IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, April 2025
Impact Factor: 7.67

Ethical Hacking: The Digital Frontier of Cyber Defence

Tejal Shrikant Bagul[1], Archita Dilip Gaikwad[2], Bharti Nivrutti Mahale[3]
Students, Department of Computer Science[1,2]
Assistant Professor, Department of Computer Science[3]
K. R. T. Arts, B. H. Commerce A. M. Science College, Nashik, India
tejalbagul00@gmail.com,gaikwadarchita1@gmail.com,bhartimahale@kthmcollege.ac.in

Abstract: *Ethical hackers are cybersecurity professionals with advanced expertise in network and information systems security. Their primary role is to identify, assess, and remediate security vulnerabilities to pre-empt unauthorized intrusions and mitigate malicious cyber threats. With the rapid expansion of internet-enabled services—ranging from e-commerce and cloud-based collaboration to digital marketing and online communications—the threat landscape has evolved considerably, necessitating proactive defence mechanisms. The discipline of ethical hacking, also known as penetration testing or red teaming, has become increasingly vital across both public and private sectors. Organizations are now more vigilant in addressing cyber risks, particularly regarding the unauthorized exploitation of sensitive corporate and personal data. Ethical hackers, commonly referred to as white-hat hackers, leverage their technical acumen to fortify systems, uncover security flaws, and ensure the resilience of digital infrastructure. Their operations are pivotal in pre-empting damage from threat actors and reinforcing the confidentiality, integrity, and availability of information assets. The central objective of ethical hacking is to rigorously evaluate and enhance a system's defensive capabilities, thereby supporting legitimate stakeholders in safeguarding their digital domains. This paper delves into the foundational principles of ethical hacking, examining prevailing methodologies, tools, and frameworks utilized in the field. Key focus areas include cybercrime mitigation, anti-forensic techniques, network reconnaissance, system enumeration, and vulnerability assessment—all of which are instrumental in fostering robust cybersecurity in an increasingly digitized world.*

Keywords: Cyber crime, cyber Security, Computer Security, Attack types, Hacking tools, computer data.

DOI: 10.48175/IJARSCT-25573