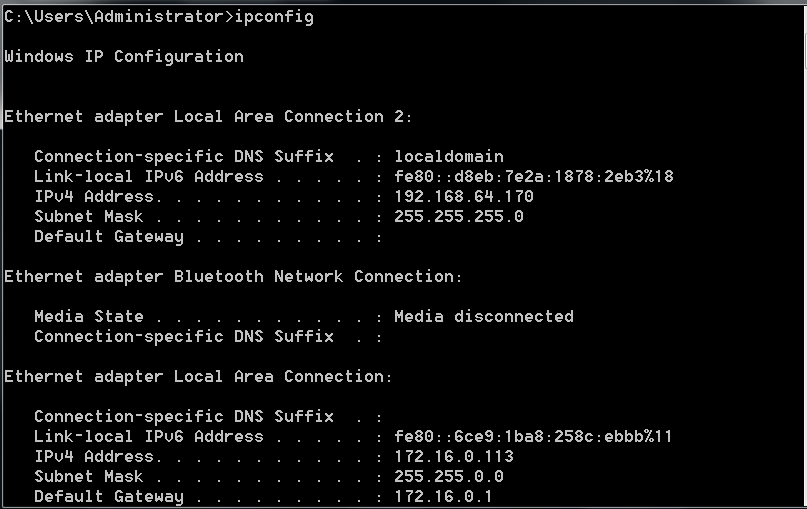
Lab-Project 3: Analyzing a Port Scan

**Finding the IP Address of Your Windows Machines**

From your Windows desktop, click **Start**. In the search box, enter **CMD** and press the Enter key.

In the Command Prompt window, enter the **IPCONFIG** command and press the Enter key. Several IP addresses appear.



**Turning Off the Windows Firewall:**

In Windows machine: click **Start**. In the search box, enter **FIRE**.

In the "Control Panel" section of the results, click "**Windows Firewall**".

On the left side of the "Windows Firewall" box, click "**Turn Windows Firewall on or off**". Click both of the "**Turn off Windows Firewall (not recommended)**" buttons.

Click the **OK** button.

A screenshot of a computer

Description automatically generated

**Pinging the Windows Machine From the Linux Machine**

**ping 192.168.64.170**

**A screen shot of a computer

Description automatically generated**

**Ping google.com**

**A computer screen shot of a computer program

Description automatically generated**

**Performing a Ping Sweep of your Network:**

+ Using nmap with command: **nmap -sn 192.168.64.0/24** to do “Ping Scan”

A screen shot of a computer

Description automatically generated

We see choose target machine is 192.168.64.170

**Using Wireshark to Analyze the Ping Sweep**

+ We can see that many ARP request. Because you are scanning your own LAN, Nmap uses ARP broadcasts rather than ICMP packets to find hosts

A screenshot of a computer

Description automatically generated

**Performing an Quick Scan of the Windows Machine:**

Using nmap command: **nmap -T4 -F 192.168.64.170**

A computer screen shot of a computer

Description automatically generated

After scanning, we should see a list of open ports including "135/tcp open" in the target machine

**Starting a New Wireshark Capture:**

**A screenshot of a computer

Description automatically generated**

**Performing a Connect Scan of Port 135 only**

Using command: **nmap -sT -p 135 -T4 -v 192.168.64.170**

**A computer screen shot of a computer program

Description automatically generated**

**Using Wireshark to Analyze the Connect Scan:**

In the filter box, type: **tcp.port = 135**

A screenshot of a computer

Description automatically generated

This is a complete TCP three-way handshake, followed by a RST to end the session