

Ethical Hacking for Cloud Security: A Comprehensive Review of Methodologies, Tools, Legal Frameworks, Bug-Bounty Ecosystems, and AI-Assisted Penetration Testing

Ananya Sunil Mengade, Prof. Bangar Abhishek Popat, Prof. Bhosale S.B.

Dept. of Computer Engineering
Jaihind College of engineering, Pune, India

Abstract- Organisations now run critical services on networks, web applications and cloud platforms that attackers probe continuously. Ethical hacking, the authorised use of attacker techniques to find weaknesses before criminals do, has become a standard part of cyber security practice. This paper presents a focused narrative review of verified sources on ethical hacking for cyber security. It examines four connected themes: the foundations and legal basis of ethical hacking, the testing methodologies and frameworks that structure an engagement, the tools and attack surfaces involved, and newer developments in bug-bounty programmes and large-language-model (LLM) assisted penetration testing. The literature shows that ethical hacking is distinguished from malicious hacking mainly by authorisation and scope, that established guidance such as NIST SP 800-115 organises testing into planning, discovery, attack and reporting, and that reward programmes can be an effective way to obtain vulnerability reports. Early studies suggest LLMs can assist some penetration-testing tasks, but they remain limited and need human supervision. Most sources, however, are descriptive or guidance documents; few report controlled comparisons of methods, and evidence on testing for Indian organisations is sparse. The review contributes a comparative analysis of representative sources, a proposed conceptual seven-layer governance-first engagement framework, and a prioritised list of research gaps.

Keywords— Ethical Hacking, Penetration Testing, Cyber Security, Vulnerability Assessment, Bug Bounty, Large Language Models

I. INTRODUCTION

Modern organisations depend on interconnected networks, web applications, mobile apps and cloud services. Each of these exposes an attack surface, and weaknesses are found by criminals as readily as by defenders. Ethical hacking addresses this by applying the knowledge and tools of attackers, with the owner's permission, to locate and report vulnerabilities so that they can be fixed first [1], [15]. Penetration testing, a closely related activity, simulates an attack against a defined target to judge how well it resists [2], [7].

Ethical hacking is not a complete answer to security. Testing can show that a flaw exists but cannot prove that none remain [2], and results depend on the skill of the tester and the scope agreed. It also raises legal

and professional questions, because the same actions are criminal offences when carried out without permission [13]. A review is therefore useful to bring together what the technical, legal and empirical literature says about how ethical hacking should be done and how well it works. This review examines four strands together: (i) foundations, definitions and legal basis, (ii) methodologies and frameworks, (iii) tools and attack surfaces, and (iv) bug-bounty programmes and AI-assisted testing. It asks how mature the evidence is and proposes a conceptual engagement framework that addresses the weaknesses identified.

II. REVIEW METHODOLOGY

This is a focused narrative review, not a systematic one. The evidence base was built from four groups

of sources: foundational papers on ethical hacking and penetration testing [1], [2], [7], [8], [15]; standards and guidance documents from NIST, ISECOM and OWASP [3], [6], [14]; threat-modelling frameworks, namely the intrusion kill chain and MITRE ATT&CK [4], [5]; and empirical or experimental studies of vulnerability reward programmes and LLM-assisted testing [9]–[12]. The Information Technology Act, 2000 [13] is included for the Indian legal context. No separate database search was run for this version, no study counts are claimed, and findings of the sources are reported as the authors describe them. Grey literature such as vendor reports and practitioner blogs was not reviewed, and this is stated as a limitation in Section IX.

III. FOUNDATIONS AND LEGAL BASIS

1. Definition and Types of Hackers

Palmer describes ethical hacking as an organisation employing skilled people to attempt to penetrate its own systems in the way an intruder would, in order to improve security [1]. Practitioners commonly group hackers by intent and authorisation. White-hat hackers work with permission to improve security; black-hat hackers act without permission for personal gain or harm; grey-hat hackers act without permission but without clearly malicious aims. The label depends less on the techniques used, which are largely the same, and more on authorisation, scope and intent [1], [15].

2. Legal and Ethical Boundaries

Authorisation is the central safeguard. Written permission, a defined scope, agreed testing windows and rules of engagement protect both the client and the tester [3], [14]. In India, unauthorised access to computer systems and related acts can attract liability under provisions of the Information Technology Act, 2000, including Sections 43 and 66 [13]. Testers should therefore confirm that the systems in scope belong to, or are controlled by, the party granting permission, and should handle any data they encounter with confidentiality. Professional ethics further require responsible reporting of findings and avoidance of unnecessary damage.

3. Types of Penetration Testing

Engagements are usually described by how much the tester knows in advance. In black-box testing the tester has no prior knowledge of the target and works as an external attacker would; in white-box testing the tester is given architecture details, source code or credentials, which allows deeper coverage in less time; and grey-box testing sits between the two [7], [15]. Engagements are also classed by target: network, web application, wireless, mobile, cloud, social engineering and, where agreed, physical access. The choice depends on the objectives, budget and risk appetite of the client.

IV. METHODOLOGIES AND FRAMEWORKS

1. Phase-Based Testing Guidance

NIST SP 800-115 gives technical guidance on planning and conducting security testing and describes penetration testing in four phases: planning, discovery, attack and reporting [3]. In the discovery phase the tester gathers information and identifies hosts, services and potential vulnerabilities; in the attack phase these are validated, and attacks may be chained to gain deeper access; the reporting phase documents findings and mitigation advice. Many practitioner descriptions use a longer list, typically reconnaissance, scanning, gaining access, maintaining access and covering tracks [15], although the last step is performed in a controlled way, or omitted, during authorised work.

2. Threat-Informed Frameworks

The intrusion kill chain models an attack as a sequence of stages, which lets defenders analyse and disrupt an adversary campaign at several points [4]. MITRE ATT&CK catalogues adversary tactics and techniques from observed behaviour and provides a common vocabulary for mapping test activities and findings [5]. Using such frameworks allows an ethical hacking report to state which real-world techniques were emulated and which defensive controls detected or stopped them.

3. Open Standards and Web Guidance

The Open Source Security Testing Methodology Manual (OSSTMM) provides a repeatable,

measurable approach to security testing [14]. For web applications, the OWASP Top 10 lists the most critical risk categories, such as broken access control, injection and security misconfiguration, and is widely used to organise web testing and training [6].

V. TOOLS, TECHNIQUES AND ATTACK SURFACES

Ethical hacking uses both general-purpose and specialised tools. Commonly described examples include Nmap for host and port discovery, Wireshark

for packet analysis, Nessus or OpenVAS for vulnerability scanning, Burp Suite for web application testing, Metasploit for exploit development and delivery, and password-auditing tools such as John the Ripper and Hydra; the Kali Linux distribution bundles many of them [7], [15]. Vulnerability assessment, which identifies and ranks weaknesses, and penetration testing, which attempts to exploit them, are complementary: assessment gives breadth while testing gives evidence of real impact [7].

Table 1: Comparison of Representative Sources Relevant to Ethical Hacking for Cyber Security

Author, year	Objective	Method / type	Major reported findings	Limitations
Palmer, 2001 [1]	Define ethical hacking	Descriptive account of an organisational ethical-hacking approach	Frames ethical hacking as authorised intrusion testing to improve security	Early paper; no controlled evaluation
Bishop, 2007 [2]	Explain what penetration testing can show	Conceptual discussion	Testing shows presence of flaws, not their absence; best used with other assessment	Not an empirical study
NIST, 2008 [3]	Guide security testing	Official technical guidance	Four phases: planning, discovery, attack, reporting	Guidance, not an evaluation; pre-dates cloud-era tools
Shah & Mehtre, 2015 [7]	Overview of VA and PT	Literature overview of techniques and tools	Separates vulnerability assessment from penetration testing; compares tool types	Overview; no new experiments
Bertoglio & Zorzo, 2017 [8]	Survey penetration-test process	Literature overview	Summarises approaches and open issues in the process	Narrative scope; coverage of recent work limited
Finifter et al., 2013 [9]	Study vulnerability reward programmes	Empirical analysis of browser vendors' programmes	Reward programmes can be an effective source of vulnerability reports	Two vendors; programmes have since evolved
Zhao et al., 2015 [10]	Study vulnerability discovery ecosystems	Empirical analysis of bug-bounty platforms	Treats bug-bounty platforms as discovery ecosystems and analyses participation	Web vulnerabilities only; older data
Happe & Cito, 2023 [11]	Test LLMs for penetration testing	Prototype using LLMs on a Linux privilege-escalation scenario	LLMs can suggest useful attack steps in a limited setting	Narrow scenario; human oversight needed

Deng et al., 2023 [12]	Automate penetration testing with LLMs	PentestGPT tool evaluated on benchmark tasks	Reported better task completion than a plain LLM baseline	Benchmark tasks; not full real-world engagements
------------------------------	--	--	---	--

Reported values are not directly comparable because purposes, datasets and designs differ. Study details are as reported by the cited sources.

Typical attack surfaces include network services, web applications and APIs, wireless networks, mobile and cloud configurations, and the human element through social engineering assessments. Overview studies note that automated tools produce false positives and miss logic flaws, so manual verification by a skilled tester remains necessary [7], [8].

VI. FINDINGS, BUG BOUNTIES AND AI-ASSISTED TESTING

1. Common Vulnerabilities and Attack Types

Ethical hackers look for weaknesses that attackers exploit most often. For web applications these include injection flaws such as SQL injection, cross-site scripting, broken authentication and access control, and security misconfiguration [6]. At network and system level, typical findings are unpatched software, default or weak passwords, exposed services and poorly segmented networks. Social engineering, particularly phishing, targets people rather than software and is often tested through authorised awareness exercises [15]. Mapping each finding to a recognised category helps clients compare results between tests.

2. Bug-Bounty Programmes

Bug-bounty programmes invite outside researchers to report vulnerabilities in return for recognition or payment. Finifter et al. studied the vulnerability reward programmes of two browser vendors and found that such programmes can be an effective way to obtain vulnerability reports [9]. Zhao et al. analysed bugbounty platforms as vulnerability discovery ecosystems and examined how researchers participate [10]. These programmes widen the pool of testers beyond a single team, but they depend on clear scope, safe-harbour rules and timely triage by the organisation.

3. LLM-Assisted Penetration Testing

Recent work explores whether large language models can help with penetration testing. Happe and Cito used LLMs in a Linux privilege-escalation setting and showed they can propose useful steps, while noting limits [11]. PentestGPT divides a test into sub-tasks handled by cooperating LLM modules and reported better task completion than a plain LLM on benchmark tasks [12]. These results are early and use constrained scenarios. LLM-generated commands can be wrong, may drift out of scope, and could be misused, so any such tool must run under authorisation, logging and human review.

4. Responsible Disclosure

When a researcher finds a vulnerability outside a formal contract, the accepted practice is to report it privately to the owner or vendor and allow reasonable time for a fix before any public discussion. Bug-bounty programmes usually publish a policy that states the scope, the permitted techniques and how reports are handled, and this policy is what separates a protected report from an unauthorised intrusion [9], [10], [13].

5. Skills, Certification and Training

Ethical hacking calls for knowledge of networking, operating systems, programming and security concepts, together with a disciplined, documented way of working. Learners commonly build skills in isolated lab environments and capture-the-flag exercises, and employers often look for certifications such as CEH, OSCP or CompTIA PenTest+. Whatever the route, training should include the legal and ethical limits of testing, since these are what make the work professional rather than criminal [1], [13].

VII. COMPARATIVE ANALYSIS

Table I summarises representative sources. The foundational and guidance sources [1]–[3], [7], [8] establish what ethical hacking is and how it is organised, the empirical sources [9], [10] examine

reward programmes, and the LLM studies [11], [12] explore automation. Most sources describe or recommend practice rather than compare methods under controlled conditions, and no row measures how engagements should be scoped and reported for Indian small and medium organisations. This defines the main gap addressed in Sections VIII and IX.

Taken together, the sources describe clear benefits: ethical hacking finds exploitable weaknesses before attackers do, shows the real impact of a flaw rather than a theoretical score, helps prioritise remediation, and supports compliance and customer trust [3], [7].

Its limits are equally clear. Results are a snapshot in time, depend on the tester's skill and agreed scope, can miss flaws, and carry operational risk if a test disrupts a live system [2], [8]. Regular retesting and combining testing with secure development and monitoring are therefore recommended.

VIII. PROPOSED CONCEPTUAL FRAMEWORK

Fig. 1 presents a proposed conceptual seven-layer engagement framework derived from the reviewed sources; it is conceptual and has not been experimentally validated.

Authorisation and scoping come first and are treated as a layer in their own right (layer 1) because legal protection depends on them [3], [13], [14]. Reconnaissance and scanning follow (layers 2 and 3), consistent with the discovery phase of [3]. Findings are validated and exploited only within scope (layer 4), and impact and evidence are recorded (layer 5).

Reporting maps each finding to OWASP categories and ATT&CK techniques with remediation advice (layer 6) [5], [6]. Retesting verifies fixes (layer 7), and lessons feed back into scoping only after independent review, keeping a human in control, including whenever LLM tools are used [11], [12].

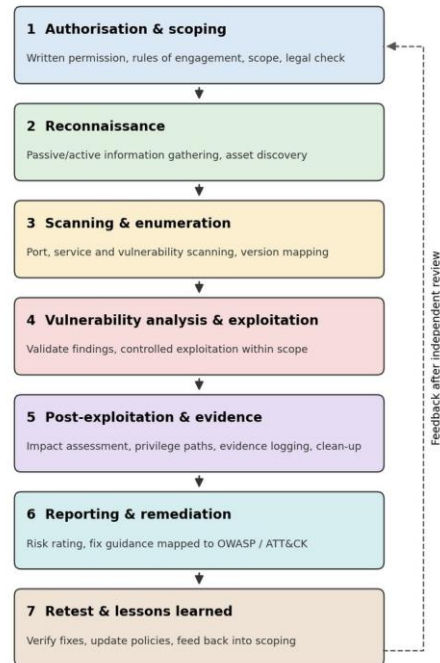


Fig. 1. Proposed conceptual framework for an ethical hacking engagement (conceptual, not experimentally validated).

IX. RESEARCH GAPS AND FUTURE DIRECTIONS

Gaps supported by the reviewed evidence. (i) Little controlled comparison: guidance documents and overviews dominate, and few studies compare methodologies or tools under controlled conditions [3], [7], [8]. (ii) Limited evidence on effectiveness: testing shows flaws, not their absence, and measures of how much risk testing actually reduces are scarce [2]. (iii) Reward-programme studies are limited to specific vendors or platforms and older data [9], [10]. (iv) LLM-assisted testing is evaluated mainly on narrow scenarios and benchmarks [11], [12]. (v) Indian context: legal guidance for testers is available [13], but empirical studies of engagements in Indian organisations were not found in this review. (vi) Limited coverage: grey literature, cloud, IoT and mobile testing were not searched systematically.

Directions requiring investigation. Priorities include controlled studies comparing manual, automated and LLM-assisted testing on the same targets; metrics

for finding quality, false positives and coverage; benchmark environments for training and evaluation; safe-harbour and disclosure practice for researchers in India; guardrails that keep AI tools within scope; and education studies that measure skill gain in ethical hacking courses rather than perceptions alone.

X. CONCLUSION

Ethical hacking combines mature building blocks: authorised scoping, phase-based methodologies, threat-informed frameworks such as ATT&CK, widely used tools, and community programmes such as bug bounties. The literature agrees that authorisation and scope separate ethical hacking from crime, and that testing is most useful as part of a wider assessment. However, the evidence base is dominated by guidance and descriptive overviews, early studies of LLM assistance are narrow, and Indian empirical evidence is thin. A governance-first, seven-layer engagement framework with independent review, as outlined here, is a reasonable design direction, but it requires empirical validation in real engagements.

REFERENCES

1. C. C. Palmer, "Ethical hacking," IBM Syst. J., vol. 40, no. 3, pp. 769–780, 2001.
2. M. Bishop, "About penetration testing," IEEE Secur. Privacy, vol. 5, no. 6, pp. 84–87, Nov./Dec. 2007.
3. K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical guide to information security testing and assessment," NIST Special Publication 800-115, 2008.
4. E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in Proc. 6th Int. Conf. Inf. Warfare Secur., 2011, pp. 113–125.
5. B. E. Strom et al., "MITRE ATT&CK: Design and philosophy," The MITRE Corporation, Tech. Rep., 2018.
6. OWASP Foundation, "OWASP Top 10: 2021," Open Worldwide Application Security Project.
7. S. Shah and B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," J. Comput. Virol. Hacking Tech., vol. 11, no. 1, pp. 27–49, 2015.
8. A. Bertoglio and A. F. Zorzo, "Overview and open issues on penetration test," J. Braz. Comput. Soc., vol. 23, art. 2, 2017.
9. M. Finifter, D. Akhawe, and D. Wagner, "An empirical study of vulnerability rewards programs," in Proc. 22nd USENIX Security Symp., 2013, pp. 273–288.
10. M. Zhao, J. Grossklags, and P. Liu, "An empirical study of web vulnerability discovery ecosystems," in Proc. ACM Conf. Comput. Commun. Secur. (CCS), 2015, pp. 1105–1117.
11. A. Happe and J. Cito, "Getting pwn'd by AI: Penetration testing with large language models," in Proc. ESEC/FSE, 2023, pp. 2082–2086.
12. G. Deng et al., "PentestGPT: An LLM-empowered automatic penetration testing tool," 2023, arXiv:2308.06782.
13. Government of India, "The Information Technology Act, 2000," as amended.
14. P. Herzog, "OSSTMM 3: The Open Source Security Testing Methodology Manual," ISECOM, 2010.
15. P. Engebretson, The Basics of Hacking and Penetration Testing, 2nd ed. Waltham, MA, USA: Syngress, 2013.