A Review and Comparative Analysis of Vulnerability Scanning Tools for Wireless LANs

Abheenesh Kejiou
University of Technology Mauritius,
La Tour Koenig, Mauritius
akejiou@umail.utm.ac.mu

Girish Bekaroo
Middlesex University Mauritius,
Flic en Flac, Mauritius
g.bekaroo@mdx.ac.mu

***Abstract*— The 21st century has been characterized by the widespread proliferation and use of wireless networks, notably, Wireless LANs, that enhanced access to information and resources to businesses and the society at large. However, WLANs are vulnerable to a range of security issues such as replay and KRACK attacks. In addition, the underlying security protocols used within WLANs, including Wired-Equivalent Privacy and the different versions of the Wi-Fi Protected Access have had security vulnerabilities that led to deprecation of few previous versions. As such, in the process of hardening security of such networks, vulnerability assessment is important and for this, various vulnerability scanners are available on the market. This paper critically reviews and analyses key vulnerability scanners for the context of WLANs. As part of the investigation, four tools, notably Nessus Vulnerability Scanner, OpenVAS, Nexpose and GFI LanGuard are reviewed, and insights are provided following practical utilization. As key findings, different vulnerability scanners were found to address different kinds and number of vulnerabilities, where some of them can be more granular than others, even in terms of output provided to the user. Moreover, the scan duration was not consistent across tools and does not corelate with the number of vulnerabilities detected.**

Keywords*— WLAN; Vulnerability Scanner; Vulnerability Assessment; Nessus Vulnerability Scanner; OpenVAS; Nexpose; GFI LanGuard.

I. Introduction

During the previous decades, there has been widespread proliferation of wireless LANs (WLANs) within businesses and the society at large. WLANs offer numerous benefits such as ease of installation and use as well as enhanced productivity due to increased accessibility to informational sources. Nonetheless, such wireless technologies also have associated vulnerabilities [1], where experts argue that these security issues are motivated by the widespread adoption and benefits of such networks in terms of costs reserves, efficiency gains, and expediency. Although common security issues like spyware, weak passwords, and missing patches have become less critical recently, other threats like unauthorized access, jamming, session hijacking and eavesdropping have gained more attention [1]. These vulnerabilities are also motivated by the wireless nature of such networks [2]. A recent survey also recommended that, enterprises must use solutions to actively identify all devices on the wireless network as the threat of wireless network attacks grows every day [3]. In addition to these security issues, underlying security protocols used within WLANs, including Wired-Equivalent Privacy (WEP) and the different versions of the Wi-Fi Protected Access (WPA, WPA2 and WPA3) have had various security vulnerabilities that made some of the protocols completely obsolete.

One of the recognised solutions to strengthen security of WLANs is via implementing hardening measures [6]. In order to effectively implement such measures, it is essential to understand underlying vulnerabilities within such networks through vulnerability assessment. Various tools are available on the market that could be utilized to scan for a range of vulnerabilities for the context of WLANs such as missing patches, open ports, services with vulnerabilities within devices connected on such networks. Furthermore, since Wireless Access Points (WAPs) utilize web-based portal, such tools can scan for vulnerabilities related to weak cipher suite and banner information, among others. In addition, certain tools also help to monitor the indicators of exposure and attack as part of a vulnerability management process to guarantee that potential vulnerabilities are not exploited thereby limiting damages. However, even though such tools are important to utilize to enhance security of WLANs, limited work has been undertaken to critically review and analyse their application within the context of WLANs. As such, this paper addresses this gap in literature to provide a review and analysis of key vulnerability scanners for the context of WLANs. The findings revealed in this paper is expected to be beneficial to enterprises, users of WLANs, as well as the research community as the study provides insights on vulnerability assessment tools that could be utilized for such networks, along with their key features and limitations.

This paper is structured as follows: In the next section, a background on the evolution of WLAN security is provided, whereby providing an overview of the key security protocols that marked the progress of such networks including WEP, WPA, WPA2 and WPA3. In section III, related works on the comparison of vulnerability assessment tools for WLANs are reviewed, before providing the methodology used to fulfil the purpose of this paper in Section IV. Sections V and VI focus on the core of the paper to review and critically compare existing vulnerability assessment tools meant for WLANs, before concluding the study in Section VII.

II. Background on the Evolution of WLAN Security

Security is a key requirement of WLANs since data is transmitted over the air and can be intercepted by anyone within the transmission range [4]. In order to secure communication of data transmitted within such networks, different protocols emerged over the years to protect confidentiality, integrity and availability of data of its wireless clients. However, various security vulnerabilities were reported over the years with security protocols of WLANs where some of them were even became obsolete. To start with, the Wired Equivalent Privacy (WEP) first emerged in 1999 and to encrypt data, the protocol utilized Ron's Code 4 (RC4) encryption algorithm using a secret key of 40 or 104 bits, with a 24-bit Initialisation Vector (IV) to generate per packet keys. However, due to vulnerabilities in its design including short IV length and FMS attack, WEP key was broken after sniffing and analysing wireless packets. It was even reported that using tools such as Aircrack-ng, the 104-bit WEP key could be broken within seconds [5]. As such, due to underlying design limitations, WEP was replaced by Wi-Fi Protected Access

(WPA) in 2003, which implemented the Temporal Key Integrity Protocol (TKIP) along with RC4. Nevertheless, WPA was only used as a temporary solution to bridge the gaps identified in WEP, until the more robust solution, notably WPA2, could be deployed. WPA2 utilizes the Advanced Encryption Standard (AES), which is considered as a more robust and scalable algorithm as compared to WPA [6]. Two modes are available for authentication within WPA and WPA2 and these are the personal mode and the enterprise mode. For personal mode, the out-of-band key sharing mechanism is used where a client needing to connect to a router simply need to enter the secret key commonly provided at the back of the router. On the other hand, the enterprise mode involves using an authentication server such as RADIUS, which manages credentials of clients in order to control access to the network. Security of WLANs were based on WPA2 for 14 years until it was broken using Key Reinstallation Attacks (KRACK) in 2017 for both home and enterprise modes [7], leading to the design and development of WPA3. In addition to KRACK, WLANs are vulnerable to a plethora of security issues such as MAC Sniffing, AP Spoofing, WPA2 flaws and Evil-Twin attacks, among others.

As such, the evolution of WLAN security protocols was marked by a range of security issues and one of the solutions to strengthen security is via implementing hardening measures [6]. Prior to implementing hardening, it is essential to understand underlying vulnerabilities within WLANs through vulnerability assessment. The overarching goal of vulnerability assessment is to identify segments of the corporate network where cyber attackers may exploit security flaws. The results of these tests are often delivered to the system owner with an evaluation of their risk to the networked environment and a remediation plan detailing the activities required to minimize the exposures, which are typically done using automated tools. Nevertheless, limited work has been done in published literature pertaining to WLAN vulnerability assessment, and these are reviewed in the next section.

III. Related Works

As related works, a previous study examined the efficacy of Vulnerability Assessment and Penetration Testing (VAPT) tools like Nessus, GFI LanGuard and Metasploit in order to provide proactive cyber protection by detecting vulnerabilities before an attacker attacks a system [4]. In addition, the study examined the most common vulnerability assessment approaches as well as several VAPT technologies. The study concluded that VAPT is an effective strategy for cyber defence technology and highlighted the need to increase the use of VAPT for complete system security. Another paper investigated cyber security vulnerabilities and mitigations while focusing on industrial radio technologies, including IEEE 802.15.4, IEEE 802.11.1, WirelessHART, Bluetooth, and ZigBee [5]. The study examined how industrial radio technology vulnerabilities may be utilized as vectors for cyberattacks on control systems in complex infrastructures. Vulnerabilities were divided into four categories, notably, reconnaissance, packet injection, denial of service, and man-in-the-middle. In addition, the article suggested various approaches for protecting wireless networks in control systems. Finally, the paper recommended that wireless networks that are vulnerable to denial of service, packet injection, or man-in-the-middle attacks, should not be employed within critical control systems. Moreover, another study presented an overview of penetration testing to identify computer system vulnerabilities [6]. The study investigated three important questions pertaining to the topic, where one of them relate to the most common tools utilized for penetration testing. As part of the investigation, port scanners, vulnerability scanner, application scanner and web application assessment proxy were reviewed, although limited critical analysis between these tools were conducted, in relation to wireless networks. Furthermore, another study conducted a review of network vulnerabilities scanning tools in terms of their types, capabilities and functioning [7]. The tools reviewed as part of the study are Shodan, Censys, ZoomEye, PunkSPIDER, Thingful, IVRE, Vulners, Nessus, Skipfish, Acunetix and Vega. In addition to the review, the study also provided the advantages and disadvantages of each tool as well as the similarities and differences between the tools.

As such, existing literature investigated a wide range of vulnerability scanning tools, which are also accessible for businesses and the general public to use. Among the tools, Nessus and OpenVAS are often considered to be among the most popular tools [8]. Nevertheless, even though these tools provide important advantages to networks and their users, limited work has been undertaken to assess their use for the context of wireless networks. As such, the present study is important to undertake.

IV. Methodology

In order to fulfil the purpose of this paper and to identify vulnerability assessment tools for the context of WLANs, a search was performed on Google using the key terms “vulnerability”, “assessment”, “WLAN”, “network”, “wireless”, “tool”, “scanner”. After an initial search via the search engine, complemented with the vulnerability scanners referred in existing literature reviewed in this paper, an initial pool of 21 tools were identified. These tools were eventually filtered based on the following criteria: popularity, features, and compatibility with the available hardware specifications, in order to select four key tools to be reviewed as basis of this paper. These tools are OpenVAS, Nessus Vulnerability Scanner, Nexpose and GFI LanGuard. For reviewing each tool, information from online resources pertaining to each tool was referred. Moreover, to complement the reviews, the selected tools were acquired and installed on a laptop running Kali Linux, also connected to a Wireless Access Point. After the installation was complete, each tool was used to scan the wireless network for vulnerabilities, including the Wireless Access Point and another device connected to the same network. Insights following practical installation and use was also complemented to findings, similar to the approach used in a previous related study [14]. Results following utilization of the tools helped to determine the mean time for scanning for vulnerabilities by the tools, the severity of vulnerabilities detected, time taken for key activities as well as detection of WLAN-specific vulnerabilities.

V. Review of Vulnerability Assessment Tools for WLANs

Using the methodology described in the previous section, four key vulnerability assessment tools for the context of WLANs were reviewed and critically compared as follows:

A. *OpenVAS*

The Open Vulnerability Assessment System (Open VAS) has been developed and is managed by the company Greenbone Networks. It is not just a tool but a whole framework comprising of various services and technologies, giving a comprehensive and robust vulnerability detection and vulnerability management solution [4]. OpenVAS is clearly a resource-intensive technology as it may use much memory and CPU during the scanning process. OpenVAS features a ready-to-use Common Vulnerability Scoring System (CVSS) calculator that can compute vulnerability scores, as shown in Fig. 1. The vulnerability scanner can discover SSL/TLS Weak Cipher Suite vulnerabilities on the router's wireless portal. In addition, the scanner can detect protocols such as Telnet and/or SSH that are enabled on the wireless network. This allows an attacker to discover router login information that is completed via Telnet. Consequently, attackers might exploit the exposed login information to gain access to the router and change its settings.

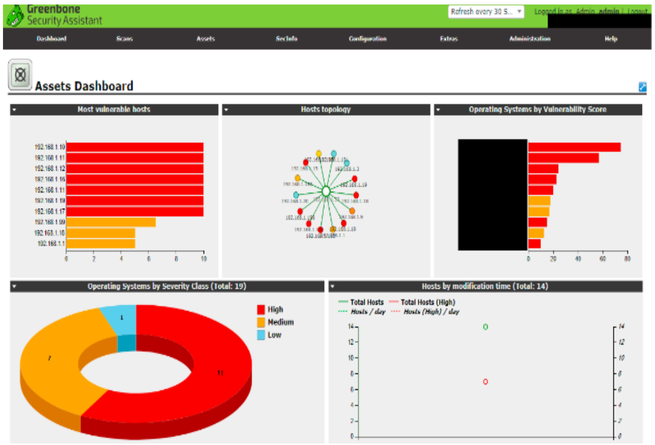
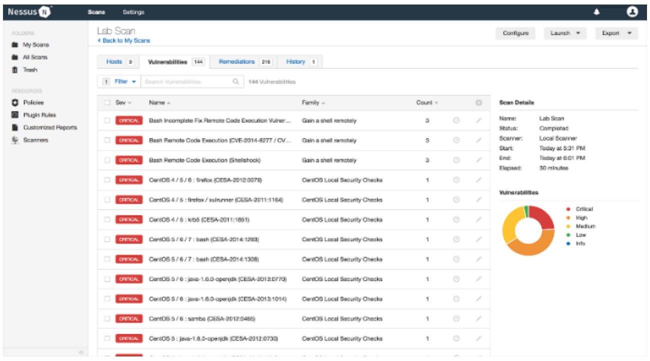


Fig. 1. OpenVAS

B. *Nessus Vulnerability Scanner*

The Nessus Vulnerability Scanner, as illustrated in Fig. 2, includes one of the most comprehensive knowledge bases of security vulnerabilities, as well as hundreds of plugins that may be triggered for deep and/or customized scans [5]. This scanner may discover security flaws in the targeted host's operating system, installed patches, and installed services, as well as recommend remedies to mitigate these security vulnerabilities. This scanner may also scan the targeted host since it has been granted local access to that host [5]. Also, the scanner can discover vulnerabilities associated to a Wireless Access Point (WAP) such as detecting the underlying OS utilizing Nessus OS Fingerprinting either via FTP, HTML, HTTP, mDNS, MDRPC, NTP, SMB, SNMP and ICMP banner to identify the remote OS. Also, because practically every WAP product offers some type of web-based settings panel, the device can be recognized by scanning for distinctive banner information.



Sev	Name	Family	Count
CRITICAL	Bash Incomplete Fix Remote Code Execution Vulner...	Gain a shell remotely	3
CRITICAL	Bash Remote Code Execution (CVE-2014-6277 / CV...	Gain a shell remotely	3
CRITICAL	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	3
CRITICAL	CentOS 4 / 5 / 6 : firefox (CESA-2012:0079)	CentOS Local Security Checks	1
CRITICAL	CentOS 4 / 5 : firefox / xulrunner (CESA-2011:1164)	CentOS Local Security Checks	1
CRITICAL	CentOS 4 / 5 : krb5 (CESA-2011:1851)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1293)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 / 7 : bash (CESA-2014:1306)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:0770)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : java-1.6.0-openjdk (CESA-2013:1014)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 / 6 : samba (CESA-2012:0465)	CentOS Local Security Checks	1
CRITICAL	CentOS 5 : java-1.6.0-openjdk (CESA-2012:0730)	CentOS Local Security Checks	1

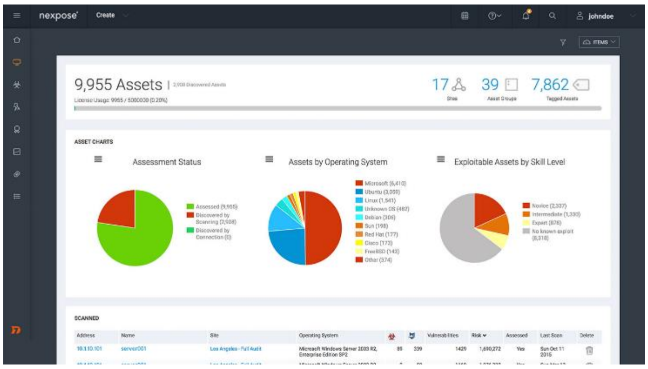
Scan Details

Name: Lab Scan
Status: Completed
Scanner: Local Scanner
Start: Today at 5:31 PM
End: Today at 6:01 PM
Elapsed: 30 minutes

Fig. 2. Nessus Vulnerability Scanner

C. *Nexpose*

Nexpose detects active services, open ports, and running applications on each device and tries to detect vulnerabilities based on the properties of the known services and applications [6]. Nexpose reports the findings in a scan report, which assists in prioritizing vulnerabilities based on risk factor and determining the most effective remedy to apply. Nexpose interfaces with Metasploit Pro to offer a vulnerability assessment and validation tool that aids in the elimination of false positives, the verification of vulnerabilities, and the testing of remedial steps. The vulnerability scanner may find SSL/TLS Weak Cipher Suite vulnerabilities on the router's wireless portal. It may also discover a vulnerability associated with a certain version of a wireless controller family which can enable an unauthenticated and remote attacker to trigger a denial of service (DoS) issue on an affected device. A screenshot of the tool is shown in Fig. 3.



Address	Name	Site	Operating System			Vulnerabilities	Risk	Assessed	Last Scan	Delete
10.1.10.101	server001	Los Angeles - Full Audit	Microsoft Windows Server 2003 R2, Enterprise Edition SP2	85	339	1429	1,690,272	Yes	Sun Oct 11 2016	

Fig. 3. Nexpose

D. *GFI LanGuard*

In addition to providing a comprehensive picture of network security, GFI LanGuard (shown in Fig. 4) offers a log of the vulnerability assessment and software auditing activities. Inexperienced users often turn to this application since it has the most user-friendly Graphical User interface [7]. GFI LanGuard discovers and scans all wirelessly connected devices. It can detect vulnerabilities in some specific wireless routers that are prone to denial of service, resulting in a device reboot, as well as an unknown vulnerability in a wireless router with a specific firmware and WPA Personal/TKIP authentication enabled, which allows remote clients to bypass authentication by connecting without encryption.

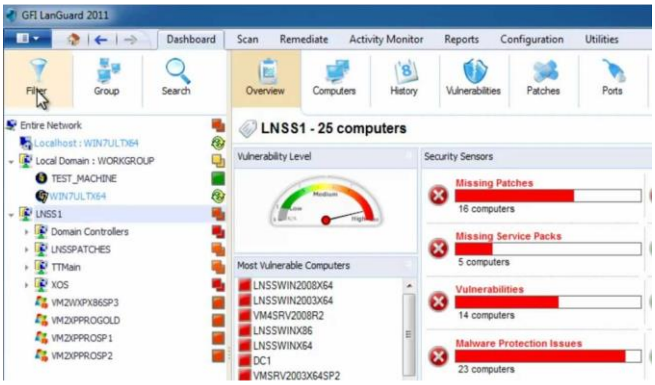


Fig. 4. GFI LanGuard

TABLE I. Comparative Analysis of Vulnerability Assessment Tools for WLANs

	Nessus (version 10.0.2)	***OpenVAS (version 7.0.3)***	***Nexpose (version 6.6.120)***	***GFI LanGuard (version 12.5)***
CVE Coverage	67K CVEs	<26K CVEs	<42K CVEs	60K
Operating System	Windows, Linux distributions, and other operating systems are supported by the OS platform.	Supports only Linux. Users must deploy their own OpenVAS binaries from source code.	Windows and Linux distribution are supported	Windows, Linux distribution and MacOS are supported
Ease of installation	Easy to install for the average user.	Complex procedure to install for the average user	Easy to install for the novice user	Easy to install for the average user.
Compliance & Configuration Templates	700+ templates for compliance and configuration (DISA STIG, HIPAA, CIS, HIPAA, USGCB, FDCC).	There are just a few configuration templates offered.	There is a limited number of setup templates supplied. For an extra fee, CIS, USGCB, FDCC, and customized policies are available.	PCI DSS, HIPAA, SOX, GLB/GLBA or PSN CoCo compliance programs.
Pre-built vulnerabilities templates	Templates for important vulnerabilities such as WannaCry, Spectre, and Meltdown.	No pre-built templates for Meltdown, Spectre & WannaCry.	There are no pre-built templates for WannaCry, Spectre, and Meltdown, for example.	There are no pre-built templates for WannaCry, Spectre, and Meltdown, for example.
Cost	Subscription to Nessus Professional: $3,000/year for unlimited IPs.	Free to download.	Nexpose subscription: a 500-IP license costs more than $10,000 per year and rises substantially as the number of IPs increases.	Pricing starts at $26 per year, and varies depending on the features selected.
Reporting	Report export formats are available in XML, HTML, PDF, CSV, Nessus DB	Report export formats are available in XML, HTML, PDF and text	Report export formats are available in HTML, CSV, PDF, XML, and RTF/text	Report export format are available in PDF, HTML, XLS, XLSX, RTF and CSV.
WLAN Vulnerability Scanning	Nessus has the ability of detecting a host acting as a Wireless Access Point & find related vulnerabilities.	OpenVAS can scan a Wireless Access Point and find related vulnerabilities.	Nexpose can find vulnerabilities on the Wireless Access Point's portal. It can also discover vulnerabilities related to DOS and unauthenticated attacks.	GFI LanGuard can find more than WLAN related vulnerabilities, it can also proactively disable Wireless Access Point.
Rogue Access Point Detection	It is possible through the use of a plugin	No plugin or option to detect a rogue access point	No plugin or option to detect a rogue access point	Can only locate Wireless Access Points.

VI. Comparative Analysis

Using the information acquired from online materials and following utilization of the four tools, a comparative analysis of these tools was conducted, as discussed in the methodology section. As part of the comparative analysis, as depicted in Table I, different criteria were considered. Firstly, for comparing such tools, understanding the Common Vulnerabilities and Exposures (CVE) addressed by the tools is essential to study. In addition to the CVE, the comparative analysis provides details on the operating system used by the tool, ease of installation, compliance and configuration templates, pre-built vulnerabilities templates, costs involved, report formats generated, WLAN vulnerability scanning and rogue access point detection.

As depicted in Table I, different vulnerability scanner addresses different kinds and number of vulnerabilities, where some of them can be more granular than others. Amongst, Nessus Vulnerability Scanner and GFI LanGuard were found to address and maintain a relatively high CVE as compared to the remaining tools. Moreover, all the tools reviewed, besides OpenVAS are compatible with both Windows and Linux operating systems, thus providing useful support towards vulnerability scanning in these popular environments. As for compliance and configuration templates, it was found that Nessus, Nexpose and GFI LanGuard provide various templates that facilitate the scanning process and creation of policies. These tools also cost in terms of license fees to be paid on an annual basis, and can also charge for other features such as training costs and advanced support provided to users. On the other hand, OpenVAS is free to download, although limited support is provided in terms of compliance, configuration and pre-built vulnerability templates, which are required to be created by users upon use. Following the scanning process, all the tools provide reports in common formats such as XML, HTML and PDF, among others. All the tools also had varying capabilities for WLAN vulnerability scanning ranging from access point detection to scanning for issues within associated portal and even disabling access points. Finally, among the tools, only Nessus showed to have the ability to detect fake or rogue access points.

A. *Vulnerability Scanning and Reporting*

In addition to the comparative review, a test lab consisting of a laptop running Windows 10 Home edition (21H2) connected to wireless access point was deployed to benchmark the scanning time of the vulnerability scanning tools. In order to measure the scanning time, a normal vulnerability scan was launched from the different tools and the ‘time elapsed’ for completing the task was recorded. The process was repeated three times to get the mean value. Results of scan is depicted in Table II, where it was found that scanning of the host completed by Nessus was faster than the remaining tools. Nessus was almost 3 times faster than OpenVAS in terms of scanning speed, thus providing the results faster.

TABLE II. MEAN TIME FOR SCANNING

Vulnerability Scanner	Mean Time (hh:mm:ss)
OpenVAS	00:09:50
Nessus	00:03:58
Nexpose	00:05:21
GFI LanGuard	00:10:20

In addition, Fig. 5 depicts a comparison of vulnerability detection with severity levels (info, low, medium, and high) for the vulnerability scanners under study. Nessus Vulnerability Scanner found more vulnerabilities as compared to the other tools and the findings could be attributed to the number of CVEs addressed and maintained, as highlighted from Table I. As for the other tools, OpenVAS detected only 1 high rating vulnerability and Nexpose detected only 4 high rating & 2 medium rating vulnerability while Nessus discovered only 2 high, 4 medium and 3 low vulnerabilities and 50 information about allowed services and ports, as illustrated in Chart 1. While Nexpose did discover more high vulnerabilities than Nessus, instead of grouping all SMB related vulnerabilities under single title, it listed them under various titles while Nessus listed it under a single title and described in more details once the user opened the vulnerability listing. OpenVAS did not identify any SMB related vulnerabilities compared to Nessus and Nexpose.

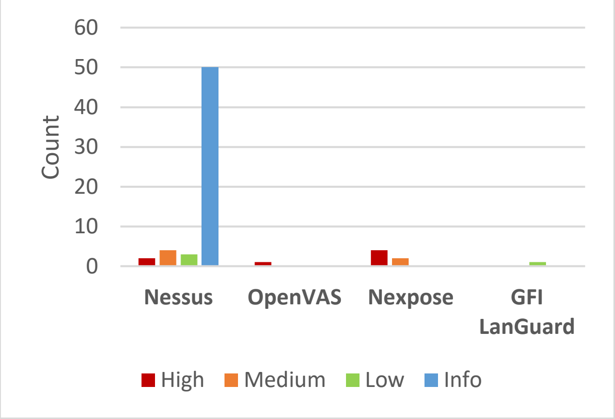


Fig. 5. Vulnerability Detection

Furthermore, Fig. 6 depicts a graphical representation of the vulnerability scanning time as well as the time taken for each vulnerability scanner to generate report in an appropriate format. Both details were obtained within the vulnerability scanners, that contain features to measure time taken for different activities. From the findings, a co-relation between number of vulnerabilities detected and report generation time was found as expected, as the process involved writing the vulnerabilities identified into the format chosen by the end user. However, the scan duration was not consistent across tools and indicates no corelation with the number of vulnerabilities detected.

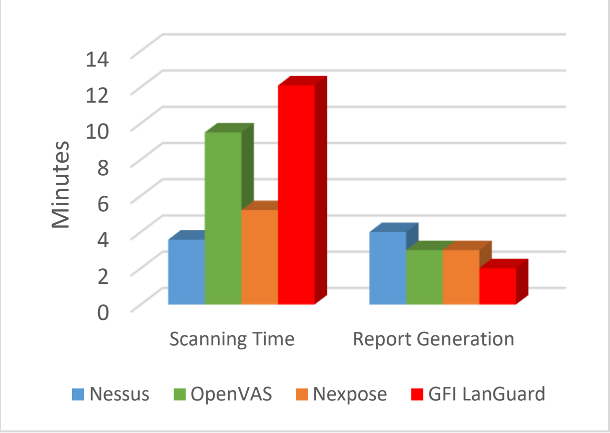


Fig. 6. Time taken for key activities

B. Detecting WLAN-related Vulnerabilities

Fig. 7 demonstrates the number of each WLAN vulnerabilities discovered by the tools under study, classified into vulnerabilities pertaining to missing updates, weak encryption as well as authentication and authorisation. Missing updates comprises of vulnerabilities that may be remedied by deploying a vendor security patch on the firmware of the Wireless Access Point, most of these were discovered by Nessus & Nexpose compared to other tools. Weak encryption vulnerabilities revealed were largely related to the encryption protocol of the Wireless Access Point, most encryption vulnerabilities identified were prior to SSL version 2. Authentication & Authorization vulnerabilities discovered were mostly connected to privilege escalation which permitted an unprivileged user to access and alter administrative settings of the Wireless Access Point. From the results, it could be noticed that only Nessus Vulnerability Scanner was able to detect vulnerabilities related to all three categories. On the other hand, OpenVAS only detected one vulnerability related to missing updates, although the tool can discover vulnerabilities pertaining to the other categories. As such, it could be deduced that although the tools studied have the ability to detect WLAN-related vulnerabilities, scan results had variances in all the three WLAN vulnerability categories.

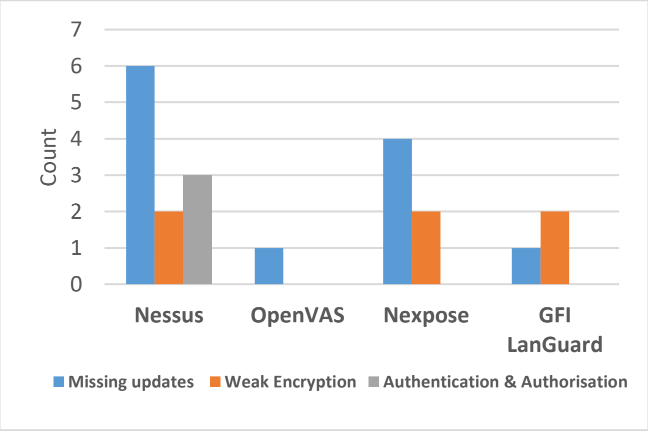


Fig. 7. WLAN Vulnerability Classification

C. Limitations of the Study

Even though the comparative analysis revealed some insightful findings regarding existing vulnerability scanners in relation to their application for identifying vulnerabilities within WLANs, different limitations however exist. Firstly, the lab under test only involved few devices running minimal applications and findings could be different within a medium or larger network involving a range of extenders and different types of computational devices including computers, smart phones and servers, among others. Moreover, the study only investigates four vulnerability scanners, which could be extended to study a more tools, including some that only focus on Wi-Fi vulnerability assessment to eventually compare against findings revealed in this study. Finally, the findings revealed are specific to the versions of the tools utilized.

VII. Conclusions

This paper reviewed and analysed four vulnerability scanners for the context of WLANs, notably, Nessus Vulnerability Scanner, OpenVAS, Nexpose and GFI LanGuard. The comparative analysis performed in this study revealed that the vulnerability scanner studied addresses different kinds and number of vulnerabilities, where the granularity of information provided, and the number of vulnerabilities scanned vary. Among the tools studied, Nessus Vulnerability Scanner was found to identify a larger number of vulnerabilities, within a shorter duration of time as compared to the other scanners. To conclude, although WLANs are more than ever popular within businesses and the society and that their security is a key requirement, scan results provided by vulnerability tools studied are somehow limited, where it was found that some of the tools do not have the ability to detect common vulnerabilities such as fake access points or underlying vulnerabilities due to use of older version of protocols.

As future work, the limitations identified in this study could be addressed to extend the study in order to include more tools to be compared, while also extending assessment within medium and larger WLANs consisting of extenders and various computing devices. Also, existing vulnerability scanners could be investigated to assess their adherence to Wi-Fi vulnerability assessment checklists [19].

References

[1] G. Bekaroo, A. Santokhee and J. Augusto, “5G Smart and Innovative Healthcare Services: Opportunities, Challenges, and Prospective Solutions,” in 5G Multimedia Communication: Technology, Multiservices, and Deployment, CRC Press, 2020, pp. 279-297.

[2] Z. Akram, M. Saeed and M. Daud, “Real time exploitation of security mechanisms of residential WLAN access points,” in 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), 2018.

[3] I. Hossain, M. Hasan, S. Hasan and M. Karim, “A study of security awareness in Dhaka city using a portable WiFi pentesting device,” in 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET), 2019.

[4] Outpost24, “The Internet of Evil Things,” Outpost24, 2020. [Online]. Available: https://outpost24.com/resources/whitepapers/internet-of-evil-things-2020-guide. [Accessed 5 Jan 2022].

[5] J. Castillo-Velazquez, M. Garcia and D. Martinez, “Hardening as a best practice for WLAN Security Meanwhile WPA3 is released,” in 2019 IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX) , 2019.

[6] E. Baray and N. Ojha, “WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique,” in 5th International Conference on Computing Methodologies and Communication (ICCMC), 2021 .

[7] E. Tews, R. Weinmann and A. Pyshkin, “Breaking 104 bit WEP in less than 60 seconds,” in International Workshop on Information Security Applications, Berlin, Heidelberg, 2007.

[8] M. Vanhoef and F. Piessens, “Key reinstallation attacks: Forcing nonce reuse in WPA2,” in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017.

[9] J. Goel and B. Mehtre, “Vulnerability assessment & penetration testing as a cyber defence technology,” Procedia Computer Science, vol. 57, pp. 710-715, 2015.

[10] B. Reaves and T. Morris, “Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems,” International Journal of Critical Infrastructure Protection, vol. 5, no. 3-4, pp. 154-174, 2012.

[11] M. Fiocca, “Literature Study of Penetration Testing,” Linköpings universitet, Sweden, 2009.

[12] A. Tundis, W. Mazurczyk and M. Mühlhäuser, “A review of network vulnerabilities scanning tools: types, capabilities and functioning,” in Proceedings of the 13th international conference on availability, reliability and security, 2018.

[13] F. Fikriyadi, R. Ritzkal and B. Prakosa, “Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method,” Jurnal Mantik, vol. 4, no. 3, pp. 1658-1662, 2020.

[14] S. Pattanavichai, “Comparison for network security scanner tools between GFI LanGuard and Microsoft Baseline Security Analyzer (MBSA),” in 2017 15th International Conference on ICT and Knowledge Engineering (ICT&KE), 2017.

[15] S. Rahalkar, “OpenVAS,” in Quick Start Guide to Penetration Testing, Berkeley, CA, Apress, 2019, pp. 47-71.

[16] A. Donevski, S. Ristov and M. Gusev, “Nessus or Metasploit: Security Assessment of OpenStack Cloud,” in The 10th Conference for Informatics and Information Technology (CIIT 2013), 2013.

[17] Rapid7, “Vulnerability scanning with Nexpose,” Rapid7, 2022.

[18] GFI Software, “LanGuard,” GFI Software, 2022. [Online]. Available: https://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard. [Accessed 10 Jan 2022].

[19] L. Phifer, “Wi-Fi vulnerability assessment checklist,” TechTarget, 2022. [Online]. Available: https://www.techtarget.com/searchnetworking/feature/Wi-Fi-vulnerability-assessment-checklist. [Accessed 30 Apr 2022].