International Journal of Advanced Research in Engineering and Applied Sciences
ISSN: 2278-6252
ImpactFactor-8.094

THE SIGNIFICANCE OF VULNERABILITY ASSESSMENT IN ENHANCING WLAN SECURITY

Mahmudul Hasan[1], Mohammad Arifin Rahman Khan[2], Mohammed Ibrahim Hussain[3], Md. Moazzam Hossain[4], Mujahid Ahmed[5], Ariful Islam Naeem[6], Hasan Miah[7], Sabbir Hasan[8]

Project student, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh[1]

Assistant Professor, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh[2]

Assistant Professor, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh[3]

Executive Data Analyst and SEO Specialist, Creatif, Dhaka, Bangladesh [4]

Project student, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh[5]

Project student, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh[6]

Project student, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh[7]

Project student, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh[8]

Corresponding Author: Mohammad Arifin Rahman Khan, E-mail: arifin.khan@bu.edu.bd

ABSTRACT: *In today's computerized environment, Wireless Local Area Networks (WLANs) have become an indispensable component of modern network connectivity across enterprise, residential, public, and IoT-integrated environments. However, their broadcast nature makes them prime targets for cyberattacks, including eavesdropping, unauthorized access, and denial-of-service (DoS) attacks. This study addresses the critical significance of WLAN vulnerability assessment in strengthening network security. This paper further highlights the significance of systematic WLAN vulnerability evaluation to combat against attacks, including man-in-the-middle (MITM), de-authentication, and cryptographic downgrade exploits. Using a qualitative methodological technique, we do reconnaissance, vulnerability scanning, and systematic vulnerability assessment using tools such as Kismet,*

Nessus, OpenVAS, Nmap, Aircrack-ng, and Wireshark. We focus on the integration of AI/ML for predictive analysis and an ethical framework for vulnerability assessment. Findings of this investigation reveal regular vulnerabilities, weak key interaction and configuration errors, and realistic exploits exposing issues in insecure WLANs. This study underscores the importance of proactive security measures and encourages AI-driven, real-time assessment solutions to boost WLAN security against emerging threats. The findings illustrate that frequent vulnerability evaluations not only reveal critical gaps but also enable the proactive reinforcement of WLAN infrastructures against evolving threats. The publication provides a complete guide for network managers, security professionals, and researchers trying to secure wireless networks in an increasingly hostile cyber environment.

Keywords: *WLAN security, vulnerability assessment, Network security, IoT vulnerability, Cyber security.*

1. INTRODUCTION

Wireless Local Area Networks (WLANs) have become an essential aspect of modern communication infrastructure. WLAN is a decentralized communication system that enables user devices to connect and send data wirelessly within a limited geographical region, such as homes, workplaces, organizations, or campuses. Initially, WLAN was designed to offer a flexible networking experience without physical cabling. Nowadays, WLANs serve as the backbone for several applications, including enterprise operations and healthcare systems, smart cities, and IoT ecosystems. Their ability to provide flexible, scalable, and cost-effective connectivity has driven widespread adoption, with global market penetration in urban environments and still continuing to penetrate into emerging economies. WLANs utilize radio frequency signals (i.e. 2.4 GHz, 5 GHz, or 6 GHz bands) and comply with IEEE 802.11 standards (e.g., Wi-Fi 6) and replace aged wired infrastructure with access points and wireless adapters. WLANs serve various devices, from smartphones to IoT systems, ensuring trustworthy high-speed communication in dynamic environments while eliminating physical cabling needs [1][2].

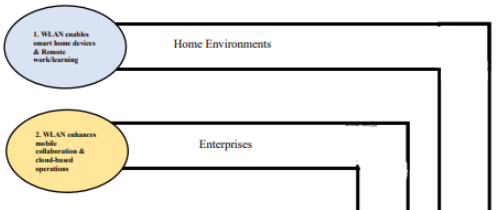

Figure 1 : Significance of WLAN in modern ecosystem.

In modern networking technology, individual consumers and organizations are seeking mobility, scalability, flexibility, cost-effectiveness, easy installation and maintenance, enhanced communication and collaboration, and integration with emerging technologies. WLAN enables flexible and affordable networks by providing seamless connectivity for smart devices such as smart televisions, streaming services, smartphones, and IoT (Internet of Things) devices. It facilitates remote work and study and removes cabling complexity in homes and apartments. WLAN enhances business productivity by decreasing infrastructure expenses and delivering cloud-based operations, real-time data monitoring across numerous departments, and mobile collaboration. WLAN offers scalable solutions to the organizations that can improve reliable and flexible connectivity, scalability and coverage, and application support. The primary objective and notable benefit over wired networks are that users can roam about while keeping network connectivity. Wireless LAN promotes operational efficiency in organizations such as healthcare, manufacturing (such as automobiles), and education by enabling telemedicine, smart manufacturing environments, real-time data monitoring, real-time data analysis, e-learning platforms, and centralized resource management [3]. WLAN technology reduces extensive cabling and occupies less physical space while providing reliable and secure connectivity. Public hotspots give services to users in hospitality or retail industries. Despite issues like security threats, WLAN's flexibility, portability, and support for upcoming technologies (5G integration, edge computing) make it important for current digital ecosystems, leading to innovation across personal, professional, and institutional domains. Market data reflects their exponential growth. According to IDC (2023), over 1.6 billion WLAN devices were shipped globally in 2022, with enterprise

WLAN infrastructure investments growing by more than 20% year-over-year [4]. According to Cisco's Annual Internet Report, the number of public Wi-Fi hotspots is expected to surpass 628 million globally by 2023, reflecting the increasing demand for wireless accessibility [5]. As per Market Research Future, the WLAN market is expected to grow from $29.75 billion to $50.1 billion by 2032. It also forecasts that the compound annual growth rate (CAGR) of the WLAN market will be 5.96% from 2024 to 2032 [6]. Markets and Markets states that the Wi-Fi market will grow which is start from $22.06 billion in 2024 to $45.12 billion by 2029. The CAGR of the WiFi market will be 15.4% [7]. According to the report published in Rots Analysis, it predicted that the CAGR of the wifi market will be 17.08%. The Wi-Fi market value will grow from $17.08 billion in 2024 to $120.25 billion by 2035 [8]. A report from Open PR shows that the industrial WLAN market value was valued at $1.60 billion in 2023. It also predicted that the CAGR will be 10.5% and the market value will be $3.22 billion by 2030 [9]. As an impact of wireless LAN technology's exponential growth, more campuses, businesses, and organizations prefer to deploy wireless networks in order to enhance workplace scalability, flexibility, and connectivity. Nowadays, Wireless Local Area Networks (WLANs) have become essential for contemporary connection but offer significant cybersecurity threats owing to their corresponding vulnerabilities. Weak encryption techniques, such as old WPS, WPA/WPA2, or vulnerable open networks, expose data to eavesdropping, man-in-the-middle (MitM) attacks, protocol exploitation, rogue access points, outdated firmware, and misconfigured routers and access points further escalate challenges, providing unauthorized access to sensitive systems [10]. Attackers commonly exploit default credentials or weak passwords to penetrate networks for data breaches or malware propagation purposes by using a brute force technique. Additionally, signal interception in public WLANs compromises user privacy. Compromising a WLAN can result in substantial consequences, including data breaches, system downtime, reputational damage, and financial losses. One of the critical consequences of WLAN security breaches is financial loss. Data breaches, service interruptions, and reputational damage can result in substantial economic costs for affected organizations (Ponemon Institute, 2023) [11]. A 2022 IBM security report estimated the average cost of a data breach in environments with compromised wireless infrastructure to be around $4.35 million [12]. For instance, a single breach in a corporate WLAN could result in operational downtime, regulatory penalties, and reputational damage, with estimated annual losses for security-focused enterprises exceeding $10.5 trillion globally by the year 2025. (Cybercrime Magazine, 2022) [13]. In these situations, WLAN security

testing is a crying need to protect valuable information and prevent unauthorized access to wireless LAN. Vulnerability assessment techniques are used to detect potential security vulnerabilities in target network architecture. It helps to identify vulnerabilities and weaknesses in the network architecture and implement appropriate security measures. Proper cyber security measures can fight against potential cyber-attacks and data breaches such as credit card credentials, personal information, user IDs and passwords, network integrity, and intellectual property. To discover potential vulnerabilities, it is important to frequently conduct WLAN vulnerability assessments and security audits [14].

Our research is intended to investigate the current security posture of WLANs, detect potential vulnerabilities, and provide feasible mitigation techniques for strengthening their ability to survive. Therefore, according to ours this study, we like to present our aim in below:

1. Perform comprehensive assessments of existing methodologies for WLAN vulnerability analysis.
2. Assess the strengths, limitations, and feasibility of current approaches.
3. Detect and classify WLAN-specific threats and develop a threat framework based on attack vectors, exploitability, and potential impact.
4. Monitor evaluation of current WLAN security protocols and identification of its risks.
5. Modern approaches for improvements in vulnerability assessment and development of proactive defense mechanisms and actionable recommendations for enhancing WLAN resilience against cyber threats.
6. These goals will help our research to contribute to a more comprehensive understanding of WLAN security and offer practical recommendations for increasing defenses in wireless environments.

Ultimately, the significance of this research lies in its ability to contribute to the construction of more secure and robust wireless networks. By addressing existing weaknesses and emphasizing opportunities for improvement, our study intends to support ongoing efforts in boosting the security posture of modern communication networks.

2. LITERATURE SURVEY

Research conducted by Nasr et al. in [15] deals with significant deficiencies in Wi-Fi security knowledge in Lebanon, identifying risks in household and commercial networks. As worldwide reliance on Wi-Fi expands, the study's focus on regional risk assessment

contributes to localized cybersecurity discourse, underlining the need for public education and governmental initiatives. The authors utilize a mixed-method approach, combining wardriving (with tools like Kismet and Acrylic Wi-Fi Professional) and surveys to evaluate Wi-Fi security protocols and public awareness. Key findings suggest 11.1% of networks still utilize weak WEP encryption, while survey data indicates widespread ignorance of basic security procedures (e.g., 54.3% are ignorant of linked devices). The research underlines urgent demands for regional security initiatives and upgraded technologies like WPA3.

In 2020, Alueendo et al. performed comprehensive research based on Wi-Fi security vulnerabilities in educational institutions. It emphasizes the risks posed by high device density and inadequate user awareness. As BYOD (Bring Your Own Device) policies proliferate, the study highlights the urgent need for robust security frameworks to mitigate threats like eavesdropping and MITM attacks, contributing to the discourse on institutional cybersecurity. The researchers utilize a systematic methodology to identify Wi-Fi threats (e.g., eavesdropping, DoS) and evaluate countermeasures like network segmentation and VPNs. From the study in [16], the paper points out the requirement for proactive vulnerability assessments and necessary remedies. The paper also declares that they will conduct penetration testing and examine socio-technical techniques that fill the gap between user behavior and institutional security standards.

Linko G. Nikolov published a research work on wireless network vulnerabilities in the year of 2018. His investigation focuses on WPA2 and WPS protocols. The investigation helps to identify WLAN vulnerabilities utilizing the Kali Linux operating system and tools such as Air cracking and Bully. His in-depth analysis also highlights the threats of brute-force and dictionary attacks. His research which has studied in [17] and it was performed in a controlled lab setup to test WPA2-Personal and WPS vulnerabilities, revealing that simple passwords (i.e., "mypassword") are compromised quickly, whereas complex sequences avoid attacks. The paper lacks emphasis on mitigation beyond password difficulty, such as AI-driven intrusion detection. The report validates the need for implementing WPA3 and removing WPS.

Kashim Kyari Mohammed in the year 2021 published a research article named WLAN Vulnerability Scanning Methodologies, which gives emphasis to the growth of wireless networks and associated security threats with them. The paper demonstrates a thorough analysis of active probing and passive scanning techniques. OpenVAS, Nessus, Zmap, and Nmap are used to perform WLAN vulnerability assessments. The study in [18], reviews

WLAN security protocols (WEP, WPA, and WPA2) and associated potential vulnerabilities, such as snooping, packet modification, masquerading, and denial-of-service attacks. The author also highlights the efficacy of active probing for real-time vulnerability detection, while passive scanning is praised for stealth but critiqued for delayed results. The researcher also reflects on the comparison between Nessus and OpenVAS.

Several significant findings about Wi-Fi security in North Cyprus using the wardriving technique were revealed by Etta et al. in 2022. The investigation also highlighted the increasing reliance on Wireless Local Area Networks (WLANs) and associated vulnerabilities. The study examined common WLAN vulnerabilities and threats for example active and passive wireless attacks. They also emphasized the significance of user awareness and encryption mechanisms in protecting against WLAN vulnerabilities. According to the study in [19], the researchers adopt a two-stage approach to perform comprehensive research that reveals that 42.82% of identified networks employ WPA2 encryption, while 25.1% remain unprotected, and 48% of access points (APs) enable WPS.

From the published a research work [20] point of view, it has seen that a significant security vulnerability addresses for wireless LANs and proposed mitigation strategies. Their investigation highlighted the limitations of single-factor authentication (SFA) and discussed the importance of multi-factor authentication (MFA). Their research also showed the proper methodology of WLAN two-factor authentication implementation via Google Authenticator and RADIUS server and implemented a time-based one-time password (OTP) for wireless LAN security. These techniques help to mitigate threats for example unauthorized access and man-in-the-middle (MitM) attacks in the perspective of growing demands for robust WLAN security in IoT and mobile computing environments.

Research in [21] is conducted on the security vulnerabilities in wireless LANs and proposes countermeasures by emphasizing the trade-offs between mobility and security. The research article highlights the evolution of WLAN standards (e.g., 802.11, WEP, WPA/WPA2) and their potential weaknesses. Their investigation categorizes WLAN attacks into snooping, modification, masquerading, and denial-of-service (DoS). The study points out WEP's vulnerabilities (e.g., weak RC4 encryption) and promotes WPA2's AES-CCMP, although it mentions its vulnerability to brute-force attacks. Suroto's study (2018) recommended countermeasures including MAC filtering, RADIUS authentication, intrusion detection systems (IDS), and safeguarding wireless networks using firewalls, encryption and decryption technology, and preventing SSID broadcast. However, the article lacks

experimental verification and misses rising concerns like IoT-based attacks. Suroto believes his future research should examine AI-driven IDS and post-quantum cryptography to manage escalating threats.

The paper by Thankappan et al. (2022) covers the growing threat of Multi-Channel Man-in-the-Middle (MC-MitM) attacks on Wi-Fi networks, specifically those secured by WPA, WPA2, and WPA3 security protocols [22]. These attacks leverage deficiencies in encryption and management frameworks, posing major challenges to IoT devices and enterprise networks. The work presents a full analysis of MC-MitM attacks,their evolution, and defense mechanisms, filling a vacuum in comprehensive analyses of such threats. The authors categorize MC-MitM attacks into base and advanced variants, explaining their technical configurations and impacts, such as key reinstallation (KRACK) and fragmentation assaults (FragAttacks). The research evaluates currently available countermeasures, including patches and Protected Management Frames (PMF), revealing their deficiencies, particularly for IoT devices. They also point out the persisting weaknesses in Wi-Fi security standards and the insufficient quality of current protections.

Despite wireless LAN's adaptability and cost-efficiency, it might be susceptible to security breaches due to its open transmission channel. In the year 2022 [23], Al Dallal and Al Sharify explore these risks, such as evil twin attacks, piggybacking, and data breaches, and recommend mitigating techniques, including encryption, MAC filtering, and WPA3 adoption. Their findings demonstrate the significance of fixing security weaknesses in IEEE 802.11 standards, specifically with the advancement of 5G and cloud computing. Their research categorizes wireless network threats into integrity, confidentiality, and access control violations. Their study includes a thorough threat analysis and effective solutions like virtual private networks (VPNs) and firewalls. The research also suggested technological alternatives like zero-trust architectures, and the recommendations remain conventional, without advanced AI-driven anomaly detection.

In their 2022 investigation, Nalukui and Lubobya carried out an in-depth assessment of Denial-of-Service (DoS) attacks in Wi-Fi broadband networks, specifically focused on public sectors where uninterrupted service is vital. Their research explores various attacks across several OSI levels, using the OPNET Modeller for simulations. Their research also finds weaknesses in IEEE 802.11 standards and highlights the necessity for appropriate mitigation strategies to ensure data integrity and network stability. The authors in [24] simulate various

DoS attacks, including jamming and HTTP flooding, and assess their effects on Wi-Fi performance.

The research carried out by Ye et al. (2020) addresses significant vulnerabilities in WLAN-based positioning systems. Their research shows that spoofing attacks such as MAC spoofing and IP spoofing and replay attacks allow attackers to gain unauthorized access. Their study also points out the key findings and existing defense mechanisms as well as proposed mitigation strategies. The unpredictability and reproducibility of Base-Station (BS) tags are used in their research to secure mobile social network services (MSNS), and bloom filters and fuzzy extractors are used to reduce transmission failures and storage overhead [25].

To identify and analyze network vulnerabilities in a WLAN, reconnaissance plays an important role. Significant research work by Mahmudul et al. (2024) in [26] explores various active and passive reconnaissance techniques for scanning and vulnerability assessment. In this research they discussed and researched the significance of network vulnerability identification and assessment techniques. Finally, their research shows the detailed process of network penetration testing and demonstrates how to identify vulnerabilities and enhance overall cybersecurity posture.

The analysis of the literature emphasizes the significance of understanding the WLAN vulnerability scanning and assessment techniques. In this continuous process of network security, future research should keep looking into comprehensive and feasible countermeasures against identified vulnerabilities of WLAN.

3. SYSTEMATIC VULNERABILLITY FRAMEWORK OF WLAN

Wireless Local Area Network (WLAN) vulnerability assessment comprises systematic approaches for detecting, investigating, and evaluating safety concerns in wireless network architectures. We must choose relevant scanning tools based on our particular needs. Key considerations include the scanner's potential to detect modern encryption vulnerabilities, its ability to identify rogue access points, and its support for current wireless standards. Before carrying out the network scan, focus on acquiring comprehensive details about the WLAN environment. This includes mapping out the network structure, identifying all connected gadgets, and understanding the security controls in place. Customize the scanning parameters based on the particular requirements of the WLAN. This may involve selecting what types of vulnerabilities to check, adapting the levels of detection accuracy, and scheduling the scan to minimize disturbance during maximum network usage. During scanning, we monitor the process for inconsistencies and performance implications. Real-time analysis can detect

imminent risks requiring quick prevention and intervention. The scan should thoroughly analyze encryption implementations, authentication processes, and any protocol weaknesses. After the scan is complete, we will review the results in depth. Identify and prioritize vulnerabilities based on their potential impact on the network. Look for weaknesses such as outdated encryption standards, misconfigured access points, or unauthorized devices.

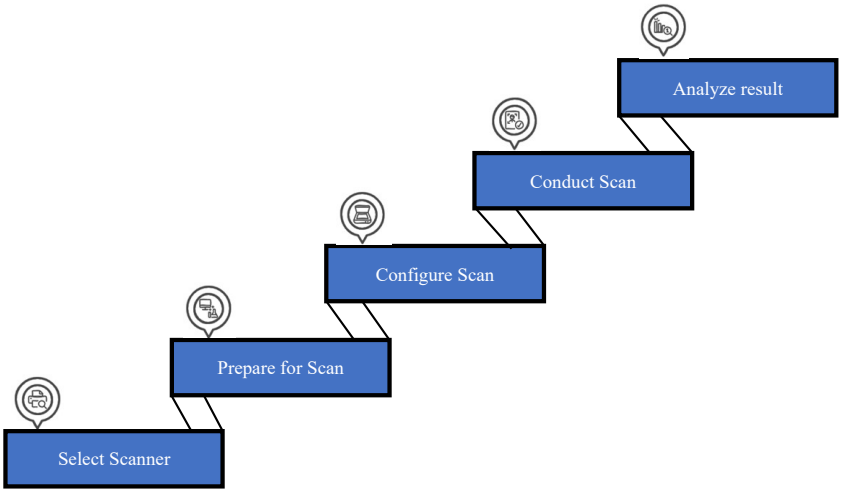

Figure 2: Systematic approach to identify weaknesses and potential threats of WALN.

3.1 PREPARATION AND PLANNING FOR WLAN VULNERABILLITY ASSESMENT

Research and the identification of targets established the foundation for effective penetration testing by identifying and profiling potential targets within a WLAN network technology. This phase is essential for acquiring a complete awareness of the WLAN environment, enabling security professionals to identify vulnerabilities, create effective testing procedures, and improve the overall security posture. It helps us figure out the potentially harmful landscape of target weakness, reveal high-value targets, conduct prospective risk assessment, discover potential vulnerabilities, and reveal specific targets inside a wireless local area network (WLAN) environment and identify attack surfaces. By recognizing and assessing target networks, we are able to lay out successful penetration testing strategies and improve the overall security architecture. It is made up of methodical processes to capture, organize, and evaluate significant information. Without executing this stage, testing efforts risk being disorganized and unproductive, potentially leaving significant potential threats overlooked. Information is the most powerful weapon in the penetration testing of a wireless local area network architecture. Gathering target information is a key component of the penetration testing of a wireless local area network. It helps penetration testers understand the

network's architecture, network topology, and security posture. Effective information gathering is a requirement for successful WLAN penetration testing. We can use information-gathering strategies to gain deep knowledge of the target wireless local area network (WLAN) architecture, identify potential vulnerabilities, and develop effective penetration testing approaches.

3.2 RECONNAISSANCE OF WLAN

Reconnaissance serves as the foundation for any comprehensive wireless local area network (WLAN) security assessment. Reconnaissance is an extremely essential component of information capturing during network (WLAN) penetration testing. There are two different types of reconnaissance, such as active and passive reconnaissance. By integrating a combination of passive and active reconnaissance techniques, we can gather potential insights into the target wireless network's architecture, determine potential vulnerabilities, gather open-source intelligence and device fingerprinting, communication protocols and misconfigurations, determine cryptographic weakness, detect rogue access points and discover hidden wireless networks, identify target service set identifiers (SSIDs), identify media access control (MAC) addresses of network devices, gather information about signal strength and channel usage, information about basic service set identifiers (BSSIDs), and available channels. Social engineering is an essential part of WLAN reconnaissance. It helps us to exploit human psychological vulnerabilities. It's very helpful in brute force and dictionary attacking techniques. Information gathering using reconnaissance techniques also identifies encryption and authentication mechanisms deployed by the network, finds open ports and vulnerabilities on wireless devices, and collects details about connected devices.

Wireless LAN (WLAN) reconnaissance is an essential phase in the initial processes of a cyber-attack, as we obtain information about the target network in order to identify vulnerabilities and build our attack methodology. Passive reconnaissance collects valuable information without interacting directly with the target network infrastructure. Packet sniffing techniques can be used to analyze wireless LAN traffic to discover information about the WLAN's architecture, services, and devices without alerting the target wireless LAN. Active reconnaissance technique is an approach that needs to interact actively with the target network infrastructure, such as pinging IP addresses or running port scans. Tools like nmap are frequently used to discover open ports and services executing on those ports and provide us with significant information with respect to possible vulnerabilities.

To wrap up preparations for wireless LAN vulnerability assessment, we will think according to attacker's points of view. In these circumstances several significant steps should follow:

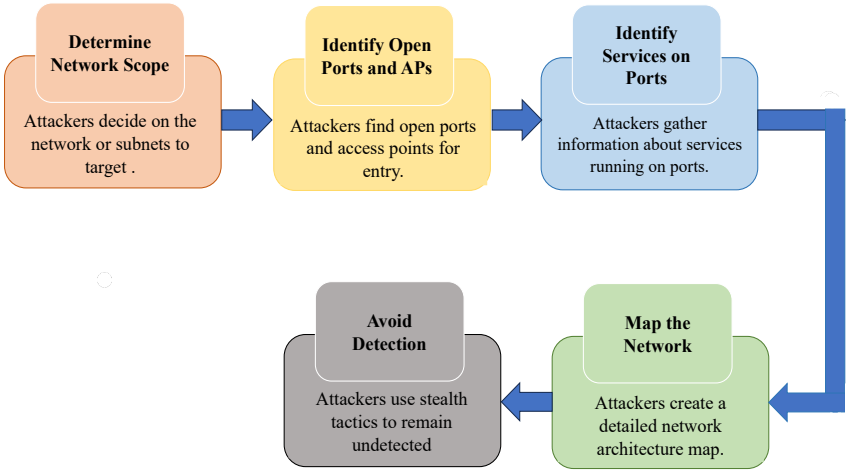

Figure 3: Prep

1. Determine Network Scope: We should determine the range of our reconnaissance by determining whether we will target the whole network or particular subnets. Understanding the layout of the network is vital for effective planning.

2. Identify Open Ports and Access Points (APs): Determining open ports becomes essential as it could function as a pathway for a security compromise. We can outline these ports and other open access points, especially for targeting Internet of Things (IoT) devices that normally have no potential security measures.

3. Identify Services on Ports: Once ports are discovered, we can obtain information about the services operating on these ports. This might involve employing banner-grabbing tactics to learn more about application protocols and their versions, which assists in creating attack strategies.

4. Map the Network: Creating an in-depth representation of the wireless local area networks (WLANs) architecture facilitates us finding out connections between devices, subnets, and services. This mapping is essential for developing suitable strategies within the WLAN architecture during penetration testing.

5. Avoid Detection: Maintaining stealth mode is important in reconnaissance initiatives. We can adopt various approaches to avoid detection by security systems. In exceptional situations, we have to spend weeks or months acquiring vital information without alerting network security infrastructure.

To do a reconnaissance, we must use a variety of tools and methods, including device discovery, network scanning, vulnerability scanning, OS fingerprinting, password cracking, social engineering, and gathering public information. By conducting extensive reconnaissance, we may uncover possible vulnerabilities and obtain a better understanding of the target network architecture before initiating an attack. This helps in planning for a focused assault and decreases the danger of finding weaknesses.

There are various tools available for wireless LAN reconnaissance, such as Nmap, Airodump-ng, Wireshark, AirCrack-ng, Kismet, Cowpatty, Reaver, Shodan, WiGLE, and Censys. These most common tools used for wireless LAN reconnaissance are essential for both wireless LAN analysis and penetration testing. It's important to note that some tools may require additional configuration and have specific requirements for the target network. Sometimes WLANs hide their identity. Gathering information about hidden networks is very crucial. To find hidden Wi-Fi networks, several tools are particularly effective, such as inSSIDer, NetSpot, Homedale, Wireless NetView, WiFi Analyzer (Android), Xirrus Wi-Fi Inspector, Vistumbler, and Netsh (Command Line Tool). These tools can be used in combination to perform a comprehensive wireless LAN reconnaissance. These tools provide various functionalities to detect hidden Wi-Fi networks effectively, catering to different user preferences and technical expertise levels.

3.3 SUITABLE WLAN VULNERABILITY SCANNERS

Several tools and techniques are needed while gathering and analyzing data in order to vulnerability assessment of wireless LANs. By using these tools and technologies, we may gather vital information about the target wireless networks through reconnaissance, traffic analysis, and vulnerability assessments. We can identify potential vulnerabilities in wireless networks and take advantage of them to obtain unauthorized access. Packet sniffing, war driving, de-authentication attacks, man-in-the-middle (MITM) attacks, vulnerability scanning, and rogue access point detection are frequently used in collecting information about the target wireless LANs.

Airodump-ng: It is a wireless network scanning tool that is used to collect packets and identify BSSIDs, SSIDs, and connected devices. This program also can find hidden networks, detect rogue access points (APs), and monitor used channels.

Kismet: Kismet is a wireless network discovery, intrusion detection system (IDS), and packet sniffing tool. It is used to do passive scanning to map WLAN topology and detect illegitimate devices. It also offers GPS mapping and protocol analysis.

NetStumbler: It is an active wireless network scanning tool that can detect access points (APs) and signal strength.

Figure 4: WLAN v

Aircrack-ng suite: Aircrack-ng is an encryption and protocol vulnerability tool. It is primarily intended for monitoring and assessing vulnerabilities in wireless networks. It can intercept packets and crack WEP/WPA-PSK encryption protocols. This utility can crack pre-shared keys (PSKs) via dictionary or brute-force assaults.

Wireshark: Wireshark is a packet analyzer that can scan unencrypted traffic, weak protocols (e.g., WEP, TKIP), and handshake problems. It can identify plain-text data breaches or KRACK (Key Reinstallation Attack) flaws in WPA2.

Fern Wi-Fi Cracker: Fern is an automated tool for cracking encryption and protocol weaknesses that can crack WEP/WPA keys and evaluate network security. It is GUI-based and interfaces with Aircrack-ng and Reaver.

Airgeddon: Airgeddon is used to identify phishing and such kinds of vulnerabilities. It is a multi-function toolbox for evil twin attacks, DoS, and credential harvesting. It also automates rogue AP creation and phishing page deployment.

Wifiphisher: Wifiphisher can construct rogue APs to launch phishing attacks and steal passwords. It can allow security analysts to measure user awareness and network vulnerability to social engineering.

Nessus: Nessus is one of the most reliable and advanced vulnerability scanners that is used at the enterprise level. It can detect outdated firmware, poor SNMP setups, misconfigurations, and CVEs in enterprise APs (e.g., Cisco, Aruba).

OpenVAS: OpenVAS is an open-source alternative to Nessus for scanning network vulnerabilities. It provides a user-friendly graphical interface and real-time updates on vulnerabilities. It can identify unpatched firmware and incorrect security policies.

Metasploit Framework: Metasploit Framework is a penetration testing and WLAN vulnerability assessment tool including modules for WLAN exploits (e.g., WPA2 handshake spoofing). It may simulate complex attacks like deauthentication floods or session hijacking.

BetterCAP: BetterCAP is a WLAN vulnerability assessment tool that can identify client-side vulnerabilities. This utility is used to monitor Wi-Fi, capture client probe requests, and MITM attacks. It also used to identify client isolation flaws and weak client authentication.

Reaver: Reaver is used to exploit WPS (Wi-Fi Protected Setup) PIN vulnerabilities. It can detect WPS-enabled routers with weak PINs.

InSSIDer: InSSIDer is a physical and signal leakage testing tool that can scan for overlapping channels, signal intensity, and rogue APs. It improves channel selection and detects physical-layer threats.

Hashcat: Hashcat is a WLAN password and credential testing tool. It can test PSK strength and rainbow table resistance. It also cracks and brute-forces WPA/WPA2 handshakes.

John the Ripper: John the Ripper is an offline password-cracking tool that can examine PSK hashes and crack passwords.

QualysGuard: QualysGuard is a cloud-based solution noted for its scalability and thorough scanning capabilities. It is best for enterprises wanting constant monitoring of their WLANs as part of a broader security strategy.

Nmap: Nmap is a strong network vulnerability analysis tool. It can scan devices for open ports and services, making it useful for discovering vulnerabilities in WLANs.

Wifite: Wifite is a wireless network auditing program that can search for wireless access points, crack WEP and WPA/WPA2 keys, and do additional security audits.

3.4 WLAN VULNERABILITY SCANNING AND ASSESMENT

In a wireless LAN (WLAN) vulnerability assessment, the network is examined for possible security flaws that unauthorized users might exploit. This assessment generally includes identifying weak encryption protocols, misconfigured access points, and outdated firmware that could leave the network susceptible to attacks. The following processes are usually carried out in or

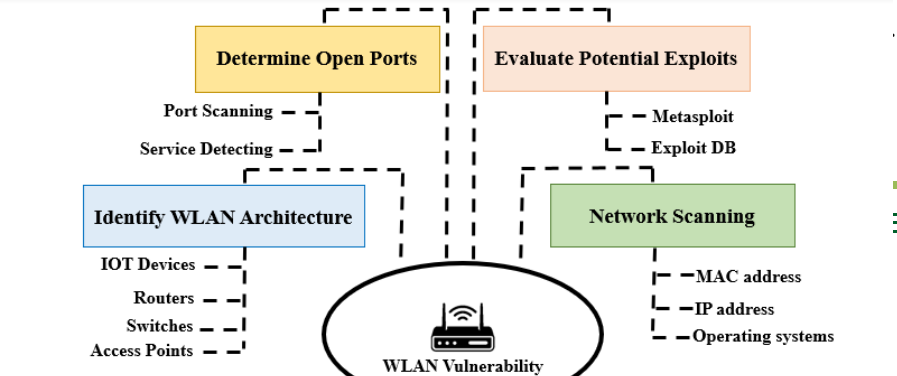

Figure 5: WLAN vulnerability assessment process.

Wireless networks are subject to several weaknesses that can be exploited by attackers. There are some common vulnerabilities in wireless networks, such as weak or default passwords, insecure configurations, insecure wireless connectivity, unencrypted traffic, insufficient security measures, outdated authentication methods, outdated or unpatched software, insider threats, weak encryption protocols, default SSIDs and passwords, deauthentication attacks, MAC spoofing, weak or predictable passwords, rogue access points, and vulnerable IoT devices. These vulnerabilities can lead to unauthorized access, data breaches, network interruptions, and other security incidents.

3.5 AI INTEGRATION IN WLAN VULNERABILITY DETECTION

An additional significant development in network security testing is the integration of artificial intelligence (AI) into WLAN vulnerability scanning. Conventional vulnerability assessment approaches generally depend on recognized standards and signatures. That's why traditional manual scanners can't identify continuously evolving vulnerabilities. We can implement machine learning (ML) algorithms to analyze enormous amounts of data to reveal patterns of potential vulnerabilities.

The following are some ways AI could improve vulnerability detection:

1. Automatic vulnerability scanning: Automatic vulnerability scanners may improve standard vulnerability detection processes by boosting their capacity to analyze logs and configuration data, identifying open ports, unencrypted connections, and unpatched software versions more efficiently than manual methods.

2. Predictive Analytics: AI employs machine learning approaches to examine previous data and predict future network activities. AI will predict where vulnerabilities may occur within WLAN infrastructures.

3. Behavior Assessment Using Deep Learning: We can integrate artificial intelligence (AI) to perform behavioral analysis to understand common user activities with the wireless LAN. Deep learning algorithms are excellent at identifying difficult behavioral patterns associated with zero-day vulnerabilities. This technique helps us to identify patterns of activity that could indicate a security vulnerability or unauthorized WLAN access.

4. Automated penetration testing: In order to find potential vulnerabilities, we can use AI to automate the penetration testing process by performing WLAN attacks. This AI-powered penetration testing tool can improve the accuracy of vulnerability assessments by adopting their methods based on past results.

5. Real-time monitoring and anomaly detection: We can employ machine learning (ML) algorithms to monitor real-time network traffic. It can determine vulnerabilities that may indicate a zero-day attack.

6. Integration with Intrusion Detection Systems (IDS): The implementation of AI-driven IDS has significantly boosted threat detection capabilities within WLANs. These systems utilize machine learning to evaluate enormous amounts of data for alerts of attack or vulnerability exploitation.

These illustrations explain how AI improves the accuracy and efficiency of WLAN vulnerability identification, which makes it an essential part of modern network security strategies.

4. CATEGORIZATION AND ANALYSIS OF WLAN VULNERABILITIES

Wireless networks are vulnerable to different vulnerabilities that can be exploited by attackers. Understanding these vulnerabilities is vital for adopting effective security approaches. Common vulnerabilities in WLAN are weak security protocols, unauthorized access points, unencrypted traffic, lack of authentication, misconfigured devices, default SSIDs and passwords, evil twin attacks, social engineering, de-authentication attacks, MAC spoofing, wardriving, and shoulder surfing.

4.1 ENCRYPTION VULNERABILITIES OF WLAN PROTOCOL

Weak encryption in WLANs creates significant threats that can lead to unauthorized access and data interception, man-in-the-middle attacks, replay attacks, insertion of malware, network manipulation, and device compromise. Protocol vulnerabilities in wireless LAN (WLAN) may arise when the network protocols used for communication between devices are not properly built or configured. Some of the most frequent protocol vulnerabilities include:

4.1.1 Wired Equivalent Privacy (WEP) protocol: WEP is now old-fashioned, and it is no longer considered secure because it has no integrity check capacity. WEP protocol is very susceptible to many attacks, such as key recovery attacks, packet sniffing, replay attacks, and brute-force attacks, because of its weak encryption and static keys. These vulnerabilities can be exploited by attackers to obtain unauthorized access, intercept data, or disrupt network functions.

4.1.2 Wi-fi Protected Setup (WPS) protocol: The vulnerabilities arising from Wi-Fi Protected Setup (WPS) create quite significant threats for unwanted access to wireless local area networks. We can exploit these vulnerabilities through several approaches such as WPS PIN Guessing, Brute-Force Attack, WPS Lockout Bypass, and Social Engineering. We will brute-force the 8-digit PIN using tools such as Reaver or Bully. Reaver and Bully divide the PIN into two parts, limiting the effective search space to 11,000 possibilities. This facilitates obtaining unauthorized access to the network by making it easier to guess the correct PIN.

4.1.3 Wi-Fi Protected Access (WPA) Protocol: Wi-Fi Protected Access (WPA) was developed as a more secure alternative to the no longer relevant WEP (Wired Equivalent Privacy) protocol. While WPA considerably improves wireless security compared to WEP, it still contains serious vulnerabilities that can be exploited by attackers. Key reinstallation attacks (KRACK), Beck-Tews attacks, packet sniffing, WPS PIN vulnerability, brute-force attacks, and rogue access points are the main vulnerabilities of the WPA encryption protocol. These kinds of vulnerabilities can compromise WLAN network security and put sensitive information at risk. The Aircrack-ng suite is used to decrypt packets or inject malicious packets

4.1.4 Wi-Fi Protected Access 2 (WPA 2) protocol: Wi-Fi Protected Access 2 (WPA2) is one of the latest versions of the WPA protocol that includes additional security features. It

utilizes the AES (Advanced Encryption Standard) encryption technique in association with the CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol). This protocol has been considered secure for home, corporate, and government networks and has resolved the weaknesses of WPA. WPA2 is a commonly used security protocol that offers encryption for wireless data. It incorporates new capabilities, such as the integrated authentication protocol (IEEE 802.1X). It can enable more powerful authentication and access control mechanisms. WPA2 is regarded as far more secure compared to its predecessors WEP and WPA; it still has flaws that may be exploited by attackers. Here are some of the most noteworthy vulnerabilities linked with WPA2 handshake capture, key reinstallation assaults (KRACK), brute-force attacks, downgrade attacks, PTK (pre-shared key) attacks, rogue access points, eavesdropping, and man-in-the-middle (MitM) attacks. Device centric vulnerabilities of WLAN (including IoT devices vulnerabilities).

4.2 DEVICE VULNERABILITIES OF WLAN

Device vulnerabilities associated with wireless local area networks (WLANs) refer to weaknesses in the hardware and software of devices connected to the network that can be manipulated by attackers. Device vulnerabilities in WLANs represent major threats to both individual users and businesses. These types of vulnerabilities can lead to unauthorized access, data breaches, and numerous sorts of cyberattacks. Device vulnerabilities connected to WLANs are rogue access points, weak encryption protocols, inadequate authentication mechanisms, firmware vulnerabilities, eavesdropping, denial-of-service (DoS) attacks, session hijacking, malware infections, outdated or vulnerable software, default or weak passwords, lack of security features, misconfigured firewalls, insufficient patch management, and insider threats.

4.2.1 IoT DEVICE VULNERABILITIES IN WLANs

Internet of Things (IoT) devices, such as smart thermostats, cameras, and sensors, rely heavily on Wireless Local Area Networks (WLANs) for connectivity. The integration of Internet of Things (IoT) devices into wireless local area networks WLANs have significantly expanded the attack surface of modern networks. Although IoT devices have their functional benefits, they do not have robust security mechanisms. These vulnerabilities make IoT devices an ideal target for attackers. IoT devices in WLANs pose a complex security

challenge due to their inherent limitations and the open nature of wireless networks. Weak authentication mechanisms (like using default credentials and not implementing multi-factor authentication), insecure communication protocols (such as obsolete encryption techniques and unsecured data transfer), irregular software and firmware updates (like not having updates available and risks from third-party software), inadequate network configuration (including flat networks and unprotected guest access), physical security problems (like hardware that can be tampered with and exposed ports), limitations on resources affecting security (like low processing power and memory), easy connections for unauthorized devices (like auto-connect features and no device authentication), and data leaks through side-channel attacks increase the chances of WLAN attacks. These IoT device vulnerabilities can lead to data theft or major disruptions in the WLAN infrastructure.

4.2.2 CONFIGURATION-BASED VULNERABILITIES

Configuration-based vulnerabilities stem from improper or insecure settings in WLAN devices, such as access points (APs) and client devices. These vulnerabilities can lead to unauthorized access, data interception, or network disruption. Outdated firmware and software, default credentials, weak passwords, weak or predictable pre-shared keys (PSKs), open ports, insecure encryption protocols, lack of standardization, inadequate logging, DoS vulnerability, open SSIDs, rogue APs, incorrect channel/frequency settings, and disabled security features are known as common configuration-based security vulnerabilities in WLANs. Misconfigurations can allow attackers to gain unauthorized access, intercept sensitive data, or disrupt network operations. For instance, weak encryption like WEP can be cracked in minutes, exposing all network traffic.

4.2.3 ACCESS CONTROL VULNERABILITIES

Access control vulnerabilities arise due to the deficiencies in the processes that manage network access. That allows unauthorized users to connect or intercept unauthorized data. Weak authentication, inadequate PSK management (WPA2/WPA3-Personal),weak 802.1X/EAP implementation, vulnerable protocols, lack of device profiling, evil twin attacks, failure of MAC address filtering, unauthorized access, bypassed captive portals, and inadequate guest network segmentation and authorization vulnerabilities are frequently seen as serious threats to WLAN security. These vulnerabilities can lead to data breaches,

unauthorized network access, or man-in-the-middle attacks. As an example, rogue access points (APs) can bypass security parameters, providing attackers with a backdoor.

4.2.4 PHYSICAL SECURITY VULNERABILITIES

Physical security vulnerabilities of wireless LAN arise due to the broadcast nature of WLANs and the physical accessibility of WLAN devices. This vulnerability enables attackers to intercept or tamper with WLAN. Physical vulnerabilities can lead to data breaches, network reconfiguration, or unauthorized access by the attacker. Unauthorized AP placement, uncontrolled signal range, lack of proper access controls, lack of AP tamper protection, device theft, shoulder surfing, RF signal leakage, unsecured PoE sources, and exposed network cabling are the most common vulnerabilities related to WLANs.

4.3 WLAN COMPROMISE DUE TO HUMAN VULNERABILITIES

Human vulnerabilities significantly lead to the compromising of wireless local area networks (WLANs). Human flaws usually originate due to user behavior, human psychology, security carelessness, and lack of understanding. Compared to technical weaknesses, these human characteristics are less predictable and more difficult to handle. These characteristics make them a persistent threat. Common vulnerabilities include weak password practices (i.e., default, easily guessable, or reused passwords); susceptibility to social engineering (i.e., phishing, pretexting, impersonation, and evil twin attacks); inadequate security awareness; carelessness in deploying updates; risk factors connected with Bring Your Own Device (BYOD) policies; improper device disposal or loss (loss of configured devices, improper wiping); misconfiguration; and physical security gaps. These practices expose WLANs to illegal access, data breaches, and malware infection.

Table 1 : WLAN vulnerabilities and it's exploitation techniques.

Vulnerability	Description	Exploit Techniques
Weak Passwords	Use of weak or default passwords on WLAN access points enables unauthorized access.	Brute-force, dictionary, and credential-stuffing attacks.
Open WLANs	Networks without encryption allow unauthorized access and traffic	Passive eavesdropping, man-in-the-middle (MitM).

	interception.	
Malware Infection	Routers or access points infected with malware can compromise the network.	Remote code execution, botnet integration.
Rogue Access Points	Unauthorized APs mimic legitimate networks to deceive users and intercept traffic.	Evil twin attacks, credential harvesting.
Port Scans	Scanning for open ports reveals vulnerabilities in WLAN-connected devices.	Network mapping, vulnerability identification.
DoS Attacks	Flooding networks with excessive traffic disrupts legitimate access.	SYN floods, ICMP flooding, spectrum jamming.
Sniffing Attacks	Capturing unencrypted data packets exposes sensitive information.	Passive packet sniffing, Wi-Fi eavesdropping.
Man-in-the-Middle (MitM)	Intercepting and modifying data between devices enables data theft and manipulation.	ARP spoofing, session hijacking, DNS cache poisoning.
Insider Threats	Employees or authorized users can exploit access to compromise network security.	Social engineering, phishing, physical tampering.
Weak Encryption (WEP)	WEP uses weak initialization vectors that are easily cracked.	IV capture and key cracking using tools like Aircrack-ng.
WPA2 KRACK Attack	Vulnerability in WPA2 allows reinstallation of encryption keys during handshake.	Handshake manipulation, key reinstallation attacks.
WPA3 Dragonblood Attack	Flaws in WPA3's Simultaneous Authentication of Equals (SAE) allow credential exposure.	Downgrade attacks, side-channel analysis.
WPS Vulnerabilities	Brute-force attacks exploit the WPS PIN mechanism to gain unauthorized access.	WPS PIN brute-forcing using tools like Reaver.

Hidden SSID Issues	Hidden SSIDs can be revealed when devices broadcast probe requests.	Probe request capture via tools like Kismet.
Jamming and DoS	Overloading the wireless spectrum disrupts network availability.	Signal interference, noise flooding.
Guest Network Exploits	Misconfigured guest networks allow attackers to move laterally within the network.	Network pivoting, unauthorized resource access.
Bluetooth Exploits	Exploitation of vulnerabilities in Bluetooth protocols and devices.	Blueborne, Bluetooth snooping, malicious payload injection.
SSID Spoofing	Creating fake SSIDs confuses or deceives users into connecting to malicious networks.	Fake AP setup, social engineering.
Insufficient Patch Management	Outdated firmware leaves devices vulnerable to known exploits.	Exploitation of unpatched vulnerabilities.
IoT Device Vulnerabilities	Insecure IoT devices on WLANs introduce significant risks to network integrity.	Exploitation of default credentials, weak protocols.
Captive Portal Exploits	Weak or misconfigured captive portals can be bypassed by attackers.	Session hijacking, manipulation of portal traffic.
Channel-Based Attacks	Poor channel management leads to interference and signal degradation.	Exploiting channel congestion, denial-of-service.
Weak Management Frame Protection	Unprotected management frames enable spoofing and disruption attacks.	Frame injection, spoofing attacks, deauthentication.

5. FUTURE WORK

Our research has provided a comprehensive analysis of Wireless Local Area Network (WLAN) Our future investigation will investigate the deployment and effectiveness of wireless intrusion detection systems (WIDS) and wireless intrusion prevention systems (WIPS) to monitor real-time activities of WLAN. However, as information technology continues to improve and cyber-attacks constantly increase, several promising directions remain open for further exploration to enhance the scope and effectiveness of WLAN

security. Future enhancements of this study will concentrate on expanding multiple aspects of research approaches demanded by the evolving complexity and diversity of WLAN-related threats. The following areas are identified as potential future research opportunities.

1. To identify emerging threats of WLAN, our future studies should focus on conducting systematic and comprehensive penetration testing across a broad range of WLAN devices.
2. Our next research will give emphasis on the design and evaluation of practical, robust, adaptive, cost-effective, and scalable mitigation strategies tailored to diverse WLAN environments. This includes addressing vulnerabilities related to outdated protocols, weak authentication, and insecure configurations, suitable for networks ranging from small home networks to large enterprise infrastructures.
3. Further research on the integration of Machine Learning (ML) and Deep Learning (DL) models to enhance automatic WLAN vulnerability detection and prediction as well as assess the associated risks.
4. Our future investigation will investigate the deployment and effectiveness of wireless intrusion detection systems (WIDS) and wireless intrusion prevention systems (WIPS) to monitor real-time activities of WLAN.
5. Enhanced Network Discovery and Traffic Analysis will explore active and passive networks. That will analyze encrypted and unencrypted traffic and can provide insights into hidden vulnerabilities and unauthorized interactions within WLANs.
6. Simulating exploitation techniques and real-world attack scenarios (i.e., packet injection, rogue Access Point (AP) deployment, man-in-the-middle (MitM) attacks, and spoofing) will help security researchers to understand attacker methodologies and evaluate the resilience of existing defense mechanisms, thereby reinforcing defensive strategies.
7. Attack simulation to crack WLAN encryption protocols (e.g., WPS, WEP, WPA, WPA2, WPA3) and compromise WLAN. It will provide a better understanding of limitations and potential vulnerabilities under real-world conditions.
8. Controlled experiments and penetration testing using Denial-of-Service (DoS) and De-authentication attacks will help in formulating resilient mitigation techniques and inform countermeasures to reinforce network resilience against service disruption.

9. Our future research will discover how social engineering facilitates WLAN compromise. And also discuss the impact of phishing attacks on WLAN security.
10. Identify WLAN device firmware vulnerabilities and perform firmware reverse engineering to analyze associated vulnerabilities.

Addressing these areas will contribute to the development of more intelligent, adaptive, and robust WLAN infrastructures capable of withstanding increasingly sophisticated cyber threats. This approach is akin to continually upgrading a castle's defenses, not just by reinforcing its walls, but also by training its guards, understanding new siege tactics, and even anticipating how attackers might try to trick their way inside.

6. CONCLUSION

Wireless networks are increasingly overtaking wired networks as the most popular choice for worldwide connectivity. As a result, communication over the air leaves WLANs vulnerable to various attacks. In this article, we have evaluated that the WLAN security is a crucial element that should not be overlooked. There are so many users of the WLAN whose personal and confidential data must be safeguarded. Our research is focusing on the significance of scanning and assessment of WLAN vulnerability. In this research, we have identified, analyzed, and described some of the common WLAN vulnerabilities. Further, we have noted that common WLAN vulnerabilities should be mitigated properly. In our future research plan, we also described the importance of performing penetration testing on WLAN. Our comprehensive research on WLAN security will inspire the next generation of researchers to overcome the potential vulnerabilities with the existing network architecture.

References

[1] Nazir, R., Laghari, A. A., Kumar, K., David, S. Ali, M. (2021). Survey on Wireless Network Security. Archives of Computational Methods in Engineering, 1–20. https://doi.org/10.1007/S11831-021-09631-5

[2] Munusami, Cholavendan, and Rajeshkumar Venkatesan. "A compact boat shaped dual-band MIMO antenna with enhanced isolation for 5G/WLAN application." *IEEE Access* 12 (2024): 11631-11641.

[3] Kurose, J. F., & Ross, K. W. (2020). Computer Networking: A Top-Down Approach (8th ed.). Pearson.

[4] IDC. (2023). Worldwide WLAN Market Grew 20.4% Year Over Year in 2022, According to IDC Tracker. https://www.idc.com/getdoc.jsp?containerId=prUS50569923

[5] Cisco. (2020). Annual Internet Report (2018–2023). https://www.cisco.com

[6] Market Research Future https://www.marketresearchfuture.com/reports/wlan-market-1012

[7] Wifi Market https://www.marketsandmarkets.com/Market-Reports/global-wi-fi-market-994.html#:~:text=The%20Wi%2DFi%20market%20is,drives%20the%20Wi%2DFi%20market.

[8] Rots Analysis https://www.rootsanalysis.com/wi-fi-market

[9] Open PR https://www.openpr.com/news/3654858/wlan-market-1-60b-in-2023-projected-to-reach-3-22b-by-2030

[10] Saxena, S., & Chaudhari, S. (2020). WLAN Security and Its Issues: A Review. Proceedings of the 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), 345–351. https://doi.org/10.1109/ICSTCEE49637.2020.9277052

[11] Ponemon Institute. (2023). Cost of a Data Breach Report. IBM Security. https://www.ibm.com/security/data-breach

[12] IBM Security. (2022). Cost of a Data Breach Report 2022. https://www.ibm.com/reports/data-breach

[13] Cyber Crime Magazine, 2022. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

[14] Khera, Yugansh, Deepansh Kumar, and Nidhi Garg. "Analysis and impact of vulnerability assessment and penetration testing." *2019 international conference on machine learning, big data, cloud and parallel computing (COMITCon)*. IEEE, 2019.

[15] Nasr, Elie, et al. "Wi-fi network vulnerability analysis and risk assessment in Lebanon." MATEC Web of Conferences. Vol. 281. EDP Sciences, 2019.

[16] Alueendo, Rauha, et al. "A Systematic Review: Vulnerability Assessment of Wi-Fi in Educational Institution." 2020 IST-Africa Conference (IST-Africa). IEEE, 2020.

[17] Nikolov, Linko G. "Wireless network vulnerabilities estimation." Security & Future 2.2 (2018): 80-82.

[18] Mohammed, Kashim Kyari. "WLAN Vulnerability Scanning Methodologies." WLAN Vulnerability Scanning Methodologies.

[19] Etta, Victor Ojong, et al. "[Retracted] Assessment and Test-case Study of Wi-Fi Security through the Wardriving Technique." Mobile Information Systems 2022.1 (2022): 7936236.

[20] Bharath Ajay Gorli, Rithik Reddy Baddam, Geethika Chowdary Talasila, " Enhancing Wireless LAN Security : A Comprehensive Analysis on Threatsand Vulnerabilities" International Journal of Scientific Research in Computer Science, Engineering and Information Technology(IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 6, pp.316-321, November-December-2023. Available at doi : https://doi.org/10.32628/CSEIT2390640

[21] Suroto, Suroto. "WLAN security: threats and countermeasures." JOIV: International Journal on Informatics Visualization 2.4 (2018): 232-238.

[22] Thankappan, Manesh, Helena Rifà-Pous, and Carles Garrigues. "Multi-channel man-in-the-middle attacks against protected wi-fi networks and their attack signatures." International Conference on Computer, Communication, and Signal Processing. Cham: Springer Nature Switzerland, 2023.

[23] Al Dallal, Haroon Rashid Hammood, and Thimar Falih Yasir Al Sharify. "Study Of Security Improvements In Wireless Network." JournalNX 8.9 (2022): 4-11.

[24] Nalukui, Akende Y., and Charles S. Lubobya. "Effects of DoS Attack in Wi-Fi Broadband Network." International Journal of Networks and Comm 12.2 (2022): 47-54.

[25] Ye, Ayong, et al. "Detection of spoofing attacks in WLAN-based positioning systems using WiFi hotspot tags." IEEE Access 8 (2020): 39768-39780.

[26] M. Hasan et al. "A COMPREHENSIVE INVESTIGATION OF RECONNAISSANCE THREATS AND ITS REMEDIATION,"in IJARMSS, vol.13, pp. 1-29, issue 11, Nov. 2024, ISSN: 2278-6236.

BIOGRAPHY

At the moment, **Mahmudul Hasan** is getting training from BUET under the course of CCNA. In the future he wants to work with a research team in the sector of cybersecurity and communication systems. Moreover, he is working as a project assistant under a supervisor named Mohammad Arifin Rahman Khan.

Mohammad Arifin Rahman Khan received one of his research degree from Edith Cowan University, Australia in 2019 and completed his M.Sc. degree from London Metropolitan University, London in 2010. He is working as a principal supervisor for this project. According to his professional career, Mohammad Khan has teaching experience from national and foreign universities. Moreover, for more than 5 years, he has experienced from the position of research assistant. He worked as a director of thesis and project for the department of CSE at Bangladesh University. His research interests include mobility management, multimedia transmission, and quality-of-service (QoS) etc. provision issues in the next-generation of wireless/mobile networks.

Mohammed Ibrahim Hussain has completed the Masters in E-Commerce from London, UK. He had completed Bachelor Degree in Computer Science and Engineering from The National Technical University of Ukraine, Kiev, Ukraine. He has successfully completed Cisco Certified Network Associate (CCNA), Microsoft Certified Technology Specialist (MCTS) and Microsoft Certified T Professional (MCITP) on Server 2008 platform. He is also nominated Book Reviewer of The National Curriculum of Textbook Board. His research interest includes Operating Systems, Networking and Microwave.

Md. Moazzam Hossain completed his B.Sc. in computer science and engineering degree in 2023 from Bangladesh University. At the current moment, he is working as an Executive Data Analyst & SEO Specialist with Creatif. In the future, he wants to involve himself as a research member for the field of wireless communication.

At the moment **Mujahid Ahmed** is working with one of his research projects under a research team in Bangladesh. He is also studying in Computer Science and Engineering course in Bangladesh University. In the future he wants to work in communication technology to earn a lot of knowledge about network security.

Ariful Islam Naeem is working on his final year project to complete his B.Sc. in computer science and engineering degree from Bangladesh University. In the future, he wants to work on a researchable project under a research team.

Hasan Miah is a final year student under the course of B.Sc. in Computer Science and Engineering Department at Bangladesh University. At the moment, he is working with a project team to try to evaluate the further improvement of computer security. In the future, he wants to work in communication technologies and the security sector.

Sabbir Hasan is a final year B.Sc. project student under the department of computer science and engineering, Bangladesh University. In the future, he wants to involve himself as a security I.T. member for the field of wireless communication, and wants to work with a research team in the future.