Module 3

Q.1 What are the different types of hacking methods?

Ans:

1. Social engineering: This involves manipulating individuals into divulging confidential information or performing actions that can compromise a system's security.
2. Phishing: This is a type of social engineering that involves sending fraudulent emails or creating fake websites to trick individuals into providing personal or sensitive information.
3. Password cracking: This involves using software tools to guess or crack passwords to gain unauthorized access to a system or account.
4. Networking hacking: This involves exploiting vulnerabilities in a network.
5. Denial of service(DoS) and Distributed Denial of Service(DDoS) attacks: These involve overwhelming a system or network with traffic, rendering it unavailable to legitimate users.
6. SQL injection: This is a type of attack that exploits vulnerabilities in a web application’s code to gain access to sensitive data stored In a database.
7. Cross-site scripting: This involves injecting malicious code into a webpage to gain access to a user’s browser and steal sensitive information.
8. Man-in-the-middle: These involves inteccepting communication between two parties to eavesdrop or manipulate the data being transmitted.
9. Malware attacks: These attacks involve infecting a system with malicious software,such as viruses, worms and Trojans, to gain unauthorized access or steal data.

Q.2 Explain Types of Password Attacks

Ans: Brute force attack: This attack involves systematically trying every possible combination of characters until the correct password is found.

Dictionary attack:It is similar to a brute force attack but uses a pre-built dictionary of commonly used passwords or words found in a dictionary.

Rainbow table attack: This involves using a pre-computed table of hash values and their corresponding plain text passwords to password quickly.

Keylogger attack: This involves installing malware on a user's device that recors all the keystrokes entered incuding passsword.

Shoulder surfing: This involves physically observing a user as they enter their password.

Social engineering: This imvolves tricking users into divulging teir password through tactics such as phishing emails, fake login pages, or phone calls.

Q.3 Explain Password Cracking Tools: pwdump7

Ans: pwdump7 is a password auditing tool that is used to retrieve Windows password hashes from a compromised system.

It is a command-line tooo that extracts the encrypted password hashes from the Security Account Manager database on a Windows system.

When a user sets a password on a Windows system, the password is encrypted and stores in the SAM database. The SAM database is a file that contains the user account information, including the encrypted password hashes.pwdump7 extracts these encrypted password hashes from the SAM database, allowing an attacker to crack them using password cracking tools. Using pwdump7 to extract password hashes from a system without permission is illegal and can lead to serious legal consequences.

Q.4 Explain Types of Steganography with QuickStego

Ans: Steganography is the practice of hiding secret information within a innocent looking cover object, such as an image, audio file, or text.

QuickStego is a popular steganography tool can be used to embed and extract hidden data from images.

Types of Steganography that can be performed using QuickStego:
1. Image Steganography: A message or data is hidden within the pixels of an image.The image can be of any format, such as JPEG, BMP, or PNG.

2. Audio Steganography: This involves hiding a message or data within an audio file such as an MP3 or WAV file.

3. Text Steganography: A message or data is hidden within the text of a document or file.

4. Video Steganography: This involves hiding a message or data within a video file, ssuch as an AVI or MPEG file.

Q.5 Perform Practical on key logger tool.

Ans: -> Identify a keylogger tool that is compatible with the operating system of the device you want to monitor.

-> Download and install the keylogger tool on the device you want to monitor.

-> Configure the keylogger tool to log the types of activity you want to monitor.

-> Activate the keylogger tool and allow it to run in the background while the device is being used.

-> Monitor the activity logs generated by the keylogger tool to gather information about the device's usage.

-> Analyze the activity logs to identify any patterns or anomalies that may indicate suspicious or unauthorized activity.

-> Take appropriate action based on the findings, such as addressing security vulnerabilities, enforcing usage policies, or reporting illegal activity to authorities.