Abstract

With the growth of attacks and hacking activities, the organizations are becoming more security conscience. The scope has changed from technical problem to a business problem within an organization. High cost is incurred to implement security policy and procedures and is viewed as an investment. However, in the quest of getting secure, the organizations hastily employ hackers to exploit the vulnerability of their system. This paper is an attempt to identify the ethical problems and legal implications associated with such act and the care to be taken before employing any outsider or insider who can break into the network and find its weaknesses. If these issues are not addressed before the implementation and deployment of the given security policies and procedures, the organizations can land themselves in serious legal actions which they may repent later.

References

- Susan C., "Vulnerability Assessment", SANS Institute Reading Room Site, July 6, 2001, Version 1.2e
- Verma, S., Singh, T. 2012. Automated Multilevel Defence Model to Investigate Packets
for Web Interface. 9th International Conference on Wireless and Optical Communications Networks

- Spitzner, L., Chapter 8. Know Your Enemy. Addison Wesley, 225- 253

Index Terms

Computer Science

Security

Keywords

Log Monitoring; Risk Analysis; Legal Implications