Borneo International Journal eISSN 2636-9826; Vol.8 (2); 2025; 40-47
Published by *Majmuah Enterprise*
www.majmuah.com

The Evolution of Wireless Penetration Testing Tools: A Case Study of Aircrack-ng and Bettercap

MUHAMMAD FADILAH ALFARIZY and MOHAMAD FADLI BIN ZOLKIPLI

School of Computing, Awang Had Salleh Graduate School College of Arts and Sciene, Universiti Utara Malaysia (UUM), 06010 Kedah, MALAYSIA
Email: alfarizy_muhammad2@ahsgs.uum.edu.my, m.fadli.zolkipli@uum.edu.my | Tel: +601140194799, +6049285058

Received: June 20, 2025
Accepted: June 24, 2025
Online Published: June 27, 2025

Abstract

The rapid advancement of wireless technologies has introduced new challenges in cybersecurity, particularly in ethical hacking practices that rely on effective wireless auditing tools. This paper investigates the development, capabilities, and limitations of two prominent tools Aircrack-ng and Bettercap by conducting a structured literature analysis of academic and technical sources from 2018 to 2025. Rather than performing empirical testing, the study focuses on synthesizing existing findings to trace the evolution of these tools and evaluate their relevance in contemporary ethical hacking scenarios. The analysis reveals that Aircrack-ng, while reliable for traditional Wi-Fi auditing, lacks adaptability to modern, multi-protocol environments. In contrast, Bettercap offers broader protocol support and real-time attack simulation, making it more aligned with dynamic, adversarial testing needs. This comparative examination highlights the shifting paradigms in wireless penetration testing, emphasizing the need for toolsets that can evolve alongside emerging threats. The findings provide ethical hacking practitioners with a clearer understanding of how tool development impacts testing strategy and operational effectiveness.

Keywords: **Wireless Security, Penetration Testing, Aircrack-ng, Bettercap, Cybersecurity Tools**

1. Introduction

Wireless technologies have become a critical backbone of modern communication, enabling mobility, scalability, and convenience in both enterprise and consumer networks. However, the widespread adoption of wireless infrastructures has also expanded the attack surface for malicious actors. This expansion is evident in the vulnerabilities identified across smart home automation platforms (Kafle et al., 2020) and in mobile cryptocurrency applications (Hu et al., 2021). With threats ranging from Wi-Fi cracking and packet injection to man-in-the-middle and spoofing attacks, the need for robust wireless security assessments has become more urgent than ever. Beyond traditional threats, contemporary challenges include advanced Wi-Fi traffic manipulation through beamforming feedback forgery (Xu et al., 2024), man-in-the-middle attacks exploiting SSL/TLS certificate validation flaws in IoT client applications and WPA Enterprise supplicants (Wang et al., 2022). Furthermore, the critical impact of these vulnerabilities extends to financial systems, with documented cases targeting e-banking platforms (Chanbuala et al., 2025) and global interbank transaction systems like SWIFT (Qin & Mogos, 2022). Within this context, ethical hacking particularly wireless penetration testing plays a vital role in identifying and mitigating vulnerabilities before they can be exploited. To carry out such assessments effectively, practitioners rely heavily on specialized auditing tools that can simulate real-world attack vectors and provide actionable insights. As wireless communication protocols evolve and diversify, the tools used in ethical hacking must also adapt to maintain their relevance and effectiveness. Wireless networks are frequent targets for attacks such as Wi-Fi cracking, ARP spoofing, and man-in-the-middle interceptions. For instance, studies on home network environments confirm the persistent vulnerability of SOHO routers to common attacks like deauthentication, dictionary attacks, bruteforcing, and ARP poisoning (Blancaflor et al., 2022), highlighting the continued relevance of these basic attack vectors.

This study focuses on tracking the development, capabilities, and limitations of two widely recognized wireless auditing tools: *Aircrack-ng* and *Bettercap*. Rather than conducting live testing, this paper employs a qualitative methodology by synthesizing existing academic and technical literature published between 2020 and 2025. The aim is to understand how these tools have evolved over time, how they support different ethical hacking methodologies, and where their strengths and limitations lie in contemporary wireless security contexts. While Aircrack-ng provides stability and procedural transparency, Bettercap represents a dynamic tool that aligns with real-time adversarial testing (Hassan & Niazi, 2024).

The findings of this study contribute to a clearer understanding of how wireless penetration testing tools align with the shifting demands of ethical hacking practices. As modern wireless environments become more complex and interconnected spanning not just Wi-Fi but also Bluetooth, mesh networks, and IoT devices ethical hackers require toolsets that evolve in tandem with technological changes. This includes the need for tools to assess the security of diverse interconnected systems, from smart home devices (Kafle et al., 2020) and mobile financial applications (Hu et al., 2021) to advanced network traffic manipulation (Xu et al., 2024) and critical certificate validation issues (Alghamdi et al., 2018; Wang et al., 2022). By tracing the historical development, functional advancements, and technical limitations of Aircrack-ng and Bettercap, this paper offers both conceptual and practical guidance. Such practical insights are crucial, particularly in cybersecurity education, where hands-on training for mobile and wireless security is emphasized to foster an adversarial mindset (O'Connor & Stricklan, 2021). It is intended to assist practitioners, educators, and researchers in selecting and applying tools that are not only technically effective, but also aligned with ethical standards, testing objectives, and operational contexts. Unlike previous studies that focus solely on performance benchmarks, this paper provides a holistic perspective by mapping the functional evolution of wireless auditing tools in relation to ethical hacking methodologies.

2. Methodology

This study adopts a **Systematic Literature Review (SLR)** as outlined by Felizardo and Carver (2020), Cruz-Benito (2016), and Shaffril et al. (2020) approach to investigate the evolution of wireless penetration testing tools, with a particular focus on **Aircrack-ng** and **Bettercap**. Rather than performing hands-on testing or direct experimentation, the research is based entirely on a structured analysis of existing academic literature, technical reports, and other scholarly sources published between 2018 and 2025. This approach allows for a comprehensive understanding of the tools' development, capabilities, and applications within the field of wireless security.

2.1 Research Design

The methodology consists of several key phases: formulating research questions, identifying and selecting relevant publications, extracting data, and conducting thematic analysis. The following research questions guide the study:

- How have wireless penetration testing tools developed over the last five years?
- What are the key strengths, limitations, and use cases of Aircrack-ng and Bettercap as reported in the literature?
- In which security contexts have these tools been effectively implemented?

2.2 Literature Search Strategy

A comprehensive search was conducted across major academic databases including IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink. Additional sources were identified using academic search engines to ensure coverage of relevant gray literature. The search strategy utilized keyword combinations such as “Aircrack-ng,” “Bettercap,” “wireless penetration testing,” and “network attack simulation tools.” Only publications written in English and published between January 2020 and April 2025 were considered. The selection process aimed to identify studies that provide meaningful insights into the functionality, evolution, or comparative assessment of the tools in question.

2.3 Inclusion and Exclusion Criteria

To ensure relevance and academic quality, specific inclusion and exclusion criteria were applied:

Inclusion Criteria:

- Peer-reviewed articles, conference papers, and technical reports
- Publications focusing on Aircrack-ng and/or Bettercap in the context of wireless security
- Studies discussing tool implementation, evaluation, or evolution

Exclusion Criteria:

- Non-academic sources such as blogs, online tutorials, or forums
- Studies that focus on unrelated or outdated tools
- Articles without full-text access or lacking methodological clarity

2.4 Data Extraction and Analysis

From each selected publication, key information was extracted including tool version, features analyzed, context of application, and major findings. A thematic analysis was then applied to identify recurring concepts, trends, and comparative observations. Particular attention was given to areas such as performance, ease of use, compatibility with modern systems, and relevance to contemporary wireless attack scenarios.

2.5 Limitations

This research is limited to secondary data obtained through literature. No practical testing or real-world deployment of the tools was conducted by the authors. As such, any performance claims or operational insights are derived from the reviewed sources. Nonetheless, the systematic nature of the review ensures a balanced and comprehensive evaluation of the selected tools.

3. Results and Discussion: Evolution and Application of Wireless Auditing Tools in Ethical Hacking

The dynamic growth of wireless technologies and the parallel rise of cyber threats have made wireless auditing tools an integral part of ethical hacking practices. This urgency is driven by the emergence of complex threats across diverse environments, including smart home IoT devices (Kafle et al., 2020), mobile applications handling sensitive data (Hu et al., 2021), and sophisticated network manipulation techniques (Xu et al., 2024; Wang et al., 2022; Chanbuala et al., 2025; Qin & Mogos, 2022). This section presents an analytical review of two widely used tools, Aircrack-ng and Bettercap, with emphasis on their development, capabilities, and limitations from 2020 to 2025. The discussion integrates insights from recent studies to contextualize each tool's role within the broader evolution of wireless security assessment.The comparison is organized around four core themes: technical evolution, usability, protocol coverage, and relevance to ethical hacking methodologies. These themes serve to trace how each tool has adapted to the demands of modern wireless security environments.

3.1 Evolution of Wireless Auditing Tools

The progression of wireless auditing tools reflects a shift in both technological architecture and testing philosophy. Aircrack-ng represents a foundational tool in Wi-Fi auditing, initially designed to crack WEP and WPA/WPA2-PSK encryptions. Its modular command-line interface and reliability have made it a staple in traditional penetration testing workflows. However, its core capabilities have remained relatively static, focusing predominantly on 802.11-based protocols. Its modularity and transparency make it a staple in academic and compliance testing environments. However, it lacks native support for newer protocols such as BLE or mesh networking. This limitation contrasts with the expanding attack surface that includes vulnerabilities in pervasive IoT systems and the need to assess a broader range of wireless communication channels beyond Wi-Fi (Blancaflor et al., 2022). In contrast, *Bettercap* has emerged as a more modern and extensible tool, developed to accommodate evolving wireless attack surfaces. It supports not only Wi-Fi attacks but also Bluetooth Low Energy (BLE), Ethernet sniffing, DNS spoofing, and various man-in-the-middle attacks. This evolutionary shift from specialized to versatile functionality marks a clear response to the growing complexity of wireless networks and the need for ethical hackers to simulate more realistic adversarial behavior. It integrates scripting capabilities and real-time manipulation features, making it suitable for dynamic environments (Wijayanto, 2023). All figures and tables presented in this paper are self-developed by the author based on synthesized findings from reviewed literature.

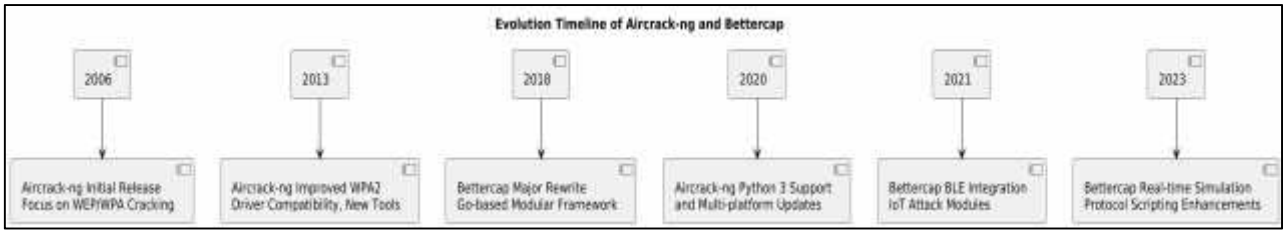

Figure 1: Timeline of Feature Evolution and Functional Capability of Aircrack-ng and Bettercap

3.2 Operational Usability and Workflow Efficiency

From a usability perspective, *Aircrack-ng* maintains a minimalistic and manual approach, requiring users to execute discrete binaries for monitoring, capturing, and cracking processes. While this provides fine-grained control, it can be time-consuming in dynamic testing environments. It is best suited for controlled audits and learning environments where procedural transparency is valued. *Bettercap*, on the other hand, integrates a comprehensive command shell with scripting capabilities, enabling faster execution of compound attack scenarios. Its automation potential and active session manipulation tools align more closely with the needs of modern ethical hacking, particularly in red team operations and simulation-based assessments where agility and adaptability are paramount.

3.3 Protocol Versatility and Threat Surface Coverage

The ability to address diverse communication protocols is a critical factor in assessing a tool's applicability to modern wireless ecosystems. *Aircrack-ng* performs well in single-protocol, Wi-Fi-centric environments but lacks support for newer communication standards like BLE or hybrid IP-based interactions. Bettercap offers a broader scope, extending its auditing functionality across multiple layers of wireless and network communication. This makes it more suitable for ethical hackers who need to engage with a wider threat landscape, including smart devices, IoT environments, and mesh networks. This wider threat landscape includes vulnerabilities in smart home IoT systems (Kafle et al., 2020; Alghamdi et al., 2018), mobile application security threats (Hu et al., 2021), advanced Wi-Fi manipulation techniques (Xu et al., 2024), and various network-level attacks in diverse settings (Wang et al., 2022; Chanbuala et al., 2025; Qin & Mogos, 2022; Blancaflor et al., 2022). Its plugin-based structure also facilitates ongoing updates to meet emerging security testing needs.

3.4 Limitations and Strategic Tool Selection

Despite their strengths, both tools have inherent limitations. *Aircrack-ng*, while stable and widely documented, does not scale efficiently to multi-vector environments. Its dependence on user-driven workflows can also hinder rapid testing. Meanwhile, *Bettercap*, although feature-rich, may pose a steeper learning curve due to its broad command set and scripting depth, potentially requiring more experience to utilize effectively. Aircrack-ng requires manual execution of binaries for monitoring and cracking, which benefits procedural clarity but hinders rapid testing. Bettercap, in contrast, features an interactive shell and automation features suitable for red teaming and complex simulations (Chatterjee, 2024; Vink, 2020). In Protocol coverage, Aircrack-ng is limited to 802.11 protocols, whereas Bettercap supports Wi-Fi, BLE, Ethernet, and hybrid interactions. In ethical hacking contexts, tool selection should therefore be guided by the specific testing objectives. For compliance testing and encryption audits, *Aircrack-ng* remains sufficient. For advanced adversarial emulation, especially when testing complex, live environments, *Bettercap* offers a strategic advantage. The evolution of these tools illustrates not just a technological trend, but a methodological shift in ethical hacking itself from narrowly scoped penetration tests to realistic, behavior-driven security evaluations. Aircrack-ng remains effective for controlled environments and compliance audits. For **strategic tool use**, Bettercap, although complex, offers superior adaptability and supports a broader threat surface, making it ideal for adversarial emulation. (Wijayanto, 2023)

Feature	Aircrack-ng	Bettercap
Protocol Coverage	Wi-Fi only	Wi-Fi, BLE, Ethernet
User Interface	CLI (modular tools)	Interactive shell + scripting
Platform Support	Linux, Windows, macOS	Linux, macOS

Power Consumption	Low	Medium to High
Community Support	Mature, Stable	Active, Developer-Driven
Scriptability	Basic (bash only)	Advanced (scripting engine)
Ideal Use Case	Education, Compliance Audit	Red Teaming, IoT Testing

Table 1: Feature Comparison Feature Comparison Between Aircrack-ng and Bettercap

3.6 Implications for Ethical Hacking Practice

This comparative study illustrates how wireless penetration testing tools have evolved from single-purpose binaries like Aircrack-ng to modular, extensible frameworks such as Bettercap. The shift reflects broader trends in cybersecurity toward realistic adversarial testing, automation, and cross-protocol compatibility (Sundberg & Carlsson, 2023). The comparative evolution of Aircrack-ng and Bettercap offers several practical insights for ethical hacking operations. As wireless technologies continue to diversify, ethical hackers are expected to simulate threats that go beyond traditional Wi-Fi exploits. Such threats include advanced mobile application vulnerabilities (Hu et al., 2021), sophisticated network manipulation through beamforming (Xu et al., 2024), and security weaknesses in enterprise Wi-Fi (Wang et al., 2022), e-banking (Chanbuala et al., 2025), and critical financial systems (Qin & Mogos, 2022). Bettercap's modularity and real-time manipulation features reflect this new demand for adaptive and situational tools. Meanwhile, Aircrack-ng retains its value in audit scenarios that emphasize repeatability, transparency, and protocol-specific testing. Practitioners should consider that ethical hacking today requires not only technical skill but also contextual awareness understanding which tool best fits the environment, threat model, and testing objective. Integrating tools into broader frameworks, such as automated testing pipelines or red team platforms, may further enhance operational impact. Furthermore, the increasing use of cloud-based wireless infrastructure raises new questions about the scalability and deployment of such tools in virtualized environments. Addressing these concerns will be essential for maintaining the relevance of auditing practices in the years ahead.

3.7 Recommendations for Future Research and Development

While this study focused on Aircrack-ng and Bettercap, the wireless security tool landscape is much broader. Future research should explore how newer frameworks, including AI-enhanced penetration testing platforms, can improve accuracy and adaptability in attack simulations. Additionally, examining the integration of wireless auditing tools into cybersecurity orchestration and automation systems (SOAR) would be beneficial. Another promising direction is the comparative analysis of tool performance in live cloud environments, including virtualized access points and containerized networks. As penetration testing increasingly targets IoT ecosystems and edge devices, new tools will need to handle limited bandwidth, low-energy protocols, and constrained hardware resources. This is crucial given the persistent security challenges in smart home IoT systems (Kafle et al., 2020), SSL/TLS certificate validation in IoT applications (Alghamdi et al., 2018), and general vulnerabilities found in IP cameras and other IoT devices (Blancaflor et al., 2022). Addressing these emerging challenges will define the next phase in the evolution of wireless auditing tools.

Summary of Comparative Attributes

Analytical Dimension	Aircrack-ng	Bettercap
Primary Focus	Wi-Fi encryption analysis	Multi-protocol offensive simulation
User Interface	Command-line (multi-binary)	Interactive shell with scripting support
Protocol Coverage	802.11 (Wi-Fi) only	Wi-Fi, BLE, Ethernet, DNS, and more
Modularity	Fixed, task-specific binaries	Modular and extensible framework

Update Frequency	Conservative, stable releases	Active development and rapid iteration
Best-fit Use Case	Academic testing, compliance audits	Red teaming, threat emulation

Table 2: Comparative Attributes of Aircrack-ng and Bettercap

In sum, this comparative evaluation reflects the broader transformation in the field of wireless auditing from narrowly scoped, tool-specific assessments to more holistic, scenario-driven simulations. Ethical hacking today demands not only knowledge of tools but also strategic judgment in choosing the right tool for the right purpose. Understanding the evolutionary path and capability profile of tools like Aircrack-ng and Bettercap allows professionals to better prepare for real-world challenges and ensure that wireless penetration testing remains both relevant and effective in safeguarding digital ecosystems.

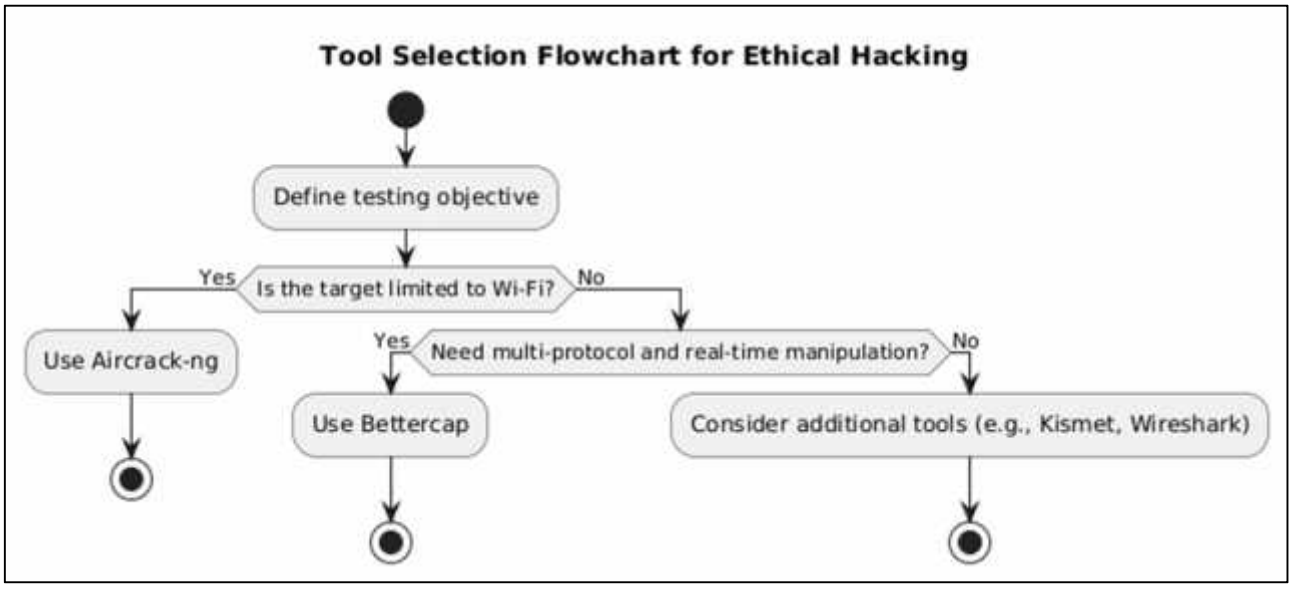

Figure 2: Tool Selection Flowchart for Wireless Penetration Testing Tools

4. Conclusions

This study has explored the development, capabilities, and limitations of wireless auditing tools within the context of ethical hacking, using Aircrack-ng and Bettercap as representative case studies. By synthesizing recent academic and technical literature, the analysis has traced how these tools have evolved in response to shifting wireless security challenges and the increasing complexity of attack surfaces (Blancaflor et al., 2022; Wang et al., 2022; Xu et al., 2024; Kafle et al., 2020). Aircrack-ng, as one of the earliest tools in wireless auditing, has demonstrated consistent reliability in testing encryption protocols, particularly in targeted Wi-Fi environments. Its continued relevance lies in its efficiency and stability, although its limited protocol coverage and manual operation model reflect a more traditional approach to penetration testing. As wireless ecosystems expand beyond standard 802.11 protocols, this tool's applicability becomes more constrained. Bettercap, in contrast, exemplifies the new generation of wireless auditing tools designed to accommodate diverse protocols, dynamic attack simulations, and real-time manipulation. Its modular design and scripting flexibility allow it to respond to a broader range of testing scenarios, particularly those requiring multi-protocol awareness and rapid execution. The findings suggest that the evolution of wireless auditing tools is closely tied to the demands of ethical hacking practices, which now require not only precision but also adaptability. As ethical hackers increasingly face sophisticated, layered threats across heterogeneous environments (Hu et al., 2021; Chanbuala et al., 2025; Qin & Mogos, 2022; Alghamdi et al., 2018), the tools they use must evolve accordingly favoring modularity, cross-platform compatibility, and integration with broader offensive security frameworks.

Ultimately, understanding the trajectory of these tools – both their strengths and inherent constraints – enables practitioners and researchers to make better-informed choices in aligning tool selection with testing objectives,

technical requirements, and ethical standards. As wireless penetration testing continues to evolve as a critical domain within cybersecurity, the ability to evaluate tools based on their historical development and operational maturity becomes increasingly important. This paper offers a foundational perspective that can inform future explorations, particularly as wireless auditing tools are integrated with automated, AI-driven testing platforms and applied to increasingly decentralized environments such as edge computing and cloud-native networks (Kafle et al., 2020; Alghamdi et al., 2018; Blancaflor et al., 2022). This study serves as a practical guide for cybersecurity professionals in selecting appropriate wireless auditing tools based on scenario-specific needs ranging from compliance-driven audits to agile, adversarial simulations in red teaming environments.

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

Chatterjee, A. (2024). *Comparative evaluation of cyber offensive tools: An ethical hacking perspective* [Doctoral dissertation, ProQuest Dissertations & Theses]. https://www.proquest.com/docview/3098795742

Cruz-Benito, J. (2016, November 7). *Systematic literature review & mapping* [PhD presentation]. University of Salamanca. https://doi.org/10.5281/zenodo.165773

Felizardo, K. R., & Carver, J. C. (2020). Automating systematic literature review. In M. Felderer & G. H. Travassos (Eds.), *Contemporary Empirical Methods in Software Engineering* (pp. 327–348). Springer. https://doi.org/10.1007/978-3-030-32489-6_12

Hassan, M. A., & Niazi, M. (2024). A comparative evaluation of ethical hacking frameworks for wireless intrusion. *Discover Internet of Things*, *4*, 153. https://doi.org/10.1016/j.dit.2024.100153

Nugroho, A. S. (2023). *Analisis Perbandingan Tools untuk Penetration Testing Jaringan Nirkabel* [Undergraduate thesis, Universitas Islam Indonesia]. https://dspace.uii.ac.id/handle/123456789/42627

Roy, S., & Mallick, P. K. (2019). Penetration testing tools: A comparative study. *Computer Science & Information Technology (CS & IT)*, *9*(12), 125–138.

Shaffril, H. A. M., Samsuddin, S. F., & Abu Samah, A. (2020). The ABC of systematic literature review: The basic methodological guidance for beginners. *Quality & Quantity*, *55*, 1319–1346. https://doi.org/10.1007/s11135-020-01059-6

Stang, C. (2017). *Cybersecurity Tools: A comparative analysis of Bettercap and Aircrack-ng* [Honors thesis, University of Akron]. https://ideaexchange.uakron.edu/honors_research_projects/1525/

Sundberg, J., & Carlsson, J. (2023). *A comparative study of wireless penetration testing tools* [Bachelor thesis]. Linnaeus University. https://www.diva-portal.org/smash/get/diva2:1870312/FULLTEXT01.pdf

Vink, M. (2020). *A comprehensive taxonomy of WiFi attacks* [Master's thesis]. Radboud University. https://www.cs.ru.nl/masters-theses/2020/M_Vink___A_comprehensive_taxonomy_of_wifi_attacks.pdf

Wijayanto, A. (2023). *Forensik jaringan terhadap serangan ARP spoofing menggunakan metode TAARA* [Master's thesis, Universitas Islam Indonesia].

Chanbuala, K., Puangpronpitag, E., Puangpronpitag, D., & Puangpronpitag, S. (2025, March 10). *Evaluating and Mitigating HTTPS Interception in Thai E-Banking Websites: Challenges and Solutions*. ICNCC '24: Proceedings of the 2024 13th International Conference on Networks, Communication and Computing, 81–86. https://doi.org/10.1145/3711650.3711662

Qin, M., & Mogos, G. (2022, December 20). *Cyber-attacks on SWIFT Systems of financial institutions*. CSSE '22: Proceedings of the 5th International Conference on Computer Science and Software Engineering, 596–599. https://doi.org/10.1145/3569966.3570116

Kafle, K., Moran, K., Manandhar, S., Nadkarni, A., & Poshyvanyk, D. (2020, December 30). *Security in Centralized Data Store-based Home Automation Platforms: A Systematic Analysis of Nest and Hue*. ACM Transactions on Cyber-Physical Systems, 5(1), 1–27. https://doi.org/10.1145/3418286

Blancaflor, E. B., Alvarez, L. A., Dionisio, N. M., Acuna, G. E., Funilas, J. R., & Odicta, J. M. (2022, January 14). *Penetration Test on Home Network Environments: A Cybersecurity Case Study*. ICMECG '21: Proceedings of the 8th International Conference on Management of E-Commerce and E-Government, 100–104. https://doi.org/10.1145/3483816.3483834

Alghamdi, K., Alqazzaz, A., Liu, A., & Ming, H. (2018, March 13). *IoTVerif: An Automated Tool to Verify SSL/TLS Certificate Validation in Android MQTT Client Applications*. CODASPY '18: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, 95–102. https://doi.org/10.1145/3176258.3176334

Xu, M., He, Y., Li, X., Hu, J., Chen, Z., Xiao, F., & Luo, J. (2024, December 4). *Beamforming made Malicious: Manipulating Wi-Fi Traffic via Beamforming Feedback Forgery*. ACM MobiCom '24: Proceedings of the 30th Annual International Conference on Mobile Computing and Networking, 908–922. https://doi.org/10.1145/3636534.3690669

O'Connor, T. J., & Stricklan, C. (2021, June 26). *Teaching a Hands-On Mobile and Wireless Cybersecurity Course*. ITiCSE '21: Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 1, 296–302. https://doi.org/10.1145/3430665.3456346

Hu, Y., Wang, S., Hu, G., Xiao, L., Xie, T., Lei, X., & Li, C.-Y. (2021, April 26). *Security Threats from Bitcoin Wallet Smartphone Applications: Vulnerabilities, Attacks, and Countermeasures*. CODASPY '21: Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, 89–100. https://doi.org/10.1145/3422337.3447832

Wang, K., Zheng, Y., Zhang, Q., Bai, G., Qin, M., Zhang, D., & Dong, J. S. (2022, October 14). *Assessing certificate validation user interfaces of WPA supplicants*. MobiCom '22: Proceedings of the 28th Annual International Conference on Mobile Computing And Networking, 501–513. https://doi.org/10.1145/3495243.3517026

Khairi, M., Husin, W. H. S. W., Mahat, S. A., & Aman, A. H. M. (2024). IoT security for smart homes: a systematic review. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-024-05187-5