# NETWORK SCANNER USING NMAP

**PRESENTED BY**

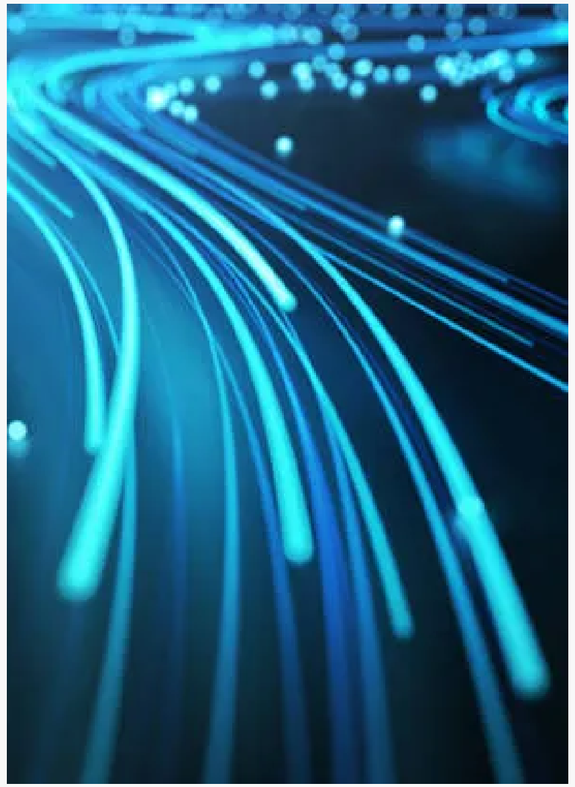
SONU KUMAR(RA2111030010021)

SHAURYA AGRWAL(RA2111030010009)

SIDDHARTH SAXENA(RA2111030010029)

# Objective

- Understanding Nmap's Role in Network Security,and its significance in  network security practices.
- Examine the various scanning techniques employed by Nmap, including host discovery, port scanning, version detection, and script scanning.
- Optimizing Scanning Methodologies:  Investigate strategies for efficient and stealthy network scans using Nmap, considering factors such as speed, accuracy, and minimizing the risk of detection by intrusion detection systems
- Conducting hands-on experiments with Nmap on test networks to showcase its practical application in different scenarios



# Introduction

Nmap, short for "Network Mapper," is a powerful and popular open-source tool for network exploration and security auditing.

It is designed to discover hosts and services on a computer network, creating a map of the network that can be used for various purposes, such as security assessments, network inventory, and troubleshooting

- Nmap can perform different types of port scans, such as TCP connect scans, SYN scans, and UDP scans. This helps identify open ports on target systems
- Often it determine the version and type of services running on open ports. This is useful for identifying potential vulnerabilities.
- includes a scripting engine (NSE) that allows users to write and execute scripts for a wide range of tasks, including vulnerability detection, service enumeration, and more

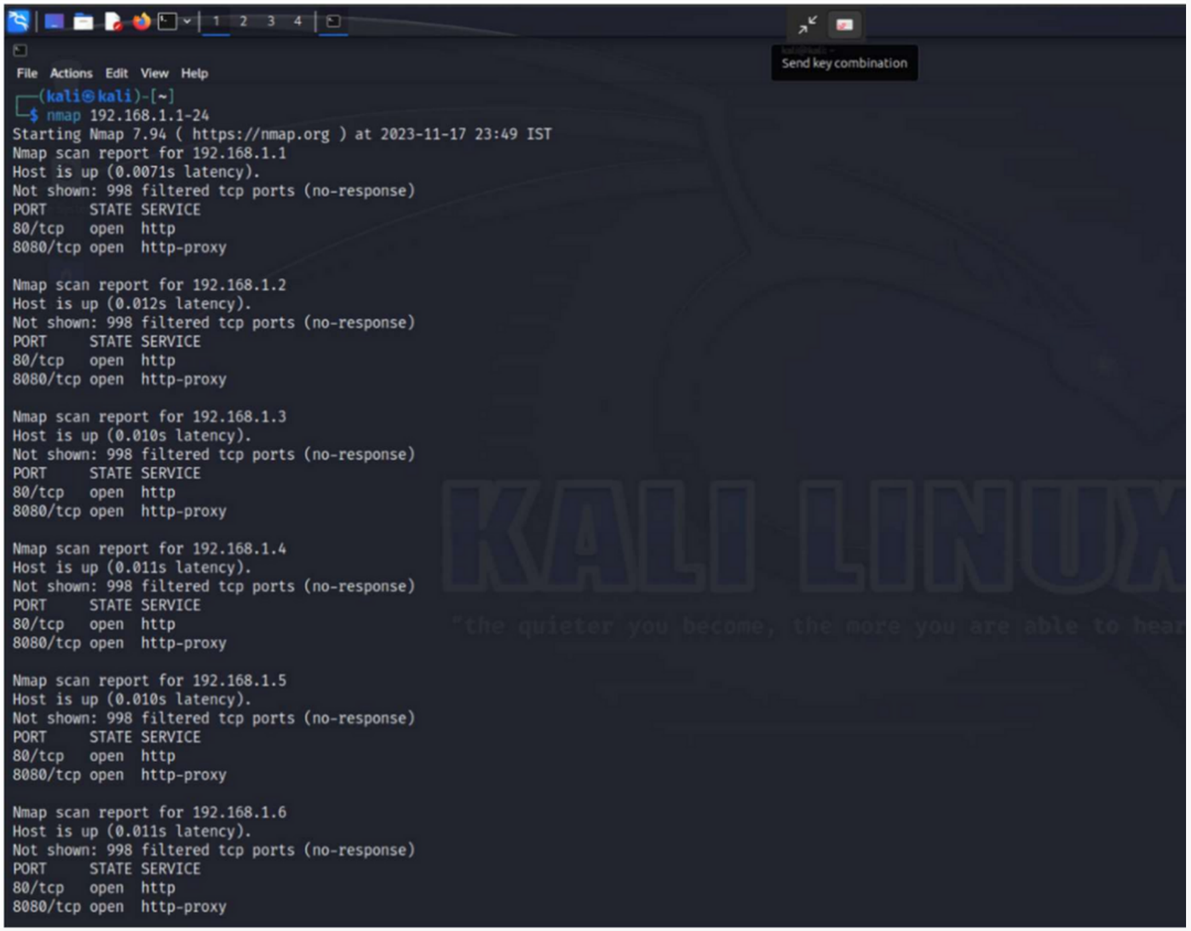
# Algorithms

- Network Discovery Algorithm: List of active networks
- Port Scanning Algorithm: List of open ports
- Operating System Detection Algorithm: Detected operating systems running
- Service Detection Algorithm: List of running services with version
- Customized Scanning Algorithm: Customized scan results

# Protocols

- ICMP (Internet Control Message Protocol): Used for network discovery to identify active hosts
- TCP (Transmission Control Protocol): TCP is a fundamental protocol for port scanning.
- UDP (User Datagram Protocol): Service Detection, Nmap employs UDP packets for service detection
- OS Detection Protocols: Operating System Detection , Nmap employs a combination of protocols and probes, including TCP and UDP, for operating system detection
- SNMP (Simple Network Management Protocol): Information Gathering

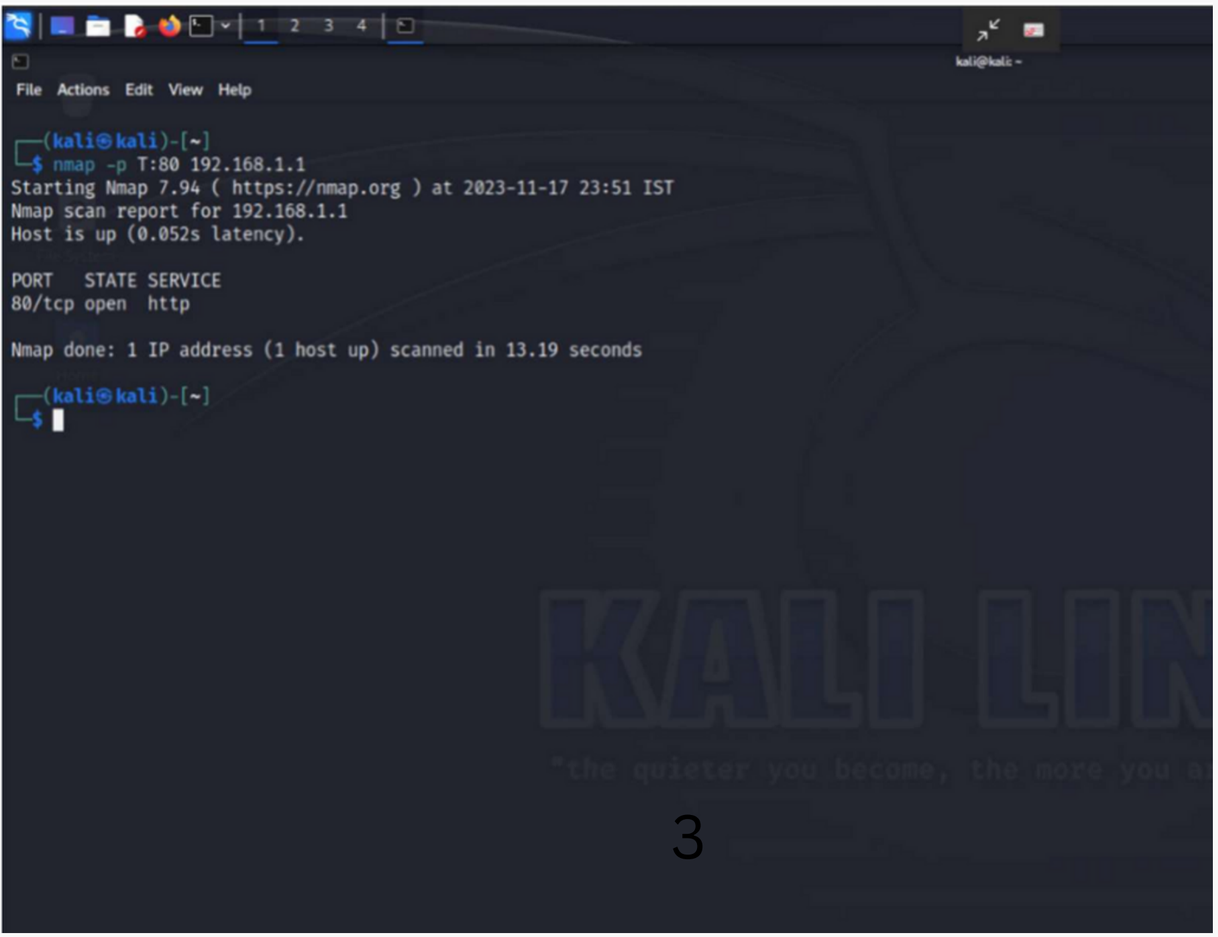
# Implementation



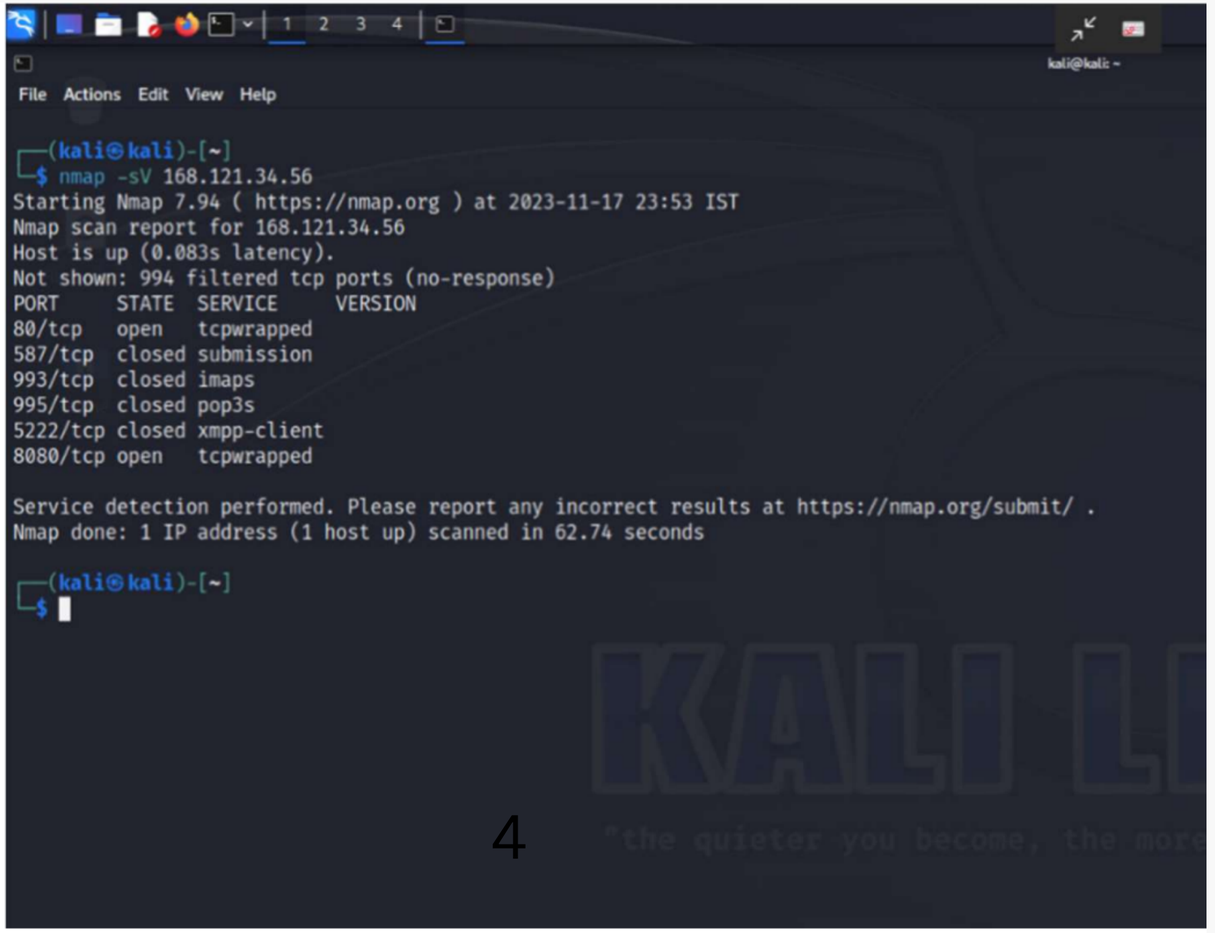


1 1

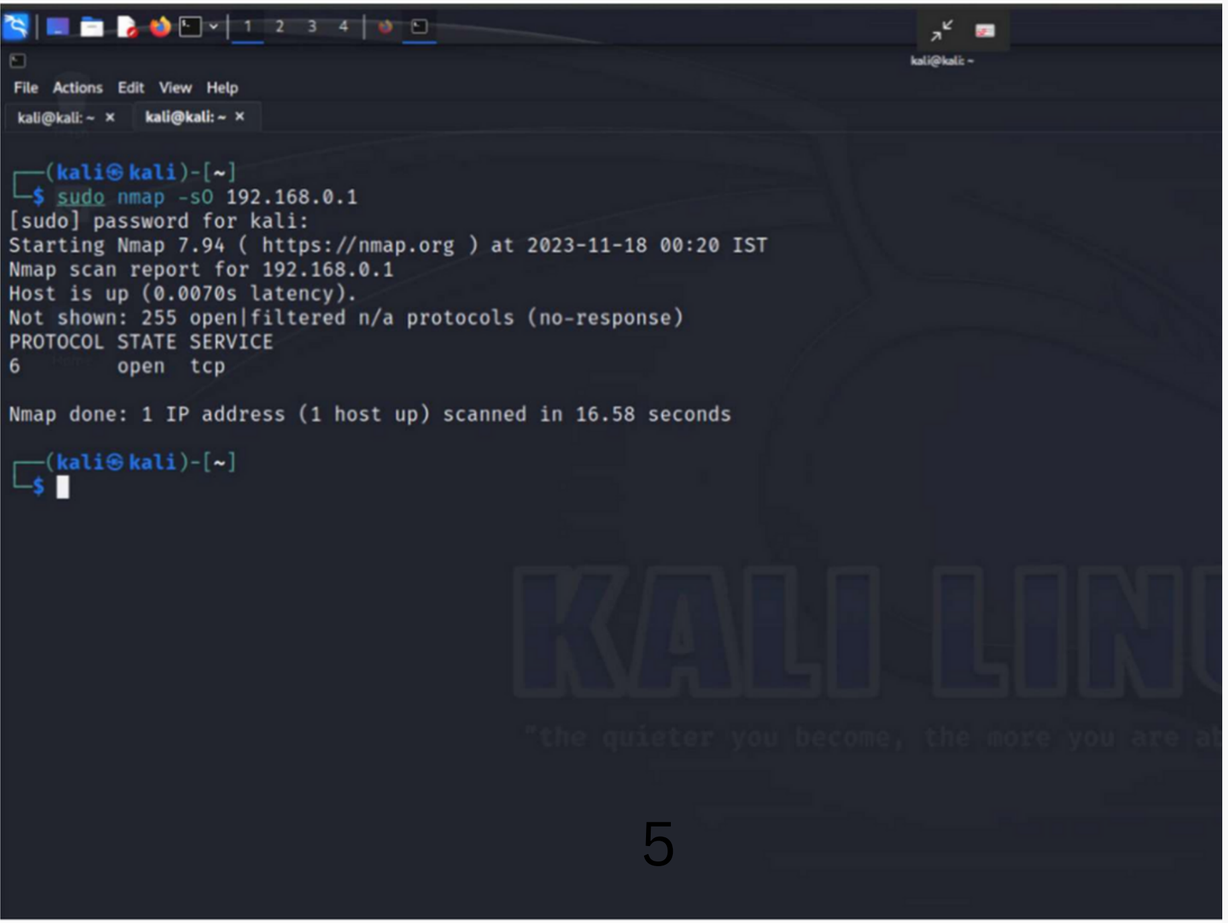
22


File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -p T:80 192.168.1.1
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-17 23:51 IST
Nmap scan report for 192.168.1.1
Host is up (0.052s latency).
PORT STATE SERVICE
80/tcp open http
Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
(kali㉿kali)-[~]
$

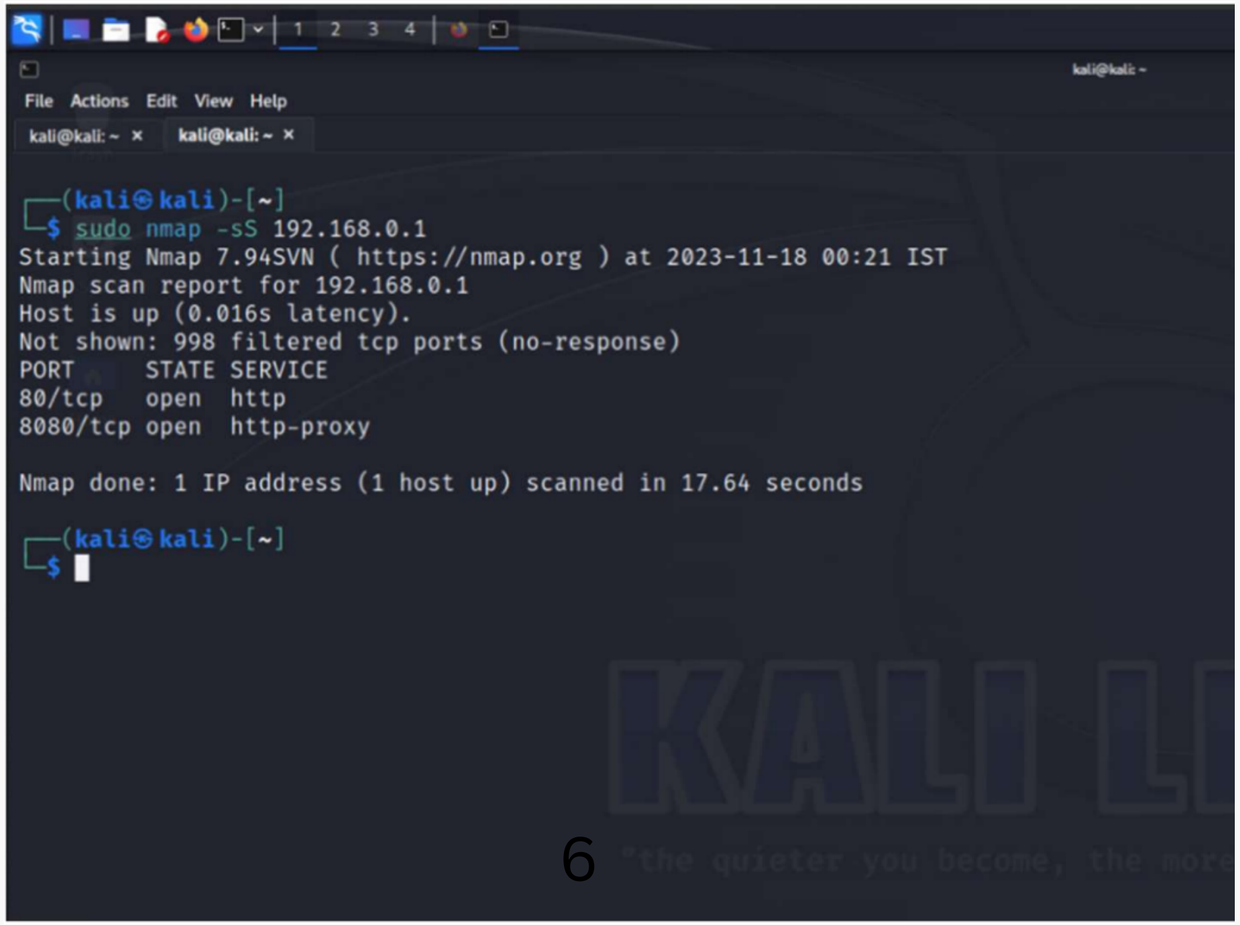
3


File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sV 168.121.34.56
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-17 23:53 IST
Nmap scan report for 168.121.34.56
Host is up (0.083s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
80/tcp open tcpwrapped
587/tcp closed submission
993/tcp closed imaps
995/tcp closed pop3s
5222/tcp closed xmpp-client
8080/tcp open tcpwrapped
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 62.74 seconds
(kali㉿kali)-[~]
$

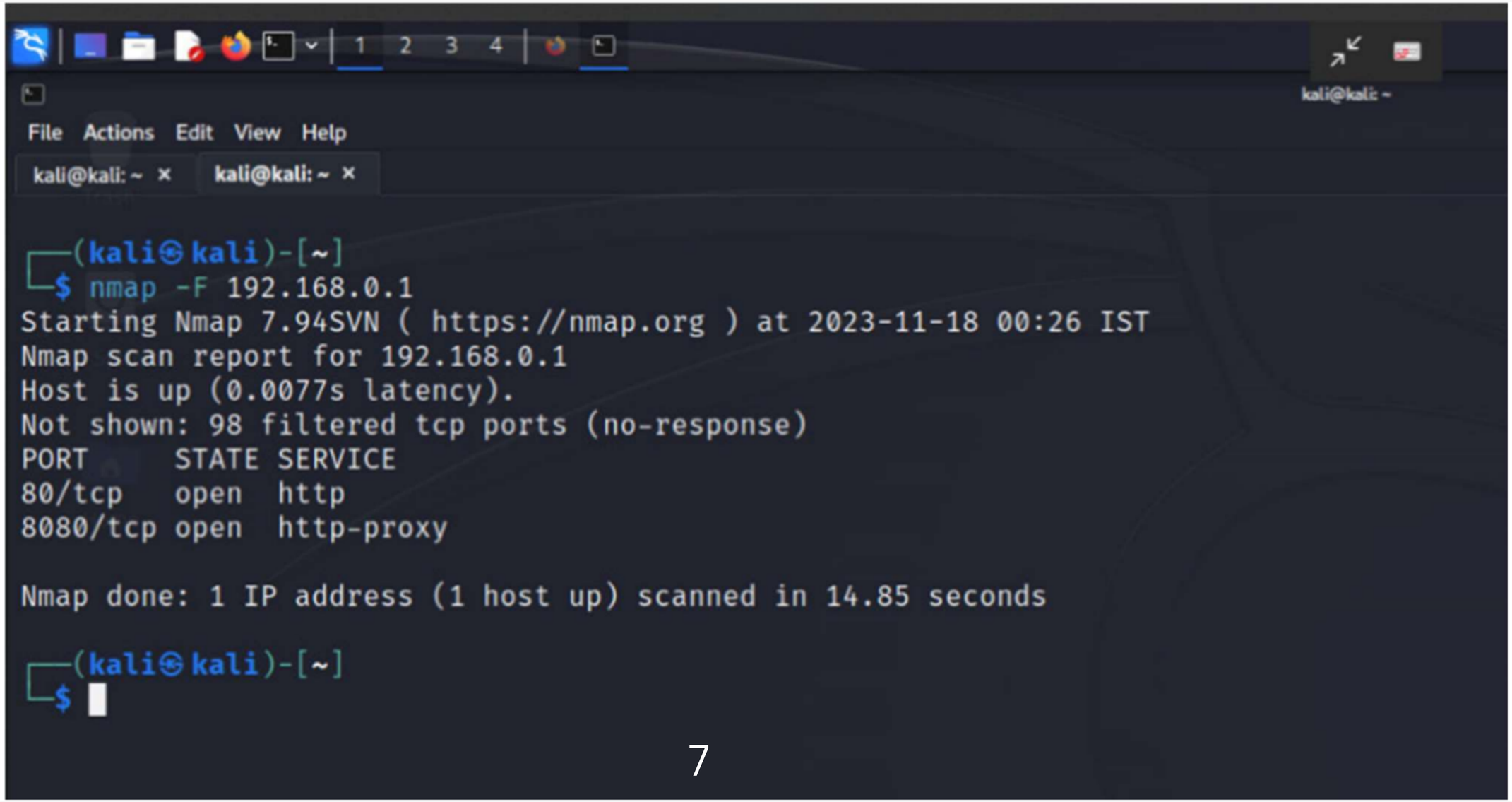
4


File Actions Edit View Help
kali@kali: ~
kali@kali: ~
(kali㉿kali)-[~]
$ sudo nmap -sO 192.168.0.1
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-18 00:20 IST
Nmap scan report for 192.168.0.1
Host is up (0.0070s latency).
Not shown: 255 open|filtered n/a protocols (no-response)
PROTOCOL STATE SERVICE
6 open tcp
Nmap done: 1 IP address (1 host up) scanned in 16.58 seconds
(kali㉿kali)-[~]
$

5


File Actions Edit View Help
kali@kali: ~
kali@kali: ~
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-18 00:21 IST
Nmap scan report for 192.168.0.1
Host is up (0.016s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 17.64 seconds
(kali㉿kali)-[~]
$

6


1 2 3 4
kali@kali: ~
File Actions Edit View Help
kali@kali: ~ ×
kali@kali: ~ ×
┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-18 00:26 IST
Nmap scan report for 192.168.0.1
Host is up (0.0077s latency).
Not shown: 98 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
8080/tcp open http-proxy
Nmap done: 1 IP address (1 host up) scanned in 14.85 seconds
┌──(kali㉿kali)-[~]
└─$

# Conclusion

- In conclusion, the exploration of network scanning using Nmap reveals a multifaceted approach to understanding and securing computer networks. Nmap, as an open-source tool, proves to be a cornerstone in the arsenal of cybersecurity professionals and network administrators
- The algorithms presented shed light on the intricacies of network discovery, port scanning, operating system detection, and service identification. These algorithms form the backbone of the project
- Network scanning using Nmap emerges not only as a technical endeavor but also as a strategic approach to fortifying digital ecosystems. By combining theoretical knowledge, practical implementation, and ethical considerations, this report aims to contribute to the ongoing discourse on cybersecurity practices