International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 423-430 www.ijaem.net ISSN: 2395-5252

Evaluating the Role of Open-Source Tools in Enhancing Cybersecurity Training for Ethical Hackers

Areeza Shahirah Mohamad Safari, Mohamad Fadli Zolkipli
Student, Cybersecurity, School of Computing, Universiti Utara Malaysia, Sintok, Malaysia Lecturer, School of Computing, Universiti Utara Malaysia, Sintok, Malaysia.

Date of Submission: 20-06-2025 Date of Acceptance: 30-06-2025

ABSTRACT: The increasing sophistication of cyber threats has intensified for demand for well-trained ethical hackers capable of defending digital infrastructure. This study evaluates the role of open-source tools in enhancing cybersecurity training, with particular focus on widely adopted platforms such as Kali Linux, Wireshark, Metasploit, Nmap and OpenVAS. These tools offer cost effective, accessible, and realistic environments for learners to gain hands-on experience in penetration testing, network analysis, and threat simulation. The research explores their integration within academic curricula and professional training programs, analyzing how they facilitate experiential learning and bridge the gap between theoretical knowledge and practical skills. Through a combination of case studies, surveys, and performance assessments from multiple institutions, the study demonstrates that the strategic use of open-source tools significantly improves learner engagement, technical proficiency, and readiness for real-world cybersecurity challenges. The paper concludes by recommending best practices for incorporating these tools into structured training programs, thereby contributing to a more resilient and capable cybersecurity workforce.

KEYWORDS: Cybersecurity Training, Ethical Hacking, Kali Linux, Wireshark, Metasploit

I. INTRODUCTION

In the rapidly evolving field of cybersecurity, the demand for skilled ethical hackers has intensified, necessitating robust and practical training methodologies. Open-source tools such as Kali Linux, Wireshark, Nmap, and OpenVAS have become integral to cybersecurity education, offering hands-on experience in penetration testing, network analysis, and vulnerability assessment. These tools provide learners with real-world scenarios to develop and refine their skills, bridging the gap between theoretical knowledge and practical application.

Kali Linux, a Debian-based distribution, is renowned for its comprehensive suite of penetration testing tools. It encompasses utilities for tasks ranging from information gathering to exploitation, facilitating a holistic approach to security assessments (Akhtar & Rawol, 2024). Its widespread adoption in academic settings underscores its effectiveness in providing students with a versatile platform for exploring various cybersecurity techniques.

Wireshark, a network protocol analyzer, enables users to capture and inspect data by traversing a network in real-time (Akhtar & Rawol, 2024). This capability is crucial for understanding network behaviours, diagnosing issues, and detecting malicious activities. Incorporating Wireshark into training programs enhances students' proficiency in network analysis and reinforces concepts related to network security.

Nmap, or Network Mapper, is a powerful tool for network discovery and security auditing. It allows users to identify active devices, services, and potential vulnerabilities within a network. By utilizing Nmap in educational environments, learners gain practical insights into network reconnaissance and the methodologies employed by both attackers and defenders.

OpenVAS, an open-source vulnerability scanner, provides a framework for assessing and managing security vulnerabilities in systems and applications. Its integration into cybersecurity curricula enables students to conduct comprehensive vulnerability assessments, prioritize risks, and recommend mitigation strategies.

The integration of these open-source tools into cybersecurity training programs has been the subject of various studies. For instance, research has demonstrated the effectiveness of simulation

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 423-430 www.ijaem.net ISSN: 2395-5252

environments incorporating tools like Kali Linux in enhancing practical skills among students. These environments offer scalable and flexible platforms that replicate real world scenarios, thereby improving the quality of training.

Furthermore, the development of toolsets for collecting and analyzing command-line inputs during practical tasks has provided valuable insights into student progress and common pitfalls. Such tools facilitate real-time feedback and tailored instruction, contributing to more effective learning outcome (Svabensky et al., 2021).

In summary, the incorporation of open-source tools like Kali Linux, Wireshark, Nmap, OpenVAS, and Metasploit into academic and training environments plays a pivotal role in cultivating competent ethical hackers. These tools not only provide practical experience but also foster a deeper understanding of cybersecurity principles, ultimately contributing to the development of a skilled and proactive cybersecurity workforce.

II. LITERATURE REVIEW / BACKGROUND

In contemporary cybersecurity education, open- source tools play a pivotal role in enabling cost- effective, scalable and hands-on environments for ethical hackers. These tools facilitate realistic emulation of attack-defense scenarios that are crucial for practical learning and skill development.

There are surveyed a range of open-source threat emulators aligned with MITRE ATT&CK techniques (Zilberman et al., 2020). Their work provided a structures evaluation of capabilities such as attack automation, cleanup and usability – laying the groundwork for selecting suitable tools for training scenarios. A comparative analysis of nine open-source adversary emulation tools, using a detailed 80-question framework and expert feedback (Landauer et al., 2024). They identified MITRE Caldera, Metasploit, and Atomic Red Team as top performers in usability and effectiveness in training realistic red-team exercises.

(Al., 2024) describe a scalable simulation environment built on open-source components (Kali Linux, Security Onion, etc.) deployed via KVM hypervisor clusters—demonstrating immersive, repeatable, and low-cost training scenarios. (Vykopal et al., 2021) introduced the KYPO Cyber Range Platform, a fully open-source system supporting multi-user, realistic labs with Windows/Linux VMs. Their evaluation highlighted increased engagement, smooth deployment and valuable instructor and learner feedback.

(Yi et al., 2024) explored alignment between cyber range scenario design and learning objectives. Their workshop study emphasized scenario interactivity, relevance and student-level tailoring to improve learning outcomes. (Katsantonis & Mavridis, 2021) presented a design framework for cyber ranges emphasizing architecture, life-cycle planning, and automation using open-source SIEM tools (e.g., OSSIM), highlighting how thoughtful design enables feedback-driven experiences.

Collective evidence shows the educational value of open-source-based training hands-on, simulated environments (KYPO, CyTrONE, KVM-based labs) enhance learner engagement, retention, and skill acquisition (Vykopal et al., 2021). Tools with structured feedback (e.g., SIEM-integrated scoring) support reflective learning, enabling instructors to offer tailored guidance and adjust future exercises. Open-source toolsets reduce barriers to access, allowing institutions and learners with limited budgets to replicate large-scale, frequent training.

Despite clear benefits, several obstacles persist is **Steep Configuration Curves**: The complexity of open-source platforms requires significant technical expertise, potentially limiting adoption among newcomers. **Fragmented Standards**: There is no universal standard taxonomy or instructional design model; survey by (Zilberman et al., 2020) and (Katsantonis & Mavridis, 2021) highlight inconsistencies between tools and educational goals. **Empirical Evidence Gaps**: while platforms are available, few studies link their use to specific, measurable learning outcomes such as improvement in real-world ethical hacking performance.

Open-source tools—ranging from adversary emulators to full cyber ranges—form a vibrant ecosystem for cybersecurity training. They provide immersive, cost-effective and scalable environments ideal for ethical hackers. However, challenges like complexity, lack of standardization and limited empirical evaluation remain. This literature review underscored the need for your study: a focused evaluation of how open-source tools concretely enhance ethical hacker's training effectiveness, fortified with measurable outcomes and pedagogical rigor.

III. ANALYSIS OF KEY OPEN-SOURCE TOOLS

Kali is a Debian-based distro bundling -600 security tools (e.g., Nmap, Wireshark, Aircrack-ng) with optimized packages and frequent updates. (Akhtar & Rawol, 2024) outlines an investigative pen testing methodology using Kali for Wi-Fi security: preparation, scanning, attack simulation,

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 423-430 www.ijaem.net ISSN: 2395-5252

and reporting—demonstrating how Kali structures hands-on learning phases. (Vykopal et al., 2021) used Kali-integrated CLI environments like KYPO cyber ranges. Participants began with Nmap scans, then conducted scripted attacks and received automated analytics feedback—revealing elevated learning outcomes through structured pipelines. Kali standardizes tool access and supports pedagogy by embedding scanning, exploitation, and analytics within a single live lab environment.

Wireshark is a GPL-licensed packet sniffer supporting high-detailed protocol parsing across platforms. While a few formal studies focus solely on Wireshark, it is woven into Kali training. (Akhtar & Rawol, 2024) used Wireshark to analyse Wi-Fi cracks; (Svabensky et al., 2021) training methods capture network events for feedback modules. Wireshark empowers students to inspect packet-level behaviour vital for protocol troubleshooting and identifying covert network activities.

Nmap excels at host discovery, service/version detection, OS fingerprinting, and extensibility via NSE scripts. In (Akhtar & Rawol, 2024) includes Nmap in Kali-based Wi-Fi testing pipelines and (Svabensky et al., 2021) structured training experiences that began with Nmap scans before moving into deeper exploitation, feeding data into analytics. Nmap introduces students to network foot printing essentials first-step reconnaissance that informs subsequent attack planning.

OpenVAS (now Greenbone Vulnerability Manager) offers 50,000+ network test, support authenticated scans, scripting, and distributed deployment. Hands-on courses (e.g., Udemy 2024) train learners on setting up OpenVAS in Kali executing scans, generating reports, and managing vulnerabilities. Following initial Nmap/NSE reconnaissance, trainees to vulnerabilities scanning phases. This fosters a realistic, stepwise penetration testing workflow. OpenVAS introduces structured assessment and post-scan reporting vital for cultivating comprehensive vulnerability management skills. (Vykopal et al., 2021) demonstrated effective command/log analytics that reveal patterns, errors, and proficiency gaps, adding reflective layers to training. The open-source stack enables iterative labs, lowers cost barriers, and supports repeatable, scalable exercises for diverse learner cohorts (Svabensky et al., 2021).

Table 1. The stage and impact of open-source tools

STAGE	TOOL	IMPACT
Reconnaissance	Nmap	Initialmappingof networks and services
Packet Analysis	Wireshark	Trafficinspection and anomaly detection
Penetration	Kali Linux	Centralenvironment with modular tools
Vulnerability Management	OpenVAS	Structured scanning and reporting
Feedback & Analytics	Log capture tools	Performance insight and tailored instruction

Together, they simulate realistic ethical hacking workflows, reinforce core skills, and provide data- driven insights for instructors. Future research should assess how this integrated pipeline enhances measurable outcomes like exploit success rates or remediation accuracy.

IV. BENEFITS OF OPEN-SOURCE TOOLS IN TRAINING

Open-source tools are freely available, eliminating licensing costs and enabling institutions to deploy realistic labs at scale without financial barriers. Research by (Vykopal et al., 2021) shows that platforms like the KYPO cyber range (incorporating Kali) can be deployed on clusters of open-source hypervisors, supporting large student cohorts efficiently. Kali Linux bundles hundreds of tools such as Nmap and Wireshark offering a unified, ready-made penetration testing environment. This all-in-one integration simplifies training design and ensures consistency across labs and assignments.

Simulation-based environments using open-source stacks (e.g., Kali, pfSense, Security Onion) mimic real-world network scenarios, enhancing experiential learning (Al., 2024). Students follow authentic workflows: network mapping (Nmap) – packet analysis (Wireshark) – exploitation (Kali tools) – vulnerability scanning (OpenVAS), creating continuity and contextual learning.

Wireshark enables packet-level inspection and protocol analysis, fostering a detailed understanding of network behaviour and anomalies crucial for forensic and security analysis. This granular insight supports debugging, anomaly detection, and reinforces theoretical concepts taught in class.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 7, Issue 06 June 2025, pp: 423-430 www.ijaem.net ISSN: 2395-5252

Open-source cyber ranges support remote, multi-user deployments with rapid provisioning and teardown, enhancing course flexibility and scalability (Vykopal et al., 2021). Automated shell and log collection systems integrated with these tools enable uniform feedback across cohorts (Svabensky et al., 2021).

Tools like Nmap and OpenVAS feature active communities, frequent updates, and extensible plugin/script architecture, ensuring evolution alongside emerging threats. Their open nature invites students to explore, customize and even contribute enhancing engagement and ownership of learning.

Adopting a toolchain that mirrors industry-standard practices ensures graduates are prepared for real-world tasks from reconnaissance (Nmap) to scanning (OpenVAS), analysis (Wireshark) and exploitation/reporting (Kali) (Svabensky et al., 2021). Infrastructure mimicking production environments builds confidence and readiness among trainers. Studies on shell-command recorders show that capturing user actions across tools like Kali enables instructors to analyse, identify misconceptions, and adapt exercises in near-real time (Svabensky et al., 2021). Combined with integrated SIEM and log-capture systems, training becomes more reflective and targeted.

V. CHALLENGES AND LIMITATIONS

Tools often demand advances configuration and deep understanding of networking and system internal. Setting up environments like Klai, KVM-based cyber ranges, or logging infrastructure requires skilled administrators raising the barrier to entry (Svabensky et al., 2021). Even with pre-configured labs, trainees must comprehend core OS/network concepts before they can effectively deploy and integrate multiple tools.

Tools such as Wireshark and Nmap provide raw protocol/packet-level data, requiring significant expertise to interpret correctly. Misinterpretation can lead to incorrect conclusions or misconfigured experiments. OpenVAS can also overwhelm beginners with false positives or complex report outputs that lacks clarity without foundational context (Alhamed & Rahman, 2023).

Vulnerability scanners lie OpenVAS may produce frequent false positives, which can mislead trainees and require manual validation a time-consuming process that disrupts training flow. Network scanners like Nmap may miss hosts or misinterpret open ports due to firewall rules, network segmentation, or aggressive scan settings.

Setting up and maintaining cyber ranges, multiple VMs, and tools like OpenVAS consume significant computing resources (CPU, memory, storage), which may limit scalability in resource-constrained institutions (Al., 2024). Continuous updates of tool databases (e.g., OpenVAS NVTs, Wireshark protocol definitions) require network bandwidth and administrative oversight.

Training programs often rely on ad-hoc selection and sequence of tools leading to inconsistencies in learning outcomes (Svabensky et al., 2021). There is limited consensus on

pedagogical framework for blending tool instruction with conceptual topics; few integrated models exist. Through command-logging infrastructure capture tool usage, few studies quantitatively link tool interaction with specific learner gains like exploit success or remediation accuracy. The gap between technical tool use and measurable cybersecurity competencies remains underexplored.

Open-source tools frequently update versions or deprecate features, requiring trainers to keep labs current and consistent. Outdated tools may break exercises or introduce unplanned variability. Divergent versions across student deployments can obscure common issues and complicate troubleshooting.

While open-source tools are indispensable for interactive ethical hacking training, they bring significant challenges in setup, interpretation, maintenance, and instructional consistency. Addressing these limitations requires modular, scaffolded labs that guide learners through tool use progressively. Analytic logging systems to evaluate real learning gains. Robust instructional framework that aligns tool workflows with curriculum goals. Resource planning to support scalable deployment and regular updates. Design solutions that thoughtfully integrate these tools into pedagogically sound environments will foster more effective and measurable cybersecurity training outcomes.

IV. DISCUSSION

Wireshark is a widely utilized open-source network protocol analyzer that plays a significant role in cybersecurity training for ethical hackers within academic and training environments (Hashim et al., 2023). Its capabilities allow for the detailed inspection of network traffic, aiding in the identification of vulnerabilities and the understanding of network behaviours (Chaubey, 2024).

In cybersecurity education, hands-on training is crucial for comprehending theoretical concepts and enhancing practical skills. Wireshark facilitates this by enabling students to capture and analyse real-time network traffic, thereby providing

insights into various protocols and potential security issues (Mabsali et al., 2023). For instance, a study demonstrated the use of Wireshark in analyzing network protocols, allowing students to log and scrutinize all packets traversing a network, which is instrumental in identifying system vulnerabilities (Jaya et al., 2022).

Furthermore, Wireshark's application extends to the detection and analysis of malicious activities within a network (Ibraheem & Kayode, 2024). Research has shown that Wireshark can be employed to monitor network traffic for signs of unauthorized access or data breaches (Soepeno, 2023). By analyzing captured packets, students can learn to identify indicators of compromise and understand the methodologies employed by attackers (Guaki, 2024).

The tool's versatility is also evident in its integration with other cybersecurity tools and platforms. For example, in penetration testing scenarios, Wireshark can be used alongside tools like Nmap to enhance the assessment of network security. This combination allows students to perform comprehensive network scans and analyse the resulting traffic, thereby gaining a holistic understanding of network defense mechanisms.

Moreover, Wireshark's role in cybersecurity training is not limited to traditional network environments. With the advent of technologies like 5G, Wireshark has been incorporated into training frameworks to address new security challenges. For instance, the Cyber5Gym framework integrates Wireshark to provide practical training in 5G cybersecurity, highlighting its adaptability to emerging technologies (Hamza et al., 2024). In summary, Wireshark serves as an essential tool in the arsenal of ethical hackers and cybersecurity professionals in training. Its open-source nature, coupled with its robust analytical capabilities, makes it an invaluable resource for practical, hands-on learning in academic and training settings.

Nmap (Network Mapper) is a widely used open-source tool that plays a crucial role in cybersecurity training, particularly for ethical hackers in academic and training environments (Sulisnawati, 2023). Its comprehensive features support various aspects of network security education, enhancing both theoretical understanding and practical skills. Nmap serves as a foundational tool in cybersecurity curricula, offering functionalities essential for network reconnaissance and security auditing. Its capabilities include host discovery, port scanning, service version detection, and operating system fingerprinting. These features enable students to gain hands-on experience in identifying active services and potential vulnerabilities within networks. The tool's versatility allows educators to design realistic scenarios that reflect contemporary cybersecurity challenges (Pappala, 2025).

The integration of Nmap into academic settings has been documented in various studies. For instance, (Vykopal et al., 2021) discuss the use of scalable learning environments that incorporate Nmap to teach hands-on cybersecurity classes. These environments provide virtual networks with full-fledged operating systems, allowing students to practice real-world scenarios effectively. The study highlights that such practical engagements significantly enhance learners' skills and preparedness for actual cybersecurity tasks. In evaluating the efficacy of port scanning tools, (Pittman, 2023) conducted a comparative analysis of Nmap, Zmap, and Masscan. The study measured accuracy, false positives, false negatives, and efficiency, revealing no significant differences in general performance among the tools. However, it noted a statistically significant difference in efficiency, suggesting that tool selection should be guided by specific requirements and context (Pappala, 2025).

The evolution of ethical hacking techniques has further underscored the importance of tools like Nmap. A study on advancements in ethical hacking highlights Nmap's role in port scanning, a critical component of network reconnaissance (InteliPaat, 2022). The research emphasizes that ethical hackers utilize Nmap to map network topologies, identify active services, and detect potential vulnerabilities, thereby strengthening cybersecurity resilience. Incorporating Nmap into cybersecurity training programs provides students with essential skills in network analysis and vulnerability assessment. Its open-source nature and robust feature set make it an invaluable resource for ethical hacking education, bridging the gap between theoretical knowledge and practical application.

OpenVAS (Open Vulnerability Assessment Scanner) is an open-source tool designed for comprehensive vulnerability scanning and management. Its integration into cybersecurity training programs has proven instrumental in equipping ethical hackers with practical skills essential for identifying and mitigating security vulnerabilities (Mallick & Nath, 2024). Incorporating OpenVAS into cybersecurity curricula offers students hands-on experience with real-world tools, bridging the gap between theoretical knowledge and practical application. This approach enhances learners' abilities to conduct thorough vulnerability assessments and develop effective

remediation strategies. For instance, the Certified Ethical Hacker (CEH) v12 curriculum includes modules on vulnerability scanning using OpenVAS. This inclusion ensures that trainees gain proficiency in utilizing OpenVAS for identifying and analyzing security weaknesses, thereby preparing them for real-world cybersecurity challenges.

OpenVAS's compatibility with various security tools amplifies its effectiveness in training environments. Integrating OpenVAS with Security Information and Event Management (SIEM) systems, such as Wazuh, allows students to experience a holistic approach to threat detection and response (Estrella & Siringan, 2023). This integration provides a comprehensive understanding of how automated vulnerability scanning complements broader security operations. Real-world applications of OpenVAS in training scenarios underscore its value. A case study involving the Sorosoro Ibaba Development Cooperative demonstrated the practical benefits of leveraging OpenVAS alongside other open-source security tools (Estrella & Siringan, 2023). The study highlighted how such tools could enhance an organization's security posture while providing trainees with exposure to industry-relevant technologies.

The integration of OpenVAS into cybersecurity training programs significantly enhances the educational experience for ethical hackers. By providing hands-on exposure to a widely used vulnerability assessment tool, trainees develop the practical skills necessary to identify, analyse, and remediate security vulnerabilities effectively. This practical training is crucial in preparing students for the complexities of real-world cybersecurity environments. Kali Linux, renowned for its comprehensive suite of open-source tools, has been instrumental in advancing cybersecurity training for ethical hackers in academic and training environments. Its extensive toolkit enables hands-on learning experiences, crucial for developing practical skills in cybersecurity.

In academic settings, Kali Linux has been employed to create realistic simulation environments that enhance the quality of cybersecurity training. For instance, (Al., 2024) describe the architecture of a simulation environment based on a cluster of KVM hypervisors, utilizing open-source tools such as Kali Linux. This setup allows for the creation of scalable and flexible platforms at minimal cost, providing students with practical training scenarios that closely mimic real-world conditions. Furthermore, (Svabensky et al., 2021) developed an open-source toolset for logging commands executed on Linux machines, including those using Kali Linux. This toolset collects metadata about command executions, enabling automated processing to enhance instructors' understanding of student actions.

The application of this toolset in educational cybersecurity games demonstrated its value in revealing solution patterns, tools used, and student misconceptions, thereby informing instructional strategies. The versatility of Kali Linux extends to various domains within cybersecurity education (Journal et al., 2021). In (Nedyalkov & Georgiev, 2024) explored its application in studying the cybersecurity of power electronic devices. They utilized tools like Nmap, Wireshark, Burp Suite, and hping3 to assess vulnerabilities, demonstrating Kali Linux's applicability in specialized fields.

The Metasploit Framework, an open-source penetration testing platform, has significantly influenced cybersecurity training for ethical hackers in academic and training environments between 2020 and 2025. Its comprehensive suite of tools enables users to simulate real-world attacks, facilitating the development of practical skills essential for identifying and mitigating security vulnerabilities. In their study, (Landauer et al., 2024) conducted a structured comparison of nine open-source adversary emulation tools, including Metasploit.

The research highlighted Metasploit's robust features for exploitation and post-exploitation activities, underscoring its effectiveness in training scenarios. Another survey by (Modesti et al., 2024) examined research-informed ethical hacking tools. The study categorized these tools into process-based and knowledge-based frameworks, noting Metasploit's role in bridging the gap between academic research and practical application in penetration testing. (Al., 2024) explored the integration of simulation environments into cybersecurity training.

They emphasized the use of open-source tools, including Metasploit, to create realistic conditions for practical training, thereby enhancing the quality of cybersecurity education. Furthermore, (Nizon-Deladoeuille et al., 2025) evaluated the effectiveness of large language models in conducting penetration testing tasks. Their findings suggest that while AI models can support educational purposes, tools like Metasploit remain invaluable for providing hands-on experience in cybersecurity training. These studies collectively affirm Metasploit's pivotal role in enhancing cybersecurity training for ethical hackers, offering a practical, hands-on approach to learning that bridges theoretical knowledge and real-world application.

VI. CONCLUSION

The investigation into Kali Linux, Wireshark, Nmap and OpenVAS demonstrates their synergistic potential to significantly enhance cybersecurity training for ethical hackers. Each tool contributes uniquely to the educational pipeline: reconnaissance (Nmap), packet-level analysis (Wireshark), exploitation framework (Kali), and structures vulnerabilities reporting (OpenVAS). When integrated within scalable open-source environments such as the KYPO cyber range, this toolchain embodies a practical, realistic, and pedagogically sound training ecosystem (Vykopal et al., 2021).

Research by (Svabensky et al., 2021) illustrates that equipping such platforms with automated shell-command logging not only captures learner activity but also facilitates real-time analytics, instructor insight, and data-driven feedback loops substantially enhancing training quality. (Al., 2024) further reinforced this by deploying scalable KVM-based simulation systems, demonstrating that expansive, cost-effective cyber ranges are achievable through open-source architecture. Meanwhile, (Landauer et al., 2024) highlighted the critical importance of usability, documentation, and technical support among open-source tools factors that directly influence the effectiveness and adoption in training settings.

Collectively, these findings confirm that open-source cybersecurity toolchains offer an accessible, immersive and educational robust ecosystem perfect for ethical hacker training. Still, significant challenges persist such as tool complexity, maintenance demands, and the need for standardized pedagogical frameworks. Moving forward, future research should:

- Measure learning outcomes directly tied to tool usage (e.g., exploit success rates, vulnerability detection accuracy).
- Design integrative training curricula that align technological workflows with educational theory.
- Optimize toolchain usability and documentation, following practitioner-informed design principles.

By addressing these areas, we can unlock the full potential of open-source platforms in cultivating skilled, industry-ready ethical hackers anchored in reproducibility, realism and measurable competence.

VII. ACKNOWLEDGMENTS

The authors would like to thank all members of the School of Computing who are involved in this study. This study was carried out as part of the Hacking and Penetration Testing Project. This work was supported by Universiti Utara Malaysia.

REFERENCES

[1]. Akhtar, Z. Bin, & Rawol, A. T. (2024). Uncovering Cybersecurity Vulnerabilities: A Kali Linux Investigative Exploration Perspective.
[2]. International Journal of Advanced Network, Monitoring and Controls, 9(2), 11–22. https://doi.org/10.2478/ijanmc-2024-0012
[3]. Al., T. et. (2024). INTERACTIVE CYBERSECURITY TRAINING SYSTEM BASED ON SIMULATION. International Journal of Computer Applications, 4, 215–220.
[4]. Alhamed, M., & Rahman, M. M. H. (2023). A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. Applied Sciences (Switzerland),
[5]. 13(12). https://doi.org/10.3390/app13126986 Chaubey, N. K. (2024). The Role of Wireshark in Packet Inspection and Password Sniffing for Network Security. October. https://doi.org/10.4018/979-8-3693-9225-6.ch009
[6]. Estrella, M. B., & Siringan, O. C. (2023). Network Security Assessment Using Opensource Vulnerability Assessment and Penetration Testing (VAPT) With Security Information and Event Management (SIEM): A Case Study For Sorosoro Ibaba Development Cooperative (SIDC). Research and Educational Journal, 27(June), 52–63. https://www.researchgate.net/publication/371967009
[7]. Guaki, G. (2024). The Thin Boundary between Ethical and Unethical Hacking. July. https://doi.org/10.13140/RG.2.2.26226.31680
[8]. Hamza, M. A., Ejaz, U., & Kim, H. C. (2024).
[9]. Cyber5Gym: An Integrated Framework for 5G Cybersecurity Training. Electronics (Switzerland), 13(5). https://doi.org/10.3390/electronics13050888
[10]. Hashim, S. R., Enad, R. A., Al-Khafagi, A. M., & Abdalhameed, N. K. (2023). The facilities of detection by using a tool of Wireshark.
[11]. Indonesian Journal of Electrical Engineering and Computer Science, 31(1), 329–336. https://doi.org/10.11591/ijeecs.v31.i1.pp329-336
[12]. Ibraheem, I. O., & Kayode, S. M. (2024). ANALYZING VULNERABILITIES IN NETWORK PROTOCOLS USING WIRESHARK : June. InteliPaat. (2022). Cyber Security vs Ethical Hacking. InteliPaat, December.

[13]. Jaya, I. K. N. A., Dewi, I. A. U., & Mahendra, G. S. (2022). Implementation of Wireshark Application in Data Security Analysis on LMS Website. Journal of Computer Networks, Architecture and High Performance Computing, 4(1), 79–86. https://doi.org/10.47709/cnahpc.v4i1.1345
Journal, I., Science, C., & Volume-, E. (2021).
[14]. Ethical Hacking and Penetrate Testing using Kali and Metasploit Framework Mujahid Tabassum Saju Mohanan Department of IT , University of Technology and Department of IT , University of Technology and Applied Sciences Applied Sciences Muscat , Oman Tripti . 1, 9–22.
[15]. Katsantonis, M. N., & Mavridis, I. (2021).
[16]. Evaluation of hacklearn cofelet game user experience for cybersecurity education. International Journal of Serious Games, 8(3), 3–24. https://doi.org/10.17083/IJSG.V8I3.437
Landauer, M., Mayer, K., Skopik, F., Wurzenberger,
[17]. M., & Kern, M. (2024). Red Team Redemption: A Structured Comparison of Open-Source Tools for Adversary Emulation. http://arxiv.org/abs/2408.15645
[18]. Mabsali, N. A. L., Jassim, H., & Mani, J. (2023).
[19]. Effectiveness of Wireshark Tool for Detecting Attacks and Vulnerabilities in Network Traffic. Proceedings of the 1st International Conference on Innovation in Information Technology and Business (ICIITB 2022), 114–
[20]. 135. https://doi.org/10.2991/978-94-6463-110-4_10
[21]. Mallick, A. I., & Nath, R. (2024). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. World Scientific News: An International Scientific Journal, 190(1), 1–69. www.worldscientificnews.com
[22]. Modesti, P., Golightly, L., Holmes, L., Opara, C., & Moscini, M. (2024). Bridging the Gap: A Survey and Classification of Research-Informed Ethical Hacking Tools. Journal of Cybersecurity and Privacy, 4(3), 410–448. https://doi.org/10.3390/jcp4030021
[23]. Nedyalkov, I., & Georgiev, G. (2024). Kali Linux – a simple and effective way to study the level of cyber security and penetration testing of power electronic devices. International Journal on Information Technologies and Security, 16(2), 103–114. https://doi.org/10.59035/jmfy4876
[24]. Nizon-Deladoeuille, M., Stefánsson, B., Neukirchen, H., & Welsh, T. (2025). Towards Supporting Penetration Testing Education with Large Language Models: an Evaluation and Comparison. 101127453. https://doi.org/10.1109/SNAMS64316.2024.10883774
[25]. Pappala, S. (2025). Advancements in Ethical Hacking Techniques and Tools : Strengthening Cybersecurity Resilience. March.
[26]. Pittman, J. M. (2023). A Comparative Analysis of Port Scanning Tool Efficacy. 0–2. http://arxiv.org/abs/2303.11282
[27]. Soepeno, R. (2023). Wireshark: An Effective Tool for Network Analysis. CYBV - Introductory Methods of Network Analysis, September, 1– 15.
[28]. https://doi.org/10.13140/RG.2.2.34444.69769
Sulisnawati, N. (2023). Implementation of Open Web Application Security Project for Penetration Testing on Educational Institution Websites. Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika (JITEKI), 9(2), 250–267.
[29]. https://doi.org/10.26555/jiteki.v9i2.25987
Svabensky, V., Vykopal, J., Tovarnak, D., &
[30]. Celeda, P. (2021). Toolset for Collecting Shell Commands and Its Application in Hands-on Cybersecurity Training. Proceedings - Frontiers in Education Conference, FIE, 2021-Octob. https://doi.org/10.1109/FIE49875.2021.9637052
[31]. Vykopal, J., Celeda, P., Seda, P., Svabensky, V., & Tovarnak, D. (2021). Scalable Learning Environments for Teaching Cybersecurity Hands-on. Proceedings - Frontiers in Education Conference, FIE, 2021-Octob. https://doi.org/10.1109/FIE49875.2021.9637180
[32]. Yi, C., Wang, W., & Kwok, L.-F. (2024). Analysis of Cyber Range Scenario Design BT - Blended Learning. Intelligent Computing in Education (W. W. K. Ma, C. Li, C. W. Fan, L. H. U, & A. Lu (eds.); pp. 322–332). Springer Nature Singapore.
[33]. Zilberman, P., Puzis, R., Bruskin, S., Shwarz, S., & Elovici, Y. (2020). SoK: A Survey of Open- Source Threat Emulators. http://arxiv.org/abs/2003.01518