

# **Active Reconnaissance Scan Report -Nmap**

**Scan target:** Host Machine : 10.0.2.3 (Local Host)

**Date of recon:** December 05, 2025

**Cybersecurity Analyst**  
Adebayo Fijabi

# Nmap Overview

Nmap is a powerful network scanning tool used to identify hosts, services, and potential vulnerabilities across a network. In addition to standard port scanning, Nmap includes a large set of built-in scripts (NSE Nmap Scripting Engine) that can be used to perform advanced enumeration and vulnerability detection.

Additional documentation, script references, and usage guides can be found at [nmap.org](https://nmap.org), particularly under the Docs and Reference sections.

## Authorization

Active scanning involves directly interacting with a target system to identify potential weaknesses. **This phase should only be performed on systems where explicit authorization has been granted**, as it generates logs and is easily detectable.

During active scanning, we gather detailed technical information about the target, including:

- **Operating System Identification (OS Fingerprinting):** Determines the type and version of the operating system running on the host.
- **Port Status Enumeration:** Identifies which ports are open, closed, or filtered, helping reveal the services exposed to the internet.
- **Service Detection:** Discovers which services are running on each port (e.g., HTTP, SSH, SMTP).
- 
- **Service Version Detection:** Determines the precise version of the service (i.e Apache 2.4.54), which is crucial for mapping known vulnerabilities (CVEs).

Active scanning provides deeper visibility into the target's attack surface and helps identify security risks that cannot be detected through passive reconnaissance alone.

## Objective

To document the results of an active reconnaissance scan conducted on a personal host using Nmap. The purpose of this assessment is to identify the host's network visibility and determine which TCP ports were exposed or responsive at the time of the scan.

# **Understanding Port States**

During a scan, Nmap identifies the state of each port it probes. Ports typically fall into one of three categories:

## **1. Open Ports**

- The port is actively accepting connections.
- A service is running and responding on this port.
- This port is reachable and can be interacted with.

## **2. Closed Ports**

- The port is reachable, but no service is listening.
- The host responds with a "closed" status.
- These ports are not currently in use but could be opened in the future.

## **3. Filtered Ports**

- Nmap cannot determine whether the port is open because a firewall, IDS/IPS, or filtering device is blocking the request.
- The port may or may not be open, but traffic to it is restricted.

## **Nmap Output Summary**

When Nmap completes a scan, it displays:

- **Open ports**
- **Port states (open/closed/filtered)**
- **Service names** running on those ports
- **Version details** (when using `-sV`)

This information helps determine the system's exposure and potential attack surface.

## Findings

- Nmap is Default to scan 1000 PORTs, Displays the 12 Open ports.

```
(kali㉿kali)-[~]
$ nmap 10.0.2.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 22:09 EST
Nmap scan report for 10.0.2.3
Host is up (0.0016s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
MAC Address: 08:00:27:E1:C7:10 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.84 seconds

(kali㉿kali)-[~]
```

Required to scan a specific range of ports (**ports 50 through 75**)

```
(kali㉿kali)-[~]
$ nmap -p50-75 10.0.2.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 23:09 EST
Nmap scan report for 10.0.2.3
Host is up (0.0013s latency).

PORT      STATE SERVICE
50/tcp    filtered re-mail-ck
51/tcp    filtered la-maint
52/tcp    filtered xns-time
53/tcp    open  domain
54/tcp    filtered xns-ch
55/tcp    filtered isi-gl
56/tcp    filtered xns-auth
57/tcp    filtered priv-term
58/tcp    filtered xns-mail
59/tcp    filtered priv-file
60/tcp    filtered unknown
61/tcp    filtered ni-mail
62/tcp    filtered acas
63/tcp    filtered via-ftp
64/tcp    filtered covia
65/tcp    filtered tacacs-ds
66/tcp    filtered sqlnet
67/tcp    filtered dhcps
68/tcp    filtered dhcpc
69/tcp    filtered tftp
70/tcp    filtered gopher
71/tcp    filtered netrjs-1
72/tcp    filtered netrjs-2
73/tcp    filtered netrjs-3
74/tcp    filtered netrjs-4
75/tcp    filtered priv-dial
MAC Address: 08:00:27:E1:C7:10 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.66 seconds
```

Required to scan Specific port -53

```
(kali㉿kali)-[~]
$ nmap -p53 10.0.2.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 23:14 EST
Nmap scan report for 10.0.2.3
Host is up (0.0011s latency).

PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 08:00:27:E1:C7:10 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Required to scan Multiple port -40,60,32,11

```
(kali㉿kali)-[~]
$ nmap -p53,22,21,11 10.0.2.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 23:20 EST
Nmap scan report for 10.0.2.3
Host is up (0.0017s latency).

PORT      STATE SERVICE
11/tcp    filtered systat
21/tcp    filtered ftp
22/tcp    filtered ssh
53/tcp    open  domain
MAC Address: 08:00:27:E1:C7:10 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.50 seconds
```

Perform a full port scan and enumerate every possible TCP port (1–65,535)

```
(kali㉿kali)-[~]
$ nmap -p- 10.0.2.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-05 23:23 EST
Nmap scan report for 10.0.2.3
Host is up (0.0019s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
49664/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49670/tcp open  unknown
49671/tcp open  unknown
49759/tcp open  unknown
65051/tcp open  unknown
MAC Address: 08:00:27:E1:C7:10 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 108.23 seconds
```

## Scanning Multiple Hosts with Nmap

To scan multiple PCs or hosts using Nmap, I created an IP list file that contains all the target IP addresses.

### Create an IP List File

Create a text file (e.g., iplist.txt) and add the IP addresses of all devices I will be scanning ,one per line.

```
(kali㉿kali)-[~/Bayodiscuss]
$ ls
iplist.txt

(kali㉿kali)-[~/Bayodiscuss]
$ cat iplist.txt
10.0.2.3
160.153.138.217
```

Required to scan port 53 and port 80 on both devices.

```
(kali㉿kali)-[~/Bayodiscuss]
$ nmap -p53,80 -il iplist.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 00:18 EST
Nmap scan report for 10.0.2.3
Host is up (0.0013s latency).

PORT      STATE      SERVICE
53/tcp    open       domain ←
80/tcp    filtered  http ←
MAC Address: 08:00:27:E1:C7:10 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 217.138.153.160.host.secureserver.net (160.153.138.217)
Host is up (0.0036s latency).

PORT      STATE      SERVICE
53/tcp    filtered  domain ←
80/tcp    open       http ←

Nmap done: 2 IP addresses (2 hosts up) scanned in 2.94 seconds
```

Understanding the range of IP Run ‘ip a’ ,it will shows the ip and the range

```
(kali㉿kali)-[~/Bayodiscuss]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 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:c9:b9:c3 brd ff:ff:ff:ff:ff:ff
→    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 504sec preferred_lft 504sec
        inet6 fe80::def8:a3e1:bc59:6cb3/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

With the Ethernet interface **eth0**, I can see that the assigned IP address is **10.0.2.15/24**. The **/24 subnet** indicates that other devices are likely present within the same network range.

To identify other active hosts on the network, run the following command:

Run command ‘ **sudo netdiscover -i eth0 -r 10.0.2.0/24**’.

This scans the entire subnet and displays a list of reachable devices, including their IP addresses and MAC addresses.

kali@kali: ~/Bayodiscuss						
Session		Actions		Edit View Help		
Currently scanning: Finished!   Screen View: Unique Hosts						
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 120						
IP	At	MAC Address	Count	Len	MAC Vendor	/ Hostname
10.0.2.2		08:00:27:1e:3f:3f	1	60	PCS	Systemtechnik GmbH
10.0.2.3		08:00:27:e1:c7:10	1	60	PCS	Systemtechnik GmbH

**Aggressive scan** → To gather detailed information about a target asset, which provides extensive details including OS detection, service versions, script results, and network behavior.

```
(kali㉿kali)-[~/Bayodiscuss]
$ nmap -p53,80 -A 10.0.2.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 00:43 EST
Nmap scan report for 10.0.2.3
Host is up (0.0013s latency).

PORT      STATE     SERVICE VERSION
53/tcp    open      domain  Simple DNS Plus
80/tcp    filtered http
MAC Address: 08:00:27:E1:C7:10 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|11|2016 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (97%), Microsoft Windows 11 21H2 (91%),
Microsoft Windows Server 2016 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT      ADDRESS
1   1.32 ms  10.0.2.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.15 seconds
```

**Perform a targeted Nmap scan** → To identify the **operating system**, Web server and detect services running on specific ports on ports 53 and 80.

```
(kali㉿kali)-[~/Bayodiscuss]
$ nmap -p53,80 -O 10.0.2.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 00:51 EST
Nmap scan report for 10.0.2.3
Host is up (0.0034s latency).

PORT      STATE     SERVICE
53/tcp    open      domain
80/tcp    filtered http
MAC Address: 08:00:27:E1:C7:10 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022|11|2016 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows_11 cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2022 (97%), Microsoft Windows 11 21H2 (91%),
Microsoft Windows Server 2016 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 5.73 seconds
```

## Detect Ports and service versions

```
(kali㉿kali)-[~/Bayodiscuss]
$ nmap -p53,80 -sV 10.0.2.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 00:30 EST
Nmap scan report for 10.0.2.3
Host is up (0.0010s latency).

PORT      STATE     SERVICE VERSION
53/tcp    open      domain   Simple DNS Plus
80/tcp    filtered http
MAC Address: 08:00:27:E1:C7:10 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 7.85 seconds
```

Run this scan against multiple devices or IP addresses to identify the service versions running on their exposed ports. In this case, the results show services such as Simple DNS Plus and Cloudflare HTTP Proxy operating on the target systems.

```
(kali㉿kali)-[~/Bayodiscuss]
$ nmap -p53,80 -sV -iL iplist.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-06 00:36 EST
Nmap scan report for 10.0.2.3
Host is up (0.0011s latency).

PORT      STATE     SERVICE VERSION
53/tcp    open      domain   Simple DNS Plus
80/tcp    filtered http
MAC Address: 08:00:27:E1:C7:10 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 217.138.153.160.host.secureserver.net (160.153.138.217)
Host is up (0.013s latency).

PORT      STATE     SERVICE VERSION
53/tcp    filtered domain
80/tcp    open      http     Cloudflare http proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 2 IP addresses (2 hosts up) scanned in 22.77 seconds
```

## Observations

- The host responded to Nmap's initial discovery probes, confirming it is active and reachable on the local network.
- Out of Nmap's full port sweep, 988 TCP ports were filtered, meaning no response was received—likely due to firewall or packet filtering controls.
- A total of 12 open TCP ports were identified during the scan, indicating active services running and potentially exposed.

- The host exhibited a latency of 6.84 seconds, which suggests it is located within the same LAN or a nearby network segment.

## Recommendations

### 1. Reduce Open Ports (**High Priority**)

- Disable any unnecessary services
- Restrict access to essential ports only
- Implement host-based firewall rules (Windows Firewall, UFW, etc.)

### 2. Perform Service Version Verification

- Check the version of each exposed service
- Compare against CVE databases (NVD, MITRE, CVE.org)
- Patch or update any outdated or vulnerable software

### 3. Strengthen Firewall Rules

- Ensure non-essential ports are blocked
- Implement segmentation or VLAN isolation if appropriate
- Enable logging for denied traffic

### 4. Conduct Regular Port Scans

- Establish routine scanning to detect new or re-opened ports
- Monitor for unauthorized services introduced by malware or misconfiguration

### 5. Implement Network Monitoring

- Enable intrusion detection (IDS) or endpoint detection (EDR)
- Monitor for abnormal activity on open port

## Summary

This vulnerability assessment was conducted to evaluate the security posture of a Windows host on a local network using industry-standard reconnaissance and scanning

techniques. The primary objective was to identify exposed services, assess network visibility, and determine potential areas where the system may be vulnerable to exploitation.

The active scan confirmed that the host is reachable and responsive, with **12 open TCP ports** exposing various services to the network. These open ports increase the host's attack surface, providing potential entry points for threat actors. Additionally, the scan identified **988 filtered ports**, indicating the presence of firewall protections, although selective services remain exposed to external probing.

Service enumeration revealed running applications such as **Simple DNS Plus** and **Cloudflare HTTP Proxy**, which, depending on their versions, may be associated with known vulnerabilities. The detection of identifiable services emphasizes the importance of version control, timely patching, and configuration hardening.

Overall, the results of this assessment highlight several risks related to unnecessary open ports, service exposure, and the potential presence of outdated or misconfigured software. While the system demonstrates partial defensive measures, additional security enhancements are required to reduce the likelihood of successful exploitation.

This executive summary provides a high-level overview of key findings and supports informed decision-making regarding risk mitigation and ongoing security improvements. Immediate actions such as closing unused ports, strengthening firewall rules, validating service configurations, and implementing continuous monitoring are recommended to enhance the security resilience of the host.