Wireless LAN vulnerabilities assessment

*Nattala Annie Supriya, MSc CyberSecurity, Northumbria University, London, United Kingdom*

**Abstract:** This assignment will entail the description of the vulnerabilities of security encryption in a Wireless local area network. The technical flaws in WLAN and how they can be bypassed by using tools like Kali Linux and a wireless adapter in monitor mode. Discussing the flaws in WEP and WPA 2 which impacts the WLAN. Identifying the 802.11 standard clients and recognizing how they can be exploited. Based on the security measures, evaluating the efficient procedures and systems that can be suitable in the environment.

**Keywords**— WLAN Authentication, Hidden SSID, MAC Filtering, WEP, WPA, WPA2, and 802.11 standards.

# Introduction

The implementation of Wireless LAN to connect mobile devices with wired infrastructure has opened new possibilities for communication, an innovative route in networking technologies. While contemplating this type of communication, protection should be a key consideration. People and businesses logged into the systems or networks without thinking about their security. People finally realized that a certain level of security was required to prevent malicious actors from misusing the information in the network. Wireless communication is more difficult to secure than wired networks unless a malicious actor within a transmitter's range has access to the transmission medium. Data privacy over a radio channel is frequently accomplished by encryption. While it is feasible to encrypt wireless communication, it frequently comes at a higher cost and offers less performance. Businesses are effectively incorporating wireless networks based on the 802.11 specifications..

A proper safety system is provided by several security features included in the 802.11 standards. Focusing on the widely used Wired Equivalent Privacy (WEP) protocol in this section. The WEP algorithm's primary objective is to prevent eavesdropping on wireless communication. Unauthorized access to a wireless network is widely thought of as a feature of WEP even though it isn't an objective of the 802.11 standards for WLAN. However, the Wired Equivalent Privacy (WEP) protocol used by 802.11 only offers an extremely limited level of support for Wi-Fi confidentiality. The IEEE review panel has left challenging security concerns, such as key management and a strong authentication system, as unresolved topics.

There are various issues with WEP that WPA fixes. The problems of security and confidentiality are reduced by using the Temporal Key Integrity Protocol (TKIP), just as the use of a RADIUS or Kerberos authentication server reduces the problems of client-to-AP authentication and unauthorized network access. The WEP-key scheme’s predictability is eliminated, the key size is significantly increased, per-user keying is permitted, an integrity-checking system is established, and more.

There are two variants of WPA that can be used: WPA-Enterprise and WPA-Personal.WPA-Enterprise employs the 802.1x authentication architecture to prevent unauthorized network access by authenticating network users with a RADIUS or authentication server and providing per-user keying.. The confidentiality of the per-user key has not yet been subject to any attacks against WPA-Enterprise. Only the computer from which it was stolen would be useful to an intruder who could deduce the key. WPA-Personal uses the same TKIP key encryption technology as WPA, but instead of the unique keys that each user receives from the authentication server, it uses a pre-shared key (PSK). This approach is frequently referred to as WPA-PSK. The WPA-PSK protocol requires users to communicate a passcode, which can be between eight and 63 ASCII characters or 64 hexadecimal digits long (256 bits). This passcode, like WEP, is kept on the client's computer and the AP and is the same for all network users. WPA-PSK were created for usage at home or in small businesses.

WPA2, like WPA, uses the 802.1X/EAP architecture to ensure centralized mutual authentication and dynamic key management. It also includes a pre-shared key for usage in homes and small offices. WPA2, like WPA, is designed to protect all 802.11 devices, including 802.11b, 802.11a, and 802.11g multi-band and multi-mode devices. One way that WPA and WPA2 vary is that WPA2 uses a mixed mode to allow WPA and WPA2-equipped devices on the same wireless network. WPA and, more specifically, its TKIP encryption mechanism can be broken. The technique is the main distinction between WPA and the more secure WPA2 standard. The encryption of packets. AES is the type of encryption used by WPA2. AES is a block cipher that encrypts packets as they are delivered using progressively larger key bit sequences. WPA2 is safer than WPA since it does not use the TKIP encryption method, instead employing the RC4 bit-by-bit stream cipher approach. To encrypt Top Secret information, the National Security Agency employs the 192-bit and 256-bit key lengths of the AES block cipher iterative encryption method as implemented in WPA2. This encryption standard is regarded to be especially powerful.

# Technical Flaws

Recent studies have demonstrated how simple techniques can readily compromise 802.11 network access. The 802.11 wireless network standard has been given a bad reputation because of academic researchers. In this demonstration, vulnerabilities are examined closely, which can make implementing wireless LANs problematic for many businesses. All are aware of the vulnerability of Internet traffic, but at least much of it is transported over fiber or wire. Due to the fact that wireless traffic is broadcast into the air, anyone with an interest in doing so can intercept it, making it even more vulnerable. Let's examine the different Wi-Fi security measures and their weaknesses. It is critical to understand what protection measures exist and what vulnerability flaws they have in order to defend a wireless network.

1. Bypassing WLAN Authentication—Hidden

Wireless local area networks can be identified only by their ESSID (Extended Service Set Identifier), a string of characters. In order to establish security through obscurity, hiding the ESSID is a bad strategy; regrettably, the ESSID may be acquired by:

* Scanning the wireless environment, seeing clients as they connect to networks, and capturing that connection.
* Deactivating a client actively to make them reconnect, then capturing that connection

Hidden SSID refers to a wireless connection that does not identify itself by displaying its SSID in broadcast beacons and does not reply to broadcast probe requests, making it unavailable even in the list of networks on Wi-Fi devices. It also implies that normal users will not be able to see this Wi-Fi network in their list of accessible networks. The absence of Wi-Fi, however, does not imply that an SSID is never broadcast over the air, but rather that it is broadcast in clear text with numerous packets between access points and devices connecting to them, regardless of the degree of security utilized. As a result, SSIDs are constantly public for all Wi-Fi network interfaces in a range, and any attacker employing different passive sniffing tools may see them..

To make it simpler for testing wireless communications, Kali Linux is embedded with several tools; nonetheless, the full effectiveness of these attacks takes comprehensive configuration steps.Before launching attacks or monitoring a wireless network, researchers should first learn the fundamentals of wireless networking. The most important tool in this operation is the wireless adapter, which connects to the wireless access point in monitor mode. The card's chipset and drivers, in particular, must be capable of inserting wireless packets into a communication stream. It must support the tools used, particularly the aircrack-ng tool suite.

Using the command “airodump-ng wlan0mon” to check the traffic in the network. We get the comprehensive list of devices (their BSSID, ESSID, encryption, etc.) connected to the network.

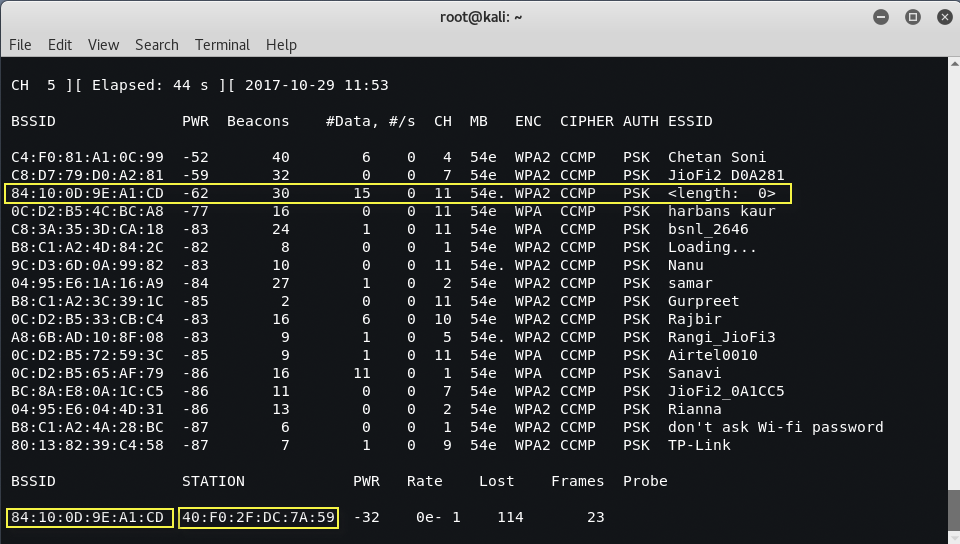


Figure 1: List of networks – Hidden SSID

As the ESSID is hidden in the figure above, the length is said to be "0," but this is not the case as all ESSID must have a designated name with characters, numbers, or symbols ranging from the length of 3 to 10 minimum.

Let's focus on that particular connection, the source of the attack to find the hidden SSID.

"aireplay-ng -0 10 -a 84:10:0D:9E:A1:CD -c 40:F0:2F:DC:7A:59 wlan0mon" is run in a new window. This command is used to send deauthentication packets to the device with the "wlan0mon" interface with that BSSID.

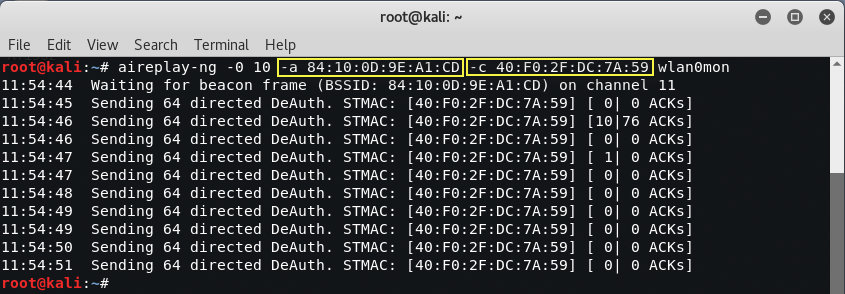


Figure 2: Deauthentication packets – Hidden SSID

This channel 11 is monitored from the previous window. Now that we are trying to connect to the device there has been a connection established.

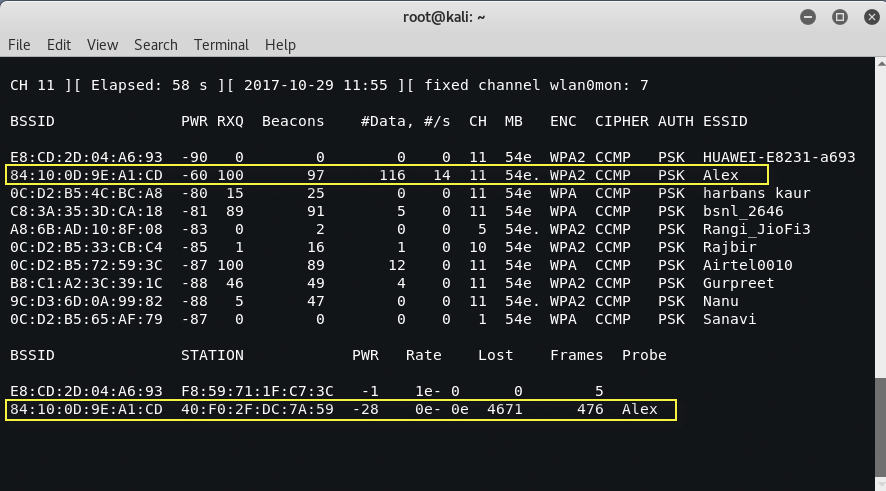


Figure 3: Revealed Hidden SSID

By scanning the network and pinpointing the connection, the hidden SSID is discovered.

1. Bypassing WLAN Authentication – MAC Filtering

A significant proportion of routers incorporate the security function known as MAC Filtering, also known as MAC Whitelist or MAC Blacklist, which enables or prevents Web access for a certain MAC Address. If such configuration is enabled, only machines that are allowed by MAC filtering can use a specific access point. In many cases, this may be adequate as a security precaution, making it slightly more difficult to access the network even when users know the password. Although this method has been proven to not be enough to secure the network or the devices.

The method to bypass MAC Filtering is to first capture the packets in the network by using the airodump-ng command. The airodump-ng command will show the list of all the connected clients. Particularly the BSSID of the device that is connected to the network.

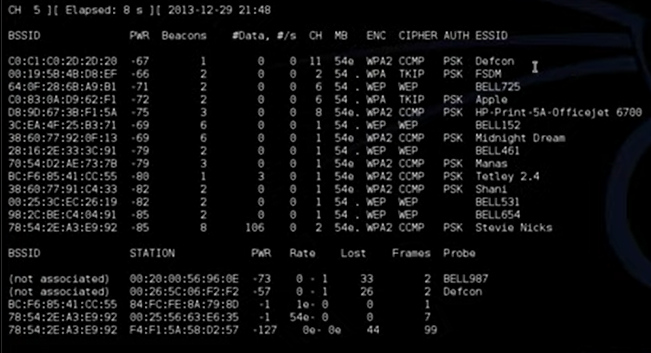


Figure 4: List of connected devices – MAC Filtering

Using the command “ airodump-ng –c 11 –bssid C0:C1:C0:2D:2D:20 wlan0” to navigate traffic of ‘Defcon’.

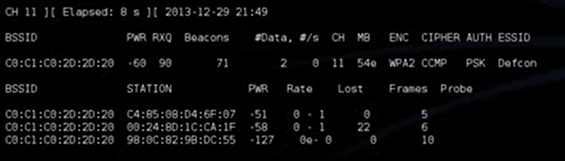


Figure 5: Traffic of accepted MAC ID

The acceptable mac addresses on the network are in the figure above. It is used to determine which devices are connected to the network. There are 3 devices/stations connected to the ‘Defcon’ network. Bad actors can temporarily change their mac address to spoof as another device that is already connected to the network to gain access. Choosing the third mac address due to the power of the connection.

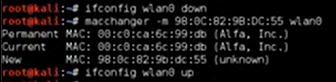


Figure 6: Changing MAC of the interface

Using ‘macchanger’ to change the MAC address of the interface wlan0 into a mac address that is acceptable in the network. In the above figure, the present mac address and new mac address can be verified. The Arp table will now show the spoofed interface with the changed mac address.

Now through the interface, a successful connection is made to the network ‘Defcon.’ By changing the MAC address any hacker can gain access to the network by bypassing the MAC filter in the demonstration.

# WLAN Encryption flaws

Considering current WLANs are based on IEEE 802.11 standards, the term "Wi-Fi" is frequently used interchangeably with "WLAN." Nowadays, everyone uses WLAN technology, owing mostly to the need for an Internet connection. People can use a smart device connected to a Wi-Fi Access Point to access the Internet from their homes, workplaces, and even public places such as coffee shops and shopping malls (AP). The issue here is that nobody actually cares if the connection is safe. Several individuals are aware of the phrases authentication, encryption, WPA, and WPA2, but few understand how they work or how they might be cracked or even evaded.

1. WEP Cracking

Firstly we must configure a WEP connection in the environment as this demonstration must follow the coursework guidelines. Connecting to the Wi-Fi provider website and configuring the network to have WEP security encryption. Resetting the router to follow that particular encryption.

Using the command “airodump-ng wlan0” to see what devices are connected to the network

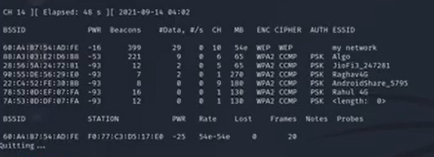


Figure 7: List of network devices – my network (WEP)

Here the connections are noted and the WEP network which was configured is seen in the traffic.

Command “airodump-ng –c 10 –bssid 60:A4:B7:54:AD:FE –w capfile wlan0” is used to write the flow of information from the traffic into the capfile. The capfile is stored in the root.

The Deauthentication command ”aireplay-ng –1 0 –a 60:A4:B7:54:AD:FE wlan0” is executed on another terminal window to make a connection through the handshake.



Figure 8: Connection success - WEP

Command “aircrack-ng capfile-01.cap” is used to test various combinations of characters to crack the password for the connection.

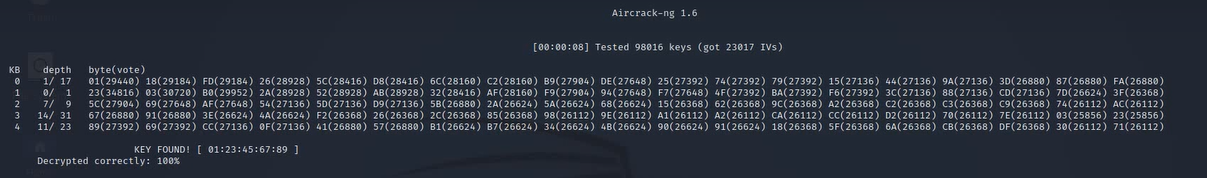


Figure 9: Successfully cracked WEP

The WEP encryption is successfully cracked in this demonstration by capturing the traffic and running aircrack-ng to find the appropriate key.

1. WPA2 Cracking

The WPA2 weakness is serious and offers a sizable attack surface, but because it can only be used locally, rather than remotely through the Internet, it has less of an impact. Totally avoiding WPA2 encrypted Wi-Fi networks is not practical. People should be practical in these situations and use the security measures that are now available for 4G mobile internet connections while they wait for the makers to create and release fixes for their devices. WPA2, the latest Wi-Fi standard, is still a more secure option than WEP. So it is strongly advised against migrating to an outdated, trivially exploited protocol. When utilizing Wi-Fi, it is preferable to keep using WPA2.

“airmon-ng mon0” used to see the devices connected in the network.

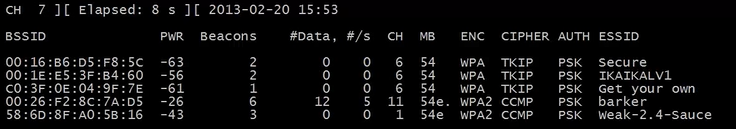


Figure 10: List of network devices – WPA2

Network ‘weak-2.4-Sauce’ is chosen for this demonstration for WPA2 encryption cracking.

The command “airodump-ng –w OURFILE –c 1 –bssid 58:6D:8F:A0:5B:16 mon0 '' is executed to write the flow of traffic into ‘OURFILE’.

Run the command “aircrack-ng –0 0 –a 58:6D:8F:A0:5B:16 mon0 '' on a new terminal without closing the one that is currently monitoring. This command sends deauthentication packets to the device.

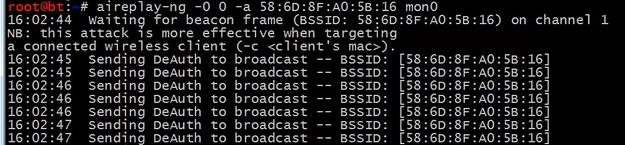


Figure 11: Sending deauthentication packets– WPA2 network

The command below “aircrack-ng OURFILE-01.cap -w/pentest/passwords/wordlists/darkc0de.lst” looks for the password encoded in the captured traffic. In the file darkc0de.lst there are the most common passwords that are generally used. This file as well as other wordlist files can be found on GitHub.

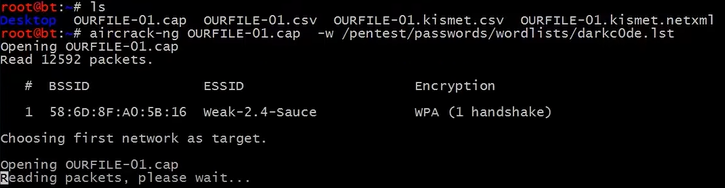


Figure 12: Running aircrack-ng for WPA2

Effectively used a dictionary brute-force attack to break a WPA2 password.



Figure 13: Successful WPA2 cracking

# 802.11 standard clients and identifying its flaws and determining how they are exploited

Working Group 11 of the IEEE LAN/MAN standards committee developed a set of wireless LAN/WLAN standards known as IEEE 802.11, also known as the Wi-Fi standard. "WEP is assumed to have been cracked recently," said Chris Rouland, director of Internet Security Systems Inc.'s X-Force vulnerability research group in Atlanta. "If you observe enough quality traffic on a WEP network, you can crack everything in about 12 hours."

According to estimates made by Newton, Massachusetts-based consultant Cahners In-Stat Group, the wireless LAN industry would grow to $2.2 billion by 2004. It is essential to determine any potential attackers' likely capabilities before analyzing the 802.11i protocol.

There are three different sorts of frames that can flow from the Link Layer of a WLAN: Management Frames, Control Frames, and Data Frames. Threats include any altering with these frames that directly or indirectly endangers data availability, confidentiality, integrity, or mutual authentication. Analysis of traffic: whether it is possible to decode full packets using recorded packets and/or knowledge of the plaintext, or whether traffic analysis methods may be utilized to obtain other valuable information.

***Message Interception:*** In message interception, an attacker has total control of the connection, the attacker can intercept a packet before the recipient. Choose to delete the packet or send it to the intended recipient after receiving it. Since the legal receiver could pick up a message before the attacker does, message interception in wireless LANs may appear challenging. A determined hacker does, however, have several possible methods for intercepting.

***Session Hijacking***: The attacker first removes a device from an active session before disguising it as it in order to make possible connections without raising the other device's awareness. In this technique, the attacker can both receive and transmit packets on behalf of the device that has been taken over. It is possible that this attack will undermine the system's authentication measures.

***DOS Attacks***: DoS attacks can be highly dangerous to WLAN networks. An attacker can disable the whole Basic Service Set (BSS) or sever connections between authorized machines. An attacker can use wireless networking features to launch DoS assaults in a variety of ways.

However, despite the WLAN being protected by 802.11i, these cyberattacks continue. Adopting a Central Manager to manage these frames particularly and spotting counterfeit frames by their aberrant behavior may be feasible. The authentication server must have additional features for this, and it must also maintain a record of the current state of all devices. This adds to the server's workload and might not be practical. Some other strategy is to initiate a 4-Way Handshake in response to Deauthentication and of disassociation frames, with the outcome revealing if the frames are real or not.

# Research Work

1. Scenario

This scenario, which will be discussed, is of a coffee shop that allows them to access the network. Based on the above research regarding the security flaws in the network the decision will be made to always use Wi-Fi Protected Access II (WPA2) to encrypt the network. After deciding to utilize the WPA2 protocol, they may also provide your customers with a login password to connect with. Sometimes the provider can direct the customers to the website to accept the terms and connection to connect the Wi-Fi in the shop. The network communication peripherals, such as wireless access points, routers, and switches, should first be physically secured. Any device with an Ethernet connection is open to intrusion by unauthorized users who can quickly plug in their own equipment and change its setup. All networking equipment must be stored in a safe place, such as a secure closet, to avoid this. In order to stop attackers from surfing and accessing your network resources and sensitive information, it is crucial to ensure that the guest network and corporate networks are strictly compartmentalized. A network firewall should be used for this purpose. To avoid rogue access points and man-in-the-middle attacks, modify the default admin passwords for all routers and switches and change the name of the SSID to a name that most consumers can recognize as being associated with the company. Merely updating the network devices' firmware. These updates often protect against newly identified vulnerabilities, which fraudsters quickly exploit (sometimes referred to as zero-day attacks). Spend some time each month checking all the gadgets for updates. Additionally, you should safeguard the users from websites that act as launching grounds for malware. By signing up for a cloud-based web filtering service, the company can simply achieve this without the requirement for extra hardware or having to bother about patch administration and installations.

1. Mitigation Techniques

*Software updates and enhancements:* As soon as updates are available, install them all. This process must be automated. Exploits could be developed very quickly after a patch is made public. Many organizations provide update services that can help with automation; just make sure you use updates sent over secure channels and test them before sending them into operation.

*Establish a formal disaster recovery plan:* A disaster recovery plan (DRP) must be established in order to successfully mitigate cyberattacks. A Contingency plan should be the priority in your strategy, followed by data safeguarding, data recovery, offshore backups, network reconfiguration, setups, and logging. Remember that a DRP should be regularly updated and evaluated because it is not a simple assignment. The entire risk mitigation plan's frequent evaluations can help to find any shortcomings.

*Investigate system breaches*: Operate as if there has been a breach, and take preemptive measures to identify, limit, and eliminate any malignant components. Research and vulnerability scan efforts should be integrated with automated technologies such as endpoint detection and response systems. By using these measures, cybersecurity defensive strategies can progress beyond simple detection approaches and toward real-time threat detection and mitigation.

*Application-aware protection can be used to segment networks*:Threat actors can disguise destructive activities and alter data by using widely used protocols that transfer data across networks. If it is determined that programs have been compromised, application-aware systems such as firewalls may impose limitations. Segregate critical networks and services first, then build network defenses to filter out unwanted traffic and enforce content restrictions..

*Restricting and managing user access:* In case malicious actors collect login information, it is recommended that the organization run the network with a zero-trust architecture. This technique only offers users account permissions when they are required. Put in place rules for safely updating passwords or automating credential management with privileged access management software. To embrace a zero-trust mentality, update your onboarding and offboarding processes as well.

1. CONCLUSION

In this assignment, WLAN network security flaws are discussed along with a demonstration of how these flaws are exploited. Particularly, Hidden SSID and MAC filtering methods. Encryptions like WEP and WPA2 are examined for efficient protection of the network. The demonstrations have proven that these encryptions can be cracked if the attackers choose to pursue to gain access to the network. Although the demonstrations were done under the legal requirements of the assignment, any hacker can find ways to break the encryption. Kali Linux is often used for such attacks as it is already embedded with tools for ethical hacking. Also, the clients of the 802.11 standards are discussed, its security flaws, and how these flaws are exploited by bad actors. Based on the analysis of all the above issues for the research portion of the assignment, a coffee shop must be set up for an optimized and secured network that can be used by the public. A detailed report of which WLAN requirements must be used and what are the mitigation techniques if something is negatively affecting the network.

*References*

1. Fadyushin, V. and Popov, A. (2016). Building a pentesting lab for wireless networks : build your own secure enterprise or home penetration testing lab to dig into the various hacking techniques. Birmingham, UK: Packt Publishing.
2. Packt Hub. (2016). Common WLAN Protection Mechanisms and their Flaws. [online] Available at: https://hub.packtpub.com/common-wlan-protection-mechanisms-and-their-flaws/amp/ [Accessed 12 Jan. 2023].
3. Lab X4 -Breaking WEP and WPA Encryption. (n.d.). [online] Available at: https://simms-teach.com/2016-fall/docs/cis76/cis76labX4.pdf [Accessed 10 Jan. 2023].
4. Kumar, S. and Dutta, K. (2016). Securing Mobile Ad Hoc Networks. International Journal of Handheld Computing Research, 7(1), pp.26–76. doi:10.4018/ijhcr.2016010103.
5. Europa.eu. (2017). An overview of the Wi-Fi WPA2 vulnerability. [online] Available at: https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability.
6. Kaur, Jaspreet. (2017). WiFi Security: WEP, WPA, and WPA2. 10.13140/RG.2.2.15707.85283.
7. Holt, Alan & Huang, Chi-Yu. (2010). 802.11 Wireless Networks Security and Analysis. 10.1007/978-1-84996-275-9.
8. N. Borisov, I. Goldberg, and D. Wagner, ìIntercepting Mobile Communications: The Insecurity of 802.11.î http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
9. William A. Arbaugh, ëAn inductive chosen plaintext attack against WEP/WEP2í. IEEE Document 802.11-01/230, May 2001.