Practical 1:

WHOIS refers to a protocol used to query databases that store registered domain names and associated information, such as the owner's contact details and domain registration data.

who.is is a website that provides a user-friendly interface to access and look up WHOIS information for domain names.

Reconnaissance/Footprinting refers to the process of gathering information about a target, often for cybersecurity or military purposes, to understand its structure, vulnerabilities, or other valuable data.

Practical 2 A:

1.Search cryptool download on google.
2.Open the 1st website that appears on result search.
3.Download the cryptool 1.4.42 English version and complete the installation setup.
4. Complete the setup click the checkbox of install crytool and ReadMe file.
5. Select finish install.
6. Open CrypTool and click on File > New
7.The pop up will appear enter your name or any text you want to encrypt .

8.Click on Encrypt/Decrypt tab > Symmetric(modern) > RC4.

9.Select key length you want to encrypt in number of bits and press encrypt and decrypt button to get the result.

Writeup:

Cryptool is a software tool used to explore and learn about cryptography, including encryption and decryption algorithms.

Encryption is the process of transforming readable data (plaintext) into unreadable data (ciphertext) using an algorithm and key to protect the data.

Decryption is the reverse process, where ciphertext is converted back into readable data (plaintext) using the correct key.

RC4 (Rivest Cipher 4) is a stream cipher encryption algorithm that can be used for encryption and decryption. It works by generating a pseudorandom keystream, which is then combined with the plaintext (using XOR operation) to produce ciphertext.

Practical 2 B:

Writeup:

1. Dictionary Attack:

A dictionary attack cracks passwords by trying every word in a precompiled list (dictionary) of common passwords and variations. It's effective against weak passwords.

2. Brute Force Attack:

A brute force attack tries every possible combination of characters until the correct password is found. It's slower but guarantees to crack the password eventually.

Practical 3 A:

cd.. : Changes the directory to the parent folder. Used to navigate the file system in command-line interfaces (CLI).

ping: Sends ICMP (Internet Control Message Protocol)echo requests to test connectivity between the local machine and a target. Used to check if a host is reachable.

ping www.google.com: Pings the Google website to check the network connection. Used to verify internet connectivity.

tracert: Traces the path packets take to reach a destination, showing each hop along the way. Useful in troubleshooting network routing issues.

tracert www.google.com: Traces the route from your computer to Google's servers, helping identify potential delays or routing issues.

ipconfig: Displays the network configuration of the computer (IP address, subnet mask, etc.). Used to check the local machine’s network settings.

netstat: Shows active network connections and listening ports. Useful for identifying open ports and monitoring network traffic for suspicious activity.

Practical 3 B:

Note: run as administrator cmd

Writeup:

ARP poisoning (also known as ARP spoofing) is a type of cyber attack where an attacker sends fake ARP (Address Resolution Protocol) messages onto a local network. This causes devices on the network to associate incorrect IP addresses with MAC addresses. ARP poisoning allows an attacker to intercept, modify, or block traffic between devices, potentially leading to man-in-the-middle (MITM) attacks or other network vulnerabilities.

`arp -s`: Adds a static ARP entry that binds a specific IP address to a MAC address.

`arp -d`: Deletes a specified ARP entry.

`arp -a`: Displays the current ARP cache.

ARP Table Manipulation: You modified the ARP table to misdirect traffic, rerouting it to an attacker's machine.

Static Entries: Using the `-s` option, you added a static entry, making your device associate an IP with an attacker's MAC address, enabling data interception.

Practical 4:

NMap (Network Mapper) is an open-source tool for network discovery and security auditing. It identifies devices on a network, detects open ports, and assesses security vulnerabilities. NMap can perform both active and passive scans; active scans send probes to the target, while passive scans gather information without direct engagement.

Forms of NMap Port Scanning:(active attack)

1. **ACK Scan**
    - **Full Form**: Acknowledgment Scan
    - **Definition**: Sends ACK packets to identify filtered ports, usually bypassing firewalls to map network topology.
    - nmap -sA -T4 scanme.nmap.org
2. **SYN Scan**
    - **Full Form**: Synchronize Scan

- **Definition**: Sends SYN packets to check for open ports without completing the TCP handshake, offering stealth.
- nmap -p 22,113,39 scanme.nmap.org

3. **FIN Scan**
   - **Full Form**: Finish Scan
   - **Definition**: Sends FIN packets to close ports to elicit RST(reset) responses from closed ports and no response from open ones, avoiding detection.
   - nmap -sF -T4 scanme.nmap.org
4. **NULL Scan**
   - **Full Form**: Null Scan
   - **Definition**: Sends packets with no flags set, attempting to bypass firewalls and IDS/IPS by causing unusual responses from closed ports.
   - nmap -sN -p 22 scanme.nmap.org
5. **XMAS Scan**
   - **Full Form**: Christmas Tree Scan
   - **Definition**: Sends packets with the FIN, URG, and PSH flags set, trying to elicit an odd response from closed ports while evading detection.
   - nmap -sX -T4 scanme.nmap.org

Practical 5 A:(passive attack)

1. Install wireshark and complete the setup
2. Open wireshark app > Click on ethernet / wifi based on ur system
3. Go on google search testphp-> click on Home of Acunetix Art
4. Click on sign up link and enter test as username and password
5. Go to wireshark
6. Search http
7. Select the get request http login.php
8. Right click on it -> follow -> tcp stream
9. Find your username and password

Writeup:

Wireshark is a free and open-source network protocol analyzer widely used for network troubleshooting, analysis, and education. It captures and displays packets in real-time, allowing users to inspect the details of network communications. Wireshark supports various network media types, including Ethernet, Wireless LAN, Bluetooth, and USB.

Practical 5 B:

Aim: Use Nemesy to launch DoS attack

A Denial of Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with excessive traffic, rendering it unavailable to legitimate users.

Key Points:

- **Objective:** To make a service unavailable to its intended users by overwhelming the target system with excessive traffic.
- **Method:** Flooding the target with a high volume of requests, consuming resources and causing service disruptions.
- **Impact:** Can lead to service outages, financial losses, and damage to reputation.
- **Tools:** Various tools can be used to conduct DoS attacks by generating traffic to test system resilience.

  Nemesy is a tool designed to perform Denial of Service (DoS) attacks by generating high volumes of traffic to test the resilience of network infrastructures. It can send various types of traffic, including TCP, UDP, and ICMP, to the target system to assess its capacity to handle large amounts of data.

  TCP – Transmission Control Protocol

  UDP – User Datagram Protocol

  ICMP – Internet Control Message Protocol

  Practical 6:

  One extra: `<LINK REL="stylesheet" HREF="javascript:alert('XSS');">`

  Cross-Site Scripting (XSS) involves injecting malicious scripts into web pages viewed by other users. These scripts execute in the context of the user's browser, potentially stealing sensitive information like cookies or session tokens. XSS attacks can be classified into three types:

1.stored xss

2. Reflected xss

3. Dom based xss

Practical 7:

1. Open Mozilla Firefox > Click on Open Application Menu > Go to More tools > Select Extensions for developers

2. Search “EditThisCookie Latest Edition” > Add the extension to your Mozilla Firefox browser

3. Open the extension -> click on edit this cookie -> click on export to extract all the cookie details.

4.open notepad -> press ctrl+v -> you will see all the cookies details.

5.Now go to more tools-> select extension for developer

6.search tamper data for quantum ff

7.add the extension-> check run on private windows .

8.open extension puzzle icon -> click on tamper data for quantum ff->Check the “tamper request only from this tab “.

9.click on yes to start tamper data

10.navigate to the URL you want to manipulate or inspect the session.

Use **Tamper Data** to manipulate requests for session impersonation

Writeups:

Session impersonation refers to the practice of mimicking or pretending to be another user during an online session, typically by manipulating session identifiers, cookies, or headers to assume the identity of that user.

Using **Firefox** and the **Tamper Data add-on**:

- **Firefox** is a popular web browser that can be customized with extensions or add-ons.
- **Tamper Data** was an add-on for Firefox that allowed users to view and modify HTTP/HTTPS requests and responses between the browser and the server. It was primarily used to inspect and manipulate the data sent during web interactions.
- **EditThisCookie**:A cookie extension is a browser tool that manages and controls cookies on websites. It helps users view, delete, block, or manage cookies for better privacy and security while browsing.

Practical 8:

SQL Injection occurs when an attacker manipulates a web application's input fields to execute malicious SQL queries. This exploitation allows unauthorized access to the application's database, enabling attackers to view, modify, or delete data.

Practical 9:

A **keylogger** is a computer program that secretly records every key you press on your computer or smartphone. This means it can capture sensitive information like passwords, credit card numbers, and personal messages without your knowledge.

Software Keyloggers: These are programs installed on your device that run in the background, tracking your keystrokes.

Hardware Keyloggers: These are physical devices connected between your keyboard and computer, capturing what you type.

Practical 10:

Metasploit is an open-source framework used for penetration testing and security research. It enables security professionals to identify and exploit vulnerabilities in systems, aiding in strengthening security measures.