**Module 01: Introduction to Ethical Hacking**

**Hacking Concepts**

▪ What is Hacking?

▪ Who is a Hacker?

▪ Hacker and their Motivations

**Module 01 - Section 02:**

**■ What is Hacking?**

Hacking refers to the act of exploiting weaknesses or vulnerabilities in a computer system, network, or software to gain unauthorized access or control over its functionalities. It can be used for both malicious and non-malicious purposes, depending on the intent of the hacker.

A person holding a computer

Description automatically generated

**Types of Hackers:**

**1. White Hat Hackers (Ethical Hackers)**

These are security professionals who use their hacking skills for legal purposes, helping organizations find and fix security vulnerabilities. They are often hired to perform penetration testing to improve system security.

Example: A white hat hacker might test a company's security defenses to ensure sensitive data is protected.

**2. Black Hat Hackers (Malicious Hackers)**

These hackers use their skills for illegal activities, such as stealing data, spreading malware, or taking control of systems for personal gain. They exploit vulnerabilities without permission, often causing damage or harm.

Example: A black hat hacker might steal personal information or credit card details from a website.

**3. Gray Hat Hackers**

Gray hat hackers operate in a morally ambiguous area. They may break into systems without permission but do not have malicious intent. Often, they reveal security flaws without causing harm but might demand payment to fix the vulnerability

Example: A gray hat hacker might hack into a system, inform the owner of the vulnerability, and ask for compensation to help fix it.

**Common Hacking Techniques:**

**1. Phishing**

Trick users into giving away sensitive information by pretending to be a legitimate entity, usually through fake emails or websites.

Example: Sending an email that looks like it comes from a bank, asking users to enter their login details.

**2. Malware**

Deploying malicious software like viruses, worms, trojans, ransomware, or spyware to infiltrate systems and steal or damage data.

Example: Ransomware encrypts files on a victim's computer and demands payment to restore access.

**3. SQL Injection**

Exploiting vulnerabilities in a website's database by injecting malicious SQL code to retrieve, alter, or delete data.

Example: Hacking a website’s login page to extract user credentials from the database.

**4. Denial of Service (DoS) / Distributed Denial of Service (DDoS)**

Overloading a server or network with excessive traffic to make it inaccessible to legitimate users.

Example: Flooding a website with fake requests so that it crashes or becomes too slow to use.

**5. Brute Force Attacks**

Repeatedly trying different combinations of passwords or encryption keys until the correct one is found.

Example: Attempting all possible combinations to break into an account with weak password protection.

**6. Social Engineering**

Manipulating or tricking people into revealing confidential information or granting access.

Example: Posing as an IT support agent to trick an employee into revealing their password.

**7. Man-in-the-Middle (MITM) Attack**

Intercepting communication between two parties (e.g., between a user and a website) to steal or alter data.

Example: Eavesdropping on an unencrypted Wi-Fi network to steal personal information like login credentials.

**8. Keylogging**

Installing software that records keystrokes on a victim’s computer, capturing passwords and other sensitive data.

Example: A hacker installs a keylogger on a public computer to steal usernames and passwords.

**■ Who is a Hacker?**

A hacker is an individual who uses technical skills and knowledge to exploit or manipulate computer systems, networks, or software. Hackers can have varying motives, ranging from malicious intent to ethical purposes. The term "hacker" encompasses a wide range of individuals with different skill levels and intentions, often classified into different types based on their actions.

**■ Hacker and their Motivations**

Financial Gain: Many hackers seek monetary rewards, either through direct theft, ransom demands, or selling stolen data.

Political/Ideological Causes: Some hackers, known as hacktivists, hack systems to promote political or social causes.

Revenge or Personal Motives: Hackers may target specific individuals or organizations for personal reasons.

Curiosity or Challenge: Some hackers, particularly gray hats, are driven by the challenge of bypassing security measures.

Corporate Espionage: Hacking may be used to steal trade secrets or intellectual property to gain a competitive advantage.

**Impact of Hacking:**

Data Theft: Personal information, financial details, or proprietary data can be stolen.

Financial Loss: Companies may suffer financial damages due to lost revenue, ransom payments, or recovery costs.

Reputation Damage: Security breaches can damage a company’s reputation, leading to loss of customer trust.

Disruption of Services: Hacking can cause system outages or disruptions, affecting businesses and services.

Preventing hacking involves employing strong cybersecurity measures such as encryption, firewalls, regular software updates, and employee awareness training. Ethical hackers and security professionals play a crucial role in detecting and fixing vulnerabilities before they can be exploited by malicious actors.