V Rajendran
Advocate, High Court of Madras
Email: venkrajen@yahoo.com, venkat.rajen@gmail.com

Hacking: Illegal but Ethical?

Preface: This article discusses in brief the techno-legal issues in the activity called 'hacking', its treatment in the Information Technology Act 2000 (later amended by the I.T. Amendment Act 2008), the practice and the social acceptability of ethical hackers and the responsibility of information system security professionals.

The **earlier Section 66** of Information Technology Act in India stated as follows:

Sec. 66: Hacking with computer system. ***(This section has since been amended)***

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or delete or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack;

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

From this it is quite clear that hacking per se is an offence with well-defined punishments and unambiguous treatment in the Act. But in practice we often come across many academic institutions and training organizations giving training in 'hacking' giving much publicity to such courses. There are quite a few number of such institutions which offer theory classes with hands-on training and practical inputs too on the nuances of hacking going in depth on issues like tracing an IP address, tracing an email, etc. A quick glance into the brochures and other material brought out by such organizations reveal much information and promise a great deal.

Teaching an illegality? Some institutes advertise stating clearly that *"while these hacking skills can be used for malicious purposes,* this class teaches you how to use the same hacking techniques to perform a white-hat, ethical hack, on your organization" (italics mine). Some institutes also advertise like "this website will help you gain entry into the minds of seasoned computer criminals, so that you can forestall their attempts and pre-empt all harmful intents and activities". Sounds too good and good Samaritan isn't it? But is there any check on the syllabus taught, admission criteria, and the knowledge imparted and above all the purpose for which the knowledge so gained is to put to.

Comparison with other crimes: Crimes such as murder, rape, robbery etc. are all well defined and have been accepted as crimes and offences which any one would shun and are not just legally but also morally and ethically treated as crimes only. On the same plane, take the offence called 'hacking'. Here lies the difference. While hacking itself is a crime recognized as an offence with well-defined punishments for it, how can there be a course or training programs called 'ethical hacking'? The protagonists say that like any other computer knowledge or programming skill or software efficiency, hacking too is a part of the knowledge and at least to protect your computer from being hacked, you should be taught and trained in hacking. *To protect ourselves from robbery or cheating or chain-snatching or eve-teasing, no institute conducts a course called 'ethical eve-teasing' or 'ethical cheating' or 'ethical robbery'.*

Besides, admission to such courses is by advertisements and wide publicity and in their eagerness to enroll more and more candidates, such institutes admit semiliterate professionals, teenaged students, and inquisitive youngsters whose antecedents are not known or verified. Verification of antecedents is strictly taboo and a firm No-No especially in the case of state-owned Universities which the author learnt during one of his interactions with one such University in their Board of Studies (syllabus drafting) meetings. Hence with no such restrictions on admission, and with such deeper knowledge about the various software forensic tools being imparted and with an inherent inquisitive and exploratory brain it is but natural that such youngsters venture into the act of hacking calling it 'an ethical act'.

It is interesting to note that to put an end to this anomalous situation of an illegality being taught in academic institutions, the lawmakers thought it fit to **remove the word 'hacking' from the Section 66 of the IT Amendment Act 2008,** which came into effect from 27th Oct, 2009. Though the section still deals with the offence of unauthorized access to a computer resource, data theft, combining it with the civil offence of data theft dealt with in Section 43, the offence still remains the same and the punishments for the act is stipulated as three years' imprisonment or a fine of five lakh rupees or both.

Perhaps by this amendment, the government has **avoided the issue,** not solved it. No doubt, hacking is still an offence, though the academicians and institutes teaching it may like to differentiate that doing it with the permission of the owner of the system (i.e. for good purposes) is hacking and doing it in an unauthorized manner i.e. malicious intent (**or *mens rea,*** to use a legal term meaning criminal intent of mind) will be called cracking. The act *per se* ultimately and *ab initio,* remains the same.

Do the governments or other regulatory authorities have a role to play in putting an end to the nomenclature to such courses? Can the syllabus or the coverage of such courses be streamlined or regulated? Admitting that such coverage is essential to spread awareness on the vulnerabilities in the system and for one's own protection, does it not border on the lines of spreading awareness on accessing other's data, other's computer systems (which again is a clear offence as per Sec. 43 of the I.T. Act)? Above all, putting an end to such courses will be a great boon to the cyber crime police and other investigating agencies in the ever increasing field of cyber crime.

Such spread of knowledge called under the fancy names of "Ethical Hacking" or "Knowledge of hacking tools" or "Hands-on sessions in hacking" etc. has led to increase in cyber crimes in the country. It is quite clear that the cyber crime police are getting more and more cases of data theft, hacking, attempted id theft, unauthorized access to systems often resulting in cyber-blackmailing and sometimes even in e-publishing of obscene material (which too is a cognizable offence even as per the original Sec. 67 with its broadened scope, additions and amendment as per I.T. Amendment Act 2008).

Conclusion: It is time that the governments, the I.T. Secretary and other regulators like RBI, TRAI, and the Ministry

Continued on Page 31

Continued from Page 30

of I.T. and Telecom and CERT-In (under the control of Ministry of I.T. with its legal position now recognized under Sec. 70-B of I.T. Amendment Act 2008) acted upon the whistle blower signals and brought some regulations on these. For instance, CERT-In (Computer Emergency Response Team India) can take initiatives to ban such courses with these fancy or misleading names like "Ethical Hacking" and enforce regulations before knowledge about hacking tools is imparted to students. ■

About the Author

V Rajendran, Advocate, High Court of Madras. His qualifications are M.A. B.L. M.Com. CAIIB, ISO-ISMS LA, STQC-CISP, Dip I.T. Law, CeISB, "Certified Forensic Examiner" conducted by IDRBT and Directorate of Forensic Science, Govt. of India. He has over 3 decades of experience in a tech-savvy Public Sector Bank in various capacities as Manager, Senior Manager and retired under Voluntary Retirement Scheme as Chief Manager Systems. An invited speaker and Guest Faculty in various Universities and Colleges, Police Training Colleges etc. on Cyber Crimes, Security Concerns in electronic delivery channels in Banks like ATMs, e-Banking etc. Authored many articles and appeared in print media and electronic media on many occasions on issues regarding cyber crimes, banking frauds etc.