**TASK – 1**

**SCAN OPEN PORTS USING NMAP**

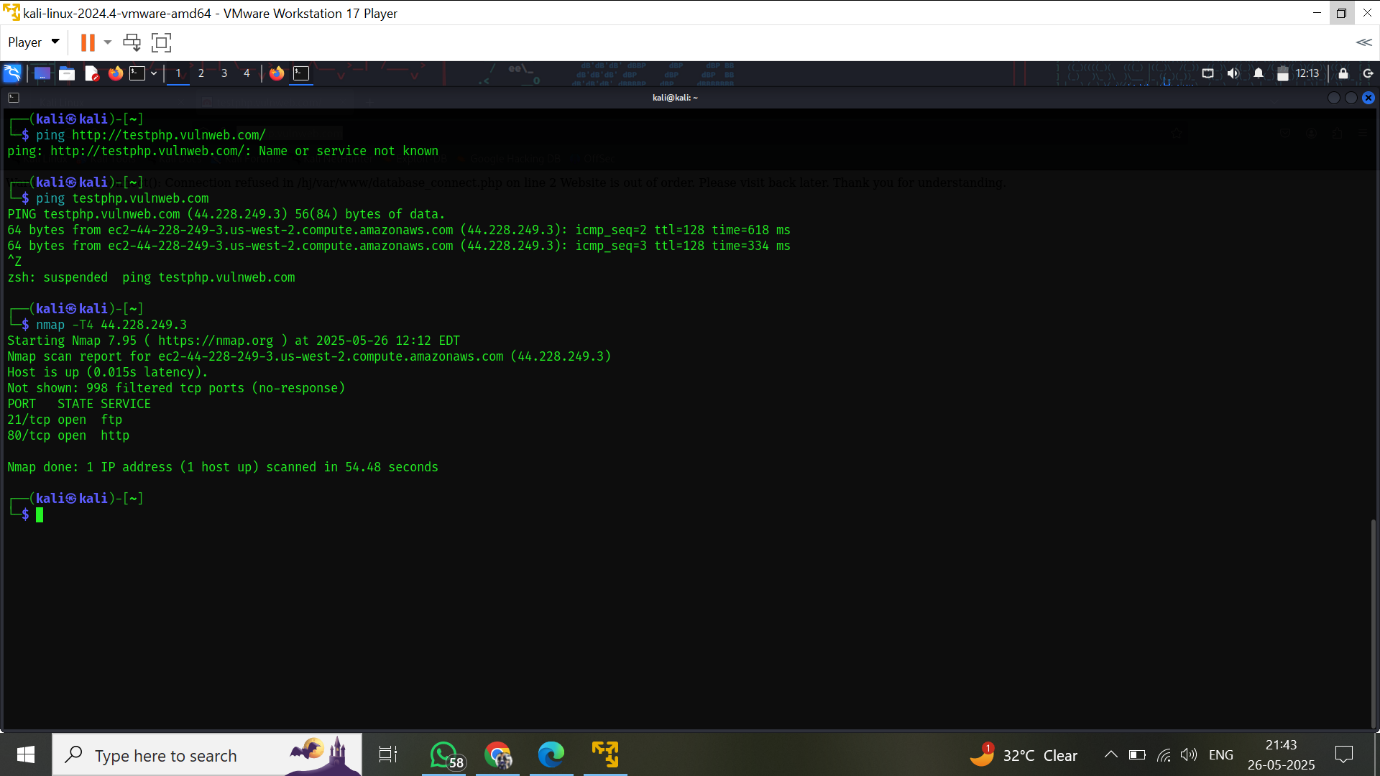
NMAP: Nmap (Network Mapper) is a powerful open-source tool designed for network exploration and security auditing. It is widely used by network administrators, penetration testers, and security professionals to discover hosts and services on a computer network, as well as to identify potential vulnerabilities.

Command:-

1. nmap -T4 44.228.249.3

Explanation

* **nmap**: The tool used for network scanning.
* **-T4**: This flag sets the scan to use the "Aggressive" timing template.
* **44.228.249.3**: The target IP address to scan.



**Key Points about -T4:**

* Much faster than the default (-T3), but increases the risk of detection by intrusion detection systems (IDS).
* Reduces the number of retries and timeouts, making scans complete more quickly.
* Suitable for responsive or local targets, but may overwhelm slow or sensitive systems

**Command:** nmap -sV 44.228.249.3

**Explanation of Flags**

* **nmap**: The tool for network scanning and security auditing[1](https://en.wikipedia.org/wiki/Nmap)[2](https://nmap.org/book/man.html).
* **-sV**: This option tells Nmap to perform service/version detection. Nmap will probe open ports to determine what service is running (e.g., Apache, SSH, FTP) and try to identify the exact version of that service[1](https://en.wikipedia.org/wiki/Nmap)[4](https://intellipaat.com/blog/nmap-commands/)5.
* **44.228.249.3**: The target IP address to scan.

