Network Scanning

1)What is Network scanning?

* Network scanning is the process of identifying active devices, hosts, services, open ports, and potential vulnerabilities on a computer network. It’s a fundamental technique in cybersecurity, used by both ethical hackers (for defense) and malicious attackers (for exploitation).

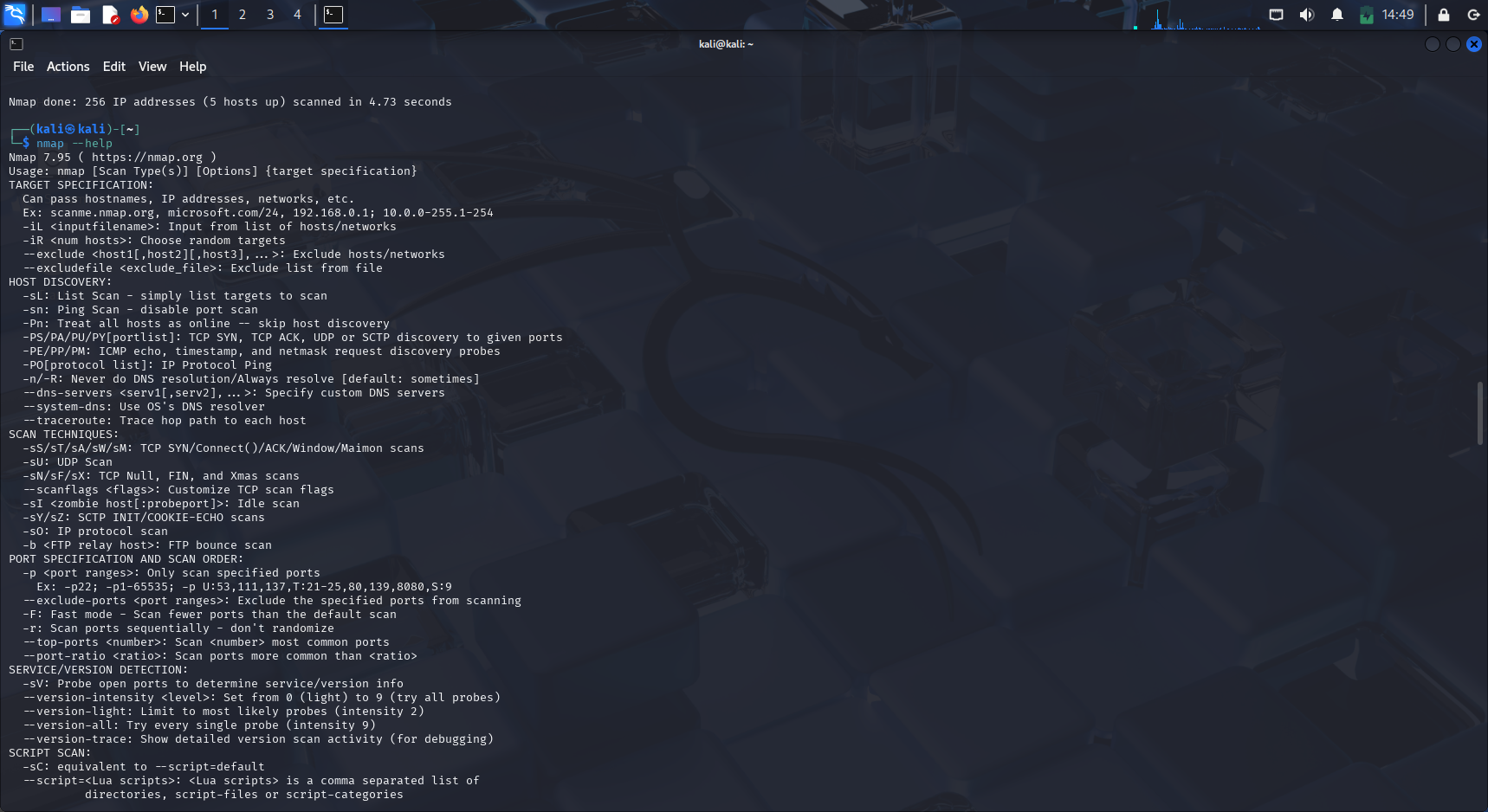
2)Why using Nmap for Network scanning?

* Nmap (Network Mapper) is one of the most popular and widely used tools for network scanning. Nmap can perform host discovery, port scanning, service detection, OS fingerprinting, and vulnerability detection. Nmap is completely free to use and open source, meaning it's transparent and community-supported.

3)Different types of scanning in network?

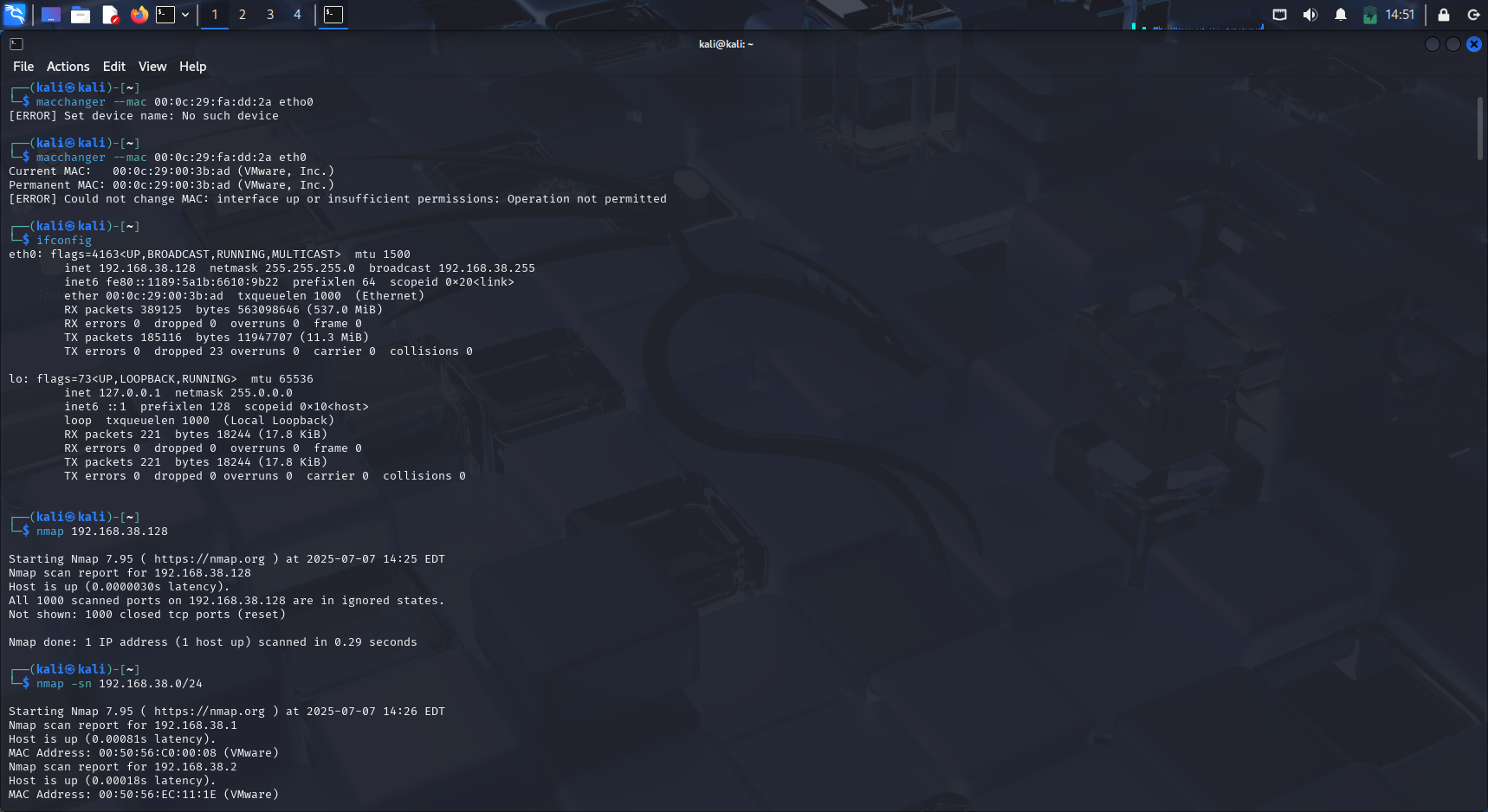
* Ping Scan (ICMP Scan):Check if a host is alive (up) or not.
* Port Scanning:Identify open, closed, or filtered ports on a target.
* Service and Version Scanning:Identify which services are running and their versions.
* Vulnerability Scanning:Detect known vulnerabilities in systems/services.

Methodology



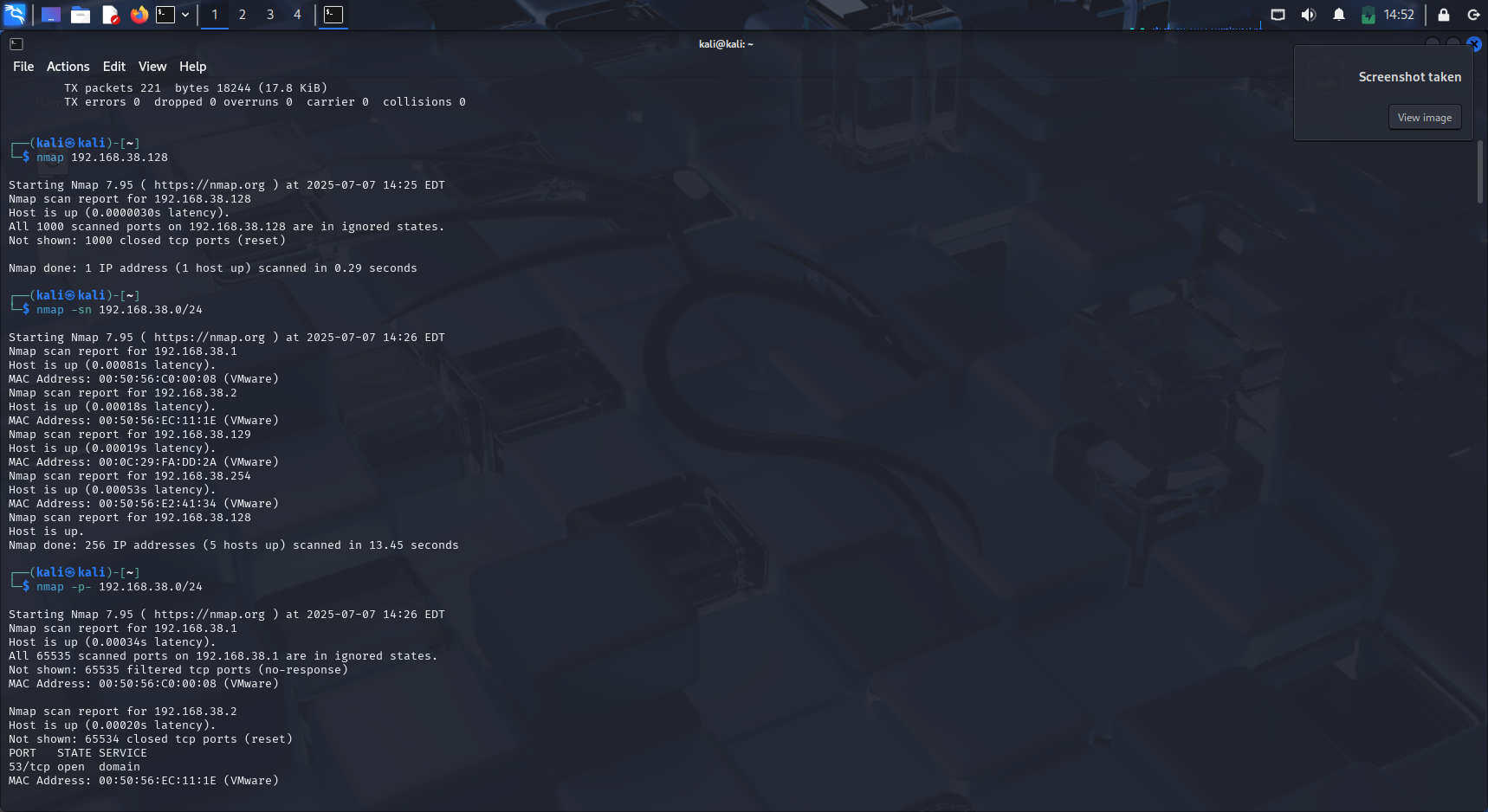
1)Select the target:

* This step involves identifying the IP address or hostname of the system you want to scan.
* Targets can be individual devices (e.g., 192.168.1.10) or entire subnets (e.g., 192.168.1.0/24).



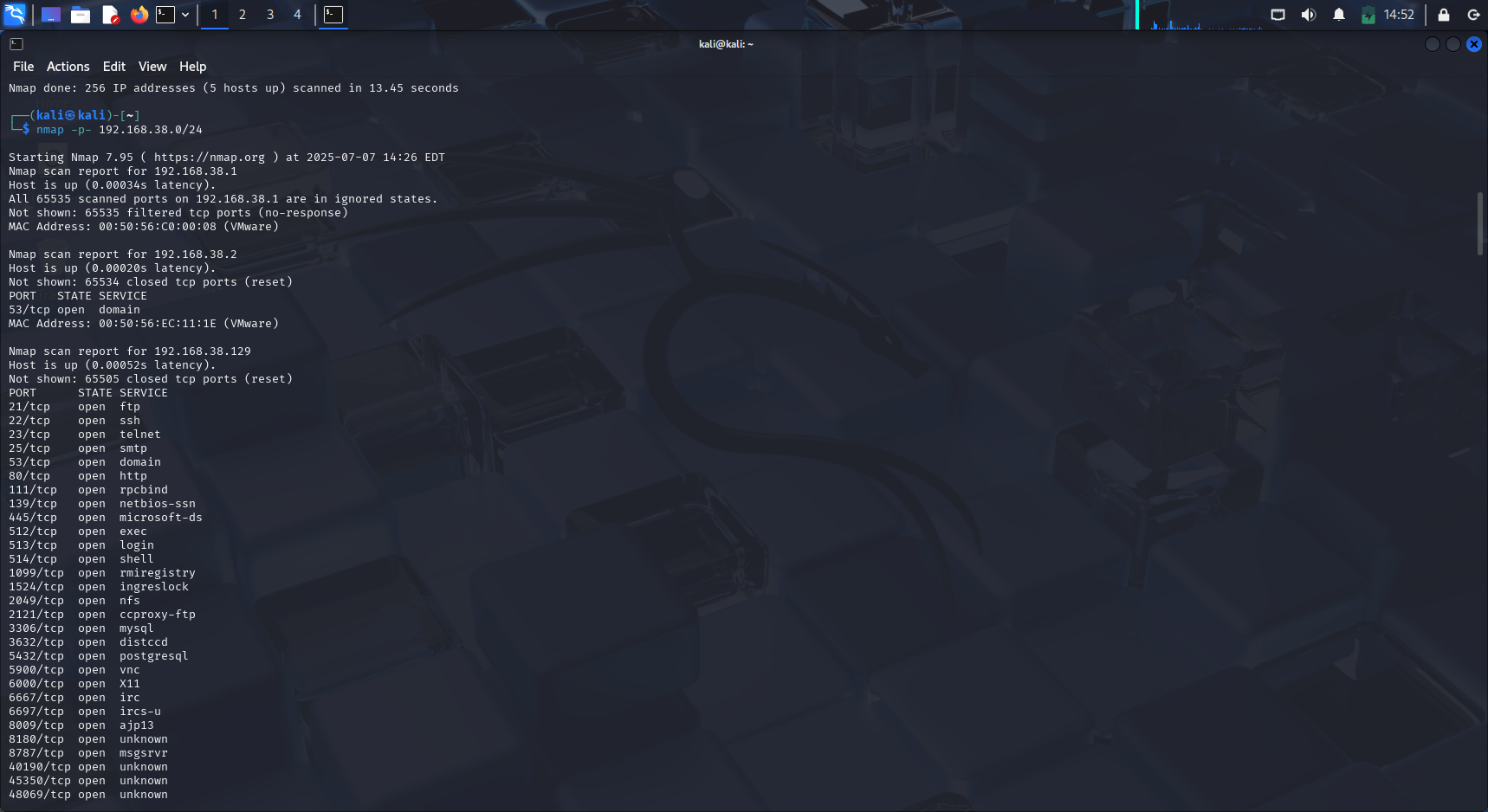
2)Find all the active devices connected to the network (scanning the IP range of a network):

* Known as host discovery or ping sweep.
* This process identifies which IP addresses on the network are currently online or responding.



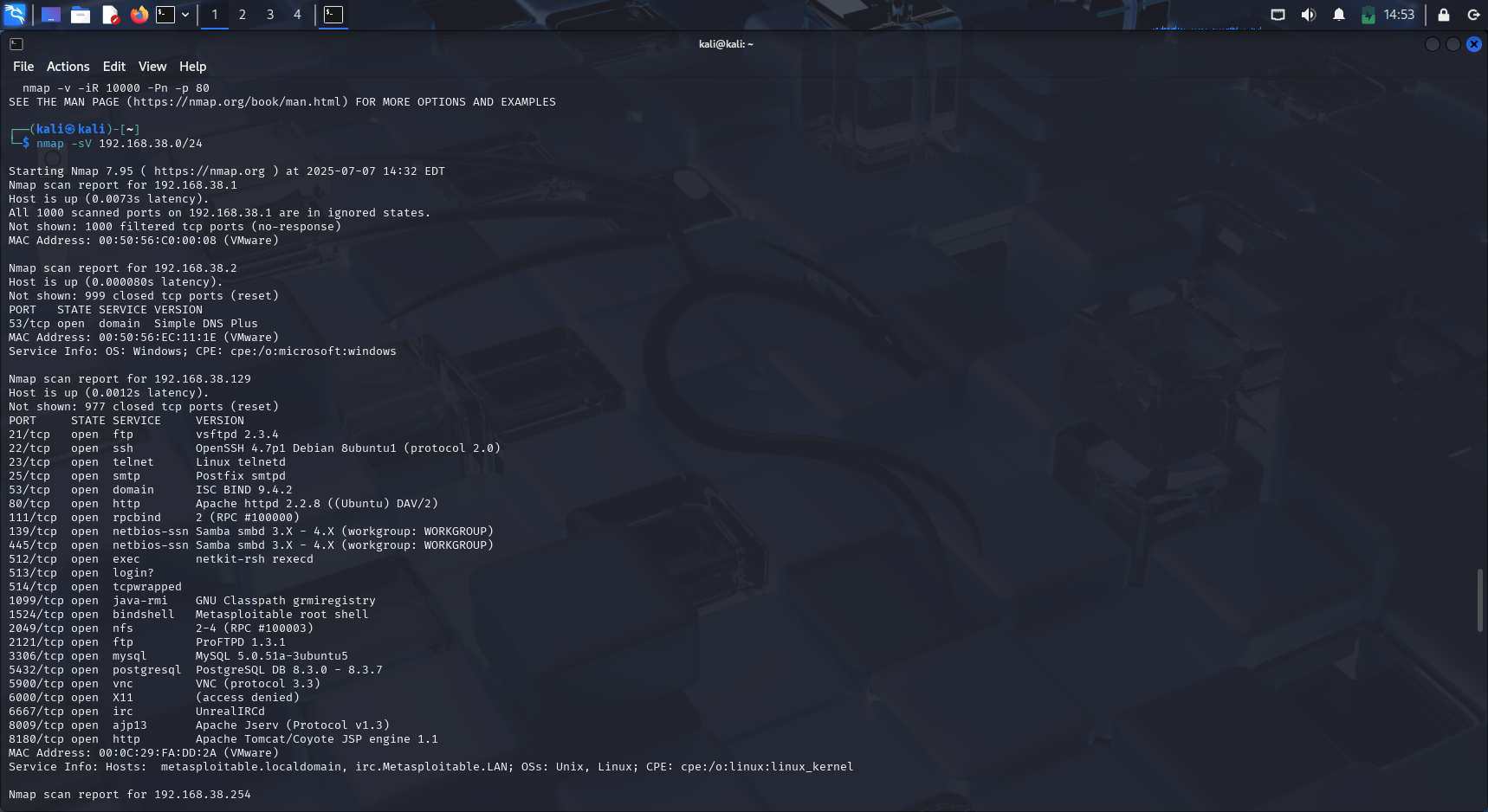
3)Scan their open ports:

* This is the process of checking which network ports on each device are open, closed, or filtered.
* Open ports indicate that services are listening and accessible.



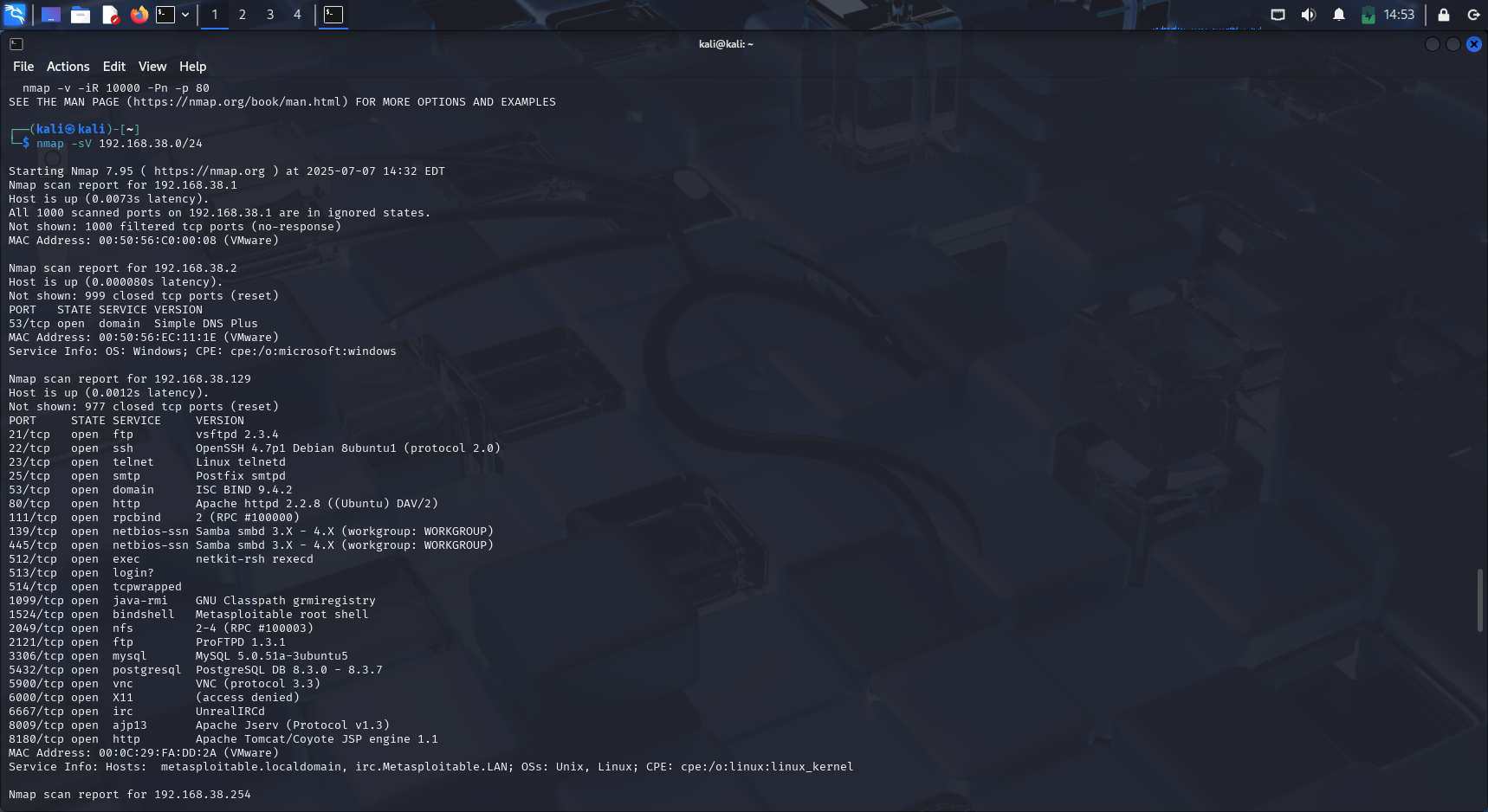
4)Find the services running on the open ports:

* Once open ports are found, scanning tools probe them to identify the services or applications (e.g., HTTP, SSH, FTP).
* Helps understand what software is accessible from the network.



5)Find the service versions running on open ports:

* In this step, the scanner tries to determine the exact version of the services found.

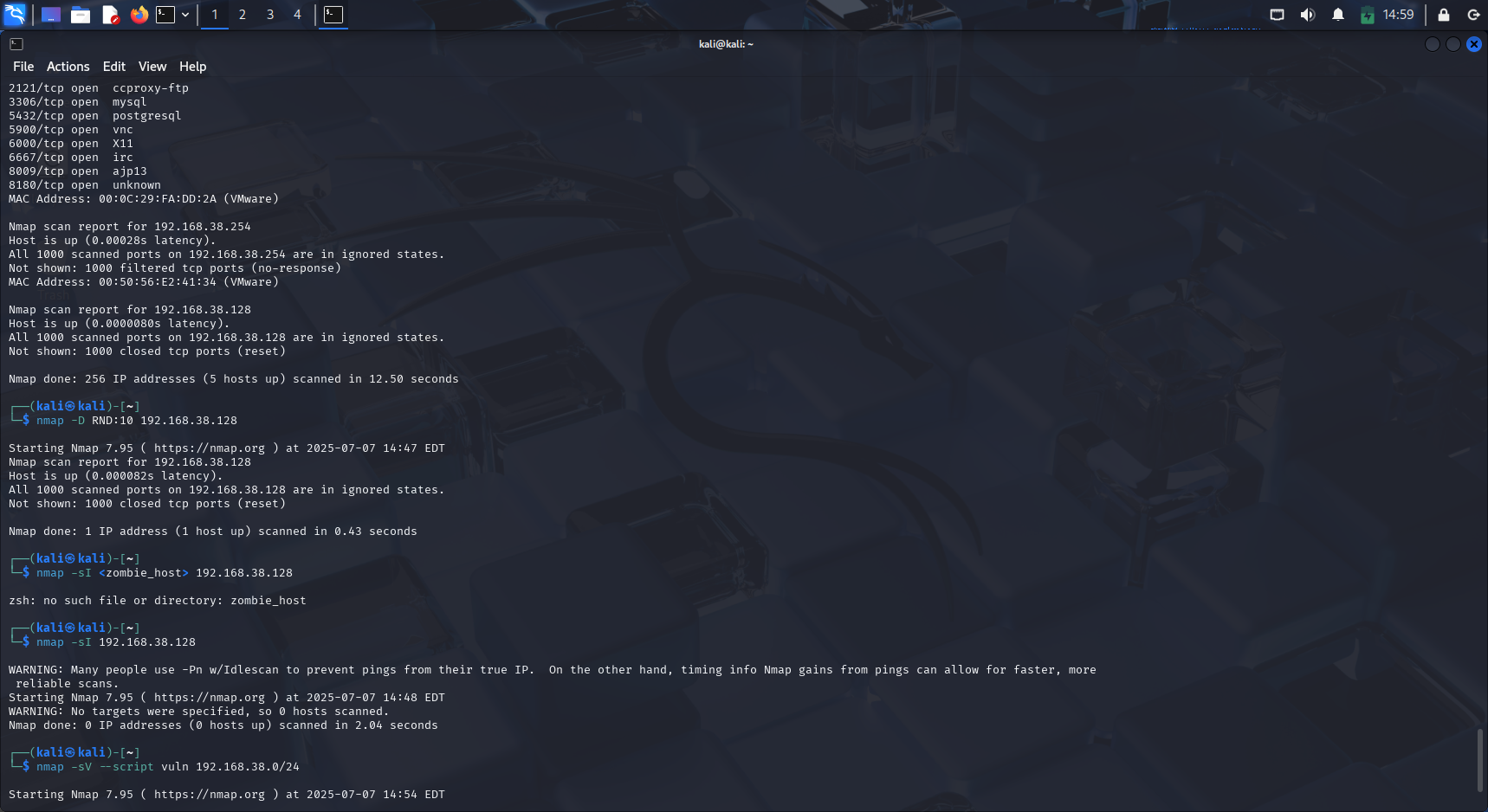


6)Segregates the vulnerabilities on the services that are accessible:

* Based on detected services and versions, the scanner compares them against known vulnerability databases (like CVEs).
* Helps identify misconfigured, outdated, or insecure services.

7)Bypass the security devices[firewall,IPS/IDS]:

* Security devices monitor and block suspicious scanning activity.



8)Select the right type of scanning techniques :

* Depending on your goals, system type, and security posture, you must choose the appropriate scan method:

** Fast scan**

** Stealthy scan**

** Full port scan**

** UDP scan**



Summary:

Network scanning involves identifying and analyzing devices on a network to assess security and functionality. It starts by selecting a target IP(192.168.38.128) or network range(192.168.38.0/24), then discovering active devices through host discovery(in 192.168.38.0/24 there are 5 hosts). Open ports are scanned to find accessible entry points, followed by identifying the services and their versions (-sV) running on those ports. Based on this information, known vulnerabilities are detected. To avoid detection by security devices like firewalls or IDS/IPS, stealth techniques such as packet fragmentation or decoy scans are used. The effectiveness of scanning depends on selecting the appropriate scan types (e.g., SYN, ACK, UDP) based on the goal, environment, and required level of stealth.