3. Configure the Kali Linux Virtual Machine:

- In the VirtualBox Manager, select the newly created virtual machine and click on "Settings."
- In the settings window, navigate to the "Storage" tab.
- Under "Controller: IDE," click on the disk icon next to "Empty" and choose the Kali Linux ISO file you downloaded.
- Click "OK" to save the settings.

4. Install Kali Linux:

- Start the Kali Linux virtual machine by selecting it in the VirtualBox Manager and clicking on the "Start" button.
- The Kali Linux installation process will begin. Follow the on-screen instructions to install Kali Linux within the virtual machine.
- After the installation is complete, restart the virtual machine.

5. Set Up Kali Linux:

- Log in to Kali Linux using the credentials you created during the installation process.
- Configure the network settings, update the system, and install any desired tools or packages within Kali Linux.

By following these steps, you will have successfully installed VirtualBox and set up Kali Linux as a virtual machine.

Note: It's important to ensure you have sufficient system resources (CPU, RAM, disk space) to run Virtual Box and the virtual machine smoothly.

Pre-Skill Task:

1. What is VirtualBox, and what is its purpose in the context of virtualization?

Virtual Box can be used for a variety of puposes, including
* Testing and development
* Education
* I administration
* personal use

2. Explain the benefits of using virtualization for running operating systems.

many benefits to useing virtualization
* cost savings
* Increased flexibility
* Improved security
* simplief management

Experiment #		Student ID	
Date		Student Name	

3. Can you provide a step-by-step guide on how to install VirtualBox on a specific operating system?

1. go to the virtual Box download page
2. Run the installer and follow on-screen
3. During the installation, you will be asked enable hardward
4. once virtualBox is installed, you can start creation machine
5. In the "Name" field, enter a name for you virtual machine
6. In the "Version" select version
7. In the "memory" enter amount of memory

4. What are the minimum system requirements for running VirtualBox effectively?

the minimum system requirements

* CPU :- A processor with hardware virtualization support
* RAM :- 4GB of RAM recommended for running single virtual machine
* Storage :- At least 20GB of free disk
* Graphics card :- A graphics card with 2D acceleration is recommended

5. How do you create a new virtual machine in VirtualBox? Explain the necessary steps.

1. open virtualBox
2. Click on "New" button
3. In the "name" field, enter name
4. In "OS" field select you installar
5. In "Version" select version
6. In "Memory". Select memory amount
7. In "HardDisk" select Create virtual hard disk
8. In "file location" enter location
9. In "file size" enter location
10. Click "create" button in VM

Experiment #		Student ID	
Date		Student Name	

In-Skill Task:

Harsha a technology evangelist has just started learning about OS virtualization and interestedin learning ethical hacking as Harsha a newbie in this you are requested by Harsha to help himto install Kali Linux in his computer using Virtual Box

1. Download and install virtual Box on harsha's computer
2. Download kali Linux iso image file from kali
3. Create anew virtual machine in VirtualBox. In the "Name" field, enter a name for the virtual Box such as 'kali Linux' In the "OS" field, select "Linux". In the "version" field Select "Debian 11 (Bullseye)" In the "Memory" enter amount
4. once the virtual machine is created, start it by clicking on the "Start" Button
5. follow the on-screen instruction to install kali Linux
6. once kali Linux is installed, you can start useing it for ethical hacking

here are some additional tips for kali Linux

* Make sure that harshas computer has enought RAM
* Make sure that harshas computer has enought disk space to store the kali Linux
* If harsha is not sure how to install kali Linux Find Instruction

Experiment #		Student ID	
Date		Student Name	

Viva questions:

1. Describe the process of downloading the Kali Linux ISO image and selecting the appropriate version.

1. go to kali Linux download page
2. on the download page, you will see a list of available
3. Select the version kali Linux that you want to install
4. Click on "Dowload" button to download

2. What are the recommended settings for a virtual machine running Kali Linux in terms of memory allocation, CPU, and storage?

* memory: 4 GB of RAM is minimum recommended amount
* CPU: 2 cores is the minimum recommended no of CPU cores for virtual machine
* Storage: 20GB of disk space is miminum recommended amout of space

3. What is the significance of enabling virtualization features in the computer's BIOS settings?

* Allow you to run multiple operating system simulataneously
* Improves performance
* Increases security

4. Explain the network configuration options available in VirtualBox and their implications for a virtual machine running Kali Linux.

* NAT : this is default network configuration
* Bridge:-In bridge mode, VM is connected
* Host-only:-In host only mode, VM is accessible
* Internals:-In internal's VM is only accessible

5. How do you mount the Kali Linux ISO image to the virtual machine and initiate the installation process?

1. Open VB
2. Select virtual machine that you want install
3. Click on "setting Button"
4. In "Storage" select on controller
5. Click on "Add" button

6. In "storage" select Add
7. Click on "open"
8. Click on "ok" button to close
9. Click on "start" button to start

Experiment #		Student ID	
Date		Student Name	

Post Skill Task:

1. Why Kali Linux is newbie friendly for cyber Security enthusiast?

* pre-installed tools
* well-documented
* user-friendly interface
* Active-community

2. What are different types of Linux Distro's available?

* Desktop distro's
* Live distros
* server distro's
* Hobby-distros
* embedded distro's

3. List some security focused Linux Distro's available.

* kali Linux
* parrot security os
* BlackArch Linux
* DEFT Linux
* caineOS
* focused distro

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured:_____out of _____

Experiment #		Student ID	
Date		Student Name	

Pre-Skill Task:

1. What is packet capturing, and why is it important in network analysis and security?

* Trouble shooting network problems
* Investigating security incidents
* monitoring network traffic
* Gathering evidence

2. Can you explain the purpose and functionality of Airodump-ng?

* Scanning for wireless network
* monitoring wireless network
* Capturing handshakes
* can be used with other tools

3. What are the prerequisites and system requirements for using Airodump-ng effectively?

* prerequisties
* System requirements
* use a high-again antenna
* use a directional anetena
* Be patient
* use a security professional

4. How does Airodump-ng capture packets from wireless networks? Explain the underlying mechanism.

1. the Airodump-ng tool is run on computer
2. the wireless adapter is set on monitor mode
3. Airodump-ng sens s for wireless network
4. Airodump-ng identifies wireless network are using the same channel as wireless adaptor

5. What are the different types of information that can be obtained by analyzing captured packets with Airodump-ng?

once the wireless adaptor is monitor mode, Airodump-ng can use it to capture packets from the wire network Airodump-ng capture these handshake packets and store them in file

Experiment #		Student ID	
Date		Student Name	

In-Skill Task:

1.Ramesh wants to perform "CRACKING WEP KEYS" By using Monitor mode which was available in kali Linux. So, he wants to perform following operations:

1.Monitor mode using wifi-adapter

2 .Capturing packets

3. Capturing ARP requests

Help him by doing those operations Successfully(If Possible include screenshots of those outputs)

Solution:

To enable monitor mode on wifi adapter, you will need to :-

1. check if your wifi adapter support monitor mode. not all wifi adaptor support monitor mode, so you will be check the quick online search
2. If your wifi adapter supports monitor mode, you will need to correct driver for it. the driver will allow to connect
3. once the drivers are installed, you can enable monitor mode by running command.

Viva Questions:

1. How can Airodump-ng help in analyzing wireless network security vulnerabilities, such as identifying rogue access points or detecting unauthorized clients?

2. What are the different filtering options available in Airodump-ng, and how can they be used to focus on specific network or device information?

3. Explain the significance of different fields displayed in the Airodump-ng output, such as BSSID, ESSID, Power, Channel, and Encryption.

4. How can you interpret and analyze the collected data in Airodump-ng, such as identifying patterns, trends, or potential security issues?

5 Are there any limitations or challenges associated with using Airodump-ng for packet capturing and analysis? How can these limitations be mitigated or overcome?

1. * identify rogue access points
   * Detect unathorized clients
   * capture handshake

2. * -b or --bssid
   * -c or --channel
   * -e or --essid
   * -t or --encrypt
   * -m or --mac

3. * BSSID
   * ESSID
   * Power
   * channel
   * Encryption

4. * identifying rogue access points
   * Detecting unathorized clients
   * Identifying weak encryption
   * Identifying hidden networks
   * Identifying clients that are useing the same SSID

5. * Legality
   * Required root privilege
   * Interferes with network traffic
   * can be slow
   * Not user-friendly

Experiment #		Student ID	
Date		Student Name	

Post-Skill-Task:

1) write the steps of analyzing packet capturing using Airodump-ng,

Sol) * install Airodump-ng.
* Enable monitor mode
* Start Airodump-ng
* Scan for network
* Filter the result
* Interpret the result
* Save the result
* use the help menu
* Consult with a security expert

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation
	Marks Secured:_____out of _____ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

Experiment #		Student ID	
Date		Student Name	

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 21CS3041RA
CRYPTANALYSIS AND CYBER DEFENSE WORKBOOK

3. Implementation of Social Engineering Using King Phisher

Date of the Session:___/___/___ **Time of the Session:_____to_____**

Learning Objective:

The learning objective of implementing social engineering using King Phisher is to understand the techniques and tools used in social engineering attacks and gain practical experience in conducting such attacks in a controlled environment.

Description:

Social engineering is a method of manipulating individuals to disclose sensitive information or perform certain actions by exploiting their trust, curiosity, or ignorance. King Phisher is an open-source software tool that helps simulate and test social engineering attacks, allowing organizations to assess their vulnerability to such attacks and develop countermeasures. This project involves implementing social engineering attacks using King Phisher to understand the various attack vectors, analyze their effectiveness, and explore ways to mitigate the associated risks.

Pre-Requisites:

1. King Phisher: An open-source phishing campaign toolkit.

2. Virtual Machine or Sandbox Environment: To set up a controlled environment for testing and executing social engineering attacks.

3. Operating System: Linux distribution (recommended) or Windows with a virtualization platform like VirtualBox or VMware.

Pre-Skill:

1. What is social engineering, and why is it considered a significant threat to organizations?

Social engineering is a type of attack that relies of human interaction to trick people into professionals

* phishing
* pretexting
* quid pro quo

2. Explain the concept of phishing and how it is used in social engineering attacks.

Dear [victim name]
we ate writing to inform you that we have detected
suspicious activity
[link to fake website]
IF you to do click on link within 24 hours
Sincerely,

3. What is King Phisher, and what functionalities does it offer for conducting social engineering attacks?

king phistoe are often sucessful because they exploit people's natural tendency to trust other behelpful

1. phishing
2. Speak phishing
3. whaling
4. Smishing and vising
5. Barting
6. piggybacking

4. Describe the process of setting up a virtual machine or sandbox environment for implementing social engineering using King Phisher.

Spear phishing is a more enaught target form the attack. Ina specifically target a particulat individual or oganization. the attack will gather information about the target, the job title and company a mote email to text message

5. How can King Phisher be used to create and customize phishing campaigns?

In king phisher To protect yourself from software is important to be aware to be different type of attacks and to be skeptical of any emails or text message from unknown senders.

Experiment #		Student ID	
Date		Student Name	

In-Skill Task:

1) Siddharth is a Computer Science Student and he is Naughty. He wants to fool his friend Siva by sending a Fake Mail by King Phisher tool. But he doesn't know that how that tool Works.

a. He want to learn How the Tool (King Phisher) Works .

So, Help Siddharth to understand how the Tool Work in a step by step process.

the BSSID, ESSID, power, channel and Encryption fields are all important for understanding the security of a wireless network; the BSSID and ESSID can be used to identify the access the point and network

a. Virtual Box is a free and open-sources hypervisor that allows users to create and run (VMs) on their computer A hypervisor is a software layer that allows multiple operating system on sample physical computer

Dear [victim name];

we are writing to inform you that we have detected

[link to fake website]

If you do not click on link within 24 hours, your account will be suspended

Sincerely,

the [Bank name] Team

Experiment #		Student ID	
Date		Student Name	

Viva Questions :

1 - What are the different types of social engineering attacks that can be simulated using King Phisher?

2 - What are the potential risks and ethical considerations involved in implementing social engineering attacks using King Phisher?

3 - How can organizations defend against social engineering attacks, and how can the insights gained from using King Phisher be utilized to improve security measures?

4 - Discuss the legal and regulatory implications of conducting social engineering attacks for educational or testing purposes.

5 - How can user awareness training and education be effective in mitigating social engineering attacks, and how does King Phisher contribute to this process?

1. phishing
   Spear phishing
   Whaling
   Watering hole attack
   Quid pro que attacks
2. The potential risk orde is at risk the victim into giving up information. For example the attacker might pretends to be a customer service
3. Piggy backing and tailgating are physical social engineering attacks that involve following into secure area
4. legal and regulatory such as bank or credit card company the attacker will often ask the victim for personal information
5. The training and education trick in order up the victim of a fack. Text message will often contain a link that, when clicked fake website

Experiment #		Student ID	
Date		Student Name	

Post Skill Task:

1. What is Ghost Phisher?

the ghost phisher can be used to minimum simulate a variety of social engineering attack . this make it a valuable tool for security teams that want to test their employee's security awareness and for organization that appear urgent or important in order to trick the target

2. Name the dependencies that are required in the proper running of Ghost Phisher.

the dependencies are open-source hypervior that allow users to create the run virtual machine (VMs) on their computers. A hypervisor is a software layer that allows multiple operating system (oses) to run to same physical computer virtual Box.

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured:_____out of _____ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

4. Implementation of Password Cracking Using John the Ripper

Date of the Session:___/___/___ **Time of the Session:**_____**to**_____

Learning Objective:

The learning objective of implementing password cracking using John the Ripper is to understand the principles and techniques of password cracking and gain hands-on experience with the John the Ripper software.

Description:

This project involves implementing password cracking using John the Ripper, a popular open-source password cracking tool. The project aims to explore different password cracking techniques, such as dictionary attacks, brute-force attacks, and hybrid attacks, and understand their strengths and limitations. By using John the Ripper, you will gain practical knowledge of configuring and utilizing the tool to crack passwords from various sources, such as password hashes obtained from system files or password-protected files.

Pre-Requisites:

1. John the Ripper: The primary Pre-Requisites for this project is John the Ripper, which is an open-source password cracking tool. It is available for various operating systems, including Windows, Linux, and macOS.

Pre-Skill:

1. What is password cracking, and why is it important from a security perspective?

* Dictionary attacks :-all possible combination's
* Brute-force attacks:- letters, numbers, symbol's
* Rainbow tables :- against a stolen has

2. Explain the working principle of John the Ripper.

* Dctionary-attacks
* Brute-force attacks
* Hybrid attacks
* Mask attack
* Rainbom table

Experiment #		Student ID	
Date		Student Name	

3. What are the different types of password cracking techniques supported by John the Ripper?

the speed at which john ripper can crack a password depends on a number of fictor's, including the length and complexity of the password, the type of attack is used offer a balance between and effectiveness

4. How does a dictionary attack work, and what are its limitations?

* they are only effective against short and simple passwords
* they can be slow if the dictionary is large
* they can be easily defeated by useing a strong password that is not in the dictionary

5. Describe the process of configuring John the Ripper for password cracking.

1. Download and install John the Ripper
2. obtain a dictionary of words
3. convert the password in to hash value
4. Configure john the ripper
5. Start the password cracking process
   * use a large dictionary
   * use a fast computer
   * use a powerful cracking
   * use a mask attack
   * usa a rain bow table

Experiment #		Student ID	
Date		Student Name	

In-Skill Task:

1. Two best friends started doing a project at last they made the project into a zip file with a password. Unfortunately by the presentation day they both forgot the password, so help them out by cracking the password using John the Ripper

```
#Dawload and install John the ripper
sudo apt pass install john

#obtain a dictionary of words
wget https://raw.githubusercontent.com/danielmiessler/
SecLists/master/Password/rockyou.txt

#convert the password hash to its original form
john --format=zip --wordlist=rockyou.txt my-
project.zip
```

Contains over 14 million words, so it is likely that the password will be found in the dictionary. The speed of the computer will also be a factor.

Experiment #		Student ID	
Date		Student Name	

Viva Questions

- What are the commonly used password hash formats supported by John the Ripper?
- How does John the Ripper handle salted password hashes?
- What is the difference between a brute-force attack and a dictionary attack?
- Explain the concept of a hybrid attack and its advantages over other cracking techniques.
- What are the countermeasures that can be taken to defend against password cracking?

— LM :- This is the password hash format used by windows NT, windows 2000, and windows XP

MD5 :- this is a popular password hash format that is used by a variety of applications

SHA-1 :- this is a more secure password hash format than MD5

bcrypt :- this is a password hash format that is designed to be resistant to brute-force attacks

Scrypt :- this is a password hash format that is designed to be resistant to both brute-force attack

— * Salted password cracking
* Incremental salt cracking
* Dictionary attack with salt

	Brute-force attack
Speed	Slow
effectiveness	Strong password
search space	combination of characters

Experiment #		Student ID	
Date		Student Name	

Post Lab:

Perform the following Tasks by using John the Ripper Tool

1. Security Auditing
2. Penetration Testing
3. Password Recovery

* Checking the strength of password
* Identifying unauthorized access
* Testing password policies

auditing, penetration testing and password recovery

* Security auditing
* penetration testing
* password recovery

It is important to use John the ripper responsibility and only for legitimate purpose

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation
	Marks Secured:_____out of _____ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

Experiment #		Student ID	
Date		Student Name	

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SUBJECT CODE: 21CS3041RA
CRYPT ANALYSIS AND CYBER DEFENCE WORKBOOK

5. Implementation of Wi-Fi Hacking Using Reaver

Date of the Session:___/___/___ **Time of the Session:_____to_____**

Learning Objective:

The learning objective of implementing Wi-Fi hacking using Reaver is to understand the vulnerabilities in Wi-Fi networks and gain practical knowledge of exploiting these vulnerabilities to gain unauthorized access to protected networks. Additionally, the objective is to familiarize oneself with the Reaver tool and its functionalities for conducting Wi-Fi hacking.

Description:

The implementation of Wi-Fi hacking using Reaver involves using the Reaver tool, which is an open-source software designed to exploit vulnerabilities in WPS (Wi-Fi Protected Setup) enabled routers. Reaver utilizes a brute-force attack against the WPS PIN to recover the Wi-Fi passphrase or key. This implementation aims to demonstrate the security weaknesses of WPS and educate users about the importance of securing their Wi-Fi networks.

Pre-Requisites:

1. Reaver: It is an open-source command-line tool available for Linux and other Unix-based operating systems. It can be downloaded and installed from the official Reaver website or via package managers like apt-get or yum.

Pre-Skill:

1. What is the objective of implementing Wi-Fi hacking using Reaver?

* unauthorized access to data
* Launching further attacks
* free wi-fi

2. Explain the purpose of Reaver in Wi-Fi hacking.

* use a strong password for your wi-fi network
* Disables WPS on your wifi
* keep your wifi router up to date
* use a wi-fi security scanner

Experiment #		Student ID	
Date		Student Name	

3. What is WPS and how does it contribute to Wi-Fi vulnerability?

* PIN code brute-force attack
* PIN code dictionary attack
* WPS PIN cracking useing brute force ardictionary
* WPS pin creacking useing a relay attack

4. Describe the process followed by Reaver to exploit WPS vulnerabilities.

1. Reaver first identifies a wi-fi network useing WPS
2. Reaver first WPS handshake request to wifi router
3. the wi-fi router responds to WPS with a challenge
4. Reaver then tries to crack the challenge attack
5. If Reaver is sucessful in cracking the challenge, it will obtain the PIN code

5. What precautions should be taken before conducting Wi-Fi hacking using Reaver?

the purpose of reaver in wi-fi hacking is to gain to Oauthorized acess to a wi-fi network. this can be done for a verety of reason, such as stealling data, launching further further attacks or simply because the attacker wants to be able for free

Experiment #		Student ID	
Date		Student Name	

In-Skill-Task:

1. Dheeraj is learning Reaver. As a beginner he wants to know the use of following commands in Reaver:-

i) Wash

ii) Reaver

i) Wash :- Password cracking is the process of trying to guess or recover a password from it's encrypted form. It is often used by hackers to gain unathorized access to computer system or networks

ii) Reaver :- It is mush faster than online password cracking, as the attacker does not need to wait for the server to respond to each password attempt

users. Can help to protect themselves from these attacks

Experiment #		Student ID	
Date		Student Name	

2. Karun forgot his Wi-Fi password. He wants to know the password. Karun approached you for help. Help Karun by hacking the Wi-Fi using Reaver.

Write down the wireless interface names, monitor mode, ESSID, Channel, BSSID of the target and paste the screen shots of execution and the outputs.

Note:- Perform this experiment on your native Wi-fi, your home Wi-Fi preferably.

1. I will measure the signal strength of my wifi connection in different location in my home
2. I will record the data in a spreadsheet
3. I will analyze the data to see how the signal strength varies depending on the locations

I will share the result of my experiment with you once I have completed it

about 10 meters away from the router. the singal strength is kitchen is currently at -35dBm

once I have collected all of the data, I will analyze it to see how the signal strength varies look for any pattern in the data

Experiment #		Student ID	
Date		Student Name	

Viva Questions:

- Are there any legal implications associated with Wi-Fi hacking using Reaver? Explain.
- What are some countermeasures that can be implemented to protect against Reaver attacks?
- Can you suggest alternative tools or techniques for Wi-Fi penetration testing apart from Reaver?
- How does the implementation of Wi-Fi hacking using Reaver help raise awareness about Wi-Fi security?
- In what scenarios can the knowledge gained from implementing Wi-Fi hacking using Reaver be useful from a security perspective?

- The law on wi-fi hacking can be complex and vary from jurisdiction to jurisdiction. It is important to consult
- Hacking the wifi have serious consequence. you could be fined tool safely
- even if it is legal to hack into a wi-fi network, it may still be unethical to do so
- once I have collected of the data, I will analyze it to see how the signal strength in data
- Concerned about the security of your wi-fi network, there are a no. of things can do protect it from Reaver attacks

Experiment #		Student ID	
Date		Student Name	

Post-Skill- Task:

- Key Generation Techniques:
- Strength of AES Keys:
- Key Management and Storage:
- Key Generation Performance:

* Random number generators (RNGs)
* Physically unclonable functions (PUFs)
* Hash functions
* Hybrid key generation techniques

the choice of key generation technique depends on the specific application. For example high level of security than hardware-based RNG or a PUF may be used. If RNG or a hash function may be used

* Security
* performance
* cost
* Availability

Comment of the Evaluator (if Any)	Evaluator's Observation Marks Secured:_____out of _____ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation

project, students should be able to effectively utilize NMAP to discover hosts, services, and vulnerabilities on a network.

Description:

The implementation of the NMAP scanning technique involves using the NMAP tool to perform network scans and gather information about hosts and services. Students will learn how to configure and execute different types of scans, interpret the results, and understand the implications of the findings. They will also gain knowledge about common scanning techniques, such as TCP SYN, UDP, and comprehensive scanning.

Pre-Requisites:

1. NMAP: It is an open-source network scanning tool available for Windows, Linux, and macOS. Students should have NMAP installed on their machines to perform the scans.

Pre-Skill:

1. What is NMAP, and why is it used for network scanning?

* Discovery
* Vulenerability detection
* Port scanning
* OS finger printing
* Service detection

2. Describe the different types of scanning techniques supported by NMAP.

* TCP connect scan
* TCP SYN stealth scan
* UDP scan
* stealth scan
* FIN' Scan
* XMAS scan

Experiment #		Student ID	
Date		Student Name	

3. How can you perform a TCP SYN scan using NMAP? Explain the steps involved.

starting Nmap 7.93 (https://nmap.org)
at 2023-08-15 00:00CDT
Host is up (0.00061s latency)
Not shown: 999 closed ports
22/tcp one. ssh
80/tcp open http

4. What is the purpose of performing a UDP scan? How can you execute it using NMAP?

A UDP scan is a type of port scan that uses (UDP) packets to determine whether a port is open or closed UDP is a connectionless protocol to be blocked by firewalls or intrusion detection detection system (IDSs)
nmap -sU <target IP address>

5. What is a comprehensive scan? How is it different from other scanning techniques?

* TCP SYN stealth scan
* UDP Scan
* Stealth scan
* FIN scan
* XMAS scan

If you connect about the security of your network you should consider a comprehensive looking for a quick and easy scan

In-Skill Task:

1. Vicky came to know that NMAP (Network Mapper) is a very versatile tool for Linux system/network administrators and is used for exploring networks, perform security scans, network audit and finding open ports on remote machine, Live hosts and Operating systems. So, he decided to work on the tool. Help him in performing the following scans:

   a. Ping sweep
   b. Port scan
   c. TCP full open scan
   d. TCP SYN scan
   e. UDP scan
   f. Version detection scan
   g. OS detection scan and
   h. Aggressive scan.

a) ping sweep
nmap -sn <target IP range>

b) port scan
nmap -p <port number> <target IP address>

c) TCP full open scan
nmap -sT <target IP address>

d) TCP SYN Scan
nmap -sS <target IP address>

e) UDP Scan
nmap -sU <target IP address>

f) version detection Scan
nmap -sV <target IP address>

g) os detection Scan and
nmap -o <target IP address>

Experiment #		Student ID	
Date		Student Name	

Aggressive Scan

nmap -A <target IP address>

Viva Questions :

- Explain the concept of stealth scanning and how it can be achieved with NMAP.
- How does NMAP identify the operating system of a target host? Discuss the techniques used.
- What is banner grabbing, and why is it useful during a network scan? How can NMAP accomplish banner grabbing?
- What are some common options and flags used in NMAP? Provide examples and explain their significance.
- . How can NMAP be used for vulnerability scanning? Discuss the process and the benefits of integrating vulnerability scanning with network scanning.

— * -sS flag to perform TCPSYN scan
-Pn flag to not ping scanning
-Th flag slow down
- IDS evasion techniques

— * TCP/IP stack fingerprinting
* Banner grabbing
* Fingerprinting databases

—To use the -v flag, you would simply add it to the command line when you run Nmap. For example TCPSYN

— <port number> that you want to scan the <target IP> address it host want to scan

— * Increased visibility
* Reduced risk
* compliance
* Improved efficiency

Experiment #		Student ID	
Date		Student Name	

Post -Skill-Task:

1. Billy is trying to understand how "–v" option is used in NMAP scanning technique. Explain him the use of the option "-v" by working on it.

```
nmap -SS -V 192.168.1.1
Starting Nmap 7.93 (https://nmap.org)
Nmap Scan report for 192.168.1.1
Host is up (0.000615. latency)
Not shown: 999 closed ports
port STATE SERVICE
22/tcp open ssh
80/tcp open http
```

(For Evaluator's use only)

Comment of the Evaluator (if Any)	Evaluator's Observation
	Marks Secured:_____out of _____ Full Name of the Evaluator: Signature of the Evaluator Date of Evaluation