4.B. Perform System Hacking using the following tools

◆ (i) Winrtgen

Aim

To generate password wordlists for password cracking.

Tools Used

- Winrtgen (Windows Rainbow Table Generator)

Steps

1. Open **Winrtgen**.
2. Select character set (alphabets, numbers, symbols).
3. Define password length.
4. Click **Generate**.
5. Save generated wordlist.

Result

Password wordlist is successfully generated.

◆ (ii) PWDump

Aim

To extract password hashes from Windows system.

Tools Used

- PWDump
- Windows OS

Steps

1. Run **PWDump** with administrator privileges.
2. Execute the tool on the target system.

3. Extract password hashes.
4. Save hashes to a file.

Result

Windows password hashes are successfully extracted.

◆ (iii) Ophcrack

Aim

To crack Windows passwords using rainbow tables.

Tools Used

- Ophcrack
- Rainbow Tables

Steps

1. Open **Ophcrack**.
2. Load password hash file.
3. Load appropriate rainbow tables.
4. Click **Crack**.
5. View recovered passwords.

Result

Passwords are successfully cracked using Ophcrack.

◆ (iv) FlexiSPY

Aim

To monitor mobile activities for security testing.

Tools Used

- FlexiSPY

Steps

1. Install **FlexiSPY** on test mobile device.
2. Configure monitoring options.
3. Access dashboard.
4. View activity logs (calls, messages).

Result

Mobile activity monitoring is successfully performed.

◆ (v) NTFS Stream Manipulation

Aim

To hide data using NTFS Alternate Data Streams (ADS).

Tools Used

- Windows NTFS File System

Steps

1. Open **Command Prompt**.
2. Create a text file.
3. Hide another file inside it using ADS.
4. Verify hidden data.

Result

Data is successfully hidden using NTFS streams.

◆ (vi) ADS Spy

Aim

To detect hidden NTFS alternate data streams.

Tools Used

- ADS Spy Tool

Steps

1. Open **ADS Spy**.
2. Scan NTFS drives.
3. Detect hidden streams.
4. View ADS details.

Result

Hidden NTFS streams are detected.

◆ (vii) Snow

Aim

To conceal data using whitespace steganography.

Tools Used

- SNOW Tool

Steps

1. Open SNOW application.
2. Select cover text.
3. Enter secret message.
4. Encode the message.
5. Save the output file.

Result

Data is successfully hidden using SNOW.

◆ (viii) QuickStego

Aim

To hide information inside image files.

Tools Used

- QuickStego

Steps

1. Open **QuickStego**.
2. Select image file.
3. Enter secret message.
4. Click **Hide Data**.
5. Save stego image.

Result

Message is successfully hidden inside image.

◆ (ix) Clearing Audit Policies

Aim

To remove audit trail records from the system.

Tools Used

- Windows Security Policy

Steps

1. Open **Local Security Policy**.
2. Navigate to **Audit Policy**.
3. Disable auditing options.
4. Apply changes.

Result

Audit policies are successfully cleared.

◆ (x) Clearing Logs

Aim

To delete system event logs.

Tools Used

- Event Viewer

Steps

1. Open **Event Viewer**.
2. Select **Security / System Logs**.
3. Click **Clear Log**.
4. Confirm deletion.

Result

System logs are successfully cleared.

⚠ Precautions / Counter Measures

- Enable strong access control
- Monitor logs regularly
- Use intrusion detection systems
- Restrict administrator privileges

✅ Overall Result

Thus, mobile network scanning and system hacking techniques were studied and performed using various ethical hacking tools.

🎤 Viva Gold Line

“System hacking techniques help in understanding how attackers hide activities and how defenders can detect them.”