12th International Conference on Recent Innovations in Science, Engineering and Management
Sri Venkateswara College of Engineering & Technology,Etcherla, Srikakulam (ICRISEM'18)
17th February 2018 www.conferenceworld.in ISBN: 978-93-87793-01-9

An Implementation of WEP/WPA/WPA2 Password Cracking using Fluxion

Fauziah Permatasari[1], Umapathy Eaganathan[2]

Student, BSc (Hons)in IT with ISS, Asia Pacific University, Malaysia

Faculty in Computing, Asia Pacific University, Malaysia

ABSTRACT

The attack described in this paper and carried here will be revolving around WEP/WPA/WPA2 password cracking. The background behind WEP/WPA/WPA2 itself is firstly explained therefore the attack itself can be described in a more informative and clearer way. There are several aspects that will be considered throughout the hypothesis and also the act of attack itself. This includes the hypothesis of the scenario, the tools and their specifications, the step by step of the attacks, and also the mitigations and recommended solutions on preventing such attack from happening. In the end of this paper, a conclusion is made by comparing to the previously defined hypothesis, aims, and objectives. This is done in order to give evaluation on the efficiency and success of the attack and its related research. All in all, this research and attack are done to give more insight towards the WEP/WPA/WPA2 attacks.

Keywords: Encryption Algorithm, Hypothesis, Kali Linux, Password Cracking, Wireless Network

I. INTRODUCTION

Wired Equivalent Privacy (WEP) is a security protocol that is specifically designed to provide a level of security that matches with the one that is implemented on wired Local Area Network. WEP is a component of the standard IEEE 802.11 WLAN [1]. WEP itself works by encrypting the data with a symmetric RC4 encryption algorithm. It uses a secret key to protect wireless communications from being breached and also reduce the possibility of the wireless network to be accessed by unauthorized patrons [2]. The key is later on used to encrypt packets before a transmission is carried out. The key itself will be shared between the mobile station and the access point. The main goal of WEP is to provide and guarantee confidentiality, access control, data integrity, efficiency [3], shown in "Fig.1 and Fig.2".

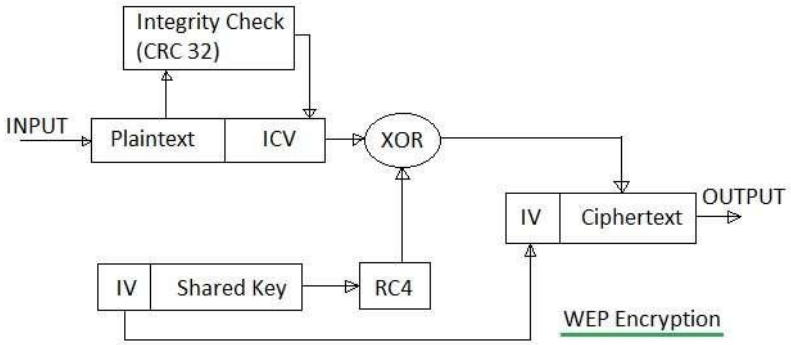


Figure.1 WEP Encryption[4]

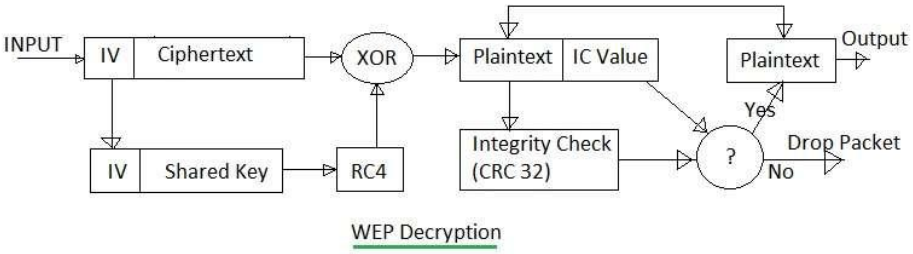


Figure.2 WEP Decryption process [4]

Due to WEP's failure to meet with the security level that is expected to par the equivalent that of wired LANs, Wireless Protected Access or often abbreviated as WPA, is created to provide for confidentiality of data and fixes most of WEP's problems [5].WPA is the subset of Robust Security Network (RSN). It is compatible with the 802.11i security standard. Although WPA and RSN share a similar architecture, there are still a few differences. Such as WPA's subset of capability that is only focused on a way in implementing a network. According to [6], another difference between WPA and RSN is, in additional of TKIP (Temporal Key Integrity Protocol), RSN also supports the AES (Advanced Encryption Standard) cipher algorithm.In short, even though WPA is more common between Wireless network users nowadays, it is suggested for them to upgrade towards a full RSN solution. The reason is because RSN architecture is more complex however it is more suitable and secure to be used in large scaled network, something that is one of the problems faced by WEP which is impractical to manage key distribution whenever it has more than tens of users [7].

WPA2 is also compatible with the 802.11i standard. As previously stated, WPA has fixed the weaknesses that are present in WEP. However, WPA also added some new vulnerabilities. Therefore WPA2 is created to provide stronger data protection and network access control, shown in "Fig.3".

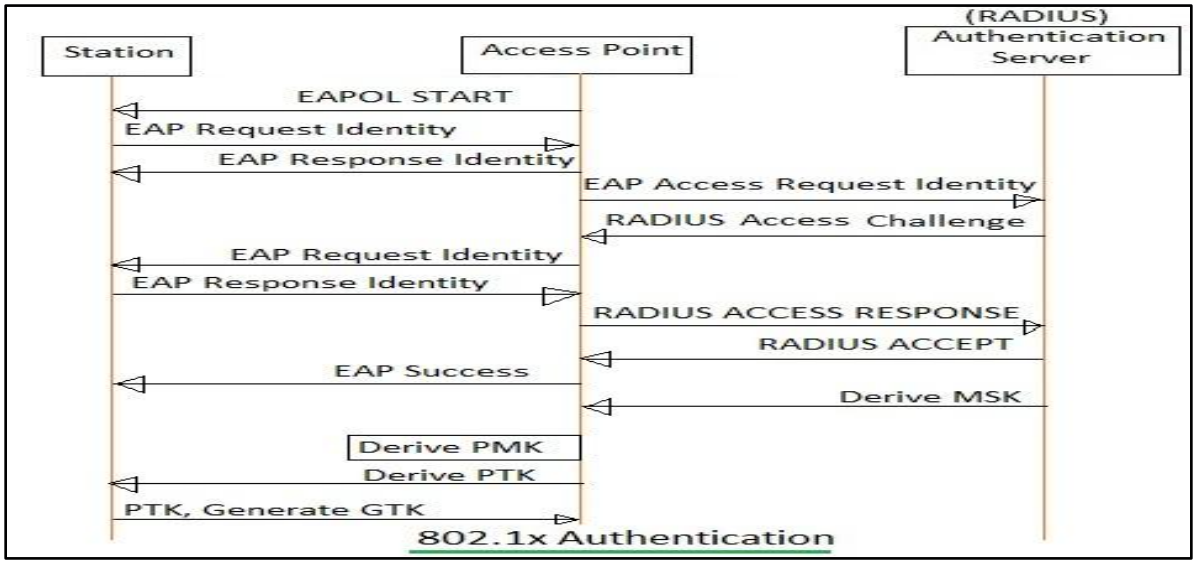


Figure.3WPA2 Authentication [4]

II . VULNERABILITIES

WEP has several basic flaws that makes it highly vulnerable to serious attacks. The vulnerabilities include its undefined method for encryption key distribution, this is because the pre-shared keys are set only once during the installation and are rarely ever updated. Other than that is its use of RC4, which was designed to be a one-time cipher and it was not intended for multiple usage. This is very vulnerable to man-in-the-middle attack because the attacker then can monitor the traffic and decipher the packets into plaintexts. This will be easily done using various tools such as AirSnort, WEPCrack, or dweputils [8]. The distribution and sharing of PSK keys in WEP is performed manually, therefore it does not have any technology security protections [9]. It is shared in non-secure methods which to whoever users who gain the access toward the key, will be assumed as an authentic user and thus approved. WPA is vulnerable to denial-of-service (DOS) attacks. And the worse thing about this vulnerability is the only workaround that can be done is by switching it completely to WEP until the attack subsides. Other than that, WPA is also vulnerable to dictionary attacks if the pre-shared 14 character key is a legitimate word [2].

A way to attack WPA encrypted network is by capturing the pre-shared key that is used to set up the WPA encryption during the initial communication between the access point and the client [6]. After the pre-shared key has been captured, then it will be used in guessing the WPA key by using standard dictionary attack [10]. Another form of attack is Evil Twin attack. It is an attack which is using homemade wireless access point that is tricking wireless users by acting as a legitimate access point in order for the attacker to gain information without the target's consent [1]. The evil twin wireless access point is positioned in the vicinity of a legitimate access point, by using the same name that is used by the legitimate access point.

III. HYPOTHESIS

The hypothesis proposed is to prove the possibility of cracking WEP/WPA/WPA2 password by tricking its users into giving their authentic login credentials. The attack will run on as illustrated below. The attack to be carried out is cracking the WEP/WPA password of a Wireless network. It is carried out on networks which are using pre-shared keys. The method used is by sending the target a phishing page that will trick them into typing in their authorized login details. The reason of choosing this method is because, only brute force technique can be used against WPA/WPA2, unlike the ones on WEP, where statistical methods can be used to speed up the cracking process [11]. And a brute force attack is very time consuming, considering that it is compute intensive, whereas a computer can only test 50 to 300 possible keys per second, depending on the computer CPU. Therefore, it can take hours or even days to go through a large dictionary of words [12],shown in "Fig.4".

3.1 Aim

The aim of this research and attack is to carry out an attack on WEP/WPA/WPA2 in order to gain unauthorized access into the network.

3.2 Objectives

- Gain more information and knowledge regarding WEP/WPA/WPA2 implementations.
- Discover the most suitable method and tools to be used on carrying out WEP/WPA/WPA2 attack.
- Gain more information related with the tools and techniques to be used in proving the hypothesis.
- Conduct a successful attack on WEP/WPA/WPA2 protected wireless network.
- Find the solutions and workarounds regarding the attacks on WEP/WPA/WPA2 protected wireless network.

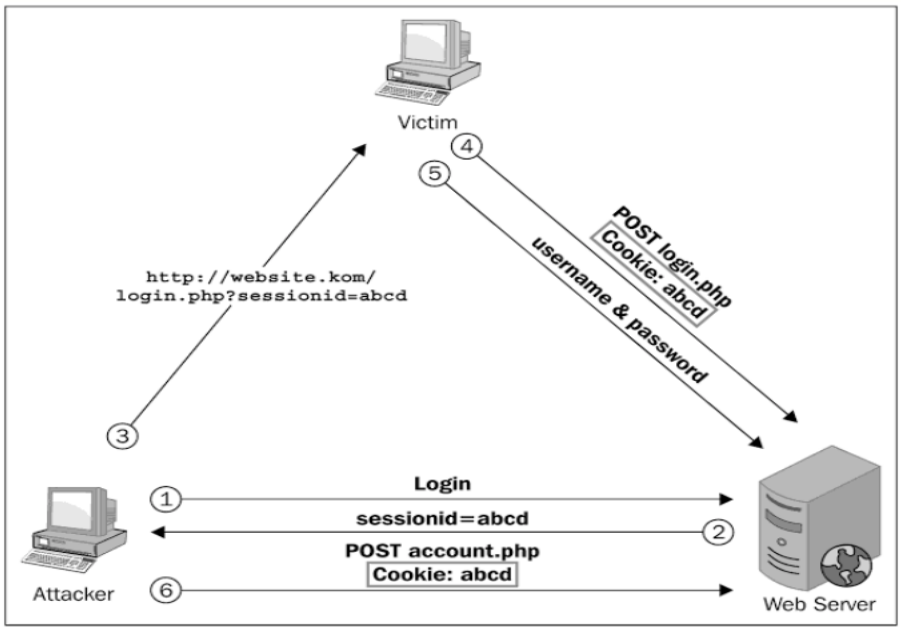


Figure 4. Illustration of the scenario [13]

IV. SELECTION OF TOOLS

There are in total four tools to be considered in carrying out the attack. Here will be explained the differences between these tools, and from the comparison then it would determine which tool is the most suitable in meeting the aim and objectives of the research. The four tools are Cain & Able, Airsnort, Aircrack, and Fluxion.

4.1 FEATURES

Kali Linux is selected as the default operating system in carrying the attack. And the tools chosen in carrying the attack include Fluxion and Aircrack-ng. The two tools work hand in hand in carrying the attack, since Fluxion mainly delivers the core of the attack that is by creating an evil twin AP, and Aircrack-ng is used to capture the handshake, shown in "Fig.5".

4.1.1 FLUXION

Fluxion is a sophisticated tool that blends the traditional password cracking method, and the use of social engineering. This makes the rate of success in running the attack to be reasonably high. Some features of Fluxion are:

1. Capture WPA handshake.
2. Control the behavior of login page and its entire script.
3. Creates an evil clone with the same name as the legitimate one.

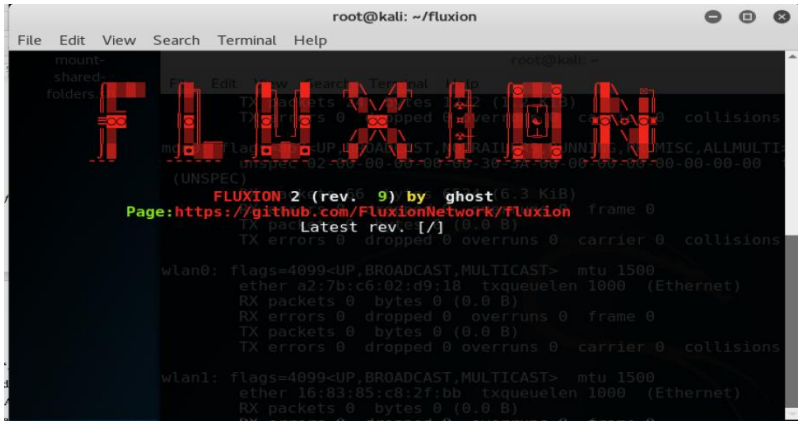


Figure5. Interface of Fluxion

4.1.2 AIRCRACK-NG

Aircrack-ng is usually used in assessing wireless network security that are focused on monitoring, attacking, testing, and cracking. It is using command line that allows heavy scripting, shown in "Fig.6". Some features of Aircrack-ng are:

1. Capturing packet and export data into text files to process them further.
2. Replay attacks, deauthenticate, fake access pints, all by using packet injection.
3. Checking wireless cards and driver capabilities.
4. WEP and WPA-PSK password cracking.

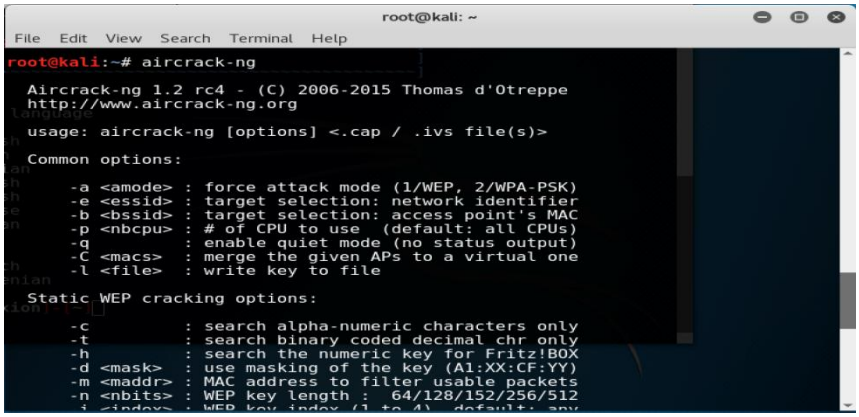


Figure 6. Aircrack-ng interface

4.2 JUSTIFICATION

The reasons behind the decision in using Fluxion and Aircrack-ng for the attack is because the two tools work in synchronize to carry the attack. Without Aircrack-ng, Fluxion will not be able to evaluate the captured handshake as valid or not. Meanwhile, without Fluxion, Aircrack-ng will not be able to create and control the entire script of the evil twin AP. Therefore, by using these two tools simultaneously, the rate of success in carrying out the attack will be much higher. Another thing is that to recover from the attack, it will be easier compared to by using other tools considering the tools do not exploit more than the password cracking itself thus it will not seriously affect the victim's device nor the network itself, shown in "Table.1" and the evaluation will be in "Table.2".

V. TEST PLAN

No.	Task Description	Objectives	Expected Result
1.	Clone and install Fluxion.	Adding Fluxion into Kali Linux's system.	Fluxion is installed and attacker will be able to perform attack using the tool.
2.	Choose a wireless network as a target.	To attack the wireless network by obtaining its password.	By choosing the selected options, a sequence of windows will appear throughout the attacking process.
3.	Capture and deauthenticate handshake.	Handshake will be captured and analyzed using the Aircrack-ng tool.	By choosing the selected options, a sequence of windows will appear throughout the capturing and analyzing process.
4.	Run and wait for the attack to take place.	Have a user to be tricked into giving up their login details.	By choosing the selected options, a sequence of windows will appear throughout the attacking process. These windows will monitor the activity of the evil twin AP, the targeted wireless network, and the active user.

5.	Obtain a login credential.	Have a user tricked into giving up their login details.	A window will appear notifying that the key has been successfully obtained.
6.	Use the password key on the targeted wireless network.	Login to the targeted wireless network.	Attacker will be able to login to the wireless network and appeared as legitimate.

Table 1. Test Plan

VI. DEMONSTRATION

Step 1: Download and install Fluxion.

Fluxion is based on previously created program such as Aircrack-ng and hostpad. It is available to be downloaded for free from github. After Fluxion has been downloaded or cloned, the installation process began as follows, shown in "Fig.7".

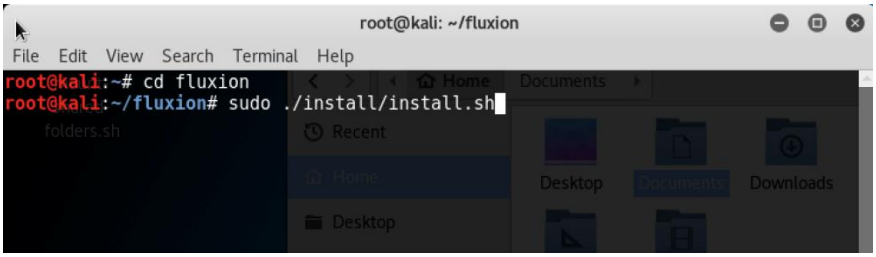


Figure 7. Command line to install Fluxion

After the command lines shown above have been run, then the Fluxion installation will start. It will check whether the components and tools required to install Fluxion have existed in the Kali system, shown in "Fig.8".

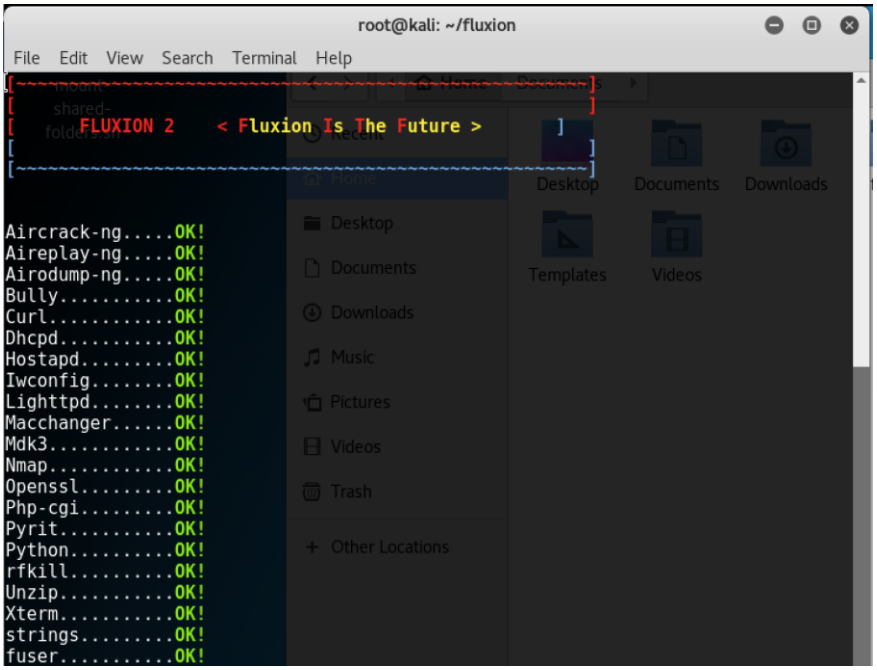


Figure 8. Installation process of Fluxion

Once everything has been checked and all required components are complete, then a display that forces the user to choose a language of Fluxion's interface will show in "Fig.9".

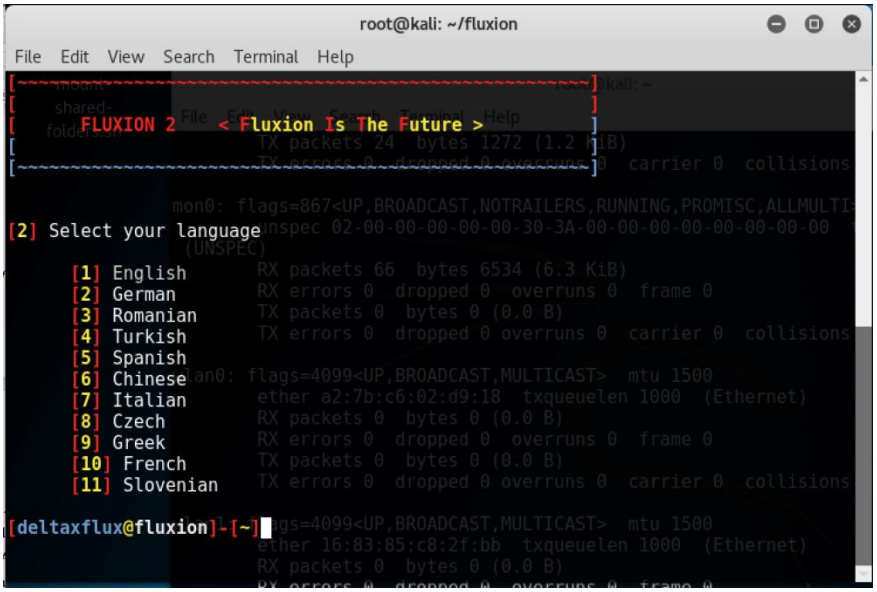


Figure 9. Select language

Step 2: Carrying the Attack

In the second step, the attack will be carried out. Firstly, attacker has to select the WLAN interface to be used in monitoring the existing wireless networks, shown in "Fig.10".

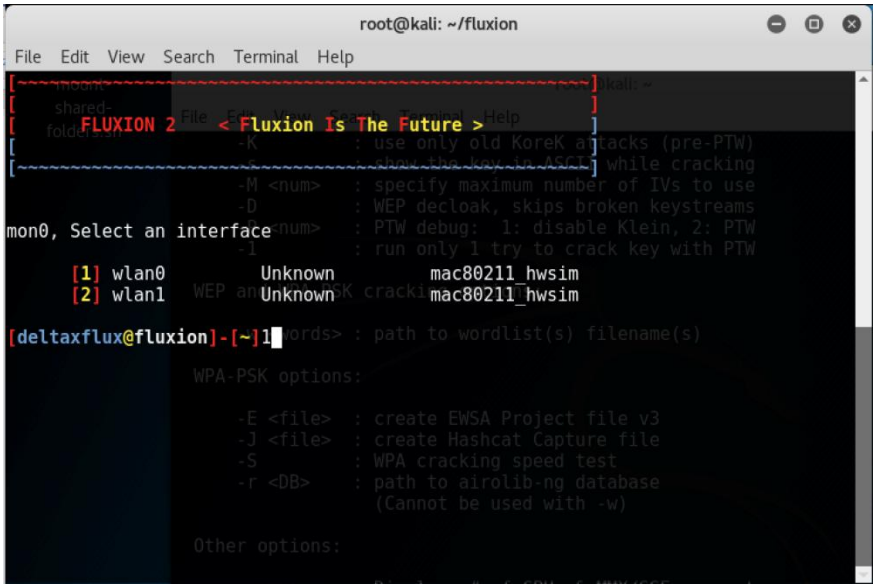


Figure 10. Select wireless interface

Then, the next step is to choose the channel, which in this case the attacker chose the first option that was 'All channels', shown in "Fig.11".

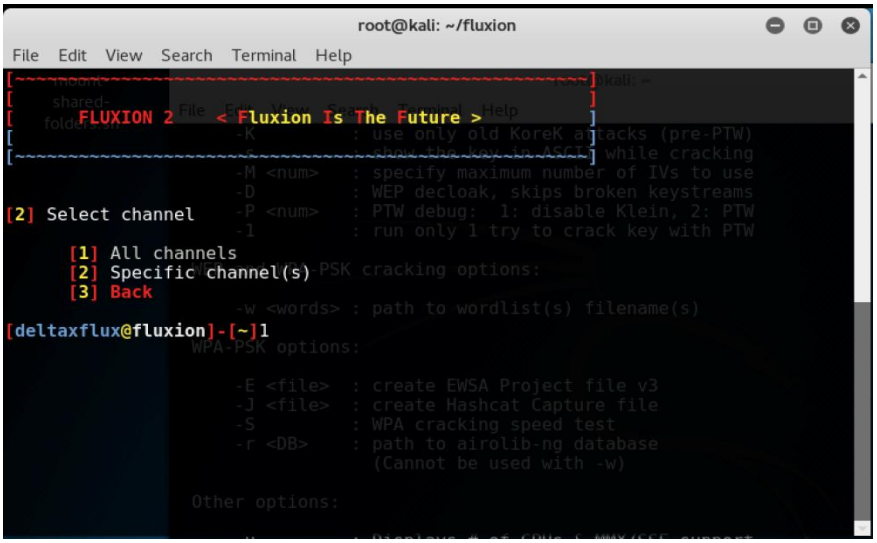


Figure 11. Selecting wireless network channel

Then a Wi-Fi monitor will appear showing the list of available wireless networks. If at first there are no wireless network detected, the attacker can go back to the Fluxion's Terminal window and type in R in order to refresh the WiFi Monitor, shown in "Fig.12".

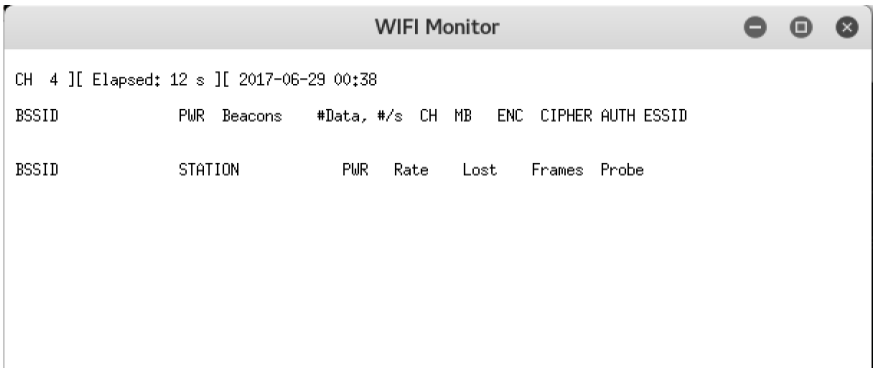
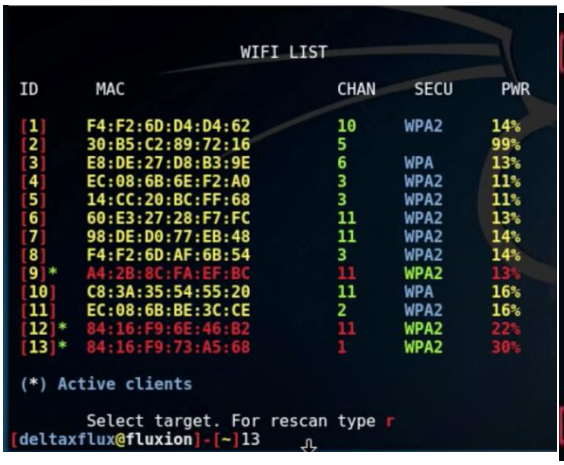


Figure 12. Wifi monitor

The detected wireless network will appear as a numbered list, and attacker has to choose which wireless network should be attacked by simply typing in the number of the specified network as shown in the list. After choosing the targeted network, a selection of attack options will appear. In this scenario, the attack chosen is Number 1, using the assistance of Hostapd. And then in the handshake capturing and checking, the tool that will assist Fluxion is Aircrack-ng. It will capture the handshake and deauthenticate it as validation, shown in "Fig.13-17".



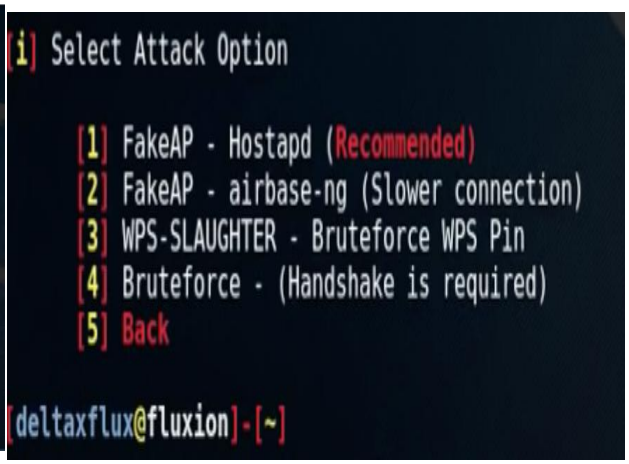


Figure 13. List of detected wireless networks **Figure 14. Options of attack**

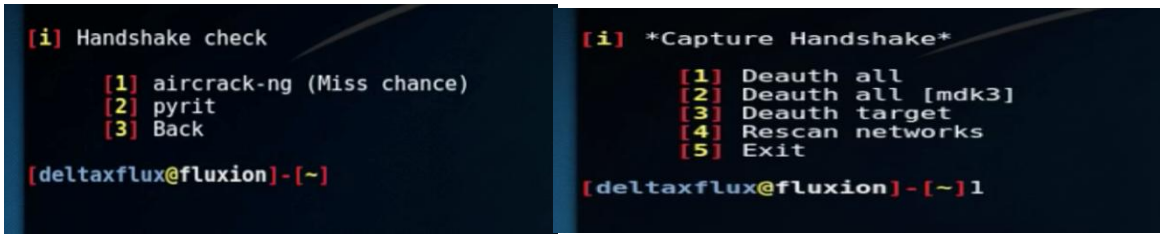


Figure 15. Handshake capturing and deauthenticating

Below is how the handshake captured appears on Fluxion's interface.

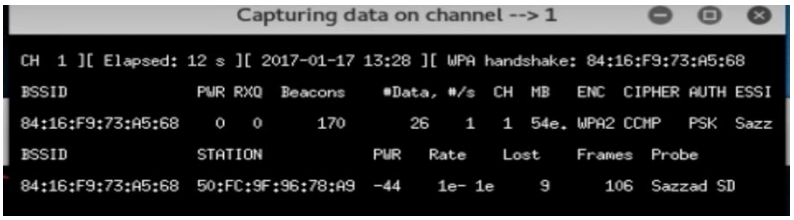


Figure 16. Captured handshake

And the next step will be creating an SSL certificate and selecting the option as 'Web Interface'.

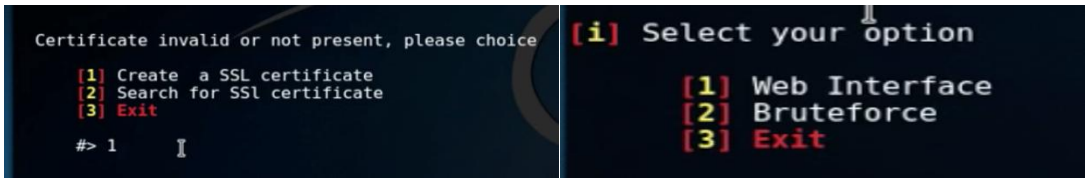


Figure 17. SSL certificate for web interface

The information of the targeted wireless network will appear, and user has to select the language for the particular evil twin AP login page. It is best to use the language that is mainly used in the area, as the purpose is to trick user into believing that the evil twin AP as legitimate, shown in "Fig.18". Fluxion itself supports many options therefore there is a long list of language that the user can choose from.

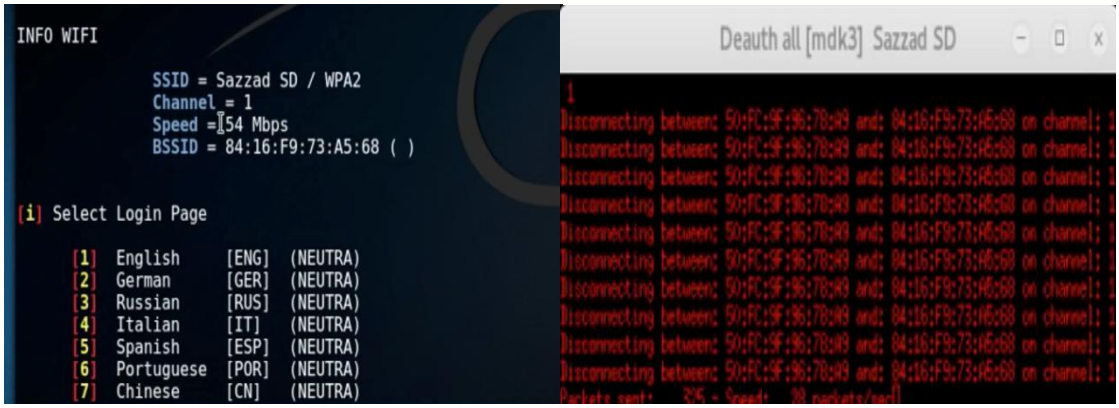


Figure 18. Twin login page creation and choosing the language and Deauthentication of handshake

After the login page language has been chosen, the following windows will appear, which are the deauthentication of captured handshake, Wireless network information, and AP details, shown in "Fig.19".

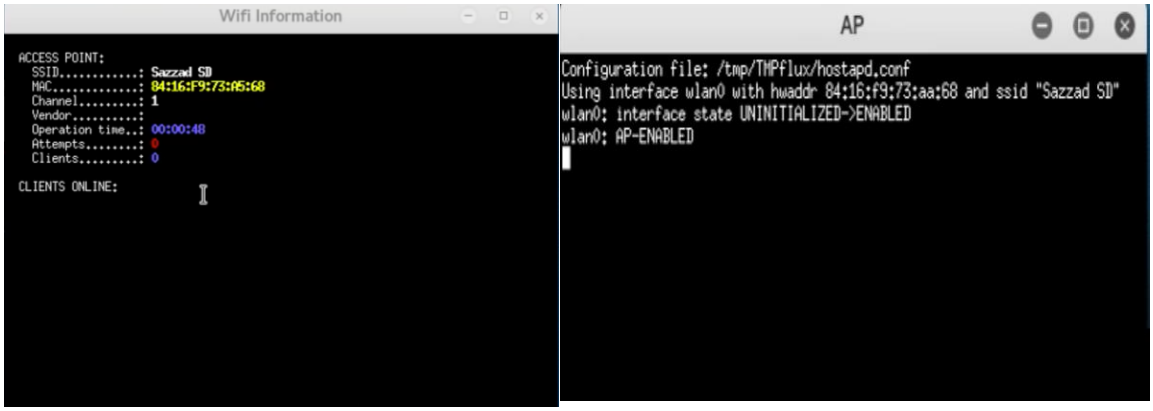


Figure 19. Targeted wireless network's information and Evil twin AP details

Once a user has been tricked into inputting his/her login credentials, the wireless network's key will be sent to Fluxion and the result will appear as follows in "Fig.20".

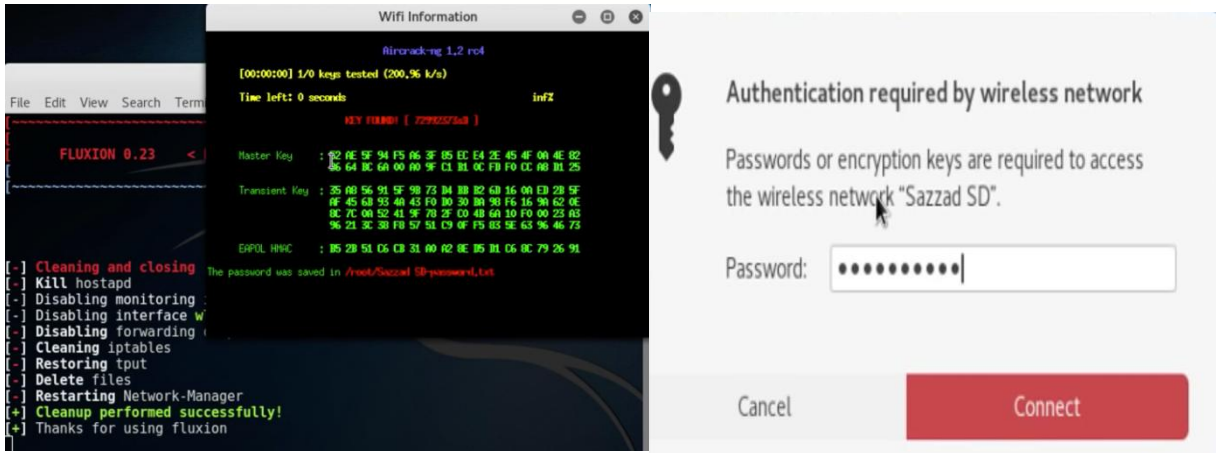


Figure 20. Key obtained and wireless network authentication

VII. EVALUATION

No.	Task Description	Objectives	Expected Result	Actual Result
1.	Clone and install Fluxion.	Adding Fluxion into Kali Linux's system.	Fluxion is installed and attacker will be able to perform attack using the tool.	Same as expected.
2.	Choose a wireless network as a target.	To attack the wireless network by obtaining its password.	By choosing the selected options, a sequence of windows will appear throughout the attacking process.	Same as expected.
3.	Capture and deauthenticate handshake.	Handshake will be captured and analyzed using the Aircrack-ng tool.	By choosing the selected options, a sequence of windows will appear throughout the capturing and analyzing process.	Same as expected.

4.	Run and wait for the attack to take place.	Have a user to be tricked into giving up their login details.	By choosing the selected options, a sequence of windows will appear throughout the attacking process. These windows will monitor the activity of the evil twin AP, the targeted wireless network, and the active user.	Same as expected.
5.	Obtain a login credential.	Have a user tricked into giving up their login details.	A window will appear notifying that the key has been successfully obtained.	Same as expected.
6.	Use the password key on the targeted wireless network.	Login to the targeted wireless network.	Attacker will be able to login to the wireless network and appeared as legitimate.	Same as expected.

Table.2 Test Plan Evaluation

VIII. RECOMMENDATIONS

Preventions against WEP/WPA/WPA2 password cracking can be done in several ways. The first way, for WEP users, is to upgrade WEP to WPA2. Then, the second method is by placing AP in a demilitarized zone (DMZ) and then utilizes firewall in front of the internal network, which this will filter traffic from unauthorized IP address. The third way is by changing the default SSID's name to make it more difficult for attackers to determine the specifications of router used [3]. The use of wireless Intrusion Prevention System also will help preventing unwanted attacks, by detecting rouge access points. It identifies the attacks by their access point's SSID, channel, signal strength, and MAC address. One of the software suggestions for this is KFSensor. It is a Windows based Intrusion Detection System (IDS). It acts as honeypot in attracting and detecting hackers and vulnerabilities. It will divert the attacks and give additional level of security by its masquerading technique [13]. However, the workarounds for WEP/WPA/WPA2 attack are much more limited compared to its preventions. The first step is by disabling the Wi-Fi connection. And for the administrators, they can adjust their router protocols, by temporarily disable the wireless network and apply the access list technique, to specifically deny traffic through their interfaces and filter the traffic itself [13].

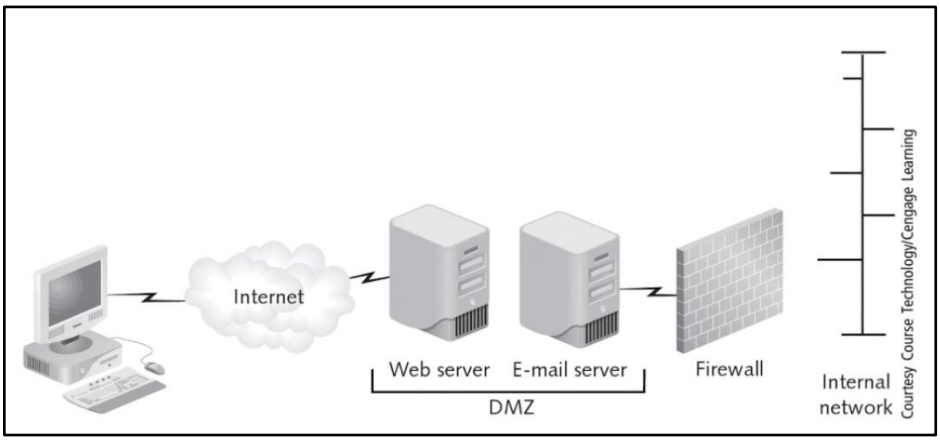


Figure21. Utilization of DMZ [13]

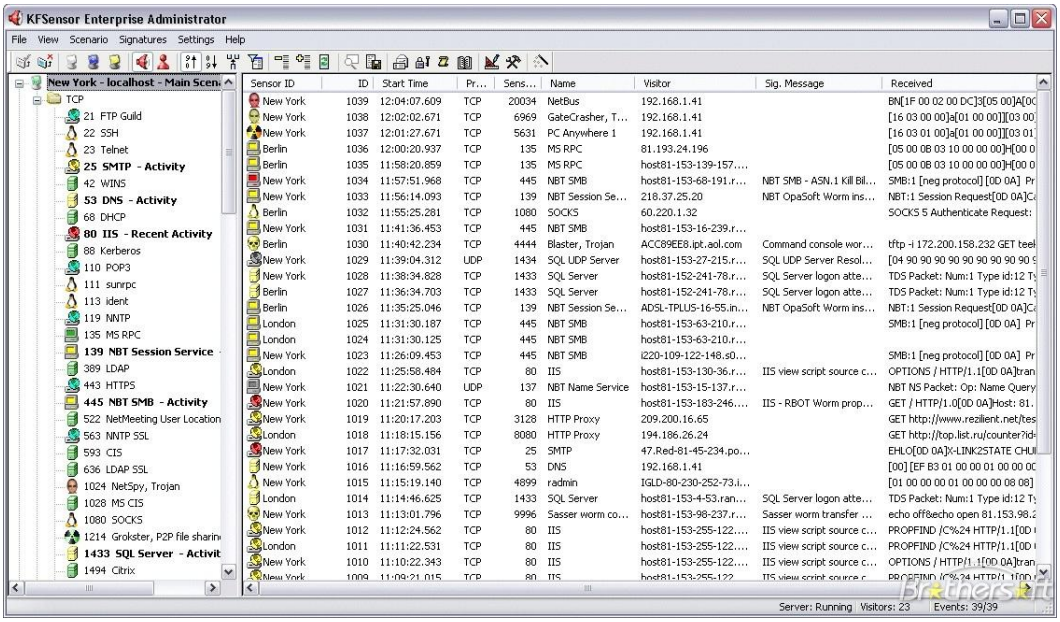


Figure 22. KF Sensor interface

IX. CONCLUSION

The research that has been done on the WEP/WPA/WPA2 security is very supportive in implementing the attack on WEP/WPA/WPA2 password cracking. The knowledge gain during the research will also be very helpful for future performances. This also brings more realization that breaching of wireless network can easily be done anywhere and

by anyone. The limitation of this research and attack is that this only covers the nutshell of WEP/WPA/WPA2 attack. Because in real life, malicious parties will exploit further and they will not stop at just cracking the wireless password. However, proper implementation of security countermeasures as recommended should be applied in order to prevent serious exploits of the network and such case will be easily prevented. In conclusion, this research and attack have been successfully carried out and have met their aims and objectives, which are to carry out an attack on WEP/WPA/WPA2 in order to gain unauthorized access into the network, find the solutions and workarounds regarding the attacks on WEP/WPA/WPA2 protected wireless network, and to conduct a successful attack on WEP/WPA/WPA2 protected wireless network.

X .ACKNOWLEDGMENT

The authors would like to share gratitude to Mr Umapathy Eaganathan, Lecturer in Computing, Asia Pacific University, Malaysia also Miss Angel Aron for the constant support and motivation helped us to participate in this International Conference and also for journal publication.

REFERENCES

[1] Akin, D., Davis, P. and Beaver, K. (2013). *Hacking wireless networks for dummies*. Hoboken, N.J.: John Wiley & Sons.

[2] Beaver, K. (2010). *Hacking for dummies*. Hoboken, N.J: Wiley Pub.

[3] Wrightson, T. (2012). *Wireless network security*. New York: McGraw-Hill.

[4] Rfwireless-world.com. (2017). *WEP vs WPA vs WPA2 | Difference between WEP,WPA,WPA2*. [online] Available at: http://www.rfwireless-world.com/Terminology/WEP-vs-WPA-vs-WPA2.html [Accessed 20 Jun. 2017].

[5] Johns, A. (2015). *Mastering wireless penetration testing for highly secured environments*. Packt Publishing.

[6] Edney, J. and Arbaugh, W. (2005). *Real 802.11 security*. Boston: Addison-Wesley.

[7] Council, E. (2016). *Ethical Hacking and Countermeasures: Secure Network Operating Systems and Infrastructures (CEH), Book 4*. 2nd ed. Cengage Learning.

[8] Council, E. (2009). *Ethical Hacking and Countermeasures: Secure Network Infrastructures*. Cengage Learning.

[9] Ciampa, M. (2014). *CompTIA Security+ Guide to Network Security Fundamentals*. 5th ed. Cengage Learning.

[10] Evans, G. (2010). *How to Become the Worlds No. 1 Hacker: Short & Simple*. 1st ed. Cyber Crime Media.

[11] Ramachandran, V. and Buchanan, C. (2015). *Kali Linux Wireless Penetration Testing Beginner's Guide*. 2nd ed. Packt Publishing.

[12] Saxena, H. (2015). *How To Hack A WiFi: Hacking WiFi*.Simpson, M., Backman, K. and Corley, J. (2011). *Hands-on ethical hacking and network defense*. Boston, MA: Course Technology, Cengage Learning.

[13] Simpson, M., Backman, K. and Corley, J. (2013). *Hands-on ethical hacking and network defense*. Boston, MA: Course Technology