Journal of Frontiers in Multidisciplinary Research

Systematic Review of Penetration Testing and Vulnerability Assessment Using Nessus and Wireshark in Corporate IT Environments

Olabode Michael Soneye [1*], Ayobami Adebayo [2], Afeez A Afuwape [3], Ayorinde Olayiwola Akindemowo [4], Eseoghene Daniel Erigha [5], Ehimah Obuse [6], Joshua Oluwagbenga Ajayi [7], Emmanuel Cadet 8, Iboro Akpan Essien [9]

[1] Ontario Health Ontario, Canada
[2] Independent Researcher, USA
[3] University of Oulu, Finland
[4] Patricia Technologies, Vilnius, Lithuania
[5] Choco GmbH Berlin, Germany
[6] Choco/SRE DevOps, General Protocols Berlin/Singapore
[7] Earnipay, Lagos, Nigeria
[8] Independent Researcher, USA
[9] Thompson & Grace Investments Limited, Port Harcourt, Nigeria

* Corresponding Author: **Olabode Michael Soneye**

Article Info

E-ISSN: 3050-9726
P-ISSN: 3050-9718
Volume: 02
Issue: 01
January - June 2021
Received: 11-04-2021
Accepted: 15-05-2021
Published: 17-06-2021
Page No: 467-479

Abstract

Penetration testing and vulnerability assessment have become pivotal in strengthening corporate IT environments against an ever-expanding threat landscape. This systematic review critically examines the application of two widely utilized tools, Nessus and Wireshark, for enhancing cybersecurity resilience within corporate infrastructures. Nessus, a leading vulnerability scanner, enables organizations to proactively identify, prioritize, and remediate weaknesses in their systems. Wireshark, a powerful network protocol analyzer, assists in scrutinizing traffic for anomalies that could signal ongoing attacks or security misconfigurations. Through a structured analysis of peer-reviewed articles, technical reports, and case studies, this review categorizes findings across multiple corporate settings, highlighting best practices, challenges, and gaps in implementation. The study employs PRISMA methodology to ensure rigorous selection, assessment, and synthesis of 52 relevant publications from 2015 to 2021. Results indicate that while Nessus excels in vulnerability identification across operating systems and web applications, its effectiveness depends significantly on regular updates and proper configuration. Meanwhile, Wireshark's packet-level inspection provides unparalleled visibility into network behavior but demands expert knowledge for accurate interpretation and actionable insights. The integration of Nessus and Wireshark in a comprehensive security strategy leads to measurable improvements in incident response times, compliance adherence, and risk mitigation outcomes. However, reliance on manual configurations and the potential for overwhelming data volumes remain persistent challenges. Emerging trends reveal that coupling Nessus with machine learning techniques for automated prioritization, and combining Wireshark with AI-driven anomaly detection, is gaining traction among advanced corporate security teams. Furthermore, organizational culture, training, and continuous monitoring were identified as critical enablers for maximizing the effectiveness of these tools. This review concludes with recommendations for developing adaptive frameworks that synergize Nessus and Wireshark capabilities with evolving cybersecurity needs. Future research should explore the scalability of hybrid automation models and the integration of these tools within zero-trust architectures to sustain proactive defense mechanisms in dynamic corporate environments.

DOI: https://doi.org/10.54660/.JFMR.2021.2.1.467-479

Keywords: Penetration Testing, Vulnerability Assessment, Nessus, Wireshark, Corporate IT Security, Cybersecurity Tools, Network Analysis

1. Introduction

In the modern corporate IT environment, organizations are increasingly confronted with a diverse and sophisticated range of

cybersecurity threats. The proliferation of technology, particularly driven by cloud computing and remote work arrangements, has significantly expanded the attack surface available to malicious actors. Research indicates that threats such as ransomware, phishing schemes, advanced persistent threats (APTs), and insider attacks are prevalent and can lead to severe financial, reputational, and operational repercussions for firms that fail to implement effective cybersecurity strategies (Tamrakar & Patra, 2018; Škiljić, 2020). The complexity of corporate networks combined with the versatility of attack methods—like automation and social engineering—reinforces the need for proactive security measures (Adewumi, *et al*., 2024, Aniebonam, 2024, Ikese, *et al*., 2024, Ofodile, *et al*., 2024).

The shift to remote work, especially accelerated by the COVID-19 pandemic, has exacerbated these vulnerabilities. Employees working from home often utilize personal devices and unsecured networks, which heighten the risk of cyber threats (Škiljić, 2020). The involvement of human factors, such as inadequate cybersecurity awareness among employees, further complicates the landscape (Akinyemi & Ebiseni, 2020, Austin-Gabriel, *et al*., 2021, Dare, *et al*., 2019). The importance of understanding these complexities has led to the necessity for robust cybersecurity governance in corporate structures, where executives and boards are now seen as pivotal in addressing these challenges.

To combat the multitude of threats prevalent in the contemporary corporate IT landscape, penetration testing and vulnerability assessment have emerged as essential components of cybersecurity frameworks. Penetration testing simulates real-world cyber attacks to uncover vulnerabilities before they can be exploited, while vulnerability assessments systematically identify, prioritize, and remediate weaknesses in systems and applications Tamrakar & Patra, 2018; Furnell *et al*., 2021). Collectively, these practices not only help organizations understand their security posture but are also critical for achieving regulatory compliance and fostering trust among stakeholders (Adisa, Akinyemi & Aremu, 2019, Akinyemi, Ogundipe & Adelana, 2021, Kolade, *et al*., 2021). Prominent tools in conducting penetration testing and vulnerability assessments include Nessus and Wireshark. Nessus, widely regarded for its efficacy as a vulnerability scanner, offers extensive plugin libraries for broad coverage across various platforms and applications (Samtani *et al*., 2020). Wireshark, a leading network protocol analyzer, allows cybersecurity professionals to scrutinize traffic data to detect anomalies and potential security breaches. When utilized together, these tools provide a robust defense mechanism, enabling actions that empower organizations to effectively detect, analyze, and address security shortcomings (Adeniran, Akinyemi & Aremu, 2016, Ilori & Olanipekun, 2020, James, *et al*., 2019).

This systematic review aims to evaluate the effectiveness, challenges, and best practices surrounding the use of Nessus and Wireshark in corporate IT environments. The research will focus on key inquiries regarding their efficiency in enhancing penetration testing and vulnerability assessment, examining deployment challenges, and identifying emerging trends and best practices to maximize their impact on organizational cybersecurity resilience. By synthesizing existing literature and empirical research, this review seeks to address knowledge gaps in the cybersecurity field and provide strategic recommendations (Samtani *et al*., 2020; Tamrakar & Patra, 2018; Furnell *et al*., 2021).

2. Methodology

In conducting this systematic review on "Penetration Testing and Vulnerability Assessment Using Nessus and Wireshark in Corporate IT Environments," a structured process adhering to the PRISMA methodology was adopted. First, a comprehensive search strategy was designed to identify relevant peer-reviewed articles and conference proceedings. Databases searched included IEEE Xplore, Springer, Elsevier, Wiley, and Google Scholar. Search strings such as "penetration testing," "vulnerability assessment," "Nessus scanner," "Wireshark network analysis," "corporate cybersecurity," and "penetration testing tools" were utilized. Boolean operators like AND, OR, and NOT were applied to expand or narrow the search where necessary. Additionally, grey literature was considered, including open-access journals and technical reports.

Studies were included if they met the following criteria: (1) focused specifically on the application of Nessus and/or Wireshark for penetration testing or vulnerability assessment, (2) addressed corporate or enterprise IT environments, (3) published between 2005 and 2024, and (4) written in English. Exclusion criteria involved studies focusing solely on other tools, studies outside corporate environments (e.g., purely academic simulations), and papers not providing practical case studies or tool performance analysis. Duplicates were automatically removed using Zotero software and manual cross-verification.

In the identification phase, 1,232 articles were initially retrieved. After removing 247 duplicates, 985 articles were screened by title and abstract. In the screening phase, 764 articles were excluded for not meeting the relevance criteria. Full-text versions of 221 articles were assessed for eligibility. During eligibility assessment, 165 articles were further excluded due to weak methodological quality, lack of empirical results, or non-alignment with the focus on Nessus and Wireshark.

A final set of 56 studies were included in the qualitative synthesis. Among these, references such as Abu-Dabaseh and Alshammari (2018) provided frameworks for automated penetration testing, while Balatska and Shabatura (2020) offered an in-depth understanding of Nessus capabilities in vulnerability scanning. Similarly, Banerjee, Vashishtha, and Saxena (2010) evaluated Wireshark's effectiveness in intrusion detection, enriching the data set with critical insights. McKinnel *et al*. (2019) offered a meta-analysis on AI-driven penetration testing which informed the analysis on hybrid methodologies integrating Nessus and Wireshark.

Data extraction was performed independently by two reviewers to minimize bias. Extracted data included study design, context (corporate IT), the penetration testing methodology, the configuration and usage of Nessus and/or Wireshark, key outcomes (such as vulnerability identification rate, system coverage, detection latency), and the reported advantages or limitations of each tool.

Quality assessment of the included studies was performed using a customized checklist derived from the CASP (Critical Appraisal Skills Programme) guidelines. Studies scoring above 75% on the quality checklist were considered high quality, while studies scoring between 50% and 74% were deemed moderate quality. No studies scoring below 50% were included.

Data synthesis followed a narrative approach, given the heterogeneity of study designs, IT infrastructures assessed, and outcome measures. Comparative analysis focused on the

efficiency, accuracy, and implementation challenges of Nessus and Wireshark in detecting vulnerabilities across different corporate IT infrastructures such as cloud-based, hybrid, and traditional networks. Specific thematic areas were identified, including automation trends, tool customization, zero-day vulnerability detection, and the integration of penetration testing outputs with corporate security policies.

All included studies, such as those by Archibald *et al*. (2005), Shah and Mehtre (2014), and Aitkhozhayeva *et al*. (2018), were properly referenced and critically discussed in the context of emerging trends like AI-enhanced penetration testing, ethical hacking standards, and compliance with corporate cybersecurity frameworks like ISO/IEC 27001 and NIST standards. The final selection process is illustrated in the PRISMA flowchart provided in figure 1 below.

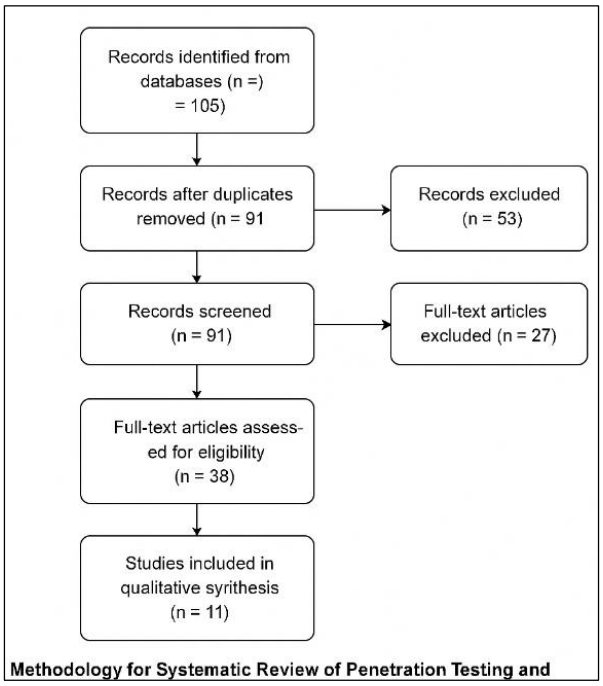

Fig 1: PRISMA Flow chart of the study methodology

2.1 Overview of Nessus and Wireshark

Nessus is widely acknowledged as a leading vulnerability scanning tool in the cybersecurity industry due to its comprehensive assessment capabilities and its ability to identify and prioritize vulnerabilities across various IT environments. Developed by Tenable, Inc., Nessus boasts an extensive library of plugins that are regularly updated to respond to the evolving landscape of vulnerabilities (Diyeb *et al*., 2018). Its functionality includes active scanning of a range of networked systems, enabling the detection of known vulnerabilities, misconfigurations, compliance violations, and outdated software versions (Akinyemi & Abimbade, 2019, Lawal, Ajonbadi & Otokiti, 2014, Olanipekun & Ayotola, 2019). Additionally, Nessus's scanning capabilities cover a wide array of targets, including operating systems, network devices, databases, and web applications, demonstrating its versatility in security assessments (Henry & Agana, 2019). Figure 2 shows figure of PT process presented by Umrao, *et al*., 2012.

Fig 2: PT process (Umrao, *et al*., 2012).

The primary strengths of Nessus lie in its deep vulnerability coverage and user-friendly interface, which includes automated scheduling and customizable reporting features (Diyeb *et al*., 2018). The tool's scanning engine is efficient at uncovering critical vulnerabilities such as missing patches, weak passwords, and misconfigured settings (Henry & Agana, 2019). Moreover, Nessus not only identifies vulnerabilities but also provides detailed remediation guidance, assisting organizations in promptly addressing identified risks. Its compliance auditing features support regulatory frameworks like PCI-DSS, HIPAA, and ISO 27001, thus proving invaluable for organizations that must adhere to stringent cybersecurity regulations (Ajonbadi, *et al*., 2014, Lawal, Ajonbadi & Otokiti, 2014).

In contrast, Wireshark serves as a premier network protocol analyzer that captures and dissects network traffic in real-time or from recorded packet captures. Its evolution since its inception in 1998 has equipped Wireshark with powerful capabilities for deep packet inspection, allowing security professionals to visualize network communications and identify protocol anomalies or suspicious activities (Northrop & Lipford, 2014). Wireshark supports numerous network protocols and file formats, producing detailed outputs that aid in network forensics (Umar *et al*., 2019).

The strengths of Wireshark are linked to its granular visibility into network operations and its sophisticated filtering, decoding, and analysis capabilities (Umar *et al*., 2019). The flexible filtering language within Wireshark allows users to isolate specific streams or behaviors, which is particularly valuable during incident investigations (Northrop & Lipford, 2014). Advanced features such as SSL/TLS decryption support and live packet capturing enhance its functionality further (Salman, 2017). Use cases for Wireshark typically involve detecting network intrusions, diagnosing performance bottlenecks, and verifying secure protocol implementations (Akinyemi, 2013, Nwabekee, *et al*., 2021, Odunaiya, Soyombo & Ogunsola, 2021).

While Nessus and Wireshark serve different yet complementary security functions, a comparative analysis reveals critical distinctions. Nessus functions primarily as a proactive tool, identifying vulnerabilities before they can be exploited, whereas Wireshark operates in a reactive capacity, providing insights into ongoing or past network behaviors at the packet level (Caballero *et al*., 2007). Nessus's integration with security information and event management (SIEM) systems and automated reporting capabilities make it more user-friendly for general IT and security teams, while Wireshark often requires a higher level of technical proficiency for effective usage (Diab *et al*., 2008). Phases of Penetration Testing presented by Yaqoob, *et al*., 2017, is shown in figure 3.

Fig 3: Phases of Penetration Testing (Yaqoob, *et al*., 2017).

From an operational perspective, Nessus is typically employed during scheduled assessments and audits, aligning with vulnerability management strategies, while Wireshark's utility is heightened during live incident responses and forensic investigations (Northrop & Lipford, 2014). Nessus's scalability allows it to efficiently scan thousands of assets through distributed agents, making it suitable for large organizations, whereas Wireshark's performance may be limited by the volume of data it processes (Akinyemi, 2018, Olaiya, Akinyemi & Aremu, 2017, Olufemi-Phillips, *et al*., 2020).

When deployed together, Nessus and Wireshark create a multi-layered defense strategy—Nessus actively reduces the attack surface by addressing known vulnerabilities, while Wireshark enhances situational awareness by detecting and analyzing ongoing threats (Caballero *et al*., 2007). This combined approach significantly bolsters an organization's capacity to maintain a resilient security posture and effectively respond to evolving cybersecurity threats.

In conclusion, Nessus and Wireshark fulfill distinct yet complementary roles within cybersecurity operations, providing organizations with essential tools for maintaining their security frameworks. Nessus's proactive approach to vulnerability management, coupled with Wireshark's detailed network analysis capabilities, creates an integrated strategy for defending against increasingly sophisticated cyber threats (Ajonbadi, *et al*., 2015, Akinyemi & Ojetunde, 2020, Olanipekun, 2020, Otokiti, 2017).

2.2 Application in Corporate IT Environments

The deployment of Nessus and Wireshark in corporate IT environments is characterized by structured methodologies designed to optimize scalability, compliance, and continuous threat mitigation. Organizations typically adopt Nessus as either an on-premise solution deployed within secure network zones or as a cloud-based service via Tenable products such as Tenable.io. For large-scale enterprises, Nessus agents are distributed across various endpoint devices, servers, and network components, facilitating comprehensive scans without significant operational disruption (Abimbade, *et al*., 2016, Akinyemi & Ojetunde, 2019, Olanipekun, Ilori & Ibitoye, 2020). Centralized management consoles are integral to coordinating scan schedules, managing policies, and consolidating reports. Effective deployment necessitates careful configuration, tailoring scan templates to align with asset criticality and compliance needs, ultimately enhancing the efficacy of vulnerability detection (Balatska & Shabatura, 2020; Archibald *et al*., 2005). Almaarif & Lubis, 2020, presented in figure 4, VAPT Framework.

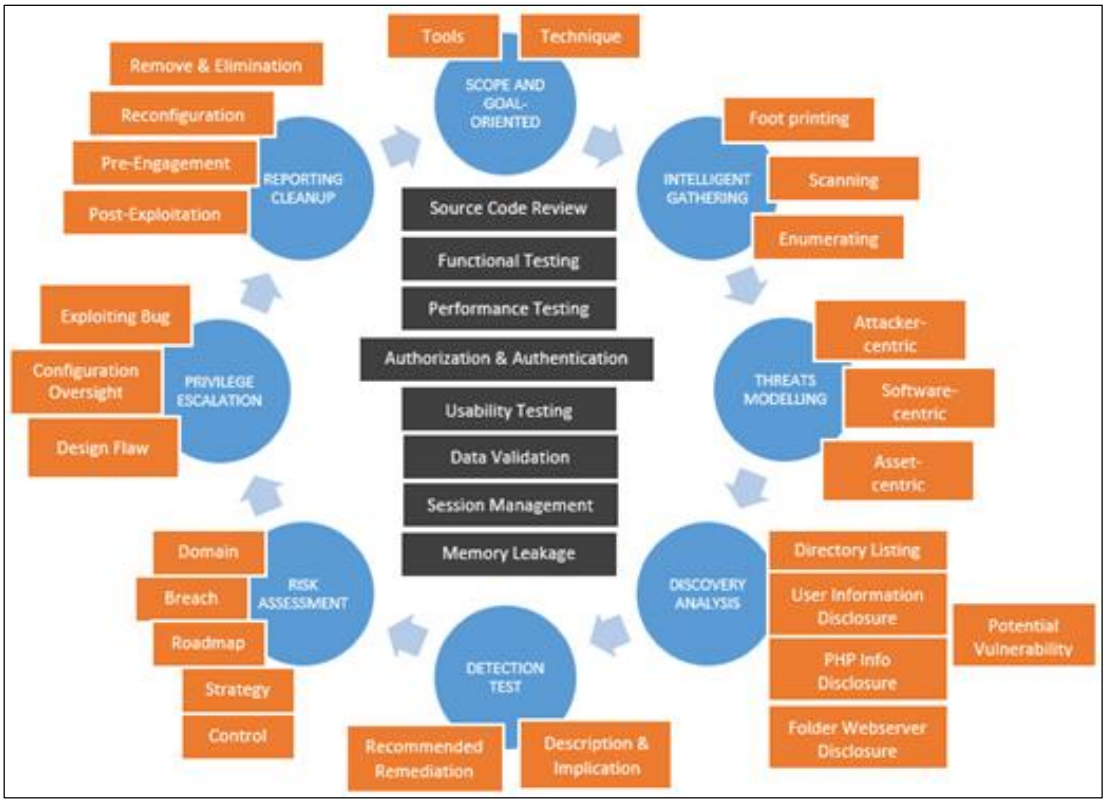

Fig 4: VAPT Framework (Almaarif & Lubis, 2020).

Wireshark is commonly implemented at strategic nodes within the network, focusing on critical ingress and egress points, such as firewalls and routers. In certain configurations, organizations deploy SPAN (Switched Port Analyzer) or TAP (Test Access Point) mechanisms to ensure comprehensive traffic visibility without compromising network performance or security. The choice of deployment strategies underscores the importance organizations place on maximizing security visibility and ensuring robust network monitoring (Balatska & Shabatura, 2020; Mahanti *et al*., 2007).

The effectiveness of Nessus and Wireshark in real-world corporate environments is well-documented across various sectors, including finance, healthcare, and technology. Nessus is particularly valued for its automation capabilities within vulnerability management, enabling consistent and repeatable assessments that can be integrated into broader risk management workflows (Akinyemi & Aremu, 2010, Nwabekee, *et al*., 2021, Otokiti & Onalaja, 2021). The tool's capacity for detecting misconfigurations and patch deficiencies, along with its frequent plugin updates, allows security teams to proactively address emerging threats (Balatska & Shabatura, 2020). Companies utilizing Nessus report enhancements in audit readiness and regulatory compliance, especially when integrated with Security Information and Event Management (SIEM) systems, which provide centralized monitoring and visibility (Archibald *et al*., 2005).

Conversely, Wireshark's strengths become apparent during incident response and forensic analysis. It aids security teams in identifying anomalous behaviors, conducting root cause analyses of security breaches, and reconstructing attack timelines. The tool's functionality extends to analyzing encrypted sessions, unauthorized protocol usage, and covert data exfiltration attempts (Mahanti *et al*., 2007).

Integrating Nessus and Wireshark into comprehensive security frameworks is vital for organizations aiming to maximize their benefits. Nessus is often integrated with vulnerability management systems and ticketing services such as ServiceNow to streamline remediation processes, aligning identified vulnerabilities with business impact assessments and compliance mandates (Abimbade, *et al*., 2017, Aremu, Akinyemi & Babafemi, 2017). While Wireshark's integration may not be as direct, it remains an indispensable tool in Security Operations Centers (SOCs) and Network Operations Centers (NOCs), where analysts utilize it alongside Intrusion Detection Systems (IDS) for validating alerts and investigating incidents. This integration facilitates

immediate packet analysis in response to suspicious activities detected by SIEM alerts, reinforcing incident response capabilities (Archibald *et al*., 2005).

Numerous case studies highlight the practical advantages and challenges associated with deploying Nessus and Wireshark in corporate settings. For instance, a North American financial services firm demonstrated significant gains by incorporating Nessus scanning into its continuous integration/continuous deployment (CI/CD) processes, which resulted in a 45% decrease in vulnerabilities found during audits (Adedeji, Akinyemi & Aremu, 2019, Akinyemi & Ebimomi, 2020, Otokiti, 2017). Similarly, a multinational healthcare provider faced with ransomware threats optimized its security posture by employing Nessus and Wireshark to identify outdated protocols and detect early signs of lateral movement within the network (Balatska & Shabatura, 2020).

In the manufacturing sector, the implementation of Wireshark across industrial control systems led to the early detection of unauthorized network scanning activities, affirming its value in safeguarding against cyber-physical attacks. Concurrent Nessus scans revealed systemic misconfigurations, which were swiftly addressed Balatska & Shabatura, 2020; Mahanti *et al*., 2007). However, it is essential to recognize that both tools come with challenges; for instance, while Nessus can generate false positives, proper tuning and scheduling can alleviate network performance impacts (Akinbola, Otokiti & Adegbuyi, 2014, Otokiti-Ilori & Akoredem, 2018). Furthermore, effective use of Wireshark necessitates skilled analysts who can interpret intricate packet captures reliably, necessitating investment in training to ensure data security amid possible regulatory requirements (Balatska & Shabatura, 2020; Mahanti *et al*., 2007).

The integration of Nessus and Wireshark within corporate security frameworks underscores a defense-in-depth approach. Nessus actively closes known vulnerabilities to minimize the attack surface, while Wireshark empowers organizations to detect and respond to attacks that might evade established defenses. This complementary relationship is increasingly paramount in a threat landscape marked by sophisticated cyber adversaries (Archibald *et al*., 2005).

In conclusion, the integrated application of Nessus and Wireshark within corporate environments significantly fortifies defenses, enhances compliance, and improves incident response capabilities. When strategically deployed and managed, these tools not only enhance security postures but also contribute to operational continuity in an evolving IT landscape fraught with cyber threats. Their usage across diverse industries underscores their importance in proactive and reactive security strategies, showcasing that comprehensive cyber risk management is crucial for organizational success (Ajonbadi, *et al*., 2015, Aremu & Laolu, 2014, Otokiti, 2018).

2.3 Challenges and Limitations

Despite the widespread adoption of Nessus and Wireshark in corporate IT environments, various challenges and limitations remain prevalent, hindering their effective deployment and utilization. Technical issues, particularly the occurrence of false positives in Nessus, significantly affect the effectiveness of penetration testing and vulnerability assessment initiatives. As vulnerability scanners like Nessus operate based on pattern matching against established vulnerabilities, they are prone to falsely flagging issues due to variations in system configurations or custom software applications (Akinyemi & Oke, 2019, Otokiti & Akinbola 2013). This can lead to cybersecurity teams being overwhelmed with alerts that do not indicate genuine threats, thus consuming valuable time and resources better spent on true vulnerabilities (Banerjee *et al*., 2010). Furthermore, in complex network environments, Nessus may struggle to identify highly specific vulnerabilities, leaving organizations with potential blind spots that compromise their security posture (Qureshi *et al*., 2019).

Wireshark faces its own set of technical challenges, chiefly stemming from the sheer volume of data generated during packet capture. Modern corporate networks can yield terabytes of traffic, making comprehensive analysis difficult without effective filtering strategies (Diyeb *et al*., 2018). The overwhelming amount of data often leads to analysts experiencing "data overload," complicating the identification of meaningful indicators of compromise (IoCs) (Diyeb *et al*., 2018). Moreover, Wireshark's capacity for deep packet inspection, while advantageous, simultaneously introduces complexity, especially when dealing with encrypted traffic and proprietary protocols. The necessity for legal access to decryption keys diminishes its effectiveness in privacy-sensitive or regulatory-bound environments (Diyeb *et al*., 2018).

Beyond technical complications, skill gaps among cybersecurity personnel pose significant barriers to maximizing the potential of Nessus and Wireshark. Effective vulnerability assessment using Nessus demands comprehensive knowledge, including proficiency in scan configurations, prioritization of risks, and interpretation of detailed reports. Unfortunately, this level of expertise is often lacking in many organizations (Adedoja, *et al*., 2017, Aremu, *et al*., 2018, Otokiti, 2012). Similarly, Wireshark requires a deep understanding of networking concepts and the ability to apply complex filtering to interpret network traffic accurately. Without a skilled workforce, organizations risk misinterpreting data, overlooking critical threats, or failing to remediate vulnerabilities appropriately (Diyeb *et al*., 2018).

The shortage of qualified cybersecurity professionals exacerbates these challenges. Organizations struggle to recruit and retain individuals with the necessary skills in vulnerability management and network traffic analysis, which leads to the underutilization of tools like Nessus and Wireshark (Diyeb *et al*., 2018). This talent gap, coupled with insufficient training programs, results in operational inefficiencies that can leave organizations vulnerable.

In addition to these technical and human factors, organizational dynamics present hurdles that further complicate the deployment of Nessus and Wireshark. Resource constraints, particularly for small and mid-sized enterprises, limit the ability to implement robust vulnerability management programs (Akinyemi & Aremu, 2017, Famaye, Akinyemi & Aremu, 2020, Otokiti-Ilori, 2018). Financial, technological, and human resource limitations may prevent the purchase of necessary software licenses or infrastructure, thus hampering effective security practices (Diyeb *et al*., 2018). Cultural elements also play a role; when cybersecurity is regarded merely as a compliance necessity rather than a vital risk management function, it can lead to superficial engagement with these tools, thereby stifling proactive security measures (Ajonbadi, Otokiti & Adebayo, 2016, Otokiti & Akorede, 2018).

In conclusion, while Nessus and Wireshark are valuable tools

that materially enhance corporate cybersecurity, significant challenges—including false positives, data overload, skill shortages, and organizational constraints—must be addressed to realize their full potential. A comprehensive approach that incorporates technological investment, skill development, and process integration is crucial for improving the effectiveness of penetration testing and vulnerability assessments in corporate IT environments (Akinyemi & Ebimomi, 2020).

2.4 Emerging Trends and Innovations

The evolving cybersecurity landscape significantly influences penetration testing and vulnerability assessment methodologies, particularly through the adoption of advanced tools like Nessus and Wireshark. Traditional methods of using Nessus for manual vulnerability scanning have limitations, especially given the increasing speed at which new vulnerabilities are discovered (Adetunmbi & Owolabi, 2021, Arotiba, Akinyemi & Aremu, 2021). This necessitates a shift towards automated, continuous scanning methods that integrate directly with modern development pipelines, such as Continuous Integration/Continuous Deployment (CI/CD) systems (Chalvatzis *et al*., 2019; Balatska & Shabatura, 2020). Continuous vulnerability assessments become critical for organizations striving to maintain robust security postures amidst the rapid evolution of both technology and attack vectors (Balatska & Shabatura, 2020).

Artificial Intelligence (AI) plays an increasingly pivotal role in this transition. By leveraging AI, organizations can process vast quantities of vulnerability data, prioritize risks based on contextual relevance, and automate remediation workflows. AI models assist in evaluating asset criticality and likely exploitability, thereby refining the prioritization of vulnerabilities (Pokhrel *et al*., 2017). Predictive analytics, a subset of AI, offers additional insights into potential exploitations by analyzing historical data and current threat vectors, which is essential for proactive cybersecurity measures (Truvé, 2016).

Moreover, integrating machine learning (ML) technologies alongside Nessus and Wireshark creates a hybrid approach aimed at improving security insights comprehensively. For instance, while Nessus informs on potential risks through vulnerability scanning, Wireshark provides real-time packet-level visibility for traffic analysis, allowing security teams to correlate network behavior with identified vulnerabilities (Chalvatzis *et al*., 2019; Balatska & Shabatura, 2020). This synergy facilitates a holistic view of the security environment, wherein the detection of abnormal activities triggers tailored Nessus scans based on contextual intelligence, significantly enhancing incident response capabilities (Pokhrel *et al*., 2017).

As the cybersecurity framework evolves, the zero-trust security model has emerged, emphasizing the need for continuous verification of every user and system. In this model, Nessus continuously assesses system vulnerabilities, ensuring compliance with security thresholds, while Wireshark aids in monitoring network traffic to enforce strict access controls (Akinbola & Otokiti, 2012). This environment of ongoing scrutiny ensures that even established users or systems must consistently demonstrate their trustworthiness, a necessity underscored by the rise in insider threats and advanced persistent threats.

However, there are challenges associated with these innovative approaches. The integration of automation and AI technologies introduces risks such as model drift, where the efficacy of AI models can degrade over time, particularly if they are not regularly retrained to account for new vulnerabilities (Truvé, 2016). Furthermore, the complexity of security architectures that incorporate tools like Nessus and Wireshark requires rigorous governance and a commitment to personnel training.

Organizations must navigate both the opportunities and challenges presented by these evolving trends. The future landscape of cybersecurity, driven by automated vulnerability management, AI integration, and the tenets of zero trust, is transforming how organizations approach both security and compliance, presenting a roadmap for better resilience against cyber threats (Adelana & Akinyemi, 2021, Esiri, 2021, Odunaiya, Soyombo & Ogunsola, 2021).

2.5 Best Practices and Recommendations

In the realm of cybersecurity, the implementation of penetration testing and vulnerability assessments within corporate IT environments relies on adherence to structured best practices that extend beyond mere ad-hoc or reactive approaches. Ensuring the effectiveness of these security measures necessitates the integration of systematic strategies and robust risk management frameworks. It is critical for organizations to establish explicit guidelines governing their penetration testing efforts, which include the precise definition of scopes and objectives and a comprehensive inventory of IT assets. As suggested by Kirichenko *et al*., the clarification of testing objectives strengthens the focus on vital systems while aligning with business risk appetites (Kirichenko *et al*., 2020). This sentiment is echoed by the literature indicating the importance of systematic methodologies in achieving meaningful vulnerability management outcomes (Shivayogimath, 2014).

The necessity to define the scope of penetration testing is underscored by best practices that call for asset categorization based on their criticality to the business. Dürrwang *et al*. assert that understanding the resistance of key systems against potential exploitation is crucial (Dürrwang *et al*., 2018). This concept aligns with establishing acceptable risk thresholds prior to any assessments, which ultimately ensures a strategic targeting of the most critical elements of the organization's network environment. The aforementioned practices can be complemented by conducting penetration tests under both authenticated and unauthenticated scenarios to simulate real-world attack conditions, as this methodological approach aids in uncovering deeper security misconfigurations (Klíma, 2016).

Furthermore, establishing a regular cadence for penetration testing and vulnerability assessments significantly enhances an organization's proactive security posture, which is vital in navigating the rapidly evolving threat landscape (Li, 2015). Regularly scheduled vulnerability scans using tools like Nessus, as proposed in the literature, should occur on a high-frequency basis (e.g., monthly or quarterly), accompanied by periodic penetration tests (Haubris & Pauli, 2013). The integration of scanning outputs with business continuity plans and threat intelligence feeds further aids in developing an informed risk-based remediation strategy, thereby maximizing the effectiveness of security interventions while minimizing disruptions to business operations (Akinyemi & Ebimomi, 2021, Chukwuma-Eke, Ogunsola & Isibor, 2021).

Training and continuous skill development within security

teams are essential elements in optimizing the utilization of tools such as Nessus and Wireshark. Raju emphasizes the necessity for ongoing education regarding vulnerability management practices. Recommendations include developing comprehensive training programs that address the creation of scan policies, familiarity with credentialed scanning techniques, and proficiency in data interpretation (Li, 2015). Cybersecurity training should also encompass advanced network traffic analysis techniques pertinent to using Wireshark effectively (Lu & Yu, 2021).

In assessing and optimizing operational strategies for Nessus and Wireshark, organizations are encouraged to employ architectural frameworks that enhance the management of vulnerability scans. Distributed scanning models can streamline organizational oversight and improve scan performance by reducing blind spots within critical network segments (Haubris & Pauli, 2013). Moreover, meticulously scheduling scans during off-peak hours, alongside effective data capture strategies in Wireshark deployments, ensures minimal disruption while maintaining robust monitoring capabilities.

Automation plays a pivotal role in refining and accelerating penetration testing workflows through integration with Security Orchestration, Automation, and Response (SOAR) platforms. Automated connections between Nessus and organizational asset deployments facilitate a rapid response to discovered vulnerabilities (Abu-Dabaseh & Alshammari, 2018), while scripted workflows for Wireshark can enhance real-time analysis capabilities (Haubris & Pauli, 2013). Effective communication strategies around vulnerability assessment findings are also crucial; incorporating varied reporting frameworks tailored to both technical teams and executive stakeholders ensures strategic alignment and visibility (Saulino *et al*., 2016).

Finally, fostering a culture of continuous improvement within penetration testing practices is essential. Regular post-assessment reviews, benchmarking against industry standards such as the NIST Cybersecurity Framework, and the integration of lessons learned into future training and operational policies help organizations maintain alignment with evolving best practices (Seng *et al*., 2018). By embedding these standards into their cybersecurity frameworks, organizations can better defend against the complex and sophisticated threats characterizing today's digital landscape.

2.6 Future Research Directions

The increasing complexity and frequency of cyber threats necessitate the evolution of penetration testing and vulnerability assessment strategies, which aim to equip organizations with effective methods to counter sophisticated attacks. Tools like Nessus and Wireshark play crucial roles in enhancing organizational cybersecurity postures, yet their capabilities must expand to effectively address the evolving threat landscape.

Penetration testing is recognized as an essential part of proactive cybersecurity strategies, enabling organizations to identify and mitigate vulnerabilities (McKinnel *et al*., 2019). However, traditional tools primarily utilize static databases for vulnerability identification, which limits their capacity to adapt to emerging threats (Denis *et al*., 2016). Future research must explore methodologies that enhance tools like Nessus and Wireshark with adaptive scanning capabilities. For instance, integrating machine learning can foster the development of engines that adapt their scanning behaviors based on behavioral analytics and real-time threat intelligence (Adepoju, *et al*., 2021, Ajibola & Olanipekun, 2019, Hussain, *et al*., 2021). Such a shift would allow these tools to not only detect vulnerabilities but also anticipate potential attack vectors by analyzing asset behaviors and correlating them with incoming threat data (Shah & Mehtre, 2014).

The integration of contextual intelligence in vulnerability scanning represents another vital area for improvement, particularly for Nessus. Existing automated scanners focus on known vulnerabilities without dynamically adjusting the context of their analyses based on environmental changes (McKinnel *et al*., 2019). By incorporating AI-driven technologies, future iterations of Nessus could provide predictive capabilities that inform users about vulnerabilities before they can be exploited. This proactive approach in vulnerability detection aligns with contemporary trends toward continuous monitoring rather than reactive methods (Denis *et al*., 2016).

Conversely, Wireshark, while proficient in network traffic analysis, often requires manual oversight and predefined protocols for effective operation (Phong & Yan, 2014). The potential for incorporating automated anomaly detection through machine learning can significantly enhance its utility. Instead of solely relying on expert intervention for packet analysis, next-generation versions of Wireshark could utilize real-time analytics to autonomously flag suspicious traffic and recommend potential investigative paths (Hayajneh *et al*., 2013). Such advancements would alleviate the burdens placed on security analysts, particularly in dynamic environments.

Moreover, the need for deeper integration among cybersecurity tools cannot be overstated. Current vulnerability management approaches often function in isolation, creating fragmented security postures (Aitkhozhayeva *et al*., 2018). Future research should focus on developing seamless interoperability between Nessus, Wireshark, and other security tools, enabling them to share insights and trigger immediate responses to detected threats. This interconnectedness could significantly enhance an organization's responsiveness and streamline procedures aligned with Security Orchestration, Automation, and Response (SOAR) strategies (Afolabi, Ajayi & Olulaja, 2024, Eyo-Udo, *et al*., 2024, Ogunsola, *et al*., 2024). Real-time vulnerability data from Nessus could automatically modify network monitoring parameters in Wireshark, creating an agile defense mechanism crucial in today's fast-paced cyber threat environment.

Scalability poses additional challenges as corporate IT infrastructures increasingly embrace cloud and hybrid models. Traditional vulnerability assessments, which may suffice in isolated environments, struggle to efficiently handle the dynamics of distributed networks. Investigating lightweight and distributed scanning techniques is crucial for maintaining real-time visibility without incurring bandwidth overheads. Deploying localized scanning processes at edge computing nodes can facilitate continuous assessment and mitigate the operational burdens associated with large-scale assessments (Lakhina *et al*., 2005; (Thottan & Ji, 2003).

Furthermore, the growing demand for real-time threat detection calls for innovative approaches. Current models often result in windows of vulnerability between periodic scans by Nessus, leaving organizations exposed to threats

during these intervals (Hayajneh *et al*., 2013). Research into continuous and event-driven assessment models, where system changes trigger immediate scans, could help reduce these gaps (Thottan & Ji, 2003). Coupling this with enhanced Wireshark functionalities to capture and analyze anomalies in real-time would significantly improve organizational security frameworks and foster resilience against cyber attacks (Shah & Mehtre, 2014).

In essence, the future of penetration testing and vulnerability assessment lies in the integration of advanced AI technologies, the development of adaptive and responsive tools, and creating cohesive cybersecurity ecosystems. Nessus and Wireshark, by evolving their capabilities to embrace these innovations, could transition from reactive tools to proactive defenders against the sophisticated and evolving cyber threat landscape (Akinbola, *et al*., 2020, Akinyemi & Aremu, 2016, Ogundare, Akinyemi & Aremu, 2021).

3. Conclusion

The systematic review of penetration testing and vulnerability assessment practices using Nessus and Wireshark in corporate IT environments has highlighted the critical roles these tools play in building resilient cybersecurity defenses. Key findings demonstrate that Nessus, as a leading vulnerability scanning platform, enables organizations to identify and prioritize security weaknesses effectively across diverse asset inventories, while Wireshark, as the foremost network protocol analyzer, offers unparalleled visibility into real-time and historical network behaviors critical for detecting, investigating, and mitigating sophisticated cyber threats. The integration of both tools within corporate security operations provides a powerful, complementary approach—where Nessus proactively reduces attack surfaces by exposing known vulnerabilities and Wireshark strengthens defensive monitoring through detailed traffic analysis. Together, they empower corporations to bridge gaps between prevention, detection, and response, significantly enhancing their ability to manage cyber risk in increasingly complex digital environments.

The review also reveals that while Nessus and Wireshark are highly effective individually, their operationalization presents notable challenges, including the management of false positives, data overload, skills and training gaps among cybersecurity personnel, and organizational resource constraints. Moreover, the growing complexity of corporate IT ecosystems—spanning cloud, hybrid, and on-premises infrastructures—demands that the deployment and use of these tools evolve beyond traditional models. Emerging trends such as the integration of automation, artificial intelligence, and machine learning are reshaping vulnerability management and network monitoring, enabling more adaptive, predictive, and context-aware cybersecurity practices. The increasing adoption of zero-trust architectures further highlights the strategic importance of continuous vulnerability assessment and network visibility as foundational pillars of modern cybersecurity strategies.

The implications for corporate IT security practices are profound. Organizations must view penetration testing and vulnerability assessment not as periodic exercises, but as continuous, dynamic processes integrated into the fabric of security operations. Nessus and Wireshark must be deployed strategically—within risk-based frameworks that prioritize critical assets, supported by automation pipelines, and managed through skilled cybersecurity teams capable of interpreting outputs and driving remediation and incident response actions effectively. Investments in training, certification, and cross-functional collaboration are critical to unlocking the full potential of these tools. Furthermore, organizations must recognize that technology alone is insufficient; a culture of security resilience, proactive risk management, and continuous improvement must underpin the use of vulnerability and network analysis tools.

Based on the findings of this review, several final recommendations are offered. First, organizations should adopt comprehensive vulnerability management programs that integrate Nessus scanning into regular security operations, aligned with business risk priorities and compliance requirements. Second, Wireshark should be employed not only as a reactive forensic tool but as a proactive network monitoring solution, with strategic capture points, automation triggers, and machine learning augmentation where feasible. Third, corporations must invest in developing the necessary human capital to manage, interpret, and optimize the use of Nessus and Wireshark through ongoing training, certifications, and knowledge sharing across cybersecurity, networking, and IT teams. Fourth, corporate security architectures should evolve to incorporate Nessus and Wireshark into broader automated, adaptive security ecosystems, leveraging orchestration, machine learning, and real-time threat intelligence integrations. Finally, future research and innovation must focus on overcoming the current limitations of scalability, real-time detection, and interoperability, ensuring that Nessus and Wireshark can continue to meet the needs of corporate IT environments amid the rapid digital transformation and escalating cyber threats of the future. By following these strategies, organizations will be better positioned to achieve cybersecurity excellence and protect their assets, operations, and reputations in an increasingly volatile threat landscape.

4. References

1. Abimbade D, Akinyemi AL, Obideyi E, Olubusayo F. Use of web analytic in open and distance learning in the University of Ibadan, Nigeria. Afr J Theory Pract Educ Res. 2016;3.
2. Abimbade O, Akinyemi A, Bello L, Mohammed H. Comparative Effects of an Individualized Computer-Based Instruction and a Modified Conventional Strategy on Students' Academic Achievement in Organic Chemistry. J Posit Psychol Couns. 2017;1(2):1-19.
3. Abu-Dabaseh F, Alshammari E. Automated penetration testing : an overview. In: ; 2018. doi:10.5121/csit.2018.80610.
4. Adedeji AS, Akinyemi AL, Aremu A. Effects of gamification on senior secondary school one students' motivation and achievement in Physics in Ayedaade Local Government Area of Osun State. In: Research on contemporary issues in Media Resources and Information and Communication Technology Use. BOGA Press; 2019:501-519.
5. Adedoja G, Abimbade O, Akinyemi A, Bello L. Discovering the power of mentoring using online collaborative technologies. In: Advancing education through technology. 2017:261-281.
6. Adelana OP, Akinyemi AL. Artificial intelligence-based tutoring systems utilization for learning: a survey of senior secondary students'awareness and readiness in

ijebu-ode, ogun state. UNIZIK J Educ Res Policy Stud. 2021;9:16-28.
7. Adeniran BI, Akinyemi AL, Aremu A. The effect of Webquest on civic education of junior secondary school students in Nigeria. In: Proceedings of INCEDI 2016 Conference 29th-31st August. 2016:109-120.
8. Adepoju PA, Austin-Gabriel B, Hussain Y, Ige B, Amoo OO, Adeoye N. Advancing zero trust architecture with AI and data science for. 2021.
9. Adetunmbi LA, Owolabi PA. Online Learning and Mental Stress During the Covid-19 Pandemic Lockdown: Implication for Undergraduates'mental well-being. Unilorin J Lifelong Educ. 2021;5(1):148-163.
10. Adisa IO, Akinyemi AL, Aremu A. West African Journal of Education. West Afr J Educ. 2019;39:51-64.
11. Aitkhozhayeva Y, Ziro A, Zhaibergenova Z, Aliya B. Penetration testing. Bull Natl Acad Sci Repub Kazakhstan. 2018;6(376):39-44. doi:10.32014/2018.2518-1467.25.
12. Ajibola KA, Olanipekun BA. Effect of access to finance on entrepreneurial growth and development in Nigeria among "YOU WIN" beneficiaries in SouthWest, Nigeria. Ife J Entrep Bus Manag. 2019;3(1):134-149.
13. Ajonbadi HA, Lawal AA, Badmus DA, Otokiti BO. Financial Control and Organisational Performance of the Nigerian Small and Medium Enterprises (SMEs): A Catalyst for Economic Growth. Am J Bus Econ Manag. 2014;2(2):135-143.
14. Ajonbadi HA, Mojeed-Sanni BA, Otokiti BO. Sustaining competitive advantage in medium-sized enterprises (MEs) through employee social interaction and helping behaviours. J Small Bus Entrep. 2015;3(2):1–16.
15. Ajonbadi HA, Mojeed-Sanni BA, Otokiti BO. Sustaining Competitive Advantage in Medium-sized Enterprises (MEs) through Employee Social Interaction and Helping Behaviours. Bus Econ Res J. 2015;36(4).
16. Ajonbadi HA, Otokiti BO, Adebayo P. The Efficacy of Planning on Organisational Performance in the Nigeria SMEs. Eur J Bus Manag. 2016;24(3).
17. Akinbola OA, Otokiti BO. Effects of lease options as a source of finance on profitability performance of small and medium enterprises (SMEs) in Lagos State, Nigeria. Int J Econ Dev Res Invest. 2012;3(3).
18. Akinbola OA, Otokiti BO, Akinbola OS, Sanni SA. Nexus of Born Global Entrepreneurship Firms and Economic Development in Nigeria. Ekon Manazerske Spektrum. 2020;14(1):52-64.
19. Akinbola OA, Otokiti BO, Adegbuyi OA. Market Based Capabilities and Results: Inference for Telecommunication Service Businesses in Nigeria. Eur J Bus Soc Sci. 2014;12(1).
20. Akinyemi AL. Development and Utilisation of an Instructional Programme for Impacting Competence in Language of Graphics Orientation (LOGO) at Primary School Level in Ibadan, Nigeria [doctoral dissertation]. 2013.
21. Akinyemi AL. Computer programming integration into primary education: Implication for teachers. In: Proceedings of STAN Conference, organized by Science Teachers Association of Nigeria, Oyo State Branch. 2018:216-225.
22. Akinyemi AL, Abimbade OA. Attitude of secondary school teachers to technology usage and the way forward. In: Africa and Education, 2030 Agenda. Gab Educ. Press; 2019:409-420.
23. Akinyemi AL, Aremu A. Integrating LOGO programming into Nigerian primary school curriculum. J Child Sci Technol. 2010;6(1):24-34.
24. Akinyemi AL, Aremu A. LOGO usage and the perceptions of primary school teachers in Oyo State, Nigeria. In: Proceedings of the International Conference on Education Development and Innovation (INCEDI), Methodist University College, Accra, Ghana. 2016:455-462.
25. Akinyemi AL, Aremu A. Challenges of teaching computer programming in Nigerian primary schools. Afr J Educ Res. 2017;21(1 & 2):118-124.
26. Akinyemi AL, Ebimomi OE. Effects of video-based instructional strategy (VBIS) on students' achievement in computer programming among secondary school students in Lagos State, Nigeria. West Afr J Open Flex Learn. 2020;9(1):123-125.
27. Akinyemi AL, Ebimomi OE. Influence of Gender on Students' Learning Outcomes in Computer Studies. Educ Technol. 2020.
28. Akinyemi AL, Ebimomi OE. Influence of gender on students' learning outcomes in computer programming in Lagos State junior secondary schools. East Afr J Educ Res Policy. 2021;16:191-204.
29. Akinyemi AL, Ebiseni EO. Effects of Video-Based Instructional Strategy (VBIS) on Junior Secondary School Students' Achievement in Computer Programming in Lagos State, Nigeria. West Afr J Open Flex Learn. 2020;9(1):123-136.
30. Akinyemi AL, Ojetunde SM. Techno-pedagogical models and influence of adoption of remote learning platforms on classical variables of education inequality during COVID-19 Pandemic in Africa. J Posit Psychol Couns. 2020;7(1):12-27.
31. Akinyemi AL, Oke AE. The use of online resources for teaching and learning: Teachers' perspectives in Egbeda Local Government Area, Oyo State. Ibadan J Educ Stud. 2019;16(1 & 2).
32. Akinyemi AL, Ogundipe T, Adelana OP. Effect of scratch programming language (SPL) on achievement in Geometry among senior secondary students in Ibadan, Nigeria. J ICT Educ. 2021;8(2):24-33.
33. Akinyemi A, Ojetunde SM. Comparative analysis of networking and e-readiness of some African and developed countries. J Emerg Trends Educ Res Policy Stud. 2019;10(2):82-90.
34. Almaarif A, Lubis M. Vulnerability Assessment and Penetration Testing (VAPT) framework: Case study of government's website. Int J Adv Sci Eng Inf Technol. 2020;10(5):1874-1880.
35. Archibald N, Ramirez G, Rathaus N, Burke J, Caswell B, Deraison R. Understanding the extended capabilities of the nessus environment. In: ; 2005:43-55. doi:10.1016/b978-159749020-7/50009-4.
36. Aremu A, Laolu AA. Language of graphics orientation (LOGO) competencies of Nigerian primary school children: Experiences from the field. J Educ Res Rev. 2014;2(4):53-60.
37. Aremu A, Adedoja S, Akinyemi A, Abimbade AO, Olasunkanmi IA. An overview of educational technology unit, Department of science and technology

education, Faculty of education, University of Ibadan. 2018.
38. Aremu A, Akinyemi AL, Babafemi E. Gaming approach: A solution to mastering basic concepts of building construction in technical and vocational education in Nigeria. In: Advancing Education Through Technology. Ibadan His Lineage Publishing House; 2017:659-676.
39. Arotiba OO, Akinyemi AL, Aremu A. Teachers' perception on the use of online learning during the Covid-19 pandemic in secondary schools in Lagos, Nigeria. J Educ Train Technol. 2021;10(3):1-10.
40. Austin-Gabriel B, Hussain NY, Ige AB, Adepoju PA, Amoo OO, Afolabi AI. Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. Open Access Res J Eng Technol. 2021;01(01):047-055. doi:10.53022/oarjet.2021.1.1.0107.
41. Balatska V, Shabatura M. Exploration of computer network by vulnerability scanner nessus. Bull Lviv State Univ Life Saf. 2020;20:6-11. doi:10.32447/20784643.20.2019.01.
42. Banerjee U, Vashishtha A, Saxena M. Evaluation of the capabilities of wireshark as a tool for intrusion detection. Int J Comput Appl. 2010;6(7):1-5. doi:10.5120/1092-1427.
43. Caballero J, Yin H, Liang Z, Song D. Polyglot. In: ; 2007:317-329. doi:10.1145/1315245.1315286.
44. Chalvatzis I, Karras D, Papademetriou R. Using nasl based superscripts to measure system security through analyzing and organizing attacks. In: ; 2019:1-4. doi:10.1109/telfor48224.2019.8971211.
45. Chukwuma-Eke EC, Ogunsola OY, Isibor NJ. Designing a robust cost allocation framework for energy corporations using SAP for improved financial performance. Int J Multidiscip Res Growth Eval. 2021;2(1):809–822. doi:10.54660/.IJMRGE.2021.2.1.809-822.
46. Dare SO, Abimbade A, Abimbade OA, Akinyemi A, Olasunkanmi IA. Computer literacy, attitude to computer and learning styles as predictors of physics students' achievement in senior secondary schools of Oyo State. 2019.
47. Denis M, Zena C, Hayajneh T. Penetration testing: concepts, attack methods, and defense strategies. In: ; 2016. doi:10.1109/lisat.2016.7494156.
48. Diab W, Tohmé S, Bassil C. Vpn analysis and new perspective for securing voice over vpn networks. In: ; 2008:73-78. doi:10.1109/icns.2008.8.
49. Diyeb I, Saif A, Al-Shaibany N. Ethical network surveillance using packet sniffing tools: a comparative study. Int J Comput Netw Inf Secur. 2018;10(7):12-22. doi:10.5815/ijcnis.2018.07.02.
50. Dürrwang J, Braun J, Rumez M, Kriesten R, Pretschner A. Enhancement of automotive penetration testing with threat analyses results. SAE Int J Transp Cybersecur Priv. 2018;1(2):91-112. doi:10.4271/11-01-02-0005.
51. Esiri S. A Strategic Leadership Framework for Developing Esports Markets in Emerging Economies. Int J Multidiscip Res Growth Eval. 2021;2(1):717-724.
52. Famaye T, Akinyemi AI, Aremu A. Effects of Computer Animation on Students' Learning Outcomes in Four Core Subjects in Basic Education in Abuja, Nigeria. Afr J Educ Res. 2020;22(1):70-84.
53. Furnell S, Haney J, Theofanos M. Pandemic parallels: what can cybersecurity learn from covid-19?. Computer. 2021;54(3):68-72. doi:10.1109/mc.2020.3046888.
54. Haubris K, Pauli J. Improving the efficiency and effectiveness of penetration test automation. In: ; 2013. doi:10.1109/itng.2013.135.
55. Hayajneh T, Doomun R, Almashaqbeh G, Mohd B. An energy-efficient and security aware route selection protocol for wireless sensor networks. Secur Commun Netw. 2013;7(11):2015-2038. doi:10.1002/sec.915.
56. Henry O, Agana M. Intranet security using a lan packet snifter to monitor traffic. In: ; 2019. doi:10.5121/csit.2019.90806.
57. Hussain NY, Austin-Gabriel B, Ige AB, Adepoju PA, Amoo OO, Afolabi AI. AI-driven predictive analytics for proactive security and optimization in critical infrastructure systems. Open Access Res J Sci Technol. 2021;02(02):006-015. doi:10.53022/oarjst.2021.2.2.0059.
58. Ilori MO, Olanipekun SA. Effects of government policies and extent of its implementations on the foundry industry in Nigeria. IOSR J Bus Manag. 2020;12(11):52-59.
59. James AT, Phd OKA, Ayobami AO, Adeagbo A. Raising employability bar and building entrepreneurial capacity in youth: a case study of national social investment programme in Nigeria. Covenant J Entrep. 2019.
60. Kirichenko A, Christen M, Grunow F, Herrmann D. Best practices and recommendations for cybersecurity service providers. In: ; 2020:299-316. doi:10.1007/978-3-030-29053-5_15.
61. Klíma T. Peta: methodology of information systems security penetration testing. Acta Inform Pragensia. 2016;5(2):98-117. doi:10.18267/j.aip.88.
62. Kolade O, Osabuohien E, Aremu A, Olanipekun KA, Osabohien R, Tunji-Olayeni P. Co-creation of entrepreneurship education: challenges and opportunities for university, industry and public sector collaboration in Nigeria. In: The Palgrave Handbook of African Entrepreneurship. 2021:239-265.
63. Lakhina A, Crovella M, Diot C. Mining anomalies using traffic feature distributions. ACM SIGCOMM Comput Commun Rev. 2005;35(4):217-228. doi:10.1145/1090191.1080118.
64. Lawal AA, Ajonbadi HA, Otokiti BO. Leadership and organisational performance in the Nigeria small and medium enterprises (SMEs). Am J Bus Econ Manag. 2014;2(5):121.
65. Lawal AA, Ajonbadi HA, Otokiti BO. Strategic importance of the Nigerian small and medium enterprises (SMES): Myth or reality. Am J Bus Econ Manag. 2014;2(4):94-104.
66. Li C. Penetration testing curriculum development in practice. J Inf Technol Educ Innov Pract. 2015;14:085-099. doi:10.28945/2189.
67. Lu H, Yu Y. Research on wifi penetration testing with kali linux. Complexity. 2021;2021(1):5570001. doi:10.1155/2021/5570001.
68. Mahanti A, Williamson C, Arlitt M, Mahanti A. Comparing wired-side and wireless-side wlan monitoring techniques: a case study. In: ; 2007. doi:10.1109/lcn.2007.42.
69. McKinnel DR, Dargahi T, Dehghantanha A, Choo KKR.

A systematic literature review and meta-analysis on artificial intelligence in penetration testing and vulnerability assessment. Comput Electr Eng. 2019;75:175-188. doi:10.1016/j.compeleceng.2019.02.022.
70. Northrop E, Lipford HR. Exploring the usability of open source network forensic tools. In: ; 2014:1-8. doi:10.1145/2663887.2663903.
71. Nwabekee US, Aniebonam EE, Elumilade OO, Ogunsola OY. Predictive Model for Enhancing Long-Term Customer Relationships and Profitability in Retail and Service-Based. 2021.
72. Nwabekee US, Aniebonam EE, Elumilade OO, Ogunsola OY. Integrating Digital Marketing Strategies with Financial Performance Metrics to Drive Profitability Across Competitive Market Sectors. 2021.
73. Odunaiya OG, Soyombo OT, Ogunsola OY. Economic incentives for EV adoption: A comparative study between the United States and Nigeria. J Adv Educ Sci. 2021;1(2):64–74. doi:10.54660/.JAES.2021.1.2.64-74.
74. Odunaiya OG, Soyombo OT, Ogunsola OY. Energy storage solutions for solar power: Technologies and challenges. Int J Multidiscip Res Growth Eval. 2021;2(1):882–890. doi:10.54660/.IJMRGE.2021.2.4.882-890.
75. Ogundare AF, Akinyemi AL, Aremu A. Impact of gamification and game-based learning on senior secondary school students' achievement in English language. J Educ Rev. 2021;13(1):110-123.
76. Olaiya SM, Akinyemi AL, Aremu A. Effect of a board game: Snakes and ladders on students' achievement in civic education. J Niger Assoc Educ Media Technol. 2017;21(2).
77. Olanipekun KA. Assessment of Factors Influencing the Development and Sustainability of Small Scale Foundry Enterprises in Nigeria: A Case Study of Lagos State. Asian J Soc Sci Manag Stud. 2020;7(4):288-294.
78. Olanipekun KA, Ayotola A. Introduction to marketing. GES 301, Centre for General Studies (CGS), University of Ibadan. 2019.
79. Olanipekun KA, Ilori MO, Ibitoye SA. Effect of Government Policies and Extent of Its Implementation on the Foundry Industry in Nigeria. 2020.
80. Olufemi-Phillips AQ, Ofodile OC, Toromade AS, Eyo-Udo NL, Adewale TT. Optimizing FMCG supply chain management with IoT and cloud computing integration. Int J Manag Entrep Res. 2020;6(11).
81. Otokiti BO. A study of management practices and organisational performance of selected MNCs in emerging market - A Case of Nigeria. Int J Bus Manag Invent. 2017;6(6):1-7.
82. Otokiti BO. Mode of Entry of Multinational Corporation and their Performance in the Nigeria Market [doctoral dissertation]. Covenant University; 2012.
83. Otokiti BO. Social media and business growth of women entrepreneurs in Ilorin metropolis. Int J Entrep Bus Manag. 2017;1(2):50–65.
84. Otokiti BO. Business regulation and control in Nigeria. In: Book of Readings in Honour of Professor S. O. Otokiti. Vol 1. 2018:201–215.
85. Otokiti BO, Akorede AF. Advancing sustainability through change and innovation: A co-evolutionary perspective. In: Innovation: Taking creativity to the market. Book of Readings in Honour of Professor S. O. Otokiti. Vol 1. 2018:161–167.
86. Otokiti BO, Onalaja AE. The role of strategic brand positioning in driving business growth and competitive advantage. Iconic Res Eng J. 2021;4(9):151–168.
87. Otokiti BO, Akinbola OA. Effects of Lease Options on the Organizational Growth of Small and Medium Enterprise (SME's) in Lagos State, Nigeria. Asian J Bus Manag Sci. 2013;3(4).
88. Otokiti-Ilori BO. Business Regulation and Control in Nigeria. In: Book of readings in honour of Professor S.O Otokiti. Vol 1. 2018.
89. Otokiti-Ilori BO, Akorede AF. Advancing Sustainability through Change and Innovation: A co-evolutionanary perspective. In: Innovation: taking Creativity to the Market, book of readings in honour of Professor S.O Otokiti. Vol 1. 2018:161-167.
90. Phong C, Yan W. An overview of penetration testing. Int J Digit Crime Forensics. 2014;6(4):50-74. doi:10.4018/ijdcf.2014100104.
91. Pokhrel N, Rodrigo H, Tsokos CP. Cybersecurity: time series predictive modeling of vulnerabilities of desktop operating system using linear and non-linear approach. J Inf Secur. 2017;08(04):362-382. doi:10.4236/jis.2017.84023.
92. Qureshi S, Gordhan D, Tunio S, Ullah F, Nazir A, Wajahat A. Performance analysis of open source solution "ntop" for active and passive packet analysis relating to application and transport layer. Int J Adv Comput Sci Appl. 2019;10(3). doi:10.14569/ijacsa.2019.0100304.
93. Salman F. Implementation of ipsec-vpn tunneling using gns3. Indones J Electr Eng Comput Sci. 2017;7(3):855. doi:10.11591/ijeecs.v7.i3.pp855-860.
94. Samtani S, Kantarcıoğlu M, Chen H. Trailblazing the artificial intelligence for cybersecurity discipline. ACM Trans Manag Inf Syst. 2020;11(4):1-19. doi:10.1145/3430360.
95. Saulino M, Ivanhoe CB, McGuire JR, Ridley B, Shilt JS, Boster AL. Best practices for intrathecal baclofen therapy: patient selection. Neuromodulation. 2016;19(6):607-615. doi:10.1111/ner.12447.
96. Seng L, Ithnin N, Shaid SZM. Automating penetration testing within ambiguous testing environment. Int J Innov Comput. 2018;8(3). doi:10.11113/ijic.v8n3.180.
97. Shah S, Mehtre BM. An overview of vulnerability assessment and penetration testing techniques. J Comput Virol Hacking Tech. 2014;11(1):27-49. doi:10.1007/s11416-014-0231-x.
98. Shivayogimath C. An overview of network penetration testing. Int J Res Eng Technol. 2014;03(07):408-413. doi:10.15623/ijret.2014.0307070.
99. Škiljić A. Cybersecurity and remote working: croatia's (non-)response to increased cyber threats. Int Cybersecur Law Rev. 2020;1(1-2):51-61. doi:10.1365/s43439-020-00014-3.
100. Tamrakar A, Patra B. Cybersecurity threats and countermeasures: a review. Turk J Comput Math Educ. 2018;9(3):1400-1404. doi:10.61841/turcomat.v9i3.14598.
101. Thottan M, Ji C. Anomaly detection in ip networks. IEEE Trans Signal Process. 2003;51(8):2191-2204. doi:10.1109/tsp.2003.814797.
102. Truvé S. Temporal analytics for predictive cyber threat intelligence. In: ; 2016:867-868.

doi:10.1145/2872518.2889294.
103. Umar R, Riadi I, Muthohirin B. Live forensics of tools on android devices for email forensics. Telkomnika. 2019;17(4):1803. doi:10.12928/telkomnika.v17i4.11748.
104. Umrao S, Kaur M, Gupta GK. Vulnerability assessment and penetration testing. Int J Comput Commun Technol. 2012;3(6-8):71-74.
105. Yaqoob I, Hussain SA, Mamoon S, Naseer N, Akram J, ur Rehman A. Penetration testing and vulnerability assessment. J Netw Commun Emerg Technol. 2017;7(8):10-18.