# *Recent developments and trends in ethical hacking: A systematic review*

**[*1]Rushikesh Shinde, [2]Archana Bendale, [3]M.K.Borse**
[*1]Student, M.Sc. (Computer Science), K.K. Wagh Arts, Commerce, Science & Computer Science College, Saraswati Nagar, Nashik
Affiliated to SPPU, Pune, Maharashtra, India
[2,3]Assistant Professor, Department of Computer Science, K.K. Wagh Arts, Commerce, Science & Computer Science College, Saraswati Nagar, Nashik
Affiliated to SPPU, Pune, Maharashtra, India

## **Abstract**:

This literature review explores the evolving role of ethical hacking in contemporary cybersecurity. What was once a niche activity, ethical hacking has evolved into a central part of proactive security activities, such as penetration testing, threat hunting, and vulnerability scanning? The review takes into account underlying ethical concerns, education's integration of ethical hacking, its use in various industries such as healthcare, and its relation to social concerns such as activism and the law. The integration of these studies indicates the expanding roles of ethical hackers in preventative and response security activities. As society's perception continues to shift, ethical hackers are increasingly being regarded as allies in the battle against cyber threats. Challenges persist, however, such as legal concerns, the need for standardized quality, and the need to continually adapt to new technologies. Overcoming these obstacles requires continued research, innovation, and adherence to ethical standards. By embracing these, ethical hacking can continue to evolve as a vital part of cybersecurity, effectively mitigating risks and enhancing the resilience of digital systems.

## **Keywords:**

Ethical Hacking, Cybersecurity, Penetration Testing, Threat Hunting, Vulnerability Assessment, Cybersecurity Education, Hacktivism, Cybersecurity Culture, Legal and Ethical Issues in Hacking, Emerging Cybersecurity Technologies.

## **1. Introduction:**

The body of literature on ethical hacking has itself developed dramatically in the past two decades, reflecting the complexity and fine detail characteristic of this extremely sophisticated field. Warren and Hutchinson's [1] early work offers cogent explorations of the ethical dimensions of hackers, specifically within the Australian context. Their thorough analysis graphically depicts the dualistic nature of hackers as, on the one hand, agents of threat for security and, on the other, guardians of the system, thus giving expression to the cogent social imperative to investigate the motivations of hackers and the ethical dimensions of their activity. This early work provides a sound base from which to construct the following more general debates, which raise a range of ethical implications and considerations inherent in hacking practice.

As time has passed, this double dimension has constantly influenced the debate around cybersecurity. With the increasing pace of digital transformation in all industries, the role of ethical hacking has also become increasingly diverse, going beyond traditional penetration testing to encompass other activities like threat intelligence, policy- making, and ethical governance. The rapid evolution of sophisticated cyber-attacks has also made it all the more crucial for governments and organizations to recruit the services of ethical hackers in creating forward-thinking defense strategies.

In addition, the ongoing metamorphosis of hacker identities evolving from lone wolves to organized groups has raised questions about their motivations, obligations, and contributions to the well-being of society. The development of bug bounty programs, threat reporting undertaken by hackers, and participation in open-source security projects demonstrates that ethical hackers are increasingly being integrated into mainstream cybersecurity mechanisms. All of this requires a reevaluation of the social and legal boundaries of ethical hacking, highlighting the need for comprehensive, up-to-date research reflecting both global practices and regional nuances.

## 2. Literature review:

Radziwill et al. [2] recommend incorporating ethical hacking into the curricula of schools, dispelling negative stereotypes and encouraging a more balanced perspective using the "white," "black," and "gray" hat categorizations.

Kelly [3] cites penetration testing as a major cybersecurity practice, and asserts that ethical hackers are at the forefront of enhancing online defenses.

Curcelli [4] considers hacktivism as the blending of activism and hacking, transgressing social taboos and examining gender dynamics within such groups.

Ertan et al. [5] mention how internal dynamics based on organizational culture and human behavior influence cybersecurity compliance and how ethical hacking education needs to include these internal dynamics.

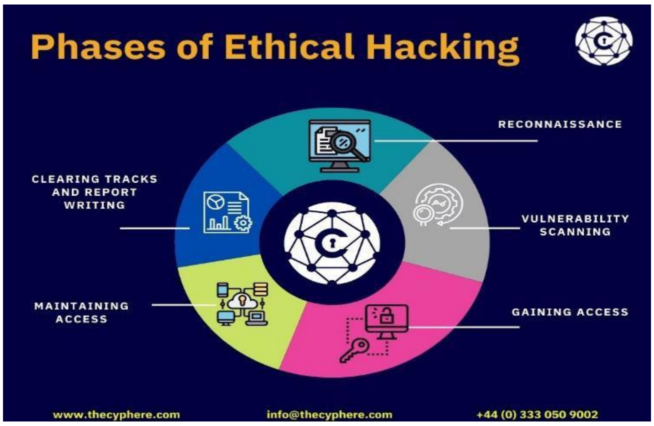
Uchendu et al. [6] provide a cybersecurity culture review with a focus on the need to align ethical hacking activities with organizational values to build effective security practices.

Lorenzini et al. [7] write about healthcare cybersecurity ethical issues, calling for collaborations between healthcare organizations and ethical hackers to enhance security.

Wang et al. [8] introduce cyber threat hunting as a proactive response, underlining the growing importance of offensive security roles in finding and eliminating threats.

Nkongolo et al. [9] present key competencies for contemporary cybersecurity professionals, establishing a connection between the development of ethical hacking and the challenges posed by an evolving job market.

### 2.1. Common phases in ethical hacking:



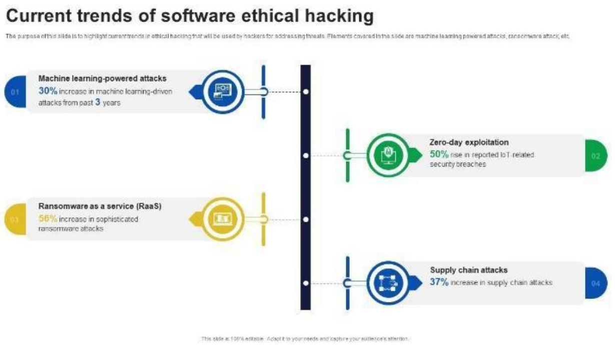
## 3. Recent trends in ethical hacking:

Recent developments in the practice of ethical hacking exhibit a clear movement towards proactive and specialist practice within the realm of cybersecurity. Utilization of Artificial Intelligence (AI) and Machine Learning (ML) has reshaped vulnerability identification at its fundamental level, enabling ethical hackers to automate routine procedures and focus on complex security concerns. This innovation enhances the productivity and efficiency of penetration testing and threat modeling.

Simultaneously, the rapid emergence of cloud computing has ushered in fresh security challenges, with ethical hackers prioritizing security in multi-cloud environments and cloud-native applications. The prioritization ensures that companies can utilize safely the advantages accruing to cloud computing [10].

The increasing quantity of Internet of Things (IoT) devices has increased the attack surface, and hence ethical hackers have been devising innovative ways of safeguarding such devices against future breaches. Ethical hackers are placing emphasis on unearthing vulnerabilities in IoT systems in an attempt to guard against potential breaches [11].

Additionally, quantum computing comes with opportunities and challenges, and the front runners in defining quantum-resistant cryptographic algorithms that will protect against future attacks are ethical hackers. Ethical hackers are researching quantum-resistant encryption algorithms to make digital communications future-proof [11].



Current trends of software ethical hacking

The purpose of this slide is to highlight current trends in ethical hacking that will be used by hackers for addressing threats. Elements covered in the slide are machine learning powered attacks, ransomware attack, etc.

01 Machine learning-powered attacks
30% increase in machine learning-driven attacks from past 3 years

02 Zero-day exploitation
50% rise in reported IoT related security breaches

03 Ransomware as a service (RaaS)
56% increase in sophisticated ransomware attacks

04 Supply chain attacks
37% increase in supply chain attacks

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

## 4. Discussion:

The landscape of ethical hacking has undergone significant transformation over the past two decades, evolving from a niche practice to a cornerstone of modern cybersecurity. Initially, ethical hacking emerged as a response to the burgeoning cyber threats of the 1990s and early 2000s, with organizations seeking proactive measures to safeguard their digital assets. This period saw the establishment of formal ethical hacking practices, including the development of certifications like the Certified Ethical Hacker (CEH), which provided standardized benchmarks for skills and knowledge [12].

With the rise of technology, ethical hackers moved beyond the conventional penetration testing. They were now instrumental in the design and implementation of preventive controls, such as threat hunting, which involves active discovery of vulnerabilities before the attackers can find and exploit them. This role in proactive security controls has been instrumental in establishing robust cybersecurity cultures within organizations.

Increased recognition of the contributions of ethical hackers has seen them being integrated into university curricula and corporate strategies. It has started to include programs and courses that specialize in ethical hacking as a means of equipping students with the necessary skills to deal with the evolving nature of cybersecurity threats. This emphasis on education has led to a group of professionals who are not only technically skilled but also ethically sound.

In addition, the profession of ethical hackers is bound up with broader issues in society, including arguments over privacy, freedom of information, and rights on the internet. Their activities most often raise questions regarding the tension between security and individual liberty, triggering debates that have implications for public policy and social norms. This intersection serves to highlight the complex ethical environment that ethical hackers navigate and underscores the importance of their work in maintaining responsible and fair technological practices.

In conclusion, the history of ethical hacking shows a dynamic interaction between technological innovation, learning development, strategic organizational behavior, and social ethics. As cyber threats are constantly evolving, the contribution of ethical hackers will continue to be crucial in creating a secure and morally ethical digital future.

## 5. Challenges in ethical hacking:

The role of ethical hackers in discovering and addressing vulnerabilities in networks is vital. However, they face numerous obstacles that often hinder their efforts and compromise the efficacy of cybersecurity protocols.

### 5.1. Quality and consistency:

The ethical hacking community is broad, consisting of a wide array of individuals and organizations that offer penetration testing services. This diversity poses a problem for organizations trying to choose providers that are consistent and deliver high-quality tests, and this impacts the effectiveness of security tests. Creation of standardized methodologies and certifications can ensure the credibility and reliability of provided services.

### 5.2. Shifting technological environment:

The fast rate of technological development necessitates a learning curve for ethical hackers that is ongoing. Keeping abreast of new technologies and their associated vulnerabilities necessitates continuous education and flexibility. Integration of ethical hacking into DevSecOps frameworks and the attainment of stackable certifications are some of the ways to deal with this fluid environment. Nevertheless, the rapid rate of technological development tends to leave the development of appropriate security measures behind, creating vulnerabilities that can be exploited by attackers. There needs to be continuous investment in training and development to fill this gap.

### 5.3. Organizational and communication challenges:

Successful collaboration among different stakeholders, such as cybersecurity experts and IT staff, is of extreme importance. Open communication ensures the proper testing parameters and understanding of the scope of engagement, thereby avoiding misinterpretations and ensuring ethical hacking activities are aligned with organizational objectives. Lack of proper alignment of security objectives and organizational priorities can result in wastage of resources and diminished efficacy of security activities. It is important to establish an environment of open communication and mutual understanding in order to address these issues.

## 6. Conclusion:

In summary, this systematic review highlights the dynamic and multi-faceted nature of ethical hacking as a field of cybersecurity. From the initial phases of ethical debate to the current applications of proactive security measures, like threat hunting, the field proves its adaptability and growing applicability. The integration of ethical hackers into education systems and organizational frameworks highlights their vital role in the strengthening of digital systems. Nevertheless, in spite of such advancements, issues persist, such as legal vagueness, the requirement of standardized quality, and the need for ongoing adjustment to emerging technologies. Counteracting such issues involves ongoing research, innovation, and firm commitment to ethical standards. With such initiatives in place, ethical hacking can continue to be an evolving but vital component of cybersecurity, effectively minimizing the risks and developing the resilience of digital systems.

## 7. References:

(1) M. Warren and W. Hutchinson, "Cyberspace ethics and information warfare," in *Information Management: Support Systems & Multimedia Technology*, IRM Press, 2003, pp. 215-227.

(2) N. M. Radziwill, J. Romano, D. Shorter, and M. C. Benton, "The Ethics of Hacking: Should It Be Taught?," *arXiv preprint*, arXiv:1512.02707, 2015. [Online]. Available: https://arxiv.org/abs/1512.02707.

(3) T. M. Kelly, "Who's In and Who's Out?: What's Important in the Cyber World?," in *Proc. 2016 Int. Conf. Cybersecurity and Cyberforensics*, 2016, pp. 24-29.

(4) G. Curcelli, "Unorthodox Hacking: Addressing Sexism in Hacktivist Communities to Expand Options for Electronic Civil Disobedience," in *Proc. 2017 ACM Conf. Computer-Supported Cooperative Work and Social Computing*, 2017, pp. 1187-1199.

(5) A. Ertan, G. Crossland, C. Heath, D. Denny, and R. J. Anderson, "Cyber Security Behaviour in Organisations," *Royal Holloway Research Portal*, 2020.

(6) B. Uchendu et al., "Developing a Cyber Security Culture: Current Practices and Future Needs," *arXiv preprint*, arXiv: 2106.14701, 2021. [Online]. Available: https://arxiv.org/abs/2106.14701

(7) G. Lorenzini, D. M. Shaw, and B. S. Elger, "It Takes a Pirate to Know One: Ethical Hackers for Healthcare Cybersecurity," *BMC Medical Ethics*, vol. 23, no. 1, pp. 1-10, 2022.

(8) J. Wang, D. Yang, X. Jiang, and T. Xin, "Cyber Threat Hunting Through Deep Learning: Challenges and Opportunities," *IEEE Network*, vol. 36, no. 3, pp. 122- 129, 2022.

(9) M. Nkongolo, N. Mennega, and I. van Zyl, "Cybersecurity Career Requirements: A Literature Review," *arXiv preprint*, arXiv: 2402.03324, 2023. [Online]. Available: https://arxiv.org/abs/2402.03324

(10) P. Čisar and R. Pinter, "Some Ethical Hacking Possibilities in Kali Linux Environment," *Journal of Applied Technical and Educational Sciences*, vol. 9, no. 4, pp. 129-149, 2019.

(11) "SecurityDaily Review," securitydailyreview.wixsite.com, 2023. [Online]. Available: https://securitydailyreview.wixsite.com

(12) E. A. Parn and D. J. Edwards, "Cyber Threats Confronting the Digital Built Environment," *Engineering, Construction and Architectural Management*, vol. 26, no. 2, pp. 245-266, 2019.