KNUV 2016; 3(49): 114-134

Antoni Masiukiewicz, Viktor Tarykin, Vova Podvornyi
Akademia Finansów i Biznesu Vistula – Warszawa

# TOOLS FOR WI-FI NETWORK SECURITY ANALYSIS

## Summary

Wi-Fi networks are particularly vulnerable to attacks from outside. This is due to unrestricted access to communication channels. Carelessness user can help hackers to gain access to confidential data. The level of danger increases when we use the network of unknown random locations. Should we give up the use of Wi-Fi networks? Absolutely not, but everybody has to take precautions and use the tools available to improve safety. The authors discuss the most important risks specific to the Wi-Fi network and selected tools for network analysis and improving safety.

**Key words:** Wi-Fi networks, network security, penetration tests, evil twin.

**JEL codes:** O61, O33, O3

## Introduction

Wi-Fi networks in addition to the mobile telephony is most widely used solution in the area of wireless technologies (Dolińska, Masiukiewicz 2013). In the case of wireless networks in comparison with networks that use media in the form of wires, there is one significant threat to safety. Anyone who is within the signal range may try to break into such a network (Dashkevich 2016; Masiukiewicz et al. 2016). Not all wireless networks are subject to a variety of activities aimed at violation of their safety. It depends on a number of aspects such as applied technology, access to equipment, the price of equipment, software available, how to manage your network, security levels, frequency licenses. Wi-Fi or WLAN is a very interesting and in many ways an easy target for hackers. The frequencies on which 802.11networks work have the nature of ISM (Industrial, Scientific Medical) it means that they are accessible to all users. There is in this case any concept of frequency protecting and each user can transmit and receive at frequencies assigned to the standard. The condition is the use of approved equipment and not to exceed the allowable power level. 802.11 is very often used to connect to the Internet, so that users transmit using this technology relevant information. Device transceiver are widely available and very cheap (Hiertz et al. 2010).

Currently, most Wi-Fi network operates in 802.11b/g/n standard versions at a frequency of 2.4 GHz. 802.11n can operate in the 5 GHz band, however,

because of the need for cooperation with 802.11b/g often it uses the 2.4 GHz frequency. Currently most of produced chipsets are compatible with 802.11n, and it is expected that in the coming years it will be 802.11ac, nevertheless, still when it comes to the market structure of devices currently running a significant place have 802.11b/g chipsets (Aruba 2012). This structure of the market, lead to a situation when most local area networks use the 2.4 GHz band, which is not preferred due to the structure of the physical layer.

Each user can configure his own point of transmission by assigning it any name, doubling the SSID of name of any AP ( Access Point) access point is not carries no formal legal consequences. Many of the Wi-Fi network is a home network. The second common type of Wi-Fi networks are the so-called. hot spots that are generally accessible or available to selected users connection points to the Internet. In the case of Wi-Fi networks we have relatively easy access to the signal produced by the various users and one can easily capture such a signal, as well as send own messages to different users (Rutkowski 2013; Steliński 2013; Smith 2013; Kowalczyk 2014, Kowalczyk 20914). In addition to a number of hackers, the log data in Wi-Fi networks are used by providersof location services (Kuebler et al. 2015; Pan et al. 2015; Damiani 2011, Damiani, Galbati 2012; Dolińska et al. 2015). It is however a broad problem to which the authors of this publication does not relate.

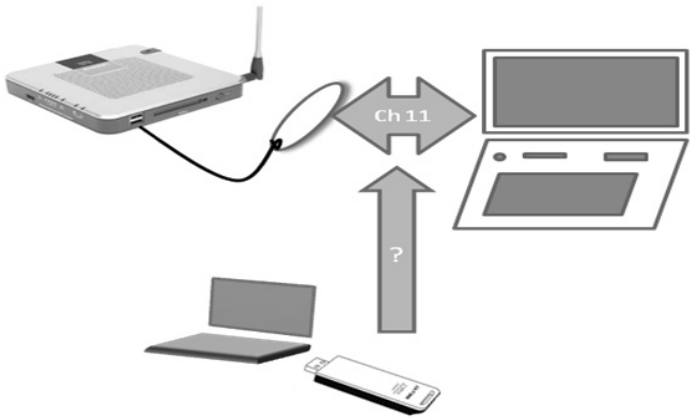
Analysis of the environment of the Wi-Fi network is one of the basic elements to ensure safety. The biggest threat to network 802.11 lies with the other users of the standard. In addressing a number of issues can help you build your own test lab. The laboratory can be built using own network access Wi-F i where a necessary element is a network card, which can operate in monitor mode. Complement the laboratory is additional software. The base may be a dedicated set of tools to test network included in the Kali Linux and additional software, eg. Xiruss_Wi-Fi_Inspector (Masiukiewicz, Szaleniec 2014). Since the part of tools for Wi-Fi network testing is linked to the performance of the so-called. penetration testing it is advisable to obey the formal and legal issues. Making such tests it is allowed on the own network or if the user of the network provide such consent. According to Art. 267 of the Criminal Code (Official Gazette 1997 No. 88, item. 553) to access a foreign telecommunications network without authorization is an offense against the protection of information, the offender shall be liable to a fine, restriction of liberty or imprisonment of up to two years. Paragraph 1 above. the article says that unauthorized persons are not allowed to access to information, which are not intended for them, or avoid or overcome this for protection. In accordance with paragraph 3 above. Do not use the article in the above. the listening purposes any devices or software ("Official Gazette" 1997).

The authors describe the construction of a test laboratory using dedicated to the analysis of network security Wi-Fi Kali Linux distribution, and discussed the selection of actions to improve the safety of the Wi-Fi networks user.

## TEST LABORATORY

Test lab was built using the Linksys router WRt54G3GV2-VF adapted for direct cooperation with the mobile operator's network using eg. HSDPA Huawei E220 modem (Cisco 2008). We use two laptop computers, one notebook which served as a tool for testing and the other was as an element of the network being tested. The laboratory configuration is shown in fig. 1.

**Figure 1. Test laboratory**




Source: own preparation.

Wireless-G Router 3G / UMTS Broadband, provides access to the Internet via HSDPA / 3G / UMTS or GPRS. You can also use a cable modem or DSL modem for broadband services. In addition, this access can be shared over the four switched ports or via the wireless transmission speeds of up to 54Mbps in 802.11g or up to 11 Mbps 802.11b. A variety of security features help protect data and privacy online. Security features include WPA2 (Wi-Fi Protected Access 2), firewall, Stateful Packet Inspection (SPI) firewall and NAT technology. Linksys routers also allow the use of MAC address filtering . With the option enabled MAC address filtering, wireless network access is only possible for wireless devices on the list of MAC addresses created by the administrator of the router. Fig. 2 shows the appearance of the router.

**Figure 2. Router Linksys WRT54G3GV2-VF**


Source: like in Figure 1.

A Wi-Fi network of SSID *ampmmlmas* was built and the key with a length of 26 characters in the hexadecimal code for WPA2 encryption using AES algorithm was automatically generated. For Internet connection a modem E220 Huawei equipped with a SIM card that allows access to the Interne was used. Basic parameters of the modem are as follows:

- modem type: external,
- connector type: USB 2.0 (modem powered from the USB port),
- built-in internal antenna LED indicates the status of the connection,
- supported network: 850, 900, 1800, 1900, 2100 MHz,
- link speed "down" (downlink)
  GPRS: Up to 53.6 kb / s,
  EDGE for up to 236.8 kb / s, Class 10,
  UMTS: Up to 384 kb / s,
  HSDPA up to 7.2 Mb / s.

The vast majority of free tools that are used to detect the gaps and threats in security are the applications running on Linux (Fratepietro et al. 2015; deft. org 2016 deftlinux.net 2016 kali.org 2016). Only for this operating system modified WLAN controllers that allow you to switch the network card in monitor mode, which is necessary to ensure that the network card could receive all data packets, not just those whose are addressed to it , are available. There are some complex .solutions. These include dedicated operating systems in which there is the whole set of tools for network analysis. Table 1 placed most common Linux distributions dedicated to the analysis of network security.

**Table 1. Linux distributions dedicated to security analysis**

| Linux distribution | Webpage | Description |
|---|---|---|
| deftlinux | www.deftlinux.net | Set of several tools for security testing |
| Back Track / Kali Linux | www.kali.org | Set of several tools for security testing |
| caine-live | www.caine-live.net | Set of several tools for security testing |
| SELinux-Security Enhaced Linux | www.selinux.pl | Set of Linux kernel modifications and tools for assigning resources to the applications |

Source: own preparation.

Most distributions include a similar range of diagnostic tools. Kali Linux 2.0 operating system was used for the tests . We tested several possible variants of installation. There are a few solutions according to the different aspects:

– because of the way to run the system: installation or Live CD,
– ue to the type of media: USB stick or CD,
– due to the type of system: the virtual machine or independent installation.

The use of a virtual machine such as Oracle Virtual Box or VMVare has several disadvantages. Application performance is slow, it is necessary to install additional software, there are also problems with setting the external Wi-Fi card in monitor mode. The advantage is the preservation of current data so that you can re-open system and recover data. The discontinuation of operation is a mode that can be called hibernating.

An interesting solution is to use a Live CD or Live USB. LIve CD – is to install the system on the media, ready to run when connected to a computer.

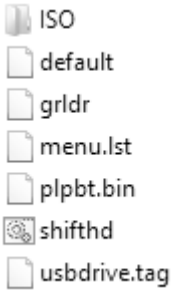
In the case of USB Live for installation media in Windows, download Kali Linux Live and program Win32 Disk Imager, select the virtual image and the name of the USB flash drive.

In a computer running Linux, you can use the command "dd" to copy the disk image to the media:

dd if = kali.iso of = / dev / sdb bs = 512k

The operating system can be installed on a flash drive and run as an independent operating system using the wizard to create multiboot flash drive, which can be downloaded from the http://www.sarducd.it/ (sarducd.it 2016). In Figure 3 shows the contents of memory stick.

**Figure 3. The contents of the USB Flash Drive Live operating system Kali Linux. ISO-folder contains the file Kali Linux-2_0-i386**




Source: like in Figure 1.

If you use a Live CD or Live USB you have set in Windows operating system the correct order of the boot. In XP and Windows 7 can do it in the boot menu but in Windows 8.1 you may need to disable the secure boot and set the boot order in the system options.

Kali Linux is a Linux distribution based on Debian Linux. It is designed for advanced users, those who first have a basic knowledge of the operation of the various distribution using Linux and have a basic knowledge of security (information / computer systems / network / web applications / portable tools etc.). Kali Linux is is a continuation of BackTrack solution. Kali Linux is a set of tools for penetration testing and security audit. It is currently considered to be the most complete set of this type available on the market. It is a tool completely free and so is ideal for users of physical and individual which of course does not limit the possibilities of using it for business purposes. Kali Linux is customizable which means you can change the selected system components and it supports the architecture ARMEL and ARMF (including the Raspberry Pi, BeagleBone, Black and others). Currently available are versions Kali Linux 2 and Kali Linux 2016.1.

Wireless interface can operate in one of three modes:

- normal mode – in the normal mode interface receives a frame whose destination MAC address coincides with the MAC address of the interface,
- promiscuous mode – a mode promiscuous interface receives all data frames that arrive to him from the wireless network to which it is connected, and therefore also those whose destination MAC address does not coincide with the MAC address of the interface,
- monitor mode- is a special monitor mode occurs only in wireless cards, in which interfaces can receive all frames 802.11 that are in the air (from any wireless network being in radio range), the frame monitoring and control.

Not all drivers are able to handle the described mode. During the operation monitor interface is not connected to any wireless network.

In the case of the normal mode and the promiscuous mode, the channel can be adjusted automatically, according to the information broadcast by an access point.. If you work in monitor mode, it is appropriate (manual) setting the working channel of the card, because we are not connected to any network. Thus, all parameters must be set manually.

After the network adapter is implementing a number of tasks assigned to the MAC layer including scanning, authentication, linking and packet transmission. Passive scanning is to browse through the client station all channels for beacon frames, sent out periodically by the access point. Such frame contains information about ESSID and BSSID, channel, the available data rates, and signal strength. Active scan works by sending the client station broadcast probe request frames to which respond with the probe response frame all access points within the radio range.

The customer usually finds a network based on ESSID, which acts as the identifier of the wireless network, which can consist of multiple access points (AP – access point). Each of given network user broadcasts a beacon frames belong to the given ESSID and own BSSID. BSSID, in turn, identifies a specific „cell" of the wireless network, ie. the part of a complex network identified by the ESSID.

The customer finds all APs advertising a membership information to ESSID where you want to connect, and selects the one whose signal is strongest. Since the AP broadcast both ESSID and BSSID, the customer sets in this way BSSID access point to which you chose to connect. Authentication is the process of determining the identity between the stations. In the basic IEEE 802.11 are two types of systems: open system and shared key system, which is based on the encryption protocol WEP, WAP or WAP2. The station sends a frame authentication request, in response to which the AP responds with authentication reply containing the information to grant or deny access.

Client station initiates the connection by sending frames association request, which contains information about the supported data rate, or SSID to which you want to join. AP reserves area in the memory for the connection and assigned ID connection, which is sent in an association response frame-type.

In networks protected by WEP authentication mechanism shared-key uses the same secret key (and the algorithm) as a mechanism for data encryption, which does not offer an additional level of security. It leads instead to the serious security threats, as it is based on:

- transmitting AP random data to the client,
- the client encrypts the data with its secret WEP key and sends the result to the AP,

– AP performs the same operations and compares the result with the received from the customer – if they are identical, this means that the client has used the correct password and is authenticated positively. If the results do not match, the client did not use the correct password and is rejected.

Although in this way the same password is not sent over the network, then sent the same data in a decrypted and encrypted. With the help of a simple XOR transformation can thus read string encryption – also correct from the point of view of mechanisms for the protection of confidentiality.

TP-LINK wireless card WN722 operates on 802.11n (TP Link 2012). With 802.11n technology, TL-WN722N allows transfer speeds up to 150 Mbp / s. It has good resistance to interference and can also work with other versions of the Wi-Fi (802.11b / g). Adapter provides WEP, WPA and WPA2 encryption to prevent intrusion from outside and to protect data. The adapter is equipped with an Atheros AR9271 chipset and can be operated using the driver ath9k_htc adapted to work in Linux. This card can be set to monitor mode, which allows you to receive all the packets in the data radio channel. Appearance network adapter is shown in Fig. 4.

**Figure 4. Wi-Fi adapter TP Link WN722**


Source: like in Figure 1.

Basic commands for configuring and managing the wireless card in Kali Linux are summarized in Table 2.

**Table 2. Commands list in Kali Linux CLI to manage a wireless network adapter**

| Command | Function |
|---|---|
| ifconfig | Looking for wireless interfaces |
| ifconfig [interface_name] up | Start up of interface |
| ifconfig [interface_name] down | Turn off of interface |
| iw list [interface_name] scanning | Looking for wireless networks within the radio range |
| iwconfig [interface_name] | Checking the status of interface |
| iwconfig [interface_name] mode monitor | Setting card to monitor mode |
| iwconfig [interface_name] mode managed | Setting card In managed mode |
| iwconfig [interface_name] channel [chanel_number] | Setting the working nhannel |
| iwconfig [interface_name] essid [network_name] | Link with open SSID |
| iwconfig [interface_name] essid [netwoek_name] key [key_wep_hexa] channel [channel_number] | Link with WEP encrypted SSID with key [key_wep_hexa] on channel [hannel _number] |
| Iwconfig [interface_name] mode managed\|monitor\|ad-hoc | Setting inteface modes |
| Ifconfig [interface_name] [adres_IP] netmask [network_mask] up | Setting IP address |
| airmon-ng | Looping for wireless interfaces- command within *aircrack* which is a part of Kali Linux 2.0 |
| airmon-ng start [inteface_name] | Setting monitor mode |

Source: like in Table 1.

The procedure for preparing the card to carry out listening comes down to the execution sequence of the following activities:

off wireless interface, switching cards in the monitoring mode, re-enable the interface, check the mode Wi-Fi card, set the channel listening, re-check the status of the interface. For wlan1 interface settings in the monitor mode, on channel 6, the command line perform the following sequence of commands:

*ifconfig wlan1 down*

*iwconfig wlan1 mode monitor*

*ifconfig wlan1 up*

*iwconfig wlan1*

*iwconfig wlan1 channel 6*

*iwconfig wlan1*

## Threats in Wi-Fi networks

Threats to Wi-Fi networks to some extent are the same as in other networks. The primary source of threats are three elements: the Internet, e-mail and the ability to capture communications session. What differentiates wireless networks from wired the possibility of intercept and interference by third parties in sessions transmission . Especially voulnerable to this type of threat are Wi-Fi networks. While, carrying out an attack on the LAN, the attacker needs to gain physical access to cable infrastructure, in case of a WLAN can operate unnoticed, found in the immediate area. And if he manages to break into a wireless network, can do various abuses. For example, canuse the Internet link to perform actions contrary to the law. It may look around the local network and try to manipulate devices connected to it, and finally can keep a passive attitude, recording all traffic, and then analyze the data acquired at home. In this way, it will find interesting information such as passwords (Pritchet, De Smet 2013; Dworakowski 2016; Dashkevich 2016; Evil Twin... 2016; Ramachandran, Buchanan 2015). Despite the risk anybody is giving up Wi-Fi communication. Such is the fashion,Wi-Fi is easy to configure and use. Everybody should understand the risks so as to avoid them or minimize the consequences.

Adding own packets by the hacker (Packet Injection) is the second major threat to the Wi-Fi networks . The data concerning the addresses of the network with the command aireplay-ng make it possible to send own packets to different networks. A hacker adapter could injected any packetsinto the network even though the terminal is not connected to an access point for the network. Injecting the packets is possible, but only to one channel at the same time if using one card. Sending deauthentication packets forces all eligible customers to disconnect and reconnect to the AP. This allows, among others, to obtain some informationnconcerning the various networks.

Another threat is to break MAC filtering. When you turn on MAC filtering only allowed MAC addresses are able to successfully pass the authentication process with the access point. If you are trying to connect to an access point device that is not on the white list of MAC addresses, the connection fails. The access point sends error messages to authenticate the rejected clients. In order to break the MAC filter, you can change the MAC address of the hacker so that the MAC address of the card was in the list of authorized MAC addresses.

One of the strongest attacks on the WLAN infrastructure is Evil Twin. As for the introduction of an additional access point in the vicinity of the attacked WLAN. This access point will have exactly the same SSID as the authorized WLAN.

Many users may accidentally connect to a fake access point, thinking that it is part of a familiar AP network. Once the connection is established, the

attacker can perform the attack Man-In-The-Middle and is able to intercept all communications. In the real environment, the attacker must be close to the victim network, so you can get lost and accidentally connected to the network substituted by an attacker. Evil Twin has the same MAC address as the authorized access point is even more difficult to detect and deter. It is also possible falsification of the BSSID and the MAC address of the access point.

The result of packets intercept may be primarily the acquisition of confidential information including various types of passwords that can lead to financial, image and others. losses. The installation of viruses and malware is not a trivial procedure, and the same intercept packets does not cause particular increased risk in this area. It is however possible with Man In The Middle. Attack of the Man-in-the-Middle occurs when coming out of your network packets do not reach the intended target system, but rather someone who acts as an intermediary in communication between the system you and the recipient, but pretend in front of you system recipient and before your recipient. This "man, located in the middle" may in this case be addressed to the recipient other than those sent. Also the response from the recipient reaches the man at the center of that changes the message and sends it to you.

You should also remember that it is possible to break security from MAC filtering to the WAP, WEP, WPA2. WPA2 however is considered as impossible to break, which is true when using the password generated automatically. If for some reason, eg. the desire to have a short password you create your own weak password, then using the methods of dictionary it is possible to break such a password.

## Selected tools for network analysis

the amount of testing tools is infinite. WE have chosen a few examples where criterion was the possibility of their use by the average user. Such a tool is Xirrus Wi-Fi Inspector, free program that allows the analysis of the physical layer, Kali Linux the most popular set of tools for network testing, Nmap (nmap.org 2016 Lyon 2016) program to analyze the network environment, Whireshark packet analyzer and Nessus dedicated software for performing vulnerability testing.

### Analysers of network physical layer

A number of tools are dedicated to the analysis of the Wi-Fi network. The first group are programs that analyze the physical layer of the network. Below (Masiukiewicz, Szaleniec 2014) the parameters and measurement capabilities of several example programs selected for the analysis of Wi-Fi networks are

described. The programs are generally available on the Internet, and their level of sophistication allows use by a normal user. These programs are based on the measurement capabilities of the card implemented in a desktop computer, laptop or other mobile device running the Windows operating system. List of measured parameters may include:

- SSID network name,
- signal level measured in dBm,
- standard type 802.11a, b, g, n,
- the type of encryption WEP/WPA/WPA2,
- the physical address of the device,
- working channel number,
- band used in GHz,
- channel width in MHz.
- maximum network throughput in Mb/s,
- spectral density of the noise power in dBm,
- the ratio of signal power to noise ratio in dB.
- the coordinates of geographical location.

Some of the parameters are analyzed by all programs, and some is optional. Geographical location coordinates are given only in the case where the card used for measuring supports 802.11v standard version ensuring distribution of information of the location of the workstation (IEEE 802.11v, 2011).We tested seven programs that allow analyze of the environment from the point of view of the basic parameters of the network. Table 3 summarizes the information about the programs tested.

**Table 3. Selected information about tested programs for network analysis 802.11**

| Name | Version | Webpage | OS |
|---|---|---|---|
| Xirrus Wi-Fi Inspector | 1.2.1.2 | xirrus.com | Windows: XP, Vista, 7, 8 |
| inSSIDer Home | 3.1.2.1 | programosy.pl | Windows: XP, Vista, 7, 8 |
| WirelessNetView | 1.55 | nirsoft.net | Windows: XP, Vista, 7, 8 |
| Ekahau HeatMapper | 1.1.4.39795 | ekahau.com | Windows: XP, Vista, 7, 8 |
| Common View for Wi-Fi[1] | 7.0 | tamos.com | Windows: XP, Vista, 7, 8 |
| Wi-Fi Hopper[2] | 1.2 | pobieralnia.pl | Windows: XP, Vista, 7, 8 |
| Network Stumbler | 0.4.0 | netstumbler.com | Windows: XP |

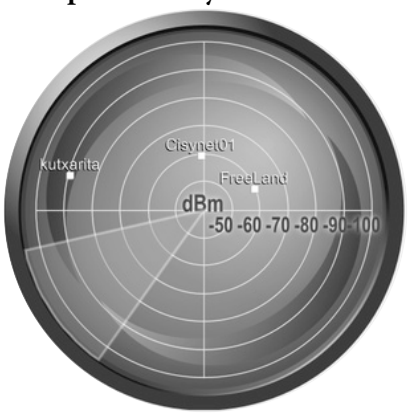
[1] Version of the time, performs the analysis in time for the 5 min from the start.
[2] Trial version.

Source: like in Table 1.

There are a number of scanners of wireless networks. First, each wireless card has a built-in wireless monitor of the environment. It allows to find at least networks within range, and determining the level of received power. Additional

software has generally more functionality. An example of a program to analyze the Wi-Fi network is the Xirrus Wi-Fi Inspector. This is a free program that can work with the built-in card or external card. Fig. 3 shows the capabilities of Xirrus Wi-Fi Inspector.

**Figure 3. Xirrus Wi-Fi Inspector analyzer RADAR window**




Source: like in Figure 1.

Sample measurements are made using the external card AzureWave AW NU-231 using Broadcom 802.11n chipset, and supports 802.11a, b, g, n and band 5 and 2.4 GHz. The program identifies all the networks that are within radio range, limited by noise ratio of – 90 dBm. For each network is assigned SSID, version of 801.11 standard, the received power level , the channel on which works the station and the station address BSSID or MAC address of the access point interface. Some analyzers allow you to identify the location but it is necessary to support the option v or k of 802.11 standard.

## Dedicated Linux operating system

Kali Linux is a Linux distribution based on Debian Linux (kalilinux.org 2016; kali.org 2016). It is designed for advanced users, i.e. those who first have a basic knowledge of the operation of the various Linux distribution and have a basic knowledge of security (information / computer systems / network / web applications / portable tools etc.). Kali Linux is a continuation of the BackTrack program. Kali Linux is a set of tools for penetration testing and security audit. It is currently considered to be the most complete set of this type available on the market. It is a tool completely free and so is ideal for users of physical and individual which of course does not limit the possibilities of using it for business purposes. Kali Linux is customizable which means you can change the selected

system components and supports the architecture ARMEL and ARMF (including the Raspberry Pi, BeagleBone, Black and others). Currently available versions are Kali Linux 2 and Kali Linux 2016.1. Tools included in the Kali Linux are grouped into 13 categories (Table 4).

**Table 4. Tools of OS Kali Linux**

| Category | Tools |
|---|---|
| Gathering information | dmitry, dnmap-client, dnmap-server, ike-scan, maltego, netdiscover, nmap, p0f, recon-ng, Sparta, zenmap |
| Vulnerability tests | golismero, lysis, nikto, nmap, openvas initial setup, openvas start, openvas stop, Unix-privesc-check |
| WEB applications analysis | Burpsuite, httrack, owasp-zap, Paros, skipfish, sglmap, Vega, w3af, webscarab |
| Data base | Bbqsql, hexorbase, jSQL, mdb-sql, oscaner, sidguesser, aqldict, SQLite database browser, sqlmap, sqlninja, sqlsus, tnscvmd10g |
| Passowrds tests | Cewl, crunch, hashcat, John, Joanny, meduza,ncrack, ophcrack, pyrite, rainbowcrack, rcracki_mt, wordlists |
| Wireless | Air crack-ng, chip, cowpatty, fern wifi crack er, gis kismet, gqrx, kismet, mdk3, moc, mfterm, pixiewps, Beaver, wifite, |
| Reverse engineering | Apktool, clang, clang++, dex2jar, edb-debbuger, flasm, jad, javasnoop, NASM Shell, ollydbg, radare2, recstudio, recstudio-cli |
| Exploration tools | Armitage, beef xss Framework, gin guma, inguma, metasploit Framework, searchsploit, social engineering toolkit, sqlmap, termineter |
| Packets analysis | Bdfproxy, drifnet, ettercap-graphical, ferret, hamster, macchanger, mitmproxy, netsniff-ng, Respondek, whireshark |
| Mail analysis | Backdoor-factory, bdfproxy, intersect, nishang, powersploit, proxychains, weevely |
| Forensics | Autopsy, binwalk, bulk_extractor, chkrootkit, dff,dff Gui, foremost, Valletta, md5deep, volafox, volatility |
| Reporting tools | Casefile, cutycapt, dra dis, keepnote, magictree, pipal, recordmydesktop |
| System services | Beef start, beef stop, dra dis start, dra dis stop, openvas start, openvas stop |

Source: like in Table 1.

The vast majority of free tools that are used to detect the gaps and vulnerabilities in security, are applications running in a Linux environment. Only this operating system is able to modified WLAN controllers that allow to switch the network adapter to supervision/monitor mode .

### NMAP

Currently available versions: 7; 6.49 Beta 1; 6.49 Beta 2; etc. NMAP (Network Mapper) free software for analysis and audit network security. NMAP

uses an innovative way IP packets to identify computers connected to the network, services offered for these computers, operating systems which are installed on computers,that systems of packet filtering and firewalls that are used. The analysis may concern both wide area networks and individual computers. NMAP is supported by all the main operating systems: Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga. NMAP contains a number of tools: Zenmap – graphical interface, Ncat- tool for managing the transmission of packets Ndiff – comparison of results, Nping – production and analysis of communication using PING. NMAP can be running on Kali Linux by executing the following statement on the command line:

*nmap [<Scan Type> ...] [<Options>] {<target specification>}*

The result of the scan by NMAP is a list of computers / servers with optional data depending on the options selected in an array on the identified ports. Key information contained in the table of results are:

- port number,
- protocol number,
- name of service / service
- port status: open, closed, filtered, unfiltered,
- details of the software version.

Example command*: # nmap -A -T4 scanme.nmap.org*

where:

- A Identification of the OS and its version of the script to scan, traceroute,
- T4 Improve speed,

scanme.nmap.org name of the computer / server.

## Nessus

Nessus – one of the most popular vulnerability scanners developed by Tenable Network Security. Until 2005, it was free software, open source, but in 2008 a paid version of the product is introduced. Still available is a free version for home networks with limited functionality. Nessus is a tool dedicated to computer security auditors, enabling fixing bugs security based on reports generated by the program. Nessus is available in versions for Microsoft Windows, Mac OS X, Linux, FreeBSD, Solaris. Nessus can also perform scans Web sites and mobile devices, eg. Android. Possible types of scans: PCI Quarterly External Scan, Host Discovery, Basic Network Scan, Credentlaled Patch Audit, Windows Malware Scan Hearbleed & CSS Injection, Web Application Tests, Mobile Device Scan, Offline Config Audliting, Amazon AWS Audit, Perform Network Vulnerability Scans for PCI, Advanced Policy. The software can detect the most common types of vulnerabilities, including:

– presence of weaker version of the service
– errors in configurations,
– weak passwords,
– refusal TCP IP by using specjalnieza using crafted packets.

The program can be from the website Nessus:

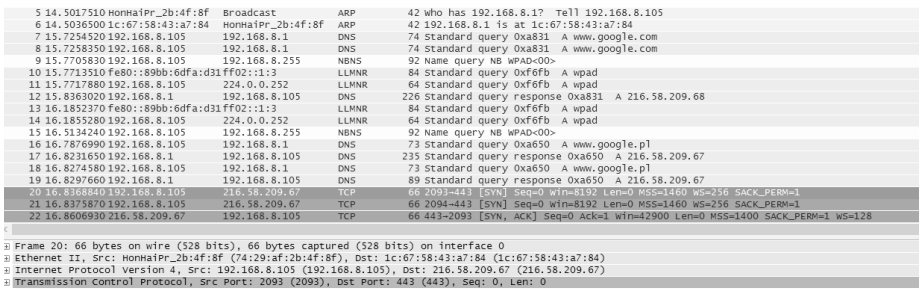
http://www.tenable.com/products/nessus/select-your-operating-system

Then run the installation file dpkg -i Nessus-5.2.5-debian6_i386.deb and finally activate the product using the command /etc/init.d/nessusd start.

## Packets analysis with the use of wireshark

Setting the network adapter in supervised mode allows for setting a separate network interface to which the packets of all stations which are within radio range are delivered. The analysis of such a pcket is possible through the use of analysis tools . There is available a variety of tools for analyzing packets such as airodump-ng, tcpdump, Tshark, Ethereal, Wireshark. The most popular packet analyzer is now Wireshark, which replaced an earlier program Ethereal. Ethereal project is no longer being developed but stable versions are still available. Depending on the level of network security, it is possible to intercept all packets on a particular channel wireless adapter-mode monitor or control only the management packets and control packets. The first situation is possible when you work in an open network without encryption. Fig. 4 shows an example of a set of packets captured in an open network.

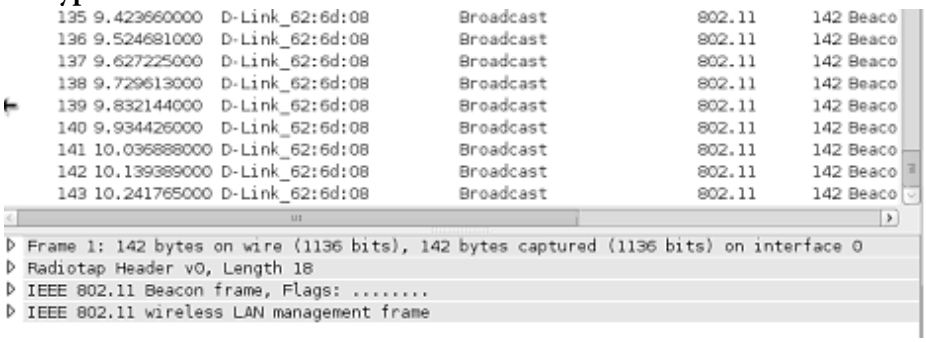
**Figure 4. Set of packets captured in the open network**




Source: like in Figure 1.

When we are dealing with encrypted network (WEP, WPA, WPA2) card receives only the broadcast packets addressed to all users. A sample set of captured packets are shown in Fig. **5.**

**Figure 5. Set of packets received through the working mode, the monitor encrypted network**




Source: like in Figure 1.

Using Wireshark, we can through the network card in supervised mode, we can get access to thousands of packets. Selection of interesting packages is possible by means of capturing results filtration. Filtering packets in Wireshark can be done through using various expressions which helps us to monitor the selected packets of devices, which we are interested in. Packet headers of management and control frames are plain text and not encrypted. Anyone can read these packets and packet headers. It is also possible to modify these packages and re-send, because there is no integrity checks in the protocol.

## Measures improving network security

for the average user the number of possible treatments that improve Wi-Fi network security is limited (Chaładyniak 2009; Dworakowski 2016; Evil Twin 2016; sekurak.pl 2015; Dashkevich 2016; Pritchet, De Smet 2013; Ramachandran, Buchanan 2015; Toxen 2004). We can:

- hide the SSID,
- use MAC filtering,
- use three possibilities WEP, WPA, WPA2,
- to apply anti-virus programs, scanners and monitors,
- analyze the network environment,
- make the right decisions about your Internet connection.

You have to remember that you can get around the various security and antivirus programs, scanners and monitors, especially those that use the database indexes virus can not cope with a number of new threats. Security can be support by programs that use artificial intelligence and heuristic methods. Nothing can replace common sense and the user caution.

In the mode of default configuration, all access points transmit their SSIDs in Beacon frames. As a result, customers in the neighborhood can discover them easily. Hidden SSID is a configuration of the access point does not broadcast its SSID in the beacon frames. Thus, only clients who know the SSID of the access point can connect to it. Unfortunately, this measure does not provide comprehensive network protection, but at least part of your network is hoping that it does.

MAC filters are quite old techniques used for authentication and authorization, and have their roots in the wired networks. Unfortunately, they have not passed the exam in the wireless world. The basic premise of authentication is based on the MAC address of the client. Filter MAC is the identification code assigned to the network interface; the router can check the code and compare it to the list of approved MAC. This list of allowed MAC addresses is maintained by a network administrator and can be given to the access point. Unfortunately, it is easy to get around filters MAC.

When you turn on MAC filtering only allowed MAC addresses are able to successfully pass the authentication process with the access point. If you are trying to connect to an access point device that is not on the white list of MAC addresses, the connection fails. The access point sends error messages to authenticate the rejected clients. In order to break the MAC filter, you can use airodump-ng to find the MAC addresses of clients connected to the access point. Then, after changing the MAC address of the card thief is on the list of authorized MAC addresses.

WPA2 is considered to provide full security. But keep in mind that this is happening when we use the keys generated by the system of the appropriate length. Simplification of the key causes a significant increase in risk. The new solutions should always use WPA2, but the older generation hardware can not support this type of encryption, and then we are doomed to WEP or WPA. In this case, one should reduce the transmission of sensitive information.

To avoid the risk of Evil Twin and Men-In-The Middle we should never use open networks. Newer versions of Windows notify link with an open network and occurrence of threat of loss of confidentiality. For older systems, it is worth checking with tools (eg. Xirrus Wi-Fi Inspector) the status of the network you want to connect to.

In certain situations, the only solution to ensure data security can be disconnection and forget the use of Wi-Fi network in your location.

## Conclusions

Wi-Fi networks are vulnerable to a variety of hacker attacks. The main threat is the availability of all channels to hackers. Currently available technical

measures possible to limit the risk, you can not say, however, to remove the risk. It seems that a very important element, which can significantly improve the safety awareness of users of Wi-Fi networks is the confidentiality of threats. It is impossible to precisely predict all of the risks but you can and must respond to unusual situations and if possible to monitor the network environment.

## References


Aruba White Paper (2012), *802.11ac Technology, Chapter I: Introduction and Technology Overview*, Aruba Networks Inc.

*Bezpieczeństwo aplikacji WWW* (2015), "sekurakoffline", nr 1, http://www.sekurak.pl [access: 03.2016].

Chaładyniak D. (2009), *Podstawy bezpieczeństwa sieciowego, Wszechnica popołudniowa: sieci komputerowe*, WWSI, Warszawa

Damiani M.L. (2011), *Third party geolocation services in LBS: privacy requirements and research issue*, "Transactions on data privacy", Vol. 4, No. 2.

Damiani M.L., Galbiati M. (2012), *Handling user-defined private contexts for location privacy in LBS*, Proceedings of the 20th International Conference on Advances in Geographic Information Systems.

Daszkiewicz K. (2016), Wi-Fi wielki test bezpieczeństwa sieci, "PCWorld", http://www.pcworld.pl/artykuly/400035/Wi.Fi.wielki.test.bezpieczenstwa.sieci.html [access: 04.2016].

Dolińska I., Jakubowski M., Masiukiewicz A. (2015), *Location Ability of 802.11 Access Point*, IEEE sponsored IDT Conference, Żylina.

Dolińska I., Masiukiewicz A. (2013), *Wireless Technologies and Application*, AFiBV, Warsaw.

E*vil Twin – i jak tu ufać hot-spotom? Ofiarą tego ataku może paść każdy* (2016), http://www.dobreprogramy.pl/Evil-twin-i-jak-tu-ufac-hotspotom-Ofiara-tego-ataku-moze-pasckazdy,News,71407.html [access: 03.2016].

Fratepietro S., Rossetti A., Dal Checco P. (2012), *Deft 7 Manual. Digital Evidence & Forensic Toolkit*, www.deft.org [access: 06.2016].

Hiertz Guido R., Denteneer Dee, Stibor Philips Lothar, Yunpeng Zang, Costa Xavier Pérea, Walke Bernhard (2010) *The IEEE 802.11 Universe*, "IEEE Communications Magazine", January.

Julong Pan, Zhengwei Zuo, Zhanyi Xu, Qun Jin (2015), *Privacy Protection for LBS in Mobile Environments: Progresses, Issues and Challenges*, "International Journal of Security and Its Applications", Vol. 9, No. 1, http://dx.doi.org/10.14257/ijsia [access: 03.2016].

Kowalczyk T. (2014), *Android na celowniku*, „Computerworld", nr 22.

Kowalczyk T.(2014a), Skuteczne wykrywanie luk, „Computerworld", nr 22.

Kowalski P. (2013), *Crafty attacks. Efficient defense*, "Computerworld", No. 25.

Kuebler K., Palm D., Slavec A. (2015), *The Ethics of Personal Privacy and Location-Based Services*, (in:) Burkhart L., Friedberg J., Martin T., Sharma K., Ship M. (Eds.), *Confronting Information Ethics in the New Millennium*, http://www.ethicapublishing.com/confronting_information.pdf [access: 16.07.2015].

Lyon G., *NMAP Network Scanning*, http://nmap.org/download.html [access: 03.2016].

Masiukiewicz A., Szaleniec P. (2014), *Pomiary w sieci Wi-Fi*, "Zeszyty Naukowe Uczelni Vistula", nr 38.

Masiukiewicz A., Tarykin V., Podvornyi V. (2016), *Security threats in Wi-Fi networks*, "IRJAES".

„Official Gazette" (Dziennik Ustaw) (1997), No. 88, item. 553 Polish Parliament.

Pritchett W.L., De Smet D. (2013), *Kali Linux Cookbook*, Packt Publishing.

Ramachandran V., Buchanan C. (2015), *Kali Linux Wireless Penetration Testing*, Packt Publishing, 2nd Edition.

Rutkowski P. (2013), *Cibersecurity common responsibility*, "Computerworld", nr 25.

Standard IEEE 802.11v, 2011.

Steliński A. (2013), *Enterprises under pressure: 5 most dangerous threats*, "Computerworld", nr 25.

Toxen B. (2004 ), *Bezpieczeństwo w Linuksie. Podręcznik administratora*, Helion, Gliwice.

TP Link User Guide (2012), *TL WN722N Wireless N USB Adapter Rev. 3.0.0,* TP Link Technologies Co., Ltd.

User Guide (2008), *Wireless-Router for 3G/UMTS Broadband Model No: WRT54G3GV2-VF*, Linksys A Division of CISCO.

http://www.sarducd.it [access: 03.2016].

http://www.nmap.org [access: 03.2016].

http://www.kalilinux.org [access: 03.2016].

http://www.klali.org [access: 05.2016].

http://www.deftlinux.net [access: 03.2016].

http://www.deft.org [access: 03.2016].

http://www.sekurak.pl [access: 03.2016].

# Narzędzia do analizy bezpieczeństwa sieci Wi-Fi

## Streszczenie

Sieci Wi-Fi są szczególnie narażone na ataki z zewnątrz. Wynika to z nieograniczonego dostępu do kanałów komunikacyjnych. Nieostrożność użytkownika może pomóc hakerom w uzyskaniu dostępu do poufnych danych. Poziom zagrożenia rośnie w przypadku, gdy korzystamy z sieci w nieznanych,

przypadkowych lokalizacjach. Czy należy zrezygnować z użytkowania sieci Wi-Fi? Absolutnie nie, ale trzeba zachować środki ostrożności i stosować dostępne narzędzia poprawiające bezpieczeństwo. Autorzy omówili najważniejsze zagrożenia charakterystyczne dla sieci Wi-Fi i wybrane narzędzia pozwalające na analizę sieci i poprawę bezpieczeństwa.

**Słowa kluczowe:** sieci Wi-Fi, bezpieczeństwo w sieci, testy penetracyjne, diabelski bliźniak.

**Kody JEL:** O61, O33, O3

Artykuł nadesłany do redakcji w maju 2016 roku.


Afiliacja:
dr Antoni Masiukiewicz
Viktor Tarykin
Vova Podvornyi
Akademia Finansów i Biznesu Vistula
Wydział Inżynierski
ul. Stokłosy 3
02-787 Warszawa
tel.: 22 457 23 00
e-mail: a.masiukiewicz_globalteam@op.pl