Task 2 – NMAP SCAN REPORT

# NMAP

## What is Nmap?

Nmap (Network Mapper) is a free and open-source tool used to:

* Discover devices on a network.
* Scan for open ports and services.
* Check the operating system and software versions.
* Find security vulnerabilities.

It’s like a security camera for your network — it tells you who’s there and what they’re doing.

## How Nmap Works

1.You tell Nmap a target → An IP or a range of IPs.

2.Nmap sends test messages (packets) to different ports on that target.

3.The target replies → The reply type tells Nmap if the port is open, closed, or blocked.

4.Nmap checks what’s running on open ports → It may also guess the software version and operating system.

5.Nmap shows the report → A list of devices, open ports, services, and extra details.

## Commands

**Host Discovery**

-sn – ping scan (check target is live or not)

-sL – list scan (scan all targets in network)

-Pn – treat all hosts as online (skip host discovery)

-PS - TCP SYN Ping – Sends SYN packets to check if host is alive.

-PA - TCP ACK Ping – Sends ACK packets to check if host responds (good for bypassing some firewalls).

-PU - UDP Ping – Sends UDP packets to see if host responds.

-PY - SCTP COOKIE-ECHO Ping – Uses SCTP protocol to detect if host is up

-PE - ICMP Echo Ping – Like a normal ping, sends ICMP Echo Request.

-PP - ICMP Timestamp Ping – Sends ICMP Timestamp Request to check if host replies.

-PM - ICMP Address Mask Ping – Sends ICMP Address Mask Request.

--traceroute - trace hop path to each host

**Scan Techniques**

-sS - TCP SYN scan – Sends SYN, waits for SYN-ACK (fast, stealthy).

-sA - TCP ACK scan – Checks firewall rules and whether ports are filtered.

-sT - TCP Connect scan – Uses full TCP connection (connect ()), slower, more detectable.

-sM - TCP Maimon scan – Sends FIN/ACK to check for open/filtered ports.

-sU - UDP scan – Sends UDP packets to detect open UDP ports.

-sN - TCP Null scan – Sends packets with no flags set, detects open/filtered ports.

-sF - TCP FIN scan – Sends FIN packets to detect open/filtered ports.

-sX - TCP Xmas scan – Sends FIN+URG+PSH flags.

**Port specification and Scan order**

-p<port range> - scan specified port

--exclude-ports – exclude ports

-F – fast mode

--top-ports<numbers> - scan common ports

**Service and Version**

-sV – service version detection

-v – print version number

**Script Scan**

-Sc – script scanning

--script – nse scripts

**OS Detection**

-O – os detection

-T – set timing templete(-T0 (slow mode) to -T5 (fast mode))

**Output**

-ON – save output as normal file

-OX – save as xml file

-open – only shows open ports

-6 – IPV6 configuration

-A – OS, version, script, traceroute

-h – help summary page

**Key Observations:**

**Open Port:** Service is available and accepting connections.

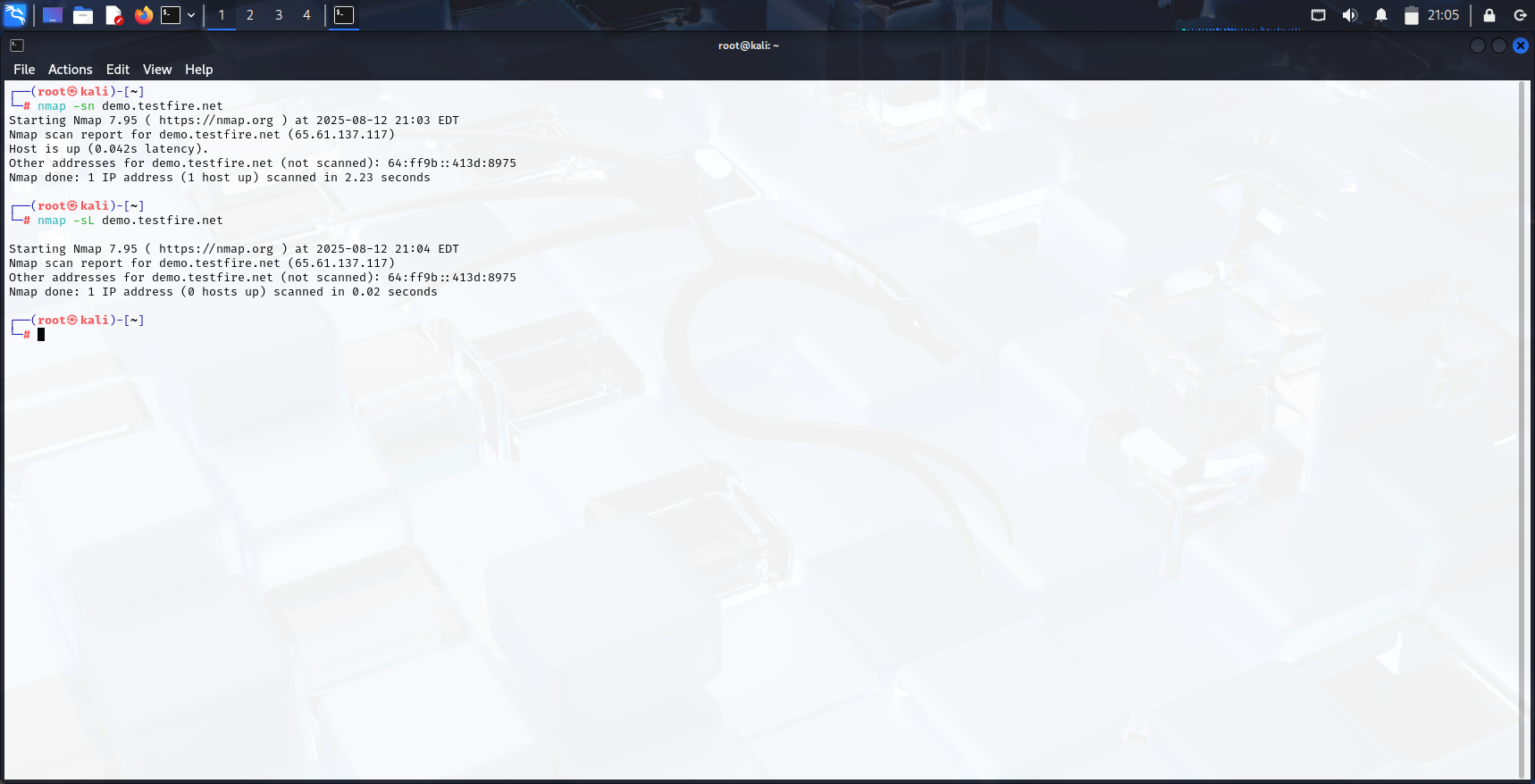
**Closed Port:** No service listening; port is reachable but inactive.

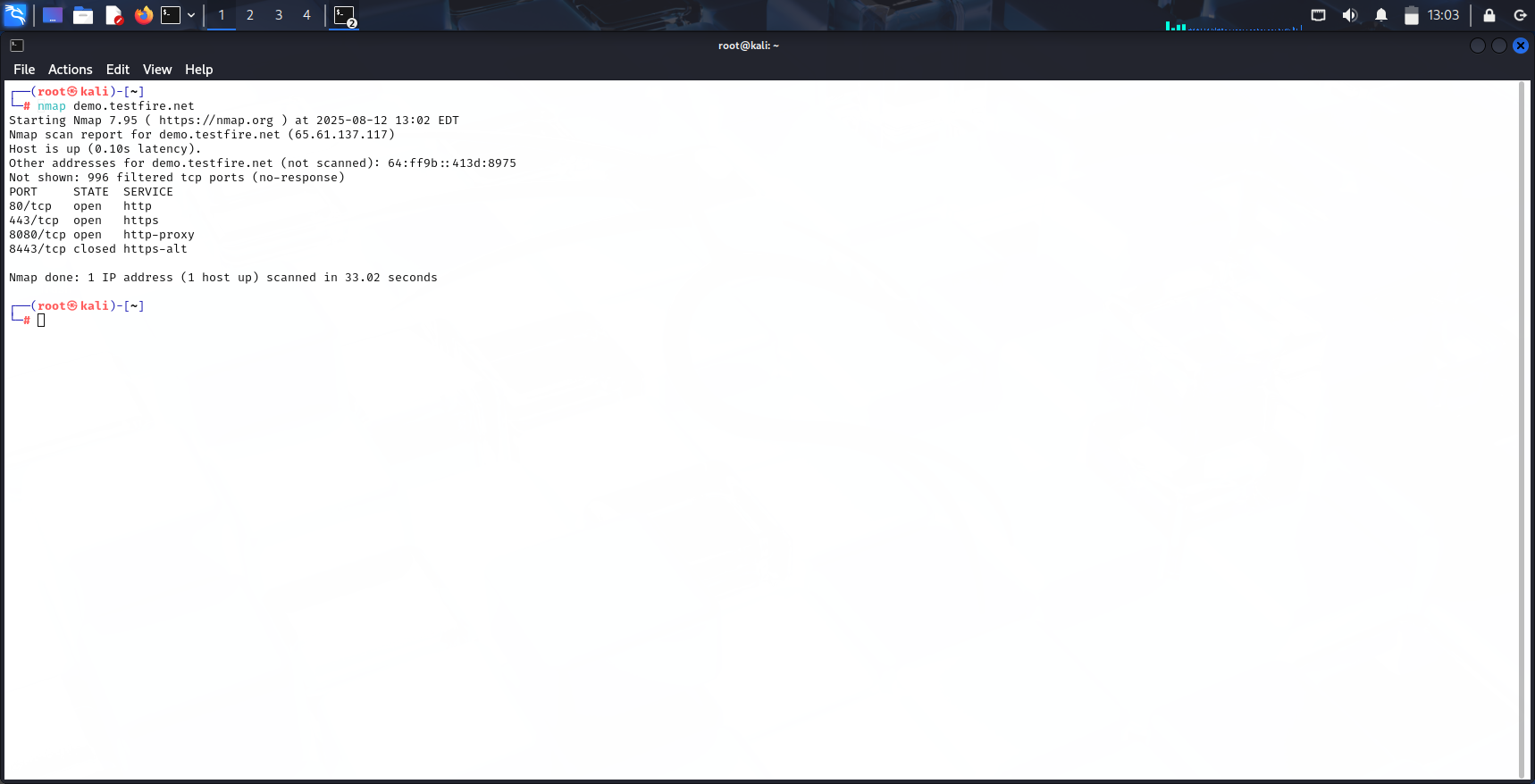
**Filtered Port:** Traffic is blocked or filtered, often by a firewall.

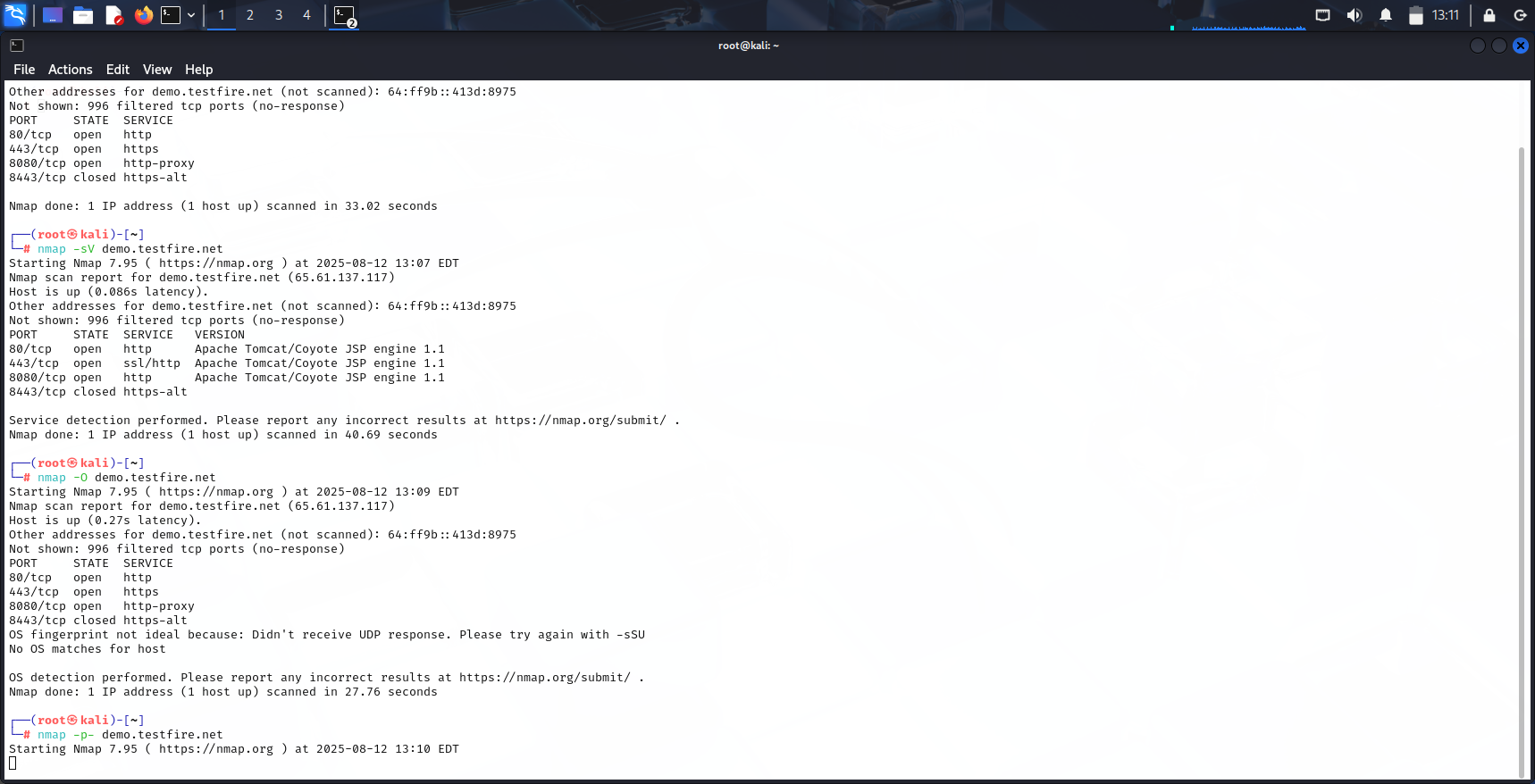
## Scanning Public Server using Nmap

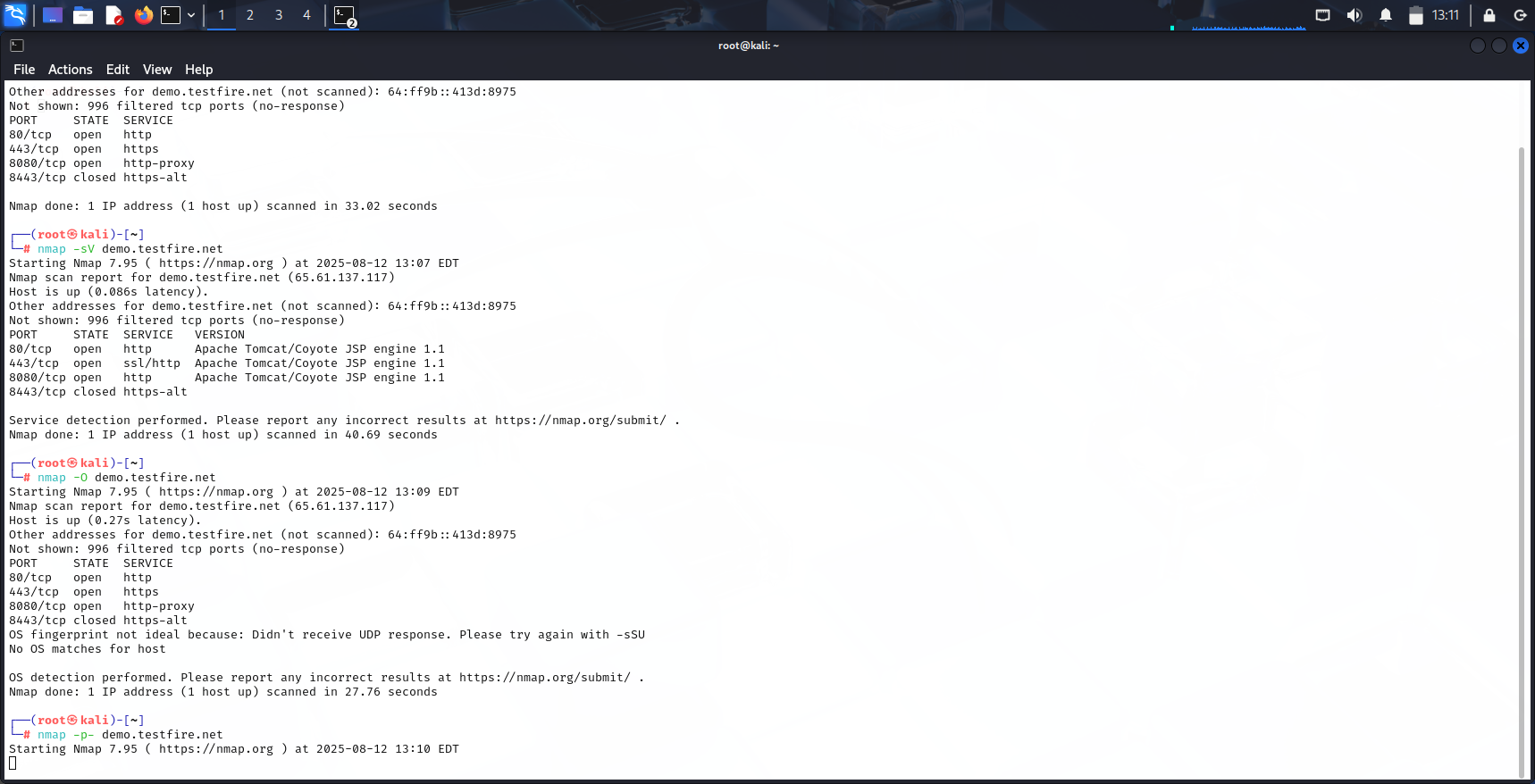
**demo.testfire.net**

**\***Ping Scan : Check target is live or not



\*Basic Scan : Lists open ports and basic service information.

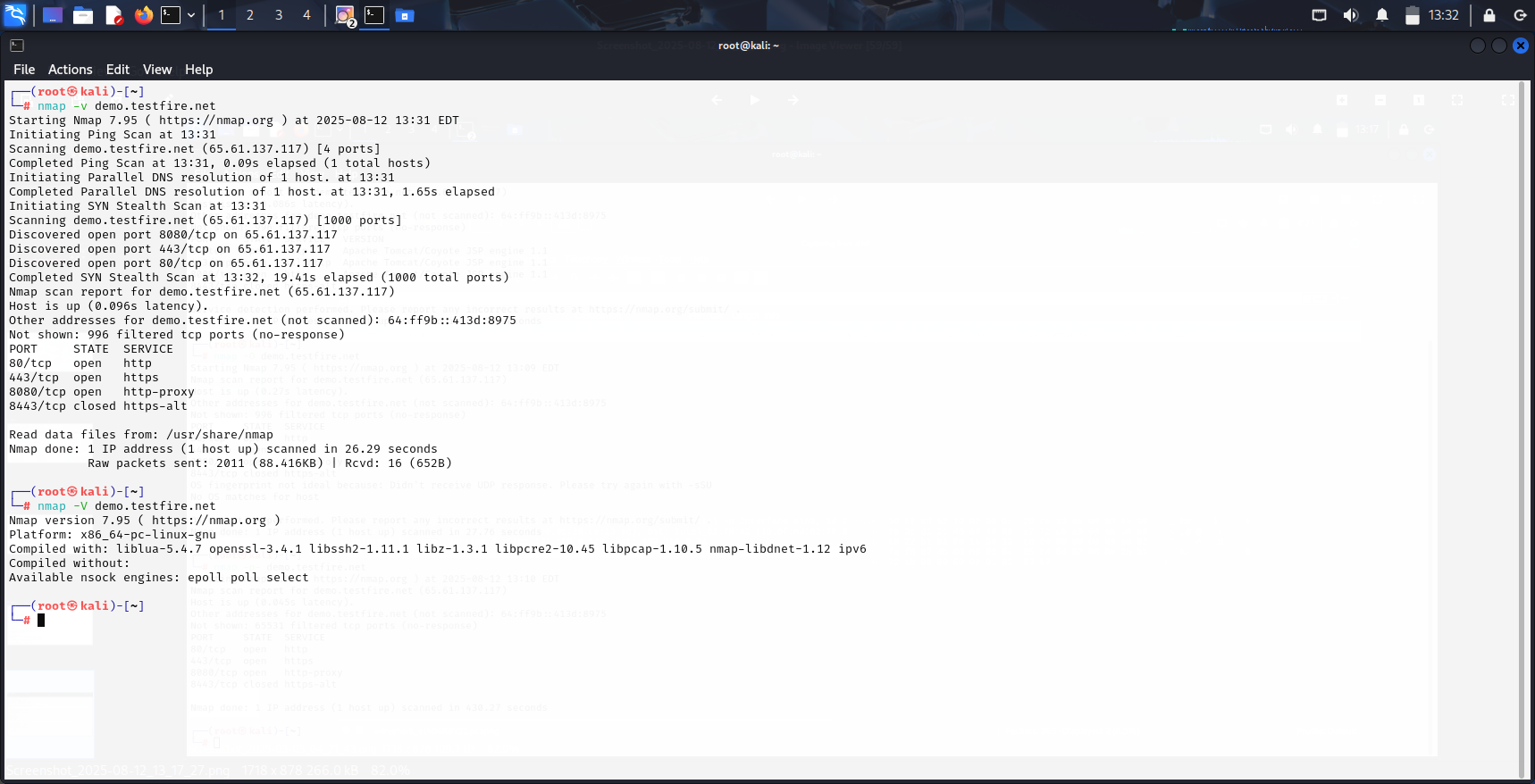
\*Service Version Detection : Detects the versions of running services.

\*Operating System Detection : Tries to identify the target’s OS using TCP/IP fingerprinting

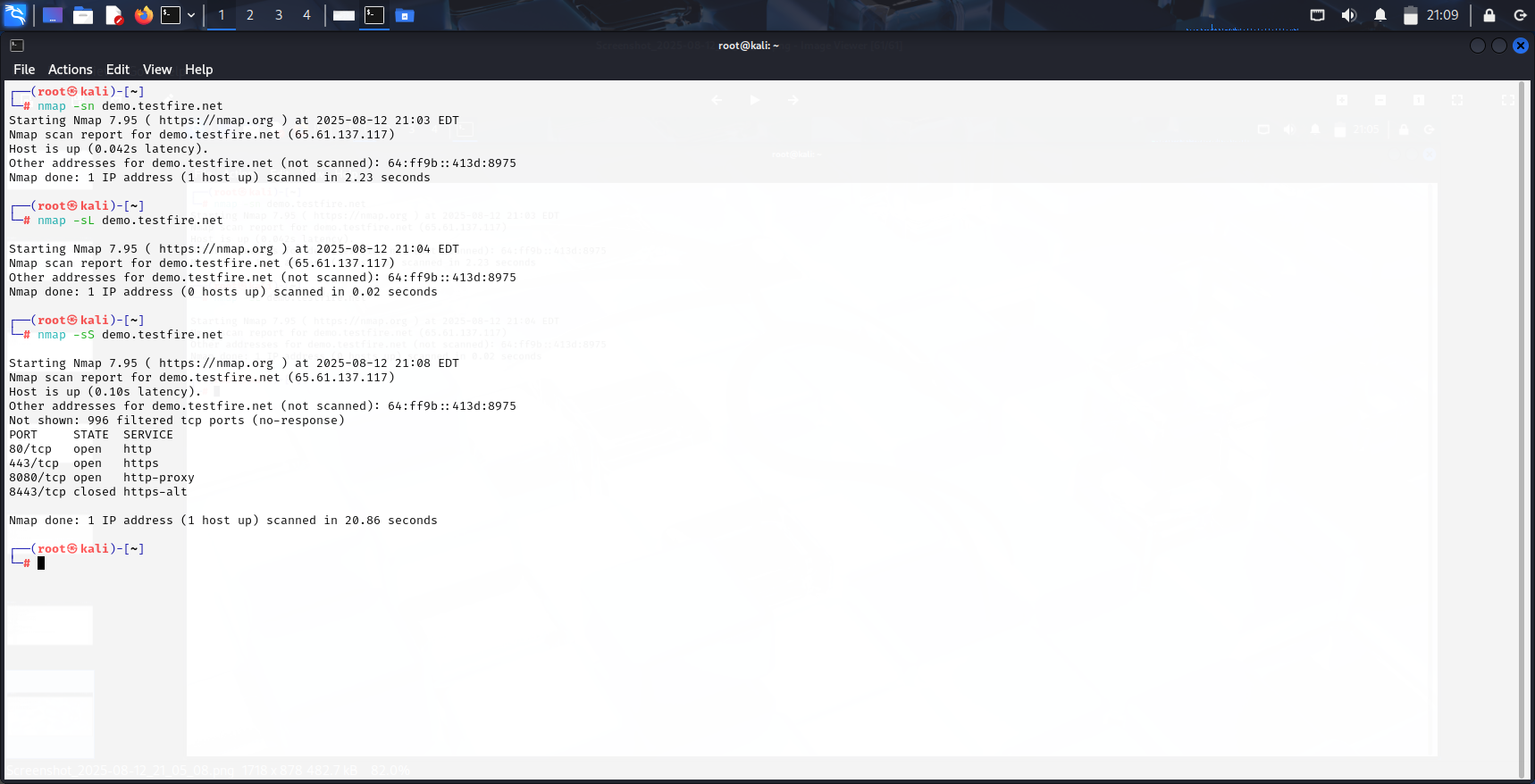
\*Scan All Ports : Scans all 65,535 ports to detect any open ones not in the default 1–1000 range.



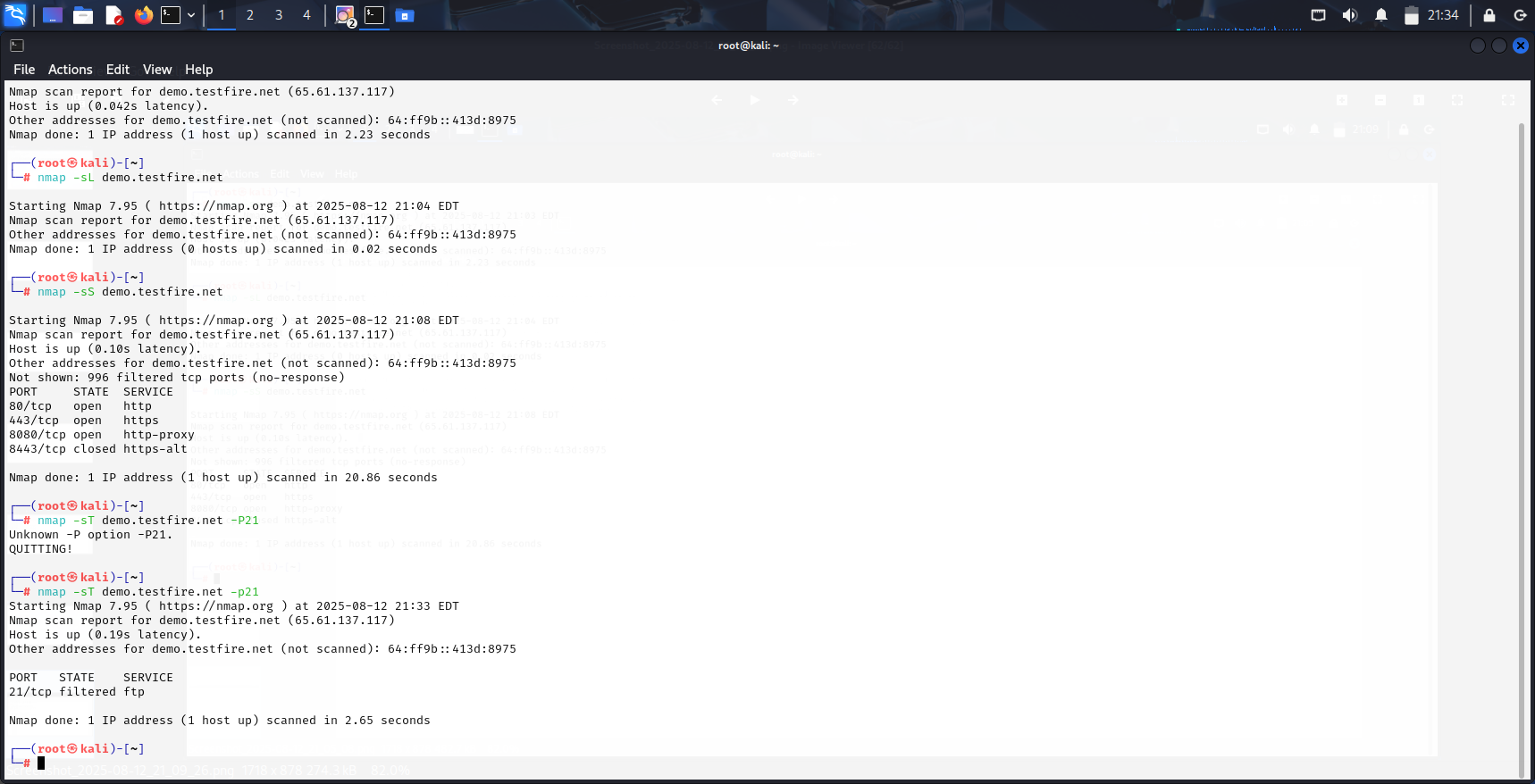
\*Version scan : Print version



\* TCP SYN scan – Sends SYN, waits for SYN-ACK



\* TCP Connect scan for a specified port number



From the Nmap scan on demo.testfire.net, it was observed that the target was live and responding to ping requests. Several open ports were detected, each running specific services that were successfully identified along with their versions through version detection. The TCP SYN scan confirmed active connections, and operating system fingerprinting provided insights into the target’s probable OS. A full port scan ensured that ports outside the default range were also checked, revealing all possible open ones.

## **Conclusion**

Nmap is a very useful tool for finding out what devices and services are running on a network. In this scan, we were able to check if the target was live, find out which ports were open, see what services were running on those ports, and even try to guess the operating system. We used different scanning methods like ping scan, TCP SYN scan, version detection, and OS detection to collect detailed information. This information helps in understanding how the target system is set up and can also show possible weak points that attackers might try to use. Network administrators and security analysts can use Nmap to regularly check their systems, make sure only the right services are open, and confirm that firewalls are working correctly. It is important to remember that scans should always be done only on systems you have permission to test, as scanning without authorization can be illegal and unethical. Overall, this scan showed how Nmap can give a complete picture of a network’s status and help in keeping it secure.