Task 1 — Local Network Port Scan

********** Author: Rohit Madhav Sabale**********

Executive Summary:-

This report documents the results of Task 1 — a local network port scan using Nmap. Scans performed: host discovery (-sn), SYN scan (-sS), and service/version detection (-sV). Three hosts were discovered on the 10.0.2.0/24 network and their results are summarized below.

Environment & Tools:-

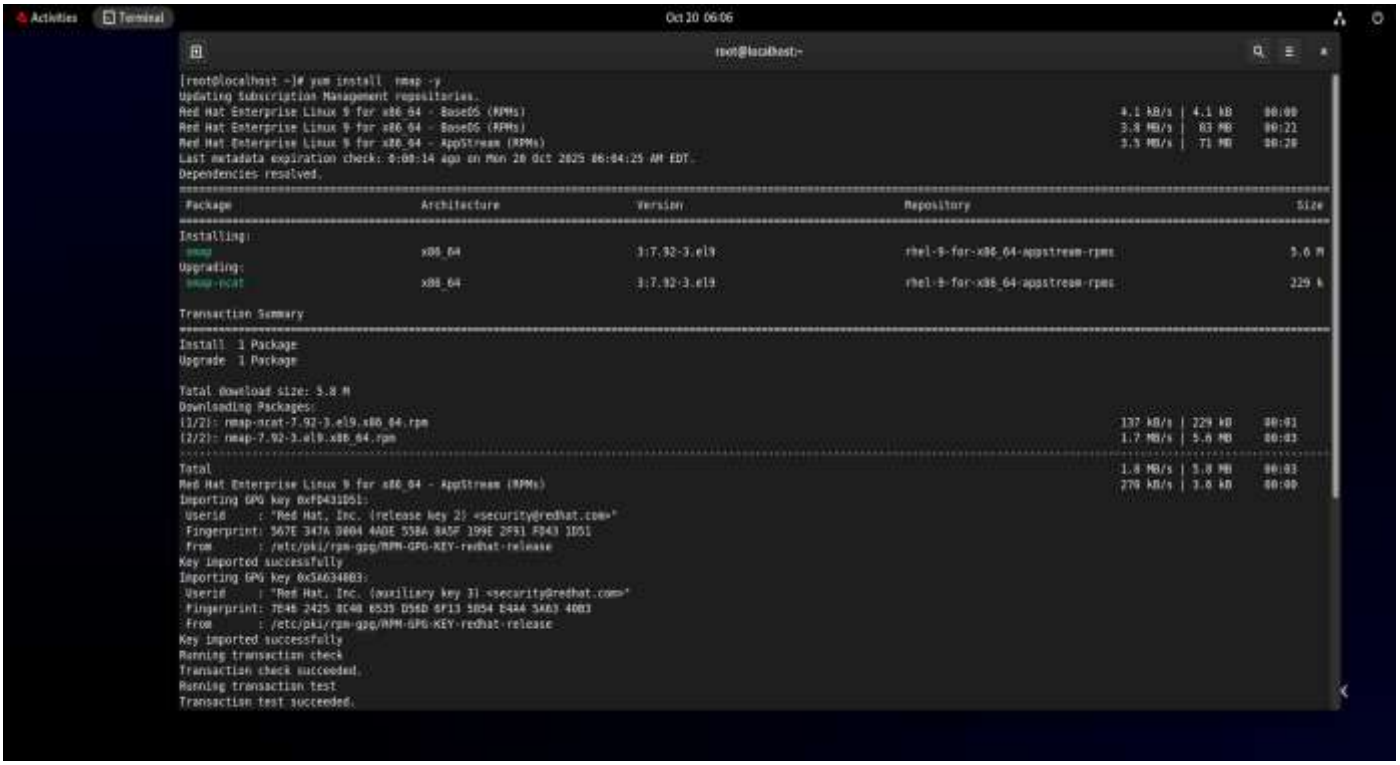
Scanner host: 10.0.2.15
Network scanned: 10.0.2.0/24
Tools: Nmap 7.92; (optional) Wireshark/tcpdump for captures.

Methodology:-

Commands executed (as provided):

- nmap -sn -oN host_discovey.txt 10.0.2.0/24
- nmap -sS -oA nmap_all_output.xml 10.0.2.0/24
- nmap -sS -sV -oN nmap_srv.txt 10.0.2.0/24

Nmap install:-



Local Ip Range :-

```
Activities   Terminal                    Oct 20 17:49
                                         root@localhost:~
[root@localhost ~]# ip route
default via 10.67.84.76 dev enp0s3 proto dhcp metric 100
10.67.84.0/24 dev enp0s3 proto kernel scope link src 10.67.84.232 metric 100
^Coot@localhost ~]# yum install ls ^C
[root@localhost ~]# yum install libxslt -y
Updating Subscription Management repositories.
^CKeyboardInterrupt: Terminated.
[root@localhost ~]# yum install libxslt -y
Updating Subscription Management repositories.
Last metadata expiration check: 0:10:29 ago on Monday 20 October 2025 05:38:42 PM.
Package libxslt-1.1.34-9.el9.x86_64 is already installed.
Dependencies resolved.
================================================================================================================================
 Package                    Architecture            Version                         Repository                              Size
================================================================================================================================
Upgrading:
 libxslt                    x86_64                  1.1.34-13.el9_6                 rhel-9-for-x86_64-appstream-rpms        245 k

Transaction Summary
================================================================================================================================
Upgrade  1 Package

Total download size: 245 k
Downloading Packages:
libxslt-1.1.34-13.el9_6.x86_64.rpm                                                      148 kB/s | 245 kB     00:01
--------------------------------------------------------------------------------------------------------------------------------
Total                                                                                   147 kB/s | 245 kB     00:01
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                                                                      1/1
  Upgrading        : libxslt-1.1.34-13.el9_6.x86_64                                                                       1/2
  Cleanup          : libxslt-1.1.34-9.el9.x86_64                                                                          2/2
  Running scriptlet: libxslt-1.1.34-9.el9.x86_64                                                                          2/2
  Verifying        : libxslt-1.1.34-13.el9_6.x86_64                                                                       1/2
  Verifying        : libxslt-1.1.34-9.el9.x86_64                                                                          2/2
```

Host_Discovery.txt:-

```
Activities   Terminal                    Oct 20 18:03
                                         root@localhost:~
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
| dns-nsid:
|_  bind.version: dnsmasq-2.51
MAC Address: 52:55:0A:00:02:03 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|printer|switch
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (97%), Samsung embedded (90%), Dell embedded (89%), Wind River VxWorks (89%), Bay Networks emb
edded (89%), Xerox embedded (89%), Allied Telesyn embedded (88%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:samsung:clp-315w cpe:/h:dell:1815dn cpe:/o:windriver:vxworks cpe:/h:baynetworks:baystack_450
 cpe:/h:xerox:workcentre_4150 cpe:/h:alliedtelesyn:at-9006
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (97%), Samsung CLP-315W printer (90%), Dell 1815dn printer (89%), VxWo
rks (89%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (89%), Xerox WorkCentre 4150 printer (89%), Samsung CLP-310N or CLX-3175RW, o
r Xerox Phaser 6110 printer (88%), Allied Telesyn AT-9006SX/SC switch (88%), Samsung CLX-3160FN printer (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   2.33 ms 10.0.2.3

Nmap scan report for 10.0.2.15
Host is up (0.000069s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.7 (protocol 2.0)
| ssh-hostkey:
|   256 fe:e4:d7:f7:8a:10:75:d3:7c:38:a9:92:f9:93:c0:d8 (ECDSA)
|_  256 ed:66:77:ab:ae:0e:1b:9d:07:e9:e5:b5:72:47:ed:5a (ED25519)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 29.97 seconds
[root@localhost ~]#
```

Nmap_output(SYN Scan)(host system ip):-

```
Activities   Terminal                    Oct 20 19:47
                                         root@localhost:~
Nmap scan report for 10.0.2.15
Host is up (0.0000050s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.35 seconds
[root@localhost ~]# ls
anaconda-ks.cfg  Downloads          nmap_aggre.txt            nmap_all_output.xml.xml  nmap_out.txt  Public          Videos
Desktop          host_discovey.txt  nmap_all_output.xml.gnmap  nmap_all.txt             nmap_srv.txt  scan_wire.pcap
Documents        Music              nmap_all_output.xml.nmap   nmap_output.txt          Pictures      Templates
[root@localhost ~]# nmap -sS 10.0.2.15/24  -oA nmap_host_output.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2025-10-20 19:46 IST
Nmap scan report for 10.0.2.2
Host is up (0.00039s latency).
All 1000 scanned ports on 10.0.2.2 are in ignored states.
Not shown: 1000 filtered tcp ports (net-unreach)
MAC Address: 52:55:0A:00:02:02 (Unknown)

Nmap scan report for 10.0.2.3
Host is up (0.00032s latency).
Not shown: 999 filtered tcp ports (net-unreach)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap scan report for 10.0.2.15
Host is up (0.0000050s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.38 seconds
[root@localhost ~]#
```

Nmap_output(SYN Scan)(net_id):-

```
Activities   Terminal                    Oct 20 19:45
                                         root@localhost:~
[root@localhost ~]# ls
anaconda-ks.cfg  Documents  host_discovey.txt  nmap_aggre.txt  nmap_output.txt  nmap_srv.txt  Public          Templates
Desktop          Downloads  Music              nmap_all.txt    nmap_out.txt     Pictures      scan_wire.pcap  Videos
[root@localhost ~]# nmap -sS 10.0.2.0/24  -oA nmap_all_output.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2025-10-20 19:45 IST
Nmap scan report for 10.0.2.2
Host is up (0.00035s latency).
All 1000 scanned ports on 10.0.2.2 are in ignored states.
Not shown: 1000 filtered tcp ports (net-unreach)
MAC Address: 52:55:0A:00:02:02 (Unknown)

Nmap scan report for 10.0.2.3
Host is up (0.00035s latency).
Not shown: 999 filtered tcp ports (net-unreach)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap scan report for 10.0.2.15
Host is up (0.0000050s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.35 seconds
[root@localhost ~]# ls
anaconda-ks.cfg  Downloads          nmap_aggre.txt            nmap_all_output.xml.xml  nmap_out.txt  Public          Videos
Desktop          host_discovey.txt  nmap_all_output.xml.gnmap  nmap_all.txt             nmap_srv.txt  scan_wire.pcap
Documents        Music              nmap_all_output.xml.nmap   nmap_output.txt          Pictures      Templates
[root@localhost ~]#
```

nmap_srv.txt (Service/version detection):-

```
[root@localhost ~]# nmap -sS -sV 10.0.2.0/24 -oN nmap_srv.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2025-10-20 18:28 IST
Nmap scan report for 10.0.2.2
Host is up (0.00033s latency).
All 1000 scanned ports on 10.0.2.2 are in ignored states.
Not shown: 1000 filtered tcp ports (net-unreach)
MAC Address: 52:55:0A:00:02:02 (Unknown)

Nmap scan report for 10.0.2.3
Host is up (0.00034s latency).
Not shown: 999 filtered tcp ports (net-unreach)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
MAC Address: 52:55:0A:00:02:03 (Unknown)

Nmap scan report for 10.0.2.15
Host is up (0.0000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.7 (protocol 2.0)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 15.95 seconds
[root@localhost ~]#
```

Research common services running on those ports:-

- 10.0.2.3 — Port 53 (dnsmasq 2.51)
  - Service type: DNS resolver
  - Purpose: Resolves domain names to IPs for local network; may also provide DHCP and TFTP services.
  - Common usage: Home routers, gateways, small networks for DNS caching and local host resolution.
- 10.0.2.15 — Port 22 (OpenSSH 8.7)
  - Service type: SSH (Secure Shell)
  - Purpose: Provides secure remote shell access, SFTP file transfer, and encrypted tunnels.
  - Common usage: Administer Linux servers, remote management, automated secure file transfers.
- 10.0.2.2 — All TCP ports filtered
  - Service type: No open services detected (ports filtered by firewall)
  - Purpose: Likely a router/gateway blocking probes. No specific services visible.
  - Common usage: Network device managing LAN connectivity, NAT, and firewall functions.

Identify potential security risks from open ports:-

- 10.0.2.3 — Port 53 (dnsmasq 2.51)
  - Risk: Open DNS service
    - Can be exploited for DNS amplification DDoS attacks if exposed externally.
    - Misconfigured dnsmasq may leak internal hostnames or DHCP info.
    - Older versions may have remote code execution (RCE) or cache poisoning vulnerabilities.
  - Recommendation: Restrict to local LAN, disable recursion for external queries, update software, and monitor logs.
- 10.0.2.15 — Port 22 (OpenSSH 8.7)
  - Risk: SSH service exposure
    - Weak passwords or enabled root login can allow unauthorized access.
    - Deprecated ciphers or protocol versions may be vulnerable.
    - Exposed SSH to the internet may be subject to brute-force attacks.
  - Recommendation: Use key-based authentication, disable root login, restrict access with firewall rules, enforce strong ciphers, and keep OpenSSH updated.
- 10.0.2.2 — All TCP ports filtered
  - Risk: Potential hidden services behind firewall
    - Device may have management interfaces (web, SNMP) not detected but still exposed.
    - Misconfigured firewall may allow unintended access from certain IPs.
  - Recommendation: Harden device (change default credentials, disable unnecessary services), apply patches, monitor logs, and verify reachability from multiple network segments.

**********THANK YOU**********