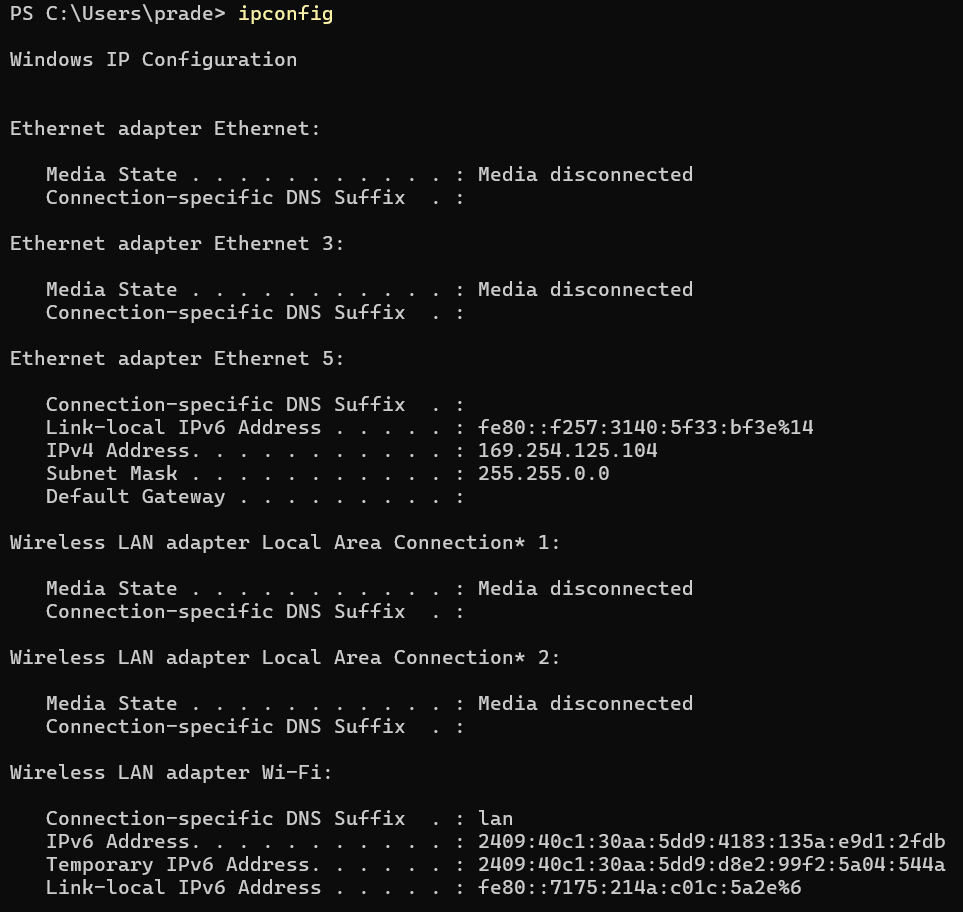


Figure 1- 'ipconfig' results in windows via command prompt

A computer screen shot of a computer

AI-generated content may be incorrect.

Figure 2 - 'ipconfig' results in windows via command prompt conti..

**RESULT FOR TCP SYN SCAN**

PS C:\Users\prade> nmap -sS 192.168.1.0/24

Following are found IP address from the scan with their open ports

**192.168.1.1**

PORT STATE SERVICE

53/tcp open domain

80/tcp open http

443/tcp open https

7443/tcp open oracleas-https

8080/tcp open http-proxy

8443/tcp open https-alt

**192.168.1.8**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

**192.168.1.10**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8000/tcp open http-alt

8899/tcp open ospf-lite

**192.168.1.60**

PORT STATE SERVICE

2869/tcp open icslap

2875/tcp open dxmessagebase2

**192.168.1.88**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8000/tcp open http-alt

**192.168.1.93**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8000/tcp open http-alt

**192.168.1.101**

PORT STATE SERVICE

23/tcp open telnet

80/tcp open http

554/tcp open rtsp

3800/tcp open pwgpsi

5000/tcp open upnp

49152/tcp open unknown

**192.168.1.102**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

**192.168.1.104**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

3800/tcp open pwgpsi

5000/tcp open upnp

49152/tcp open unknown

**192.168.1.109**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

3800/tcp open pwgpsi

5000/tcp open upnp

49152/tcp open unknown

**192.168.1.111**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8000/tcp open http-alt

8899/tcp open ospf-lite

**192.168.1.112**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8000/tcp open http-alt

8899/tcp open ospf-lite

**192.168.1.113**

PORT STATE SERVICE

23/tcp open telnet

80/tcp open http

554/tcp open rtsp

3800/tcp open pwgpsi

5000/tcp open upnp

49152/tcp open unknown

**192.168.1.115**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8000/tcp open http-alt

8899/tcp open ospf-lite

**192.168.1.116**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8086/tcp open d-s-n

**192.168.1.117**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

**192.168.1.161**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

**192.168.1.163**

PORT STATE SERVICE

80/tcp open http

8000/tcp open http-alt

9101/tcp open jetdirect

**192.168.1.165**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8086/tcp open d-s-n

**192.168.1.172**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

3800/tcp open pwgpsi

5000/tcp open upnp

49152/tcp open unknown

**192.168.1.210**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8086/tcp open d-s-n

**192.168.1.221**

PORT STATE SERVICE

80/tcp open http

443/tcp open https

554/tcp open rtsp

3800/tcp open pwgpsi

5000/tcp open upnp

**192.168.1.233**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8086/tcp open d-s-n

**192.168.1.234**

PORT STATE SERVICE

9080/tcp filtered glrpc

**192.168.1.235**

PORT STATE SERVICE

23/tcp open telnet

80/tcp open http

554/tcp open rtsp

3800/tcp open pwgpsi

5000/tcp open upnp

49152/tcp open unknown

**192.168.1.242**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8086/tcp open d-s-n

**192.168.1.244**

PORT STATE SERVICE

80/tcp open http

554/tcp open rtsp

8086/tcp open d-s-n

**192.168.1.162**

PORT STATE SERVICE

135/tcp open msrpc

139/tcp open netbios-ssn

445/tcp open microsoft-ds

903/tcp open iss-console-mgr

COMMON SERVICES FOUND ON THOSE PORTS

**Port 23** – Telnet protocol used for remote access and management of devices over a network.

**Port 53** – Domain Name System (DNS) used for translating domain name to IP address for communication.

**Port 80** – A communication medium between client computers and servers to handle HTTP requests and responses.

**Port 554** – Associated with RSTP for streaming media.

**Port 445 or 139** – Server Message Block (SMB) allows local network devices to share files and printer. Port 139 is for windows-based network.

**Port 135** – Microsoft RPC (Remote Procedure Call) services and DCOM (Distributed Component Object Model) used by Windows to manage communications between applications and networked services. Essential in domain environments (e.g., Active Directory, Exchange, etc.).

**Port 903** – For VM (virtual machine) console access to the ESXi host to run.

**Port 9101** – It used for printing over the internet by printer software.

**Port 8000** – It is used by web servers and HTTP based application for development.

**Port 443** – Port 443 is used by **web servers and browsers** for secure web traffic. When you visit a website that starts with https://