TASK 1 (Day 1)

Installation of Nmap from the official website.

I have used the official website to download the Nmap tool / software for completing the required task.

[Download the Free Nmap Security Scanner for Linux/Mac/Windows](https://nmap.org/download)

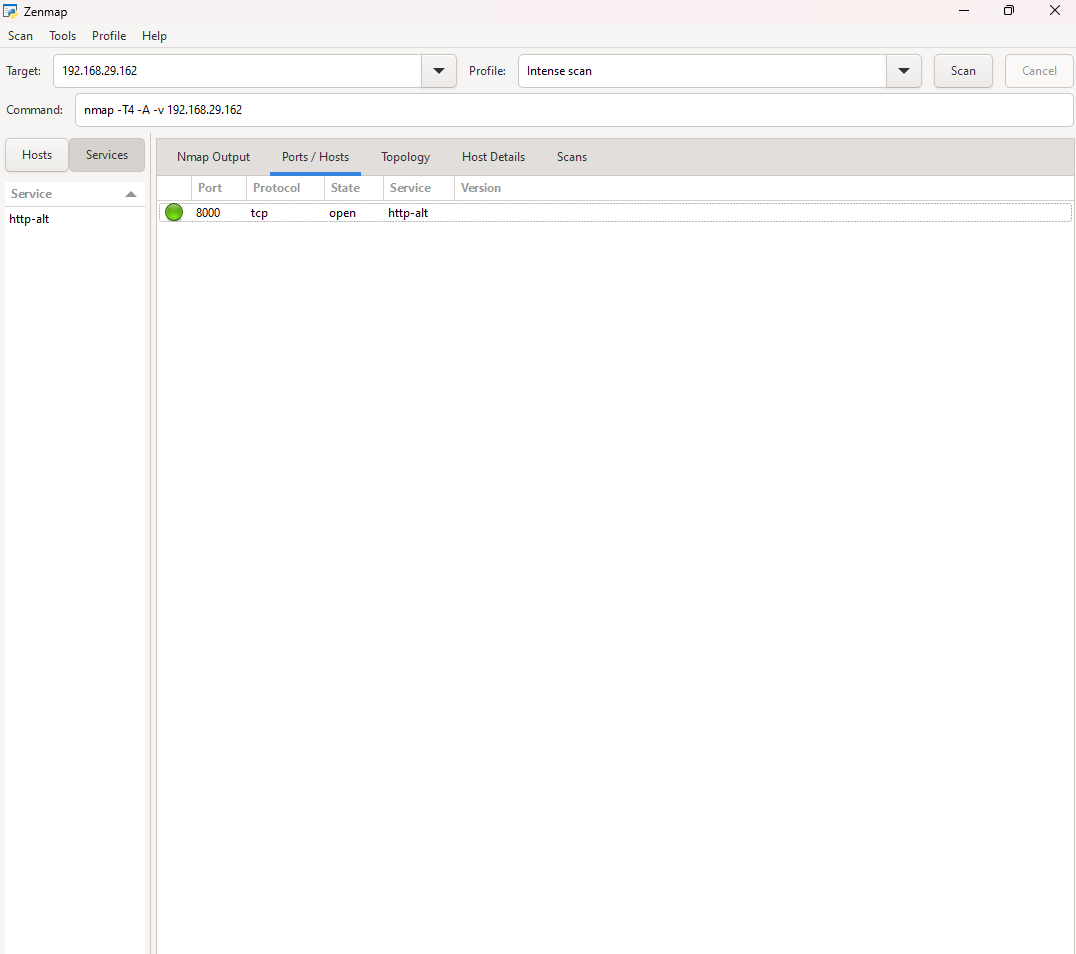
After installation of Nmap on my system, I further configured it and proceeded with the second task.

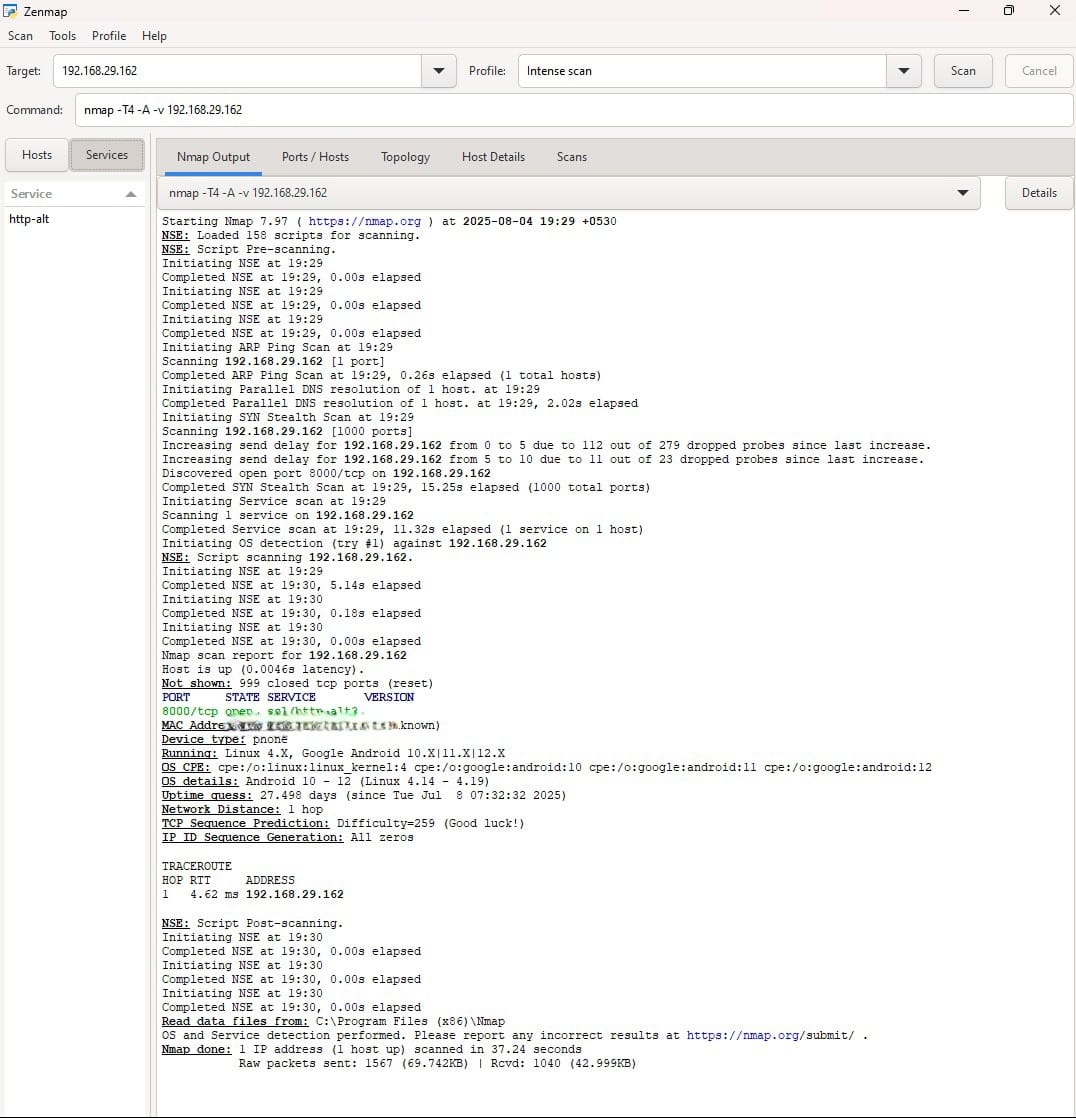
Finding a Local IP

For reference, I have used a Local IP 192.168.29.162

Further, I did an Intense scan for the IP address 192.168.29.162 using the Nmap tool and I found that there was one open port on that particular IP address.

For reference, I have also attached two snaps of the scanned results below.





The image displays the results of an **Nmap Intense Scan** conducted on the IP address **192.168.29.162** using **Zenmap**, a graphical interface for Nmap. Here’s a detailed breakdown of the scan output:

**General Information:**

* The **Nmap version** used is **7.91**.
* The **Intense Scan** profile was selected, which performs a comprehensive examination of the target, including port scanning, OS detection, and version detection.
* The scan results are based on a total of **1000 ports** and include multiple services associated with the target host.

**Key Findings:**

1. **Host Information**:
   * **Host Up**: The target host (IP **192.168.29.162**) is responsive and online.
   * **OS Detection**: The host appears to be running an **Android operating system**. Specifically, versions **10**, **11**, or **12** are identified based on the OS fingerprints and **Linux kernel version 4.14.0 - 4.19**.
   * The scan suggests it is an Android device because it matches specific CPE (Common Platform Enumeration) patterns tied to **Google Android OS**.
2. **Ports and Services**:
   * **Port 8000/tcp**: The only open port detected is **8000/tcp**, which is commonly used for **HTTP-alt** services (alternative HTTP server or custom applications). The service on this port is actively running, but the version details are not explicitly mentioned.
   * No other open ports or services were discovered during the scan.
3. **Network Details**:
   * The scan indicates the device is located on the **local network** with only **1 hop** to reach the target. This suggests the device is in the same network or subnet as the scanning machine.
   * **Traceroute** information was obtained, showing the target’s IP path is direct, confirming it is reachable with minimal network routing.
4. **Operating System Details**:
   * The host is identified as **Android** based on specific system fingerprinting, along with its associated **CPE** details.
   * The **Uptime** of the system is noted as **27,498 days**, a figure suggesting a probable calculation error or a default value in the Nmap report.
5. **TCP Sequence Prediction**:
   * The **TCP Sequence Prediction** test shows a difficulty of **259**, meaning the target's TCP sequence numbers are predicted with this level of difficulty, giving an estimate of how complex it might be for attackers to spoof TCP connections.
   * The result of **TCP Sequence Generation** is marked as **all zeros**, meaning the TCP sequence number generation does not exhibit any randomness, which could be a security concern.
6. **Scan Timing**:
   * The scan completed in **37.24 seconds**, indicating a reasonably fast process for scanning a host within a local network.
   * There were **279 dropped probes** due to network issues, which led to the scan being retried. This is generally not critical but may suggest some packet loss during the scan.
7. **Additional Information**:
   * A message at the bottom of the scan output encourages users to submit any incorrect results to Nmap for further refinement.
   * The scan used **Zenmap**'s graphical interface for easier interpretation of the results, showing the details in a structured format.

Identifying potential security risks from open ports for the IP 192.168.29.162

The Nmap scan shows that the system has an open port (8000/tcp) running the http-alt service. Here's a breakdown of potential security risks associated with open ports and the service revealed by this scan:

### Open Port: ****8000/tcp****

* **Service**: http-alt (Alternative HTTP)
  + Port 8000 is often used for development or non-standard HTTP services. It's commonly associated with web applications, sometimes during testing or as an alternative to the default HTTP port 80.

### Potential Security Risks:

1. **Exposure of Development Environments**: Port 8000 is often used by web developers to test applications. If the service on this port is not properly secured, it could expose unfinished, untested, or vulnerable web applications to attackers.
2. **Unsecured Web Services**: If the service running on port 8000 is a web application, it may have weak or outdated code. Attackers could exploit known vulnerabilities (e.g., Cross-Site Scripting (XSS), SQL Injection, Remote Code Execution (RCE)) to gain unauthorized access.
3. **Lack of Encryption**: If the service on port 8000 is running over plain HTTP (as opposed to HTTPS), it would transmit data in plaintext. Sensitive information could be intercepted in transit, making it vulnerable to man-in-the-middle attacks.
4. **Exposed to External Attacks**: Depending on the system's firewall and network configuration, an open port like 8000 might be exposed to the internet, increasing the attack surface. If the service is improperly configured or vulnerable, attackers could exploit it remotely.

### Recommended Actions:

* **Close unnecessary ports**: If port 8000 is not needed, it should be closed to reduce the attack surface.
* **Firewall configuration**: Ensure that access to port 8000 is restricted using a firewall to limit connections only from trusted IPs.
* **Update and secure the web service**: If the service on port 8000 is a web application, ensure it is patched, and follows secure coding practices (e.g., input validation, secure authentication).
* **Use HTTPS**: If the service is used for web applications, ensure it uses SSL/TLS encryption to protect data in transit.

Running the command nmap -sS 192.168.1.0/24

