# ASSIGNMENT - 2

K. Naveen Abhiram

21BCE7357

## NMAP TOOL IN KALI LINUX

### NMAP

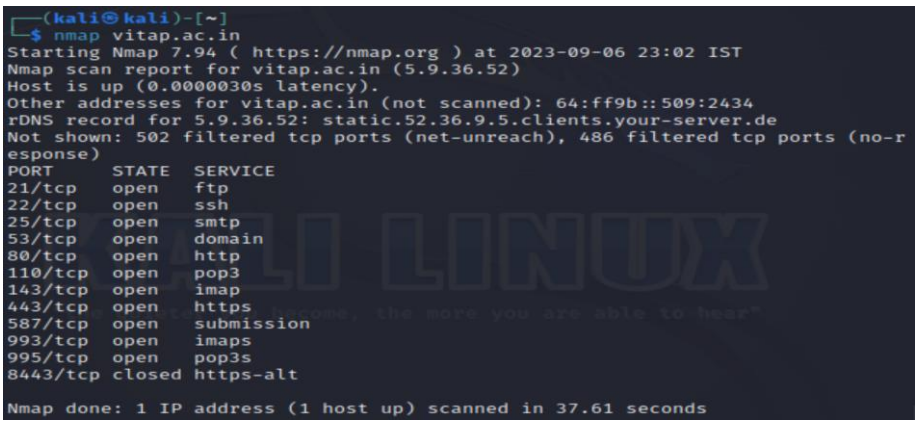
A potent open-source network scanning tool for network discovery and security audits is called Nmap (Network Mapper). It is frequently included in Kali Linux, and security experts, network administrators, and ethical hackers all utilize it extensively. You may investigate networks with Nmap and find hosts, services, vulnerabilities, and more.

### Command Commands:

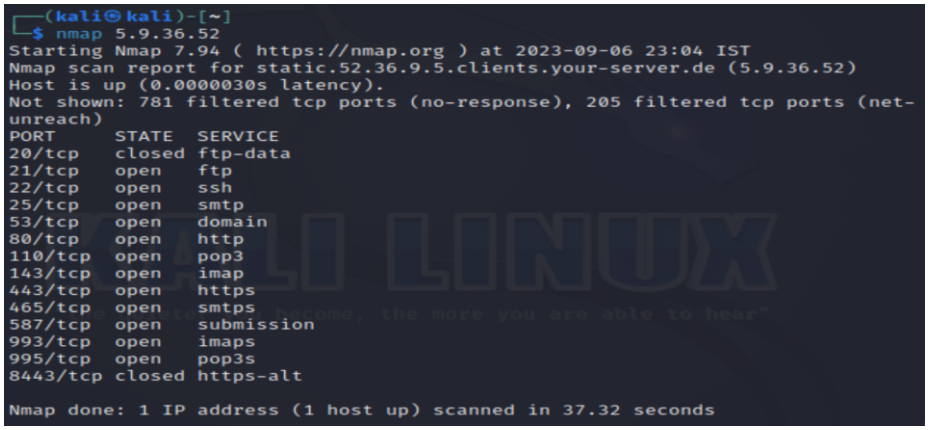
- -p: Specifies ports or port ranges to scan.
- -A: Enables OS detection, version detection, and script scanning.
- -oN: Saves output to a file.
- -sV: Attempts to determine the version of services running on open ports.
- -v: Increases verbosity for more detailed output.

### Simple Scan:

- nmap vitap.ac.in

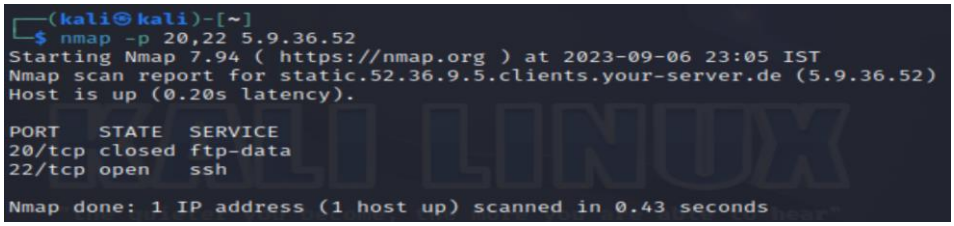


- nmap 5.9.36.52



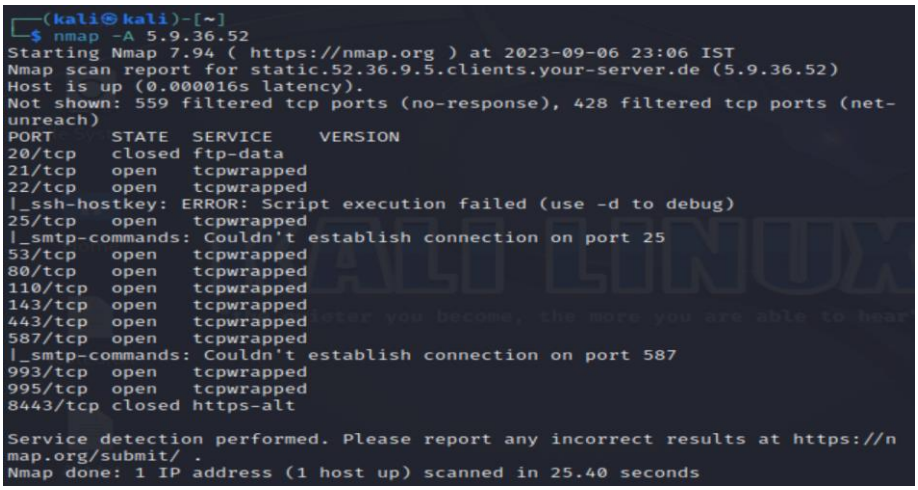

## Scan Specific Ports:

- nmap -p 20,22 5.9.36.52



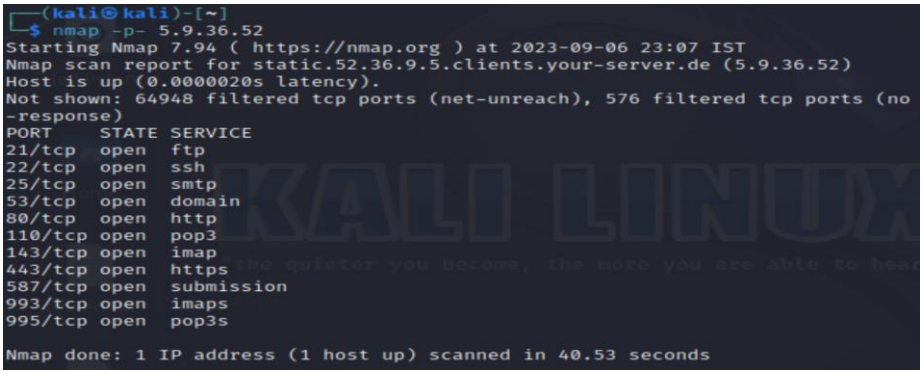

## Detect OS and Service Versions:

- nmap -A 5.9.36.52




## Scan All Ports:

- nmap -p- 5.9.36.52




## Scan UDP Ports:

- nmap -sU 5.9.36.52

## Save Output to a File:

- nmap -oN results.txt 5.9.36.52

Nmap offers a wide range of additional capabilities and options, such as the scripting engine (NSE) enabling unique scanning and sophisticated scripting. Nmap can be intrusive and may cause service disruptions, so use it responsibly and only on networks and systems you are permitted to scan. Always conduct network scanning in accordance with the law and ethical principles.