Borneo International Journal eISSN 2636-9826; Vol.8 (2); 2025; 48-59
Published by *Majmuah Enterprise*
www.majmuah.com

Case Study on the Effectiveness of Penetration Testing in Securing a University Network Infrastructure

MUHAMMAD EIZZAT ABDUL RAZZAK, MUHAMMAD FADILAH ALFARIZY, NUR SABRINA MOHD SHAFAWI, MOHAMAD FADLI ZOLKIPLI
School of Computing, Awang Had Salleh Graduate School, College of Arts and Science, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA
Email: m_eizzat_abdul@ahsgs.uum.edu.my, alfarizy_muhammad2@ahsgs.uum.edu.my, n_sabrina@ahsgs.uum.edu.my, m.fadli.zolkipli@uum.edu.my

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

Abstract

The increasing complexity and openness of university network infrastructures have rendered them highly susceptible to various cybersecurity threats. In response, penetration testing has emerged as a widely recommended approach to proactively identify system vulnerabilities before they can be exploited. This study investigates the effectiveness of penetration testing within the context of higher education institutions by conducting a systematic review of relevant academic literature published between 2020 and 2024. Rather than performing empirical testing, this research synthesizes previous findings from peer-reviewed journals, case studies, and technical reports to explore the methodologies, tools, implementation strategies, and outcomes associated with penetration testing in university environments. The findings suggest that, although penetration testing offers significant benefits in improving network security posture and institutional awareness, its overall effectiveness is influenced by several contextual factors, including administrative support, technical expertise, and the scope of engagement. This study contributes a structured overview of current practices and challenges, providing a foundation for future research and policy development in cybersecurity strategies for academic institutions.

Keywords: Penetration Testing; University Network; Vulnerability Assessment; ISSAF; OWASP;

1. Introduction

As digital infrastructures become increasingly integral to the operation of higher education institutions, the security of university networks has emerged as a critical concern. Higher education institutions manage data from donors, trustees, board members, alumni, students, parents, applicants, faculty, staff, medical patients, consumers, and vendors, encompassing sensitive research, financial, medical, employment, personal, and tax data (Ulven & Wangen, 2021). This positions universities not merely as educational entities but also as financial and medical institutions, subject to various regulations (Ulven & Wangen, 2021). The inherently open and decentralized nature of university networks, designed to promote accessibility and collaboration, simultaneously expands the attack surface for potential cyber threats (Lallie et al., 2025; Ulven & Wangen, 2021). This environment, characterized by academic freedom and information sharing, often conflicts with traditional cybersecurity principles of strict confidentiality and access control (Ulven & Wangen, 2021). Penetration testing, a form of ethical hacking, has been recognized as an essential tool for evaluating the security readiness of IT systems. By simulating real-world attack scenarios, penetration testing allows institutions to detect security flaws, assess the effectiveness of existing defense mechanisms, and implement necessary mitigation strategies. For universities, which often face budgetary and staffing constraints in their IT departments, such testing can offer valuable insights into potential vulnerabilities that may otherwise go unnoticed.

Although the practice of penetration testing is well established in commercial and governmental sectors, its adoption in academic settings remains uneven. Some institutions have integrated it as part of routine security audits, while others have yet to fully explore its strategic value. Existing studies have documented various outcomes, methodologies, and challenges related to penetration testing in university contexts, yet a consolidated understanding remains limited. This study aims to address this gap by reviewing and synthesizing existing research on the application and effectiveness of penetration testing in university networks. Rather than conducting new penetration tests, the research focuses on analyzing findings from previous literature to identify recurring patterns, assess best practices, and evaluate the impact of such testing on institutional cybersecurity resilience.

2. Methodology

This research employs a **systematic literature review (SLR)** as outlined by Felizardo and Carver (2020), Cruz Benito (2016), and Shaffril et al. (2020) to explore the effectiveness of penetration testing in the context of university network security. The SLR approach is chosen for its capacity to provide a comprehensive and structured synthesis of existing knowledge, allowing for the identification of trends, gaps, and critical insights without engaging in primary data collection.

2.1 Research Design

The review process followed a structured protocol comprising four key stages:
(1) formulation of research questions;
(2) identification and selection of relevant studies;
(3) extraction and analysis of data; and
(4) synthesis and interpretation of findings.
The primary research question guiding this review is: *To what extent has penetration testing proven effective in enhancing the security of university network infrastructures?*

2.2 Data Sources

Academic publications were sourced from reputable databases including IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, Scopus, and Google Scholar. The search focused on literature published between 2020 and 2025 to ensure coverage of contemporary practices and technologies. In addition to peer-reviewed journals and conference papers, the review also includes high-quality technical documentation, whitepapers, and insights from credible knowledge-based websites related to cybersecurity and penetration testing.

Search terms included combinations of:

- "penetration testing" AND "university network"
- "ethical hacking" AND "higher education"
- "cybersecurity" AND "campus network infrastructure"

Inclusion criteria:

- Peer-reviewed journal articles and conference papers
- Studies discussing real-world application or evaluation of penetration testing in university or academic contexts
- English-language publications

Exclusion criteria:

- Articles focusing solely on private, military, or governmental networks
- Non-empirical works without clear findings or methodology
- Duplicate or inaccessible full texts

2.3 Data Extraction and Analysis

A qualitative thematic analysis was used to identify key themes across selected studies, including the types of penetration testing employed (e.g., black-box, white-box, grey-box), commonly used tools and frameworks, documented vulnerabilities, mitigation strategies, and institutional outcomes. The analysis also examined organizational factors influencing the implementation and success of penetration testing.

2.5 Limitations

This study is limited by its reliance on published literature, which may omit unpublished or proprietary penetration testing practices conducted within universities. Additionally, the lack of direct empirical experimentation restricts the scope of technical evaluation, though this is mitigated by the depth and breadth of the literature reviewed.

3. Purpose and Challenges in Penetration Testing

3.1. The Escalating Cyber Threat Landscape in Higher Education

Higher education institutions are currently navigating an increasingly perilous cyber threat landscape. These organizations have become prominent targets for a diverse array of malicious actors, leading to significant financial,

operational, and reputational damage. Statistical evidence paints a stark picture of this escalating threat (Rahn, 2025). According to a reputable ransomware report, educational institutions rank as the fourth-most affected sector by ransomware. 1 Between April 2023 and April 2024, these organizations were subjected to 217 ransomware attacks, representing a year-over-year increase of more than 35% (ZScaler, 2024). Universities present uniquely attractive targets for cybercriminals, necessitating an urgent focus on robust network security. These institutions are custodians of vast quantities of sensitive data, including students' personally identifiable information (PII), faculty members' groundbreaking research and intellectual property (IP), and comprehensive financial records. The traditionally open nature of university networks, designed to foster collaboration and knowledge sharing, inadvertently creates a more permeable security perimeter. This openness, coupled with often limited cybersecurity budgets and a diverse, transient user base comprising students, faculty, and staff, compounds the security challenge.

3.2. Penetration Testing as a Proactive Defence Mechanism

Penetration testing stands as a cornerstone of proactive cybersecurity defence as part of ethical hacking activities. It is a methodical process of simulating a cyberattack against an organization's computer systems, networks, or applications to identify exploitable vulnerabilities. Unlike passive security assessments, penetration testing actively attempts to breach security controls, mimicking the techniques and strategies employed by malicious attackers. The fundamental role of penetration testing is to proactively identify and assess security weaknesses before they can be discovered and exploited by actual adversaries. By uncovering these vulnerabilities in a controlled manner, organizations gain critical insights into their security posture, enabling them to prioritize remediation efforts, strengthen defenses, and ultimately reduce their risk of suffering a damaging cyber incident. While penetration testing is undeniably a powerful tool for unearthing security vulnerabilities within complex university networks, its ultimate success in genuinely enhancing an institution's security posture is not guaranteed by the technical execution alone. The central argument of this paper is that the efficacy of penetration testing is maximized when it is implemented within a well-structured, comprehensive framework and is supported by the active, informed, and collaborative involvement of diverse university stakeholders. An ad-hoc or purely technically focused penetration test may identify flaws, but without a strategic framework guiding its integration into the broader security program and without stakeholder buy-in to act upon its findings, its long-term impact will be limited.

3.3. Foundational Penetration Testing Methodologies

A variety of established methodologies guide the execution of penetration tests, providing structured frameworks to ensure comprehensive and repeatable assessments. Understanding these foundational approaches is crucial for universities to select and tailor testing strategies that align with their specific security objectives and network environments. The Open Web Application Security Project (OWASP) Testing Guide (WSTG) is a specialized framework focusing on web application security, a critical area for universities with numerous student portals, learning management systems, and administrative web services. The WSTG is structured around the OWASP Top 10, a list of the most critical web application security risks. Its testing phases are often integrated within the Software Development Life Cycle (SDLC). One of the most interesting parts is a dedicated section on Penetration Testing Execution Standard (PTES), which offers a comprehensive, seven-phase approach to penetration testing: Pre-engagement Interactions, Intelligence Gathering, Threat Modeling, Vulnerability Analysis, Exploitation, Post Exploitation, and Reporting (OWASP, 2025). PTES is valued for providing not only a process flow but also hands-on technical guidelines regarding what and how to test, the rationale for testing, and recommended tools. NIST Special Publication 800-115, "Technical Guide to Information Security Testing and Assessment," provides a structured approach for conducting a wide range of security testing and assessment activities. Rather than being a rigid set of controls, it is a guide that outlines methodologies, techniques, and procedures. Its key areas of focus include Security Assessment Planning, Security Assessment Execution, Post-Testing Activities, Vulnerability Scanning, and various Security Testing Techniques such as reviews, target identification and analysis, and target vulnerability validation (Scarfone et al., 2008). This framework is valuable for universities in planning comprehensive security assessments and ensuring that testing activities are systematic and well-documented.

Table 1: Comparison of Key Penetration Testing Methodologies

Methodology	Key Phases/Focus	Strengths for University Context	Limitations for University Context
OWASP WSTG	Integrated with SDLC; focus on OWASP Top 10 web vulnerabilities; Includes dedicated section on Penetration Testing Execution Standard (PTES)	Highly relevant for securing numerous university web applications (portals, LMS); detailed web-specific test cases; Comprehensive lifecycle coverage.	Primarily focused on web applications; less direct guidance for network infrastructure or physical security. Can be resource-intensive if all technical guidelines are followed meticulously.

NIST SP 800-115	Security Assessment Planning, Execution, Post-Testing; Vulnerability Scanning; Review, Target ID & Analysis, Vulnerability Validation techniques	Provides a strong framework for planning and conducting various security assessments; aligns well with governmental/compliance needs.	More of a general assessment guide than a specific penetration testing execution manual; may require supplementation for deep technical tests.

No single methodology serves as a silver bullet for the diverse and complex security needs of universities. These institutions manage a wide array of assets, from public-facing websites and extensive internal networks to sensitive research databases and critical operational systems. Each of the discussed methodologies offers distinct advantages: OWASP WSTG excels in web application security, PTES provides a thorough lifecycle for engagements, while NIST SP 800-115 offers a robust structure for assessment planning and documentation.

3.4. Comparative Analysis of Penetration Testing Types and Their Suitability for Universities

Penetration tests are broadly categorized based on the level of information provided to the testing team about the target environment: black-box, white-box, and grey-box testing. Each type offers different perspectives and depths of assessment, and their suitability for universities varies depending on the specific objectives and assets being tested (Tidmarsh, 2023).

3.4.1. Black-box Testing

Black-box testing simulates an attack from an external adversary who has no prior knowledge of the internal workings of the target system or network. Testers typically start with minimal information, such as a domain name or IP address range.

- Advantages for Universities: This approach provides the most realistic simulation of an external attacker's perspective, making it valuable for assessing the effectiveness of perimeter defenses and identifying publicly exploitable vulnerabilities.
- Disadvantages for Universities: Because testers have no internal knowledge, black-box tests can be time-consuming, especially for large and complex university networks. There's a risk that internal vulnerabilities might be missed if the perimeter defenses are robust enough to prevent initial entry within the test's timeframe.

3.4.2. White-box Testing

White-box testing, also known as clear-box or open-box testing, provides the testing team with complete knowledge of the target system, including source code, architecture diagrams, network maps, and potentially administrative credentials.

- Advantages for Universities: This method allows for the most comprehensive and in-depth assessment, including detailed static code analysis of custom applications and thorough examination of internal system configurations. It is particularly useful for evaluating the security of critical internal systems, sensitive data repositories, or newly developed in-house applications.
- Disadvantages for Universities: White-box tests can be extremely time-consuming and require a high level of expertise from the testing team due to the sheer volume of information to analyze. While thorough, the findings may not always reflect the path an external attacker without such privileged knowledge would take.

3.4.3. Grey-box Testing

Grey-box testing represents a hybrid approach, where testers are provided with partial knowledge of the target environment, such as user-level login credentials or limited network diagrams. This simulates scenarios like an attacker who has compromised a standard user account or an insider with limited privileges.

- Advantages for Universities: Grey-box testing strikes a balance between the realism of black-box testing and the depth of white-box testing. It is particularly effective for universities in assessing the risks associated with compromised user accounts—a significant threat given their large and diverse user populations. It allows for more focused and efficient testing of internal systems and applications from a privileged user's perspective.
- Disadvantages for Universities: If not carefully scoped, grey-box tests might not achieve the full depth of a white-box assessment or the pure external perspective of a black-box test. The level of "partial knowledge" needs to be clearly defined to meet test objectives.

3.4.4. Suitability of Testing Methods

For universities, a combination of grey-box and black-box testing often yields the most favorable cost-benefit ratio. The extensive internal networks and numerous user accounts within academic institutions make insider threats and

compromised credentials significant risks; grey-box testing directly and efficiently addresses these vulnerabilities. Periodic black-box tests remain essential for validating the security of the external perimeter against attackers with no prior knowledge. Full white-box tests, due to their considerable cost and time implications, might be strategically reserved for the most critical, custom-developed applications, such as research systems handling exceptionally sensitive data or intellectual property, or financial systems processing significant transactions. This hybrid strategy allows universities to achieve a balanced approach to security assessment, covering a wide range of threat vectors while managing resource allocation effectively, a crucial consideration given typical university budget constraint (Tidmarsh, 2023).

4. Review of Penetration Testing within University Networks

4.1. The Penetration Testing (PTES) Lifecycle Tailored for Educational Institutions

The Penetration Testing Execution Standard (PTES) provides a comprehensive, structured lifecycle for conducting penetration tests. When adapted for educational institutions, this framework ensures that testing is not only thorough but also contextually relevant to the unique challenges faced by universities.

The PTES lifecycle comprises seven key phases:

- Pre-engagement Interactions: These involve more than just scope definition. This phase in higher education requires clear communication with a variety of departments, including academic deans, legal offices, IT services and sometimes student representatives. It also includes defining acceptable use of test environments, particularly when sensitive student or research data is involved (Asassfeh et al., 2024).
- Intelligence Gathering: Intelligence gathering must involve cloud services (like Google Workspace and Moodle), internal databases, faculty research platforms, BYOD (Bring Your Own Device) settings, and remote learning tools due to the diversity of university systems (Dong & Xie, 2025). Through publications and institutional repositories, open-source intelligence (OSINT) can also uncover system settings, research information, and exposed academic emails.
- Threat Modelling: Universities are prime targets for various threat actors. According to Jawaid (2023), attackers may include cybercriminals aiming to exploit valuable research data, hacktivists targeting politically active campuses, or even students engaging in unethical behavior. Threat modeling helps prioritize testing around critical systems like student records, finance systems, and research grants.
- Vulnerability Analysis: Tools such as Nessus, Nikto, OpenVAS, and even machine learning-enabled scanners are used. AI-enhanced vulnerability identification can be important in dynamic environments like IoT-enabled smart campuses (Koroniotis et al, 2021)
- Exploitation: Ethical hackers demonstrate how real-world attacks works and often using hybrid approaches that combine automated tools with manual testing (Al-Ahmad et al., 2023).
- Post-Exploitation: This phase evaluates the extent of access gained and the potential for lateral movement within the network.
- Reporting: Customized reports should reflect both technical findings and operational impact. In education, reports must often be split into technical (for IT) and non-technical (for management) summaries to ensure actionable insights are communicated clearly and actionable roadmaps for mitigation (Al-Ahmad et al., 2023).

This structured approach ensures that penetration testing is not a one-off technical exercise but a strategic component of the institution's broader cybersecurity program.

4.2. Common Vulnerabilities in University Network Infrastructures

Universities are particularly vulnerable to cyber threats due to their open-access policies, diverse user base, and complex IT ecosystems. Common vulnerabilities identified across multiple studies include:

- Weak Authentication Mechanisms: Many universities still rely on outdated login systems (username-password) and this method can be easily exploited by the attackers. Despite the availability of SSO and MFA, implementation remains inconsistent due to cost or legacy systems (Alhamed & Rahman, 2023).
- Unpatched Software: Legacy systems and outdated applications often remain unpatched due to resource constraints or compatibility concerns.
- Misconfigured Firewalls and Access Controls: According to Asassfeh et al. (2024), misconfigured cloud services and firewalls are among the top causes of vulnerabilites. Inadequate segmentation between administrative and academic networks can allow attackers to move laterally once they could go inside.
- Insecure Web Applications: OWASP vulnerabilities like XSS and insecure session management persist across LMS and portals. Sulisnawati & Subektiningsih (2023) demonstrated how public-facing student portals often lack even basic input validation.
- Flat Network Architectures: Without proper segmentation, attackers can easily pivot across departments once inside.

These vulnerabilities are not merely theoretical. For instance, Alzahrani (2018) found critical flaws in Albaha University's network, while Adu-Boahene et al. (2021) documented similar issues at the University of Education, Winneba.

4.3. Penetration Testing in Action

4.3.1. Case Study 1: University of Education, Winneba (Adu-Boahene et al., 2021)

This university conducted a comprehensive penetration test targeting both internal and external systems. The assessment employed black-box (no prior knowledge of the system) and grey-box (partial knowledge) methodologies to simulate real-world attack scenarios.

- Tools Used: Metasploit for exploitation, Burp Suite for web application testing, and Nmap for network scanning.
- Key Vulnerabilities Identified:
  - Exposed administrative interfaces accessible without authentication.
  - Default credentials have been used across multiple systems.
  - Transmission of sensitive data over unencrypted channels.
- Remediation Measures:
  - Implementation of Multi-Factor Authentication (MFA) across critical systems.
  - Firewall rules have been updated to restrict access to sensitive endpoints.
  - Cybersecurity awareness workshops for faculty and staff have been conducted

4.3.2. Case Study 2: Albaha University (Alzahrani, 2018)

Albaha University in Saudi Arabia conducted internal audit using a custom-developed penetration testing tool tailored to its network architecture. The focus was on evaluating the security of wireless networks and the student information system.

- Approach: The audit was conducted by internal IT staff using a proprietary tool, allowing for deep inspection of system configurations.
- Key Vulnerabilities Identified:
  - Weak encryption protocols in wireless networks, making them susceptible to eavesdropping.
  - Insecure access controls in the student information system and leads to privilege escalation.
- Remediation Measures:
  - Deployment of Intrusion Detection Systems (IDS) to monitor network traffic and detect anomalies.
  - Regular patch management cycle to ensure timely updates of software and firmware.
  - Enhanced logging and monitoring capabilities to track user activities and detect suspicious activity.

5. Discussion: Evaluating the Effectiveness and Impact of Penetration Testing in Academia

A pragmatic and effective strategy for universities often involves a blended approach. This means selecting and adapting elements from various methodologies based on the specific systems being tested, the identified risks, and the overall security objectives of the institution, rather than rigidly adhering to a single framework. For example, a university might use PTES to structure the overall penetration testing engagement, employ OWASP WSTG for detailed testing of its student information portal, refer to NIST SP 800-115 for guidance on assessment planning and reporting,

5.1. Quantifiable Benefits

The implementation of penetration testing within academic institutions yields a multitude of quantifiable and qualitative benefits that directly contribute to a stronger security posture and the overall well-being of the university community.:

- Protecting Sensitive Data: Universities are repositories of vast amounts of sensitive information, including student PII, confidential staff details, valuable research data, and financial records. Penetration testing plays a crucial role in safeguarding this data by proactively identifying and enabling the remediation of vulnerabilities that could otherwise lead to breaches, identity theft, or intellectual property loss.
- Reduction in Vulnerabilities and Financial Loss: Institutions that conduct regular testing report a significant drop in critical vulnerabilities over time. Also, cyberattacks can result in significant financial burdens for universities, encompassing costs related to system recovery, data restoration, legal fees, regulatory fines, and incident response.
- Improved Incident Response: Simulated attacks help IT teams refine their detection and response capabilities. The penetration testing process itself serves as a valuable learning opportunity for a university's internal IT and security teams. They gain firsthand insights into attacker methodologies, common vulnerabilities within

their specific environment, and effective remediation techniques, thereby enhancing their capacity to protect systems and respond to future threats

- Enhanced Awareness: Faculty and staff become more security-conscious, especially when findings are shared through training and workshops. By simulating real-world attack scenarios, penetration testing provides actionable insights into the effectiveness of existing security measures. The findings enable institutions to pinpoint weaknesses and implement targeted improvements, thereby bolstering their defenses against the constantly evolving threat landscape.
- Compliance and Accreditation: Educational institutions are often subject to stringent data protection regulations. Penetration testing supports compliance with standards such as ISO/IEC 27001 and helps meet audit requirements. In Malaysia, the Personal Data Protection Act 2010 (PDPA), mandates the need on regulating the processing of personal data to safeguard the privacy of individuals. This means that Universities are in scope as they have control over or authorizes the processing of personal data in connection with commercial transactions for students and academicians.

Alhamed & Rahman (2023) noted that universities implementing structured penetration testing programs saw a 40–60% improvement in their overall security posture within two years. Data breaches can severely damage an institution's reputation, potentially impacting student enrollment and staff morale. A commitment to robust cybersecurity, demonstrated through regular penetration testing, builds trust among students, parents, faculty, staff, alumni, and research partners.

5.2. Challenges in Executing an Effective Penetration Testing in Universities

Despite its clear benefits, implementing penetration testing in universities is fraught with unique challenges spanning logistical complexities resource constrains.

5.2.1. Logistic Constrains

One of the primary challenges is the timing of the penetration test exercise. Universities in particular have their own cycles of registration, examinations, holidays, and critical research periods, imposes significant constraints on scheduling penetration tests (Bertoglio et al., 2023). They IT team may face resistance from stakeholders; faculty and administrative staff may view testing as intrusive or unnecessary. Testing activities must be carefully planned to avoid disrupting these core academic functions, or expose sensitive data if not carefully managed.

The prevalence of Bring-Your-Own-Device (BYOD) policies in university environment also means that a vast number of student and faculty-owned devices are connect to the university network. These devices are often unmanaged from a central IT perspective, significantly expanding the attack surface and adding complexity to defining the scope and assessing the security of the network environment (Lallie et al., 2025a).

5.2.2. Resource Constrains

Many universities operate with limited cybersecurity budgets, making it difficult to hire skilled testers or purchase advanced tools. Compared to many private sector corporations, universities often operate with more constrained cybersecurity budgets (Alhamed & Rahman, 2023b). Comprehensive penetration testing can be a costly endeavor, encompassing fees for external expert testers, internal staff time for coordination and remediation, and potential investments in security tools or upgrades identified by the tests.

The other concern is on the availability of skilled personnel to execute the activity. Internal IT staff may lack the expertise to interpret test results or implement recommended changes. There is a well-documented global shortage of qualified cybersecurity professionals (Bertoglio et al., 2023). Universities may struggle to recruit and retain sufficient in-house expertise to conduct sophisticated penetration tests or to effectively manage and remediate the vulnerabilities identified by external testers.

5.3. Acknowledging the Limitations

While penetration testing has emerged as a vital component of cybersecurity strategies in academic institutions, several limitations must be acknowledged to contextualize its conclusions and guide future research.

- Absence of Primary Data Collection

  This study is based entirely on a systematic review of secondary sources, including academic articles, case studies, and technical reports. As such, it does not include:
  - First-hand penetration testing results
  - Interviews with cybersecurity professionals or university IT staff
  - Direct observations of testing procedures or outcomes

  This reliance on existing literature may limit the depth of insight into institution-specific practices or emerging trends not yet published.
- Lack of Empirical Validation

This review depends on secondary data drawn from published literature and case studies (Alhamed & Rahman, 2023; Al-Ahmad et al., 2023). Without direct empirical testing or firsthand involvement in penetration tests, verification for the accuracy, scope, and real-world impact of the reported outcomes are not so accurate. For example, the case study of Adu-Boahene et al. (2021) and Alzahrani (2018) provide valuable insights into vulnerabilities and remediation steps, the depth of technical implementation and long-term impact are not consistently documented.

- Publication Bias and Limited Access to Internal Reports
  Many successful penetration tests and their findings remain unpublished due to confidentiality, reputational concerns, or institutional policies (Ulven & Wangen, 2021; Yaacoub et al., 2021). As a result, the reviewed literature might reflect a publication bias, over-representing more proactive institutions or more severe cases. In contrast, unsuccessful tests or those that led to negligible change are underreported, skewing the perception of effectiveness.
- Variability in Institutional Maturity
  Not all academic institutions are equally equipped to conduct or interpret penetration tests. Institutions with limited IT budgets or cybersecurity expertise may struggle to conduct the test, as highlighted by Alhamed & Rahman (2023) and Lallie et al. (2025). This can result in superficial remediation efforts or prolonged exposure to known vulnerabilities.

The challenge of decentralized IT within universities warrants particular attention. A purely top-down, centrally mandated penetration testing program might encounter resistance from autonomous departments or prove difficult to implement consistently across varied local IT environments. Institutions can adopt phased testing approaches, use virtualized environments for high-risk tests, and engage stakeholders early in the planning process. This collaborative model respects departmental autonomy while promoting a consistent baseline of security assessment across the entire institution, ultimately leading to more effective risk mitigation and a stronger overall security culture.

5.4. Metrics for Success: Gauging Risk Reduction and Security Posture Improvement

Evaluating the success of a penetration testing program in a university setting extends beyond merely counting the number of vulnerabilities discovered. True effectiveness is measured by tangible improvements in the institution's overall security posture and a demonstrable reduction in risk. To evaluate the effectiveness of penetration testing, universities should track:

- Reduction in Critical/High Vulnerabilities Over Time: Tracking the number and severity of vulnerabilities identified in successive penetration tests can indicate trends. A consistent decrease in high-impact vulnerabilities suggests that remediation efforts are effective and the security baseline is improving.
- Time-to-Remediate: Measuring the average time taken to fix identified vulnerabilities, especially critical and high-priority ones, reflects the efficiency of the university's remediation processes. A decreasing time-to-remediate indicates improved responsiveness.
- User Awareness Levels (via surveys or phishing simulations): If penetration tests include social engineering components (e.g., phishing simulations), improvements in click-through rates or reporting rates in subsequent campaigns can be a metric. Furthermore, tracking the completion rates and assessment scores of security awareness training programs, especially if content is updated based on test findings, can indicate improved human defenses.

These metrics help institutions move from reactive to proactive security management and demonstrate the return on investment (ROI) of penetration testing initiatives. Tracking such metrics to measure the penetration test's impact on fostering a more deeply embedded security culture, rather than just focusing on the reactive patching of isolated technical flaws. This deeper level of change signifies a more profound and sustainable enhancement of the university's security posture.

6. Key Findings

The analysis of theoretical foundations, practical applications, and evaluative aspects of penetration testing within the higher education context reveals several key findings crucial for optimizing these security assessments. The effectiveness of penetration testing is not solely dependent on technical prowess but is significantly amplified by strategic framing and organizational integration.

6.1. The Necessity of a Well-Architected Implementation Framework

Ad-hoc or isolated penetration tests, while potentially uncovering some vulnerabilities, are insufficient for achieving a sustained improvement in a university's cybersecurity posture. A well-architected implementation framework is necessary to ensure that penetration testing is a systematic, continuous, and strategically aligned activity.

Established frameworks like the NIST Cybersecurity Framework (CSF) provide an excellent overarching structure for a university's entire cybersecurity program. The CSF's core functions - *Identify, Protect, Detect, Respond*, and *Recover* - offer a comprehensive approach to managing cybersecurity risk (Armas & Taherdoost, 2025). Penetration testing directly supports the "Identify" function by discovering vulnerabilities and the "Detect" function by testing the efficacy of detection mechanisms. The recent introduction of a "Govern" function in NIST CSF 2.0 is particularly pertinent for universities, emphasizing the importance of integrating cybersecurity risk management into institutional governance, strategy, and policy-making (U.S. Department of Commerce, 2024).

6.2. The Indispensable Role of University Stakeholder Engagement

The technical execution of a penetration test is only one part of the equation for success. The active and informed engagement of a diverse range of university stakeholders throughout the entire lifecycle of the penetration testing program is indispensable for maximizing its impact. Stakeholder engagement in all critical stages, including planning, execution and post-testing, is crucial – the success of the exercise depends on the collaboration of IT staff, faculty, and administrators. When stakeholders are actively engaged, it fosters a sense of shared ownership for security, facilitates smoother and more effective testing engagements, and significantly increases the likelihood that findings will lead to meaningful and lasting security improvements. A particularly valuable, yet often underutilized, approach to stakeholder engagement in universities is to involve students not merely as passive users to be protected, but as potential *partners* in the cybersecurity process. Given that students represent a significant user base and, inadvertently or otherwise, a potential insider threat vector, a proactive engagement strategy can yield multiple benefits (Lallie et al., 2025). Such initiatives provide students with practical, real-world cybersecurity experience, foster a greater sense of digital responsibility, and can help cultivate a pipeline of future cybersecurity professionals.

6.3. Common Pitfalls and Success Factors in University Penetration Testing

The journey of implementing and benefiting from penetration testing in universities is often marked by common pitfalls that can undermine effectiveness, and conversely, key success factors that can amplify its positive impact.

Table 2: Pitfall and Success Factors in Pen Test Stages

Stages	Common Pitfalls	Success Factors
Initial Planning	Ambiguous, narrow, or overly broad scope	Well-defined goals and strong leadership support
	Insufficient support from administration and stakeholder buy-ins.	Engagement from senior administration and department heads
Selecting Penetration Testers	Opting for cheaper, less experienced testers due to cost constraints	Testers with proven expertise and certifications
	Over-reliance on automated tool or scanners	Selecting suitable tools based on testing methodologies and types
Execution	Inadequate testing timeframe	Allows adequate time for comprehensive testing
	Poor communication with IT staff	Maintain open, proactive communication channels
	Overlooking physical security	Include thorough physical security assessment
Evaluation & Reporting	Inadequate documentation and reporting method	Detailed reports with clear, prioritized actions and actionable recommendations
	Failure to communicate findings to stakeholders	Disseminate findings to all relevant parties
Remediation	Insufficient resources for remediation - budget, personnel, or expertise constraints	Commitment to remediation and re-testing - dedicated and effective follow-up on remediation actions
	Failure to act on findings with lack of follow-through on remediation	Ensure prompt and thorough remediation of identified vulnerabilities
Post-Testing Review	Treating penetration testing as a one-off compliance checkbox	Integration into a Continuous Improvement (CI) cycle: using findings to continually improve security policies and postures
	Ignoring the need for periodic retesting	Schedule regular penetration tests and awareness

7. Recommendation

Universities should develop a customized penetration testing program aligned with their unique risk profiles, critical assets, operational context, and strategic objectives (Armas & Taherdoost, 2025). This begins with comprehensive risk assessments to identify high-risk systems, evaluate the potential impact of their compromise, and understand specific threats. Clear objectives for each test must be defined to guide the scope, methodology, and type of test, ensuring focused and actionable results. Selecting appropriate testing methods, whether black-box, grey-box, or white-box, and developing a multi-year testing schedule prioritizes and systematically addresses security validation (Isnaini et al., 2024). Managing the penetration testing lifecycle effectively, from procurement to remediation, is crucial. Universities should engage qualified and certified professionals who have experience with higher education environments. Detailed Statements of Work (SOW) should be developed, clearly defining the scope, objectives, methodologies, deliverables, and rules of engagement (Isnaini et al., 2024). During execution, maintaining open communication and monitoring activities ensures adherence to protocols and facilitates immediate attention to critical vulnerabilities (Ulven & Wangen, 2021). Post-testing involves prioritizing and systematically remediating vulnerabilities, followed by re-testing to verify fixes. Comprehensive documentation of all activities aids in tracking improvement and informing future cycles, with a "Purple Team" model enhancing real-time collaboration between internal security teams and testers (Isnaini et al., 2024).

Penetration testing should catalyse a culture of continuous security improvement throughout the university by informing and refining policies, and enhancing security awareness training with real-world examples (Sufatrio et al., 2022). Establishing a cycle of regular testing, remediation, and re-testing demonstrates ongoing commitment to security (Alhamed & Rahman, 2023). Finally, integrating penetration testing outcomes into strategic planning and budgeting ensures sustained investment in cybersecurity improvements, recognizing security as a strategic priority essential to protecting the university's mission, assets, and reputation (Sufatrio et al., 2022).

8. Conclusion

Penetration testing proves to be a vital component in the cybersecurity strategy of universities, allowing them to identify and mitigate vulnerabilities in their systems, applications, and processes proactively. To harness its full potential, universities must develop a bespoke penetration testing program that aligns with their specific risks, assets, and strategic objectives, incorporate comprehensive testing methodologies tailored to their environment, and ensure active stakeholder involvement throughout the testing lifecycle.

As the cyber threat landscape continues to evolve, universities must adapt their penetration testing practices, incorporating emerging technologies like artificial intelligence and automation, and adopting a more integrated and continuous testing model. Embracing these evolving practices will enhance the effectiveness of penetration testing, thereby safeguarding sensitive data, ensuring compliance, and ultimately protecting the core missions of higher education institutions.

9. Acknowledgment

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

Adam, H. M., Widyawan, & Putra, G. D. (2023). A review of penetration testing frameworks, tools, and application areas. *2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 319–324. https://doi.org/10.1109/icitisee58992.2023.10404397

Adu-Boahene, C., Nikoi, S. N., & Nsiah-Konadu, A. (2021). Campus network and systems security assessment using penetration testing: The case of the university of education winneba, kumasi. *Asian Journal of Research in Computer Science*, 7–25. https://doi.org/10.9734/ajrcos/2021/v12i130273

Al-Ahmad, A. S., Kahtan, H., & Alzoubi, Y. I. (2023). Overview on case study penetration testing models evaluation. *Emerging Science Journal*, *7*(3), 1019–1036. https://doi.org/10.28991/esj-2023-07-03-025

Alhamed, M., & Rahman, M. M. H. (2023). A systematic literature review on penetration testing in networks: Future research directions. *Applied Sciences*, *13*(12). https://doi.org/10.3390/app13126986

Alzahrani, M. E. (2018). Auditing Albaha University Network Security using in-house Developed Penetration Tool. *Journal of Physics: Conference Series*, *978*, 012093. https://doi.org/10.1088/1742-6596/978/1/012093

Armas, R., & Taherdoost, H. (2025). Building a cybersecurity culture in higher education: Proposing a cybersecurity awareness paradigm. *Information*, *16*(5), 336. https://doi.org/10.3390/info16050336

Asassfeh, M., Samara, G., Zaid, A. A., Laila, D. A., Al-Anzi, S., Alqammaz, A., Al Smadi, A., Al-Shaikh, A., & Al-Mousa, M. R. (2024). Penetration testing overview-opportunities and ethical considerations: Literature notes.

2024 International Jordanian Cybersecurity Conference (IJCC), 131–135. https://doi.org/10.1109/ijcc64742.2024.10847295

Ayyagari, R., & Tyks, J. (2012). Disaster at a university: A case study in information security. *Journal of Information Technology Education: Innovations in Practice*, *11*, 085–096. https://doi.org/10.28945/1569

Bertoglio, D. D., Gil, A., Acosta, J., Godoy, J., Lunardi, R. C., & Zorzo, A. F. (2023, November 21). *Towards new challenges of modern Pentest*. arXiv.Org. https://arxiv.org/abs/2311.12952

Blancaflor, E., Caberto, D. J., lara, C. G., & Mancilla, D. F., l. (2024). Guarding against phone scammers: An examination of gaining access to phone contacts through smishing social engineering exploits. *Proceedings of the 2024 10th International Conference on Computing and Artificial Intelligence*, 365–372. https://doi.org/10.1145/3669754.3669810

Dong, X., & Xie, Y. (2025). Research on cloud computing network security mechanism and optimization in university education management informatization based on OpenFlow. *Systems and Soft Computing*, *7*, 200225. https://doi.org/10.1016/j.sasc.2025.200225

Heiding, F., Süren, E., Olegård, J., & Lagerström, R. (2023). Penetration testing of connected households. *Computers & Security*, *126*, 103067. https://doi.org/10.1016/j.cose.2022.103067

Isnaini, K., Asyari, M. H., Amrillah, S. F., & Suhartono, D. (2024). Vulnerability assessment and penetration testing on student service center system. *ILKOM Jurnal Ilmiah*, *16*(2), 161–171. https://doi.org/10.33096/ilkom.v16i2.1969.161-171

Jawaid, S. A. (2023). Cyber security threats to educational institutes: A growing concern for the new era of cybersecurity. *International Journal of Data Science and Big Data Analytics*, *2*(2). https://doi.org/10.51483/ijdsbda.2.2.2022.11-17

Koroniotis, N., Moustafa, N., Turnbull, B., Schiliro, F., Gauravaram, P., & Janicke, H. (2021). A deep learning-based penetration testing framework for vulnerability identification in internet of things environments. *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 887–894. https://doi.org/10.1109/trustcom53373.2021.00125

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers*, *14*(2), 49. https://doi.org/10.3390/computers14020049

Li, Q., & Wu, J. (2025). Efficient network attack path optimization method based on prior knowledge-based PPO algorithm. *Cybersecurity*, *8*(1). https://doi.org/10.1186/s42400-024-00288-8

OWASP. (2025). *Web Security Testing Guide (WSTG) - PTES*. OWASP Foundation. https://owasp.org/www-project-web-security-testing-guide/stable/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies

Rahn, D. (2025, April 17). *Top cyber threats to educational institutions in 2025*. The ENGAGE Blog by Blackbaud. https://blog.blackbaud.com/top-cyber-threats-to-educational-institutions/

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2021, April 23). *SP 800-115, technical guide to information security testing and assessment*. CSRC. https://csrc.nist.gov/pubs/sp/800/115/final

Sholawati, A., Setyadi, H. J., & Masa, A. P. A. (2024). Implementasi penetration testing pada sistem informasi terpadu layanan prodi menggunakan framework issaf. *Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto)*, *25*(2), 73. https://doi.org/10.30595/techno.v25i2.21140

Sufatrio, Vykopal, J., & Chang, E.-C. (2022). Collaborative Paradigm of Teaching Penetration Testing using Real-World University Applications. *Proceedings of the 24th Australasian Computing Education Conference*, 114–122. https://doi.org/10.1145/3511861.3511874

Sulisnawati, N., & Subektiningsih, S. (2023). Implementation of open web application security project for penetration testing on educational institution websites. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *9*(2), 250–267. https://doi.org/10.26555/jiteki.v9i2.25987

Tan, W. H., Ismail, S. A., & Abas, H. (2022, June). *View of penetration testing process: A preliminary study*. https://oiji.utm.my/index.php/oiji/article/view/190/144

Tidmarsh, D. (2023, December 4). *Blackbox Pentest vs Whitebox pentest vs Greybox Pentest*. Cybersecurity Exchange; EC-Council. https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/black-box-gray-box-and-white-box-penetration-testing-importance-and-uses/

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), 39. https://doi.org/10.3390/fi13020039

U.S. Department of Commerce. (2024). *The NIST cybersecurity framework (CSF) 2.0*. National Institute of Standards and Technology. https://doi.org/10.6028/nist.cswp.29

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2021, March 28). *A survey on ethical hacking: Issues and challenges*. arXiv.Org. https://arxiv.org/abs/2103.15072

ZScaler. (2024). *ThreatLabz Ransomware Report*. Zscaler. https://www.zscaler.com/campaign/threatlabz-ransomware-report

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

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