**Introduction to Ethical Hacking**

**Index:**

|  |  |
| --- | --- |
| 1. **Elements of Information Security** | 2 |
| 1. **Classification of Attacks** | 2 |
| 1. **Hacking Methodology** | 2 |
| 1. **What is Hacking?** | 3 |
| 1. **Who is a Hacker?** | 3 |
| 1. **Hacker Classes** | 3 |
| 1. **What is Ethical Hacking?** | 3 |

**Elements of Information Security:**

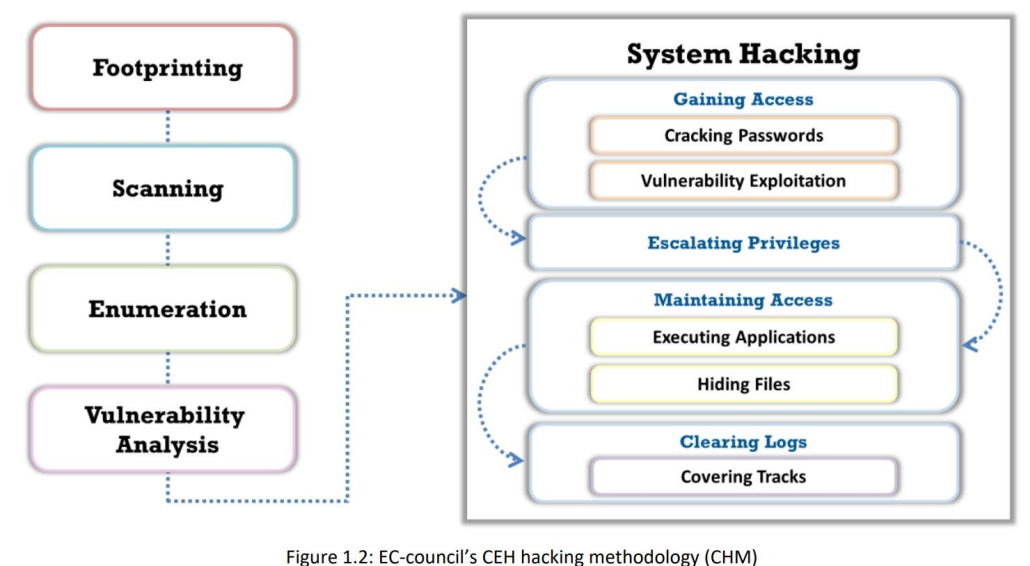
1. Confidentiality: assurance that the information is accessible only to authorized.
2. Integrity: prevention of improper and unauthorized changes-the assurance that information is sufficiently accurate for its purpose.
3. Availability: System is responsive to the authorized users only.
4. Authenticity: to confirm that a user is genuine.
5. Non-Repudiation: Non-repudiation ensures that the sender cannot deny sending a message, and the recipient cannot deny receiving it, often achieved through digital signatures.

**Classification of Attacks:**

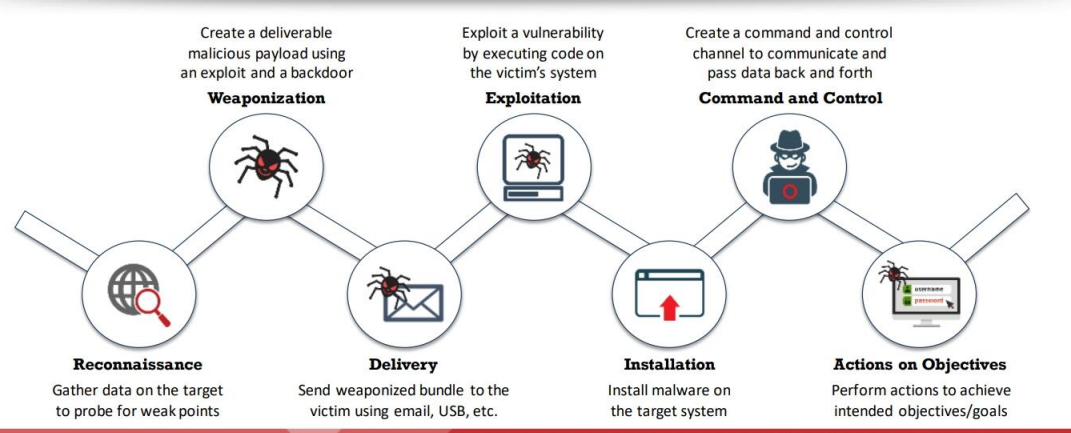
1. Passive Attacks: Eavesdropping or monitoring communication without altering it.
2. Active Attacks: Intercepting, modifying, or disrupting data in transit.
3. Close-in Attacks: Gaining physical proximity to systems to access or compromise them.
4. Insider Attacks: Malicious actions by authorized individuals within an organization.
5. Distribution Attacks: Inserting malicious components into hardware or software during the supply chain process.

**Hacking methodology:**

1. CEH Hacking Methodology:



1. Cyber kill chain methodology:



**What is Hacking?**

Hacking exploits system vulnerabilities to gain unauthorized access, often for theft, disruption, or intellectual property redistribution, using tools like viruses, phishing, and DoS attacks

**Who is a Hacker?**

A hacker is someone with advanced computing skills who breaks into systems, either to gain knowledge or for malicious purposes, like stealing sensitive data or causing harm.

**Hacker Classes:**

1. White hat hackers, also known as ethical hackers, work legally to improve security by identifying vulnerabilities and are often hired by companies to conduct penetration testing.
2. Black hat hackers, or malicious hackers, perform illegal activities to steal data, disrupt systems, or cause damage, engaging in cybercrime for financial gain, revenge, or political motives.
3. Gray hat hackers operate in both ethical and illegal ways; they may hack without permission but typically reveal vulnerabilities without malicious intent.
4. Script kiddies are inexperienced hackers who use pre-made tools and scripts to attack systems, usually motivated by thrill or reputation among peers
5. Hacktivists use hacking to promote political or social agendas by targeting government websites or organizations to send a message.
6. State-sponsored hackers are employed by governments to conduct espionage or disrupt other nations, focusing on political, military, or economic targets.
7. Cybercriminals, also called crackers, hack for personal gain through activities like ransomware, data theft, or fraud, operating individually or as part of criminal networks.
8. Insider threats involve employees or former employees who misuse access to harm the organization, motivated by revenge, financial gain, or negligence.

**What is Ethical Hacking?**

Ethical hacking involves legally breaking into systems or networks to identify and fix security vulnerabilities. It helps organizations strengthen defences by simulating cyberattacks, ensuring protection against malicious hackers and safeguarding sensitive data.