Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 46 No. 4
April 2025

The Importance of Vulnerability Assessment & Penetration Testing in Cyber Defense

Kifory Lamine Kone[1*]

[1]MD, Master of Computer Applications (MCA) Department, Faculty of IT & Computer Science, Parul university, P.O.Limda, Ta. Waghodia- 391760 Dist. Vadodara, Gujarat

Corresponding Email : kiforylaminekoneprofessional@gmail.com

Djomou Aquilas Lieumou[2]

[2]MD, Master of Computer Applications (MCA) Department, Faculty of IT & Computer Science, Parul university, P.O. Limda, Ta. Waghodia- 391760 Dist. Vadodara, Gujarat

Email Id: karteuraquilas@gmail.com

Faruk Abdulla[3]

[3]Assistant Professor, Master of Computer Applications (MCA) Department, Faculty of IT & Computer Science, Parul university, P.O. Limda, Ta. Waghodia- 391760 Dist. Vadodara, Gujarat

Email Id: faruk.abdulla30274@paruluniversity.ac.in

ABSTRACT

In the swiftly advancing digital environment, cyber threats have grown more intricate, presenting substantial dangers to both enterprises and individuals. Cybersecurity strategies, including Vulnerability Assessment (VA) and Penetration Testing (PT), are essential for detecting and addressing security vulnerabilities prior to exploitation by malevolent entities. This study investigates the significance of VA and PT in enhancing cyber security tactics, emphasizing their function in safeguarding digital assets, reducing cyber risks, and guaranteeing adherence to regulatory standards. The study seeks to elucidate how proactive security measures improve overall cybersecurity by discovering system vulnerabilities, evaluating attack vectors, and executing effective mitigation tactics. A qualitative research methodology is employed, utilizing secondary data gathered from 2018 to 2025, encompassing academic literature, industry reports, case studies, and cybersecurity frameworks. The results underscore the efficacy of VA and PT in mitigating data breaches, diminishing the attack surface, and improving incident response capabilities. Conversations highlight the difficulties in executing VAPT tactics, including the necessity for proficient personnel, ongoing surveillance, and alignment with evolving cybersecurity paradigms like Zero Trust Architecture and AI-enhanced security measures. The study indicates that firms should integrate regular Vulnerability Assessments and Penetration Testing into their cybersecurity risk management plan to proactively minimize cyber threats. This research highlights the imperative for ongoing security evaluations, adherence to cybersecurity rules, and the implementation of automated and AI-driven VAPT solutions for a resilient cyber defence in the changing threat environment.

Keywords: *Cyber Security, Vulnerability Assessment, Penetration Testing, Cyber Defence, Web Applications*

INTRODUCTION

In the digital era, cybersecurity has emerged as a fundamental component of contemporary technological infrastructure, safeguarding the confidentiality, and integrity, along with availability of data across multiple domains. As enterprises increasingly depend on digital platforms, cloud computing, and interconnected networks, the risk of cyber assaults has escalated significantly. Organizations, authorities, and individuals encounter considerable cybersecurity concerns

stemming from the swift evolution of technologies and the surge of intricate assaults [1, 2]. A solitary security breach may result in significant financial losses, and reputational harm, legal penalties, and potential national security threats. The growing reliance on e-commerce, online banking, smart

technology, and industrial control systems (ICS) has rendered cybersecurity an essential element of digital transformation. Therefore, firms must implement proactive security measures to safeguard critical information and maintain continuous operations. Conventional cybersecurity protections, including firewalls, and antivirus software, along with intrusion detection systems (IDS), are inadequate for countering advancing threats [3, 4]. Continuous risk assessment, vulnerability detection, and security validation are essential for sustaining a strong cybersecurity posture.

Organizations face phishing, ransomware, DDoS, SQL injection, XSS, and insider dangers due to rising cyber threats. To avoid detection and exploit system weaknesses, cybercriminals constantly innovate attack techniques using AI, deepfake technology, and advanced malware. Attackers exploit software, network, web app, and IoT vulnerabilities, therefore organizations must detect and resolve them. Data breaches like the Equifax breach, SolarWinds attack, and Colonial Pipeline ransomware outbreak highlight the need for strong cybersecurity. Enterprises must rely on reactive security methods as cyber threats increase [5, 6]. Instead, they must use proactive, intelligence-driven techniques to identify and fix weaknesses before hackers do. VA and PT are excellent cybersecurity strategies. Security specialists must use these two methodologies to find vulnerabilities in IT infrastructures, applications, and networks to prevent exploitation. Vulnerability Assessment meticulously checks systems for security vulnerabilities, misconfigurations, and outdated software that adversaries could exploit. To assess an organization's security against infiltration, penetration testing simulates cyberattacks. Cybersecurity approach with VA and PT improves risk management, regulatory compliance, and security [6, 7]. These proactive methods help organizations detect security weaknesses, prioritize risks, and take corrective action to avoid cyber crises. As cyber threats develop, VA and PT become more important in cyber defence, giving organizations a powerful strategy to safeguard their digital assets, decrease cyber risks, and remain resilient to evolving attacks [6, 7]. The figure 1 explains the Work flow of VAs and PT in detail.

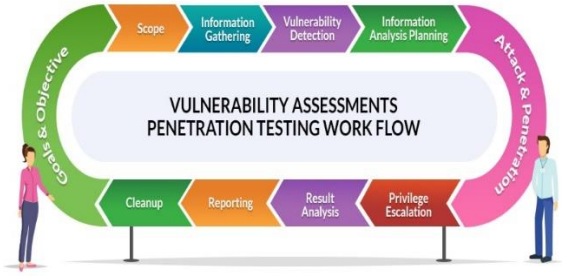

Figure 1. Work flow of Vulnerability Assessments and Penetration Testing – An overview[1]

This study investigates how VA and PT find, analyse, and fix security problems to improve cyber defence. Proactive security helps organizations protect their digital assets from cyberattacks, improve security resilience, and meet legal obligations. This also article examines VA and PT strategies, tools, and real-world implementations to limit the attack surface, avoid security breaches, and improve cybersecurity.

Vulnerability Assessments

Vulnerability Assessment (VA) is a methodical procedure for finding, analysing, and prioritizing security vulnerabilities in an organization's IT infrastructure, networks, applications, and digital assets. It seeks to spot vulnerabilities that may be exploited by cyber assailants, offering firms practical insights to alleviate security threats prior to compromise. The principal objective of VA is to improve an organization's security stance by proactively detecting vulnerabilities, minimizing the attack surface, and assuring adherence to cybersecurity standards and best practices. In contrast to reactive security measures that emphasize incident response, VA adopts a proactive strategy that allows firms to foresee possible threats and execute appropriate remedial steps [7, 8]. By persistently evaluating systems for weaknesses, firms can anticipate evolving cyber threats and avert future breaches. Vulnerability assessment is a crucial element of a holistic cybersecurity strategy, offering a systematic tact to

[1] https://www.aristatechnologies.ca/vulnerability-assessment-penetration-testing.php

spotting weaknesses inside network settings, operating systems, web applications, databases, and cloud environments. Vulnerability assessments can be classified into many types according to the evaluation scope and the individual elements under analysis. Each assessment type concentrates on distinct facets of an organization's IT infrastructure to guarantee a comprehensive security examination. The principal categories of vulnerability assessments are network-based, host-based, application-based, and cloud/IoT-based evaluations [8]. Assessments are performed via automated scanning techniques, manual analysis, and a hybrid approach to deliver a comprehensive understanding of security vulnerabilities. The figure 2 below illustrates the overview of vulnerability assessment in detail.

Figure 2. Vulnerability Assessment in cyber defence – An overview[2]

An organization's routers, switches, firewalls, and network-connected devices are examined in a network-based vulnerability assessment. It helps security teams find misconfigurations, unprotected ports, outdated protocols, and unpatched services that attackers may exploit. Network-based evaluations use Nessus, OpenVAS, and Qualys to scan internal and external networks. Mitigating cyber threats like man-in-the-middle (MITM) attacks, and denial-of-service (DoS) attacks, along with unauthorized access to critical network resources requires these evaluations. Servers, workstations, and endpoints are assessed for vulnerabilities using host-based vulnerability assessments [9, 10]. It targets operating system, application, and security configuration vulnerabilities. Privilege escalation, outdated software, poor authentication, and unresolved system vulnerabilities must be identified throughout this exam. Security teams use host-based vulnerability scanners like MBSA and Nexpose to find vulnerabilities and provide fixes.

Application-based vulnerability evaluations are vital to cybersecurity as web apps and software services become more prevalent. Web apps, APIs, and software applications are tested for SQL injection, cross-site scripting (XSS), failed authentication, and unsafe direct object references. Burp Suite, OWASP ZAP, and Acunetix are used for static and dynamic application security testing (SAST & DAST) to find vulnerabilities and improve security. As companies go to the cloud and connect IoT devices, new security issues arise. Cloud vulnerability assessments look for misconfigurations, poor access controls, and susceptible APIs in AWS, Azure, and GCP [10, 11, 12]. IoT vulnerability evaluations examine the security of networked smart devices, sensors, and industrial control systems (ICS), which fraudsters attack owing to poor security. To efficiently assess cloud and IoT security vulnerabilities, CIS Cloud Benchmarks and IoTSF Guidelines are used. Organisations use automated scanning techniques and security frameworks to assess vulnerabilities. Nessus, Qualys, OpenVAS, Rapid7 Nexpose, Burp Suite, and Nikto are popular vulnerability scanners. Security teams may scan IT assets for vulnerabilities and generate detailed remediation reports with these tools. The NIST Cybersecurity Framework, MITRE ATT&CK, and OWASP Top 10 provide systematic guidelines for identifying and fixing security vulnerabilities [11, 12].

Challenges in Conducting Effective Vulnerability Assessments

Notwithstanding the benefits of VAs, companies encounter numerous obstacles in their effective implementation. A significant difficulty is the

[2] https://www.maltego.com/blog/common-pitfalls-to-avoid-in-vulnerability-risk-assessments/

occurrence of false positives and false negatives, wherein vulnerability scanners may erroneously identify secure components as vulnerabilities or neglect to recognize actual security threats. This may result in the misallocation of security resources and prolonged repair periods. Patch management presents a significant difficulty, since numerous firms encounter difficulties in swiftly applying security patches due to operational limits and compatibility concerns. Moreover, scalability and complexity present considerable challenges, particularly for large organizations with massive IT infrastructures and numerous interconnected systems. Adhering to regulatory mandates like GDPR, HIPAA, and PCI-DSS introduces additional complexity to vulnerability assessments. The ongoing shortage of skilled cybersecurity personnel is a significant challenge, as firms need educated experts to analyse vulnerability scan results, prioritize risks, and execute suitable security solutions [10, 11]. By tackling these difficulties and combining automated vulnerability assessments with manual security evaluations, organizations may bolster their cybersecurity resilience and safeguard their digital assets against growing cyber-attacks.

Penetration Testing (Pt)

PT, commonly called ethical hacking, is a simulated cyberattack performed to assess an organization's IT infrastructure's security. In contrast to vulnerability assessment, which aims to find security holes, penetration testing actively exploits these vulnerabilities to evaluate their real-world implications and analyse potential methods of system infiltration by an attacker. The principal aim of PT is to detect security vulnerabilities, assess the efficacy of current security protocols, and offer practical recommendations to reduce risks prior to exploitation by malevolent hackers. It assists enterprises in evaluating their security posture, identifying misconfigurations, testing incident response capabilities, and ensuring compliance with industry laws including GDPR, HIPAA, and PCI-DSS [12, 13]. Ethical hackers employ penetration testing to replicate the methods of actual cybercriminals, thereby offering critical insights into possible attack paths and enhancing overall cybersecurity resilience.

Penetration testing can be categorized into distinct forms according to the testers' knowledge of the system and the particular attack surface under assessment. The three principal categories are Black Box, and White Box, along with Gray Box testing.

1. Black Box Testing: In this methodology, testers possess no prior grasp of the internal architecture of the target system. They replicate an external hacker's attempt to infiltrate the system without insider knowledge, hence providing valuable insights for evaluating authentic attack scenarios.
2. White Box Testing: Testers possess comprehensive understanding of the system, encompassing network architecture, source code, and security configurations. This method is frequently employed for comprehensive security evaluations of apps and infrastructure to identify deeply ingrained vulnerabilities.
3. Gray Box Testing: This is a hybrid methodology wherein testers possess partial knowledge of the system, emulating attacks from an insider or a malicious user with a certain degree of access. It offers a comprehensive assessment of both external and internal security threats.

Moreover, penetration testing can be classified into External and Internal Testing. External penetration testing concentrates on evaluating publicly accessible systems, including online apps, APIs, and corporate networks, to discover potential entry routes for attackers. Conversely, internal penetration testing assesses security vulnerabilities from within the organization's internal network, simulating attacks posed by malicious workers or hacked user accounts [13, 14].

A penetration test adheres to a systematic process comprising several phases, each enhancing the comprehensive evaluation of security vulnerabilities.

1. Planning and Reconnaissance: This step entails the collection of intelligence regarding the target system, including domain names, IP addresses, employee email addresses, and publicly accessible information, to ascertain probable entry points. Open-source intelligence (OSINT)

instruments such as Shodan, Maltego, and Google Dorking are frequently employed.

2. Scanning and Enumeration: During this phase, testers systematically scan the target system to spot open ports, active services, and vulnerabilities. Instruments like Nmap, Nessus, and Nikto assist in detecting vulnerable security setups and possible attack paths.

3. Exploitation and Access Acquisition: The reported vulnerabilities are leveraged through many hacking methodologies, including SQL injection, XSS, and buffer overflow attacks. Ethical hackers employ tools such as Metasploit and Burp Suite to replicate attacks and breach the system.

4. Privilege Escalation and Post-Exploitation: Following initial access, attackers seek to elevate privileges by leveraging misconfigurations, inadequate credentials, or unpatched software vulnerabilities. The objective is to ascertain the extent of an attacker's infiltration into the system and the vital data that can be accessed.

5. Reporting and Remediation: Upon completion of the test, findings are recorded in a comprehensive report that include identified vulnerabilities, exploitation techniques, risk evaluations, and suggested security protocols. This phase is essential for enterprises to apply requisite updates, revise security policies, and strengthen overall cybersecurity measures [15, 16].

Through rigorous penetration testing, businesses may proactively spot and rectify security weaknesses, thereby mitigating the risk of cyberattacks, enhancing incident response, and fortifying their overall security posture.

Importance of Vulnerability Assessment and Penetration Testing in Cyber Defence

VA and PT are essential in cyber defence, allowing firms to proactively spot and address security vulnerabilities prior to exploitation by criminal actors. Cyber dangers are ever advancing, rendering conventional security methods like firewalls and antivirus software inadequate for safeguarding against complex attacks. Vulnerability assessment identifies security deficiencies in an organization's digital infrastructure, whereas penetration testing advances this process by simulating actual attack scenarios to evaluate the efficacy of current security measures. By detecting vulnerabilities early, firms can mitigate risks before they result in data breaches, financial losses, or operational interruptions [17, 18]. This proactive strategy diminishes the probability of cyber events, lowers downtime, and fortifies the resilience of IT systems against evolving threats.

A vital component of VAPT is its function in minimizing the attack surface in both IT (Information Technology) and OT (Operational Technology) environments. Information Technology systems, encompassing networks, databases, and online applications, are often targeted by cybercriminals, although Operational Technology systems, including industrial control systems (ICS) and Internet of Things (IoT) devices, are progressively emerging as attack vectors. An effectively organized VAPT program identifies and secures all potential entry points for attackers, thereby reducing security risks inside digital ecosystems. Furthermore, VAPT improves incident response and threat intelligence by offering critical insights into system vulnerabilities and attack methodologies [18, 19]. Security teams can utilize penetration test outcomes to enhance their threat detection abilities and optimize their response techniques, so assuring a more formidable defence against cyber threats.

Moreover, VAPT is crucial for adhering to compliance and regulatory standards, like ISO 27001, NIST, GDPR, HIPAA, and PCI-DSS, which mandate enterprises to do frequent security evaluations. Regulatory compliance not only mitigates legal and financial repercussions but also enhances customer trust and organizational credibility. Ultimately, VAPT is crucial for safeguarding essential infrastructure and digital assets, encompassing financial institutions, healthcare systems, government networks, and cloud environments [19, 20]. Through the ongoing evaluation and enhancement of security protocols, firms may secure critical information, defend against cyber espionage, and maintain operational continuity in a more digital landscape.

Integration of Vapt in Cyber Security Strategy

Incorporating VA and PT into an organization's cybersecurity strategy is crucial for establishing a robust defence against advancing cyber threats. Although both VA and PT aim to find security

vulnerabilities, they differ in their methodology and objectives. Vulnerability Assessment is a comprehensive, automated procedure aimed at scanning and discovering security deficiencies within an organization's network, and applications, along with systems. It offers a comprehensive enumeration of possible vulnerabilities but refrains from exploiting them. Conversely, Penetration Testing emulates genuine cyberattacks by proactively seeking to exploit vulnerabilities, so aiding firms in comprehending the true danger associated with security deficiencies. By integrating both methodologies, businesses can detect vulnerabilities and evaluate their consequences, thereby establishing a proactive and risk-oriented security strategy.

An essential factor in VAPT deployment is the equilibrium between automated and manual testing methodologies. Automated tools like Nessus, OpenVAS, and Qualys may effectively scan systems for recognized vulnerabilities and misconfigurations, rendering them suitable for routine evaluations. Nonetheless, manual penetration testing conducted by ethical hackers is crucial for detecting logic-based vulnerabilities, zero-day threats, and security issues that automated techniques could miss. A hybrid strategy, utilizing automation for efficiency and human knowledge for thoroughness, guarantees a strong security stance.

Notwithstanding its benefits, firms encounter numerous obstacles in executing VAPT plans, such as elevated expenses, a deficiency of skilled personnel, and complications in integration. Numerous firms lack qualified security personnel to do comprehensive testing and accurately interpret results. Moreover, performing regular penetration tests may interfere with corporate activities, necessitating meticulous scheduling. Compliance and regulatory mandates introduce complexity, necessitating that firms maintain ongoing surveillance while conforming to security standards [21, 22]. Organizations must invest in AI-driven security solutions, automated testing tools, and proficient cybersecurity personnel to effectively incorporate VAPT into their cybersecurity architecture and enhance overall cyber resilience.

Securing Digital Assets with Vulnerability Assessment & Penetration Testing

As enterprises increasingly depend on digital infrastructure for the storage, processing, and transmission of sensitive data, the necessity for stringent security measures has become critical. VA and PT function as proactive security strategies to safeguard digital assets against various cyber-attacks. Digital assets, including as web applications, networks, cloud environments, IoT devices, and Industrial Control Systems (ICS), are primary targets for attackers aiming to exploit weaknesses for financial profit, espionage, or system disruption [23]. Implementing VAPT guarantees ongoing surveillance, identification, and rectification of security vulnerabilities across multiple domains, substantially mitigating the threat of data breaches, service interruptions, and unauthorized access.

VAPT for Web Application Security

Web applications function as the principal interface for user engagement, rendering them a common target for cyberattacks. Common security vulnerabilities in online applications, as delineated by OWASP's Top 10, encompass SQL Injection, XSS, Cross-Site Request Forgery (CSRF), and Remote Code Execution (RCE). These vulnerabilities may result in data breaches, session hijacking, and complete system penetration if not adequately mitigated. Organizations can discover and manage threats with VAPT by doing automated vulnerability scans and manual penetration tests. SQL Injection may be averted by employing parameterized queries and web application firewalls (WAFs), whilst XSS assaults can be reduced through input validation and Content Security Policies (CSPs). By implementing secure coding techniques, conducting frequent security audits, and utilizing real-time monitoring, businesses may strengthen their web apps against cyber-attacks and improve user confidence [24].

VAPT for Network Security

Network security constitutes the cornerstone of an organization's cybersecurity strategy, regulating data transit, system access, and remote connectivity. An inadequately secured network architecture offers attackers numerous access

points to exploit weaknesses. VAPT assists in detecting network vulnerabilities by evaluating firewall misconfigurations, insecure VPNs, exposed ports, and inadequate Intrusion Detection/Prevention Systems (IDS/IPS). Moreover, the implementation of a Zero Trust Architecture, which mandates continuous authentication and least privilege access, can substantially diminish attack surfaces. DoS and DDoS attacks constitute significant threats to network security by inundating network resources and resulting in interruptions [25]. Organizations can utilize penetration testing to simulate DDoS assaults, identify bottlenecks, and implement mitigation methods such as rate limiting, and traffic filtering, along with anomaly detection to ensure network stability.

VAPT for Cloud Security

As enterprises transition to the cloud for scalability, flexibility, and cost-effectiveness, they must also confront the security concerns linked to cloud storage, virtual machines, and shared computing resources. Cloud environments function on the Shared Responsibility Model, wherein cloud service providers (CSPs) safeguard the infrastructure, while enterprises are tasked with securing data, applications, and user access. VAPT allows enterprises to evaluate vulnerabilities in cloud storage, including misconfigured access restrictions, unencrypted data, and inadequate API security, which may result in data breaches and insider threats. Security teams can utilize penetration testing to simulate cloud-based attacks, detect authentication vulnerabilities, unsecured container deployments, and privilege escalation threats, while also implementing multi-factor authentication (MFA), data encryption, and stringent IAM regulations to bolster cloud security [25].

VAPT for IoT and Industrial Control Systems (ICS) Security

The expansion of IoT devices and ICS has created new security issues, as these systems frequently lack inherent security measures and are significantly susceptible to cyber threats. IoT gadgets, including smart home systems, medical devices, and autonomous vehicles, are vulnerable to assaults due to inadequate authentication, absence of encryption, and unpatched firmware. Via VAPT, security teams may do security audits on IoT devices, find firmware vulnerabilities, unsecured communication protocols, and data leakage threats, and establish secure boot processes, intrusion detection systems, and device isolation techniques [26].

Likewise, Supervisory Control and Data Acquisition (SCADA) systems employed in industrial sectors like energy, transportation, and manufacturing are excellent targets for cyberattacks due to their antiquated security frameworks and absence of network segmentation. Malefactors can use SCADA vulnerabilities to influence operations, disrupt essential services, and inflict physical damage. VAPT for ICS security entails identifying vulnerable endpoints, strengthening access controls, and guaranteeing safe remote access. Organizations may protect critical infrastructure from cyber threats and preserve operational efficiency by employing sophisticated threat detection, endpoint protection, and conducting regular security assessments.

Future Trends in Vulnerability Assessment and Penetration Testing

The future of VA and PT is influenced by improvements in AI and ML, facilitating automated threat identification, anomaly analysis, and predictive security modelling. Red Team against Blue Team exercises are essential for mimicking authentic cyberattacks and enhancing incident response proficiency. The Zero Trust Security Model and Continuous Threat Exposure Management (CTEM) emphasize the eradication of implicit trust and the implementation of ongoing verification of digital assets. The increasing significance of ethical hackers and bug bounty programs is assisting enterprises in identifying and rectifying vulnerabilities prior to exploitation by harmful entities.

RESEARCH GAP AND CONCLUSION

Notwithstanding progress in VAPT, research deficiencies remain in penetration testing's automation through AI, the incorporation of VAPT into DevSecOps, and the mitigation of emerging

risks in IoT and cloud settings. The absence of established approaches for AI-driven security testing and the restricted integration of real-time threat intelligence impede effectiveness. This study emphasizes the essential function of VAPT in proactive cyber defence, regulatory adherence, and the protection of digital assets. Future research must concentrate on augmenting automation, refining AI-driven vulnerability identification, and formulating adaptive security frameworks to combat growing cyber threats and maintain a robust, threat-aware cybersecurity stance across many industries.

REFERENCES

1. Untawale, T. (2021). Importance of cyber security in digital era. *International Journal for Research in Applied Science and Engineering Technology*, *9*(8), 963-966.
2. Dalal, A. (2020). Cybersecurity and privacy: Balancing security and individual rights in the digital age. *Available at SSRN 5171893*.
3. Craig, A. J., & Valeriano, B. (2018). Realism and cyber conflict: Security in the digital age. *Realism in Practice*, *85*(3), 1-11.
4. Kettani, H., & Cannistra, R. M. (2018, October). On cyber threats to smart digital environments. In *proceedings of the 2nd international conference on smart digital environment* (pp. 183-188).
5. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, *12*(6), 1333.
6. Khera, Y., Kumar, D., & Garg, N. (2019, February). Analysis and impact of vulnerability assessment and penetration testing. In *2019 international conference on machine learning, big data, cloud and parallel computing (COMITCon)* (pp. 525-530). IEEE.
7. Almaarif, A., & Lubis, M. (2020). Vulnerability Assessment and Penetration Testing (VAPT) framework: Case study of government's website. *International Journal on Advanced Science, Engineering and Information Technology*, *10*(5), 1874-1880.
8. Vegesna, V. V. (2022). Utilising VAPT technologies (Vulnerability assessment & penetration testing) as a method for actively preventing cyberattacks. *International Journal of Management, Technology and Engineering*, *12*, 81-94.
9. Süzen, A. A. (2020). A risk-assessment of cyber-attacks and defence strategies in industry 4.0 ecosystem. *International Journal of Computer Network and Information Security*, *15*(1), 1.
10. Heiding, F., Katsikeas, S., & Lagerström, R. (2023). Research communities in cyber security vulnerability assessments: A comprehensive literature review. *Computer Science Review*, *48*, 100551.
11. Yamin, M. M., & Katt, B. (2022). Use of cyber-attack and defence agents in cyber ranges: A case study. *Computers & Security*, *122*, 102892.
12. Zhang, K., & Liu, J. (2020, March). Review on the application of knowledge graph in cyber security assessment. In *IOP Conference Series: Materials Science and Engineering* (Vol. 768, No. 5, p. 052103). IOP Publishing.
13. Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2023). Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-Physical Systems*, *3*, 280-308.
14. 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.
15. Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of scientific research and management*, *9*(12), 669-710.
16. Bella, G., Biondi, P., Bognanni, S., & Esposito, S. (2023). Petiot: Penetration testing the internet of things. *Internet of Things*, *22*, 100707.
17. Lachkov, P., Tawalbeh, L. A., & Bhatt, S. (2022). Vulnerability assessment for applications security through penetration simulation and testing. *Journal of Web Engineering*, *21*(7), 2187-2208.
18. Chandrakant, B. A., & Prakash, J. P. (2019). Vulnerability assessment and penetration testing as cyber defence. *Int. J. Eng. Appl. Sci. Technol*, *4*(2), 72-76.

19. Safitra, M. F., Lubis, M., & Widjajarto, A. (2023, March). Security vulnerability analysis using penetration testing execution standard (PTES): case study of government's website. In *Proceedings of the 2023 6th international conference on electronics, communications and control engineering* (pp. 139-145).
20. Alhamed, M., & Rahman, M. H. (2023). A systematic literature review on penetration testing in networks: future research directions. *Applied Sciences*, *13*(12), 6986.
21. Alquwayzani, A., Aldossri, R., & Frikha, M. (2024). Mitigating Security Risks in Firewalls and Web Applications using Vulnerability Assessment and Penetration Testing (VAPT). *International Journal of Advanced Computer Science & Applications*, *15*(5).
22. Nidhi, R. K., Pradish, M., & Suneetha, M. N. (2024). Cyber Security Analysis of a Power Distribution System Using Vulnerability Assessment and Penetration Testing Tools. *Power Research-A Journal of CPRI*, 17-25.
23. Fatima, A., Khan, T. A., Abdellatif, T. M., Zulfiqar, S., Asif, M., Safi, W., ... & Al-Kassem, A. H. (2023, March). Impact and research challenges of penetrating testing and vulnerability assessment on network threat. In *2023 International Conference on Business Analytics for Technology and Security (ICBATS)* (pp. 1-8). IEEE.
24. Ventura, R., Franco, D. J., & Akram, O. K. (2023). A Novel Vapt Algorithm: Enhancing Web Application Security Trough OWASP Top 10 Optimization. *arXiv preprint arXiv:2311.10450*.
25. Hassan, B., Muhammad, K. B., & Ahmed, K. (2025). Ethical Hacking in the AI Era: Enhancing Cybersecurity for Sustainable Digital Transformation. *THE ASIAN BULLETIN OF GREEN MANAGEMENT AND CIRCULAR ECONOMY*, *5*(1), 37-49.
26. Bonaventura, D., Esposito, S., & Bella, G. (2025). A case of smart devices that compromise home cybersecurity. *Computers & Security*, *151*, 104286.