Article published on April 9th 2012 | Education

Having such hackers in the organization would help the organization to know the loop holes which are harmful to the organizationâ€™s security systems. There are many companies and organizations which hire ethical hackers who are expertise in their field of hacking. There professional use their ways of hacking either the computer hardware or software, or both. In this process, the organization would know the loop holes that let the unethical hacker to get into the security system of the organization. These loop holes will then be covered by developing other software which protect the organizationâ€™s data. Once these loop holes are covered the hackers would again try to break through the security system and check the other loop holes which let the outside hackers get into the organizationâ€™s network.

Ethical hacking is mostly used for Security Evaluation. In United States Air Force of the Multics operating systems for "potential use as a two-level (secret/top secret) systemâ€•. Their evaluation found that while Multics was "significantly better than other conventional systems," it also had "... vulnerabilities in hardware security, software security, and procedural security" that could be uncovered with "a relatively low level of effortâ€•. The reports hence had a result of tightening the security system as the intruder could get into the system in some ways.

The term hacker refers to a person who tries to invade into the security system of an organization and tries to hack or steal the passwords of a computer or a user who uses the computer and changes the data of the computer or the user. The effects of hacking would be changing the passwords of the user and not letting the user take the ownership of the computer or the data. The person who tries to invade into the computer without permission is called as intruder. Organizations hire such professional hackers and evaluate their security system time to time; so that they can cover up the loop holes from which any other hacker can get into their security system. Unethical hacking leads to hacking the data and then modifying them. But in ethical hacking, the hackers are hired by the organization to figure out the loop holes from which the security system can be breached. Once the security system is hacked, the hackers would let the administrator know about the loop hole and would then cover the loop hole with some security software so that other hackers would not get into the system illegally.

Ethical hacking is also known as white hat method and unethical hacking is known as Black hat methods. The organizations hire ethical hackers who are specialized in the field and are certified into it. There are Grey hat hackers who are not hired by the organizations, but these hackers would eventually hack the system and let the organization know that the system can be hacked with certain method. These hackers then make a deal of disclosing the method and the way to protect the system in order to not to get hacked in such way.

Article Source:
http://www.articleside.com/education-articles/ethical-hacking-helps-in-increasing-organization-s-security-system.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 a Ethical hacking

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

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