**Task 1: Scan Your Local Network for Open Ports**

Objective: Learn to discover open ports on devices in your local network to

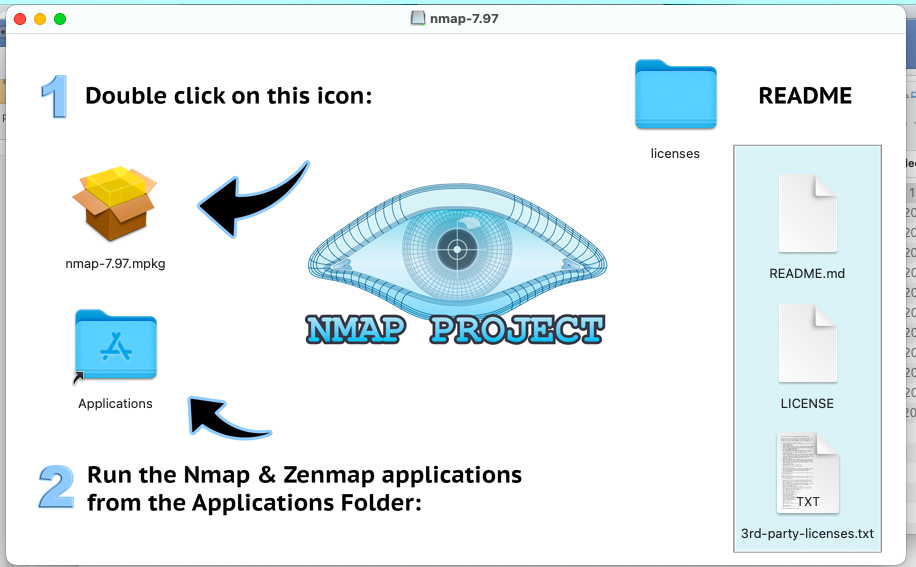
understand network exposure.

Tools: Nmap (free), Wireshark (optional)

Steps followed:-

1.Installed Nmap from official website.

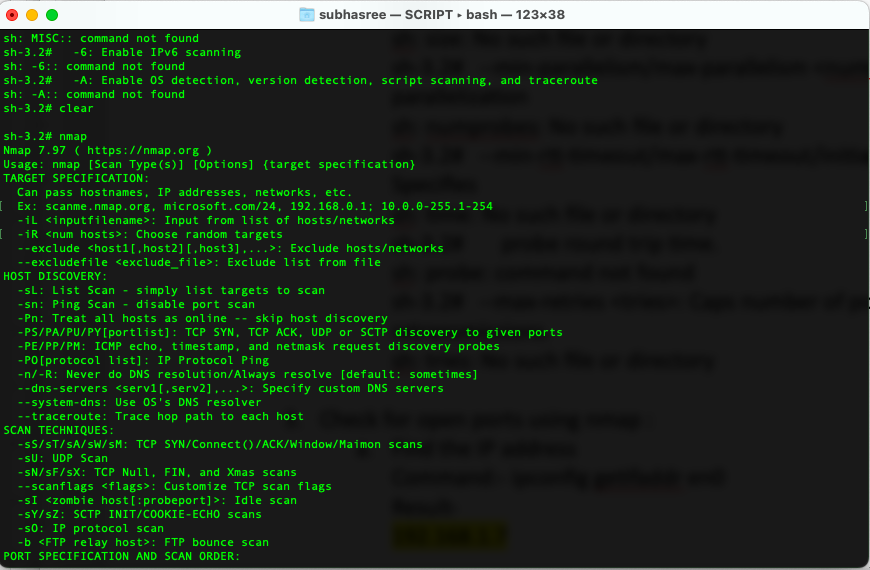
* 1. Go to url -> <https://nmap.org/download.html#macosx>
  2. Download latest stable release version nmap installer (e.g. <[**nmap-7.97.dmg**](https://nmap.org/dist/nmap-7.97.dmg)>)
  3. By double clicking on the downloaded file <nmap-7.97.dmg>, followed the instructions and installed the nmap.



* 1. Checked the nmap in terminal:-

Command : nmap

Result:-



1. To find my PC’s local IP range used below commands-

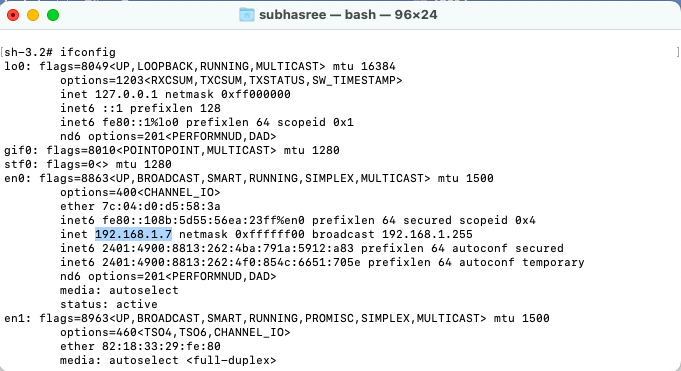
*Command*:-

1. ipconfig getifaddr en0

*Result*- 192.168.1.7

1. ifconfig

Screenshot-

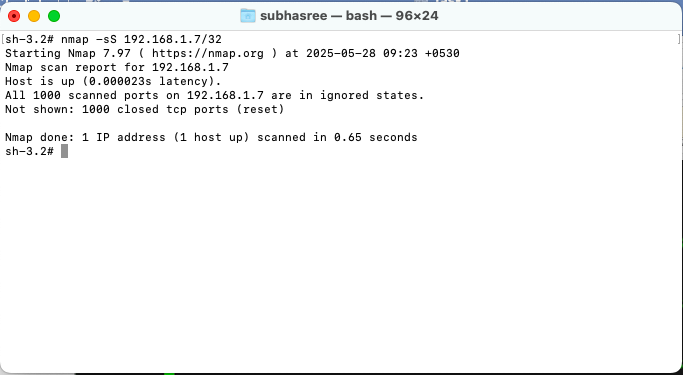


3. Performed TCP SYN scan on my local IP address range.

*Command* : nmap -sS 192.168.1.7/32

*Result*: Only 1 IP address (host) is up.

Screenshot:



4. IP addresses and open ports found are -

**Result** – Nmap scan report for 192.168.1.7

Host is up (0.000029s latency).

All 1000 scanned ports on 192.168.1.7 are in ignored states.

Not shown: 1000 closed tcp ports (reset)

The Nmap result explanation:

* "All 1000 scanned ports on 192.168.1.7 are in ignored states", indicates that Nmap was unable to determine whether those ports were open or filtered due to a lack of response or a firewall blocking the scan.

**Ignored States:** This state implies during the Nmap scans of the ports, it send a probe packet looking for a response, but no response is received, so it's difficult to specify if the port is open (listening) or if it's being filtered by a firewall. In this case, the 1000 ports scanned were in this "open / filtered" state.

* "Not shown: 1000 closed tcp ports (reset)", means that Nmap detected the ports were closed, but those were not shown in the output because they are often numerous and the results are filtered for readability.

**Closed Ports (Not Shown):** This stateNmap also detected closed ports, which are not listening for connections. These are typically indicated by a "reset" signal, which means the connection attempt was rejected. Nmap filtered out the vast majority of closed ports to avoid overwhelming the user with a long list of non-open ports.

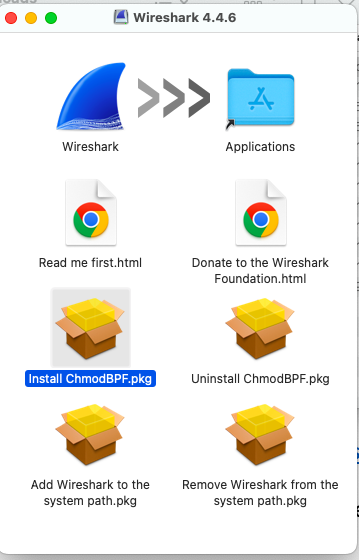
* "Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds" confirms that Nmap performed a scan of the specified IP address and found it to be up and running.

**Host Up:** It confirms that the target IP address (192.168.1.7) was successfully scanned and found to be online and responsive, as it responded to the probe sent by Nmap.

5. Installed and analyzed packet capture with Wireshark

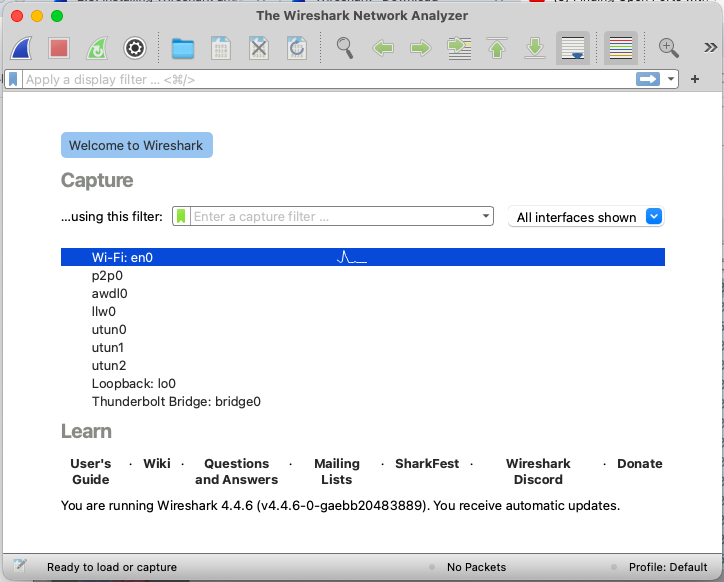
1. Installation-

* Download Wireshark from url :- <https://www.wireshark.org/download.html>
* Select “macOS Intel Disk Image” and the .dmg file gets downloaded.
* Go to downloads folder and open the downloaded file and follow the instructions:

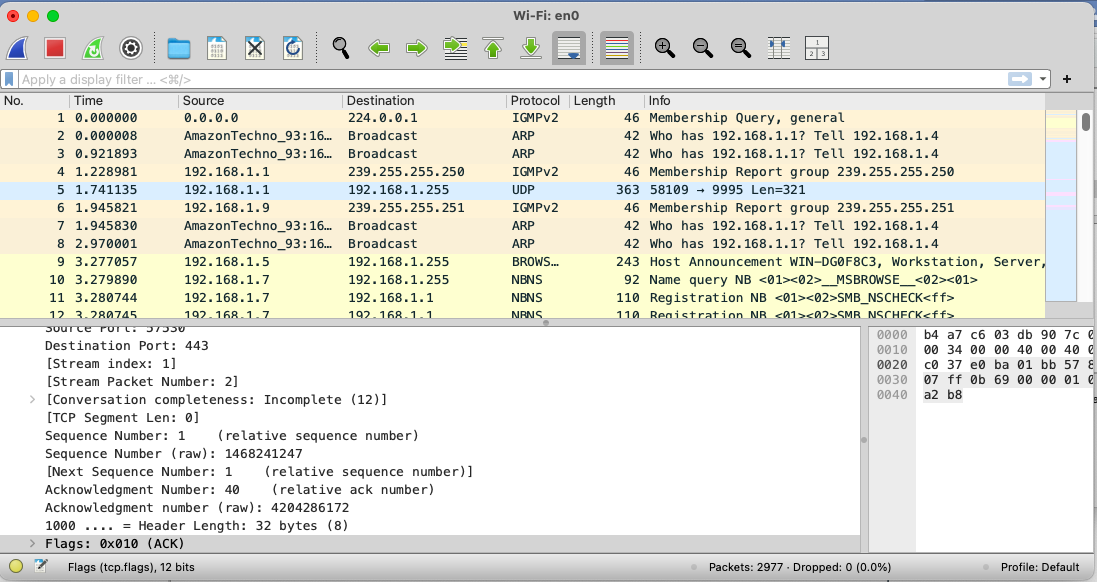


b)Check for open ports using Wireshark

* Open the Wireshark from the launchpad and double click on- Wifi: en0



* Run Wireshark scan by clicking on the shark tail icon on top and stop the scan by clicking the red square icon.



* To find all the ports pinged by the host IP address with completed handshake TCP flag ACK (0X10):

Use Filter : ip.src==192.168.1.7 and tcp.flags==0X010

Screenshots:-

