Ethical Hacking

Ethical hacking and ethical hacker are terms used to describe hacking performed by a company or individual to help identify potential threats on a computer or network. An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers. This information is then used by the organization to improve the system security, in an effort to minimize or eliminate any potential attacks.

What constitutes ethical hacking?

For hacking to be deemed ethical, the hacker must obey the following rules:

1. Expressed (often written) permission to probe the network and attempt to identify potential security risks.
2. You respect the individual's or company's privacy.
3. You close out your work, not leaving anything open for you or someone else to exploit at a later time.
4. You let the software developer or hardware manufacturer know of any security vulnerabilities you locate in their software or hardware, if not already known by the company.

The term "ethical hacker" has received criticism at times from people who say that there is no such thing as an "ethical" hacker. Hacking is hacking, no matter how you look at it and those who do the hacking are commonly referred to as computer criminals or cyber criminals. However, the work that ethical hackers do for organizations has helped improve system security and can be said to be quite effective and successful. Individuals interested in becoming an ethical hacker can work towards a certification to become a Certified Ethical Hacker, or CEH. This certification is provided by the International Council of E-Commerce Consultants (EC-Council).
Types of Hackers

- **White Hat Hackers:**
  - A **White Hat** who specializes in penetration testing and in other testing methodologies to ensure the security of an organization's information systems.

- **Black Hat Hackers:**
  - A **Black Hat** is the villain or *bad guy*, especially in a western movie in which such a character would stereotypically wear a black *hat* in contrast to the hero's white hat.

- **Gray Hat Hackers:**
  - A **Grey Hat**, in the hacking community, refers to a skilled hacker whose activities fall somewhere between white and black hat hackers on a variety of spectra.

**Why Do We Need Ethical Hacking**

Government agencies and business organizations today are in constant need of [ethical hackers](#) to combat the growing threat to IT security. An ethical hacker is someone who is "trying to figure out if they are able to protect your system and if the system has been sufficiently protected." An ethical hacker needs to think and act like a hacker in order to aid an organization in its efforts to protect valuable information assets.

Banks are major targets therefore they always remain under cyber-threats. “Defending against cyber-attacks account for a significant portion of the $25 billion banks worldwide spend annually on security technology”. To stop a hacker, one needs to think like one and this is what ethical hacking is all about. Ethical hackers also perform security tasks like hackers; however it is to protect the computers and networks of an organization. They have the permission to hack organization's network in order to perform tests that keep it safe from illegal hacking. Ethical hackers help in improving the security of systems in organizations.