# VULNERABILITY SCANNING REPORT

Tool Used: Nmap

Target Network: 10.0.2.0/24

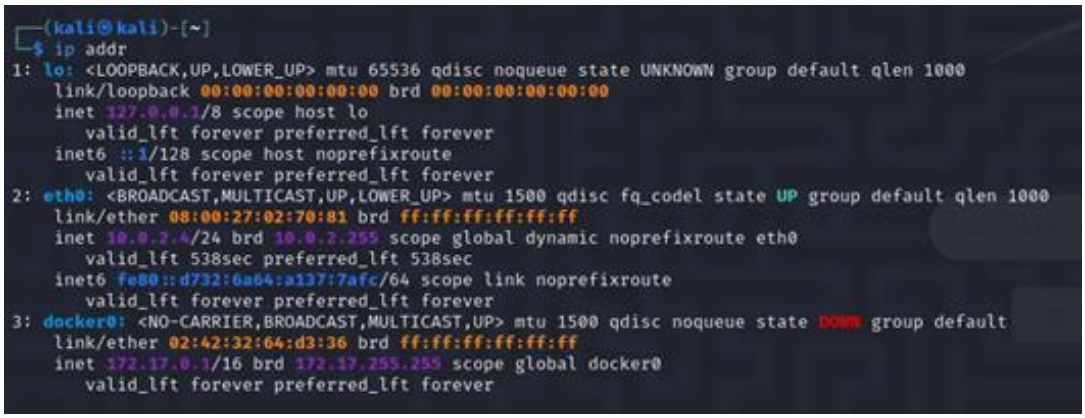
Date: July 30, 2025

Submitted by: Athira K (aathu968@gmail.com)

# Vulnerability Scanning Report (Nmap)

## 1. Network Interface Information

This report documents a basic vulnerability scan conducted on a local network using the Nmap tool. The following screenshot shows the network interfaces available on the Kali Linux system used for scanning.
This confirms that the active scanning interface was `eth0` with the IP address `10.0.2.4/24`, which falls within the target subnet of the scan.



```
┌──(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 08:00:27:02:70:81 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 538sec preferred_lft 538sec
    inet6 fe80::d732:6a64:a137:7afc/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:32:64:d3:36 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

## 2. Methodology

This report presents a vulnerability scan conducted using the Nmap tool on a local network with IP range 10.0.2.0/24. The scan was executed on 30 July 2025 using the following command:

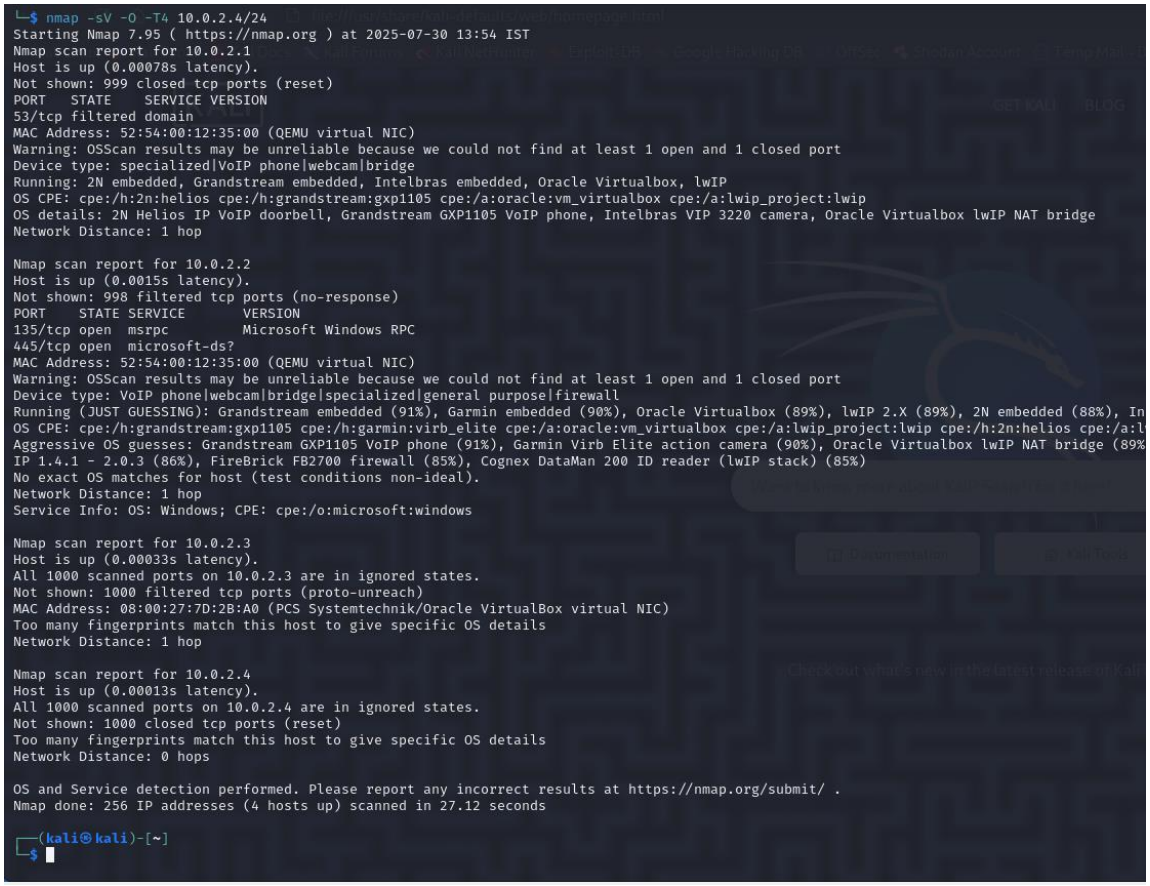
```
nmap -sV -O -T4 10.0.2.4/24
```

Where:
-sV enables version detection.
-O enables OS detection.
-T4 increases the speed of the scan.

The purpose of the scan was to identify active hosts, open ports, running services, and possible operating system details within the 10.0.2.0/24 subnet.

## 3. Scan Execution Screenshot

Below is a screenshot of the scan execution and partial results:



```
└─$ nmap -sV -O -T4 10.0.2.4/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 13:54 IST
Nmap scan report for 10.0.2.1
Host is up (0.00078s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
53/tcp filtered domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|VoIP phone|webcam|bridge
Running: 2N embedded, Grandstream embedded, Intelbras embedded, Oracle Virtualbox, lwIP
OS CPE: cpe:/h:2n:helios cpe:/h:grandstream:gxp1105 cpe:/a:oracle:vm_virtualbox cpe:/a:lwip_project:lwip
OS details: 2N Helios IP VoIP doorbell, Grandstream GXP1105 VoIP phone, Intelbras VIP 3220 camera, Oracle Virtualbox lwIP NAT bridge
Network Distance: 1 hop

Nmap scan report for 10.0.2.2
Host is up (0.0015s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
445/tcp open  microsoft-ds?
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP phone|webcam|bridge|specialized|general purpose|firewall
Running (JUST GUESSING): Grandstream embedded (91%), Garmin embedded (90%), Oracle Virtualbox (89%), lwIP 2.X (89%), 2N embedded (88%), In
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite cpe:/a:oracle:vm_virtualbox cpe:/a:lwip_project:lwip cpe:/h:2n:helios cpe:/a:l
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (91%), Garmin Virb Elite action camera (90%), Oracle Virtualbox lwIP NAT bridge (89%
IP 1.4.1 - 2.0.3 (86%), FireBrick FB2700 firewall (85%), Cognex DataMan 200 ID reader (lwIP stack) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.2.3
Host is up (0.00033s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:7D:2B:A0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

Nmap scan report for 10.0.2.4
Host is up (0.00013s latency).
All 1000 scanned ports on 10.0.2.4 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.12 seconds

┌──(kali㉿kali)-[~]
└─$
```

## 4. Key Vulnerabilities Identified

| IP Address | Port | Service | Vulnerability/Observation |
|---|---|---|---|
| 10.0.2.2 | 135 | msrpc | Potential exposure of Microsoft RPC services |
| 10.0.2.2 | 445 | microsoft-ds | SMB port open - susceptible to SMB-based attacks |
| 10.0.2.3 | - | - | Too many fingerprints matched, no specific OS details |
| 10.0.2.4 | - | - | All scanned ports closed, host unresponsive |

## 5. Recommendations

Based on the findings from the Nmap scan, the following actions are recommended:

1. **Restrict access to critical ports**, such as 135 and 445, using host-based or network firewalls. These ports should only be open if absolutely necessary and should be limited to specific, trusted IP ranges.
2. **Ensure regular patching and updates** are applied to all machines on the network. Known vulnerabilities in older versions of services can easily be exploited if patches are delayed or skipped.
3. **Monitor hosts with incomplete or inconsistent OS information**, like 10.0.2.3. This may indicate active evasion or outdated systems that require a manual review.
4. Use **additional tools** to enhance and cross-verify scan results:
    - **Wireshark** can be used to capture and analyze real-time network traffic, helping detect anomalies or unauthorized activity.
    - **OpenVAS** is a more comprehensive vulnerability management solution that builds on basic scanning by including CVE mapping and detailed vulnerability descriptions.
    - **Nessus**, is a highly regarded vulnerability assessment tool with strong reporting capabilities.
5. Lastly, consider adopting a **security framework** like **ISO/IEC 27001**, which provides a structured approach to managing information security across an organization.