Article published on May 4th 2012 | Education

This process is done by computer and network experts called Ethical or white hat hackers. These people analyze and attack the security system of an organization with the intention of finding and exposing weaknesses that crackers can exploit and take advantage of. It is important to understand that unlike crackers, ethical hackers get permission from the relevant authority to go on and test the security of their information system. Crackers cause harm and loss to an organization and affect negatively to the integrity, availability and confidentiality of an information system. So how did the concept of ethical hacking came up and how is it done?

The field of ethical hacking has been there in the computer world now for a while. Today, this subject has continued to gain much attention due to the increasingly availability and usage of computer resources and the internet. This growth and expansion of computer infrastructure has provided another avenue for interaction and so has attracted major organizations in businesses and governments. These bodies want to fully take advantage of the benefits offered by technology so that they can improve the quality of service they offer to their customers. For example organizations want to use the internet for electronic commerce and advertising among others. On the other hand governments want to use these resources to distribute information to its citizens. Even though they want to utilize this new potential that has been enhanced by technology there is fear of security. Organizations fear the possibility of their computer information system being cracked and accessed by unauthorized people. On the other hand potential customers and users of these services worry about the safety of the information they are prompted to give. They fear that these information like credit card numbers, social security numbers, home addresses and contacts will be accessed by intruders or outsiders who are going to use their data for other purposes outside the one that was intended. By so doing their privacy is going to be inter-feared with, something that is not desirable to many people if not all.

Due to the above raised fear, organizations sought to find a way to approach and counter this problem. They came to discover that one of the best methods they can use to limit and control the threat posed by unauthorized personal to a security system is to employ independent professionals in security matters to try the security measures of a system. In this scheme, hackers use the same tools and techniques used by intruders but they do not damage the system nor do they steal from it. They evaluate the system and report back to the owners the vulnerabilities their system is prone to. They also recommend what needs to be done to the system so as to make it more secure.

As evidenced from above, ethical hacking go hand in hand with security strengthening. Though it has done much in increasing security matters, still more needs to be done. It is impossible to obtain absolute security but even though, doing nothing to computer security is dangerous and undesirable.

Article Source:
http://www.articleside.com/education-articles/ethical-hacking-what-is-the-need-to-learn.htm - Article Side

David Raju - About Author:
Hacker School is a professional a Ethical Hacking training Institute in India. Hacker School trained many students in Ethical Hacking

Article Keywords:
ethical hacking training, ethical hacking Hyderabad, ethical hacking institute, ethical hacking, ethical training, ethical hacker, penetration testing, training

You can find more free articles on Article Side. Sign up today and share your knowledge to the community! It is completely FREE!