APPLICATION OF FREE TOOLS IN THE PROCESS OF PROTECTION OF WIRELESS NETWORKS

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

Abstract: Users in physical state have mostly gotten used to this view of a computer network, above all due to its price and simplicity of its installation, where with minimal spending results on one network on a high level. However, with the rise of mobile devices comes the need to use its capabilities, and up until now it hasn't been possible to access and execute any of these high-level operations. However, the fact that the complete traffic is done aerially leads users to a question, who is able to access their data. [2]

Wireless technology creates new threats and raises a certain level of compromising of data on a significantly lower level. The complete traffic takes place on radiofrequency waves which comprise over the air which is available to all, unlike communications through older mediums, where the protocol of data is concretely defined. In case of unencrypted data, that is, encrypting with the "weaker" algorithm, the attacker can very easily access the data and compromise the trust of the file. Besides that threat come other negative characteristics of that type of networking. The reach, that is, the geological tracking is not on the visible level, because the user is in someone's sight of "the golden cage", which has the ability to move, that is, to change positions in the network and if nothing is interrupted, while that all restricts it to be in certain range of the access point, as in the case of greater distancing or interruptions on the side of certain objects, where heavier emitting of radiofrequent signals come to a significant influence on the quality, which contributes to the lessening of speed and consistency.

Keywords: cybersecurity, cybercrime, security, wireless network

INTRODUCTION

How are the basic components of the wireless computer network Access Point (*AP*), as the central rope which secures data sharing through the network through radiowaves between on the end of user devices and particular users. In concrete technical-organisational manner, the user does not have a selected role, but in this safe aspect, the user is the weakest link in this chain. The user is the most

common target of the attack. This exception gets in years, or even decades behind, because complete technology establishes that every system gets constructed in a way that can serve its user, above all to ease and execute certain processes. The sole construction of the system and its later implementation can, in a way, rely on the user, whereas the admin of the system usually possesses maximal privileges. These privileges exist most commonly either due to malice or some other factor of abuse, all in the goal of compromising and abusing the system. In a clear example of defense of computer networks, this link comes in as one of the most basic problems. Before projecting the system of defense is that the first principle of defense be simple on the front-end users for understanding, so that opposition to its use does not come up.

The basic factors of the multi-factor authentification are founded on the authentification of users on the basis of[3]:

- What the user knows – password
- What the user possesses – smart card, identification chip
- What the user is – biometric data

These factors can also be combined together, of which security level is raised, but far from perfect, that is impenetrable to threats and attacks. Solutions through chip-based identification, or biometric data requires a significantly more developed infrastructure, where the sole source of biometric data in digital form takes a large portion of memory, so these two solutions are not taken in quality for implementation.

Since a technical capability to commit to this much data did not exist in a relatively short period, it was necessary to find the most optimal solutions, or a compromise of a solution that is the cheapest for implementation and accessible to the users. That solution was the only acceptable use of a password, which is in use to this day. Solution like a step in authentification requires the selection characters to be inputted, so that examination could be done and access be allowed. The input of these commands is a simply possible access point to the network, in case there are no additional settings connected to controlling security, with any device and from any user in the network. Only the sharing of passwords is founded on a particular way of sending, verbal sharing between users, which represents the only layer of and the sharing of models of authentification, which allows access to the wireless computer network. The system of defense depends on cryptological algorithms, which contributes to defense measures on a great level, but in fact is implementing cryptological protocols, try to compensate the faults of this measure of defense. All of these protocols are shown to be implemented, if the end user with their own malice (accidental or purposeful) does not reveal password in plain text, to which attackers are made possible "at hand" to give possibility of the access point.[4]

The possibility of abuse of the user does not represent the only threat on this type of network, as attackers have several goals from the access point, and with that develop their attacks, so that they could damage other links in the system.

THE TERMINOLOGY OF THE ATTACKS

The terminology of the attacks encompass many basic steps which are attempted to be realised in theory is called "*Cyber Kill Chain*", which describes the structure of the attacks[5]:

1. Reconnaissance

Approaching information on potential targets, so that the attacker the target, it is most commonly done through certain webpages, which could present a potential bait for "catching" targets, that is, working pages to which they are accessed. Including followed networks and communications, which are ordered to receive additional information on potential targets

It can comprise of next activities, which can and do not need to be connected[6]:

- Identifiyng targets – ordering selected target of the attack, which reveal which information is committed, which in this case is an individual target being attacked
- Selection – refers to determining greater numbers of potential targets which on the basis of certain parametres become able to decide, these parametres can be united
- Prolification – refers to a string of actions which certain groupings characterising same personalities be instituted

There are two types of reconnaissance:

- Active – the attacker's goal is taking information and generating fakes, exchanging information which is done through the network. In this category includes: *SPAM* messages, *Phishing*, social engineering and scanning ports.
- Passive – the attacker eavesdrops network traffic, does not commit packet exchange, but exclusively commits their later analysis. This type of reconnaissance is difficult to detect, as they are not affecting the network's status, like using packets. Some of the informative tools which are used for this type are: *Shodan, Whois, Censys, Dumpster Diving*

2. Weaponization

This step is done on the side of the attacker, without the interaction with the victim. The attacker creates malicious software, the way the attack would be realised. There are two notable tools for this (*Metasploit* and *Unicorn*).

3. Delivery

The attacker sends a malicious "package", the target is attacked through shared programs, use of social engineering techniques, physical.

4. Activating tools

Execution of scripts on the victim

5. Allowing access

Installation of malicious software on the machine

6. Forwarding commands and controls

The attacker through channels made possible by victim's computer forwards commands on another computer

7. Actions on objects

5 Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Hutchins E., Cloppert M., 2011

6 Technical Aspects of Cyber Kill Chain, Yadav T., Rao M., 2016

The attacker takes over steps on concrete selections, to which they achieve their goal, of which these objects are most frequent: history of payment, logging data, account data and other confidential data.

The goal of discovering this chain of elements and just its defining is indeed on learning countermeasures, from which any of the steps may be prevented. Learning these certain measures can lead to prevention of further consequences of the attack, and learning of other steps. Measures which can be evaluated are:

1. Discovering – confirmation on whether the attacker is commiting reconaissance tasks, like examination of suspicious activities which enables attacker's reconaissance before the attacker.
2. Rejection – prevention of unsolicited breaches in the system, preventing inputting of malicious tools.
3. Interruption – stopping or redirecting outgoing traffic, which prevents finalising changing packets for the attacker.
4. Cancellation – commands which could commit a counterattack, which will be targeted at the attacker.
5. Deception – laying data for the attacker, which will serve as its bait
6. Segmentation of the network – use of techniques of networking gains performance and additional level of security.

Wireless connection represents a significant risk for organisation, as the attacker will not be physically present in company rooms to commit attacks. Wireless attacks can be committed by a malicious user from distant location without the physical presence. With that, the structure of attack and defense differs from classical terminology of attacks[7]. The terminology which could be used for wireless computer network would be comprised of the next steps:

1. Discovery – the emiting of signal is done to which tools are used like: *NetStumbler*, *NetSurveyor* и *Xirrus Wi-Fi Inspector* like other tools which are used for scanning suitable networks in range and strength of the signal.

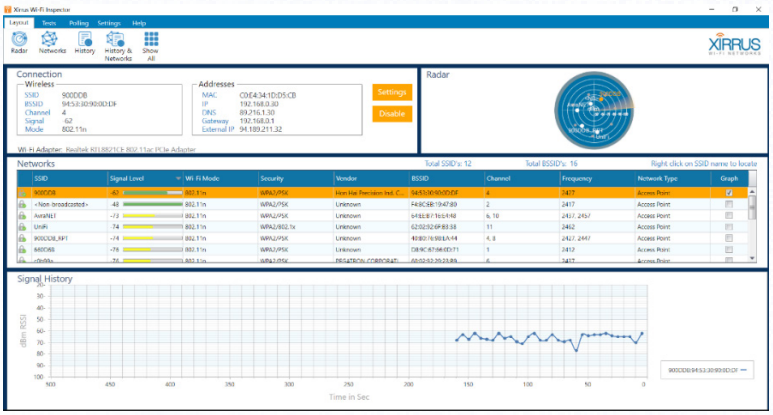


Figure 1. *Display of tool Xirrus Wi-Fi Inspector for scanning available networks and signal strength*

2. Mapping – once the list of wireless computer networks (*Wi-Fi*) is displayed, it can geographically visualise through geographic maps. „*WiGLE*" is one such service based on the webpage, which accepts information on networks from scanners and shows the networks on a map.

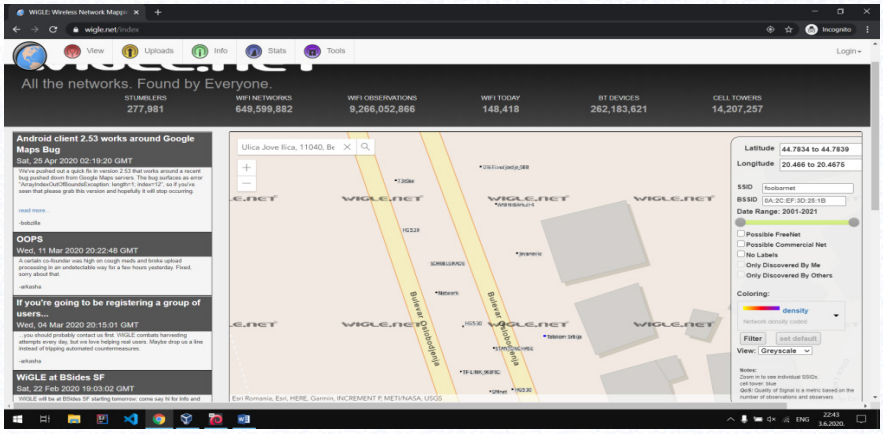


Figure 2. *Display of tool for mapping available wireless computer networks Wigle*

3. Analysis – setting tools for following activity of network traffic. Manufacturers of operating systems have foreseen potential security threats, so "*Microsoft*" before creating its own operating system allowed following (eavesdropping) traffic, but does not allow putting packets in. While operating systems "*Linux*" allow both functions. The tool that makes it possible to do is „*Aircrack-ng*" (on the condition it has an appropriate network adapter with the possibility of the *Monitoring* mode). The tool which is supported on more operating systems is „Wireshark".

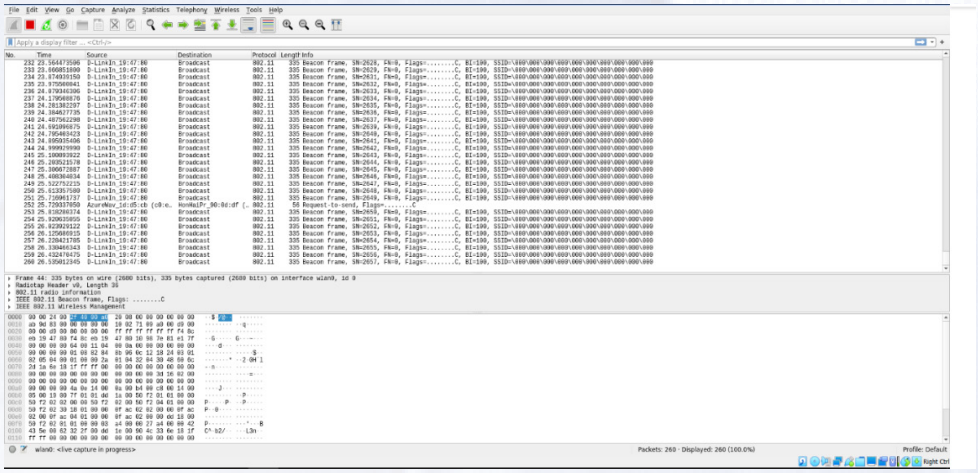


Figure 3. *Display of tool for analysing networks Wireshark*

4. Executing an attack – after fulfilling conditions for executing an attack come the possibilities for final realisation of the attack. The choice for the attack depends on the attacker and the goal needed to meet:

a) MAC Spoofing – access points have an ability of filtering *MAC* addresses which means that on a wireless network can only be connected by devices whose *MAC* is in a whitelist. Changing the network adapter also leads to changing the *MAC* address. With the help of the tool „*SMAC*" exchanging addresses can be done, generating virtual network adapter.

b) Attack on authentification – this type of attack is used for pre-meditated shutting of a user who are legitimately logged on selected access point.

c) Man in the middle – in this type of attack, the attacker first deactivates the active legitimate user from the access point, and then forces the victim to connect to the fake access point, and by the end intercepts all data which victim and receives during the session.

5. Probing encryptions – searching for the encryption key which is used on a wireless computer network. Using a toolset „*Aircrack*“ makes it possible to execute probing the secret encryption key.

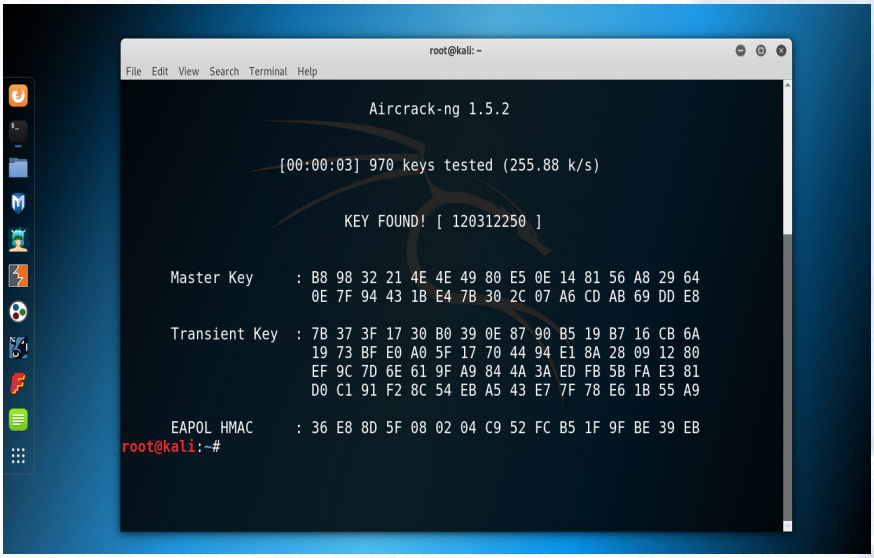


Figure 4. *Display of tool for probing encryption Aircrack*

Terminology of wireless computer network defense is turned to the following string of next steps:

1. Consideration – establishing a polis is done, right of access, separating a certain part of the network for „guests“
2. Discovery – ordering a degree of discovering/hiding *SSID* of adjacent access points, filtering *MAC* address, establishing a naming convention, establishing necessary tools for protection
3. Encryption – establishing a secure protocol for encryption
4. Testing – phase in which simulation of potential attacks is done and examining established aspects of defense. In this step we have two types of targets in which simulated attacks are done:
    a) Access point – attacks are done here on access point, and those are attacks of deauthentification of the user, *DOS/DDOS*, spoofing *MAC* address, *Evil-Twin*
    b) User – attacks which are based on human weaknesses and using particular moments of impatience and are done by Man in the Middle, following traffic, methods of social engineering
5. Analysis – on final testing the analysis of the status is done and evaluation of potential improvements.

ATTACKS ON WIRELESS COMPUTER NETWORK

Often in practice are two terms for labelling grouping for attacks used, where individual attacks are grouped by combined characteristics and the way of committing in the next categories:

- Active attacks – where the goal for the attacker changes data and generate spoofed changes of informations, which are transmitted through the network. In this group of attacks come attacks which are more commonly called: *Unauthorized Access*, *Active Eavesdropping*, *Man in the Middle Attack*), *Session Hijacking*, „*Denial of Service*“, acronym „*DOS*“ and *Replay*

- Passive attacks – the attacker eavesdrops network traffic, does not commit packet exchange, but exclusively commits their later analysis. Passive attacks are difficult to detect, as they are not

affecting the network's status, like using packets. This type of attack uses a weakness of free range of information aerially, where the user, or rather an access point, cannot detect exchanges, as there are none, as it has to do with the impact of normal function of the network. This could be characterised as another weakness, as exclusively detection of packet exchanges or interruption of signal is characterised as an attack. In both groups can attacks be detected through *Traffic Analysis* and *Passive Eavesdropping*.

WIRESHARK

"*Wireshark*" is a free tool for scanning and analysis of networks, following communications, receiving and sending network packets and sights. This tool is used for network analysis of a packet and following traffic and activities in network's frame. It's used largely in the framework of support of solving network problems, where a source of certain problems can be found, compared to the desired status with real, and comparison analyses. Examining of application repair, where programmers can see a way of application's behaviour which use secure or networked protocols, for their control and higher development. Following packets for security reasons is one of the functions which is used to a large measure, as with this examination a detailed analysis is done and it is possible to look into certain parametres which can mark certain faults in great measure in the network.[8]

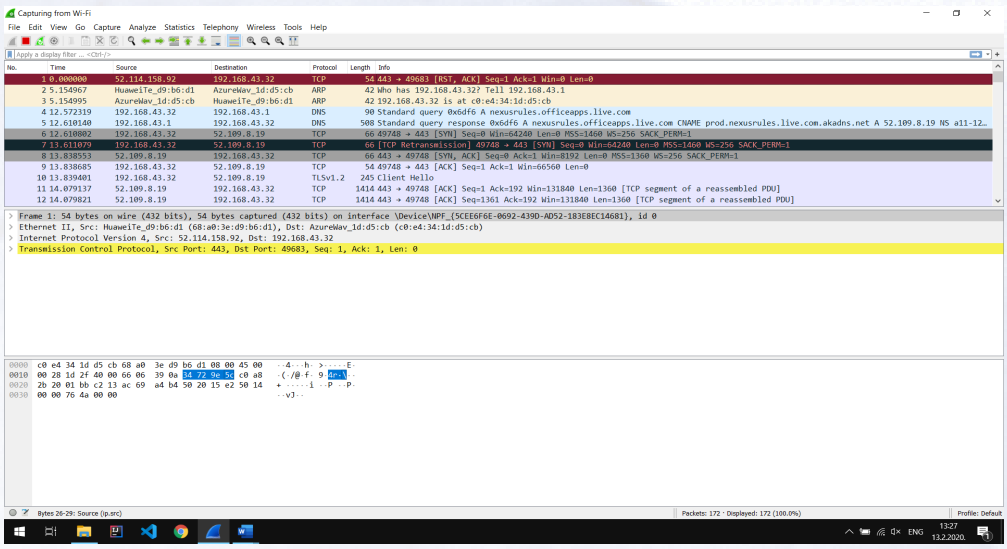


Figure 5. *Display of recording packets through tool „Wireshark"*

Every packet represents in the frame of one column, meaning it is possible to get information from the receiver, sender, protocol, length and just information on the packet. The platform is very useful, because it is visually accessible to the user, so they could better identify types of packets, protocols, and certain anomalies. Protocols are divided by colours, where "*TCP*" packets represent green, "*UDP*" blue, and in case of certain faults or anomalies are represented in red colour, this display is possible to change depending on the user. Display of analytic data, which pertain to activity of traffic in the frame of wireless computer network is one of the options, so that the user could get the big picture of the traffic protocol through a network.

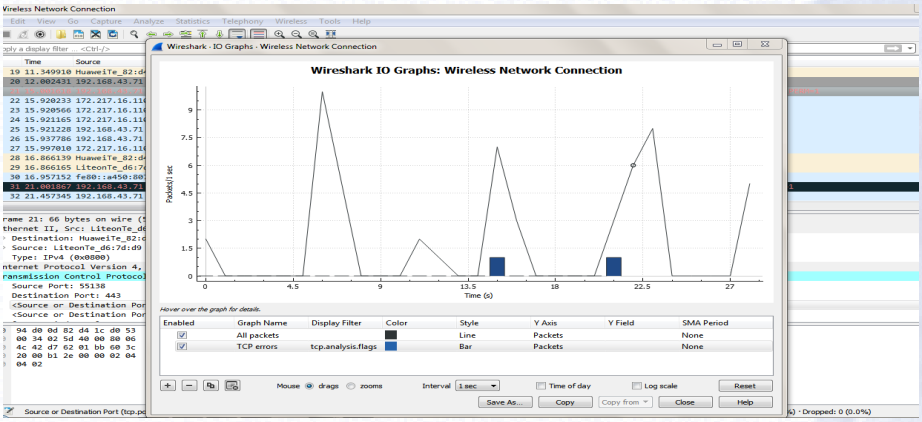


Figure 6. *Display of generated graphic following traffic activity*

ACRYLIC WIFI

Represents the pool of tools which enables following statuses of wireless computer networks. These tools makes network analysis possible, where details of access points can be examined, signal strength, security protocols, packet density. Because this version of the software is commercial, certain functions are available exclusively to select users, while the free version of the software only has basic information on the network status. Examination and control of the device connected on the network, and their geolocating, on the basis of signal quality which comes to them can be useful in the case of following and controlling a certain number of devices, and potential defenses from unauthorised devices. In the process of working with this tool is the free version used, which in a passive way can look at certain more detailed information on access points, but an accent is put on the quality of a signal and rates cryptographic protocols. It is compatible to *Windows* operating systems.

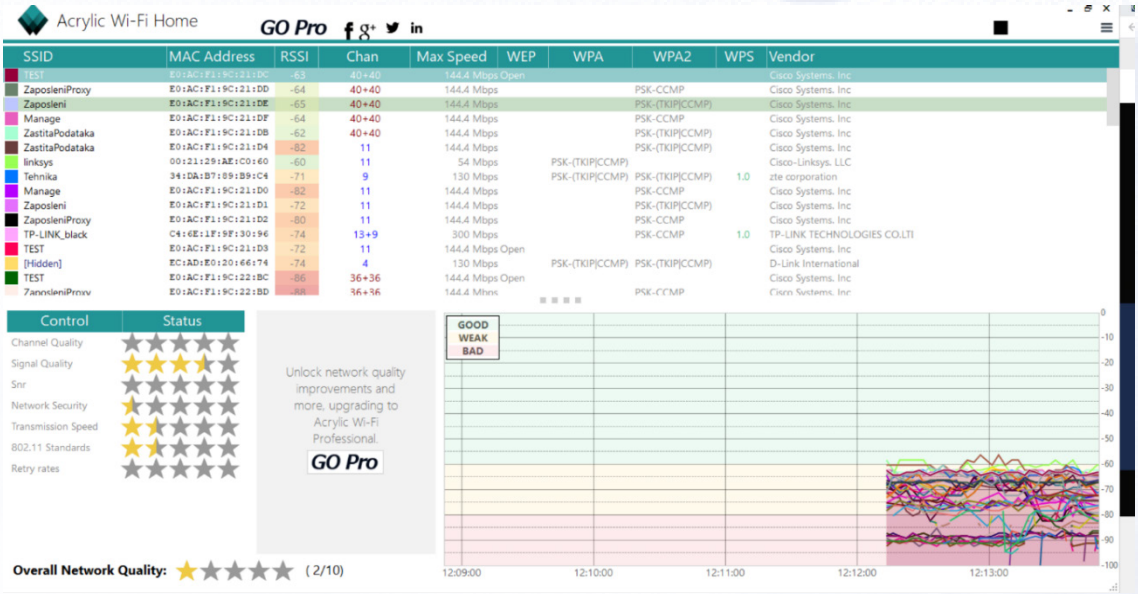


Figure 7. *Display of tool for network and signal analysis Acrylic WiFi*

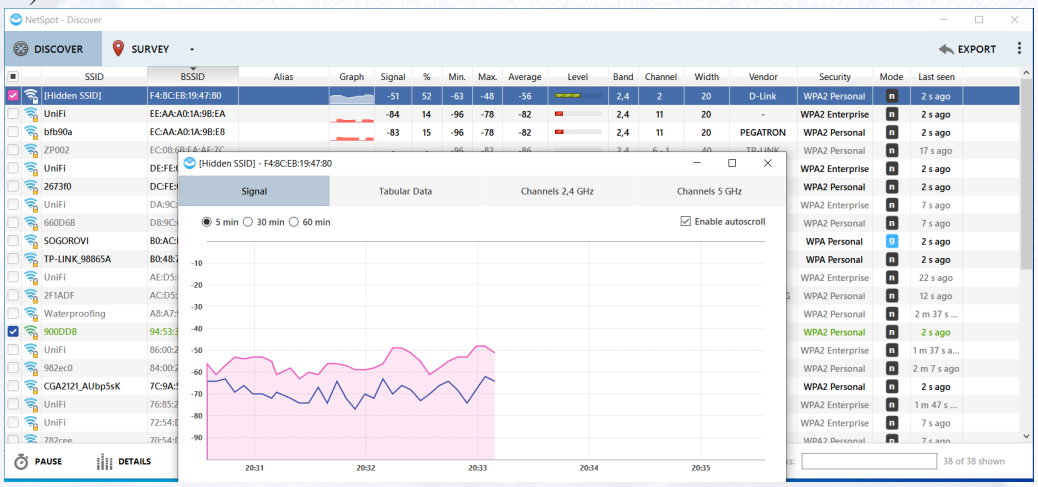
NETSPOT

A tool meant for monitoring statuses of wireless computer networks which brings user examination of availability of wireless computer networks. Besides basic data on the network (*MAC*, *SSID*, security protocols for encryption), there are also other features for users, which deal with statistical displays and signal strength inside a network. This tool works in two modes[9]:

1. Discovery – mode for discovering available networks in the area with data pertaining to signal quality and type of defense
2. Survey – mode for surveying places, that is visualisation two-dimensial display of a device place, in which couverage is examined, speed, quality of a signal and potential blocks from interference.

This tool is an optimal solution for institutions and professional workplaces, where it is necessary to have a coverage of the place, for optimisation of resources. The tool is free to download and supports *MAC OS X*.

a)



b)

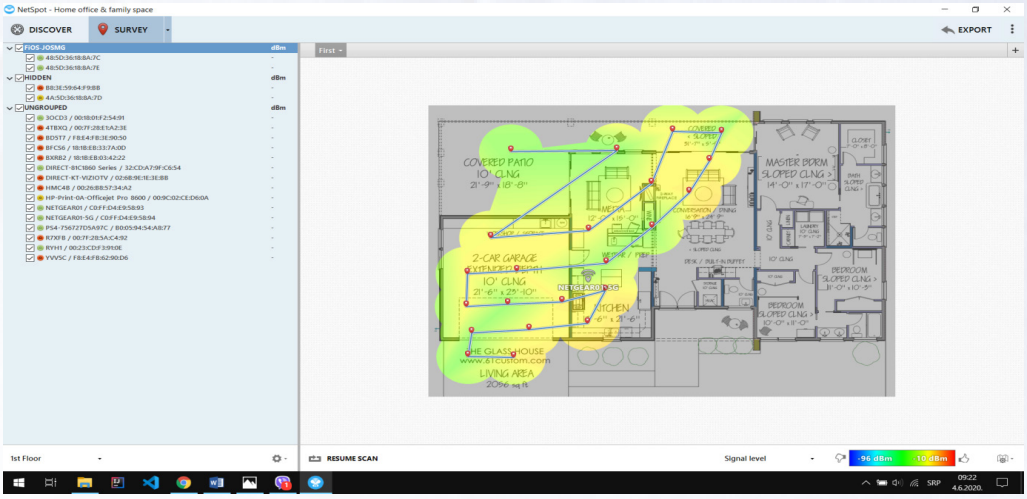


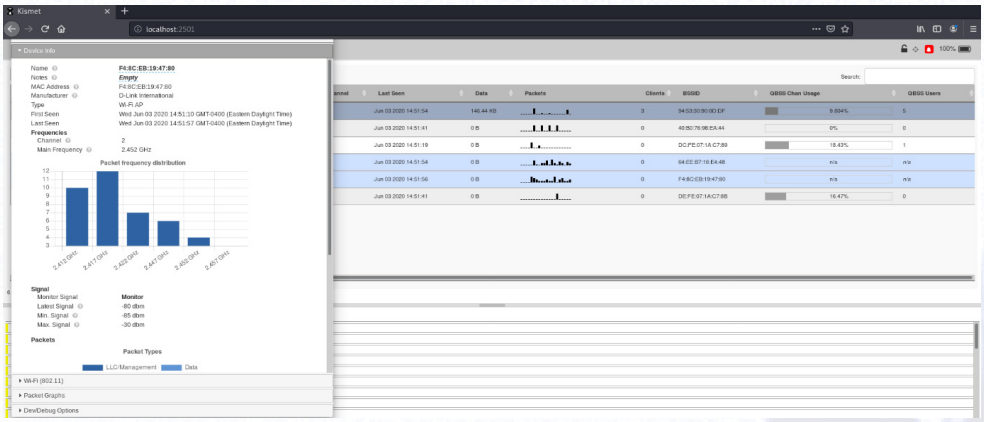
Figure 8. Display of NetSpot tools with overlaid view of an architecture of a place and signal range a) Discovery mode b) Survey mode

KISMET

This tool falls on a group of tools which are used in "*Kali Linux*" operating system. „*Kismet*" is an open-source tool which scans networks, following packets, detections of activity in a wireless network, detections fall on a network. For a successful functioning of these tools, it is necessary to possess a networking interface which supports *Monitoring mode*.

Visualisation of a display of packets and data, eases the user just following network activities, where in activity of the packet protocol is their presentation done. With this tool, the user can have a visual in suspicious activities in the network frame, data on devices which are connected, their use of networks, and the potential malicious attempts breaches from an attacker.[10]

a)



b)

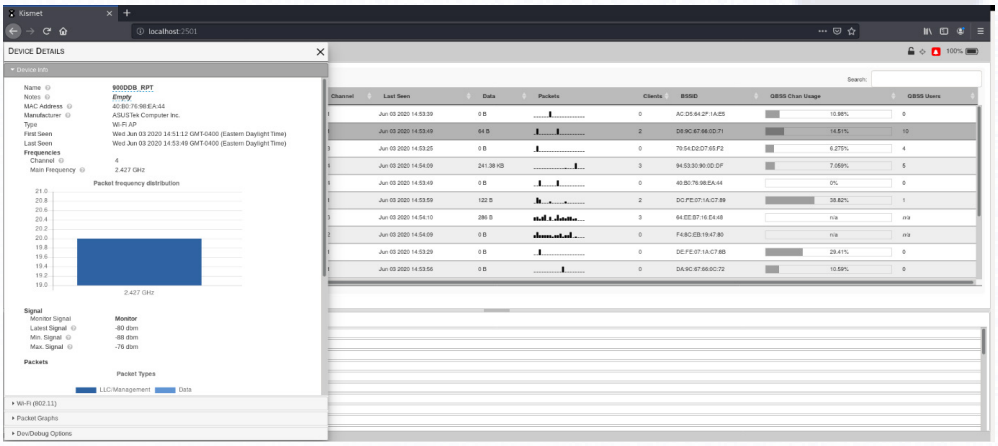


Figure 9. Display of window „Kismet" tool
a) network taken by a DOS attack б) network not under attack

PRTG NETWORK MONITOR

This tool is developed by a company "*Paessler*", so the acronym means „"*Paessler Router Traffic Grapher*". The software is used for overseeing and classification of individual parts of a system connected to a network, like a range, packet activity, but the main feature is collecting statistical data of network

components, through switches, routers, servers and other devices and applications so that a complete picture of potential activities and alarms can be gotten in case of unwanted effects[11]. The mode of automatic scanning does not require from a user to do manual types of scanning, but rather it is expected that in a certain measure sets fields which could be first showed and in which software to pay attention to. The software offers a free trial use from calendar days, which after that requires payment.

In the frame of investigating the tool is used in the process of a "*DOS*" attack, which the software timely felt a significant increase in *ping*, which automatically means that a problem was found. The visual of a problem is examined, where with a graphic diagram which a gradual spike can be seen, which is clearly differentiating from previous status.

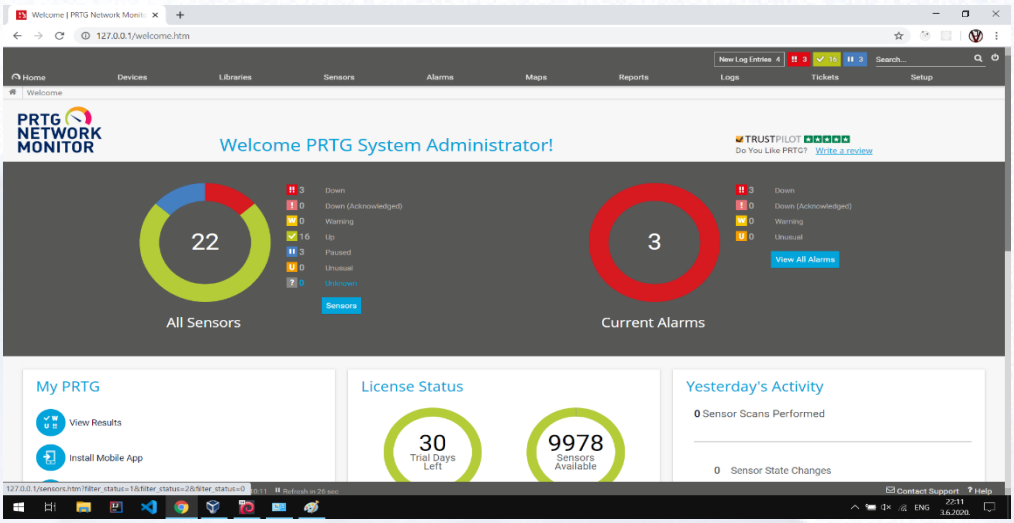


Figure 10. *Display of starting form of tool for monitoring networks PRTG Network Monitor*

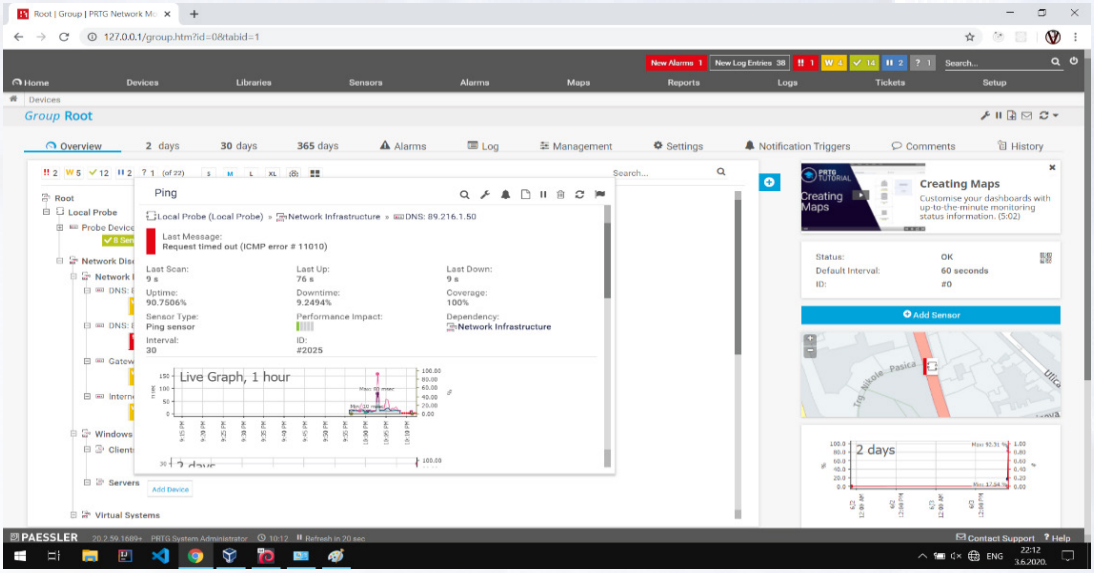


Figure 11. *Display of a detailed examination of alarmed parts of the system, where a graphical display of a call and reasoning for an alarming*

The control for the user would present a frame which could be usable in both cases (for wireless and wired computer networks), where the concrete "*MAC*" device address is ordered to be connected to a network and besides the knowledge of the credentials. The supervision of the network like its exam-

ination is with the help of tools like "*Wireshark*" able to detect certain anomalies in traffic and packets shared through the network. Use of the system detection and prevention of breaches in the network is integrated in such tools like "*Kismet*", which the examination of activity and packet amount is done in "*Kali Linux*" operating system, which is possible to react in case of increased amounts of requests or fluctuations of the same packets. The presented tools, whose work is presented are based on an analysis of all network, which is expected by users to actively react to attacks and potential anomalies on the network. Tools which are made possible to work even on "*Windows*" operating system are available to the whole auditorium of the user. "*Acrylic WiFi*" is a tool which is exclusively aimed at analysing signals and which could help the user over potential evaluation of available network on the basis of certain parametres, pertaining to signals, security, potentially low range, forests etc. The user could find it useful before examining potentially malicious networks with suspicious degrees of protection, forests, where it could be concluded that is done on a malicious attempt. "*NetSpot*" is a tool which could be put into a group for projecting the architecture of wireless computer networks on an individual level. The possibility of bringing maps, could show possibility of calculating in realistic conditions and free calculations of signal coverage, where it is possible to get answers on questions on where to put access point, so that a more optimal and secure signal flow could be made possible. "*PRTG Network Monitor*" is a tool which could be put into this category, as it pertains to a commercial tool, but gives a possibility of complete examination of status and reacting to alarming activities, which are detected through calls. Active eavesdropping of the status contributes to a fast reaction, which besides examined threats are certain advises to the user also done, with potential solutions. Statistical collection and examination of data contributes to a future analysis of status and advancing to parts of the system where the outage was made. Rates are given by parameters not enough (1), enogh (2), thoroughly (3).

Table 1. *Display of evaluation tools*

	Display encription types	Operating systems	Package analysis	Visualization of channel activities	Responding of attacks	Monitoring	Rating
Wireshark	1	3	3	2	2	1	2
Acrylic WiFi	3	1	1	2	1	2	1,67
NetSpot	2	2	2	2	1	2	1,83
Kismet	3	1	2	3	2	3	2,17

CONCLUSION

The present terminology of attacks (*Cyber Kill Chain*) is established, so that a system of defense could also be uniformly defined, which is founded stopping individual parts of the chain. The use of tools for scanning and testing surrounding networks (*Acrylic WiFi and NetSpot*) is it possible to establish access to malicious and suspicious clones of the network, which are activated on the intention for redirecting traffic to them. After potential committing of an attack (i.e. *DOS*) the tool "*Kismet*" examined and showed a raised level of traffic and channel takeover, which the interruption of network, where the user can see that they are in the target of the attack.

Each of these presented solutions require a certain degree of administration, so the end user is not able to expect a total automation of these functionalities, which would be prevented, that is, removed an unauthorised attack on a wireless computer network.

It is necessary to establish a clear principle of defending computer networks, as the fall of network infrastructure, leads to fall of the whole system. A question is made on the amount of contribution to system defense that open-source tools have, which could be available to anyone, and just that advanced in certain segments. Operating system of open-source "Linux", as one of its versions offers "Kali", which is aimed towards ethical hacking, because it provides tools of open-source for the realisation of various tests, but can also be used for defense.

REFERENCES

1. Wireless Security Threat Taxonomy. IEEE Workshop on information assurance, Welch D., Lathrop S., 2003
2. Multi-Factor Authentication: A Survey, Ometov A., Bezzateev S., Mäkitalo N., Andreev S., Mikkonen T., Koucheryavy Y., 2018
3. Wireless Network Security: Vulnerabilities, Threats and Countermeasures, 2011
4. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Hutchins E., Cloppert M., 2011
5. Instant Wireshark Starter, Singh A., 2013
6. Technical Aspects of Cyber Kill Chain, Yadav T., Rao M., 2016
7. Modified cyber kill chain model for multimediaservice environments, Kim H., Kwon H., Kim K., 2018
8. Analysis of the Coverage Area of the Access Point UsingNetspot Simulation, Suryani A., Pantjawati A., 2018
9. A Study on the Kismet-Based Wireless Intrusion Prevention System, Kim C., Xun C., Jung H., 2016
10. Network Monitoring Tools and Techniques uses in the Network Traffic Management System, Rahman W., Nguyen P., Rusliyadi M., Lydia E., Shankar K., 2019
11. Xirrus Wi-Fi Inspector, https://www.techspot.com/downloads/6901-xirrus-wifi-inspector.html, 2020
12. WiGLE, https://wigle.net/, 2020
13. Aircrack, https://www.aircrack-ng.org/doku.php?id=cracking_wpa, 2020
14. Wireshark, https://www.wireshark.org/, 2020
15. Acrylic WiFi, https://www.acrylicwifi.com/en/wlan-wifi-wireless-network-software-tools/wlan-scanner-acrylic-wifi-free/, 2020
16. Netspot, https://www.netspotapp.com/, 2020
17. Kismet, https://www.kismetwireless.net/, 2020
18. PRTG Network Monitor, https://www.paessler.com/, 2020