**What is Ethical Hacking?**

Ethical hacking (also known as penetration testing or white-hat hacking) is the practice of legally breaking into computer systems, networks, or applications to identify and fix security vulnerabilities before malicious hackers (black-hat hackers) can exploit them. Ethical hackers use the same techniques as cybercriminals but do so with permission and defensive purposes.

**Key Aspects of Ethical Hacking**

* Authorized Access
  + Ethical Hackers must have explicit permission from the system owner before testing.
  + Unauthorized hacking is illegal, even with good intentions.
* Purpose
  + Improve security by finding weakness.
  + Prevent data breaches, financial losses, and reputational damage.
* Methods & tools
  + Scanning networks for vulnerabilities (e.g. using Nmap).
  + Exploiting flaws (e.g., SQL injection, XSS, phishing simulations).
  + Using tools like Metasploit, Burp Suite, Wireshark, and Kali Linux.
* Type of Ethical Hackers
  + White Hat Hackers – Legally hack to improve security
  + Grey Hat Hackers - Hack without permission but disclose vulnerabilities legally ambiguous)
  + Black Hat Hackers – Malicious hackers (illegal)
* Certifications
  + CEH (Certified Ethical Hackers) – Popular certification by EC- Council
  + OSCP (Offensive Security Certified Professional) – Hands-on penetration testing certification.
  + CISSP, CompTIA Security+ - Broader cybersecurity certifications.

**Stage of Ethical Hacking**

1. Reconnaissance – Gathering information about the target
2. Scanning – Identifying open ports, services, and vulnerabilities.
3. Gaining Access – Exploiting weaknesses to penetrate the system
4. Maintaining Access – Checking if persistent threat can remain
5. Covering Tracks – (For malicious hackers; ethical hackers document instead).
6. Reporting – providing a detailed vulnerability assessment.

**Why is Ethical Hacking Important?**

* Protects sensitive data (financial, personal, government)
* Ensures compliance with security regulations (GDPR, HIPAA).
* Prevents cyberattacks like ransomware, phishing, and DDoS.
* Builds trust with customers and stakeholders.

**Conclusion**

Ethical hacking is a crucial part of cybersecurity, helping organizations stay ahead of cybercriminals. By simulating real-world attaks, ethical hackers strengthen defenses and safeguard digital assets.