ANALYSIS OF ATTACK ON THE WIRELESS COMPUTER NETWORK

Vladimir Jovanović[1]
Ministry of the Interior of the Republic of Serbia

Abstract: In the recent years, things have turned more towards the concept of "Internet of Things", which represents networking, mostly wireless different types of objects that are in mutual communication. This may include various physical objects, vehicles, buildings and other things with built-in electronic devices, software, sensors and networks that enable sharing information between the connected devices that can be remotely monitored and controlled. While it brings many benefits, it also brings to the focus the question of security. It is considered as one of the most importance, especially having in mind that most of the above-mentioned systems are used for critical infrastructure, where the system is expected to work towards perfection, and where any kind of influence on the network may be fatal for their performance. Since wireless networks become dominant compared to wired ones, their security evaluation is widely researched. There are different tools avaliable for security evaluation of local wireless computer networks. In this paper, we are focusing on tools that can be found within Kali Linux OS. For evaluation purpose, we were launching a set of different attacks on wireless networks, and afterwards we made a comparison of their performance. Our experiment has shown that wifi is prone to attacks, that they can easilly be performed by using avaliable free platforms and that Kali Linux provides tools for that which are efficient.

Keywords: cybersecurity, cybercrime, security, wireless network

INTRODUCTION

Modern society is embracing the emerging concept of "Internet of Things" (IoT) representing '*a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction*'.[2] Although the traditional form of wired network connection is still in use, wireless connection is the technology that provides the wide utilization of IoT.

1 v-jovanovic@hotmail.com
2 https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

There are several advantages and disadvantages of wireless standards 802.11 utilization. Advantages include the mobility, usability and flexibility, and disadvantages are related to limited bandwidth in comparison to wired networks and security issues. Security issues are particulary important because anyone who is within signal transmission radius might be able to record (listen) and analyze network traffic. There exist different ways how WEP and WPA/WPA2 authentication can be bypassed. For example, WEP is susceptible to FMS (Fluhrer, Mantin and Shamir) attacks, including Korek and PTW variations and ChopChop attacks, while WPA and WPA2 are susceptible to dictionary attacks and Bruteforce (Kanawat S. D., Parihar P. S., 2011).

There are different tools avaliable for security evaluation of local wireless computer networks. One of them includes penetration testing, where a simulation of attack is performed in order to find vulnerabilities and provide protection for them. One of the most popular and most advanced Penetration Testing Distribution is Kali Linux.[3]

Kali[4] represents a version of Linux operating system, with built in tools and framework, which does testing on the network, system, penetrative tests and such. Like other versions of Linux operating systems, it is free with a large support from the community. The possibility exists of booting the OS in Live mode, directly from the USB or some other device. It can also be used in forensic mode, preventing any interaction with the hard disk, which can be verified through unchanged hash value of hard disk image.

It is possible to control the path of graphic and command interface, however it is more effective to use the command in terminal mode due to its stability, which responds to optimization of hardware resource usage needed for the display of graphical elements (Beggs R., 2014).

In our experiment, we were testing different tools avaliable within Kali framework. The aim was to compare their performance in order to evaluate both: the security of wireless networks as well as the ability of used tools to simulate real attack and find vulnerabilities.

The tools in Kali that we used for simulation of attack on WiFI are:

- Crunch
- Aircrack
- Evil twin
- Cowppaty

In order to perform this kind of attack the wireless adapter should be working in the monitor mode, in order to be able to view and capture the network packages. For our experiment we used "*TP Link WN722N*" *version* 1.0 which has this ability.

The rest of the paper is organized as follows. In the first section, we gave the brief description of two popular attacks that we are going to use in our simulation

3 https://www.kali.org/
4 more on https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/

of attack. In section 2 we gave the results of our simulation of attack. The paper is closed with the conclusion section and list of used references.

ATTACKS ON WIFI NETWORKS
tcp handshaking flood

enabling communications takes place where a user who requires communications, through TCP protocol by sending the SYN packet (initiating communications), after receiving, the other side sends back SYN and ACK, where the user sends ACK again and the enabling communications starts. The first step the attacker performs is to repeatedly send SYN packets at the other side (server), using falsified IP addresses (spoofing), to which the server responds with ACK packets. The communication is not established since the server is waiting for the response (which never arives). Since the table of the avaliable connections is filled, when it comes to legitimate users they are kicked out of the establishing communication (Figure 2). Nowdays, this kind of attack is very efficient due to the fact that our devices (cellphones, laptops, sensors, etc.) are set to constantly receive the network traffic and if they find themselves on the receiving end, then networks enable the exchange of credentials in the established communication (Beggs R., 2014).

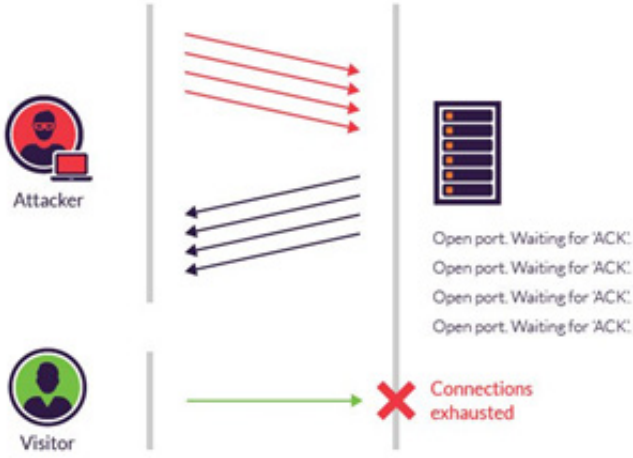

Figure 1. *TCP Hanshaking Flood attack*[5]

5 adapted from https://www.google.com/url?sa=i&source=images&cd=&ved=2ahUKEwj-l6TF-MriAhVE_aQKHQa8CHgQjRx6BAgBEAU&url=https%3A%2F%2Fwww.imperva.com%2Flearn%2Fapplication-security%2Fsyn-flood%2F&psig=AOvVaw3KFfimucO68gyjb9U38DQF&ust=1559569841643159

EVIL TWIN

This technique is very compelling for use because it can give a desired result in short term. It must use more tools for an attack, as it is important to fabricate an IP address (spoofing), disconnect users, and then take the packet with credentials. In some ways, it is a hybrid type of an attack, because it covers the method of social engineering, where the main target is the end user (Beggs R., 2014).

The same attack can be initiated systematically (step by step), through the use of special kinds of tools, but there exist more types of solutions which integrate more kinds of tools, so that it can ease up the end user's initiation of the attack. Integration of these tools requires minimal interaction between users and the system. The breach into the network is done firstly by committing the deauthentication of the user then the valid device tries to establish a connection. It relies on a stronger signal of the chosen station, which sends a request for connection with a fake station, after that the user is expected to input their password. This option is done through a specially generated station, so that the user has an impression of communication with the geniune device, with consequences that password is sent to the hacker who then immediately use it (Figure 2).

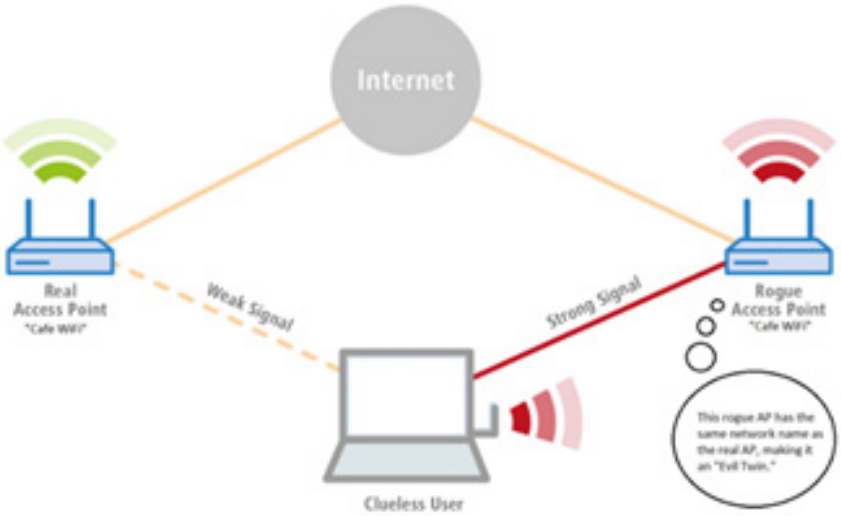

Figure 2. *A graph of an Evil Twin attack*[6]

SIMULATION OF ATTACK ON WIFI NETWORK

Before the beginning of the simulation the router that is to be used for an attack is set. The safety parameters in WPA2 are set (Figure 3), and the chosen password is put in under the guide of the most widely-used factory settings - the last few keys are the serial number of the device.

6 adapted from: https://thecybersecuritymancom.files.wordpress.com/2018/08/evil-twin.png?w=925

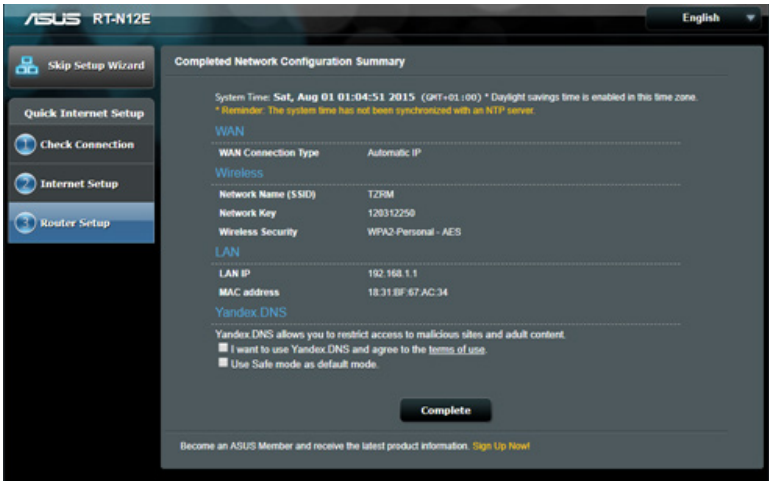

Figure 3. *The safety parameters of the router*

After the successful setting of the router, we are performing the scaning of the network, which gives us the list of available signals of different networks with a detailed description of devices they emit (MAC address, type of protection, SSID, etc.).

Then we perform the command: airodump-ng wlan0 where the result is shown in Figure 4.

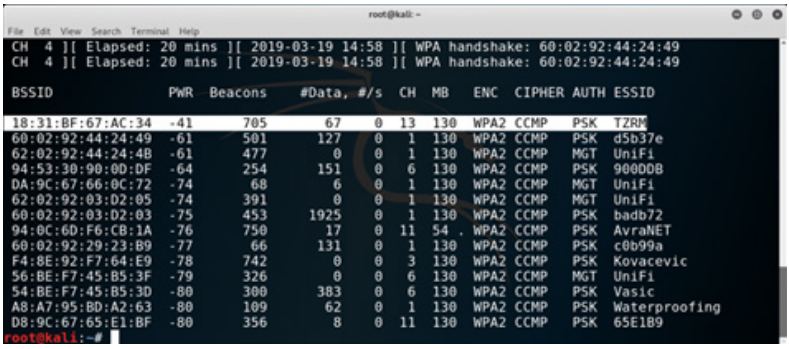

Figure 4. *The display of online signals in the network*

We perform this function by entering the number of channels we want to listen to, the file in which we place the packets, which we later "catch", the MAC address of the device, as well as the interface through which we go online.

By reviewing the list of devices and their communication in the network, we choose a potential target, focusing on the device which we want to follow. We do this by inputting the number of the channel which we want to listen (eavesdrop), we dedicate the file in which we will save network traffic packets we were able to

capture, the device's MAC address and the interface through which we go into the network.

Then we perform command: airodump-ng –c (number of channels) –w fajl –bssid (MAC devices) wlan0

Figure 5 shows the process of following (listening) the seleceted device.

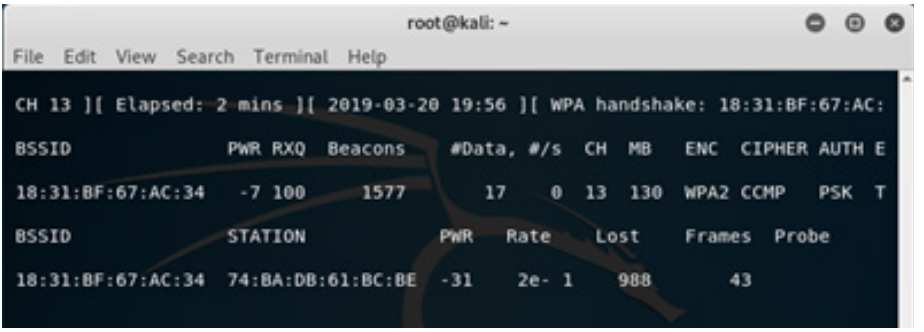

Figure 5. *Showing the following of the selected device*

After listening to the network traffic (eavesdropping), we initiate "TCP Handshaking Flood", where we send frequent requests to the device in order to drop other networks out of communication. With tool aireplay, we initiate connection, a function which will lead to kicking out every legitimate user of the device, then we input the MAC address of the device and one client, as well as an interface which we use to connect to the network.

The result of performing the command: aireplay-ng -0 5 –a (MAC device) –c (MAC client) wlan0 is shown in Figure 6.

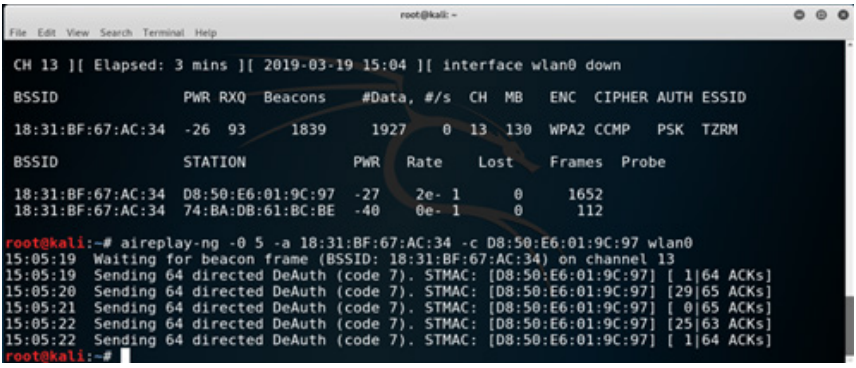

Figure 6. *Showing the already sent requests for communication by which the kicking of every legitimate user is done*

After the user is dropped out of the network (disconnected) the attacker is waiting for the new attempt of the device to reconnect to the network. At that point, packets with secure credentials (authentication) can be captured and saved

in the dedicated file and the crunch tool in combination with aircrack can be applied. By doing so, a brute force attack is initiated, where every possible combination of characters is tried. This is made possible through the crunch tool that tries out every combination, and as additional parameters, we can input how many characters the password may contain as well as the specific group to which they belong. Every listed value is then compared with the content of the file containing the captured network traffic packets of the targeted device. For that puprose, we use the aircrack tool (Figure 7). The command we have performed is: crunch 9 9 1234567890 | aircrack -w- fajl.cap –bssid (MAC device)

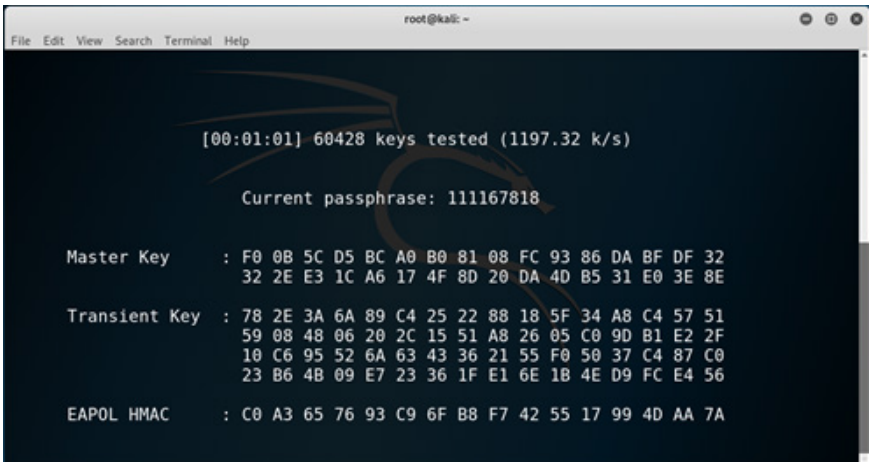

Figure 7. *Listing and trying to codebreak the passwords*

After the process is finished, the user's password is shown in the ASCII code, understandable to a human, that is, the end user.

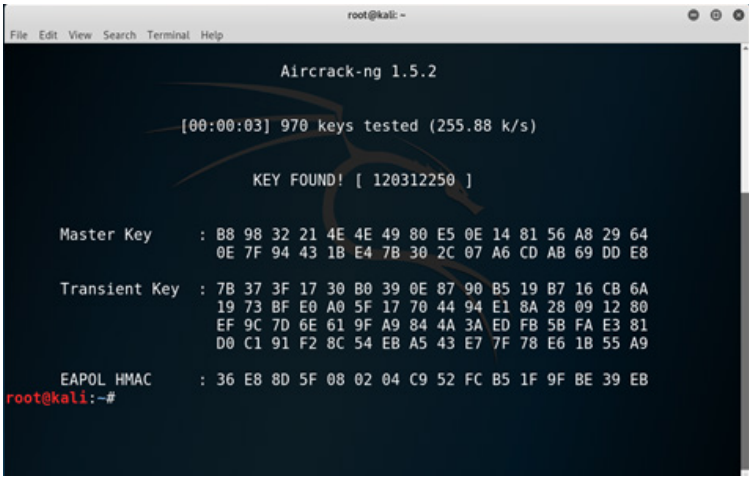

Figure 8. *Final result of the broken password*

The attack was successfully completed, regardless of the type of protection, but with used parameters (the lenght of the password), the process lasted for approximately 1 hour and 43 minutes. This method of attack represents the combination of many types of individual tools, having their own roles in completing the process. Additional integrated solutions provided by other vendors alow the hackers to simply initiate the selected types of attacks. These tools are available in Github (a platform for development and sharing of software applications) where simple downloading makes it possible to use it as well as to make the additional changes and developments. All tools provide similar hacking methods, since the most popular techniques are "TCP Handshaking Flood" and "Evil Twin" (Smet D., Pritchett W., 2013).

The first integrated solution we considered is "Fluxion".[7] It is freely available containing several tools that can be used for simulation of attack at wireless computer networks (Figure 9).

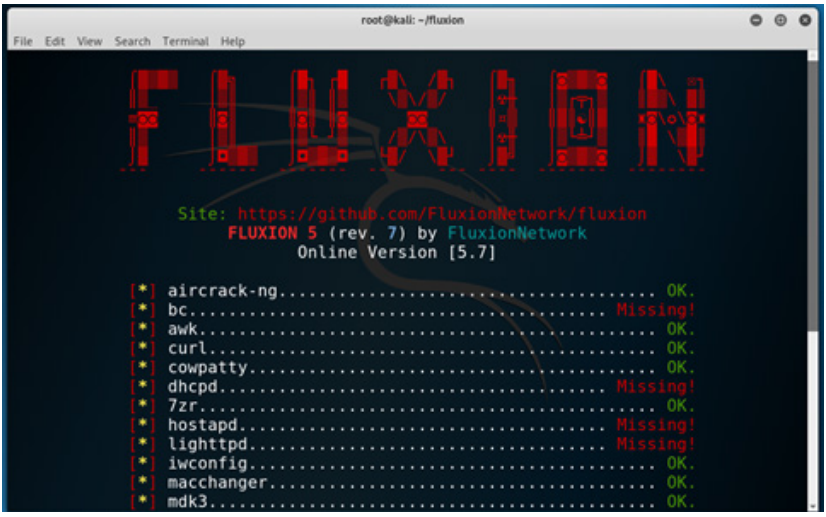

Figure 9. *"Fluxion" tools*

During the initialization of the tool, a loading of the existing tools is done, since this collection of tools uses the ones that are already installed. In the case that a specific solution does not exist, it is possible to initiate downloading of the missing tools. Built-in funtions that are available include (as shown in Figure 10) creation of a virtual Access Point, as a malicious duplicate of the geniune one, which will receive the packet with the password in the form of open text. Another one is "TCP Handshaking Flood", a function that was already covered in the previous part of this section.

7 https://github.com/FluxionNetwork/fluxion

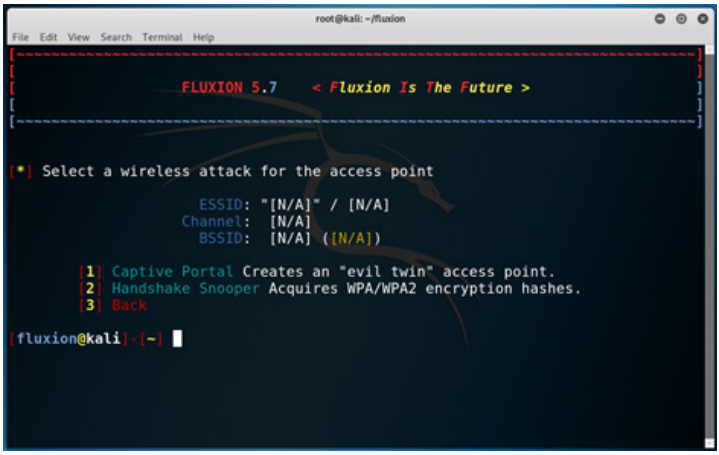

Figure 10. *A window showing a choice for an attack*

By scanning the network, the analysis of the available nearby networks prone to attack is performed. This automated method is done by itself, where the user is simply expected to provide a choice of targeted network.

TCP HANDSHAKING FLOOD

As stated in the earlier part of the presentation, the process of viewing the network traffic is done when the network adapter is in "monitor" mode. The second and third types, shown in Figure 11, are about active way of shutting other devices from the network, which is done through constant sending of SYN packets.

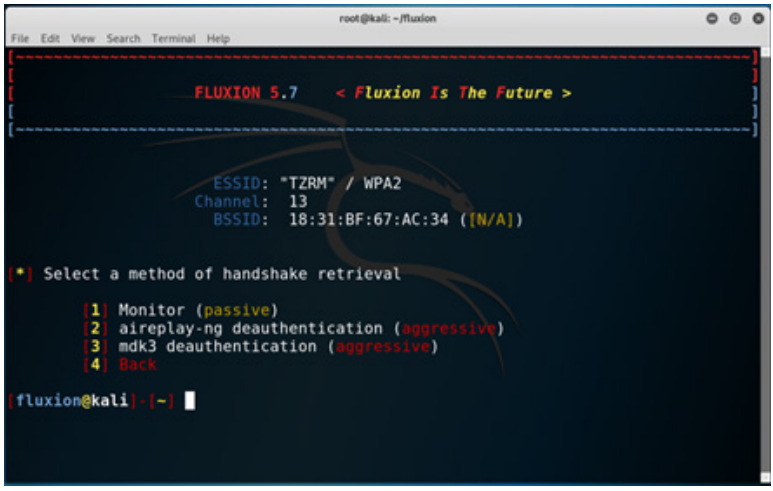

Figure 11. *The choice of methods for deauthentication of the user*

The method of deciphering of packets with credentials is possible, along with the previously used tool "aircrack", by using tools "mdk3" and "cowpatty".

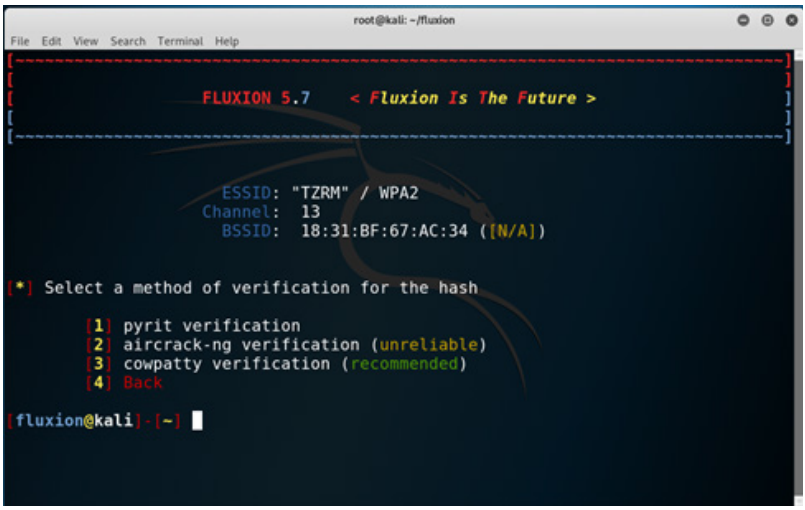

Figure 12. *Types of tools for deciphering*

After selecting the right tool, the automated process for listening (eavesdropping) of the targeted network and its traffic packets, the attack is initiated (Figure 13). Its goal is to deactivate devices from the network in order to force them to reconnect (log back in) when their credentials will be captured and afterwards decrypted.

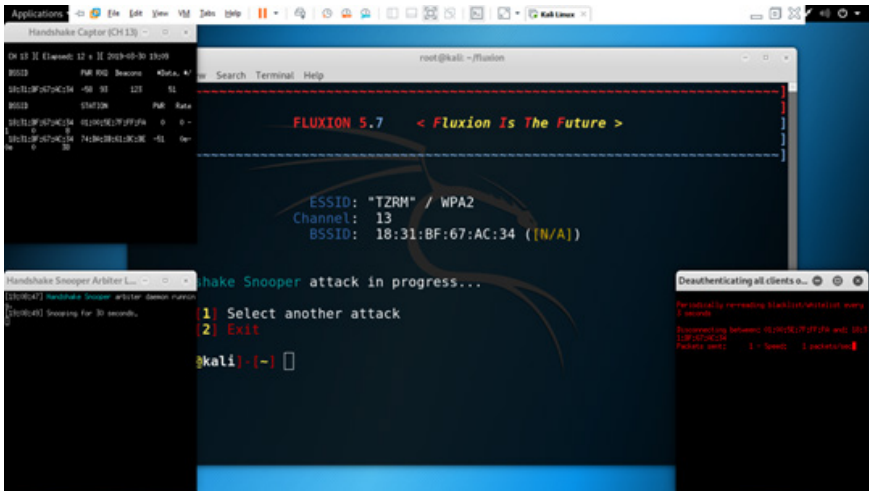

Figure 13. *Iniating an attack*

EVIL TWIN

This type of attack clones the existing station, in which a fake MAC address and name is generated, so that it can fool a user to connect to a fake network and input credentials. This method to a larger extent depends on the user, as it is important for the user to provide log-in credentials to a particular generated station. This method is suitable for use in public locations, where it is necessary to register to the network in order to have internet access.

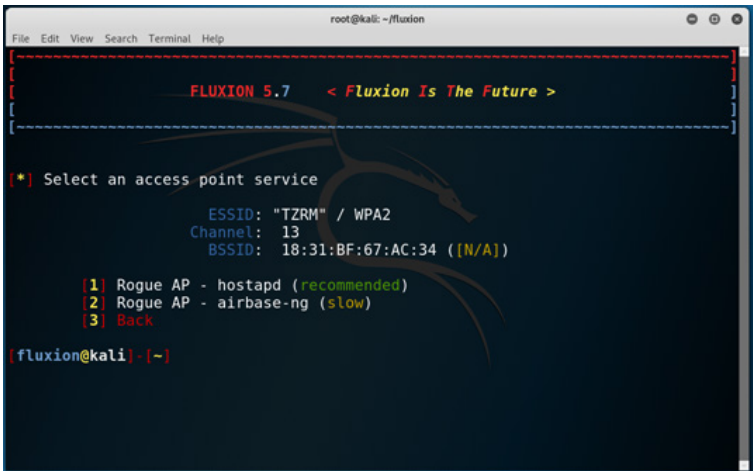

Figure 14. *The choices for a type of generating fake wireless network device*

Access to a page is done through "http" protocol, but the possibility of showing "SSL" certificate exists in order to ensure the user that he is in the mode of safe (encrypted) communication (as shown in Figure 15).

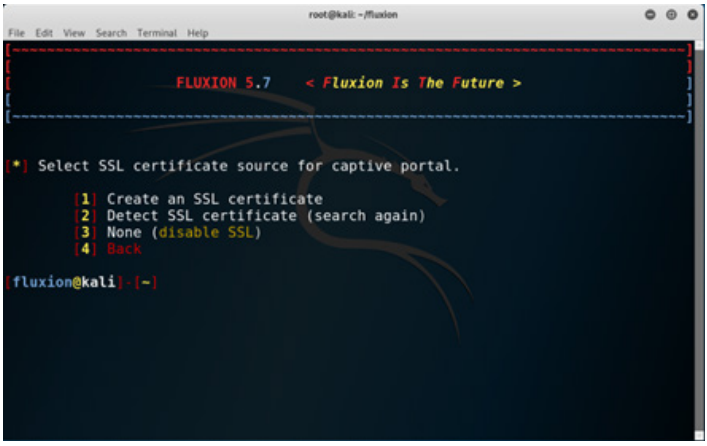

Figure 15. *A selection of creating a digital certificate*

By selecting an option for creating a digital certificate, the user is given an opportunity to choose a type of web page, i.e a type of a generic station where the user will leave their own access credentials (password). In our experiment, a generic page in Serbian is selected (Figure 16).

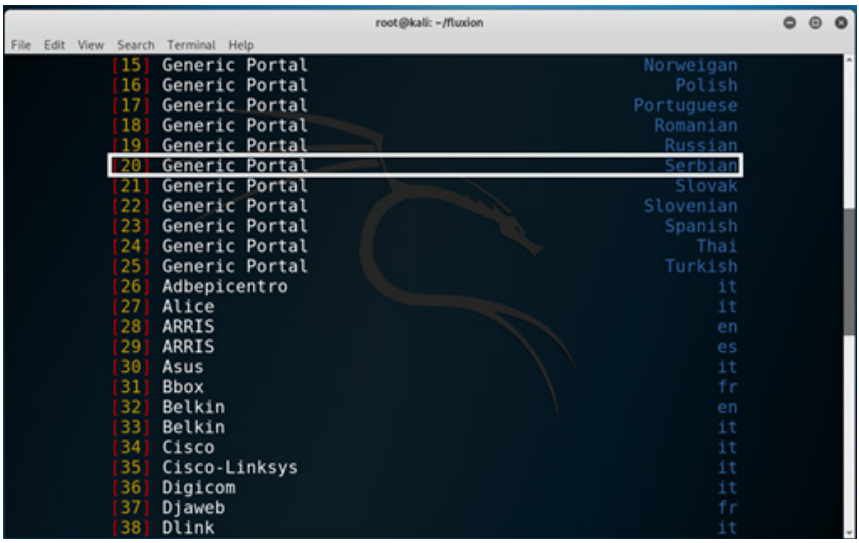

Figure 16. *Possible choices for a generic station*

After this step we enter to the production phase, where SYN packets are frequently sent in order to deactivate (disconnect) valid users. The expected result is that users are going to try to reconnect (log to the network) where they will be forwarded to the (fake) page for validation with the expectation that users will give their credentials to that fake router. This whole process is monitored as shown in Figure 17.

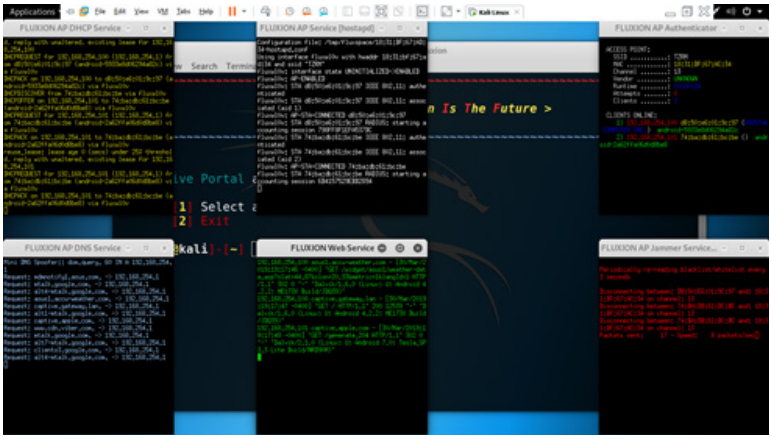

Figure 17. *Monitoring the state of fake routers*

Page display is available in many different languages and it is possible to choose different pages, which are identical to the factory-set pages of service providers, as shown in Figure 18.

Figure 18. *Log-in page*

After logging with credentials, the packet is immediately sent to the attacker where it is stored in a separate file in a form of open (readable) text (Figure 19).

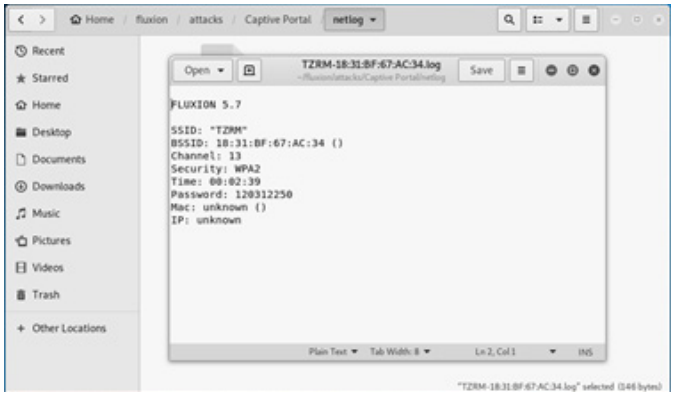

Figure 19. *Text file with parameters for network access*

The attack (hacking) process alone takes approximately 3 minutes, which at first glance seems like a good result. However, the main disadvantage of this approach is that it relies on the user attempt to reconnect, sending the access credentials over the network, which in some situations will not be the case. Sometimes the user will understand that something is wrong and will refuse to attempt to reconnect. Nevertheless, many users, especially in public areas using free wifi spots, will try to reconnect exposing themselves to this kind of attack. Once the attacker is in position to have someone's network access credentials, he can use them in order to perform more attaks with the aim to have access to all data (including private and sensitive) of the targeted user.

CONCLUSION

In this paper we presented two methods recognized as most widely used for attacking the security of wireless computer networks. In every system, the weakest point is the human, who is commonly the main target of the attack. In the first type of attack we performed, human interaction is not needed to a large extent, but the device must already be in possession of network access credentials. It requires more time since the captured packets containing password must be decrypted. The other type of attack we demonstrated requires a greater human interaction, otherwise this attack is useless. The process of disabling (disconnecting) the device from the network and reconnecting does not differ much from the first approach, but what comes afterwards is different. This method forces user to connect to the network with the strongest signal strenght, redirecting him to the login page where he will provide access credentials, meaning that the attacker will be able to get them (in a form of open text) and have immediate access to the network. Since there is a plenty of avalibale integrated tools for attack, requiring little or no knowledge at all, along with software that can be downloaded from "Github" platform, we can confirm that the security of wifi networks is questionable. Therefore, the appropriate measures must be taken in order to minimize their vulnerability. As one of very helpful measures that does not require financing or technical skills is raising the awereness of end-users to this kind of attack in order to be able to protect themselves when using public/open wifi spots.

REFERENCES

1. Kanawat S. D., Parihar P. S., Attacks in Wireless Networks, 2011
2. Beggs R., Mastering Kali Linux for Advanced Penetration Testing, 2014., Packt
3. Allen Lee, Heriyanto T., Ali S., Kali Linux – Assuring Security by Penetration Testing, 2014., Packt
4. Smet D., Pritchett W., Kali Linux – Cookbook, 2013., Packt

5. Ramachandran V., Buchanan C., Kali Linux Wireless Penetration Testing, 2015., Packt
6. Sharma H., Kali Linux – An Ethical Hacker's Cookbook, 2017., Packt
7. Kennedy D, O'Gorman J., Kearns D., Aharoni M., Metasploit – The Penetration Tester's Guide, 2011.
8. Fluxion alat, https://github.com/FluxionNetwork/fluxion, 2018.
Kali Linux, https://www.kali.org/downloads/