Practical 1

Environment setup

A screenshot of a computer

Description automatically generated

Open kali linux

A screenshot of a computer

Description automatically generated

Turn on power on this virtual machineA screenshot of a computer

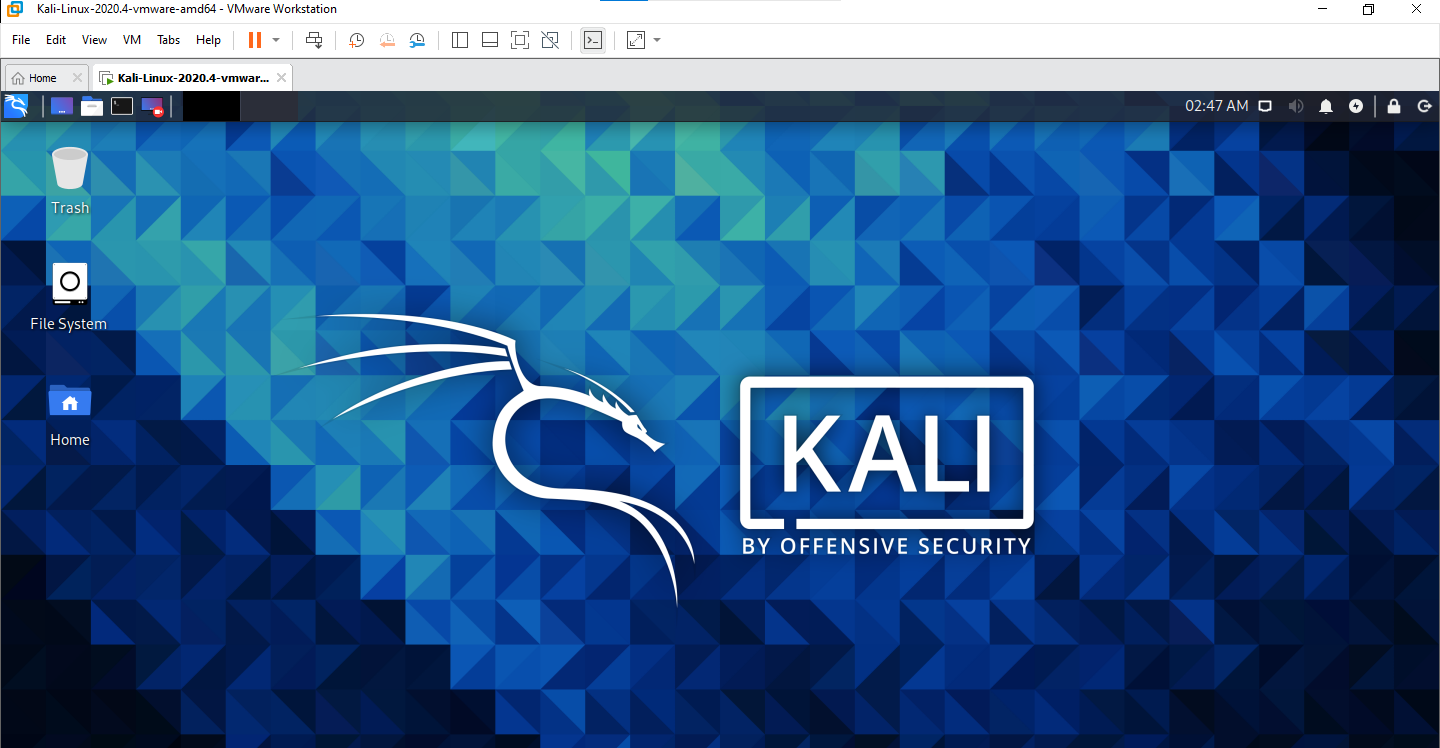
Description automatically generated

Username kali

Password kali

A screenshot of a computer

Description automatically generated



**Practical 2**

Uses of open-source intelligence and passive reconnaissance

Use of open-source intelligence and passive reconnaissance ( 2 )

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer code

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A blue background with white text

Description automatically generated



A screen shot of a computer

Description automatically generated

A screen shot of a computer

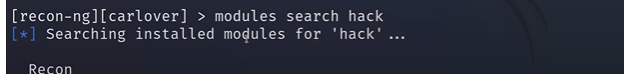
Description automatically generated

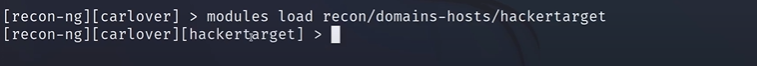
A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated





A screen shot of a computer

Description automatically generated







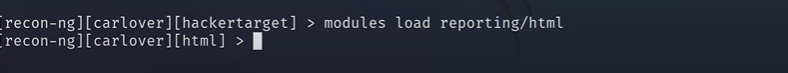
A screenshot of a computer

Description automatically generated



A screen shot of a computer screen

Description automatically generated





A screenshot of a computer program

Description automatically generated

A computer screen shot of a computer code

Description automatically generated







A screenshot of a computer

Description automatically generated

A screenshot of a computer

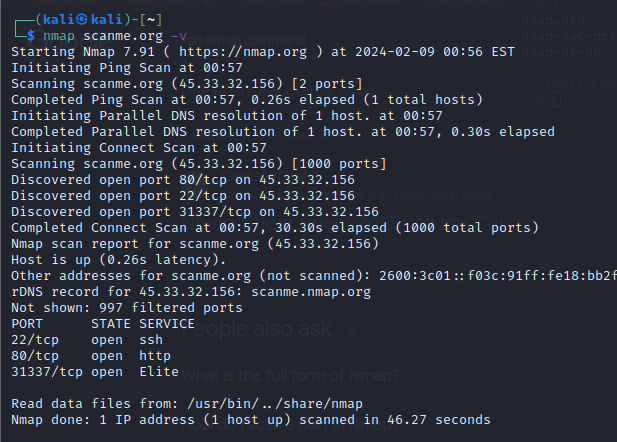
Description automatically generated

**Practical 3**

Aim : on enumerating host, port, and service scanning

Step 1:

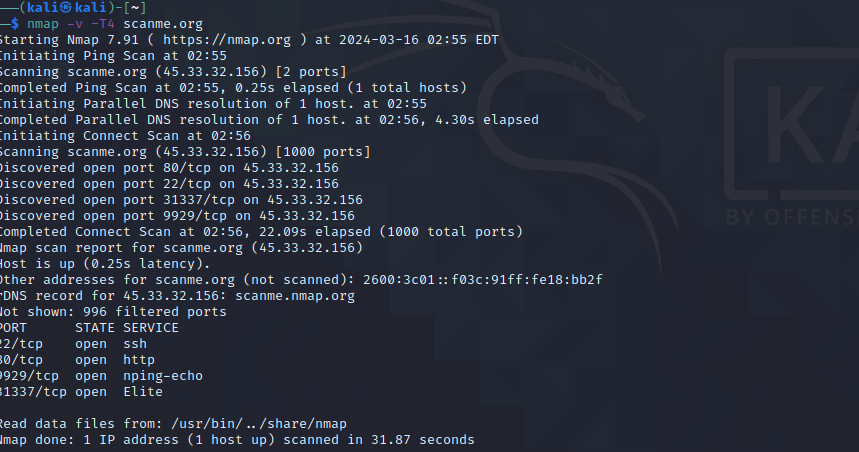
Run command : nmap scanme.org -v

-v :stand for verbose . It provides detailed and extensive output or information

Step 2:

Command : nmap -v -T4 scanme.org

-T4: Set timing template (higher is faster)



Step 3:

command : sudo nmap -v -sT -scanme.org

-sT: Scan TCP

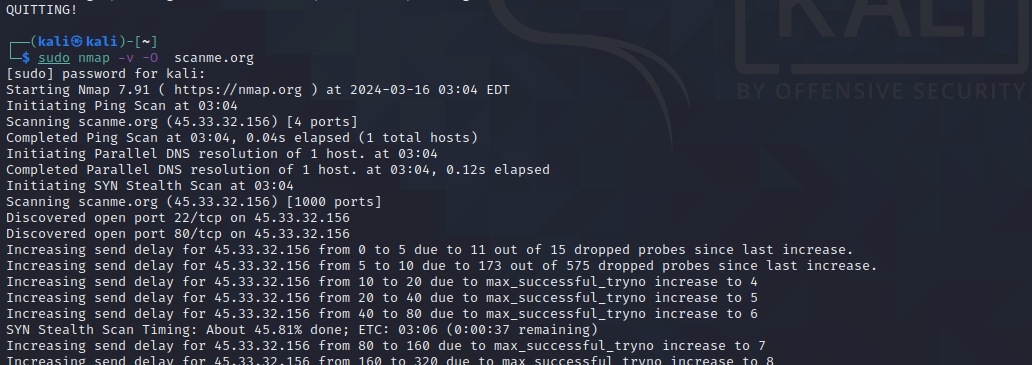
A screenshot of a computer program

Description automatically generated

Step 4:

Command : sudo nmap -v -O scanme.org

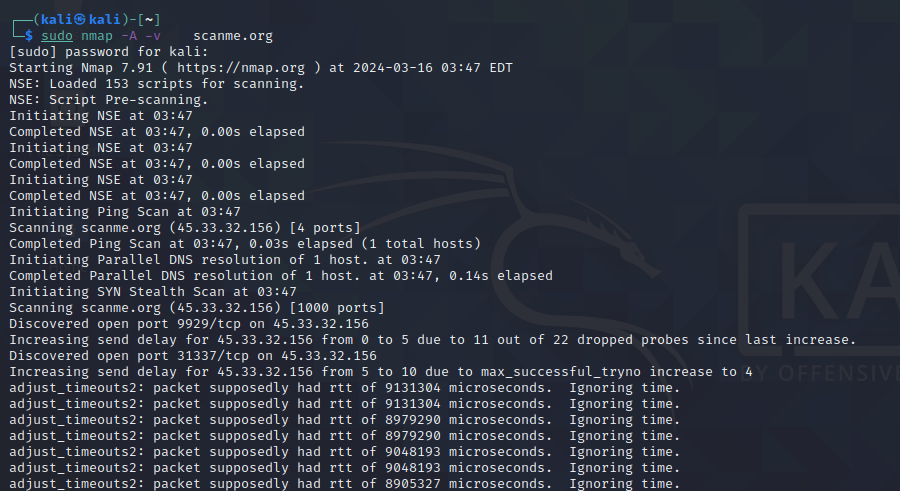
-O :Detect Operating system



Step 5

Command : sudo nmap -v -A scanme.org

-A aggressive scan



Practical 4

AIM on vulnerability scanning and assessment

ZAP

A screenshot of a computer

Description automatically generated

Use can type any domain in url attack box

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

.

Practical 5

AIM : on use of Social Engineering Tookit

Step 1:

A blue line with white text

Description automatically generated

Step 2:

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

A screen shot of a computer

Description automatically generated

A screen shot of a computer screen

Description automatically generated

A computer screen shot of text

Description automatically generated

A screenshot of a computer program

Description automatically generated

New tab

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

Practical 6

AIM : Exploit web based application

Using nmap

Command:

sudo nmap -v -sA -O -sV open.spotify.com -T4 --script=vulners

sudo stand for super user

nmap stand for network mapping

-v stand for verbose

-O stand for finding operating system

-sA stand for aggressive scan

-sV stand for version detection

-T4 kuch tho tumlog search karo

--script=vulners it scan vulnerability

Or external k time ye ek command type kar k mat baith jana divided kar k scanning perform karna

Like

sudo nmap -v open.spotify.com

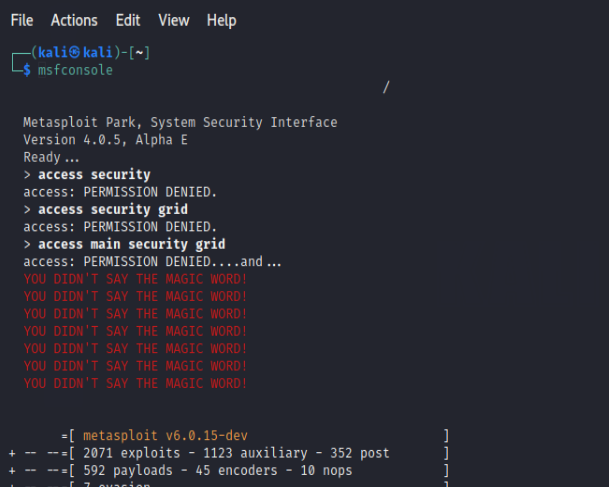
sudo nmap -v open.spotify.com -O

sudo nmap -v open.spotify.com -O -sA

sudo nmap -v open.spotify.com -O -sA --script=vulners

Practical 7

AIM : using Metasploit Framework for exploitation







A screen shot of a computer program

Description automatically generated

A computer screen shot of a program

Description automatically generated

A screen shot of a computer

Description automatically generated

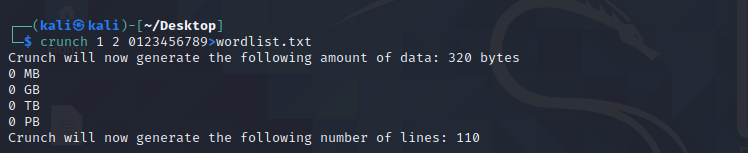
A screenshot of a computer code

Description automatically generated

Practical 8

Aim based on Password analysis for password cracking

Command : crunch 1 2 12345678>wordlist.txt



command : crunch 10 10 -t manav^%%%%

