Borneo International Journal eISSN 2636-9826; Vol. 6 (1); 2023; 44-52
Published by *Majmuah Enterprise*
www.majmuah.com

Cybersecurity Strengthening through Penetration Testing: Emerging Trends and Challenges

ABDUL KADIR BIN MAHAMOOD, MUZDALINI BINTI MALIK, ADI BADIOZAMAN BIN RUHANI and MOHAMAD FADLI BIN ZOLKIPLI
School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: kadirjpn@gmail.com, muzdalini@gmail.com, adryunosuke@gmail.com , m.fadli.zolkipli@uum.edu.my
Tel: +60134368080, +60135840083, +601137150046, +60177247779 |

Received: February 21, 2023
Accepted: February 24, 2023
Online Published: March 01, 2023

Abstract

Penetration testing is an important tool for assessing system security posture and detecting vulnerabilities. Cybersecurity risks, such as hacking and data breaches, have become increasingly complex, necessitating the implementation of effective security measures by organisations. Penetration testing has evolved as an important tool for evaluating system security posture and detecting vulnerabilities. This paper aims to explore the emerging trends and challenges in cybersecurity strengthening through penetration testing. This paper provides an overview of penetration testing, its benefits, and the various approaches used like. This paper further discusses the challenges associated with penetration testing, such as the threats, dealing with professional liability, accuracy and reliability, security and privacy concerns. It also discusses strategies to effectively strengthen their cyber security ensure effective cybersecurity strengthening through penetration testing. Finally, this paper offers recommendations the key strategies for strengthening cybersecurity through penetration testing. The research findings can guide policymakers, system administrators, and cybersecurity experts in understanding the emerging trends in penetration testing and how to address the challenges to strengthen cybersecurity effective.

Keywords: pentest; penetration test; cybersecurity, vulnerability; emerging trends

1. Introduction

Penetration testing, commonly referred to as "pentesting," is a security testing technique that simulates a real-world cyberattack against a computer system, network, or web application in order to find gaps and vulnerabilities that attackers could exploit. Penetration testing's objectives are to provide companies information about their security posture and to assist them in prioritising and addressing possible security threats. Penetration testing is often carried out by qualified experts who use a range of instruments and methods to find security flaws and provide suggestions for fixing them. Penetration testing is a critical aspect of cybersecurity as it helps to identify vulnerabilities in systems, applications, and networks. By simulating an attack, cybersecurity experts can uncover weaknesses in a system that could be exploited by a malicious actor. Penetration testing can help organisations to identify and remediate vulnerabilities before they are exploited, reducing the risk of a cyber-attack, and protecting sensitive data. It is a proactive approach to cybersecurity that enables organisations to stay ahead of the evolving threat landscape. Regular penetration testing is recommended to ensure that security measures are up to date and effective in mitigating emerging threats.

Research on penetration testing has been done in a number of academic papers. For instance, (Beattie & Goodwill, 2018) studied penetration testing's advantages and drawbacks in their research and stressed the need of using an organised method to ensure the testing's maximum efficacy. In a separate piece, (Ezzati & Zakerolhosseini, 2018) reviewed the literature to assess the state of the art in penetration testing and noted a number of issues, including the lack of standardisation and the need for continuous testing. Gonzalez, Garcia, and Clark (2019) analysed several penetration testing approaches and discovered that each methodology has benefits and drawbacks, and the methodology chosen should be based on the particular needs of the company. The requirement for a risk-based strategy was stressed by (Hagen & Snekkenes, 2018), who also suggested a framework for assessing penetration testing approaches.

The structure of this paper begins with describing the background and related work. The rest of paper is structured as follow: Section 2, overview of penetration testing. Section, 3 explore the emerging trends in Penetration Testing. Section 4, present the challenge in penetration testing. The discussion is drawn in Section 4. and Section 5 will conclude our paper.

Importance of Penetration Testing in Cybersecurity

One of the most important aspects of cybersecurity is penetration testing, commonly referred to as "pentesting" or "ethical hacking." In order to find and exploit vulnerabilities, it entails simulating an attack on a computer system or network. This gives insight into possible security flaws that need to be fixed.

Penetration testing is crucial for cybersecurity for a number of reasons, some of which are listed below:

i. Finding vulnerabilities: Penetration testing helps find holes in a system or network, giving information on possible avenues of access for hackers. Organisations that manage financial transactions or store sensitive data may find this to be of special importance.

ii. Risk reduction: Pentesting enables companies to manage and reduce risks before they are used by attackers by finding vulnerabilities. This may lessen the risk of data breaches, monetary loss, and reputational harm.

iii. Penetration testing is often necessary to comply with industry standards or laws like PCI-DSS (Payment Card Industry Data Security Standard) or HIPAA (Health Insurance Portability and Accountability Act). Legal sanctions, fines, and reputational harm may come from noncompliance.

iv. Continuous development: In order to maintain continuing defence and spot any newly emerging vulnerabilities, penetration testing should be carried out on a frequent basis. This method of approaching cybersecurity aids businesses in maintaining their security and staying ahead of emerging threats.

Overall, penetration testing is a crucial component of a thorough cybersecurity plan. It assists firms in identifying vulnerabilities, minimising risks, ensuring compliance, and continuously enhancing their security posture to remain one step ahead of attackers.

2. Overview

Pentesting is a crucial part of cybersecurity, but as the threat environment changes, new patterns and problems are appearing that businesses need to address to maintain the efficacy of their testing. These are some of the current trends and difficulties in penetration testing:

Cloud security: As cloud services become more widely used, more businesses are increasingly deploying crucial systems and applications on cloud platforms. Due to the architecture and security measures being often considerably different from those of conventional on-premises setups, penetration testing in the cloud might offer special difficulties. In order to properly replicate attacks on cloud settings, pen testers must have a thorough grasp of cloud security.

IoT Devices: Another development that is transforming penetration testing is the ubiquity of Internet of Things (IoT) devices. Due to their varied designs and limited resources, these devices may be difficult to test, and they often contain default passwords or other vulnerabilities that need to be found and fixed.

Automation: To assist enterprises increase the efficiency and accuracy of their testing, automation is becoming increasingly crucial in penetration testing. Pentesters still need to possess the abilities to evaluate and understand the data since automated solutions are not a panacea.

Social Engineering: Attacks using human manipulation, such as phishing and other types of social engineering, continue to be a severe problem for enterprises. To evaluate an organisation's capacity to recognise and counteract social engineering assaults, pen testers must be able to successfully mimic these attacks.

Regulation and compliance: As laws governing data protection and cybersecurity continue to change, it is crucial for businesses to make sure their pen testing initiatives adhere to the law. Due to this, pentesters must have a thorough awareness of legal and compliance frameworks.

In conclusion, the current trends and difficulties in penetration testing show how important it is for businesses to keep up with the changing threat environment and refine their testing procedures to maintain a strong and effective security posture.

3. Emerging Trends in Penetration Testing

Automated Penetration Testing

The effectiveness of pentesting largely depends on the skill level of the cybersecurity experts involved. With complex network structures and evolving attack vectors, the requirements for pentest experts are increasing. Automation can provide a solution to these issues. Automated pentesting comprehensively considers network security and helps to reduce costs and resources, which is significant for the development and popularization of pentesting (Hu *et al*., 2020).

Automated penetration testing is simulating assaults on a system or application using software tools. These programmes may automatically search for and exploit vulnerabilities in order to obtain unauthorised access to the system. Automated penetration testing is beneficial for swiftly finding known vulnerabilities and may be used to conduct large-scale testing. However, automated testing has limitations in that it may not detect all vulnerabilities and may result in false positives or false negatives. As a result, it should be used in conjunction with manual penetration testing to offer a holistic picture of a system's security posture. Automated penetration testing may supplement manual testing while also improving overall security.

Cloud Penetration Testing

The importance of securing cloud-based systems cannot be overstated due to the extensive use of cloud infrastructure. As every component of the system is connected to the Internet, even minor security vulnerabilities can potentially compromise the entire system infrastructure. In order to ensure the safety of cloud-based systems, it is essential to conduct thorough investigations to identify potential security flaws. Vulnerability assessment and penetration testing are among the methods that can be used to achieve this objective (Al-Ahmad et al., 2019).

Cloud penetration testing is the practise of assessing the security of a cloud-based system or application by simulating an attack by a hostile actor. The goal of cloud penetration testing is to detect vulnerabilities and security flaws in the cloud infrastructure that might be exploited by attackers to obtain unauthorised access to the system or data. Cloud penetration testing is an important part of cloud security since it allows enterprises to examine their cloud security posture. The testing is often carried out by a team of cybersecurity professionals who employ a number of tools and techniques to find vulnerabilities in the cloud environment. Testing may involve vulnerability scanning, network scanning, penetration testing, and application testing. Cloud penetration testing generally consists of the following steps:

i. Scoping: The process of determining the scope of the test, which includes the cloud environment, applications, and systems that will be tested.

ii. Reconnaissance: The process of obtaining information about a target system or application in order to uncover possible vulnerabilities.

iii. Vulnerability scanning: The process of searching a target system for known vulnerabilities using automated techniques.

iv. Exploitation: trying to obtain unauthorised access to the system by exploiting the discovered vulnerabilities.

v. Post-exploitation: testing involves running extra tests to uncover other vulnerabilities that an attacker may exploit.

vi. Reporting: entails recording the test results and making suggestions for corrective action.

Penetration Testing for IoT Devices

Currently, security concerns are a major obstacle for the widespread adoption of Internet of Things (IoT) systems. As a result, certifying and communicating the security level of devices is critical for their acceptance. This means that there is a need for reliable methods of ensuring the security of IoT systems to improve public trust and acceptance (Matheu-García *et al*., 2019). Penetration testing for IoT (Internet of Things) devices is a technique that evaluates the security of these devices by simulating a malicious hacker's attack. The purpose of penetration testing is to find vulnerabilities and flaws in IoT devices and networks before attackers exploit them. This procedure is carried out to ensure the overall strength of an organisation's defence against cyber thieves attacking IoT devices. According to (Heiding *et al*., 2023)**,** Cybe**r** attackers can use this as an entry point. The abundance of successful cyber assaults on home IoT devices implies that the security of these devices, or the security of apps associated with these devices, is frequently weak. Penetration testing for IoT devices can be performed in a variety of ways, including black-box and white-box testing. The hacker has no knowledge of the company's network during black-box testing, simulating a real-life attack situation. In white-box testing, on the other hand, the tester has comprehensive knowledge of the network and can utilise this knowledge to uncover potential vulnerabilities. IoT penetration testing often includes device security, cloud API security, network security, device firmware security and device application security.

The author (Chu & Lisitsa, 2019), suggests that the IoT penetration testing process is carried out in 4 phases, namely the information phase, collection, exploitation analysis and reporting. The collection of information done at the initial stage is a critical step that will determine the success of penetration testing from all three IoT structural layer (perception, network, and application). During the analysis step, information about the target must be compiled, processed, and then a plausible attack method and plan to achieve target access privileges must be differentiated. The validity research must next be conducted in this experimental environment. The actual attack is carried out at the exploitation level depending on the attack path and planning done at the analysis level. Ensure vulnerabilities during test simulations against target owners at the reporting level. This data will then be utilised to improve future security. **Figure 1** shows the IoT penetration testing procedure.

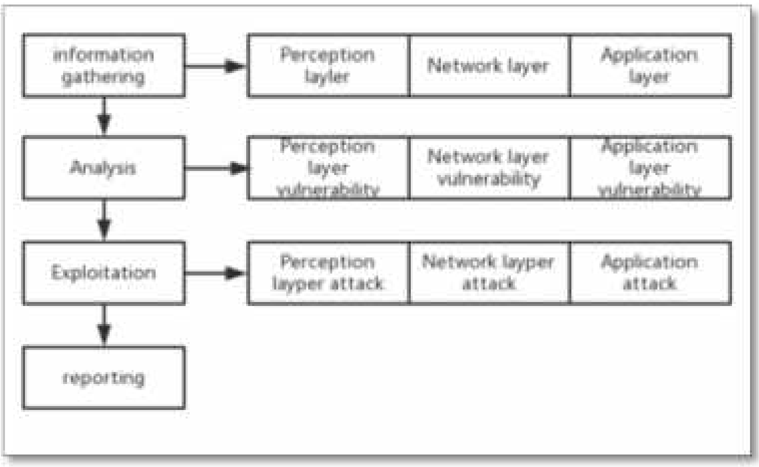

Figure 1 : The Process of IoT Penetration Testing (Chu & Lisitsa, 2019).

Web Application Penetration Testing

Web application penetration testing is a way of analysing a web application's security by simulating an attack from a hostile hacker. The purpose of web application penetration testing is to find vulnerabilities and flaws in the programme that an attacker may exploit to obtain unauthorised access to sensitive information or cause harm to the system. A web application is a critical necessity in the information and digitalization era. Web applications move through quick development phases with short turnaround periods, making it difficult to eradicate vulnerabilities. The penetration testing approach may be used to examine an online application's vulnerability.

There are two methods for performing web application penetration testing: black-box testing and white-box testing. The tester in black-box testing does not know the inner workings of the web application and is supposed to imitate an attacker looking for vulnerabilities from the outside. White-box testing allows the tester complete access to the application's source code and architecture, allowing for a more thorough examination of the application's security. Using the black box approach, the researcher (Alanda *et al*., 2021) tests online application security against the Open Web Application Security Project's (OWASP) list of the most prevalent threats, namely SQL Injection. SQL injection is a type of attack that is commonly used to compromise an online application. The attacker executes SQL instructions using input variables in the web application to carry out this attack. It affects key security services in terms of confidentiality, authentication, authorization, and integrity (Chen *et al*., 2021).

Web application penetration testing is a vital component of a complete security programme since it assists in identifying and addressing possible security problems before attackers can exploit them. Organisations may lower their risk of a data breach or other security event while still maintaining the confidence of their customers and users by conducting frequent penetration testing.

4. Challenge in Penetration Testing

Keeping Up with New and Evolving Threats

Penetration testing is an essential component of any organisation's cybersecurity strategy since it identifies vulnerabilities and weaknesses in systems before attackers can use them. However, with new and developing threats arriving all the time, penetration testers may find it difficult to keep up with the current security vulnerabilities. The rising complexity of systems, networks, and applications is a huge challenge. As technology progresses and the Internet of Things (IoT) expands, businesses' attack surface area grows, making it increasingly difficult to analyse the security of all systems and guarantee that they are appropriately safeguarded. This is especially true for IoT devices, which are frequently poorly secured and hence a prime target for attackers.

Another challenge is the ongoing growth of hacker attack methods and strategies. This means that penetration testers must stay current on security threats and be able to quickly react to new and developing attack tactics. They must also be able to assess the security of new and innovative technologies, such as cloud-based services, which can introduce new security concerns that must be handled (Bai *et al*., 2011). Furthermore, attackers' increased use of artificial intelligence (AI) and machine learning (ML) technologies provides difficulty for penetration testers. These technologies can be used to automate assaults and make them more sophisticated and difficult to detect, necessitating a deeper grasp of AI and ML and how they can be employed in an attack by penetration testers.

Addressing the Shortage of Qualified Security Professionals

Many firms experience a dearth of trained security personnel in the field of penetration testing. The rising need for cybersecurity measures has resulted in a growth in the demand for competent security experts, but the supply of qualified workers has not kept pace. Designing an effective educational program for individuals seeking to enhance their cybersecurity skills is challenging due to several limitations. Institutions offering such programs often face limited resources for creating a suitable learning environment, limited teacher time for maintaining the system, and inadequate administrative support due to a lack of understanding of the importance of cybersecurity skills. Misuse of tools and skills can also hinder the growth of a cybersecurity program. As a result, the curriculum may become excessively theoretical, with insufficient focus on developing practical skills required for professionals (Whipple *et al*., 2015).

As cyber threats become more advanced, organizations are struggling to find skilled cybersecurity professionals to protect their systems from malicious attacks. Cybercriminals cause billions of dollars in losses each year, while state-sponsored hacking groups pose an even greater threat. Therefore, the demand for professionals who can secure networks against attackers is higher than ever. However, educational and training institutions are struggling to keep up with the demand for cyber talent (Crumpler & Lewis, 2019).

Ensuring the Accuracy and Reliability of Testing Results

There are various concerns that might affect the accuracy and reliability of penetration testing results:

i. Inadequate testing coverage: It is necessary to conduct extensive testing that includes all critical components and systems. Any overlooked regions or weaknesses might lead to inaccurate results and perhaps false negatives.

ii. Human error: Because penetration testers are human, they are prone to errors such as inaccurate data entry or misunderstanding of results. This can lead to untrustworthy outcomes.

iii. Lack of standardisation: Each tester may use a distinct testing technique, resulting in diverse and inconsistent outcomes across tests.

iv. Use of outdated testing tools: Technology evolves quickly, and older testing techniques may be incapable of detecting new vulnerabilities or effectively evaluating newer systems.

v. Use of obsolete testing tools: Technology evolves quickly, and older testing methods may be unable to uncover new vulnerabilities or test newer systems effectively.

vi. Biased results: The tester's objectives and biases might influence test findings, potentially leading to incorrect results. A tester, for example, may not disclose a vulnerability if they feel it is minor.

Balancing Security and Privacy Concerns

In penetration testing, balancing security and privacy considerations is a big challenge. On the one hand, businesses must guarantee that their systems and networks are protected from cyber-attacks and data breaches. On the other hand, they must preserve their customers' and workers' privacy. Penetration testers may get access to sensitive data and personal information during a penetration test, raising privacy concerns. During the testing process, it is critical to guarantee that all data is handled securely, and that privacy rules and regulations are followed. As stated by (Archibald & Renaud, 2019), the authors advocated for the development of cybersecurity frameworks that prioritise ethical considerations and protect user privacy. They proposed a modification of the PoinTER (Prepare TEst Report) Human Pentesting Framework that aligns with the General Data Protection Regulation (GDPR) and respects privacy.

5. Discussion

Integrating Penetration Testing into the overall security strategy involves considering it as a crucial component of a comprehensive security plan and incorporating it into regular security assessments. Improving the quality and effectiveness of Penetration Testing can be achieved through the use of advanced testing techniques, tools, and methodologies. Collaborating with industry partners and stakeholders can help organisations share best practices, knowledge, and resources to enhance security posture. Investing in research and development to address emerging challenges is crucial to stay ahead of evolving threats and continuously improve penetration testing methods and technologies. By following these strategies, organisations can effectively strengthen their cybersecurity posture through penetration testing.

Integrating Penetration Testing

For an organisation's cybersecurity initiatives to be effective and efficient, integrating penetration testing into the overall security plan is a critical step. Penetration testing evaluates the security of a computer system or network by simulating a real-world cyber-attack. It can identify vulnerabilities, determine the potential impact of a successful attack, and help organisations prioritize their security efforts. By incorporating penetration testing into their overall security strategy, organisations can gain a comprehensive understanding of their security posture and determine areas that require improvement.

When integrated into the security strategy, penetration testing should be conducted regularly to identify new and emerging threats. Organisations should also consider a variety of testing methods, including internal and external testing, and use a combination of manual and automated testing tools to achieve the most thorough and accurate results. Due to penetration testing's growing importance as a method for identifying vulnerabilities in computer networks, tools that automate the process of identifying and mitigating vulnerabilities are required (Filiol *et al*., 2021). To ensure the effectiveness of penetration testing, it should be performed by trained security professionals who understand the organisation's specific security needs and requirements. Integrating penetration testing into the overall security strategy also requires collaboration between various departments, such as security, operations, and development, to ensure that all stakeholders understand the importance of testing and are involved in the process. This can also help organisations prioritize their security efforts and make informed decisions about where to allocate resources.

Enhancing Penetration Testing

There are several ways to enhance the quality and effectiveness of penetration testing, including the use of advanced testing techniques, tools, and methodologies. One way to improve the quality of penetration testing is to use a combination of manual and automated testing methods. Automated testing can be used to identify basic vulnerabilities quickly, while manual testing can be used to confirm and further explore the results of automated testing. This can help organisations comprehensively understand their security posture and identify known and unknown vulnerabilities.

Another way to enhance the quality of penetration testing is to use a variety of testing methodologies. For example, organisations can use both black-box and white-box testing to evaluate the security and quality of their systems (Hamza & Hammad, 2019). Black-box testing simulates a real-world cyber-attack, while white-box testing provides a detailed examination of the underlying code and architecture. Utilizing both methodologies can provide organisations with a more comprehensive understanding of their security posture. (Rohela, 2018) has developed a framework to simplify penetration testing and security hardening tasks by leveraging advanced technologies such as AI, cloud computing, and big data. The framework utilizes AI to establish connections between collected data, identify vulnerabilities in the configuration or versions of assets, and suggest or execute exploits to test asset hardening. The cloud serves as the platform for processing and storing data, while big data is used for managing AI training datasets. This framework allows for a more efficient and effective approach to penetration testing and security hardening by automating many of the processes involved, and leveraging cutting-edge technologies to improve accuracy and reliability.

According to (Ghanem & Chen, 2020) study, an AI-based system called Intelligent Automated Penetration Testing System (IAPTS) has been proposed and evaluated. This system uses reinforcement learning (RL) techniques to learn and reproduce average and complex pentesting activities. IAPTS includes a module that can be integrated with industrial PT frameworks, allowing it to capture information, learn from experience, and replicate tests in similar future testing cases. The purpose of IAPTS is to improve the efficiency and accuracy of penetration testing by reducing the need for human resources and increasing the frequency of testing. The proposed system promises to produce better results in terms of time consumption and reliability.

In addition to utilizing advanced testing techniques, organisations should also invest in the training and development of their security professionals. Training can be delivered on-site or remotely, employing a mentorship method, live simulation, red-team/blue-team activities, or cloud computing for cybersecurity instruction (Gkioulos & Chowdhury, 2021). This can help ensure that the individuals performing penetration testing have the necessary skills and knowledge to effectively identify and mitigate security risks. Organisations should also consider hiring third-party security firms to perform penetration testing, as these firms often have the expertise and resources to perform more thorough testing.

Smart Collaboration

Organisational performance may be influenced by incorporating the assistance, cooperation, and partnership of relevant stakeholders (Awan *et al*., 2021). Collaborating with industry partners and stakeholders can help organisations share best practices, knowledge, and resources to enhance their security posture. One way to collaborate with industry partners is to participate in industry-wide penetration testing initiatives. These initiatives can provide organisations with the opportunity to compare their security posture to that of other organisations in their industry, identify areas for improvement, and learn from the experiences of others. Additionally, participating in these initiatives can help organisations stay informed about the latest trends and challenges in the field of cybersecurity, and stay ahead of emerging threats.

Another way to collaborate with industry partners is to engage in information sharing and analysis. This can help organisations exchange information about security threats, vulnerabilities, and best practices, and work together to identify and mitigate potential risks. Information sharing and analysis can also help organisations stay informed about the latest trends and challenges in the field of cybersecurity and stay ahead of emerging threats. (Tounsi & Rais, 2018) states, organisations are increasingly moving to the cloud, which is causing changes in indicators of compromise (IOC). This shift means that organisations need to better protect their data, which is now accessible through email accounts, web applications, documents stored on cloud systems, and mobile devices.

Threat intelligence (TI) has become increasingly important in this area as it can help organisations discover covert cyber-attacks and new malware, provide early warnings, and selectively distribute TI data. According to (Zenebe *et al*., 2019), cyber threat intelligence refers to any useful information, knowledge, or insights about potential threats that can aid in preventing security breaches in digital environments. The identification of cyber threat intelligence can help organisations take proactive measures to safeguard their systems. By detecting threats before they become an issue, security measures can be strengthened to prevent cyber-attacks. In addition to collaborating with industry partners, organisations should also engage with stakeholders, such as customers and regulatory bodies, to ensure that their security posture meets their specific requirements and expectations. This can help organisations ensure that they are effectively protecting sensitive information and maintaining the trust of their stakeholders.

Investing in R&D for Emerging Challenges

Addressing current issues in cybersecurity, especially in the area of penetration testing, requires significant investment in research and development. As technology evolves, organisations must be proactive in developing new tools and techniques to detect and mitigate new threats and vulnerabilities. (McIntosh *et al*., 2022) stated the rise in cyber threats has resulted in a rapid increase in research aimed at understanding and mitigating these attacks. The research will cover different aspects, including identifying known threats, protecting systems from unauthorized modifications or access, and stopping attacks on targets. However, despite these efforts, cyber criminals continue to find new ways to bypass existing security measures. They have discovered new attack methods and platforms that make it easier to defeat current mitigation techniques.

One-way organisations can invest in research and development is by establishing internal research and development teams. These teams can focus on developing new tools and techniques for identifying and mitigating security risks, as well as exploring new methods for conducting penetration testing. By investing in internal research and development, organisations can stay ahead of emerging threats and maintain a competitive advantage in the field of cybersecurity. Another way organisation can invest in research and development is by partnering with academic institutions and research organisations. These partnerships can provide organisations with access to the latest research and development in the field of cybersecurity, as well as the opportunity to collaborate with experts in the field (Gkioulos & Chowdhury, 2021). Additionally, academic partnerships can provide organisations with the opportunity to participate in research initiatives and contribute to the advancement of the field of cybersecurity.

6. Conclusion

In conclusion, the importance of penetration testing in strengthening cybersecurity cannot be overstated. Organisations may find vulnerabilities in their security posture and weaknesses by simulating actual attacks, and then rectify those gaps before attackers take advantage of them. The key strategies for strengthening cybersecurity through penetration testing include integrating penetration testing into the overall security strategy, improving the quality and effectiveness of penetration testing, collaborating with industry partners and stakeholders, and investing in research and development to address emerging challenges. Looking to the future, the field of cybersecurity and penetration testing is expected to continue to evolve as new technologies are developed and new threats emerge. Organisations must stay informed about the latest trends and challenges in the field and continuously evaluate and improve their security posture to stay ahead of emerging threats.

7. Acknowledgment

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by Universiti Utara Malaysia.

References

Al-Ahmad, A. S., Kahtan, H., Hujainah, F., & Jalab, H. A. (2019). Systematic Literature Review on Penetration Testing for Mobile Cloud Computing Applications. *IEEE Access*, *7*, 173524–173540. https://doi.org/10.1109/ACCESS.2019.2956770

Alanda, A., Satria, D., Ardhana, M. I., Dahlan, A. A., & Mooduto, H. A. (2021). Web application penetration testing using sql injection attack. *International Journal on Informatics Visualization*, *5*(3), 320–326. https://doi.org/10.30630/joiv.5.3.470

Archibald, J. M., & Renaud, K. (2019). Refining the PoinTER “human firewall” pentesting framework. *Information and Computer Security*, *26*(4), 575–600. https://doi.org/10.1108/ICS-01-2019-0019

Awan, U., Sroufe, R., & Shahbaz, M. (2021). Industry 4.0 and the circular economy: A literature review and recommendations for future research. *Business Strategy and the Environment*, *30*(4), 2038–2060. https://doi.org/10.1002/bse.2731

Bai, X., Li, M., Chen, B., Tsai, W. T., & Gao, J. (2011). Cloud testing tools. *Proceedings - 6th IEEE International Symposium on Service-Oriented System Engineering, SOSE 2011*, *August 2020*, 1–12. https://doi.org/10.1109/SOSE.2011.6139087

Beattie, S., & Goodwill, S. (2018). A study of penetration testing. Journal of Cybersecurity Education, Research and Practice, 2018(1), 13-29.

Chen, D., Yan, Q., Wu, C., & Zhao, J. (2021). SQL Injection Attack Detection and Prevention Techniques Using Deep Learning. *Journal of Physics: Conference Series*, *1757*(1). https://doi.org/10.1088/1742-6596/1757/1/012055

Chu, G., & Lisitsa, A. (2019). Penetration Testing for Internet of Things and Its Automation. *Proceedings - 20th International Conference on High Performance Computing and Communications, 16th International Conference on Smart City and 4th International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2018*, *February*, 1479–1484. https://doi.org/10.1109/HPCC/SmartCity/DSS.2018.00244

Crumpler, W., & Lewis, J. A. (2019). The Cybersecurity Workforce Gap. *Center for Strategic and International Studies (CSIS)*, *July 2016*, 1–10. http://www.isaca.org/Knowledge-Center/

Ezzati, R., & Zakerolhosseini, A. (2018). Penetration testing: a review of the state of the art. International Journal of Computer Science and Information Security, 16(1), 19-28.

Filiol, E., Mercaldo, F., & Santone, A. (2021). A method for automatic penetration testing and mitigation: A Red Hat approach. *Procedia Computer Science*, *192*, 2039–2046. https://doi.org/10.1016/j.procs.2021.08.210

Ghanem, M. C., & Chen, T. M. (2020). Reinforcement learning for efficient network penetration testing. *Information (Switzerland)*, *11*(1), 1–23. https://doi.org/10.3390/info11010006

Gkioulos, V., & Chowdhury, N. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

Gonzalez, J., Garcia, S., & Clark, J. (2019). A comparative study of penetration testing methodologies. Journal of Cybersecurity Education, Research and Practice, 2019(1), 41-58.

Hamza, Z. A., & Hammad, M. (2019). Web and mobile applications' testing using black and white box approaches. *IET Conference Publications*, *2019*(CP758), 20–23. https://doi.org/10.1049/cp.2019.0210

Heiding, F., Süren, E., Olegård, J., & Lagerström, R. (2023). Penetration testing of connected households. *Computers and Security*, *126*. https://doi.org/10.1016/j.cose.2022.103067

Hu, T., Zhou, T., Zang, Y., Wang, Q., & Li, H. (2020). APU-D* lite: Attack planning under uncertainty based on D* lite. *Computers, Materials and Continua*, *65*(2), 1795–1807. https://doi.org/10.32604/cmc.2020.011071

Matheu-García, S. N., Hernández-Ramos, J. L., Skarmeta, A. F., & Baldini, G. (2019). Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. *Computer Standards and Interfaces*, *62*, 64–83. https://doi.org/10.1016/j.csi.2018.08.003

McIntosh, T., Kayes, A. S. M., Chen, Y. P. P., Ng, A., & Watters, P. (2022). Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. *ACM Computing Surveys*, *54*(9). https://doi.org/10.1145/3479393

Rohela, A. (2018). Vulnerability Assessment and Penetration Testing through Artificial Intelligence. *International Journal of Recent Trends in Engineering and Research*, *4*(1), 217–224. https://doi.org/10.23883/ijrter.2018.4028.rdd10

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

Whipple, A., Smith, K. B., Rowe, D. C., & Moses, S. (2015). Building a vulnerability testing lab in an educational environment. *ASEE Annual Conference and Exposition, Conference Proceedings*, *122nd ASEE*(122nd ASEE Annual Conference and Exposition: Making Value for Society). https://doi.org/10.18260/p.23640

Zenebe, A., Shumba, M., Carillo, A., & Cuenca, S. (2019). Cyber Threat Discovery from Dark Web. *EPiC Series in Computing*, *64*, 174–183.