A Review Paper on Ethical Hacking

Aniket Kalbende, Bharat Zile, Bhairav Shende, Jayesh Gharad, Pranav Kherde
Department of Master of Computer Application
Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, India

Abstract*: An ethical hacker is the network specialist & computer who pounce some security systems on the behalf of its possessor seeking amenability that could be exploited by a malicious hacker. The Internet's explosive growth has conduct many virtuous things: e- commerce, e-mail, collaborative computing & new fields for advertisement and information distribution. Ethical hacking has become a main anxiety for businesses & governments, also known as the intrusion testing or penetration testing or red teaming. Organizations are concerned about the probability of being "hacked" & potential clients are concerned about keeping personal information under control. Hackers are classified according to their work and knowledge. The white hat hackers are the ethical hackers. Ethical hackers use hacking approaches to ensure safety. Ethical hacking is needed to protect the system from the hacker's damage. The major reason behind the ethical hacking study is to assess the security and report back to the owner of the target system.*

Keywords: Cybercrimes, Clearing Tracks, Computer Security, Ethical Hacking

REFERENCES

[1] G. R. Lucas, "Cyber warfare," in The Ashgate Research Companion to Military Ethics, 2016.
[2] P. Engebretson, "Reconnaissance," in The Basics of Hacking and Penetration Testing, 2011.
[3] Ehacking, "Scanning and Enumeration- Second Step of Ethical Hacking," ehacking, 2011.
[4] R. Baloch, Ethical Hacking and Penetration Testing Guide. 2017.

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-12491

ISSN
2581-9429
IJARSCT

586