Ethical hacking

ETHICAL HACKING Ethical Hacking According to Raymond, the term 'Hacker' has a dual usage in the computer world. Originally, the term was defined as: HACKER noun 1. A person who enjoys learning the details of computer systems and how to stretch their capabilities-as opposed to most users of computers, who prefer to learn only the minimum amount necessary. 2. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming (Raymond, 1991).

From the above definition it is clear that, the original idea behind hacking has nothing malicious in its intent. According to me hacking is justified, provided the intent behind performing a hack is not destructive.

Today organizations are increasingly getting networked as information is exchanged at the speed of thought. Even mundane day to day tasks rely on the use of computers. Technology is evolving at an unprecedented rate and as a result the products that reach the market are engineered more for ease of use rather than secure computing. With the increased numbers and expanding knowledge of ill-intentioned crackers, combined with the growing number of system vulnerabilities and other unknowns, organizations (universities, corporate companies, NGOs, hospitals etc) need to be more proactive in securing their sensitive networks and data. More and more companies now believe in the quote: " To catch a thief, think like a thief" and hiring ethical hackers to ensure information system security.

For a long time, the term Ethical Hacking has been termed to be an oxymoron. This is mainly because of the misappropriate information imparted by misinformed or more appropriately, 'lesser informed' people. Since a long time, zealous and intelligent information system professionals who can get around a computer issue through innovation have categorized

themselves into two categories: Black Hat Society (Crackers) and White Hat Society (Hackers). Programmers who use their skills to cause trouble, crash machines, release computer viruses, steal credit card numbers, make free long distance calls (the phone system is so much like a computer system that is a common target for computer criminals), remove copy-protection, and distribute pirated software fall under the category of Black Hat Society (Crackers). On the contrary, programmers who apply their knowledge to test systems, get around technical issues, identify vulnerabilities and develop methods to overcome technical loopholes and in general those in general who do not apply their skills for destructive purposes fall under the category of White Hat Society (Hackers).

Case Study

Dti. gov. uk, a government website of UK, reports a hacking case study of a business corporation in UK in the previous year. The company was infiltrated online by crackers, who altered prices on the site's catalogue. The crackers changed the prices of all products on the catalogue to one-tenth of the original price. The company suffered big losses because of this. Fortunately, they recovered from the event quickly and prevented a recurrence by employing a specialist e-commerce oriented consultancy. This involved additional expense, but less than the amount they lost in the hacking attack. This is just one of the several case studies that reveal the necessity of ethical hacking. Regardless of any kind of innovative technology in place to prevent intrusion, complete prevention in next to impossible. Crackers always find ways to get across a barrier. Therefore only someone who can think like a cracker can actually defend the IT infrastructure against attack.

Role of Internet in Hacking

Although Internet has acted as a boon to mankind, it is not without its shortcomings. The Internet is a great place to share knowledge, meet people and improve business; while at the same time, it is a breeding ground for the black hat society too. There are several ways in which Internet acts as a spring board for unethical activities. Firstly, there are several websites which impart wrong information to the public who would want to know about hacking. Secondly, these websites also allow novices to download scripts and softwares that are aimed at performing illegal and/or unethical activities such as sniffing passwords, defacing a website or spreading viruses and Trojans. Malicious crackers can get all the prior information they need about companies they are intending to target on the Internet. Websites such as 'whois' database offers critical information such as domain names, registrations, IP addresses, e-mail addresses etc. The Internet is also a great place to connect. Using either raw coding or softwares, crackers then connect to a company's network and create a 'backdoor' over the public Internet. This backdoor is then used for all malicious activities like eavesdropping, changing data streams and introducing viruses in to the company networks.

Security Remedies

A successful organization not only relies on finding innovative solutions or products but also on the effective implementation of those solutions. Here, technology plays a major role as these technological developments can make the implementations simpler, providing a wide range of choice. But the question arises so as to which is the right choice This can only be answered by thorough research on the cost, stability and reliability of the technology to be used (WALSHAM, 1993). The Information System of the firm should be

able to process this task by taking the external (technology functionality) and internal (business environment) entities into account. Thus, the understanding and integration of technological innovations plays a key role in the modeling of any Information System to support the business goals and strategies. The organization has to analyze all the possibilities and provide the solution that is technological stable and cost-effective, to implement, maintain and modify in future.

The management plays the most important part in building a successful IT infrastructure (Royce, 1998). Management's responsibility goes beyond the basics of support. They are the ones responsible for setting the tone for the entire security program. It is not enough just to bless the program (niser. org, nd). Management must take thorough responsibility of the program by becoming a part of the process. Apart from investing in the most effective security practices, companies should contract third party ethical hacking teams with reputation to test (penetration testing) the existing IT infrastructure and identify any loopholes and promptly patch them up. Finally and most importantly, novice IT programmers must not fall for the traps laid online and be educated about the legality of IT acts. The choice to choose a path is in the individual's hand. The most crucial question each upcoming programmer must ask himself is, " Which hat should I choose"

References

E. S. Raymond (1991), " The New Hacker's Dictionary", MIT Press, Cambridge, MA.

WALSHAM, G. (1993), " Interpreting Information Systems in Organizations".

Wiley, Chichester.

Walker Royce (1998), " Software Project Management - A Unified Approach", Addison-Wesley Professional.