International Journal of Safety and Security Engineering
Vol. 16, No. 4, April, 2026, pp. 837-848
Journal homepage: http://iieta.org/journals/ijsse

A Comprehensive Survey on Ethical Hacking, Footprinting, and AI-Driven Penetration Testing in Modern Cybersecurity

S. Hemalatha[1*], Jency A.[2], A. Gnanasekar[3], R.V.V. Krishna[4], S. K. Satyanarayana[5], Charanjeet Singh[6]

[1] Department of Information Technology, Panimalar Engineering College, Chennai 600123, India
[2] Department of Artificial Intelligence and Data Science, R.M.K College of Engineering and Technology, Puduvoyal, Chennai 601206, India
[3] Department of Computer Science and Engineering, R.M.D. Engineering College, Chennai 601206, India
[4] Department of Electronics and Communication Engineering, Aditya University, Surampalem, Kakinada District 533437, India
[5] Department of Electronics and Communication Engineering, Sreenidhi Institute of Science and Technology, Hyderabad 501302, India
[6] Department of Electronics and Communication Engineering, Deenbandhu Chhotu Ram University of Science and Technology, Murthal 131039, India

Corresponding Author Email: pithemalatha@gmail.com

https://doi.org/10.18280/ijsse.160411

Received: 22 February 2026
Revised: 15 April 2026
Accepted: 27 April 2026
Available online: 30 April 2026

Keywords:
ethical hacking, penetration testing, footprinting, artificial intelligence-driven security, Open-Source Intelligence, governance-aware cybersecurity, human-centered security, system-level security engineering framework

ABSTRACT

Reconnaissance techniques radically change traditional security assessment processes. But from a system engineering perspective, the integration of human involvement, regulatory frameworks, governance and security design for sustainability is still fragmented and under-formalized. This study has conducted a systematic review based on a Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework of 51 peer-reviewed research papers published between 2022 and 2025. The review highlights the research across six key areas of AI-driven penetration testing, footprinting and open-source intelligence (OSINT) reconnaissance, web application security, network and Internet of Things (IoT) security, legal and governance, and human-centered cybersecurity education. Our findings reveal that automated and AI-powered security risk assessment models are clearly emerging in place of human-driven, skill-based penetration testing. However, some key structural gaps exist in the ecosystem. Although AI-based automation is technologically mature, areas such as sustainable security engineering, human-AI cooperation, legal-technical compatibility, and governance integration are less mature. In this research, a quantitative research gap scoring approach, based on existing evaluation criteria (such as technological readiness, implementation readiness, operational readiness, and resilience), is recommended to capture these variations. A heat map is also developed to visually represent topics of focus and gaps. An integrated system-level ethical hacking approach is proposed, based on the identified gap. It explicitly represents module interconnectedness, data flow architecture, and workflow among automated discovery, AI-based threat intelligence, human-in-the-loop verification, defensive feedback loops and governance-aware compliance control. The proposed methodology provides a systematic foundation for developing system-oriented, intelligent and responsible penetration testing systems to support real-world cybersecurity practices. This paper offers an empirical gap analysis, a holistic framework for AI-Human-Governance systems, and a structured taxonomy to encourage future work and support more responsible and engineering-centered cybersecurity innovation.

1. INTRODUCTION

Artificial intelligence (AI)-based technologies are increasingly impacting the current highly connected and data-rich digital world. Recent research shows that advanced decision-making support provided by AI technologies is transforming critical infrastructure. processes, smart automation, and forecasting across various domains such as communication networks, energy, and transportation [1]. Besides supporting business transformation through improving operational efficiency, decision-making and strategic responsiveness in the corporate environment, AI adoption has also helped organisations transform [2-4].

The rapid digitisation and increasing connectivity of systems, has also increased the surface of attack, opening critical infrastructure and Internet of Things (IoT) systems to more evolved and agile threat landscapes [5, 6]. Penetration testing and ethical hacking are well documented as proactive

cybersecurity practices that aim to discover and repair vulnerabilities before they can be exploited by hackers [7, 8].

Traditionally, ethical hacking approaches have been primarily manual and heavily dependent on security expert analysis. But recent studies reveal a clear trend toward automated and AI-powered penetration testing systems to improve speed, efficiency and adaptive adversarial emulation [9, 10]. From a system engineering perspective, this evolution represents a shift in security testing processes from isolated security testing to integrated security processes that include automated analysis, monitoring and iterative validation. Despite this, human oversight is still required for effective cybersecurity systems to ensure situational context, ethical considerations and decision making [11].

The emergence of AI-powered penetration testing systems that leverage automation and generative models in the stages of reconnaissance, vulnerability identification and exploitation is also emphasised in several studies [12, 13]. Furthermore, research suggests that incorporating human oversight into the workflows, the use of structured reasoning and large language models can improve the accuracy and reduce hallucinated or unrealistic responses [14, 15]. Industry assessments show that while generative AI's use in cybersecurity is increasing, many enterprises still face challenges in translating automated results into risk mitigation strategies, leaving critical vulnerabilities unaddressed [16]. The promise and current limitations of automated security evaluation methods are highlighted by empirical evidence, such as AI-based vulnerability detection in open-source cryptographic software (OpenSSL).

Some AI-based ethical hacking tools are only evaluated in a controlled or simulated environment, and not validated in an operational environment, despite the technological progress [17, 18]. Additionally, automated penetration testing procedures may not yet fully include governance and compliance procedures, which can cause operational and legal problems [19]. Also, there's a higher risk of misinterpretation, inaccuracies, and security gaps when there's excessive reliance on automated decision-making without human supervision [20]. AI-based security models still fail to sufficiently address human-related security risks, such as social engineering attacks [21]. Finally, intrusion detection and other cybersecurity defence systems are often developed in isolation from offensive security simulation tools, resulting in fragmented security testing processes and reduced system security [6]. This highlights an important weakness in the development of integrated cybersecurity systems, where defensive and offensive processes are not fully integrated [17].

This article offers a comprehensive review of the literature on ethical hacking and penetration testing from 2022 to 2025 to address these challenges. The research summarises the evolution of cybersecurity education and governance, automation through AI and Open-Source Intelligence (OSINT) driven reconnaissance [12, 22, 23]. By considering how technical, human and governance elements might be integrated and operationalised in a single cybersecurity system, this paper highlights system integration rather than survey-based research. The assessment also highlights the need for human-centred, systemic and governance-sensitive cybersecurity designs [19, 24].

The structure of this article is as follows. Section 1 discusses the problem statement and key challenges in ethical hacking and penetration testing research, along with the study's main contributions. It also presents a gap analysis approach and the proposed system-level framework. The systematic literature review process based on Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA), the data sources, search and screening process, and analysis methods are elaborated in Section 2. Section 3 reviews the evolution of ethical hacking and footprinting, and emerging trends in new cybersecurity systems. In Section 4, we provide a thematic review of some of the literature in terms of technical, human, legal, and governance aspects. The findings and discussion, major findings, confirmed gaps and system-engineering implications are outlined in Section 5. Finally, the paper is concluded in Section 6 with a summary and recommendations for future research.

1.1 Problem statement

The scale and scale of cybersecurity has dramatically grown as a result of the rapid digitalisation of public service systems, enterprise ecosystems, and infrastructure dangers. Vulnerability detection, verification and remediation actions become more complex as interconnected digital environments are growing and system attack surfaces are expanding and changing. In this context, proactive cybersecurity approaches such as ethical hacking and penetration testing are often used to detect vulnerabilities for potential abuse in future attacks.

The current research landscape is still fragmented, tool-centric, and lack of system-level integration across technology, human and governance aspects despite significant research in areas such as footprinting, OSINT based reconnaissance, vulnerability analysis and penetration testing. One major weakness is that much of the current research focuses on automation and AI-based penetration testing, often neglecting human judgement, ethical oversight, and regulatory enforcement processes. As a result, many automated reconnaissance and attack simulation systems do not have jurisdiction-specific governance boundaries, built-in compliance enforcement procedures, and human-level reasoning capabilities, which could affect their reliability and safe operationalisation in real-world scenarios.

Another significant drawback is the absence of a standard benchmarking or evaluation framework to assess the effectiveness, scalability and practicability of footprinting and OSINT-based reconnaissance techniques, despite the abundance of research conducted in these areas. Most existing research employs small experiments, simulations, or datasets, which reduces generalisability and could lead to reduced applicability to real cybersecurity systems.

Moreover, defensive cybersecurity methods and technologies such as proactive threat hunting, deception technologies, moving target defence, and counter-reconnaissance strategies are often developed in isolation from penetration testing. This often limits the design of closed-loop security systems, where simulated attacks can feed directly into the adaptive cybersecurity defences and prevent the design of integrated offensive-defensive cybersecurity systems.

Lastly, the technical research on penetration testing still does not fully consider legal, ethical and sustainability aspects. Legal restrictions are not often translated into practical constraints in automated security operations and AI-based testing platforms; rather, they are typically considered conceptually or within specific jurisdictional settings. Likewise, green security and energy-efficient computing are examples of sustainability-oriented cybersecurity technologies

that are still evolving and have yet to be systematically integrated into ethical hacking processes.

Finally, studies on cybersecurity education and training often emphasise teaching approaches that are more focused on learning outcomes than integration with AI-based penetration testing systems, automation in security processes and skills demanded in the cybersecurity industry. Overall, these limitations highlight the absence of a holistic system-engineering approach that can integrate automation, AI, human-in-the-loop verification, governance enforcement, and sustainability into penetration testing and ethical hacking processes. For ethical hacking to evolve from isolated technology applications to a system-engineering, governance-oriented and structured cybersecurity engineering discipline that can facilitate flexible and resilient cyber infrastructures, these challenges need to be addressed.

1.2 Contributions

The present research offers the following important contributions to overcome the gaps identified in the previous literature:

1.2.1 Organised system-based taxonomy of research on ethical hacking

This paper provides a structured taxonomy for ethical hacking and penetration testing research in six interrelated areas: intelligence gathering, vulnerability discovery, AI-based security analysis, defensive measures, governance and ethics, and human-centred cybersecurity education. Unlike traditional survey taxonomies, this taxonomy is developed from a system-engineering perspective, in particular highlighting the relationship and interdependence between the components of a cybersecurity process rather than individual research areas. This approach allows holistic analysis of technical and non-technical factors and improves understanding of the topic.

1.2.2 Systematic review of literature (2022-2025)

This research compares the current literature on footprinting, OSINT-driven reconnaissance, web and network security, AI-based penetration testing, legal aspects, and cybersecurity education. Along with summarising the current approaches, the comparative evaluation considers functionality, automation level, the scope of operation, and integration capabilities. This makes identification easier of persistent limits within fields, technological blending and methodological developments.

1.2.3 Quantitative research gap analysis using heatmap and scoring model

In this paper, we use themed heatmap representation to supplement quantitative gap analysis of research. The proposed scoring system measures the research maturity in various domains including impact on system resilience, readiness, technology advancement and implementation. This approach offers organised, semi-quantitative evidence of research gaps, and goes beyond traditional descriptive review approaches, particularly in areas such as governance integration, human-AI interaction, and sustainable cybersecurity design.

1.2.4 Integrated ethical hacking in AI, human and governance

This study proposes a system integration of ethical hacking based on the gaps identified. It comprises of automated scanning, AI-based intelligence analysis, human-in-the-loop verification, defensive feedback control, and governance-aware compliance checks. The framework enables continuous interaction between offensive and defensive cybersecurity components as it is designed as an operation model with dependencies between the modules and data streams. This enables better accountability, transparency, and controllability, while reducing risks associated with fully autonomous penetration testing.

1.2.5 Future research directions for safe and ethical cybersecurity

The paper proposes a number of future research paths including regulation-aware AI penetration testing, sustainable cybersecurity operations, adaptive reconnaissance countermeasures, and standardised benchmarking for ethical hacking tools among others. These methods demonstrate the transition from tool development to cybersecurity system engineering, where specific operational, governance, and evaluation aspects are explicitly integrated into the security design.

1.2.6 Integrating human, technical and governance

Contrary to traditional surveys that address mostly tools, algorithms or attack methods, this research considers the interplay between technical cybersecurity controls, human compliance and cybersecurity education. This interdisciplinary integration better represents the cybersecurity landscape and is more in line with the needs of contemporary security engineering, especially in socio-technical technical systems.

2. SYSTEMATIC LITERATURE REVIEW METHODOLOGY

To ensure transparency, repeatability and scientific rigour of the review process, this work follows the PRISMA approach [25]. To structure study selection, prevent selection bias, and ensure transparent inclusion criteria, PRISMA is often used in systematic reviews. Moreover, the design follows standard procedures for systematic reviews in the areas of technological and cybersecurity research [26, 27]. To assist with product- and engineering-level analysis and synthesis rather than a descriptive review, PRISMA is extended in this research with a system-oriented classification perspective.

2.1 Review objectives

The primary objective of this systematic review is to identify and assess the recent advancements in penetration testing and ethical hacking studies with a focus on system oriented cybersecurity advancements. The scope extends to footprinting and reconnaissance techniques, AI-supported penetration testing models, vulnerability assessment tools for web, network, IoT and mobile platforms and governance, legal and human factors perspectives on cybersecurity. We limited our search to only include peer-reviewed research published between 2022-2025 for relevance and technological timeliness. This period reflects the transition towards AI-driven automation in cybersecurity, emerging threats, and evolving governance and regulatory requirements.

2.2 Sources of data and search strategy

We searched major scientific databases relevant to cybersecurity and computer science research, including IEEE Xplore, SpringerLink, Elsevier ScienceDirect, ACM Digital Library, MDPI, CRC Press/Taylor & Francis, and Wiley Online Library, for related literature. To ensure we captured relevant literature, search strings were developed employing a mix of keywords and Boolean operators relevant to the field. Some of the keywords used were "ethical hacking", "penetration testing", "footprinting", "reconnaissance", " OSINT", "AI-driven penetration testing", "generative AI in cybersecurity" and "counter-reconnaissance techniques". Search queries were tailored to the indexing structure of each database to ensure consistency and completeness of searches across different sources.

2.3 Inclusion and exclusion criteria

To ensure rigour, uniformity and relevance, inclusion and exclusion criteria were set.

Studies were included if they

- Were academic book chapters, conference proceedings, or peer-reviewed journal articles
- Were released between 2022 and 2025.
- Were in English
- Addressed cybersecurity controls, pentesting, ethical hacking and reconnaissance.
- Research article was Exclusion if it
- Was not peer-reviewed (e.g., blogs, tutorials, white papers)
- Had been published before 2022
- Were incomplete and/or duplicated?
- Were not related to cybersecurity and ethical hacking studies.

This screening process will ensure that only the best, relevant and rigorous studies are included in the synthesis.

2.4 Selection of studies

The PRISMA stages of identification, screening, eligibility and inclusion were followed during the study selection process.

320 records were identified in the selected databases during the identification phase. After removing the duplicates, there were 235 unique records. Titles and abstracts were considered irrelevant or not technical enough to be included in the review for 142 studies which were excluded in the screening phase. 42 of the 93 studies that were carefully reviewed at the "full-text eligibility" stage were excluded because they only made theoretical contributions, had weak methodological underpinnings or did not align with the purpose of the review. 51 studies were included in the qualitative synthesis and comparative analysis. These studies form the basis of the gap analysis, framework development and classification. The whole process of selecting the research is presented in Figure 1 and provides a clear overview of the filtering and inclusion process.

2.5 Data extraction and analysis

We employed a systematic data extraction process for each selected study. The data collected included publication details, aims of the study, methodology, tools and techniques used, main findings and limitations of the study. The analysis used a multi-faceted approach that involved topic synthesis, comparative assessment, taxonomy creation, and quantitative assessment of research gaps. Furthermore, to visualise research intensity and gaps in research across the cybersecurity ecosystem at the domain level, we developed a research gap heatmap. This method provides a more rigorous review outcome, allowing for both analytical and descriptive assessment.

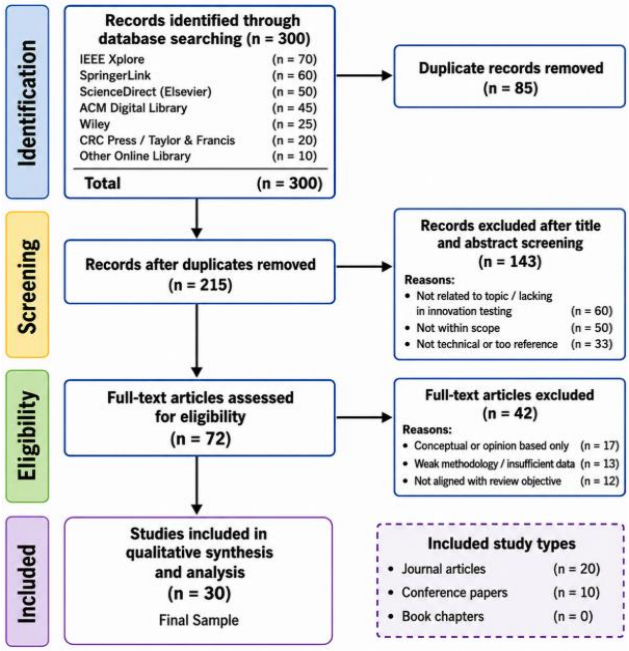

Figure 1. PRISMA flow diagram of the process for selection of research

2.6 Evaluation of quality

Each selected study was methodically evaluated for quality in order to ensure validity and relevance. Research goal clarity, method appropriateness, technological novelty on ethical hacking, validation and replicability of results were the criteria considered. Only the research that met minimal quality criteria is synthesised. This ensures the final framework and taxonomy are derived from technically and methodologically valid sources.

2.7 Validity of methods

PRISMA increases the traceability, auditability and transparency of the review process. The research minimises selection bias and enhances methodical rigour by documenting the identification, screening, eligibility and inclusion processes. Further, the traditional PRISMA approach is extended from a descriptive synthesis to engineering-focused cybersecurity assessment, via the use of system-oriented classification and quantitative gap analysis. This provides a stronger foundation for future gap modelling, framework development and thematic analysis.

3. INNOVATIONS IN MODERN CYBERSECURITY, ETHICAL HACKING AND FOOTPRINTING

3.1 Context and inspiration

The rapid adoption of cloud computing in the connected

digital environment, IoT and AI technologies have significantly increased the attack surface of modern cyber-physical and enterprise systems, increasing the range and nature of cyberthreat [28]. For this reason, ethical hacking and penetration testing are often employed as system-level, proactive security validation approaches that simulate possible adversarial actions to discover vulnerabilities [7]. Footprinting and reconnaissance are perhaps the most important stage of ethical hacking as they are the foundation of the entire process of penetration testing that relies on the quality, accuracy and depth of intelligence gained at this stage for the subsequent stages of attack simulation and defensive analysis [8, 22].

3.2 Stages of ethical hacking and alignment with the cyber kill chain

The Cyber Kill Chain and other models of real-world attacks are consistent with the defined cycle of ethical hacking [7, 29]. Reconnaissance, scanning, exploitation, and post-exploitation are examples of key processes that demonstrate both offensive and defensive cybersecurity activities [8]. Reconnaissance and footprinting, in particular, are essential in the initialisation of a system as they determine the effectiveness of vulnerability assessment processes and the comprehensiveness of threat intelligence [22]. Poorer threat modelling, fuzzier attack simulations, and less effective penetration testing results could be the outcome of insufficient or ineffective reconnaissance [18]. From a systems-engineering perspective, these steps can be viewed as interconnected components in an attack-defense loop in which subsequent security testing and defence strategies are influenced by reconnaissance.

3.3 Methods of reconnaissance and footprinting

3.3.1 Gathering and tracking

"Footprinting" refers to the systematic collection of intelligence across multiple sources about an organisation and its systems, including data from public databases, freely accessible technical systems and social media networks [22]. To build a hybridised intelligence-gathering framework, contemporary footprinting methods integrate human intelligence and automated scanning tools, along with third-party data aggregators [8].

3.3.2 Machine learning-supported footprinting

Machine learning algorithms such as Decision Trees and Naïve Bayes classifiers are increasingly used to identify patterns in data and classify potential attack vectors as data sets become more complex [6]. Footprinting with AI support offers improved scalability, pattern recognition and analysis consistency; however, model reliability, data bias and testing limitations remain significant challenges in real world applications [20].

3.4 Reconnaissance process automation

Automation and AI-based reconnaissance tools are making the processes of penetration testing more efficient, scalable, and consistent [10, 11]. Web application security is still primarily focused on lifecycle-based vulnerability detection in line with OWASP best practices [30]. OSINT helps support multiple phases of the Cyber Kill Chain, such as profiling and early reconnaissance [22, 29]. But there are challenges with explainability, result predictability and governance control when incorporating generative AI. Human oversight and legal considerations are still necessary to ensure the safe use of automated scanners [21, 31].

3.5 Assessing vulnerabilities of web applications (penetration testing)

Web applications are still highly vulnerable due to their direct link to critical back-end systems and public exposure (OWASP Foundation, 2021). The focus of these studies is mainly on security issues such as SQL injection, cross-site scripting (XSS) and configuration vulnerabilities [6]. Scanning with a tool is not enough, despite the fact that automated tools such as Burp Suite and OWASP ZAP significantly speed up the testing process [7, 30]. So, an end-to-end approach that includes vulnerability detection, exploit analysis, risk assessment and remedial planning within a loop for security validation is vital in web penetration testing.

3.6 Cyber kill chain and open-source intelligence

Today's reconnaissance relies on OSINT that leverages publicly available information sources such as social media, public records, and system metadata [22]. OSINT has a part in various stages of the Cyber Kill Chain, especially profiling and reconnaissance [29, 8]. Both sides can leverage the same sources of information for situational awareness, threat anticipation and to achieve more stealth and precision. Because of the potential for misuse and privacy concerns, OSINT activities must have strong governance, ethical constraints and usage policies because of the dual-use nature of OSINT [31].

3.7 AI and generative AI-based penetration testing

AI, particularly generative AI, is increasingly transforming penetration testing by offering automated vulnerability identification, reasoning and adaptive attack simulation [10, 11]. To ensure systematic threat modelling and assessment, recent AI-based security systems are often aligned with structured cybersecurity frameworks such as the Cyber Kill Chain and MITRE ATT&CK [29]. But there are several significant issues with generative AI, including its lack of explainability, hallucinations, and governance problems in security settings where decisions are critical. As a result, human-in-the-loop and governance-aware AI systems that integrate operational and ethical constraints in automated penetration testing workflows are the subject of current research [20, 31].

3.8 Human and social engineering

Humans remain a weak link in cybersecurity systems despite advancements. Experience and research consistently shows that insider threats, spear phishing and social engineering attacks are still extremely effective as they exploit human biases and psychological manipulation [32, 33]. Employees, administrators and other users with permitted access to systems are critical insider risk factors that increase the risk of unauthorised access to data or systems [34, 35]. In order to reduce the human-centred vulnerabilities, effective cybersecurity approaches should include technical safeguards and human behaviour training, awareness, and security culture building [36, 37].

4. REVIEW OF RESEARCH ON ETHICAL HACKING AND PENETRATION TESTING

Following the systematic review, this chapter offers a structured thematic overview of research into ethical hacking and penetration testing. The selected studies are categorised into six related sectors that reflect the socio-technical and technical considerations of cybersecurity [20]. This work draws attention to system-level interactions, cross-sectoral interdependencies and governance integration gaps across cybersecurity processes, unlike narrative reviews. The dialogue also brings to the fore new developments and persistently weak points in human oversight, regulatory fit, and AI use [38-41].

4.1 AI-augmented technical methods

AI-powered ethical hacking [42-45] is a rapidly growing area of cybersecurity research. There is an increasing adoption of machine learning and generative AI to automate tasks in penetration testing, as Table 1 illustrates. Traditional models, such as Decision Trees and Naïve Bayes, have been very accurate (often above 98%) in the areas of footprinting and reconnaissance. These results, however, may not be completely relevant to real-world adversarial environments as they are typically derived under controlled environments.

Generative AI and large language models (LLMs) are new models that support automated attack simulations, dynamic vulnerability hunting and security reporting. These systems now use reasoning-based security analysis, instead of rule-based automation. Despite these developments, the literature continues to point out unresolved problems such as regulatory uncertainty, deployment challenges, explainability, and underpinning existing security frameworks. Crucially, the effectiveness of existing AI-powered penetration testing solutions is constrained by their failure to connect with enforcement and human verification layers.

Footprinting and reconnaissance remain an integral part of ethical hacking. The research in Table 2 identifies passive and active intelligence gathering techniques for identifying attack surfaces and system vulnerabilities. Modern OSINT platforms utilise multi-source correlation, Python-based intelligence gathers, and data gathering. Additionally, these studies demonstrate a broader expansion of the attack surface by extending reconnaissance from the network to hardware and environmental intelligence extraction.

Table 1. AI-driven ethical hacking and intelligent penetration testing

Authors	Year	Methodology	Key Contribution	Research Gap
Verma et al. [46]	2023	Decision Tree, Naïve Bayes	ML-based Footprinting (>98% accuracy)	Limited ML diversity
Alnuaimi et al. [47]	2025	ChatGPT evaluation study	Validated AI-assisted hacking training	Practical limitations
Maleh [48]	2025	Generative AI PT frameworks	Adaptive AI penetration testing	Regulatory ambiguity
Prakash et al. [49]	2022	Digital footprint monitoring	AI-based anomaly detection	SOC dependency

Table 2. Footprinting, reconnaissance, and open-source intelligence (OSINT)

Authors	Year	Methodology	Key Contribution	Research Gap
Venkadasubbiah et al. [50]	2022	Passive & Active Footprinting	Hidden digital identity concept	No mitigation model
Cochran [51]	2024	Conceptual reconnaissance	Importance of pre-attack intelligence	No automation
Ahmed et al. [52]	2023	SearchOL (Python)	Efficient OSINT aggregation	Privacy concerns
Kaushik et al. [53]	2022	Python recon automation	Bug bounty automation	Recon-only focus
Gupta et al. [54]	2022	OCR-based hardware recon	Automated hardware Footprinting	Hardware-specific
Roy et al. [55]	2023	Recon taxonomy survey	Adversarial classification	Limited defensive validation
Yamin et al. [56]	2022	OSINT–Kill Chain mapping	Tool-to-phase intelligence mapping	Tool variance
Reiner et al. [57]	2025	Data footprint analysis	Supply-chain footprint risks	Not cybersecurity-centric

Table 3. Web application security & vulnerability assessment

Authors	Year	Methodology	Key Contribution	Research Gap
Alby et al. [58]	2023	Website Footprinting & scanning	Real-world vulnerability detection	Single case
Desai et al. [59]	2025	Browser-based scanners	Real-time extension scanning	Partial lifecycle
Jose et al. [60]	2022	Parameter tampering	Demonstrated business impact	Limited defence
Lachkov et al. [61]	2022	PT simulation framework	Full PT lifecycle	Tool-dependent
Alhogail and Alkahtani [62]	2024	Automated extension PT	Faster identification	Limited exploit depth
Gandikota et al. [63]	2023	OWASP-based assessment	Comprehensive taxonomy	Case-based
Brandi et al. [64]	2024	Modular fuzz testing	Advanced input fuzzing	Computational overhead

Table 4. Network security, IoT & infrastructure protection

Authors	Year	Methodology	Key Contribution	Research Gap
Mohan et al. [65]	2023	Network exploit lifecycle	Complete attack simulation	Environment-dependent
Tiwari et al. [66]	2023	IoT automation testing	Holistic IoT security testing	Complex deployment
Żal et al. [67]	2024	Moving Target Défense	Recon disruption	Infrastructure requirements
Mahajan and Singh [68]	2022	Honeypot flood testing	Intrusion detection	Limited attack scope
Courtney et al. [69]	2023	Risk scoring model	Quantified severity	Needs automation
Rehman et al. [70]	2024	Smart assistant testing	Smart home vulnerabilities	Single-device focus
Vajpayee and Hossain [71]	2024	Optimization framework	Risk-investment balance	Domain-specific
Katoch and Garg [72]	2023	Android penetration testing	Mobile vulnerabilities	OS-specific

But, instead of a fully integrated approach with defensive systems such as validation or mitigation, most research focuses on building reconnaissance. Furthermore, the lack of benchmarking for evaluating OSINT makes it difficult to compare and reproduce research. Furthermore, ethical concerns and privacy risks are not sufficiently tackled.

Web application security remains a popular and well-studied field of ethical hacking. Common vulnerabilities and failures include SQL injection, cross-site scripting (XSS), parameter manipulation and insecure configurations, as shown in Table 3. To enhance detection, recent studies emphasise fuzz testing, extensions, and scanners. However, most existing approaches are still tool-based and fail to provide end-to-end security testing in particular with respect to post-remediation assessment and exploitation. Automation improves productivity but for complex real-life applications, too much reliance on scanner-based approaches without human intervention reduces the quality of the assessment.

Cybersecurity has become more complex with the advent of IoT, mobile and cloud computing. Table 4 contains research on mobile penetration testing, automated IoT security, and modelling the attack lifecycle. There is more research on defensive approaches such as risk-based scoring models, honeypots and Moving Target Defence (MTD). Software Defined Networks (SDN) used in conjunction with MTD have the potential to thwart reconnaissance-based attacks while ensuring quality of service. But scalability of many proposed solutions are hampered by the need for specific deployment environments or complex setups. A lack of interface between adaptive real-time defence and IoT security testing is a significant shortcoming.

4.2 Human, legal, and educational perspectives

The research in Table 5 illustrates differences in legal and governance frameworks across jurisdictions. For example, unlike uses in the private sector, ethical hacking is often more explicitly authorised in government. The research also examines the policy implications of zero-day vulnerabilities, discourse on cybercrime, ethical computing and sustainability. However, most governance research is still conceptual and does not lead to technical rules that can be implemented in penetration testing systems. A key area for further research is the gap between governance discussion and system implementation. Techniques for enhancing compliance with different jurisdictions are not common in current AI-based security tools.

Human factors are still critical for cybersecurity. Table 6 shows studies on behavioural risk assessment, educating with assault simulations, training models and problem-based learning (PBL). Research shows that preparing cybersecurity education in line with industry standards yields better analytical and readiness skills. However, most educational models are still isolated from real-time security automation and AI-based penetration testing systems.Vulnerability to insider attacks and social engineering suggest the need for holistic human-system cybersecurity approaches that combine machine-based defence approaches with human behaviour.

Table 5. Ethical, legal, and governance perspectives

Authors	Year	Methodology	Key Contribution	Research Gap
Pal and Gulati [73]	2025	Doctrinal legal study	Legislative gaps in ethical hacking	Region-specific
Arsat et al. [74]	2025	Economic analysis	Ethical hacking & economic stability	No empirical validation
Guseva and Pliva [75]	2024	Linguistic analysis	Cybercrime ecosystem framing	Non-technical
Pasricha and Wolf [76]	2024	Ethical computing analysis	Ethics from hardware to AI	Conceptual
Das et al. [77]	2023	Zero-day terrorism review	Policy & economic impact	Non-technical
Friedl et al. [78]	2024	Sustainable forensics	Green cybersecurity perspective	Early-stage research

Table 6. Cybersecurity education, training & human-centric security

Authors	Year	Methodology	Key Contribution	Research Gap
Schmeelk and Dragos [79]	2023	NIST-based curriculum	Industry-aligned training	Academic scope
Bhatia et al. [80]	2023	PBL for ethical hacking	Improved critical thinking	Scalability issues
Bhatia et al. [81]	2024	PBL + MITRE mapping	Enhanced real-world readiness	Academic context
Samrouth et al. [82]	2023	Attack tree dataset	Reduced time-to-solve	Preliminary dataset
Alsmadi [83]	2023	NICE framework	Structured threat modelling	Conceptual
Udofia [84]	2025	Human-centric risk analysis	Behavioural cybersecurity focus	Non-technical
Stoddart [85]	2022	Social engineering study	Insider & phishing analysis	Defensive depth limited
Beuran [86]	2025	Attack training methodology	Structured pentesting training	Learning-centric
Altulaihan et al. [87]	2022	Threat awareness review	Awareness gap identification	Limited technical depth

4.3 Gap analysis: Distribution, heatmap, scoring

The final classification consists of 42 articles from six fields (Figure 2):

- AI-based penetration testing (4 articles)
- Footprinting and OSINT (8 articles)
- Web application security (7 articles)
- Network/IoT security (8 articles)
- Law and Governance (6 articles)
- Human-Centric Security and Education (9 articles)

Education and human-centric security has the largest proportion, which indicates workforce development is increasingly being emphasised. But much of this is still theoretical and academic, while not being integrated within the system. Today's more complex attack surfaces are reflected in footprinting and IoT security. Governance research is small but very important. The most disruptive is AI-based penetration testing, albeit smaller in size. Overall, the research supports the move towards AI-powered cybersecurity; however, there is a need for system-level integration of technology automation with governance.

A heatmap was designed to understand the maturity of research across six cybersecurity domains and multiple assessment criteria, including automation, AI, deployment, governance, human-centred and sustainable cybersecurity. The results reveal a clear gap between technical and non-

technical research maturity. While governance, human-centricity and sustainability are still poor or in their infancy, technical domains such as Web security and AI-based penetration testing show high automation and maturity to frameworks. Important Research Gaps Found:

- Law and Technology Gap: Technical penetration testing tools lack legal integration.
- AI-Governance Gap: AI-based tools are not connected with enforcement of regulation and verification of compliance.
- Human-Automation Gap: Automation of testing processes is not linked to behavioural cybersecurity research.
- Green Gap: Green or energy-efficient cybersecurity operations research is lacking.
- Integrated Model Gap: Absence of a unified model for governance, human-in-the-loop and AI.

To verify the qualitative findings, a scoring approach was adopted. AI Integration, Human-Centricity, Automation, Governance and Validation were scored.

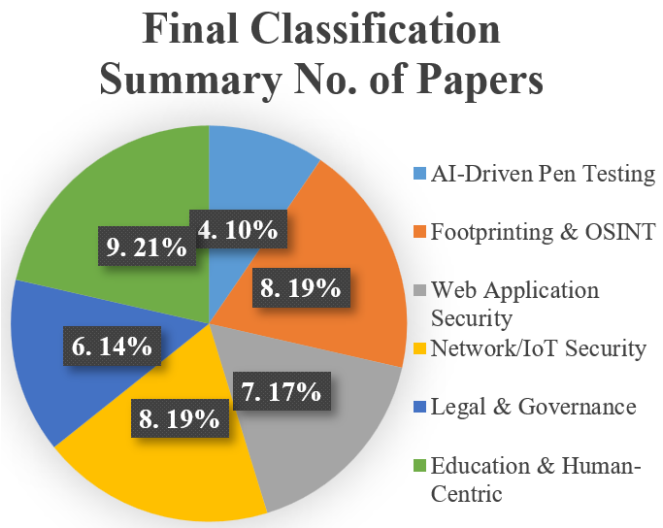

Figure 2. Final classification includes

The calculation of gap scores is as follows:

Gap Score = 5 - (AI + Automation + Validation + Governance + Human)

- 0-1: Thoroughly investigated
- 2-3: Moderately investigated
- 4-5: Crucial gap

The findings indicate:

- Network/IoT, Web security and footprinting → moderate maturity
- High tech but low governance in AI-powered PT
- Law vs ethics → the key disparity
- The basic missing human factor in security
- Sustainability → the greatest gap

These research results provide evidence that the areas of ethical hacking which need more research are still sustainability, human integration and governance.

4.4 Cross-disciplinary trends and proposed integrated framework

Technologies are advancing at a much faster pace than governance, human-centricity, and sustainability, and this trend is universal. While the legal, ethical and human-related areas are still in their infancy, AI-based penetration testing, OSINT and cybersecurity are highly technologically advanced. This highlights the absence of an integrated system-level cybersecurity architecture that can facilitate defensive feedback, automation, human oversight and compliance.

The proposed integrated ethical hacking model involves:

- The use of automated reconnaissance
- AI-driven intelligence processing
- Human-in-the-loop verification
- Defensive feedback loops
- Governance-aware compliance enforcement

By turning ethical hacking from tools to a system engineering design, this approach addresses the found gaps.

5. FINDINGS AND DISCUSSION

According to the review, which looked at 51 papers published between 2022 and 2025, there is a growing trend in ethical hacking research from manual to automated and AI-powered penetration testing. Vulnerability scanning, reconnaissance and simulation of attacks increasingly heavily depend on AI techniques such as machine learning, generative AI and reinforcement learning. As reviewers generally focus on, there is one major concern despite these advancements: governance, legal compliance and sustainability do not match technological advancement. While automation and footprinting improve effectiveness in OSINT, there is no code of ethics and no standardised assessment methods. While they are more tool-based and only applicable in regulated cases, web, network, and IoT security is still advanced. The most rapidly evolving area is AI-powered ethical hacking but there are no standards, compliance measures or explainability. The absence of links between defensive cybersecurity and AI-based attacks is a major obstacle to adaptive security development. The disconnect between technology and non-technical elements (legal, ethical, human oversight and sustainability) is a major concern of reviews. Overall, the area is rapidly evolving, but it remains patchy.

6. CONCLUSION

Research into ethical hacking between 2022 and 2025 will see a change in focus from manual security testing to smart, AI-enabled penetration testing, the study found. There have been great improvements in automation, OSINT, web security and IoT penetration testing, where AI improves the coverage and speed of testing. The study would argue that this advancement is not yet mature, safe, and responsible, as the governance, explainability or legal compliance are still absent.

The key contribution of this review is to point out three gaps:

- The lack of legal and technical integration (no compliance-aware systems)
- The human-AI gap (lack of human assessment in AI)
- The absence of sustainable cybersecurity (no focus on energy-efficient cybersecurity)

The research concludes that instead of only focusing on technological innovation, the future of ethical hacking should embrace a balanced approach with a combination of AI automation, human oversight, regulatory compliance and sustainability.

Rather than focusing purely on improving technical

efficiency, future research should focus on addressing the key gaps identified in this review.

The main areas are:

- Developing legal and ethical compliant AI penetration testing tools
- Enhancing human-in-the-loop approaches for validating and making decisions regarding AI-powered security solutions
- Creating benchmarks and standardised data sets to improve replicability and the ability to compare
- Building environmentally friendly and energy-efficient cybersecurity models to reduce their environmental impact
- Integrating defensive techniques (such as deception and cyber-adaptive defence) with an offensive approach using AI
- Encouraging cross-disciplinary collaboration among behavioural science, legal and cybersecurity experts

Overall, it is expected that future research on ethical hacking will prioritise smart, sustainable, human and controlled cybersecurity models that adapt to cyber threats.

REFERENCES

[1] McMillan, L., Varga, L. (2022). A review of the use of artificial intelligence methods in infrastructure systems. Engineering Applications of Artificial Intelligence, 116: 105472. https://doi.org/10.1016/j.engappai.2022.105472

[2] Parwani, D., Tahilyani, M., Devnani, M. (2024). AI in industry 5.0: Transforming business in the digital age. In Industry 5.0 and Emerging Technologies, pp. 59-86. https://doi.org/10.1007/978-3-031-70996-8_4

[3] Rashid, A.B., Kausik, M.A.K. (2024). AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications. AI Perspectives and Hybrid Advances, 7: 100277. https://doi.org/10.1016/j.hybadv.2024.100277

[4] Argyroudis, S.A., Mitoulis, S.A., Chatzi, E., Baker, J.W., et al. (2022). Digital technologies can enhance climate resilience of critical infrastructure. Climate Risk Management, 35: 100387. https://doi.org/10.1016/j.crm.2021.100387

[5] Pourrahmani, H. Yavarinasab, A. Monazzah, A.M.H., Van herle, J. (2023). A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain. Internet of Things, 23: 100888. https://doi.org/10.1016/j.iot.2023.100888

[6] Buczak, A.L., Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2): 1153-1176. https://doi.org/10.1109/COMST.2015.2494502

[7] Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A. (2008). Technical guide to information security testing and assessment. NIST Special Publication 800-115. https://doi.org/10.6028/NIST.SP.800-115

[8] Tounsi, W., Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & Security, 72: 212-233. https://doi.org/10.1016/j.cose.2017.09.001

[9] Fei, C., Shen, J. (2023). Machine learning for securing Cyber–Physical Systems under cyber attacks: A survey. Franklin Open, 4: 100041. https://doi.org/10.1016/j.fraope.2023.100041

[10] Wong, A.Y., Chekole, E.G., Ochoa, M., Zhou, J. (2023). On the security of containers: Threat modeling, attack analysis, and mitigation strategies. Computers & Security, 128: 103140. https://doi.org/10.1016/j.cose.2023.103140

[11] Ghanem, M.C., Chen, T.M. (2020). Reinforcement learning for efficient network penetration testing. Information, 11(1): 6. https://doi.org/10.3390/info11010006

[12] Kaur, R., Gabrijelčič, D., Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97: 101804. https://doi.org/10.1016/j.inffus.2023.101804

[13] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A., Chen, S., Liu, D., Li, J. (2020). Performance comparison and current challenges of using machine learning techniques in cybersecurity. Energies, 13(10): 2509. https://doi.org/10.3390/en13102509

[14] Yang, X., Kong, L.S., Liu, Z., Chen, Y.L., Li, Y.M., Zhu, H.L. (2018). Machine learning and deep learning methods for cybersecurity. IEEE Access, 6: 35365-35381. https://doi.org/10.1109/ACCESS.2018.2836950

[15] Das, B.C., Amini, M.H., Wu, Y.Z. (2025). Security and privacy challenges of large language models: A survey. ACM Computing Surveys, 57(6): 1-39. https://doi.org/10.1145/3712001

[16] Pearce, H., Ahmad, B., Tan, B., Dolan-Gavitt, B., Karri, R. (2022). Asleep at the keyboard? Assessing the security of GitHub Copilot's code contributions. Communications of the ACM, 68(2): 96-105. https://doi.org/10.1145/3610721

[17] Zaazaa, O., El Bakkali, H. (2022). Automatic static vulnerability detection approaches and tools: State of the art. In The International Conference on Information, Communication & Cybersecurity, Khouribga, Morocco, pp. 449-459. https://doi.org/10.1007/978-3-030-91738-8_41

[18] Sommer, R., Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE Symposium on Security and Privacy, Oakland, CA, USA, pp. 305-316. https://doi.org/10.1109/SP.2010.25

[19] Taddeo, M., Floridi, L. (2021). How AI can be a force for good-an ethical framework to harness the potential of AI while keeping humans in control. In Ethics, Governance, and Policies in Artificial Intelligence, pp. 91-96. https://doi.org/10.1007/978-3-030-81907-1_7

[20] Sarker, I.H., Kayes, A.S.M., Watters, P. (2019). Effectiveness analysis of machine learning classification models for predicting personalized context-aware cybersecurity. Journal of Big Data, 6: 57. https://doi.org/10.1186/s40537-019-0219-y

[21] Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Indianapolis, IN, John Wiley & Sons. https://doi.org/10.1002/9781119433729

[22] Pastor-Galindo, J., Nespoli, P., Mármol, F.G., Pérez, G.M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access, 8: 10282-10304. https://doi.org/10.1109/ACCESS.2020.2965257

[23] Floridi, L. (2023). The Ethics of Artificial Intelligence: Principles, Challenges, And Opportunities. New York,

NY, Oxford University Press. https://doi.org/10.1093/oso/9780198883098.001.0001
[24] Zhang, B., Li, J., Ren, J., Huang, G. (2021). Efficiency and effectiveness of web application vulnerability detection approaches: A review. ACM Computing Surveys (CSUR), 54(9): 1-35. https://doi.org/10.1145/3474553
[25] Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372. https://doi.org/10.1136/bmj.n71
[26] Kitchenham, B., Brereton, O.P., Budgen, D., Turner, M., Bailey, J., Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review. Information and Software Technology, 51(1): 7-15. https://doi.org/10.1016/j.infsof.2008.09.009
[27] Siddaway, A.P., Wood, A.M., Hedges, L.V. (2020). How to do a systematic review: A best practice guide for conducting and reporting narrative reviews, meta-analyses, and systematic reviews. Annual Review of Psychology, 70: 747-770. https://doi.org/10.1146/annurev-psych-010418-102803
[28] Khan, R., Kumar, P., Jayakody, D.N.K., Liyanage, M. (2019). A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. IEEE Communications Surveys & Tutorials, 22(1): 196-248. https://doi.org/10.1109/COMST.2019.2933899
[29] Hutchins, E.M., Cloppert, M.J., Amin, R.M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, 1(1): 80.
[30] Tomescu, A., Chen, R., Zheng, Y., Abraham, I., Pinkas, B., Gueta, G.G., Devadas, S. (2020). Towards scalable threshold cryptosystems. In 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, pp. 877-893. https://doi.org/10.1109/SP40000.2020.00059
[31] Taddeo, M., McCutcheon, T., Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. Nature Machine Intelligence, 1(12): 557-560. https://doi.org/10.1038/s42256-019-0109-1
[32] Albladi, S.M., Weir, G.R.S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. Human-centric Computing and Information Sciences, 8(1): 5. https://doi.org/10.1186/s13673-018-0128-7
[33] Vishwanath, A., Harrison, B., Ng, Y.J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. Communication Research, 45(8): 1146-1166. https://doi.org/10.1177/0093650215627483
[34] Greitzer, F.L., Kangas, L.J., Noonan, C.F., Dalton, A.C., Hohimer, R.E. (2012). Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. In 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, pp. 2392-2401. https://doi.org/10.1109/HICSS.2012.309
[35] Legg, P.A., Buckley, O., Goldsmith, M., Creese, S. (2017). Automated insider threat detection system using user and role-based profile assessment. IEEE Systems Journal, 11(2): 503-512. https://doi.org/10.1109/JSYST.2015.2438442
[36] Bada, M., Sasse, A.M., Nurse, J.R.C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? Computers & Security. https://doi.org/10.48550/arXiv.1901.02672
[37] Puhakainen, P., Siponen, M. (2010). Improving employees' compliance through information security training: An action research study. MIS Quarterly, 34(4): 757-778. https://doi.org/10.2307/25750704
[38] Huang, J. (2020). Applicable law to transnational personal data: Trends and dynamics. German Law Journal, 21(6): 1283-1308. https://doi.org/10.1017/glj.2020.73
[39] Svantesson, D.J.B. (2011). The regulation of cross-border data flows. In International Data Privacy Law, pp. 180-198. https://doi.org/10.1093/idpl/ipr012
[40] Hublet, F., Basin, D., Krstić, S. (2024). Enforcing the GDPR. In Computer Security – ESORICS 2023. Springer, Cham, pp. 400-422. https://doi.org/10.1007/978-3-031-51476-0_20
[41] Beckerman, C.E. (2022). Is there a cyber security dilemma? Journal of Cybersecurity, 8(1): tyac012. https://doi.org/10.1093/cybsec/tyac012
[42] Cath, C. (2018). Governing artificial intelligence: Ethical, legal and technical opportunities and challenges. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376(2133): 20180080. https://doi.org/10.1098/rsta.2018.0080
[43] Cobbe, J., Singh, J. (2021). Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges. Computer Law & Security Review, 42: 105573. https://doi.org/10.1016/j.clsr.2021.105573
[44] Zheng, J., Namin, A.S. (2019). A survey on the moving target defense strategies: An architectural perspective. Journal of Computer Science and Technology, 34(1): 207-233. https://doi.org/10.1007/s11390-019-1906-z
[45] Franco, J., Aris, A., Canberk, B., Uluagac, A.S. (2021). A survey of honeypots and honeynets for Internet of Things, industrial Internet of Things, and cyber-physical systems. IEEE Communications Surveys & Tutorials, 23(4): 2351-2383. https://doi.org/10.1109/COMST.2021.3106669
[46] Verma, J., Baggan, V., Kaur, I., Sethi, M., Snehi, M., Harnal, S. (2023). Ethical hacking through foot printing: A machine learning strategy. In 2023 7th International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, pp. 1-5. https://doi.org/10.1109/ICCUBEA58933.2023.10392124
[47] Alnuaimi, R., Alawida, M., Al-Rawashdeh, M., Mejri, S. (2025). ChatGPT's impact on ethical hacking and cybersecurity. In Examining Cybersecurity Risks Produced by Generative AI, pp. 573-608. https://doi.org/10.4018/979-8-3373-0832-6.ch024
[48] Maleh, Y. (2025). Generative AI-driven penetration testing: Frameworks, methodologies, and ethical considerations. In Generative AI for Cybersecurity and Privacy, pp. 243-282. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003597476-17/generative-ai-driven-penetration-testing-yassine-maleh.
[49] Prakash, G., Ganeshan, M., Shenbagavalli, A., Satheesh Kumar, M., Srujan Raju, K., Suthendran, K. (2022). A proactive threat hunting model to detect concealed anomaly in the network. In Smart Intelligent Computing and Applications, pp. 553-565.

https://doi.org/10.1007/978-981-16-9705-0_54
[50] Venkadasubbiah, S., Yuvaraj, D., Ali, S., Uvaze Ahamed Ayoobkhan, M. (2022). Data footprinting in big data. In Big Data Analytics and Computational Intelligence for Cybersecurity, Springer, pp. 203-218. https://doi.org/10.1007/978-3-031-05752-6_13
[51] Cochran, K.A. (2024). Information gathering and footprinting in cybersecurity. In Cybersecurity Essentials. Apress, pp. 33-53. https://doi.org/10.1007/979-8-8688-0432-8_3
[52] Ahmed, F., Khatri, P., Surange, G., Agrawal, A. (2023). SearchOL: An information gathering tool. In Intelligent Systems Design and Applications, pp. 343-349. https://doi.org/10.1007/978-3-031-35501-1_34
[53] Kaushik, K., Yadav, S.A., Chauhan, V., Rana, A. (2022). An approach for implementing comprehensive reconnaissance for bug bounty hunters. In 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, pp. 189-193. https://doi.org/10.1109/IC3I56241.2022.10072942
[54] Gupta, K., Dineshan, A., Nair, A., Ganesh, J., Anjali, T., Sriram, P., Harikrishnan, J. (2022). Automated hardware recon-A novel approach to hardware reconnaissance process. In Inventive Computation and Information Technologies, pp. 267-279. https://doi.org/10.1007/978-981-16-6723-7_20
[55] Roy, S., Sharmin, N., Acosta, J.C., Kiekintveld, C., Laszka, A. (2023). Survey and taxonomy of adversarial reconnaissance techniques. ACM Computing Surveys, 55(6): 1-38. https://doi.org/10.1145/3538704
[56] Yamin, M.M., Ullah, M., Ullah, H., Katt, B., Hijji, M., Muhammad, K. (2022). Mapping tools for open source intelligence with cyber kill chain for adversarial aware security. Mathematics, 10(12): 2054. https://doi.org/10.3390/math10122054
[57] Reiner, V., Malik, A.,Murray, J. (2025). Can global modern slavery be footprinted for corporate due diligence? A data review and analysis. Journal of Industrial Ecology, 29(4): 1077-1089. https://doi.org/10.1111/jiec.70037
[58] Alby, M.F., Ruslan, I.F., Muharman, M.L. (2022). Information security test on websites and social media using footprinting method. In Proceedings of the 8th International Conference on Industrial and Business Engineering, New York, NY, USA, pp. 521-525. https://doi.org/10.1145/3568834.3568868
[59] Desai, D., Baria, H., Chauhan, A., Yadav, G., Patidar, M., Mahale, M. (2025). Website vulnerability scanning extension. In Parul University International Conference on Engineering and Technology 2025, Hybrid Conference, Vadodara, India, pp. 130-136. https://doi.org/10.1049/icp.2025.1286
[60] Jose, L., Khanna, M.R., Meganathan, D., Praveen Kumar, B.T. (2022). Web based parameter-tampering on shopping site using BurpSuite testing. In Artificial Intelligence and Communication Technologies, SCRS, India, pp. 527-535. https://doi.org/10.52458/978-81-955020-5-9-51
[61] Lachkov, P., Tawalbeh, L., Bhatt, S. (2022). Vulnerability assessment for applications security through penetration simulation and testing. Journal of Web Engineering, 21(7): 2187-2208. https://doi.org/10.13052/jwe1540-9589.2178
[62] Alhogail, A., Alkahtani, M. (2024). Automated extension-based penetration testing for web vulnerabilities. Procedia Computer Science, 238: 15-23. https://doi.org/10.1016/j.procs.2024.05.191
[63] Gandikota, P.S.S.K., Valluri, D., Mundru, S.B., Yanala, G.K., Sushaini, S. (2023). Web application security through comprehensive vulnerability assessment. Procedia Computer Science, 230: 168-182. https://doi.org/10.1016/j.procs.2023.12.072
[64] Brandi, C., Perrone, G., Romano, S.P. (2024). Sniping at web applications to discover input-handling vulnerabilities. Journal of Computer Virology and Hacking Techniques, 20: 641-667. https://doi.org/10.1007/s11416-024-00518-0
[65] Mohan, A., Aravind Swaminathan, G., Shafana, J. (2023). Systematic approach for network security using ethical hacking technique. In Intelligent Communication Technologies and Virtual Mobile Networks, pp. 47-59. https://doi.org/10.1007/978-981-19-1844-5_4
[66] Tiwari, P., Rajendran, S., (2023). Automatic performance verification of industrial gateway using Python framework. In 2023 14th International Conference on Computing Communication and Networking Technologies, Delhi, India, pp. 1-7. https://doi.org/10.1109/ICCCNT56998.2023.10307262
[67] Żal, M., Michalski, M., Zwierzykowski, P. (2024). Implementation of a lossless moving target defense mechanism. Electronics, 13(5): 918. https://doi.org/10.3390/electronics13050918
[68] Mahajan, V., Singh, J. (2022). Performance analysis of honeypots against flooding attack. In 2022 6th International Conference on Electronics, Communication and Aerospace Technology, Coimbatore, India, pp. 1-6. https://doi.org/10.1109/ICECA55336.2022.10009485
[69] Courtney, K., Oleary, E., Anand, S., Amutha, S. (2023). Vulnerability analysis and risk scoring of networks. In 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), Kirtipur, Nepal, pp. 320-324. https://doi.org/10.1109/I-SMAC58438.2023.10290524
[70] Rehman, F., Hashmi, J., Abdullah, M., Zaman, H. (2024). Guarding voices, protecting homes: A comprehensive case study on voice assistant security in smart living. In 2024 12th International Symposium on Digital Forensics and Security (ISDFS), San Antonio, TX, USA, pp. 1-6. https://doi.org/10.1109/ISDFS60797.2024.10527336
[71] Vajpayee, P., Hossain, G. (2024). Cognitive cybersecurity in transportation 5.0 and supply chain: A multi-objective optimization framework. In 2024 IEEE International Conference on Electro Information Technology (eIT), Eau Claire, WI, USA, pp. 698-704. https://doi.org/10.1109/eIT60633.2024.10609882
[72] Katoch, S., Garg, V. (2023). Security analysis on Android application through penetration testing. In Proceedings of Fourth Doctoral Symposium on Computational Intelligence, pp. 221-234. https://doi.org/10.1007/978-981-99-3716-5_20
[73] Pal, K., Gulati, P. (2025). Legality of ethical hacking in data mining and enhancing information security. In Innovations in Data Analytics, pp. 457-467. https://doi.org/10.1007/978-981-96-6297-5_35
[74] Arsat, N., Daoud, H.I., Zainol, Z., Kumar, G. (2025). The role and impact of ethical hacking in modern society's

economy. In Proceedings of 4th International Conference on Mathematical Modeling and Computational Science, pp. 310-326. https://doi.org/10.1007/978-3-031-91008-1_29

[75] Guseva, I., Pliva, E. (2024). The conceptual content of cybersecurity ecosystems: A professional language perspective. In Ecosystems Without Borders 2024, pp. 208-214. https://doi.org/10.1007/978-3-031-67354-2_22

[76] Pasricha, S., Wolf, M. (2024). Ethical design of computers: From semiconductors to IoT and artificial intelligence. IEEE Design & Test, 41(1): 7-16. https://doi.org/10.1109/MDAT.2023.3277815

[77] Das, N., Gupta, D., Chaudhary, I., Fulmali, R., Kishore, S., Sandeep, V. (2023). Understanding cyber terrorism with a special focus on zero-day attacks. In Recent Advancements in Computational Finance and Business Analytics, pp. 621-628. https://doi.org/10.1007/978-3-031-38074-7_53

[78] Friedl, S., Zajewski, C., Pernul, G. (2024). Sustainability in digital forensics. In Proceedings of the 19th International Conference on Availability, Reliability and Security, New York, NY, USA, pp. 1-9. https://doi.org/10.1145/3664476.3670894

[79] Schmeelk, S.E., Dragos, D.M. (2023). Penetration testing and ethical hacking: Risk assessments and student learning. In 2023 IEEE Frontiers in Education Conference (FIE), College Station, TX, USA, pp. 1-6. https://doi.org/10.1109/FIE58773.2023.10342914

[80] Bhatia, S., Elhadad, S., Deshmukh, A., Yellela, M.K., Vangala, O.S.R. (2023). Hack the problem: A problem-based learning approach for ethical hacking and network defense curriculum. In Proceedings of the 54th ACM Technical Symposium on Computer Science Education V.2, New York, NY, USA, pp. 1346-1346. https://doi.org/10.1145/3545947.3576292

[81] Bhatia, S., Elhadad, S., Ahmed, I. (2024). PATCH: Problem-based learning approach for teaching cybersecurity and ethical hacking in community colleges. In 2024 17th International Conference on Security of Information and Networks (SIN), Sydney, Australia, pp. 1-9. https://doi.org/10.1109/SIN63213.2024.10871628

[82] Samrouth, K., Nassar, M., Harb, H. (2023). Revisiting attack trees for modeling machine pwning in training environments. In 2023 3rd Intelligent Cybersecurity Conference (ICSC), San Antonio, TX, USA, pp. 46-53. https://doi.org/10.1109/ICSC60084.2023.10349984

[83] Alsmadi, I. (2023). Threat analysis. In The NICE Cyber Security Framework, pp. 373-380. https://doi.org/10.1007/978-3-031-21651-0_17

[84] Udofia, E. (2025). A Human-Centric Approach to Cyber Risk Mitigation., Boca Raton, FL, CRC Press, pp. 241-259. https://www.taylorfrancis.com/chapters/edit/10.1201/9781032714806-17/human-centric-approach-cyber-risk-mitigation-ediomo-udofia.

[85] Stoddart, K. (2022). Hacking the human. In Cyberwarfare, pp. 281-349. https://doi.org/10.1007/978-3-030-97299-8_5

[86] Beuran, R. (2025). Attack training. In Cybersecurity Education and Training, pp. 41-72. https://doi.org/10.1007/978-981-96-0555-2_4

[87] Altulaihan, E., Almaiah, M.A., Aljughaiman, A. (2022). Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions. Electronics, 11(20): 3330. https://doi.org/10.3390/electronics11203330