

ELEVATE LABS CYBER SECURITY INTERNSHIP

Task-1:

1) 1.Install Nmap from official website.

Used the linux command sudo apt install nmap in my kali linux and downloaded the nmap.

```
(kali@kali)-[~]
$ sudo apt install nmap
nmap is already the newest version (7.95-dfsg-3kali1).
The following packages were automatically installed and are no longer required:
icu-devtools libgeos3.12.0 liblibfsgs0 libpython3.12-stdlib python3-aioclient python3-packaging-whl python3-pyview python3-tomlkit ruby-zeitwerk
libflac12t64 libglapi-mesa libpoppler145 libpython3.12t64 python3-dunamai python3-poetry-dynamic-versioning python3-requests-ntlm python3-wheel-whl sphinx-rtd-theme-common
libfuse3-3 libicu-dev libpython3.12-minimal libutempter0 python3-nfsclient python3-pyinstaller-hooks-contrib python3-setproctitle python3.12-tk strongswan
Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 7
(kali@kali)-[~]
$
```

2.Find your local IP range

```
(kali@kali)-[~]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b4:a1:05 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 369sec preferred_lft 369sec
    inet6 fe80::a823:3ffe:2b42:bcb7/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(kali@kali)-[~]
$
```

Here I can find my ip address as 10.0.2.5 with the subnet /24. Now I am scanning this in the nmap using the command sudo nmap -sn 10.0.2.5/24 to perform ping scan without a port scan

```
(kali㉿kali)-[~]  
$ sudo nmap -sn 10.0.2.5/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 11:43 IST  
Nmap scan report for 10.0.2.1  
Host is up (0.00021s latency).  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
Nmap scan report for 10.0.2.2  
Host is up (0.00017s latency).  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
Nmap scan report for 10.0.2.3  
Host is up (0.00064s latency).  
MAC Address: 08:00:27:C8:A0:19 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Nmap scan report for 10.0.2.5  
Host is up.  
Nmap done: 256 IP addresses (4 hosts up) scanned in 4.62 seconds
```

```
(kali㉿kali)-[~]  
$
```

3.Run: `nmap -sS 10.0.2.5/24` to perform TCP SYN scan.

```
(kali㉿kali)-[~]  
$ nmap -sS 10.0.2.5/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 11:46 IST  
Nmap scan report for 10.0.2.1  
Host is up (0.00073s latency).  
Not shown: 999 closed tcp ports (reset)  
PORT      STATE SERVICE  
53/tcp    open  domain  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
  
Nmap scan report for 10.0.2.2  
Host is up (0.0011s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
135/tcp   open  msrpc  
445/tcp   open  microsoft-ds  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
  
Nmap scan report for 10.0.2.3  
Host is up (0.00056s latency).  
All 1000 scanned ports on 10.0.2.3 are in ignored states.  
Not shown: 1000 filtered tcp ports (proto-unreach)  
MAC Address: 08:00:27:C8:A0:19 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 10.0.2.5  
Host is up (0.0000020s latency).  
All 1000 scanned ports on 10.0.2.5 are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 11.57 seconds
```

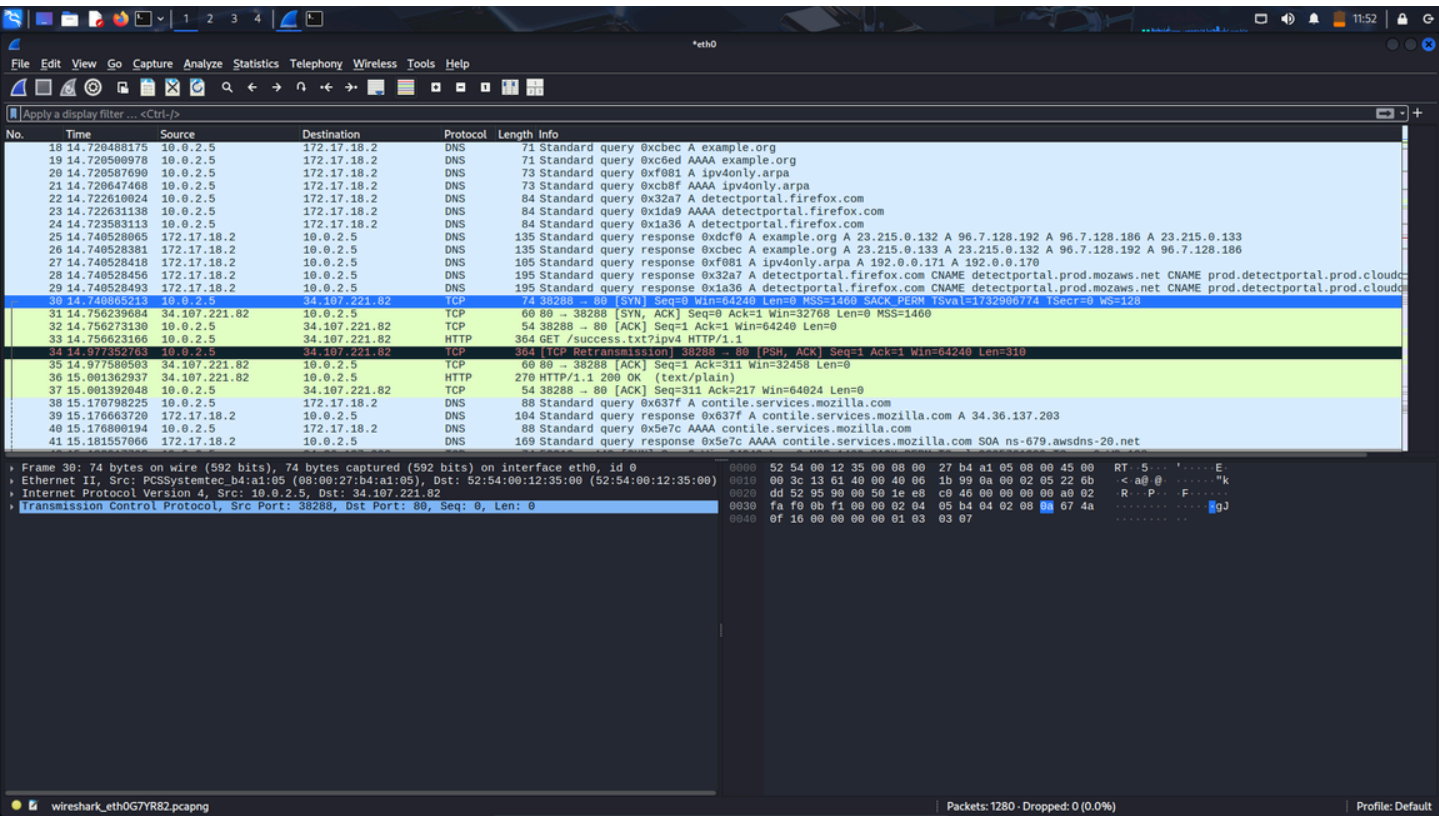
```
(kali㉿kali)-[~]  
$
```

4.Note down IP addresses and open ports found.

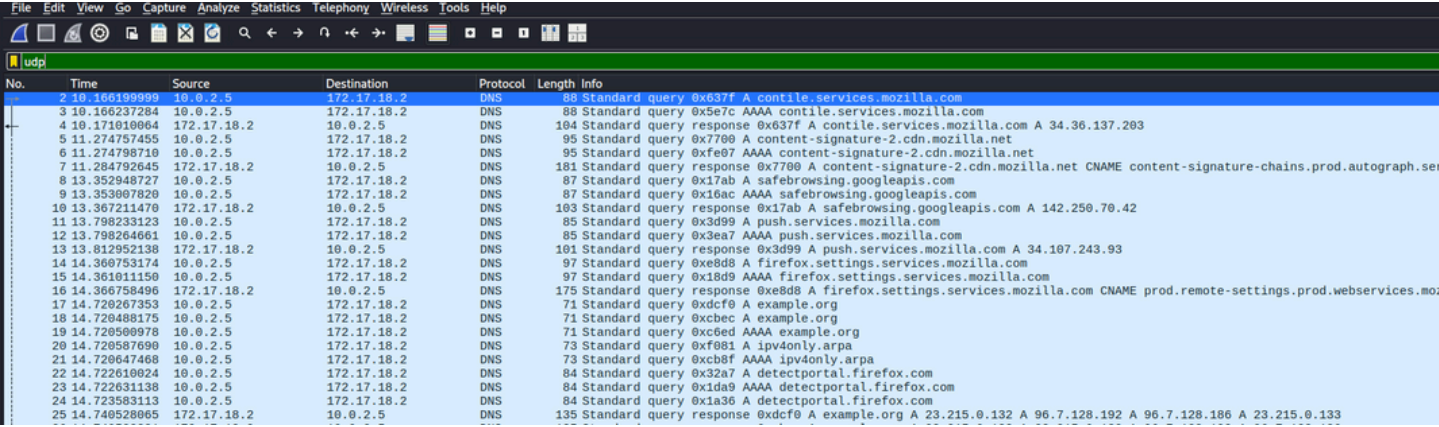
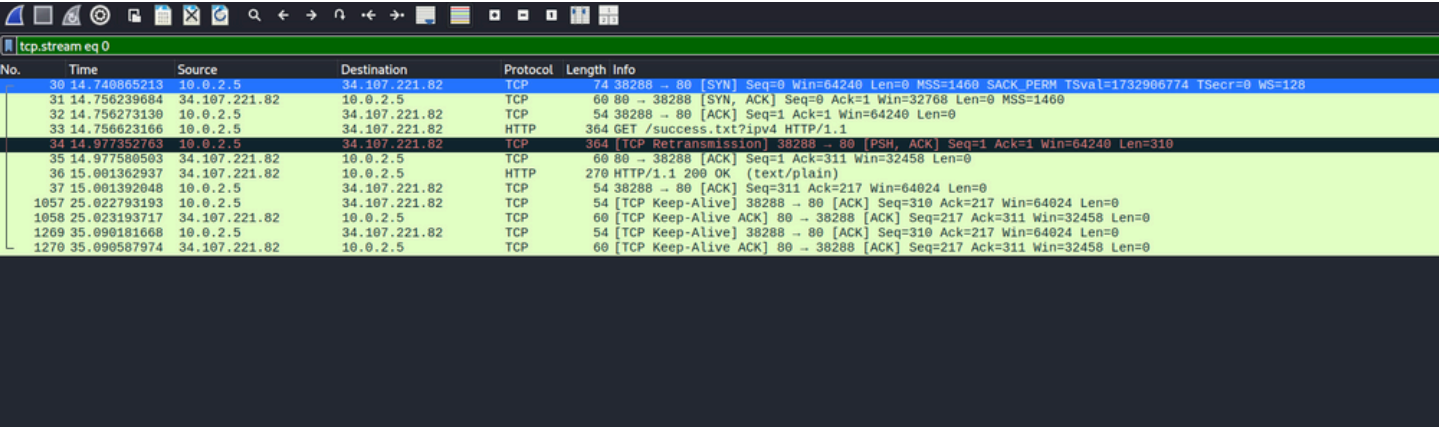
The IP addresses of the open ports found are 10.0.2.1 (1 open port) and 10.0.2.2 (3 open ports)

5.Optionally analyze packet capture with Wireshark.

Captured the live traffic through wireshark



Analysing the traffic using some of the available filters.



6.Research common services running on those ports.

Port	Service	Purpose
135/tcp	MSRPC	Enables communication between Windows applications and services over a network
445/tcp	Microsoft-DS (SMB)	Supports file sharing, printer sharing, and network resource access on Windows systems
3306/tcp	MySQL	Handles connections to MySQL databases for querying, updating, and managing data
53/tcp	DNS (TCP)	Resolves domain names to IP addresses and supports DNS zone transfers and large queries

7. Identify potential security risks from open ports.

Port	Service	Potential Security Risks
135/tcp	MSRPC	- Target of Windows vulnerabilities and exploits- Can be used for remote code execution or lateral movement
445/tcp	Microsoft-DS (SMB)	- Common in ransomware attacks (e.g., WannaCry)- Allows unauthorized file access or code execution
3306/tcp	MySQL	- Exposes database to brute-force or injection attacks- May leak sensitive data if not secured
53/tcp	DNS (TCP)	- Can be abused for DNS tunneling and data exfiltration- Vulnerable to spoofing or cache poisoning if misconfigured

8. Save scan results as a text or HTML file.


```

(kali㉿kali)-[~]
$ nmap -sS 10.0.2.5/24 -oN scan_results.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 12:11 IST
Stats: 0:00:02 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.28% done
Stats: 0:00:02 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.68% done
Stats: 0:00:02 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 5.60% done; ETC: 12:11 (0:00:00 remaining)
Stats: 0:00:02 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 13.93% done; ETC: 12:11 (0:00:00 remaining)
Stats: 0:00:02 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 23.93% done; ETC: 12:11 (0:00:00 remaining)
Stats: 0:00:03 elapsed; 252 hosts completed (3 up), 3 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 66.93% done; ETC: 12:11 (0:00:00 remaining)
Nmap scan report for 10.0.2.1
Host is up (0.00067s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0020s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
8009/tcp  open  ajp13
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.000049s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:C8:A0:19 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.5
Host is up (0.0000020s latency).
All 1000 scanned ports on 10.0.2.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 16.64 seconds

(kali㉿kali)-[~]
$

```

Here this result is saved as scan_results.txt file.