Threats to Information Security are Rising. Is "Ethical Hacking" another Technique to Enhance Information Security? Research Based on Mumbai and Pune, India

Prepared by: Sagar Ravishankar Dhande

ABSTRACT

Term information security is frequently used to describe the risks of guarding information that is in a digital format. This digital information is typically manipulated by processor, transmitted over a network (such as internet, intranet) and usually stored in computers, server, database, disks etc. Today Information Systems plays valuable role in corporate and personal world, companies and individuals practicing different techniques (using software and hardware's) to secure data and information. Tremendous security threats like virus, bots, denial of service attack, telecom fraud, unauthorized access, and phishing etc., are rising at rate more than 25% – 30% than previous year. Research conducted by McAfee Security journal, 2008 states, social engineering (Phishing attacks), spam are increasing; and always upgrading with new methods to obtain personal and confidential information from users. Whereas the old techniques and scripts (virus programs) are decreasing or under control (as they are constantly under view) new techniques and methods are targeting information and are successful in drafting the threats graph high against security. This emerging and upgrading threats are required to be treated with new advanced countermeasures, one of them is Ethical Hacking. Antivirus, ant spyware's, hardware security tool and rules, laws are already is used and are not sufficient to tackle the problem. New advanced Ethical hacking approach includes Ethical hacker who practices hackers techniques and strategies to find the vulnerability (security holes) by attacking the system in the same way as hacker could have (intentionally ethical) and if found any security holes or vulnerabilities then Ethical Hackers finds the way to fix and cover it.