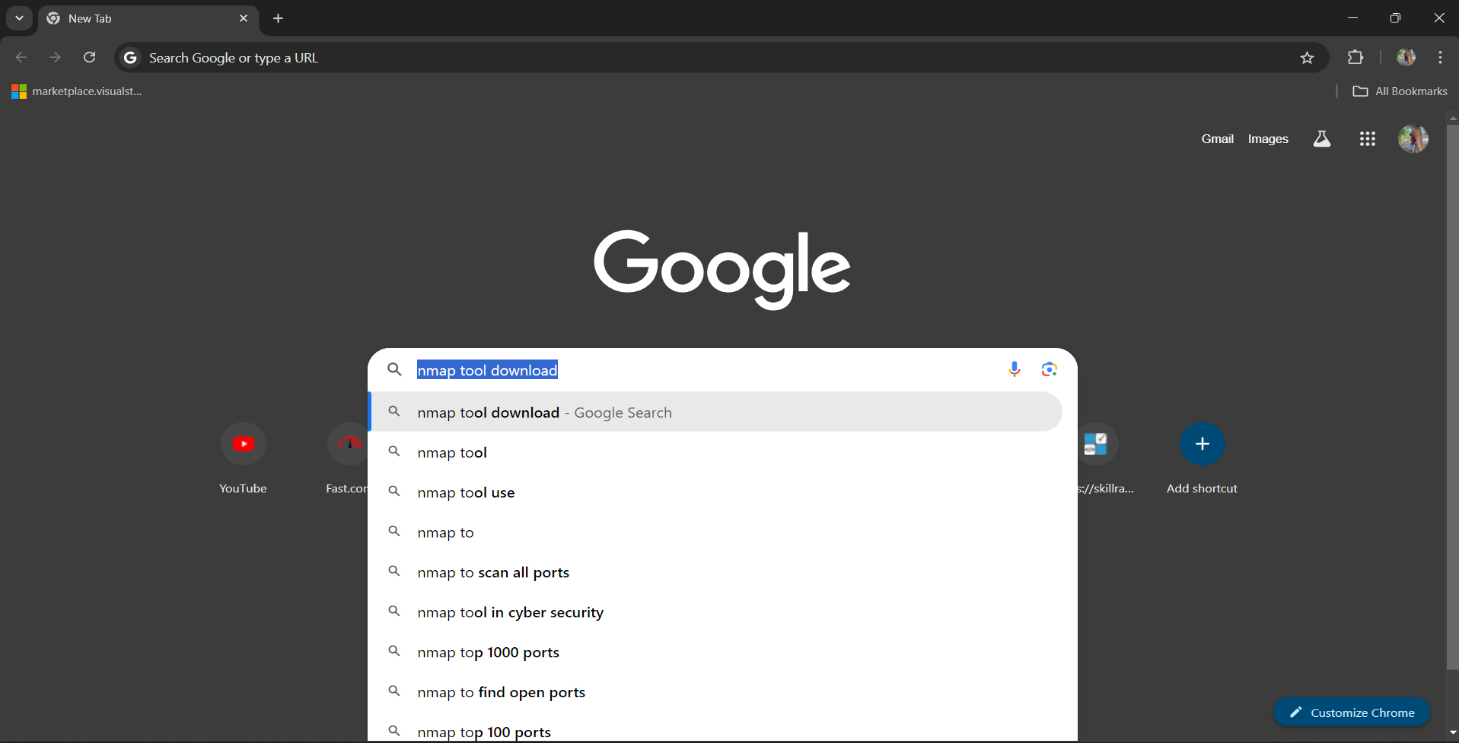
*PORT SCANNING MY OWN SYSYTEM USING* **NMAP**

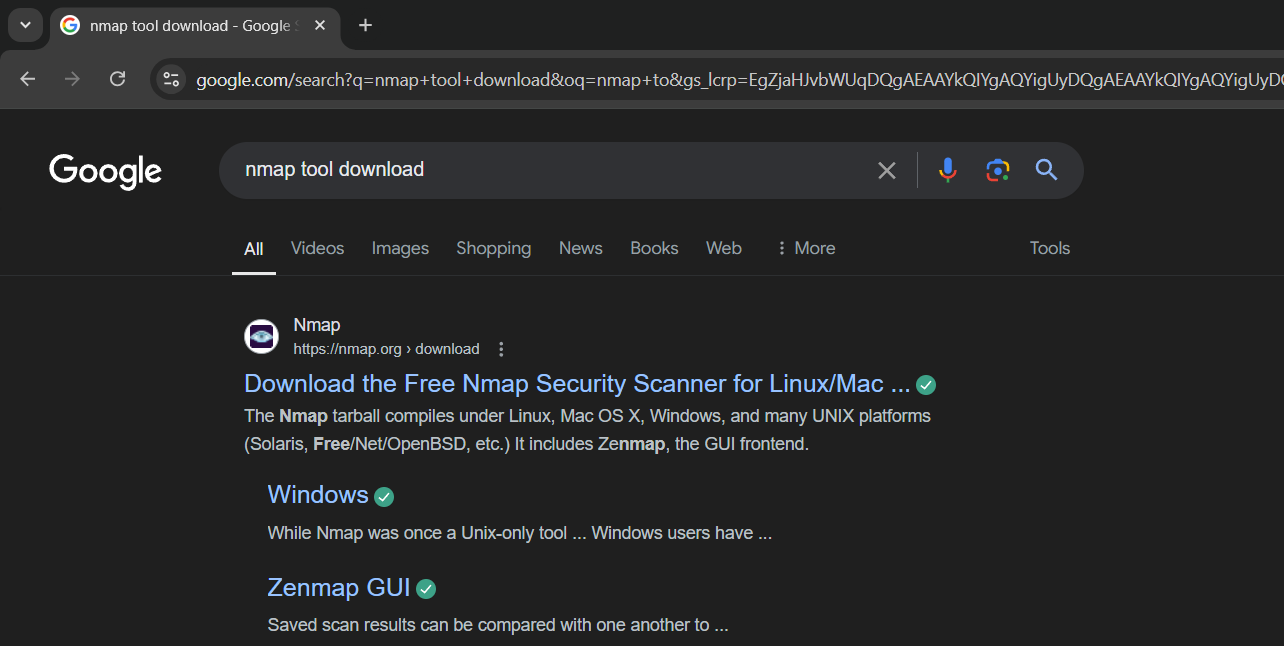
**STEP 1:**

Open a web browser and search for **“Nmap tool download**”.



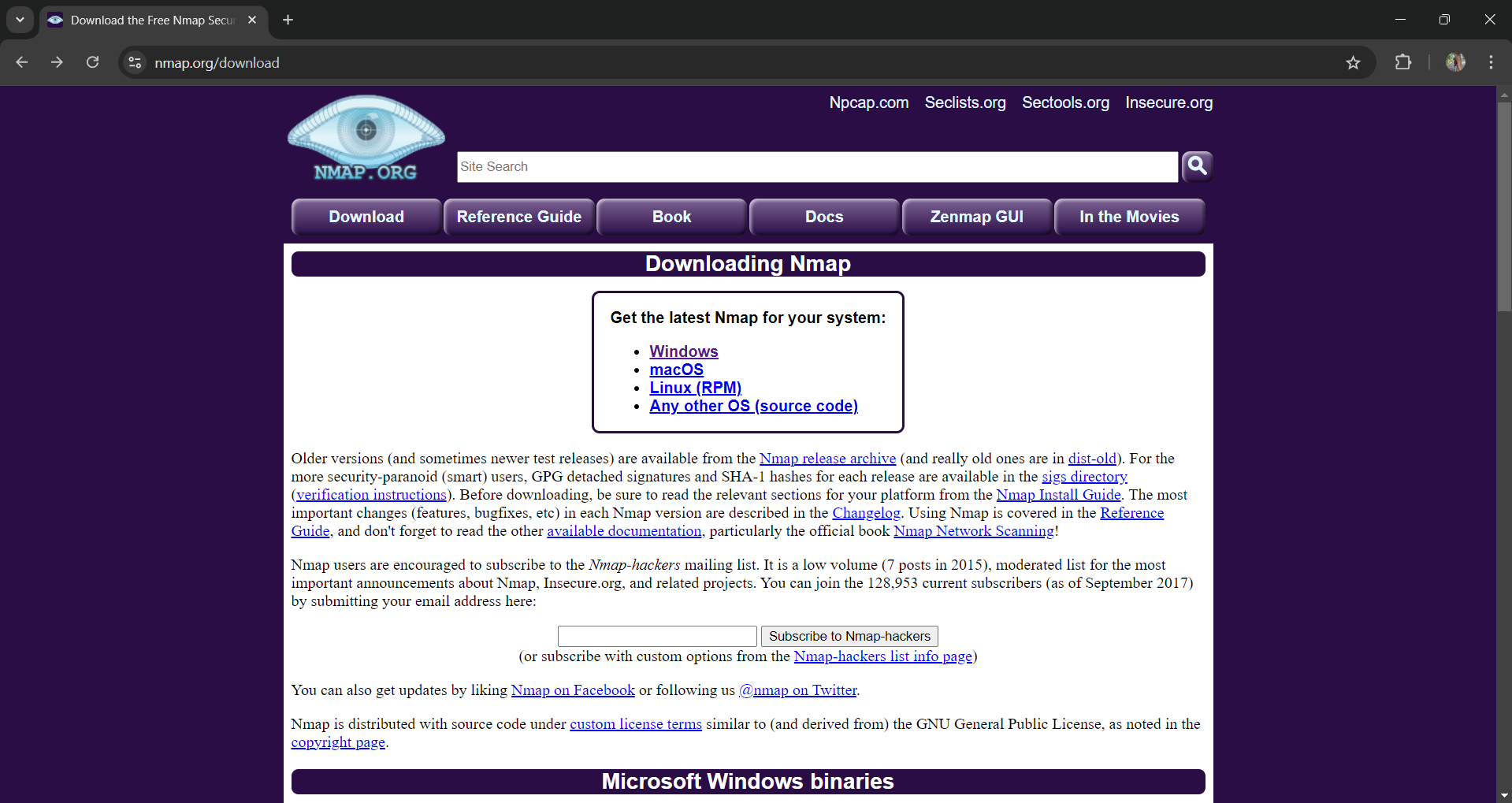
**STEP 2:**

You will see the first link in the search results; click on it.



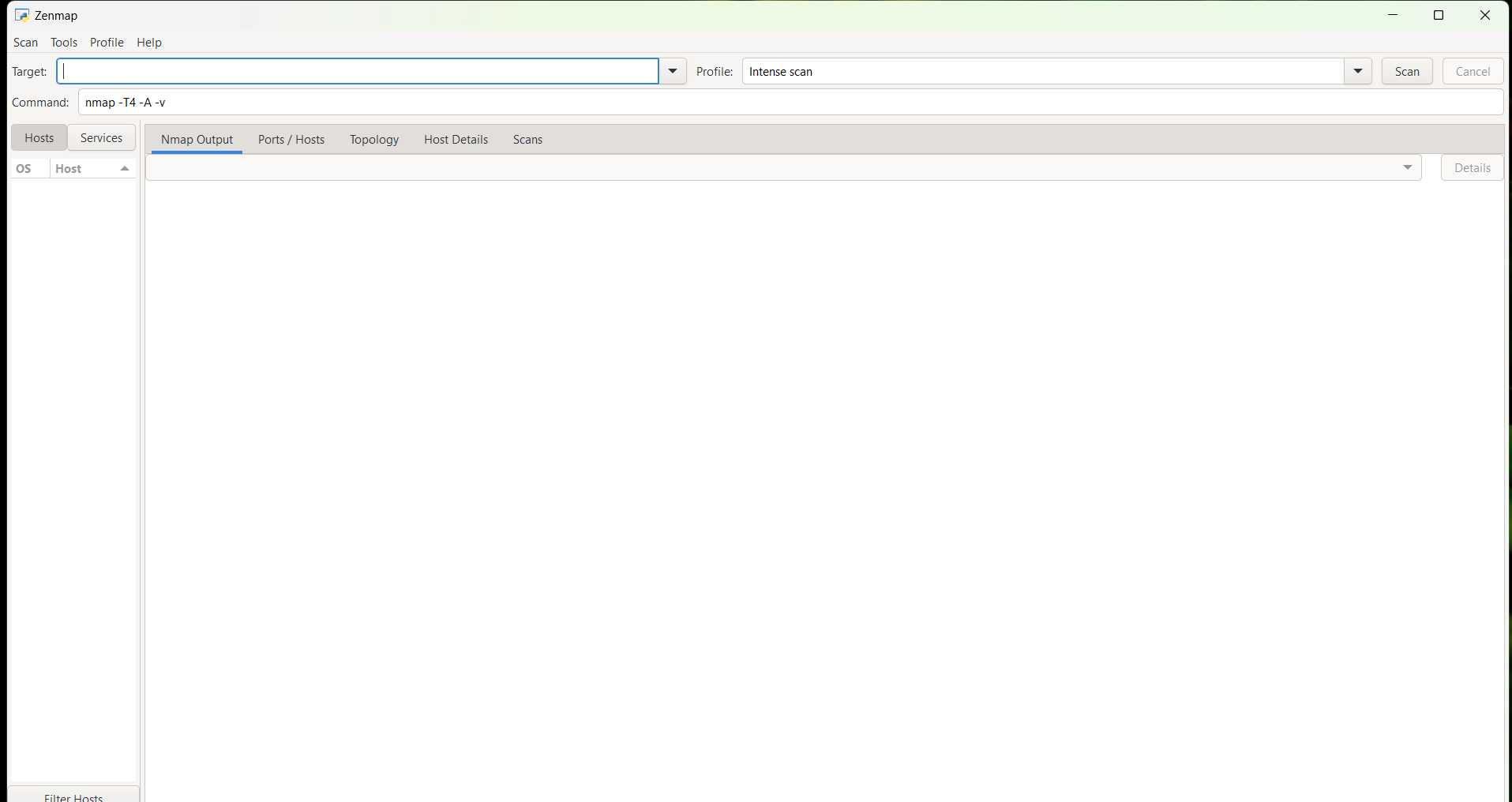
**STEP 3:**

Download the Nmap tool according to your system's operating system, such as Windows, macOS, Linux, etc.



**STEP 4:**

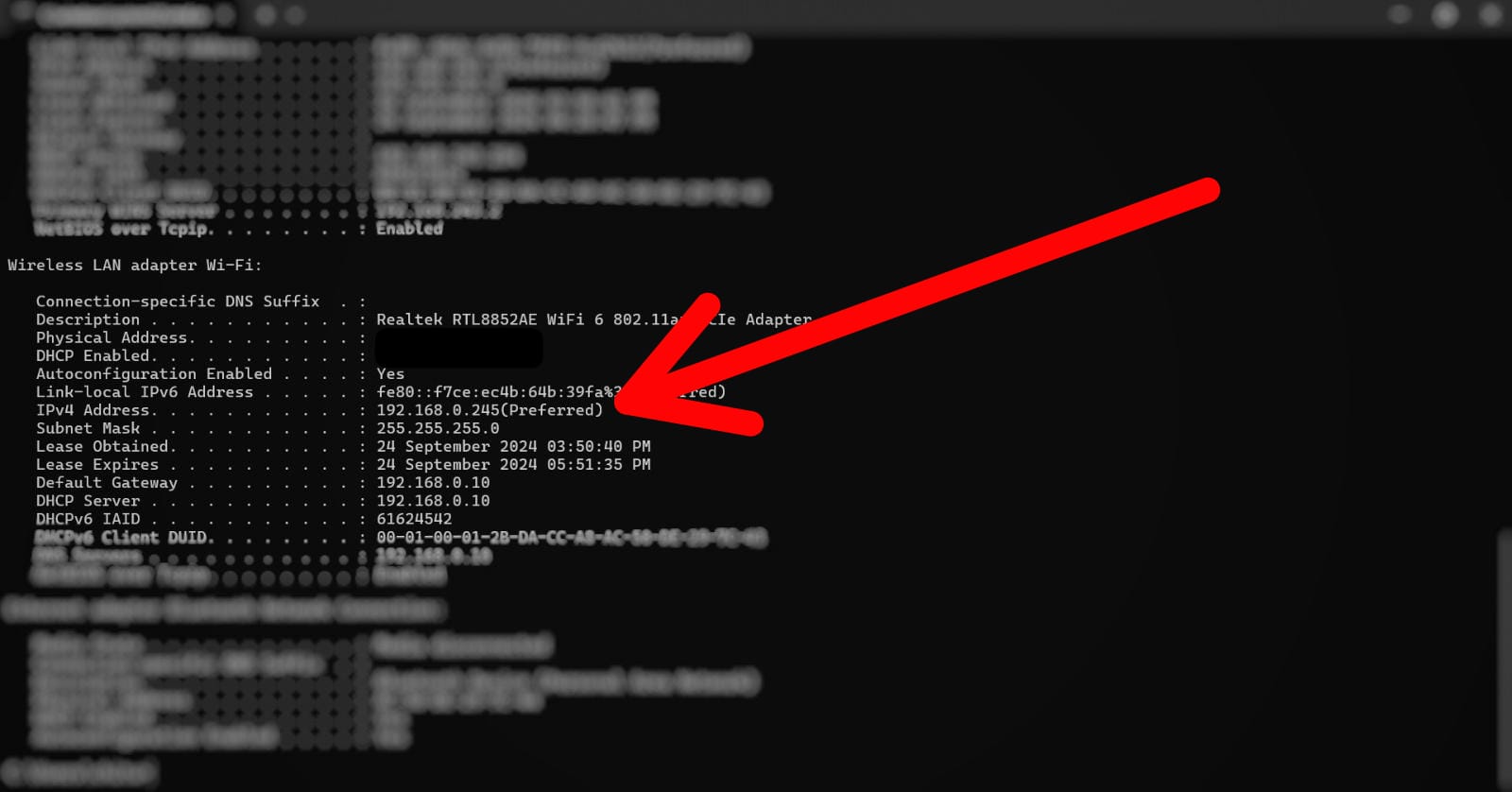
Install the Nmap tool on your system and launch it. Upon opening, you will see an interface similar to the following:



**STEP 5:**

To check the IP address of your system, open the command prompt and run the command: **ipconfig /all**

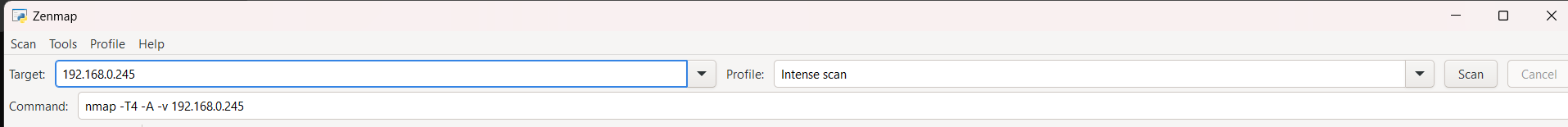
****

****

**Note:** As I am connected to the internet via Wi-Fi, I will check my IP address under the **"Wireless LAN adapter Wi-Fi"** section.

**STEP 6:**

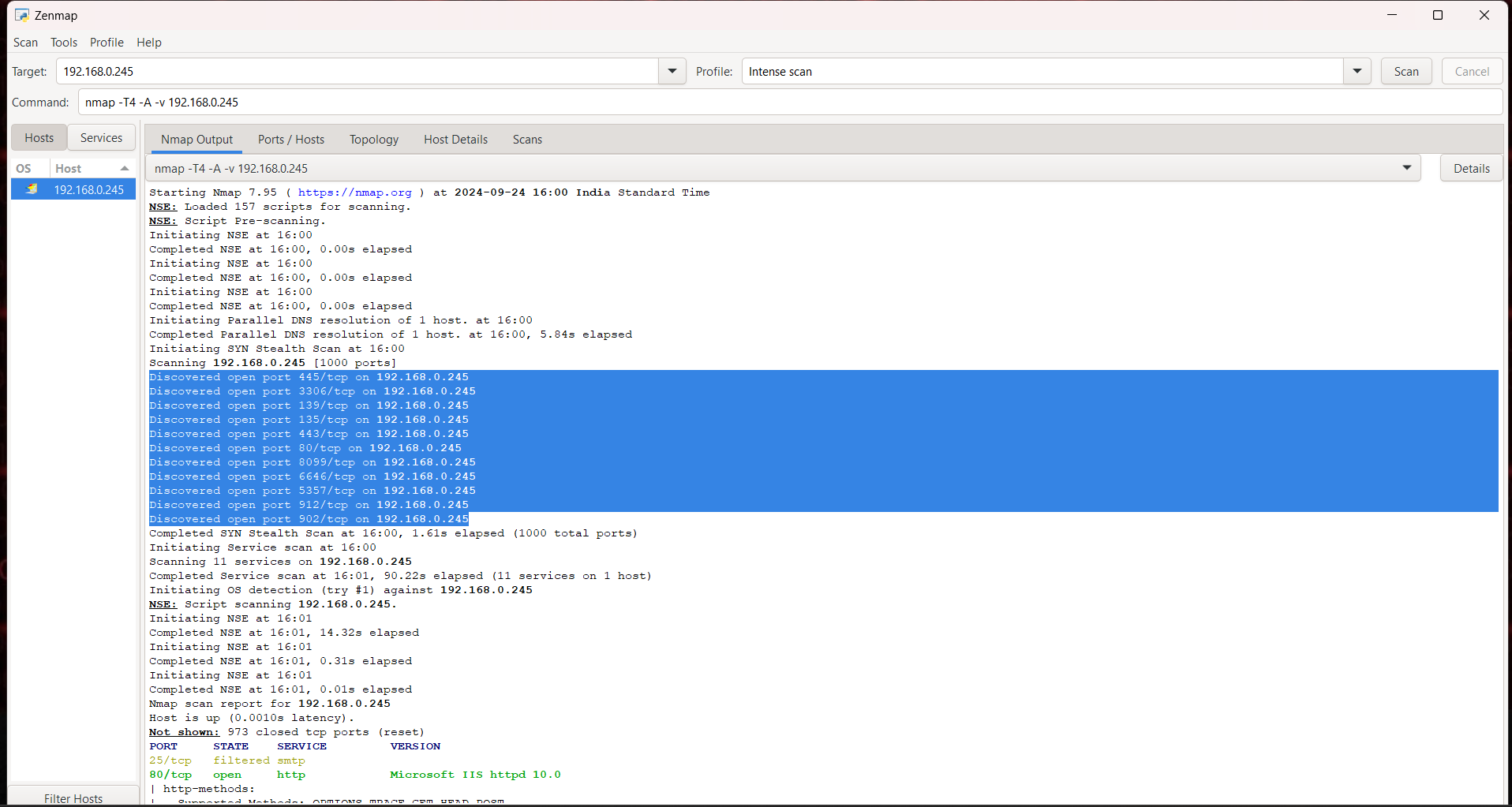
Copy the IP address, open the Nmap tool, and paste it into the **"Target"** section for scanning and analysis.



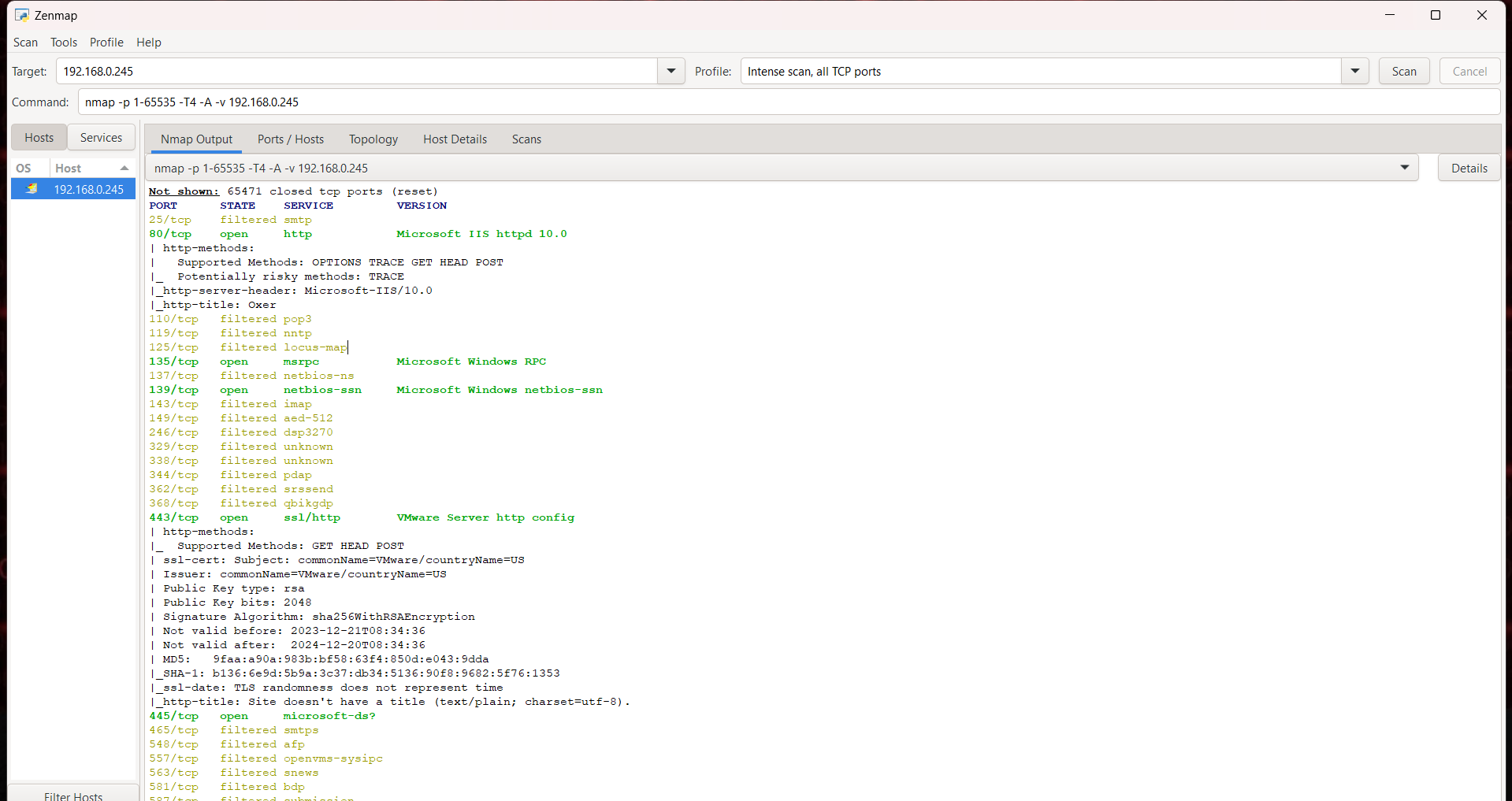
In the **"Profile"** section, select the desired scanning type. I have chosen the default option, **"Intense scan"**. Once selected, click the **"Scan"** button to initiate the scan on my system.

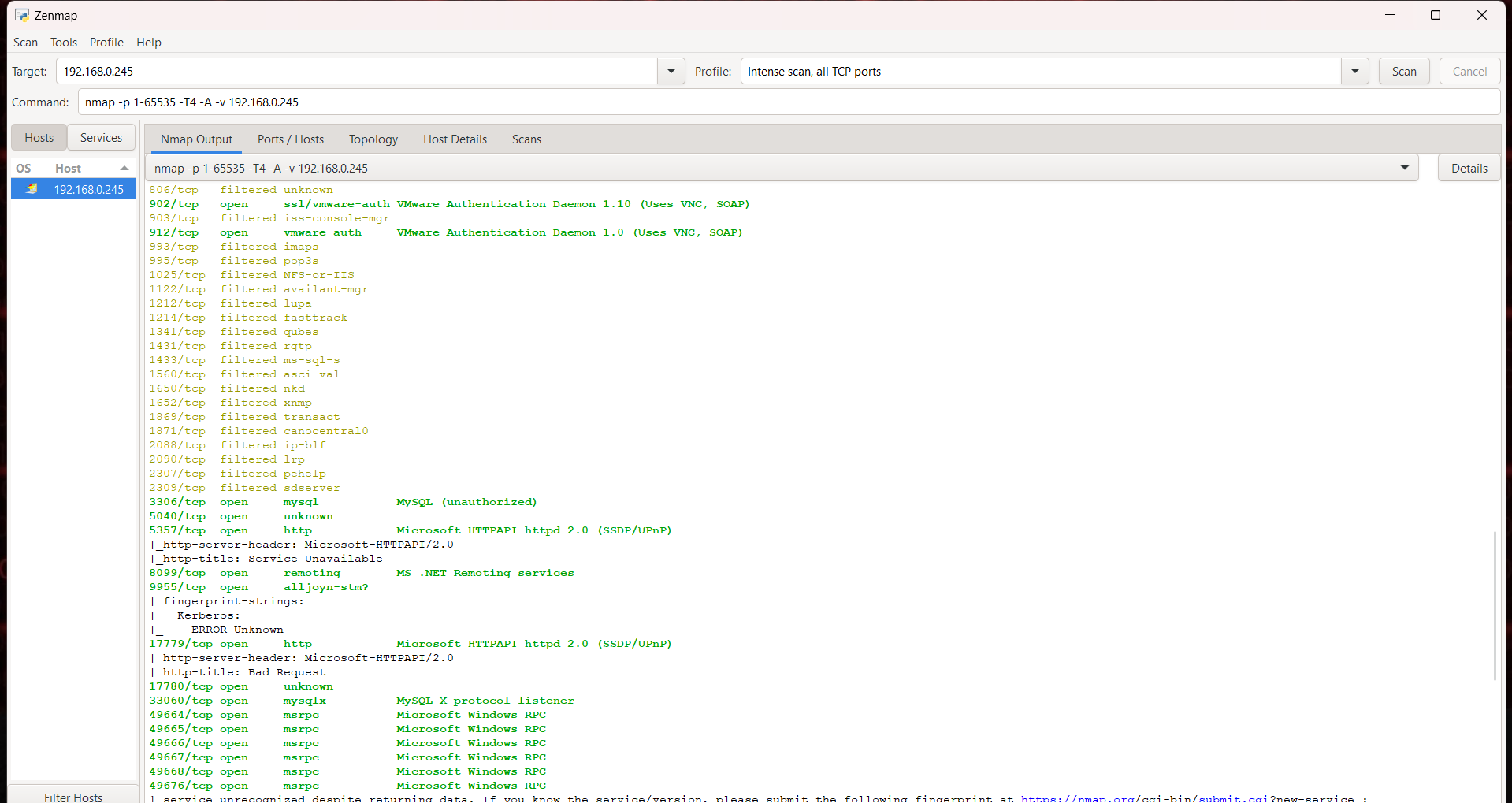
**STEP 8:**

Nmap will automatically scan my system and generate a report displaying the **open port numbers**, along with their **state**, associated **services**, service **versions**, and additional relevant information.



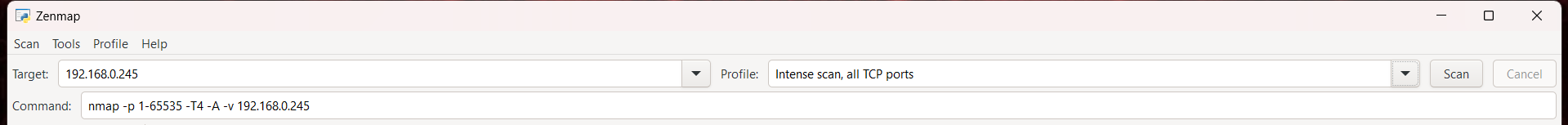
These are the records generated by the Nmap tool.

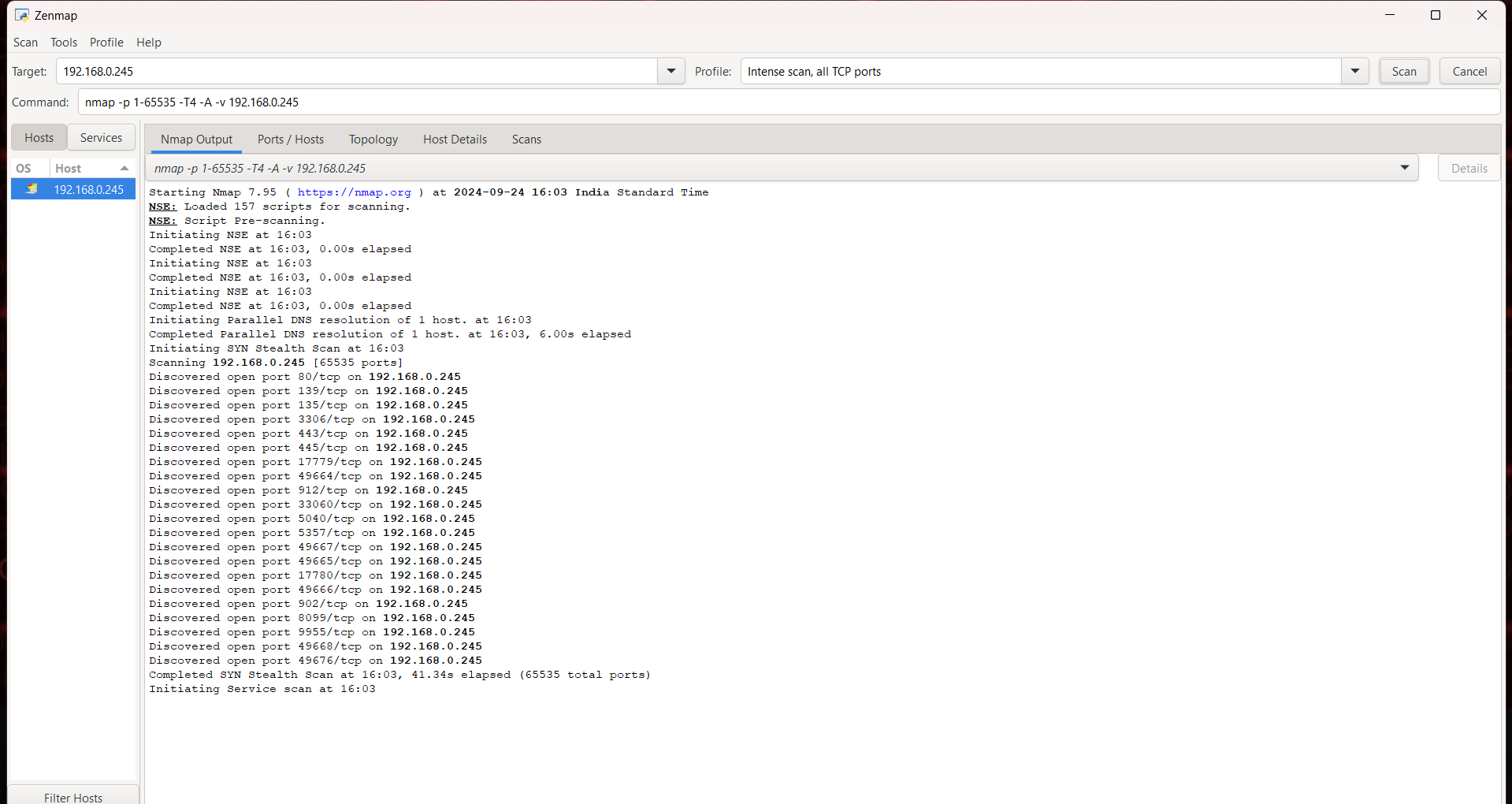


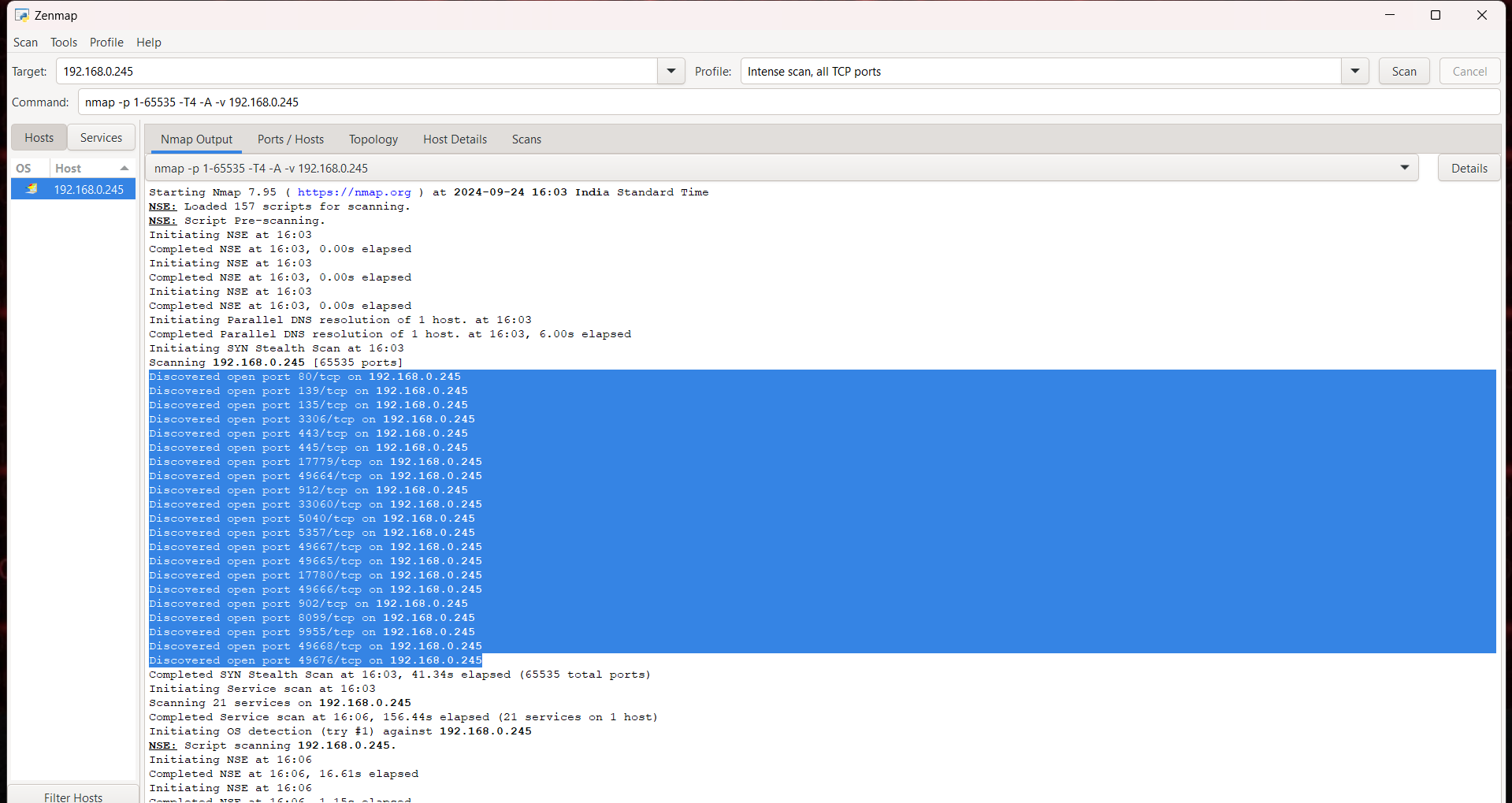


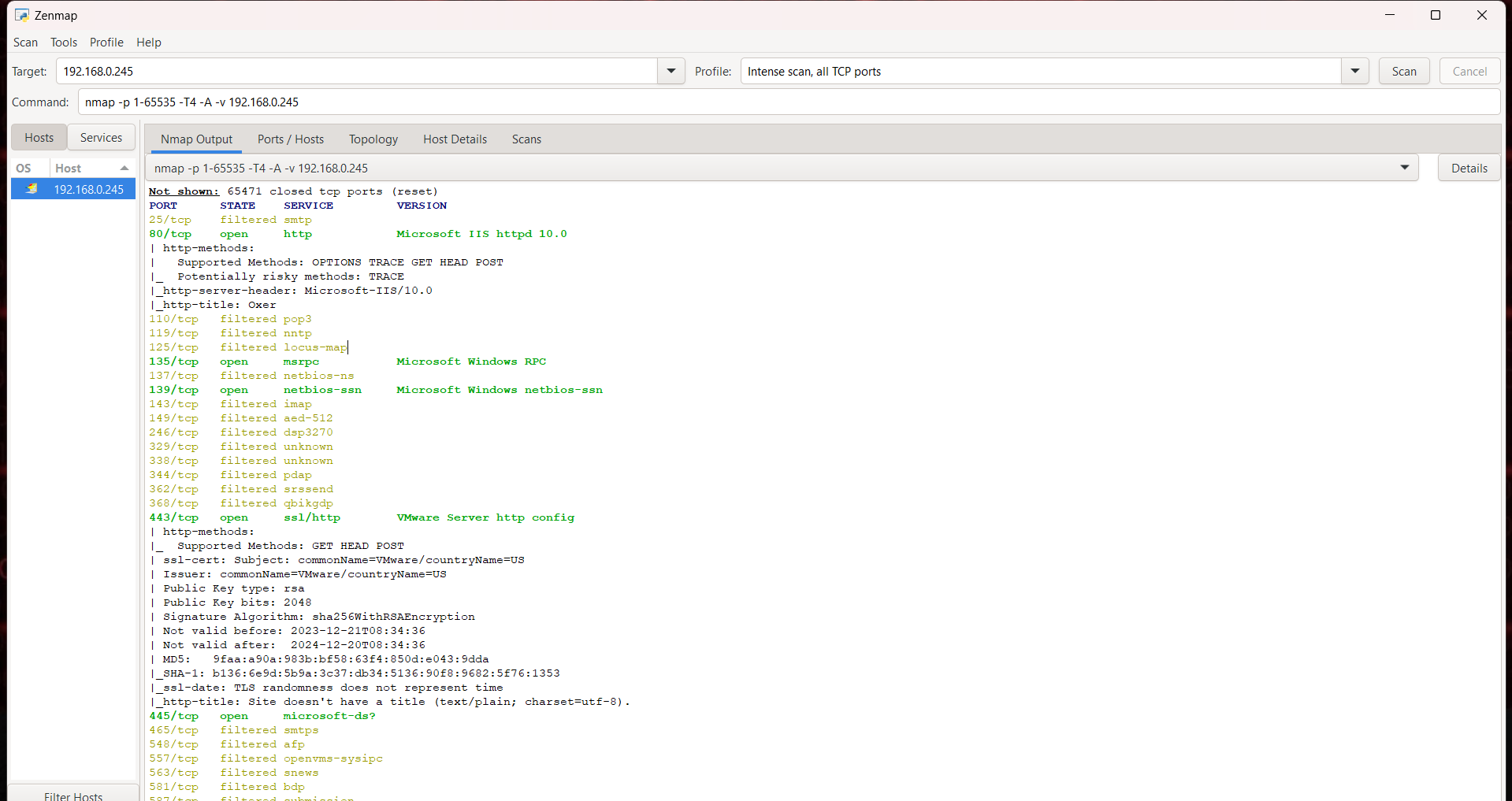
**STEP 9:**

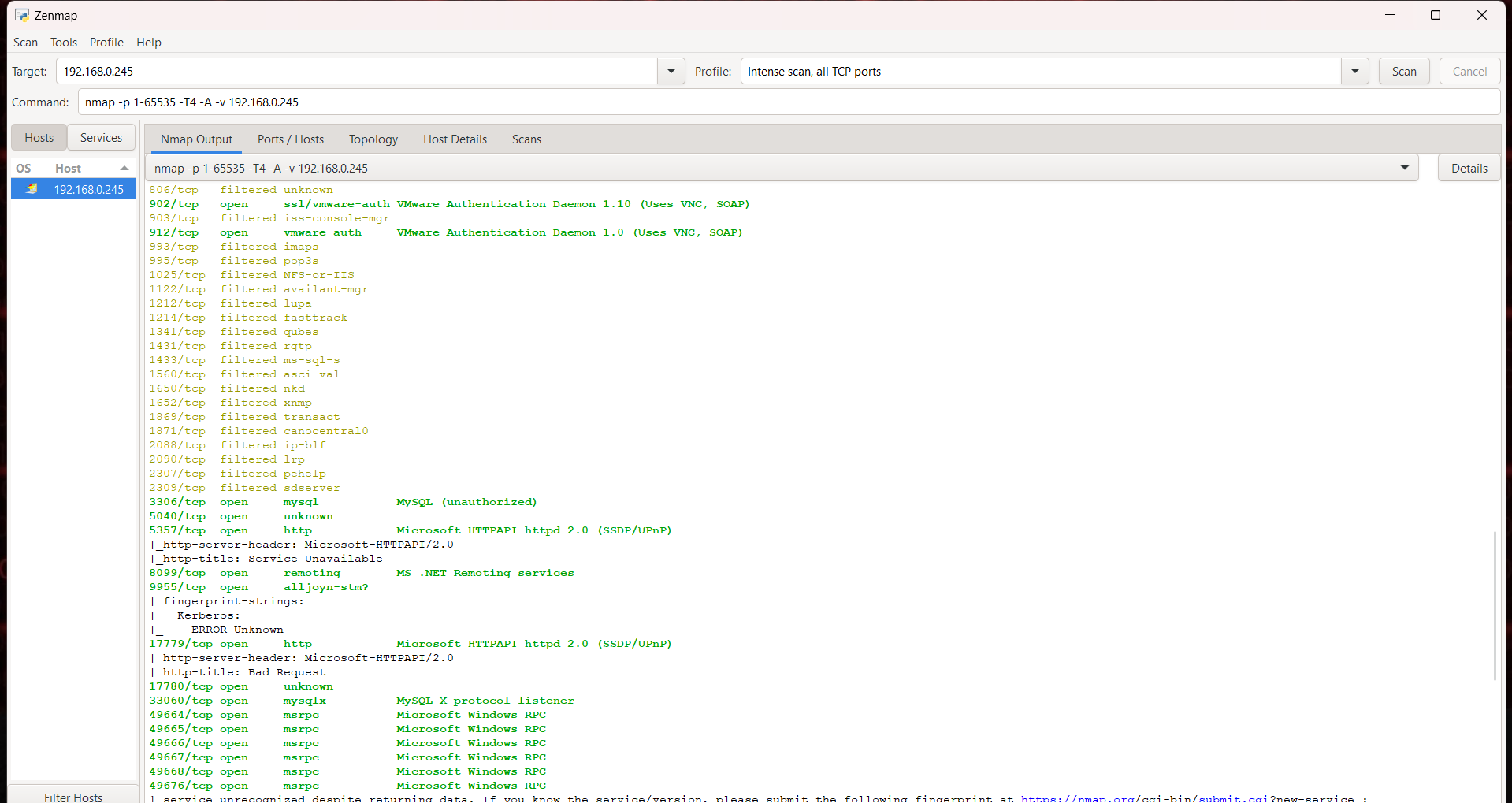
I have also performed a scan using the **"Intense scan, all TCP ports"** option, which provides additional detailed information.











**STEP 10:**

Additionally, Nmap offers features such as viewing only the open ports in the **"Ports/Hosts"** section. You can also visualize the network topology, showing how the local host is connected, in the **"Topology"** section.

