**Name** : Vaibhav Soni

**Enrolment No.** : IU2141230287

**Branch** : CSE – A

**Sem** : 7

**Subject** : Cyber Security

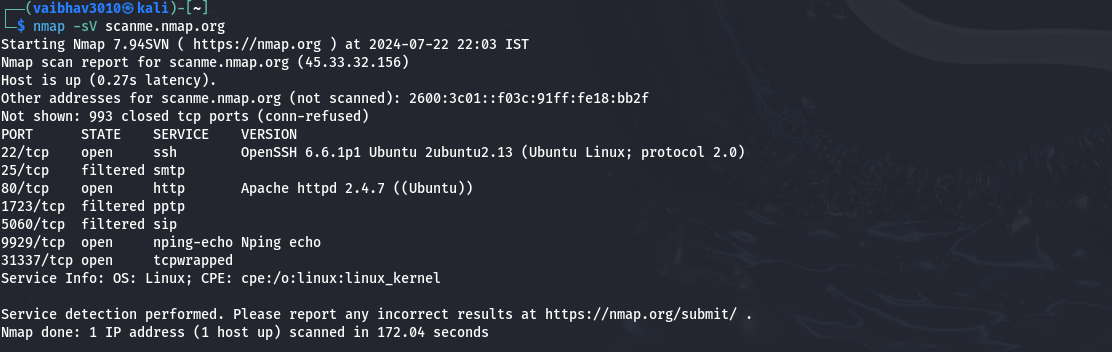
**Lab – 2**

**Aim :** Port Scanning using NMAP.

**Input :**

nmap -sV scanme.nmap.org

**Output :**

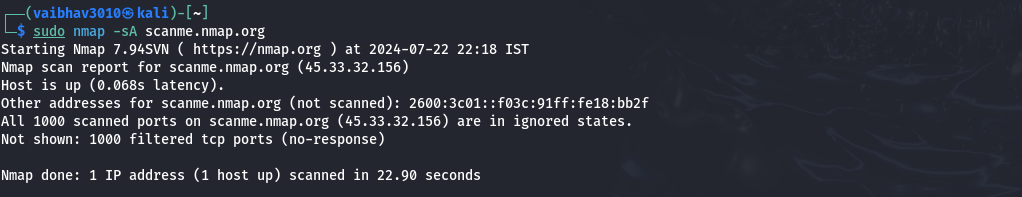
****

* The command `nmap -sV scanme.nmap.org` performs a service version detection scan on the domain `scanme.nmap.org`.This command is used to scan the target `scanme.nmap.org` to identify open ports and determine the version of the services running on those ports. This helps in understanding the software and versions in use, which can be useful for security assessments and network inventory.

**Input :**

nmap -sA scanme.nmap.org

**Output :**

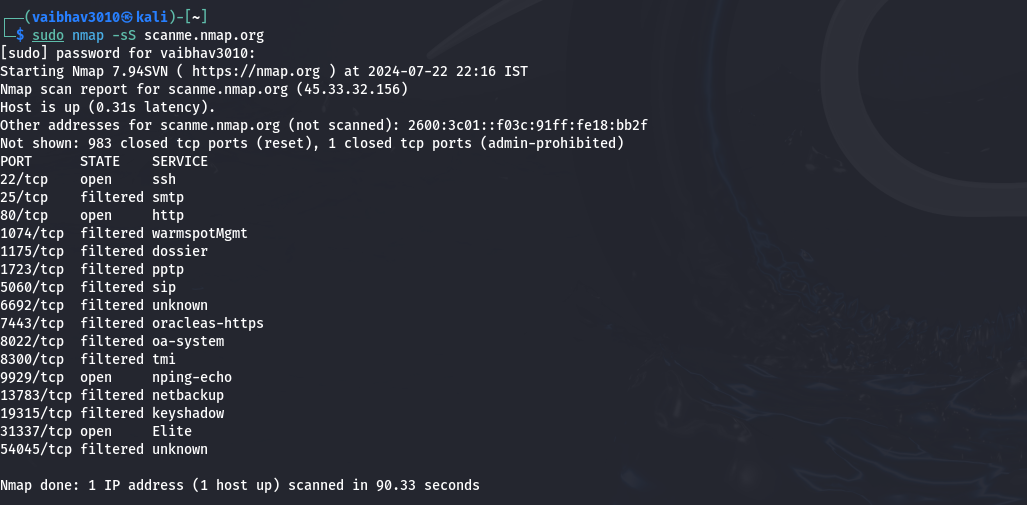
****

* The command `nmap -sA scanme.nmap.org` performs an aggressive scan to determine firewall rules, detect service versions, and assess the operating system of the target `scanme.nmap.org`. It provides detailed information about the target's network defenses and services.

**Input :**

nmap -sS scanme.nmap.org

**Output :**

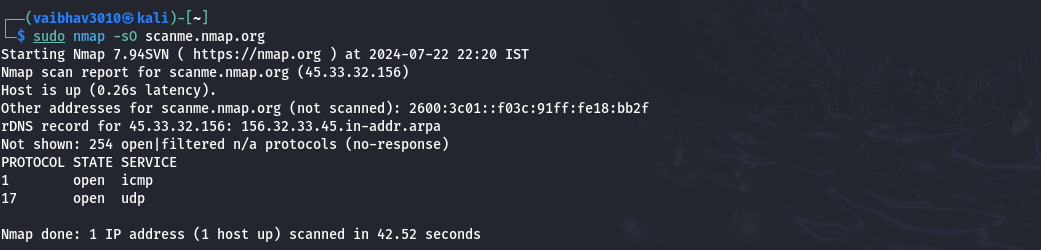
****

* The command `nmap -sS scanme.nmap.org` performs a TCP SYN scan on the target `scanme.nmap.org`. It checks for open ports by sending SYN packets and analyzing the responses, providing a quick and stealthy method to identify active services on the target.

**Input :**

nmap -sO scanme.nmap.org

**Output :**

****

* The command `nmap -sO scanme.nmap.org` performs an IP protocol scan on the target `scanme.nmap.org`. It identifies which IP protocols (such as ICMP, TCP, UDP) are supported by the target, helping to understand the network services and communication methods in use.