UNIT 2: Tools and Methods Used in Cybercrime

1. Phishing and Identity Theft

1.1 Phishing

Definition:

Phishing is a cybercrime technique where attackers impersonate legitimate entities to deceive individuals into revealing sensitive information such as login credentials, credit card details, or personal information through fraudulent emails, websites, or messages.

Features/Process of Phishing:

- Deceptive messages that appear to be from trusted sources.
- Use of fake websites mimicking legitimate services.
- Psychological manipulation to create urgency (e.g., account suspension warnings).
- Harvesting sensitive data for identity theft or financial fraud.

Types of Phishing Scams:

1. **Email Phishing:** Fraudulent emails with links to fake websites.
2. **Vishing (Voice Phishing):** Attackers use phone calls to extract sensitive information.
3. **Smishing (SMS Phishing):** Fraudulent SMS messages containing malicious links.
4. **Clone Phishing:** Replicating a legitimate email but with a malicious link.
5. **Pharming:** Redirecting users to fake websites through DNS poisoning.

1.2 Methods of Phishing

1. **Deceptive Phishing:** Sending emails pretending to be a legitimate organization.
2. **Malware-Based Phishing:** Distributing malware through attachments or downloads.
3. **Man-in-the-Middle (MITM) Phishing:** Intercepting communication between a user and a service to steal credentials.
4. **Search Engine Phishing:** Fake websites appearing in search results to deceive users.

1.3 Spear Phishing

Definition:

Spear phishing is a targeted phishing attack aimed at a specific individual or organization, often using personalized information to appear more convincing.

Features:

- Highly personalized messages.
- Exploits trust relationships.
- Often used in corporate espionage or advanced persistent threats (APTs).

1.4 Phishing Toolkits and Spy Phishing

Phishing Toolkits:

Phishing toolkits are pre-packaged sets of software tools that enable attackers to create phishing attacks easily.

Spy Phishing:

Spy phishing involves using spyware or keyloggers to secretly collect user credentials and personal data.

---

2. Identity Theft

2.1 Personally Identifiable Information (PII)

Definition:

Personally Identifiable Information (PII) refers to any information that can be used to identify an individual.

Types of PII:

- **Sensitive PII:** Social Security Number, credit card details, medical records.
- **Non-sensitive PII:** Name, address, phone number (can be used for social engineering).

2.2 Types and Techniques of Identity Theft

1. **Financial Identity Theft:** Stealing credit card or bank information.
2. **Medical Identity Theft:** Using someone’s medical details for healthcare fraud.

3. **Criminal Identity Theft:** Using someone's identity when arrested for crimes.
4. **Synthetic Identity Theft:** Creating a fake identity using stolen data.

Techniques Used:

- **Dumpster Diving:** Retrieving personal details from discarded documents.
- **Skimming:** Capturing credit card data via hidden devices.
- **Social Engineering:** Manipulating individuals to divulge confidential data.

---

3. Password Cracking

Definition:

Password cracking is the process of recovering passwords from stored or transmitted data using various techniques.

Methods of Password Cracking:

1. **Brute Force Attack:** Trying every possible combination until the password is found.
2. **Dictionary Attack:** Using a pre-compiled list of common passwords.
3. **Rainbow Table Attack:** Using precomputed hash values to find matches.
4. **Credential Stuffing:** Using stolen credentials from previous data breaches.

---

4. Keyloggers and Spyware

4.1 Keyloggers

Definition:

A keylogger is a malicious software or hardware that records keystrokes to steal passwords, messages, and other sensitive data.

4.2 Spyware

Definition:

Spyware is a type of malware that secretly collects user information without their consent.

---

5. Backdoors

Definition:

A backdoor is a hidden method of bypassing normal authentication to gain unauthorized access to a system.

Types of Backdoors:

1. **Hardware Backdoors:** Embedded in computer chips or firmware.
2. **Software Backdoors:** Hidden within applications or operating systems.
3. **Remote Access Trojans (RATs):** Malware that allows remote control over a device.

---

6. Steganography

Definition:

Steganography is the practice of concealing messages or data within other non-suspicious digital media, such as images, videos, or audio files.

Methods of Steganography:

1. **Image Steganography:** Hiding data within image pixels.
2. **Audio Steganography:** Embedding messages in sound files.
3. **Video Steganography:** Concealing data in video frames.
4. **Text Steganography:** Using invisible characters or encoding text.

---

7. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

7.1 DoS Attack

Definition:

A DoS attack floods a system, server, or network with excessive traffic, making it unavailable to users.

7.2 DDoS Attack

Definition:

A DDoS attack uses multiple compromised computers (botnets) to perform a large-scale DoS attack.

Types of DDoS Attacks:

1. **Volumetric Attacks:** Overloading bandwidth with traffic.
2. **Protocol Attacks:** Exploiting weaknesses in network protocols.
3. **Application-Layer Attacks:** Targeting web applications with malicious requests.

---

8. SQL Injection

Definition:

SQL Injection is a web attack technique where malicious SQL queries are inserted into input fields to manipulate the database.

Types of SQL Injection:

1. **Classic SQL Injection:** Directly inserting malicious SQL code.
2. **Blind SQL Injection:** Extracting data by observing responses.
3. **Union-Based SQL Injection:** Using the `UNION` SQL operator to retrieve data.

---

9. Buffer Overflow

Definition:

A buffer overflow occurs when a program writes more data into a buffer than it can hold, leading to memory corruption and potential execution of malicious code.

Types of Buffer Overflow:

1. **Stack Overflow:** Overwriting return addresses in the stack.
2. **Heap Overflow:** Corrupting dynamically allocated memory.
