Hacking   Ethical Hacking

1 ◄ **Definition**

Hacking is the process of exploiting the security flaws, bugs or vulnerabilities in a network or software in order to steal the data, destroy the data or interrupt normal operations.

Ethical hacking is the process of exploiting security flaws, vulnerabilities or bugs in a software or network in order to identify the security loopholes and fix them before a malicious hacker finds them.

Hacking	Ethical Hacking

2 < **Identity**

A person who performs hacking activities is called a hacker, a cracker, an attacker or a black hat hacker.

A person who performs ethical hacking is called an ethical hacker, White hat hacker

Hacking	Ethical Hacking

3 < **Intension**

Hacking is a Negative Intension Activity.

Ethical hacking is a positive intension Activity.

Hacking	Ethical Hacking

4 — Legality

Hacking is illegal activity. If any one caught he is she will go to the Gail.

Ethical hacking is legal Activity. Ethical hacking is sanctioned and authorized by the company, you are protected by a contract and it's completely legal.

Hacking	Ethical Hacking

5 ◀ **Compensation**

A hacker seeks to profit by illegally acquiring sensitive information and selling it on the dark web or simply transferring the money directly from your bank account to theirs once they have your credit card info. It's dirty money.

He is entitled to a salary and all the benefits, in exchange for his services in securing company user data, business operations and keeping the attacker in check. It's clean money, completely cool.

Hacking   Ethical Hacking

6 ◄ **Professional Development**

In hacking no scope of professional Development. Hacker is hacker hacker is hacker and hacker is hacker that's all.

In Ethical hacking great scope of professional development as you are any employee of any organization or a company.
- ❑ Senior penetration tester
- ❑ Network administrator
- ❑ Information security specialist
- ❑ Cyber security consultant etc.

Hacking   Ethical Hacking

7 — **Task Involved**

In Hacking
- Stealing sensitive identifiable user information
- Destroying, modifying or erasing a company's database
- Bringing down a network by interrupting its normal operations

Ethical Hacking
- To identify and remedy security vulnerabilities to secure the system
- To assess an organization's security measures and quality assurance
- Implementing data security regulatory compliance, like GDPR