Experimental Evaluation of Different Penetration Security Levels in Wireless Local Area Network

Ali M. Alsahlany, Zainalabdin H. Alfatlawy, and Alhassan R. Almusawy
Department of Communication Techniques Engineering, Al-Furat Al-Awsat Technical University, Al Najaf 31001, Iraq
Email: alialsahlany@atu.edu.iq; zain9797@gmail.com; alhassanmusawy@gmail.com

Abstract —WLANs use air as a medium for transferring data between users. This medium permits the hackers listening and sniffing the transferred data from away distance without the need for a real physical connection. In this paper, the threats of different security levels, such as SSID, MAC filter, and WPA II used to ensure protection of WLANs are investigated. The structure and fundamental concept of every security mechanism are analyzed and discussed. The penetration test for cryptanalysis WPA II in the PSK mode, discovering hidden SSID, and bypassing MAC filter is illustrated experimentally. The assessment process is executed using the Kali Linux platform and many other tools.

Index Terms—WLAN security, SSID, WPA/WPA II, MAC filter.

I. Introduction

One of the most important features of Wireless Local Area Networks (WLANs) is the mobility. Mobility gives users the ability to move from one place to another without wires, by sending data through the air. The data transmission through the air makes the WLANs vulnerable. Today, there are many techniques used to ensure the security of WLANs. A hidden SSID technique used to protect the WLANs by preventing the access point (AP) from broadcast the network name to clients [1]. Also, the MAC filter technique depends on the set table included the MAC addresses for the legal wireless card. Enabling this technique in the AP prevents the wireless card from access to the WLANs if its MAC address not found in the table [2]. Finally, the wireless protected access protocols such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and (WPA II) protect the WLANs through setting a secret key in the AP. Knowing the key allows anyone access to the WLAN.

There are many authors discussed different security levels of WLANs. Authors in Ref. [3,4] proved the weakness of WEP encryption practically by using the replay attack method; they are showing the possibility of knowing the WEP key by capturing 24000, 27000 initialization vectors (IVs). Using the same attack method Kumkar et al., [5] discovered 64 bits of WEP key in 15 minutes by capturing 15000 IVs. Furthermore, they cracked the key of WPA II successfully in 10 minutes using dictionary attack method. Cracking process executed experimentally with considering the point to point mode. Alsahlany [6], shown the possibility of cracking the WEP technique with key length 128 bits by capturing 5000 IVs in less than 40 seconds. The author considered already there are more than one clients connected with the AP. The program used is Airoscript Viejo and Wifiway as Operation System (OS).

Chen *et al*. [7], investigated the vulnerabilities of WPA/WPA II and showed the possibility of cracking these protocols by using a traditional dictionary attack. However, they depend on the human social factor to guess passphrase. Hidden SSID was discussed practically in Ref. [8], the obtained results showed the real name of SSID could be discovered successfully by using the Aircrack tools. Nixon *et al*. [9], found that an attacker can access to the AP that enabled the MAC filter through change its MAC address by one of the authorized clients. Tanuj *et al*. [10], mentioned that the MAC address for the AP and the clients broadcasted without encryption over WLAN and anyone can access to it easily. The authors proposed innovative method depend on using the MAC address as an authentication technique between the AP and the clients. Also, they showed that relying on this method is not suitable for providing high-level protection, but it is suitable for small coverage area.

In this paper, different security techniques such as Hidden SSID, MAC filter, and WPAII in the PSK mode will be used at the same time to protect the WLAN, the threats and vulnerabilities, which may be utilized by the assailant for hacking wireless network will be assessed theoretically and experimentally.

The arrangements of paper they are as follows. Section II describes the structure and concept of the security levels used in the evaluation process. Section III shows the software and hardware requirements. The practical penetration assessment presented in section IV. Finally, section V discusses the conclusion.

II. WLAN Secuirty Levels

A. WPA

WPA is a security protocol developed by the Wi-Fi Alliance. It became available in 2003. It is compatible with the IEEE 802.11i. The Alliance defines it for making cryptographic of data more complex. WPA works in two modes:

Manuscript received April 12, 2018; revised November 23, 2018.
Corresponding author email: alialsahlany@atu.edu.iq
doi:10.12720/jcm.13.12.723-729

- The first mode is Per-Shared Key (PSK), this mode operating in the small coverage area, it's called the personal mode. In this mode, the AP configured for having only one secret key (from 8 to 63 characters) used to authenticate clients with the AP [11].
- The second mode is Enterprise. It needs an administrator for setup authentication process with the network, each client in the network given a unique username and password for getting authentication [12, 13].

The algorithm used in the WPA is Rivest Cipher 4 (RC4). The WPA is enhanced with 128 bits Temporal Key (TK) and 48 bits TKIP Sequence Counter (TSC) for crypto-graphic data. Message Integrity Check (MIC) algorithm with length 64 bits used for verifying integrity of the transmitting data [9], [13]. Fig. 1 illustrates the encryption process of the WPA. At first, the TSC, MAC destination address, and TK are entered into the key mixing, which operates as a hash function to change places of bytes at several times based on IV. The output of key mixing with length 128 bits will become an input to the RC4 algorithm to produce the keystream. The data frame and MIC will process by Michael algorithm; the result of Michael algorithm is a MAC Protocol Data Unit (MPDU). Finally, the MPDU and the Integrity Check Value (ICV) mixed with the keystream using an XOR function to produce the cipher text.

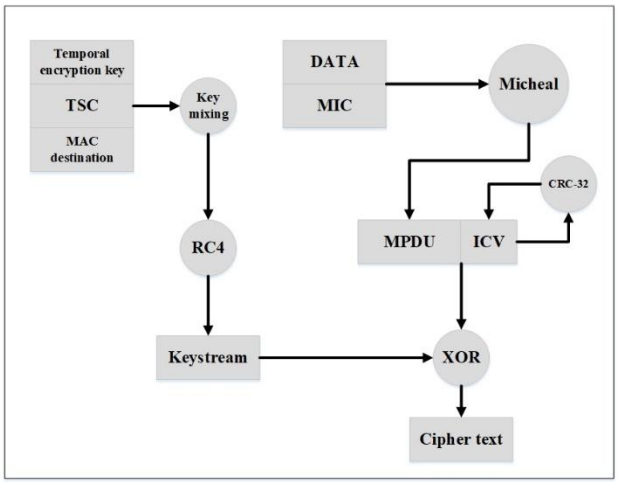

Fig. 1. WPA encryption process.

B. WPA II

The newest version of WPA appeared in 2004 by Alliance called WPA II. It replaced the previous security protocols WEP and WPA. The WPA II uses the Advanced Encryption Standard Counter Mode CBC-MAC Protocol (AES-CCMP) for encryption and integrity instead of the RC4 algorithm in the WPA. However, WPAII used TKIP for compatibility with old APs [9, 12, 13]. The cryptographic algorithm used in the WPA II is AES-CCMP, it works in the two modes: counter mode for providing more security against the eavesdropping attack, and the CBC-MAC Protocol mode, for ensuring the integrity and preventing repeat using the same cipher text. The procedure of encrypted data by using the WPA II presented in Fig. 2. At first, the plaintext, TK, and Additional Authentication Data (AAD) taken from the MAC header are entering to the AES-CCMP encryption algorithm for protecting the frame from change. The Packet Number (PN) and the MAC header are entered to build a Nonce, as a portion of AES-CCMP encryption process, CCMP enhanced by adding a PN to protect the network against a replay attack. Finally, there are two outputs, the encrypted data, and encrypted MIC.

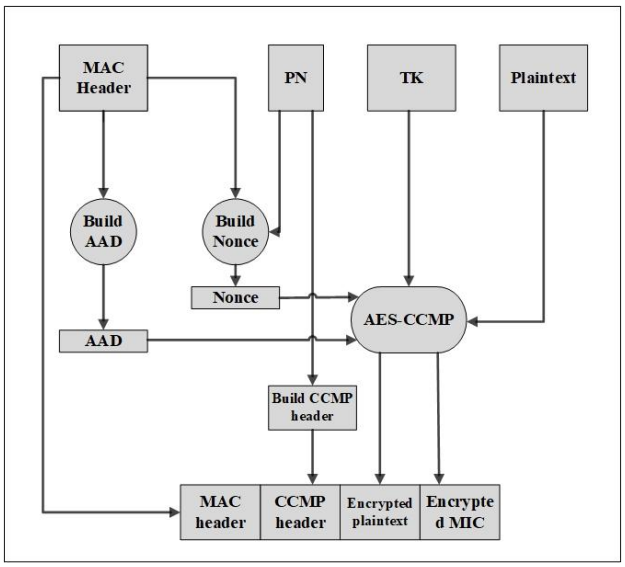

Fig. 2. WPA II encryption process.

C. Four-Way Handshaking

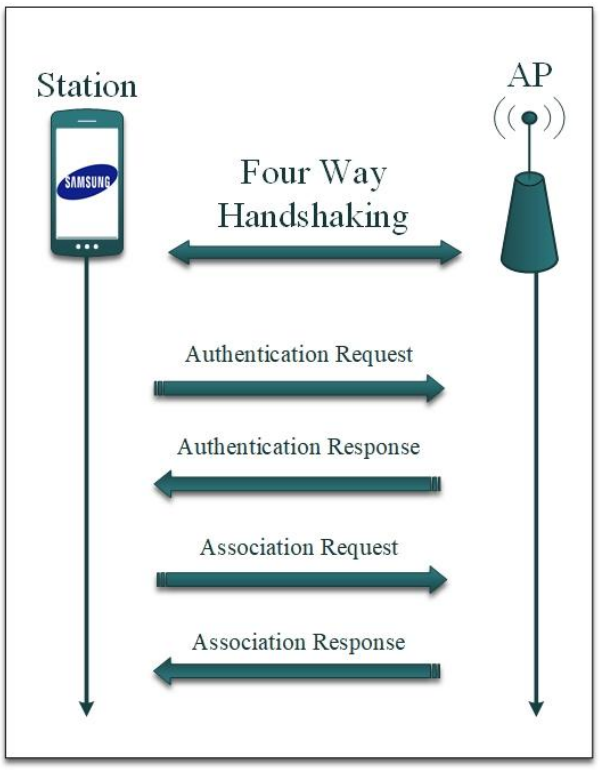

Fig. 3. Authentication and association process.

In the WLANs users connected to the AP through doing authentication and association process as illustrated in Fig. 3. After that, A Four-Way Handshaking (FWH) process executed between the AP and the user using Extensible Authentication Protocol Over Lan (EAPOL) to prove they know the PSK without revelation [8, 14, 15]. This process is explained in Fig. 4. Firstly, the client and the AP derive Pair Master Key (PMK) from the PSK, then the AP generates a random number (ANonce) and sent to the client. The client will derive a Pairwise Transient Key (PTK) and sends a message containing a random number (SNonce) to the AP. The AP drives PTK and generates a Group Temporal Key (GTK) and resends it to the client, GTK used for protecting a broadcast data. Finally, the client sends a message for a successful connection.

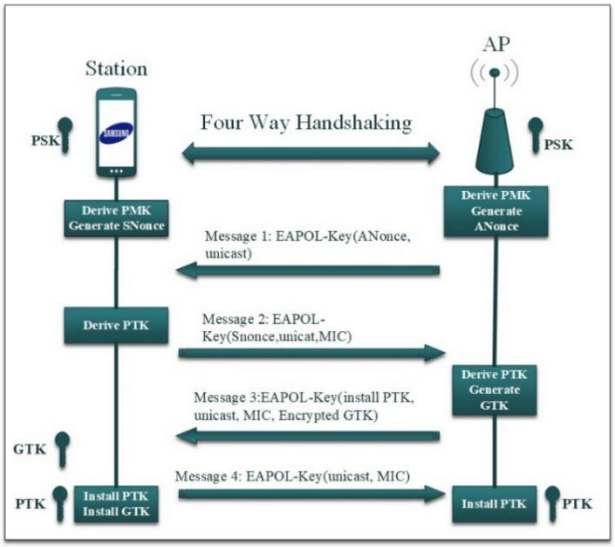

Fig. 4. Four way handshaking process in WPA II the PSK mode.

D. MAC Address Filtering

Every network equipment has a unique physical address called Media Access Control (MAC) address. The MAC address filter is one of the security mechanism used by IEEE 802.11 standards to ensure the protection of WLANs. In this mechanism, the AP configured with a table contain the authorized MAC addresses, when the AP find matching between the MAC addresses, send in the authentication response frame by the clients and one of the addresses in the table, it will accept the request otherwise it drops the authentication request [8]. However, this mechanism is vulnerable to attack using different methods. Hackers can easily find out the list of authorized MAC addresses and change MAC address of the assailant card to match with one of addresses found in the table and overrun this filter [16].

E. Hidden Service Set Identifier

Every AP in the WLANs has the network name called the SSID. The SSID is 1 to 32 alphanumeric characters string broadcasting by the AP. The purpose of the SSID in the WLANs is identifying the membership to the AP [4]. The beacon frame is one of IEEE802.11 management frames; it's broadcast periodically by the AP to every client in its coverage area. The beacon frame has information about the AP including the WLAN name (SSID) [8]. Fig. 5 shows the beacon frame structure. Vendors find that preventing the AP from broadcasting the SSID gives more privacy to the WLAN, this security mechanism called Hidden-SSID [17], [19].

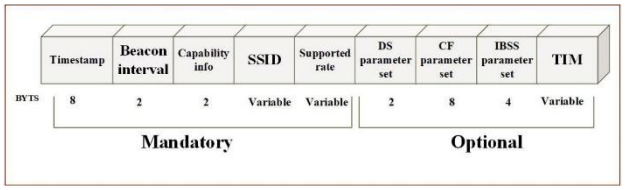

Fig. 5. The structure of the beacon frame.

III. The Environment of Wireless Network Penetration Testing

With respect to WLANs security levels aforementioned in the previous related sections, many methods used for assessing the threats and countermeasures of these levels are executed in the laboratory of wireless network penetration testing. The hardware devices used to set up the laboratory are mentioned in Table I.

Table I: Hardware Used in The Laboratory for Wireless Network Penetration Testing.

Hardware device	Specification
Router	- TP-LINK TL-WR940N, - IEEE802.11n, g, b, a compatible. - MAC (E8: 94: F6: E2: 06: 86).
Assailant device	- HP laptop (Elite Book 84700p), - core i5 CPU 2.8 GHZ. - RAM 8 GB.
Authorize client	- Samsung Mobile as a client device. - MAC (48: 5A: 3F: 4B: 0C: 9A).
Wireless card	- ALFA (AWUS036NHA). - IEEE802.11 b/g/n compatible. - MAC (00: C0: CA: 92: 69: 56) - Transfer rate 150 Mbps - Antenna with 5dbi - Sensitivity -91dbm

Table II: Information About The Target AP.

The type of characters used to form the passphrases	Long of passphrases
ESSID (SSID)	"Wireless-Network Lab", hidden SSID.
MAC Filter	Enabled on Mobile client (48: 5A: 3F : 4B : 0C : 9A).
Encryption	WPA2 PSK mode, passphrase: 46789921.
Cipher	AES

On another side, the software packages and tools such as ("airodump-ng", and "aircrack-ng") are used for listening, sniffing, and capturing the WLAN traffic. "mac-changer" tool, and "aireplay-ng" used for spoofing the AP and authorized clients. All tools are downloaded and installed on the assailant device (HP laptop), which

used Kali Linux as a penetration test OS. The client machine (Samsung mobile) knowing all tips about the target network. The specifications of WLAN are listed in Table II. The client device configured with Android KitKat version 4.4.2 OS. The Android de-vice connected to the Internet via the AP. Fig. 6 describes the laboratory environment used in the penetration testing process.

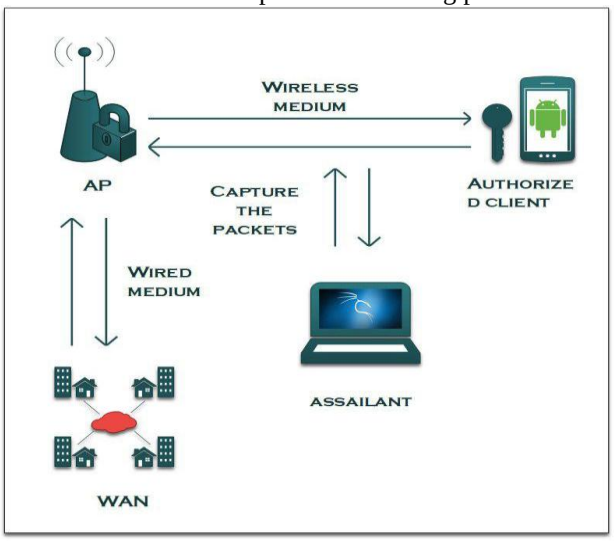

Fig. 6. The environment of wireless network penetration testing.

IV. The Penetration Test Procedure

In our proposed experiment there are three security levels are used (Hidden SSID, MAC Filtering, and WPA II) together to secure the target WLAN with SSID "Wireless-Network Lab.". The assessment of protection and the extraordinary methods used by the assailant to access the target network through crack these levels are shown in this section. At first, discovering the hidden network name. Secondly, spoofing the AP by changing the MAC address of the HP laptop to be identical to one of the authorized addresses. Finally, apply many cracking methods to find the passphrase of WPA II.

A. Discovery Hidden SSID

For discovering hidden SSID a probe request packet sent from the user to the AP must be captured and analyzed. This packet contains the SSID of the wireless network and sends from the authorized clients (Samsung mobile) to associate with the AP. There are two ways of capturing: wait for one of an authorized client starts the association process with the AP or cut service from a user connected previously and enforce him to re-associate. This operation is done practically by using "aireplay-ng" tool. For using this tool, the assailant (HP laptop) must convert the ALFA card from the mange mode to the monitor mode. Monitor mode enables the wireless card to inject and capture packets without having a connection to the AP. The "airmon-ng" tool used for converting as shown Fig. 7. Scanning and capturing packet for the target network done by using "airodump-ng" tool as shown Fig. 8. After that, assailant enforces the client to re-associate with the network by disconnecting it using "aireplay-ng" tool as shown in Fig. 9. It spoofs the AP by disconnecting the Samsung mobile out of the network through sending five de-authentication frame requests to the AP. After that, the Samsung mobile try reconnects with the AP by sending a beacon frame. Finally, the HP laptop catches the probe request frame which contains the SSID of the target AP. Fig. 10 appears the real name "Wireless-Network Lab." on "airodump-ng" terminal.

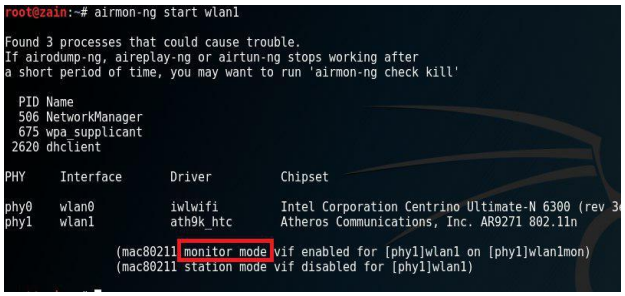

Fig. 7. Turning the ALFA card into the monitor mode.

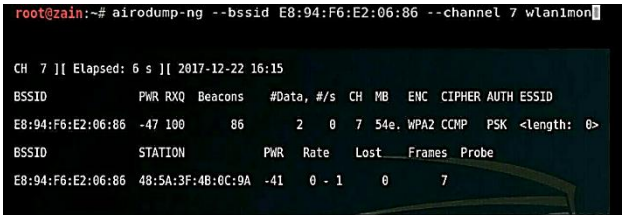

Fig. 8. Capturing the packets of the target WLAN.

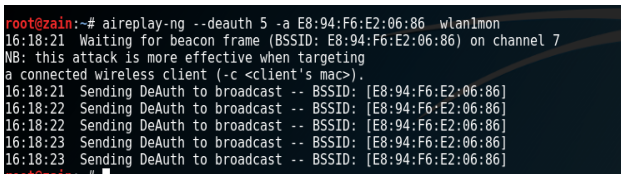

Fig. 9. Force the client to re-associate with target AP.

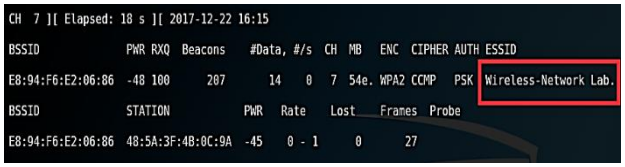

Fig. 10. Discover hidden SSID of the target AP.

B. Bypassing MAC Address Filtering

The next step of breakthrough the target AP is bypassing the MAC fitter security level. After executing "airodump-ng" important information about the Samsung mobile and the AP such as network name (SSID), MAC address of the AP, list of authorized MAC addresses, encryption type, and channel are getting. For spoofing the AP and passing MAC filter, we will change the MAC address of the ALFA card to one of the authorized MAC addresses. "macchanger" tool used for executing this attack as shown in Fig. 11. "macchanger" is a GNU/Linux utility for viewing and manipulating the MAC address for the wireless network interfacing card (WNIC).

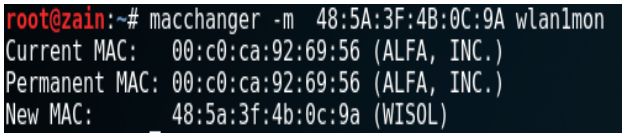

Fig. 11. Change MAC address of WINC.

C. Breaking WPA II Encryption Protocol

In this subsection, the methods used by the assailant to bypass the WPA/WPA II security levels will be described. The assailant can cryptanalysis the WPA/WPA II in the PSK mode by implementing the brute force attack, the basic concept of this attack is trying many passphrases until finding the correct one. The assailant utilizes this attack in two ways: Dictionary attack and Reaver attack.

D. Dictionary Attack

Every This type of attack depends on creating a dictionary by the assailant contain many passphrases. For easy remember passphrase client usually choice a simple passphrase to configure a security key in the AP such as birthdays, mobile phone, family names, and so on. By considering the social human factors, the assailant generates a dictionary contains expected passphrase, which may be used by the authorized client [18]. All the passphrases construct from different characters such as numbers, small letters, capital letters, and special characters (i.e. @, #, $, %, &, …). The number of passphrases generated in the dictionary file can be calculated as depicted in Equation (1).

$$m = n^l \quad (1)$$

where m refers to the number passphrases, n represents the number of alphanumeric, and l indicates the length of the passphrase.

The maximum size of the dictionary file in the byte can be calculated as demonstrated in Equation (2).

$$s = mx8 \quad (2)$$

where s represents the size of the dictionary file in bytes.

"crunch" tool used for creating a dictionary file and set standard characters. Fig. 12 shows creating the dictionary file "wordlist" consisted from 108 passphrases constructed by using numbers only. After creating the dictionary file, the FWH packets captured and saved on the hard disk of the HP laptop under the file name "targetAP." The assailant utilizes the important packets found in the "targetAP" file such as ANonce, SNonce, and PTK for creating a PTK identical to the PTK packet that captured in the "targetAP". The tool used for capturing the FWH packets is "airodump-ng" as shown in Fig 13. Dictionary attack executed using "aircrack-ng" for getting real password successfully as presented in Fig. 14. In our experiment, the amount of size required to save generated passphrases is 858 MB. Also, the total time required for exhausting all attempts to find the matching between passphrase extracting from the FWH packets and the "targetAP" file is 49 minutes. This amount of time obtained by using the HP laptop with processor 2.8GHz. Using laptops with high specification leads to minimize the time required for the matching process. The number of passphrases, the size needed to save generated passphrases depends on different characters, and the time required for matching all passphrases in the dictionary file is shown in Table III.

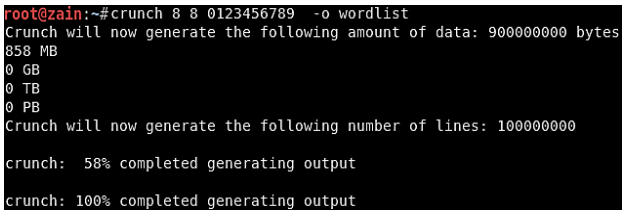

Fig. 12. The process of creating wordlist dictionary.

Fig. 13. The process of getting the WPA handshake.

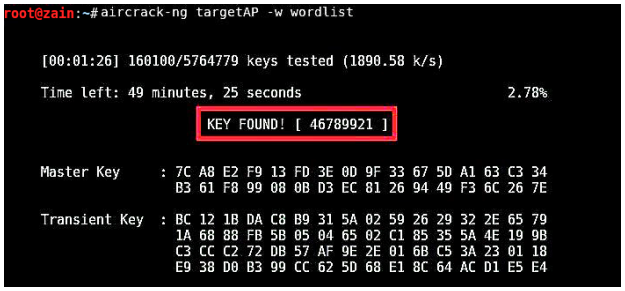

Fig. 14. The execution of "aircrack-ng" tool and discover the passphrase of target AP successfully.

TABLE III: EXPERIMENTAL RESULTS TO CALCULATE NUMBER, SIZE, PATTERN, AND TIME REQUIRED FOR THE MATCHING PROCESS OF DIFFERENT GENERATED DICTIONARY FILE.

The type of characters used to form the passphrases	Long of passphrases	The maximum number of passphrases generated	The maximum time required for testing all the generated passphrases	Size of the dictionary file in Byte
Birthday pattern	12 characters (19**19**19**)	970,299	17.38 minutes	8 MB
Phone numbers	11 characters (07*********)	10^9 passphrase	298 hours	8 GB
Decimal numbers	10 characters	10^{10} passphrase	124 days	80 GB
26 English letters + 10 numbers	13 characters	$360 * 10^{12}$ passphrase	12445 years	2880 TB
52 English letters (small and capital) + Decimal numbers	15 characters	$62 * 10^{15}$	2113986 years	496 PB

E. Reaver Attack

The Reaver attack method used to discover the Personal Identification Number (PIN) of the AP by utilizing the vulnerabilities in the WPS protocol. The Wi-Fi Protected Setup (WPS) is a protocol created by Wi-Fi Alliance organization in 2006 for the users that does not have any acknowledgment of how to configure password of the AP. This protocol allows client for connecting to the WLAN by using the default password provided by the manufacturer, which setting from eight numbers instead WPAII passphrase. The assailant executes this attack by using "reaver" tool through trying insertion all the possible PIN (8-digits) for registration with the AP until connected. Also, the assailant determines the network that activates the WPS protocol in his coverage area by using "wash" tool as presented in Fig. 15.

Fig. 16 shows the execution of "reaver" tool. The time required for exhausting all attempts take in our experiment 6 hours. The results of PIN discovered shown in Fig. 17.

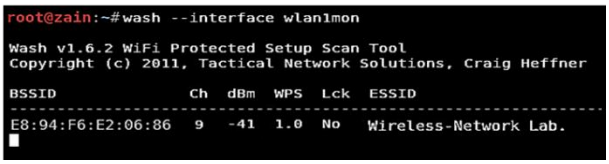

Fig. 15. The execution of the "wash" tool to determine the network that activates WPS protocols.

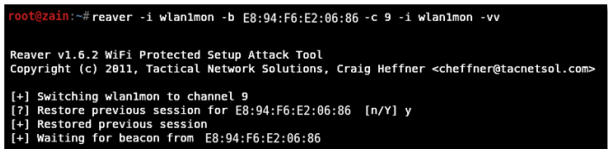

Fig. 16. The execution of the "reaver" tool for discovering the PIN.

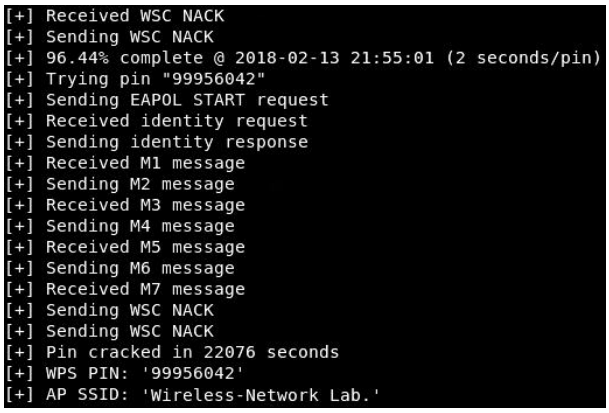

Fig. 17. Appear the PIN of the target AP.

V. Conclusions

In this paper, the vulnerability points for different WLANs security protocols are proved experimentally. Kali Linux and different penetration tools used to assess the security strength of Hidden SSID, MAC filtering, and WAP2. Results showed that the real name of Hidden SSID could be easily discovered, by capturing 27 frames only and through 18 seconds. MAC filter is not a hard obstacle for the attackers because the MAC addresses of the clients and the AP already announced by the beacon frame and the assailant can change it to another one by using "macchanger" tool efficiently. The WPA II proved is a weakness against the brute force attack and human social factors, the WPA II can be cracked after 1.24 minutes. The WPS protocol is one of the hiatuses which made cracking WLANs is very easy when it be activated. The maximum required time to recover the PIN code by using this method is 10 hours.

Based on penetration assessment of this paper and to improve the security of the WLANs, it is better to configure the security mode of the AP by activating all security levels (hidden SSID, MAC address filter, and WPA II AES encryption) at the same time. Also, turn off the WPS protocol to prevent an assailant from utilizing weak points of this protocol and discover default PIN number. In addition, used complex WPA II passphrases through compound length more than 16 alphanumeric and including small letters, capital letters, special characters, numbers, avoid using consecutive numbers and letters. Also, change passphrases periodically and reduce the coverage area of the broadcasting signal as possible by controlling the transmitted power to prevent assailants from utilizing the vulnerabilities and access to the WLANs. Finally, working on detecting a new security level to overcome all threats to ensure protection.

References

[1] T. Aziz, M. R. A. Razak, and N. E. A. Ghani, "The performance of different IEEE802.11 security protocol standard on 2.4 Ghz and 5GHz WLAN networks," in *Proc. International Conference on Engineering Technology and Technopreneurship*, pp. 1-7, 2017.

[2] A. P. U. Siahaan, "A review of IP and MAC address filtering in wireless network security," *International Journal of Scientific Research in Science and Technology*, vol. 3, pp. 470-473, 2017.

[3] S. L. Wang, J. Wang, C. Feng, and Z. P. Pan, "Wireless network penetration testing and security auditing," in *Proc. ITM Web of Conferences*, 2016, pp. 03001.

[4] S. S. Tung, N. N. Ahmad, and T. K. Geok, "Wireless LAN security: Securing your access point," *IJCSNS*, vol. 6, pp. 173, 2006.

[5] V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta, and S. Shrawne, "Vulnerabilities of wireless security protocols (WEP and WPA2)," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol. 1, pp. 34-38, 2012.

[6] A. M. Alsahlany, "Experimental analysis of WLAN security weakness by cracking 64 & 128 bit WEP key," *The Islamic College University Journal*, vol. 9, pp. 165-176, 2012.

[7] C. M. Chen and T. H. Chang, "The cryptanalysis of WPA & WPA2 in the rule-based brute force attack, an Advanced and efficient method," in *Proc. Information Security Asia Joint Conference*, 2015, pp. 37-41.

[8] V. Chopra and S. Mehra, "Cracking and hardening hidden SSID mechanism in 802.11 using PYTHON," *International Journal of Computer Applications*, vol. 106, pp. 51-55, 2014.

[9] S. Nixon and Y. Haile, "Analyzing vulnerabilities on WLAN security protocols and enhance its security by using pseudo random MAC address," *International Journal of Emerging Trends & Technology in Computer Science*, vol. 6, pp. 293-300, 2017.
[10] S. Tiwari, T. Tiwari, and T. Tiwari, "A secured MAC address based login system," *European Journal of Electrical Engineering and Computer Science*, vol. 2, pp. 11, 2018.
[11] O. Nakhila, A. Attiah, Y. Jinz, and C. Zoux, "Parallel active dictionary attack on WPA2-psk wi-fi networks," in *Proc. Military Communications Conference, MILCOM*, pp. 665-670.
[12] S. P. Prastavana and P. Suraiya, "Wireless security using Wi-Fi protected access 2 (WPA2)," *International Journal of Scientific Engineering and Applied Science (IJSEAS)*, pp. 2395-3470, 2016.
[13] O. Nakhila and C. Zou, "Parallel active dictionary attack on IEEE 802.11 enterprise networks," in *Proc. Military Communications Conference*, 2016, pp. 265-270.
[14] V. Priyadharshini and K. Kuppusamy, "Prevention of DDOS attacks using new cracking algorithm," *International Journal of Engineering Research and Applications*, vol. 2, pp. 2263-2267, 2012.
[15] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in WPA2," in *Proc. ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1313-1328.
[16] C. Liu and J. Yu, "A solution to WLAN authentication and association DoS attacks," *IAENG International Journal of Computer Science*, vol. 34, 2007.
[17] P. S. Ambavkar, P. U. Patil, and P. K. Swamy, "Exploitation of WPA authentication," *IOSR Journal of Engineering (IOSRJEN)*, vol. 2, pp. 320-324, 2012.
[18] A. Garg, "A novel approach to secure WEP by introducing an additional layer over RC4," in *Proc. Computing for Sustainable Global Development (INDIACom) Conference*, 2016, pp. 551-555.
[19] A. M. Alsahlany, A. R. Almusawy, and Z. H. Alfatlawy, "Risk analysis of a fake access point attack against Wi-Fi network" *International Journal of Scientific & Engineering Research*, vol. 9, pp. 322-326, 2018.

Ali M. Alsahlany was born in Najaf, Iraq, in 1984. He received the B.Sc. degree from the Al-Furat Al-Awsat Technical University, in 2006, in communication engineering, and received master degree from the University of Basrah, Basrah, in 2012, in electrical engineering. He is lecturer in Communication Techniques Engineering, Engineering Technical College/Najaf. His research interests include wireless communication and security.

Zainalabdin H. Alfatlawy has got BSc in Communication Engineering from Al-Furat Al-Awsat Technical University, Iraq. He is interested in the field of wireless communication and ethical hacking

Alhassan R. Almusawy has got BSc in Communication Engineering from Al-Furat Al-Awsat Technical University, Iraq. He is interested in the field of wireless communication and ethical hacking.