Hindawi
Complexity
Volume 2021, Article ID 5570001, 8 pages
https://doi.org/10.1155/2021/5570001

Research Article

Research on WiFi Penetration Testing with Kali Linux

He-Jun Lu[1] **and Yang Yu**[2]

[1]*The School of Big Data and Artificial Intelligence, Anhui Xinhua University, Hefei, Anhui 230088, China*
[2]*Science and Technology on Reactor System Design Technology Labortory, Nuclear Power Institute of China, Chengdu, Sichuan 610213, China*

Correspondence should be addressed to He-Jun Lu; luhejun@axhu.edu.cn

Received 19 January 2021; Revised 31 January 2021; Accepted 13 February 2021; Published 27 February 2021

Academic Editor: M. Irfan Uddin

Aiming at the vulnerability of wireless network, this paper proposed a method of WiFi penetration testing based on Kali Linux which is divided into four stages: preparation, information collection, simulation attack, and reporting. By using the methods of monitoring, scanning, capturing, data analysis, password cracking, fake wireless access point spoofing, and other methods, the WiFi network penetration testing with Kali Linux is processed in the simulation environment. The experimental results show that the method of WiFi network penetration testing with Kali Linux has a good effect on improving the security evaluation of WiFi network.

1. Introduction

With the rapid development and wide application of wireless network technology, the problem of information security becomes more and more important. Especially in recent years, with the wide use of smart terminals such as smartphones, which bring great convenience to our daily life, the information security problems arising therefrom are also increasing [1, 2]. More and more researchers pay attention to networks' security and calculations [3, 4]. Wireless Fidelity (WiFi) is a current wireless network model based on the IEEE 802.11 standard [5]. The Wireless network itself has some vulnerabilities. It uses radio waves to transmit signals and needs to establish a connection before it can be used; therefore, the channel is more likely to be monitored and to be attacked by intermediaries [6, 7]. The management frame, control frame, and data frame of the wireless network frame are not encrypted, the information is easy to read, and the integrity of the management frame and control frame is not protected. Lack of integrity protection for management frame and control frame makes injection attack and replay attack easy to occur. At the same time, there are some flaws in the open authentication mechanism and the shared key authentication mechanism. In the open authentication mechanism, the client can connect to the wireless network without authentication. In the mechanism of shared key authentication, if the whole authentication process is monitored, it is easy to bypass the authentication, which makes the WiFi network easy to be broken. Aiming at the vulnerability of WiFi network, this paper proposes a WiFi penetration test method based on Kali Linux, which uses the methods of monitoring, sniffing, capturing, data analysis, WiFi password cracking, pseudo-wireless access point spoofing, and so forth to enhance the security of WiFi networks.

The penetration test [8] is a malicious attack on a target system and gain access control by simulating the techniques and methods of an attacker with the legal authorization of the client; it is a test method for evaluating security control measures of information systems. There are many methods of penetration testing, and the corresponding methods can be chosen according to different requirements, common methodologies including the Open Source Security Testing Manual [9], the Penetration Testing Execution Standard [10], and the Open Web Application Security Project [11, 12]. Penetration testing includes Black Box Testing, White Box Testing, and Gray Box Testing [13]. Penetration testing is generally divided into the detection, scanning, vulnerability assessment, vulnerability utilization, maintenance access, reporting phase, and so on [14, 15].

2. Kali Linux

Kali Linux is an open-source comprehensive penetration testing platform that includes various toolsets for penetration testing, as shown in Table 1.

According to the characteristics of the vulnerability of the WiFi network, the penetration test of the WiFi network under Kali Linux is divided into four stages: preparation, information gathering, simulation attack, and reporting, as shown in Figure 1.

2.1. Preparation Stage. The preparation stage is mainly to determine the scope of the penetration test, determine the boundaries, obtain the authorization of the customer, obtain the legality of the penetration test, plan the penetration test to be carried out, and evaluate the workload of the penetration test.

2.2. Information Gathering Stage. The information gathering phase is mainly to collect information on wireless networks and devices within the scope of penetration testing; list the wireless network, network devices, and device list information connected to the target network in the penetration test range; draw the network topology; determine the network coverage; and find out the possible attack sites within the range.

2.3. Simulated Attack Phase. The simulated attack phase is mainly to verify the possible vulnerabilities with performing a simulated attack. This includes attacks against WiFi encryption, infrastructure, and clients.

The main method of the WiFi encryption mode attack is to determine the encryption mode of the target WiFi network firstly, analyze the vulnerability of the encryption mode, select the corresponding password cracking method, crack the WiFi password, and test whether the password is secure.

An attack on a target infrastructure is a penetration test of a licensed target infrastructure. Further penetration testing of the target infrastructure is performed by means of port scanning, viewing service processes, enumerating open services, and finding and exploiting vulnerabilities.

Client attacks can be performed by the method of establishing a pseudo-AP, connecting the client to the pseudo-AP, and performing penetration testing on the client.

2.4. Reporting Phase. The test report is the final phase of the WiFi penetration test. After the test is completed, it is necessary to analyze the vulnerabilities discovered during the penetration test and how to report to the customer, in order to facilitate the customer to improve security awareness, repair security problems, and improve the overall security level. The test report should mainly include detailed penetration testing procedures, technical method routes, results of penetration testing findings, and recommendations.

Table 1: Kali Linux toolset.

Serial number	Toolset
1	Information gathering
2	Vulnerability analysis
3	Web application analysis
4	Database assessment
5	Password attacks
6	Wireless attacks
7	Reverse engineering
8	Exploitation tools
9	Sniffing and spoofing
10	Postexploitation
11	Forensics
12	Reporting tools
13	Social engineering tools

3. The Vulnerability Analysis of WiFi Network

WiFi access point (AP) broadcasts its information to the environment via radio waves. In order to be able to access all the data flowing through the test site, the penetration tester needs a network card that supports a promiscuous mode of operation before the penetration test begins, a promiscuous mode network card can read all the data that flows through it, regardless of whether the destination address is it or not. In order to monitor the network, we need to set it to monitor mode and then scan the target network to get the basic information of the target network, including the number of AP, working channel, signal intensity, and client basic information. Record the Media Access Control (MAC) of the target AP and the MAC address of the client to prepare for monitoring the target network. Also, find the hidden Service Set Identifier (SSID) and the name of the wireless router. Typically, the AP broadcasts its own SSID, but for security purposes, by hiding the SSID to protect the WiFi network, only clients that know the SSID can connect to the AP. However, a hidden SSID does not really protect the WiFi network. When legitimate clients connect to the AP, they exchange authentication information that contains SSID information, which is not encrypted. By extracting the SSID, penetration tests are conducted on WiFi networks with hidden SSID. Some AP turned on the MAC address filter function, only the client with a legitimate MAC can log on to the AP. The purpose of logging client MAC is to solve the problem of MAC filtering protection. Through MAC address filtering, only the legitimate MAC client can establish a connection with the AP, so that the attacker cannot connect to the WiFi network, thus protecting the WiFi network. Since the MAC information is not encrypted, the AP is duped by sniffing the legitimate MAC and then logging in disguised as the legitimate MAC. After obtaining valid information of the target network, monitoring of the specific target network can be implemented. After the valid data packet is captured in the listening mode and the modification, the attack is reinjected. It can also analyze and crack by listening to the target network and grabbing the valid data of the target AP.

At present, the main authentication encryption modes of WiFi networks are WiFi Protected Setup (WPS)

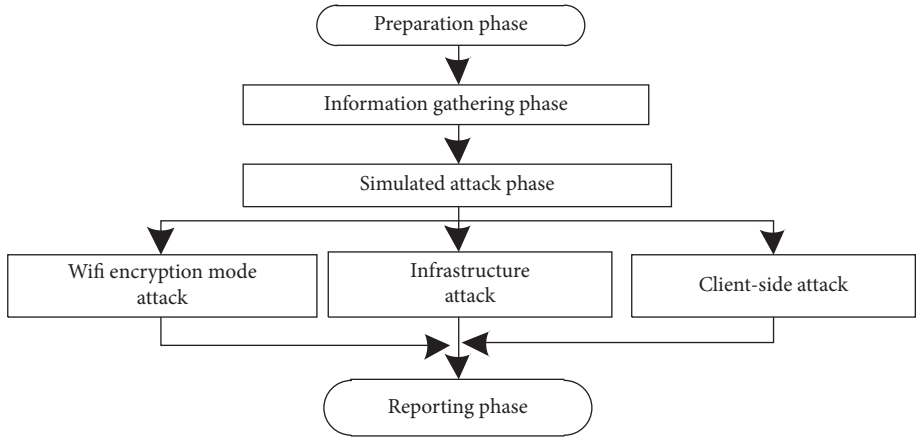

Figure 1: WiFi penetration test process.

encryption mode, Wired Equivalent Privacy (WEP) encryption mode, and WiFi Protected Access (WPA) encryption mode.

Password cracking needs to analyze the encryption mode adopted by the target network and then take the corresponding cracking method. For example, to break the WEP password, we need to grab a large amount of data between the client and the AP, to analyze and calculate. When we break the WPA encryption, we need to grab the four handshake protocol packets between the valid client and the AP and then analyze and calculate access codes.

3.1. The Vulnerability Analysis of WPS Encryption. The WPS Encryption of the wireless network makes the process simple, by entering the PIN code or pushing the Push Button Configuration (PBC) to access, and some routers refer to WPS as Quick Secure Setup (QSS). The new device joins the wireless network by entering the PIN code or pressing the PBC button. WPS initiates the process of information exchange between the device and the registry. The registry issues an authorized network certificate for the device joining the wireless network, and the device completes mutual recognition. There are certain security vulnerabilities in the WPS protocol [16]. The PIN code authentication mechanism is vulnerable. In the WPS WiFi encryption mode, the PIN code is the only authentication method for access between devices. There is no other identification requirement, which provides a possibility for brute force cracking. The PIN itself is composed of 8-bit decimal numbers between 0 and 9, only 100 million possible combinations. In fact, the 8^{th} bit of the PIN code is the check bit, and just figuring out the first 7 bits can crack PIN code, only 10 million possibilities, so it is easy to crack with violence. For security reasons, many new wireless network cards no longer support the WPS protocol. However, most of the AP currently in use has not been updated in a timely manner, leaving WPS open by default. It is a common penetration test method to brute crack pin code by using the PIN verification mechanism vulnerabilities, crack WPS encryption mode, and crack WEP encryption or WPA encryption through known PIN code.

3.2. The Vulnerability Analysis of WEP Encryption. The WEP protocol adopts RC4 stream encryption technology, and WEP encryption uses the RC4 algorithm to generate a pseudorandom sequence stream of the initialization vector and the key sequence to perform XOR encryption on the plaintext and the check code and then send the initialization vector and the generated ciphertext. The principle of the WEP encryption process is shown in Figure 2.

The receiver decrypts the ciphertext by using the same pseudorandom sequence to perform an exclusive XOR operation on the ciphertext to obtain plaintext. WEP encryption has security vulnerabilities [17]. WEP uses XOR encryption. When the plaintext and ciphertext are known, the pseudorandom sequence stream can be calculated by XOR operation, which can be used to encrypt other data to deceive the AP without knowing the real key. Cracking WEP encryption takes advantage of the repeated use of short initialization vectors and the vulnerability of RC4 itself.

WEP encryption initialization vectors are transmitted in plaintext and are easily accessible and reusable. When enough data packets are captured and XOR is performed in the first-byte header information with the ciphertext, some fragments of pseudorandom sequence stream can be obtained. When enough initialization vectors and ciphers are captured, WEP ciphers can be analyzed and calculated.

The key to cracking WEP code is to capture a large number of data packets. In this paper, a large number of data packets are captured by means of an ARP attack. The captured data packets are calculated by the above-mentioned calculation method, and the target network of WEP encryption is penetrated and creaked.

3.3. The Vulnerability Analysis of WPA Encryption. WPA has improved based on WEP and is a widely used wireless encryption mode. It is divided into WPA and WPA2. WPA/WPA2 encryption also has certain vulnerabilities [18, 19]. WPA is mainly encrypted by the TKIP algorithm. WPA2 is encrypted by the AES-CCMP algorithm with higher strength. At present, the attack on WPA/WPA2 is mainly by grabbing four handshake packets and attacking them with a dictionary attack. If you have a good dictionary, you can

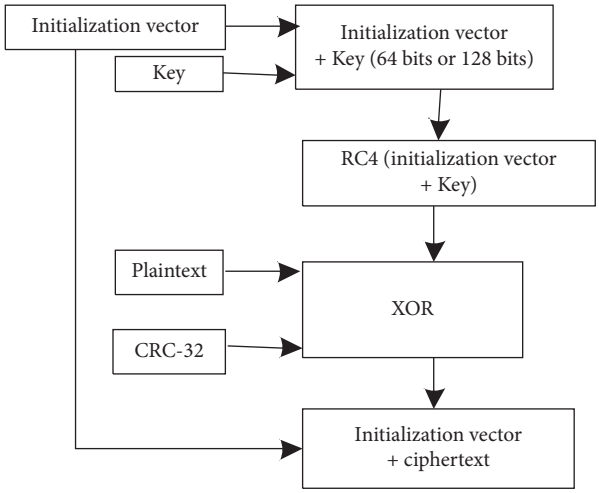

Figure 2: WEP encryption principle.

break the password by force, or you can use WPS to turn on the function and exhaust each other's PIN codes to crack the WPA code.

The main infiltration process is as follows: firstly, the wireless network card listening mode is turned on, the target wireless network is scanned through the listening port, the target network information is obtained, the client and the AP are reconnected through the offline attack, and the four-way handshake data packet between the AP and the client is captured. The captured packet is subjected to a dictionary attack to crack WPA/WPA2 encryption to obtain a password. The key to the success of WPA/WPA2 encryption penetration is the ability to capture valid handshake packets and the quality of the dictionary.

4. Methodology

The main technical methods of Kali Linux WiFi penetration test include setting wireless network card monitoring mode, scanning network, collecting target network information, monitoring target network, cracking the WiFi password, injecting packets or capturing packets, offline attack, and fake AP spoofing. The main technical methods are as shown in Figure 3.

5. Experiments and Results

The experimental environment topology of WiFi penetration testing with Kali Linux is shown in Figure 4. It consists of a wireless router, a physical host, a virtual attack machine (VM Kali Linux attack machine), a USB wireless network card, a pseudo-AP constructed by a wireless card, and two mobile intelligent terminals.

The Kali Linux attacker uses VMware virtualization technology. The host uses Intel Core i7-6700HQ 2.6 GHz 8-core processor, 16G RAM, 128G SSD + 1 TB mechanical hard disk. The virtual attack machine is Kali Linux. The pseudo-AP is built with the extension N82 USB wireless network card. The wireless access point uses a brand of wireless router, and the mobile intelligent terminal uses a brand of smartphone.

5.1. Information Gathering. When the wireless network card is set to the listening mode, it can capture all the data packets that the network card can receive. By running the command of the airudump-ng the information about the nearby wireless AP and the connected client can be get. Here, other AP network information is masked, and the part of information of the AP (testwifi) used in the experiment is given, as shown in Figure 5. Some important information, such as the physical address, user name, encryption mode, and channel of the target AP, is recorded, and at the same time, the MAC address and other information of the connected client can be obtained.

Kismet can also be used in Kali Linux to scan the wireless network and save the captured packets to a file.

The information obtained by using the kismet scan target WiFi is as shown in Figure 6. The information such as the physical address of the target AP and the MAC information of the client is recorded, which provides support for pseudo-AP attacks and offline attacks. If the target router uses MAC address filtering, even when the password is cracked, the login cannot be performed. You can use the obtained MAC address to fake client's MAC address to establish a connection with the router and spoof it.

5.2. Password Cracking. In order to better develop the penetration test and crack the wireless network password, it is necessary to build a powerful dictionary and have a good dictionary, which will bring convenience to the cracking work. The experiment in this article is to create a Brute Force Dictionary "myword. txt" by using Crunch. Brute Force Dictionary will take up a lot of disk space. For example, it will produce 5, 925, 787, and 425 GB file size, containing 636, 954, 190, 679, 126, and 528 passwords to create a length of 1-to-12-bit dictionary, containing the uppercase and lowercase letters, numbers, underscores, spaces, special characters, and other characters of the Brute Force Dictionary, as shown in Figure 7.

The WPS function of the target AP is enabled. Some products are called QSS, and the security authentication mode of the wireless network is set to "WPA-PSK/WPA2-PSK" and the password is set to "12345678." The known PIN code is "20972745;" if we crack WiFi password with reaver, in the case of the known PIN code, it only takes a few seconds to crack out WPA PSK, and the result is as shown in Figure 8. As long as the WPS function is enabled, even if the AP password is changed, it can be cracked again. After changing WPA PSK to "ABCD1234," using the PIN code, we cracked the WPA PSK password again by the experiment. The experimental results are shown in Figure 9. Even if you do not know the PIN code, you can brute force the AP password, which takes a long time. This shows that, with the use of WPS encryption of WiFi, there is a greater security risk.

According to the vulnerability and cracking method of the WEP protocol, the target AP is set to WEP encryption

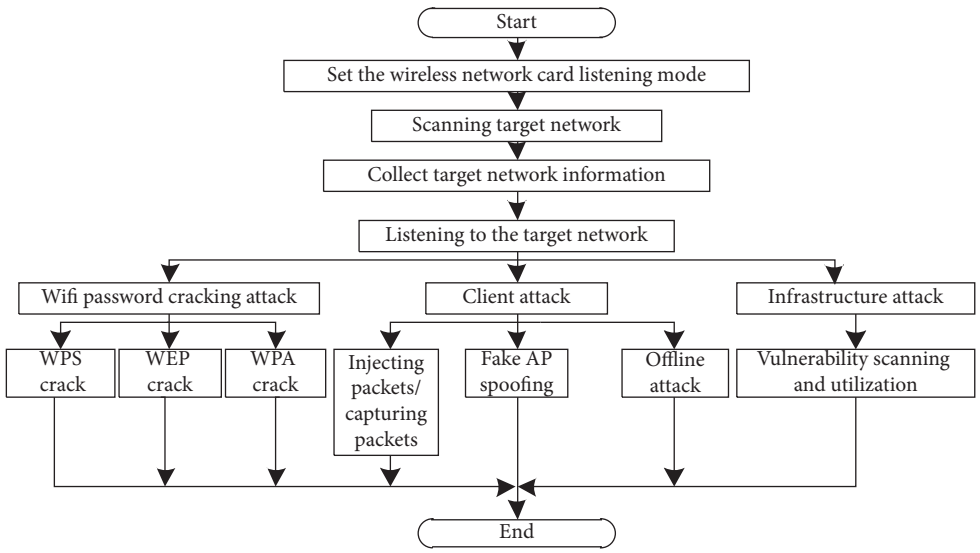

Figure 3: Kali Linux WiFi penetration test's main technical methods.

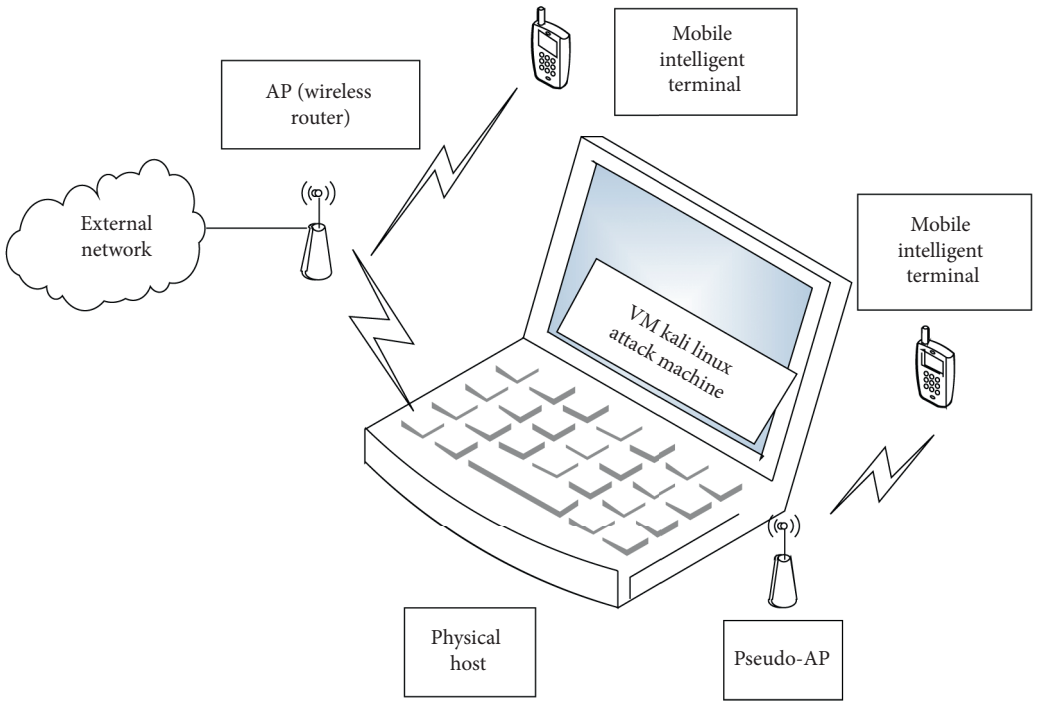

Figure 4: Experimental network topology.

[CH11] [Elapsed; 2mins] [2020-04-15 04:57]

BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
28:2C:B2:7D:57:58–36		54	4	0	1	54e.	WPA2	CCMP	PSK	testwifi

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
28:2C;B2:7D:57:58	30:92:F6:44:A1:26	–60	0 – 1	33	7	

Figure 5: Target AP information.

Name	T	C	Ch	Pkts	Size
Testwifi	A	0	1	226	96 B
BBSSID: 28:2C:B2:7D:57:58 Last seen: Apr 20 05:57:01 Crypt: WPA PSK AESCCM Manuf: Tp-LinkT					

Figure 6: Kismet scan target AP results.

Crunch will now generate the following amount of data: 6362765798379785220 bytes 6068006323222 MB
5925787425 GB
5786901 TB
5651 PB
Crunch will now generate the following number of lines: 636954190679126528

Figure 7: Crunch generates a brute force dictionary.

[+] Pin	Cracked
[+] WPS	PIN: ' 20972745'
[+] WPA	PSK: ' 12345678'
[+] AP	SSID: ' testwifi'

Figure 8: Reaver crack results.

[+] Pin	Cracked
[+] WPS	PIN: ' 20972745'
[+] WPA	PSK: ' abcd1234'
[+] AP	SSID: ' testwifi'

Figure 9: Reaver crack results again.

mode firstly, and the password is set to "abcde." Select the target AP (testwifi), implement ARP attack on the client, and grab a large number of valid data packets to crack. Get the WEP KEY value: "abcde"; the crack is successful.

The target AP (testwifi) to WPA-PSK/WPA2-PSK encryption mode is set firstly, using AES encryption, and the password is set to "abcd1234." Then, the Aircrack-ng tool is used to crack the WPA password. In the listening mode, the target network effective handshake data packets are captured for cracking, and the result is shown in Figure 10.

The captured data packet is cracked by the created password dictionary (myword. txt), and the result is shown in Figure 11. The password appears in the "KEY FOUND" option: "abcd1234"; the brute force attack is successful.

5.3. Pseudo-AP Phishing Client Penetration Test. A pseudo-AP hotspot is a fake WiFi with a real AP function. Usually, a hacker uses a pseudo-AP to implement WiFi phishing. After the pseudo-AP is created, the user is forced to connect to the pseudo-AP and the WiFi phishing client penetration test is performed. The packet capture tool is used to capture all the data packets sent and received by the client connected to the pseudo-AP, to achieve the objective of the attack.

Take the case of creating a pseudo-AP with Easy-Creds as an example. In the experiment, the ESSID of the pseudo-AP is set to "test AP." When the mobile phone is connected to the pseudo-AP hotspot "test AP," the MAC information of the client can be obtained through "Airbase-NG"; "DMESG" can obtain the IP address and system information of the connected mobile phone; the open connection URL information of the client can be captured through "SSLStrip" and "URL Snarf" windows.

When the pseudo-AP is built, according to the information of network scanning, the client working on some channels is forced offline and reconnected to the pseudo-AP, so as to penetrate the attack.

Using Wireshark to select the wlan0mon interface for data capture, all packets passing through the target AP are captured, and then specific packets can be filtered and analyzed to get the desired information.

6. Suggestions

Since WiFi uses wireless channel to transmit information, the signal is easier to capture, coupled with the existence of a number of vulnerabilities in the protocol, through the above WiFi penetration test experiment can be seen. At present, the above several commonly used encryption modes of WiFi cannot guarantee its absolute security. There are several ways to enhance its security:

(1) Modify the default password of the administrator of the router. The default password is admin. It is recommended to change the password to a complex password of 12 characters or longer to avoid the administrator password being guessed.

(2) Turn off QSS and adopt a relatively secure authentication encryption mode. It is recommended to use the WPA2 + AES authentication encryption method with higher security.

(3) Set the MAC address filtering.

(4) Disable SSID broadcasting.

(5) Turn off the Wlan automatic connection function.

(6) An open network that is not connected at will.

(7) Set a long and complicated WiFi password.

(8) Enhance the awareness of prevention, strengthen network supervision, improve network anomaly detection and intrusion detection capabilities, and open logs, and so forth.

[CH6] [Elapsed:1 min] [2020-04-03 08:02] [WPA handshake: E4:D3]

BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
E4:D3	−52	0	880	77	1	6	54e.	WPA2	CCMP	PSK	testwifi

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
E4:D3	30:92	−8	le – 1	0	431	
E4:D3	B0:E2	−62	le – 6e	1	78	testwifi

Figure 10: Airodump-ng capture results.

[00:00:33] 99708/10089016 keys tested (2995.29 k/s)
Time left: 55 minutes, 35 seconds 0.99%
Key found! [abcd1234]
Master key: 8F 9C 28 EA 16 07 07 5D 15 A6 58 46 44 3F 8D 29
B8 7A ED 48 02 50 99 AB D8 CE 7A 23 3c 37 C4 89
Transient key: 37 B2 C6 0E 05 42 5A BF 38 08 61 74 D0 AC 5E 85
C6 F0 44 CC 08 88 10 16 AE 41 DA 1C C7 1D B1 F4
99 94 5F 48 0F 33 88 0B F C D0 AB 01 1B C2 60 E5
4A 30 EB 2E 04 6E D9 70 85 35 ED 7C 82 BB 17 81
EAPOL HMAC: 77 50 B2 5D 2F 36 8E 01 2F B2 3E 2B CA 14 DF 1F

Figure 11: Aircrack-ng crack WPA results.

7. Summary

By analyzing the vulnerability of WiFi network and the vulnerability of common encryption methods, this paper puts forward the penetration test flow and main technical methods of Kali Linux wireless network, the various stages and technical methods of WiFi penetration test based on Kali Linux are described in detail. The penetration test of target WiFi network is carried out through simulation experiment, and the effectiveness of the WiFi penetration test methods based on Kali Linux, such as listening, scanning, grabbing, WiFi password cracking, offline attack, and pseudo-AP spoofing, is verified. It has a good effect on improving the security evaluation of WiFi network. The results show that WiFi penetration testing with Kali Linux can change passive defense into active defense and find out the hidden trouble of WiFi network security, which is helpful to improve the security of WiFi network.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

All authors contributed to this paper equally.

Acknowledgments

This work was supported by the Project of the Quality Engineering of Education Section of Anhui Province of China (2020xfxm27, 2015ckjh117, 2016mooc190, and 2017ghjc228), the Project of the Quality Engineering of Anhui Xinhua University of China (2019sysxx03), and the Project of the Cooperation between Production and Education of Ministry of Education of the People's Republic of China (201702139041).

References

[1] W. Z. Guo, "Research on computer wireless network and information security," *Applied Mechanics and Materials*, vol. 416-417, no. 1, pp. 1450–1453, 2013.

[2] C. Balaji, B. Ramadoss, and N. Yasuyuki, "Secure information transmission framework in wireless body area networks," *Journal of Applied Security Research*, vol. 15, no. 2, pp. 279–287, 2020.

[3] J.-B. Liu and J. Cao, "The resistance distances of electrical networks based on Laplacian generalized inverse," *Neurocomputing*, vol. 167, no. 1, pp. 306–313, 2015.

[4] J. B. Liu, S. Wang, C. Wang, and S. Hayat, "Further results on computation of topological indices of certain networks," *IET Control Theory & Applications*, vol. 11, no. 13, pp. 2065–2071, 2017.

[5] J. Kaur, "Wireless security issues and their emerging trends," *International Journal of Control Theory and Applications*, vol. 10, no. 13, pp. 85–90, 2017.

[6] R. Rana, "Man-in-the-Middle attack," *International Journal of Recent Advancement in Engineering & Research*, vol. 1, no. 3, 2017.

[7] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "MARINE: man-in-the-middle attack resistant trust model in connected vehicles," *Institute of Electrical and Electronics Engineers Internet of Things Journal*, vol. 7, no. 4, pp. 3310–3322, 2020.

[8] M. Kandias and D. Gritzalis, "Metasploit the penetration tester's guide," *Computers & Security*, vol. 32, no. 1, pp. 268-269, 2011.

[9] P. Herzog, "Open-source security testing methodology manual," *Communications of the Acm*, vol. 50, no. 5, 2003.

[10] M. C. Ghanem and T. M. Chen, "Reinforcement learning for efficient network penetration testing," *Information*, vol. 11, no. 1, 2020.

[11] K. Anwar Sedek, N. Osman, and H. Mohd Nizam Osman and, "Kamaruzaman jusoff, "developing a secure Web application using OWASP guidelines," *Computer and Information Science*, vol. 2, no. 4, pp. 137–143, 2009.

[12] F. Ö. Sönmez, "Security qualitative metrics for open Web application security Project compliance," *Procedia Computer Science*, vol. 151, no. 4, pp. 998–1003, 2019.

[13] M. E. Khan and F. Khan, "A comparative study of white Box, Black Box and grey Box testing techniques," *International Journal of Advanced Computer Science & Applications*, vol. 3, no. 6, pp. 1–12, 2012.

[14] R. Colistra, "Shaping and cutting the Media agenda," *Journalism & Communication Monographs*, vol. 14, no. 2, pp. 85–146, 2012.
[15] M. A. L. Joseph, "Web penetration testing with Kali Linux," *Computers & Security*, vol. 1, no. 09, p. 40, 2013.
[16] Y. L. Liu and Z. G. Jin, "Security analysis of WPS in WLAN," *Computer Engineering & Applications*, vol. 49, no. 21, pp. 87–89, 2013.
[17] G. F. Wu, D. Q. Hu, and P. D. Wang, "Research and improvement in the security of WEP protocol based on RC4 algorithm," *Journal of Hefei University of Technology*, vol. 35, no. 5, pp. 617–637, 2012.
[18] V. Kumkar, A. Tiwari, P. Tiwari et al., "Vulnerabilities of wireless security protocols (WEP and WPA2)," *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 1, no. 2, pp. 34–38, 2012.
[19] A. Tsitroulis, D. Lampoudis, and E. Tsekleves, "Exposing WPA2 security protocol vulnerabilities," *International Journal of Information and Computer Security*, vol. 6, no. 1, pp. 93–107, 2014.