Ethical hacking refers to gaining unauthorized access to a system through different strategies. An ethical hack is carried out by following the footsteps of real hackers who mean harm to the system. By duplicating their strategies ethical hackers can identify vulnerabilities in the system. Once these activities are identified there is a better chance of resolving the issues before actual hackers find a way to gain access to your system or application.

## What do Ethical Hackers Do?

Ethical hackers are also known as "white hats", they can be thought of as experts who perform security assessments to ensure that an organization's security is not at risk. Companies hire teams of ethical hackers who help to identify system vulnerabilities and ensure that the security of the company is not compromised in any way. They generally follow four key protocols listed and explained below:

1. **Stay within legal limits:** Ethical hackers are required to adhere to legal limits. They also require proper approval from the company before they can carry out ethical hacking on the organization's system. Although they are working for the organization, they have to follow a certain set of protocols.
2. **Defining the scope:** Defining the scope at the initial stages is necessary to ensure that the team of ethical hackers and the company both are on the same page. Therefore, once the scope of the assessment is defined it should be discussed between both parties so that the hackers remain within legal limits.
3. **Report security vulnerabilities:** Once the team of ethical hackers has identified the security vulnerabilities it is up to them to report them to the organization. Moreover, they are also supposed to provide advice to resolve security issues.
4. **Agree on a non-disclosure agreement:** While the team is busy resolving issues, they will naturally be going through data that is sensitive to the organization. This is why companies make ethical hacking teams sign a non-disclosure agreement before they even begin the assessment.

## Why hire Ethical Hacking Teams?

With the availability of digital tools, it is becoming common for companies to use automated hacking tools to help them find security vulnerabilities in their system instead of hiring teams. However, tools don’t provide results that are easy to comprehend. The long reports can be difficult for the layman to decipher. Tools could help identify certain security vulnerabilities but they cannot provide the same level of efficiency and detail as a dedicated team would.

A dedicated team would scrutinize every aspect of the system bit by bit. For example, if a team of hackers is supposed to find out system vulnerabilities in a [standard proximity card](http://www.cardzgroup.com/ContactLessSmartCard.html) they would use their years of experience of knowledge of the latest malicious attack and the latest technology being used to carry it out. Automatic tools might even be able to reveal the pattern of the attack that is expected but they will not be able to observe as the human eye would and provide a solution that is suited to the company.

An organization must invest in a reliable and efficient and cybersecurity team that would help to conduct immunity tests. The tests are designed to counterfeit the activities of real hackers which helps to access the level of security. A dedicated cybersecurity team is constantly working to improve the security of hackers and develop a thicker wall against any external attacks.

## What problems do ethical hackers identify?

The initial goal of ethical hackers is to gain access to the system and to get as much information as they can get. Once they have gained the information, they use it to exploit the system. The security assessment can expose vulnerabilities in even the most sophisticated systems. Some of the most common problems identified are as follows:

1. Confidential data exposed
2. Software vulnerabilities
3. Security misconfigured
4. Broken authentication
5. SQL injections

Once the assessment is over the team prepares a report which encloses all the vulnerabilities and how the loopholes can be fixed to avoid a cyberattack in the future. The more detailed the assessment is, the more issues the team will be able to find and the organization will be less prone to external attacks.