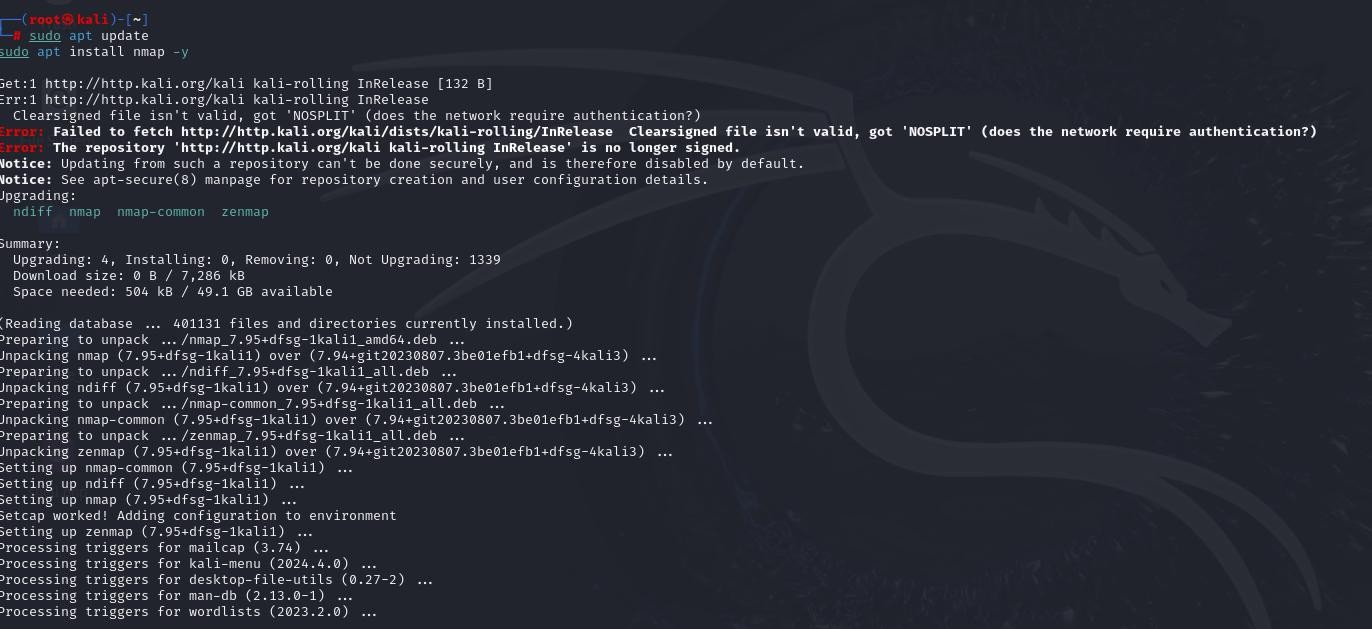
1. **Install Nmap from Official Website**

Kali Linux typically comes with **Nmap pre-installed**. However, to ensure it’s installed or to upgrade it:

To install or update Nmap:

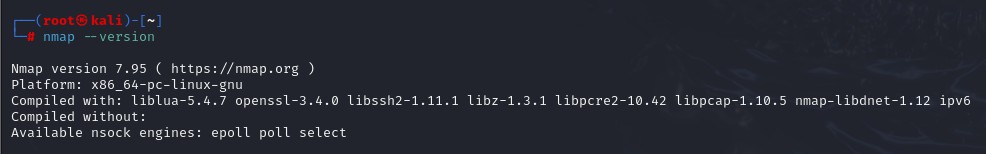
sudo apt update

sudo apt install nmap -y



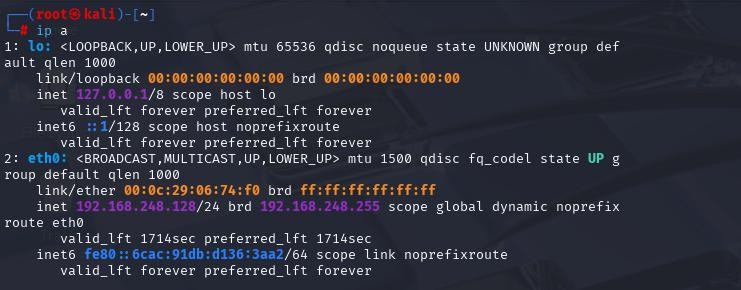
To check if Nmap is installed:

nmap –version



1. **Find Your Local IP Range (e.g., 192.168.1.0/24)**

To scan your local network, you need to determine the IP address and subnet.

Use the following command scan local network: ip a



Active Network Interface (eth0):

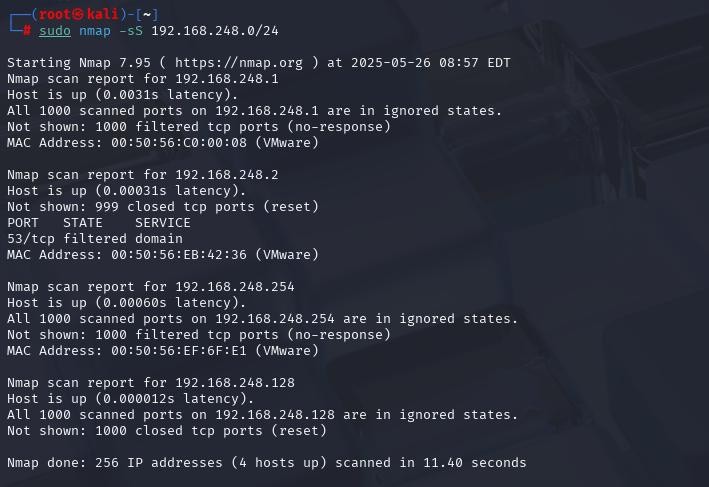
* + **IP Address: 192.168.248.128**
  + **Subnet Mask: /24**
  + **Broadcast Address: 192.168.248.255**
  + **Subnet Range: 192.168.248.0/24**

1. **Run: Nmap -sS, 192.168.248.128/24 to Perform a TCP SYN Scan**

The -sS flag instructs Nmap to perform a **TCP SYN (stealth) scan** which sends SYN packets and observes responses without completing TCP handshakes.

Run the command:

sudo nmap -sS 192.168.248.128/24



This scan identifies:

* + **Live devices** (hosts that respond)
  + **Open TCP ports**
  + **Running services (if identifiable)**

|  |  |  |  |
| --- | --- | --- | --- |
| **IP Address** | **Status** | **Open Ports** | **Notes** |
| 192.168.248.1 | Up | None (filtered) | Host responded, no open port |
| 192.168.248.2 | Up | 53 (filtered) | DNS service, filtered |
| 192.168.248.254 | Up | None (filtered) | Host responded, no open port |
| 192.168.248.128 | Up (Kali) | None (reset) | This is the scanning machine |



Observations

* + Only port 53 (DNS) on 192.168.248.2 was detected, and it is **filtered**.
  + Other hosts had **all ports filtered or reset**, indicating strong firewall rules or inactive services.
  + The scan completed in **11.40 seconds**.

1. **Note Down IP Addresses and Open Ports Found**

From the scan output,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP Address** | **Status** | **Open Ports** | **Service** | **Remarks** |
| **192.168.248.1** | Up | None | — | All 1000 TCP ports filtered |
| **192.168.248.2** | Up | 53/tcp | Filtered (domain) | Likely running DNS service |
| **192.168.248.254** | Up | None | — | All ports filtered |
| **192.168.248.128** | Up | None | — | This is the Kali machine itself |

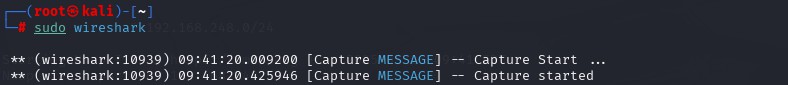
Additional Notes:

* + **192.168.248.2** is the only host with a detected **filtered port (53/tcp)**, which commonly indicates a DNS service—possibly a DNS server or firewall filtering responses.
  + Other hosts responded to the scan but showed **no open ports**, meaning they may be protected by firewalls or not running services on standard TCP ports.
  + **Filtered ports** suggest that a firewall is blocking Nmap from determining the actual state (open/closed).

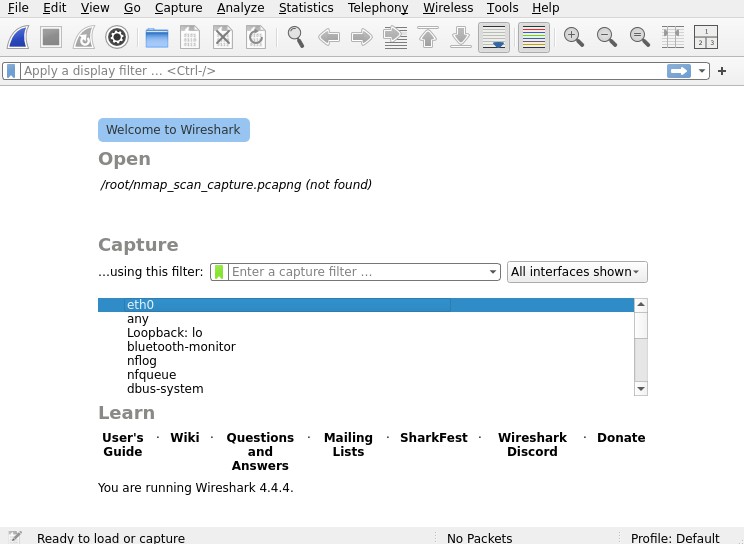
1. **Optionally Analyze Packet Capture with Wireshark**

Wireshark helps visualize the traffic generated during a scan and understand how devices respond.

Steps:

1. **Open Wireshark in Kali: sudo wireshark**
2. **Chooses active interface (likely eth0 for wired or bridged).**

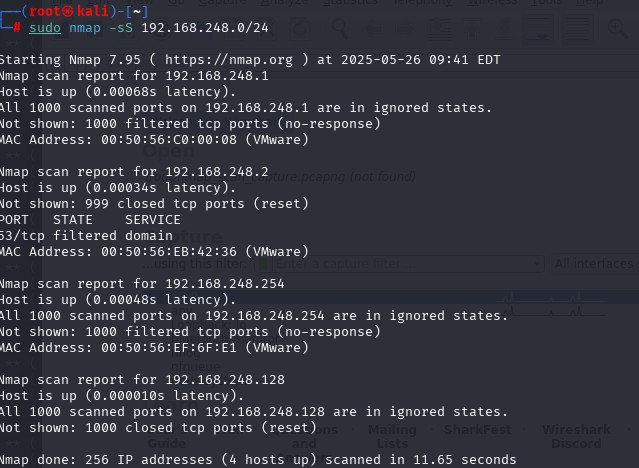




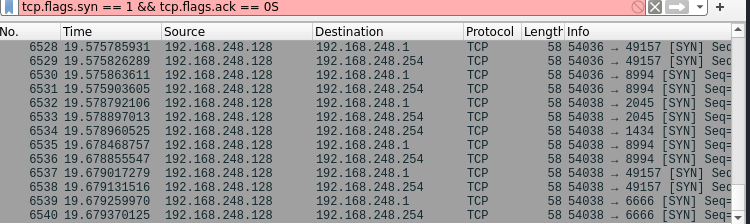
WE HAVE CHOOSES eth0 and then Start capturing before running the Nmap scan.

1. **In a new terminal, run:**

sudo nmap -sS 192.168.248.0/24

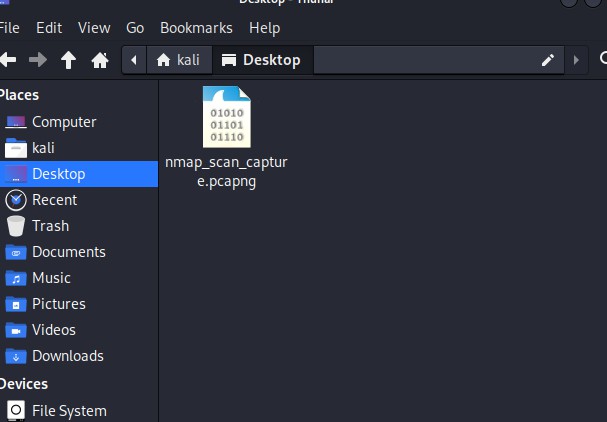


1. **Return to Wireshark and apply this filter to see SYN packets: tcp.flags.syn == 1 && tcp.flags.ack == 0**





1. **Observe That:**
   * **How SYN packets are sent.**
   * **Responses like SYN-ACK (open port) or RST (closed) are received.**
2. **Then Stop the capture and save it:**
   * **File → Save As → nmap\_scan\_capture.pcapng**



1. **Research Common Services Running on Those Ports From scan:**
   * **Only 192.168.248.2 has a detected open (filtered) port:**
     + **Port 53/tcp → Service: domain**
     + **This refers to the DNS (Domain Name System) service. About Port 53:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Port** | **Protocol** | **Service** | **Description** |
| **53** | **TCP/UDP** | **DNS** | **Resolves domain names (e.g., google.com → IP address). Typically runs on DNS servers.** |

1. **Identify Potential Security Risks from Open Ports Risks of Exposing Port 53 (DNS):**

|  |  |
| --- | --- |
| **Threat** | **Description** |
| **DNS Amplification Attacks** | **Can be abused for DDoS attacks by spoofing requests.** |
| **DNS Cache Poisoning** | **Attacker manipulates DNS cache to redirect traffic to malicious sites.** |



|  |  |
| --- | --- |
| **Zone Transfers (if misconfigured)** | **May reveal internal domain details to attackers.** |
| **Information Leakage** | **Poor DNS configuration might expose subdomains or hostnames.** |

Mitigation:

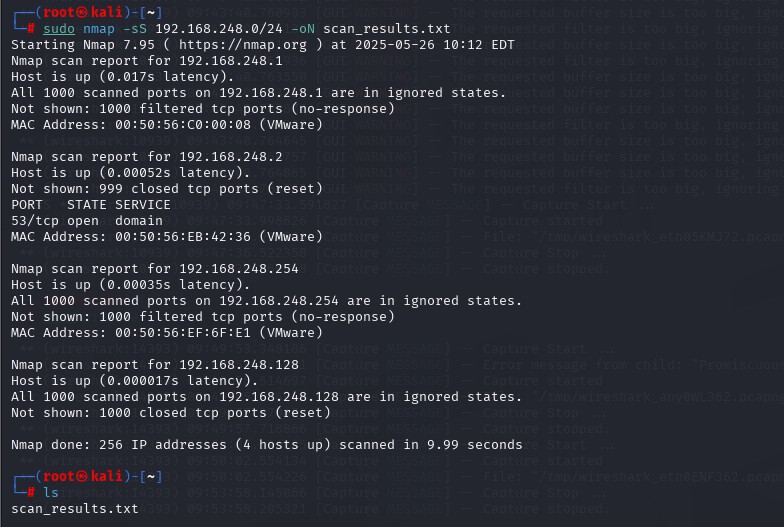
* + **Restrict DNS access to trusted IPs.**
  + **Disable zone transfers unless absolutely necessary.**
  + **Keep DNS server software updated.**
  + **Monitor DNS traffic for anomalies.**

1. **Save Scan Results as a Text or HTML File**

To document your work and submit it as part of your internship or GitHub task, here are two ways to save your Nmap results:

Option 1: Save as Plain Text (.txt)

sudo nmap -sS 192.168.248.0/24 -oN scan\_results.txt

* + **-oN = Normal text format**
  + **Output will be saved as scan\_results.txt in your current directory.**

GitHub Repository Link

All files, documentation, and supporting evidence for Task 1 have been uploaded to the following GitHub repository:

Repository URL:

<https://github.com/CyberSIDH/Task-1->

Repository Contents:



* + README.md – Full explanation of the task
  + scan\_results.txt – Output from the Nmap TCP SYN scan
  + nmap\_scan\_capture.pcapng – Wireshark packet capture file

