Module -3

Q-1 What are Different types of hacking methods ? Ethical Hacking

A-1 Hacking can refer to a variety of methods used to gain unauthorized access to computer systems or networks. Some hacking methods are illegal and are used for malicious purposes, while others are legal and are used for security testing and auditing purposes (also known as ethical hacking). Here are some of the different types of hacking methods:

1. Social Engineering: Social engineering is a technique where hackers use psychological manipulation to trick people into giving up confidential information, such as usernames, passwords, or sensitive data. This can be done through methods like phishing, baiting, pretexting, or impersonation.

2. Password cracking: Password cracking is the process of guessing or cracking passwords to gain unauthorized access to a computer system or network. This can be done through brute-force attacks, dictionary attacks, or rainbow table attacks.

3. Network scanning: Network scanning is the process of identifying and mapping the devices connected to a network, including servers, computers, routers, and other network devices. This information can be used by hackers to identify vulnerabilities in the network and plan attacks.

4. Vulnerability scanning: Vulnerability scanning is the process of identifying and assessing vulnerabilities in computer systems or networks. This can be done through automated tools or manual testing.

5. Denial of Service (DoS) attacks: DoS attacks are used to flood a network or system with traffic, making it unavailable to legitimate users. This can be done through methods like TCP SYN flooding, Ping of Death, or Smurf attacks.

6. Man-in-the-middle (MITM) attacks: MITM attacks are used to intercept and modify communication between two parties. This can be done through methods like ARP spoofing, DNS spoofing, or SSL stripping.

These are just a few examples of the different types of hacking methods. Ethical hackers use these methods to identify vulnerabilities and strengthen security measures in computer systems and networks. It is important to note that using these methods for malicious purposes is illegal and can result in severe legal consequences.

Q-2 Explain Different types of Password Attacks.

A-2

There are several types of password attacks that hackers use to gain unauthorized access to computer systems or networks. Here are some of the most common types of password attacks:

1. Brute Force Attack: This type of attack involves trying all possible combinations of characters until the correct password is found. This method is time-consuming and requires a lot of computational power. Brute force attacks can be made more effective by using dictionaries or wordlists that contain commonly used passwords.

2. Dictionary Attack: This type of attack uses a pre-existing dictionary or wordlist to try common words and phrases as possible passwords. This method is faster than a brute force attack because it only tries likely passwords rather than all possible combinations.

3. Rainbow Table Attack: This type of attack uses precomputed tables of hashes to quickly look up the original passwords. This method is more efficient than a brute force attack because the hashes are precomputed, and the process of looking up the original password is quick.

4. Shoulder Surfing: This type of attack involves watching someone enter their password and memorizing it. This method is particularly effective in public places like cafes, airports, or libraries, where people enter their passwords in public.

5. Phishing: This type of attack involves creating a fake website or email that looks like a legitimate website or email, with the intention of tricking the user into entering their password. Once the user enters their password, the hacker can use it to gain unauthorized access to the system.

6. Keystroke Logging: This type of attack involves using software or hardware to record every keystroke made by the user, including passwords. Once the keystrokes are recorded, the hacker can use the information to gain unauthorized access to the system.

It's important to note that these attacks can be prevented by using strong passwords, multi-factor authentication, and other security measures. Additionally, it's crucial to stay vigilant and be wary of suspicious emails, websites, or software.

Q-3 Explain Password Cracking tools: pwdump7

A-3

Pwdump7 is a password cracking tool that is designed to extract Windows account password hashes from the Security Account Manager (SAM) database. This tool is often used by security professionals to test the strength of passwords and to identify weak passwords that could be easily cracked by attackers.

Pwdump7 works by extracting the password hashes from the SAM database, which is a database that stores the local user accounts and their password hashes on a Windows computer. Once the password hashes are extracted, Pwdump7 can then attempt to crack the passwords using a variety of methods, including brute force attacks, dictionary attacks, and rainbow table attacks.

Brute force attacks involve trying every possible combination of characters until the correct password is found. This method is time-consuming and requires a lot of computational power, but it is effective against weak passwords.

Dictionary attacks involve using a pre-existing dictionary or wordlist to try common words and phrases as possible passwords. This method is faster than a brute force attack because it only tries likely passwords rather than all possible combinations.

Rainbow table attacks involve using precomputed tables of hashes to quickly look up the original passwords. This method is more efficient than a brute force attack because the hashes are precomputed, and the process of looking up the original password is quick.

Once Pwdump7 has successfully cracked a password, the user can then use that password to gain unauthorized access to the computer system or network. It's important to note that using password cracking tools like Pwdump7 without permission is illegal and can result in severe legal consequences. These tools should only be used by authorized security professionals for testing and auditing purposes.

Q-4 Explain Different types of Steganography with Quickstego .

A-4

Steganography is the practice of concealing a message or data within another file or image in a way that is not easily detectable. There are several types of steganography techniques, and QuickStego is a steganography tool that can be used to implement some of these techniques. Here are some of the most common types of steganography:

1. Image Steganography: Image steganography involves hiding data within an image file. This technique works by altering the least significant bit (LSB) of each pixel in the image. QuickStego can be used to embed a message within an image file by replacing the LSB of each pixel with the message bits.

2. Audio Steganography: Audio steganography involves hiding data within an audio file. This technique works by altering the LSB of each audio sample. QuickStego can be used to embed a message within an audio file by replacing the LSB of each audio sample with the message bits.

3. Text Steganography: Text steganography involves hiding data within a text file. This technique works by using special characters or whitespace to represent the hidden data. QuickStego can be used to embed a message within a text file by adding whitespace or special characters to represent the message bits.

4. Video Steganography: Video steganography involves hiding data within a video file. This technique works by altering the LSB of each pixel in the video frames. QuickStego can be used to embed a message within a video file by replacing the LSB of each pixel in the video frames with the message bits.

5. Network Steganography: Network steganography involves hiding data within network traffic. This technique works by embedding the data within the header or payload of network packets. QuickStego can be used to embed a message within network traffic by modifying the header or payload of network packets to include the message bits.

It's important to note that steganography tools like QuickStego can be used for both legitimate and illegitimate purposes. While steganography can be used for privacy and security purposes, it can also be used for nefarious activities, such as hiding malware or sensitive data theft.