Ministry of Education and Science of Ukraine

Odessa National Academy of Food Technologies

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2021

Information Technology, Automation and Robotics

Proceedings

Odessa, ONAFT 2021

UDC 004.01/08

Editorial board:

Black Sea Science 2021: Proceedings of the International Competition of Student Scientific Works. Information Technology, Automation and Robotics. / Odessa National Academy of Food Technologies; B.Yegorov, M. Mardar, S.Kotlyk (editors-in-chief.) [*et al.*]. – Odessa: ONAFT, 2021. – 526 p.

These materials of International Competition of Student Scientific Works «Black Sea Science 2021» contain the works of the contest participants in the section «Information technologies, automation and robotics» (not winners).

The author of the work is responsible for the accuracy of the information.

Organizing committee:

Prof. Bogdan Iegorov, D.Sc., Rector of Odessa National Academy of Food Technologies, Head of the Committee

Prof. Maryna Mardar, D.Sc., Vice-Rector for Scientific and Pedagogical Work and International Relations of Odessa National Academy of Food Technologies, Deputy Head of the Committee

Prof. Stefan Dragoev, D.Sc., Vice-Rector for Scientific Work and Business Partnerships of University of Food Technologies (Bulgaria)

Prof. Baurzhan Nurakhmetov, D.Sc., First Vice-Rector of Almaty Technological University (Kazakhstan)

Prof. Mircea Bernic, Dr. habil., Vice-Rector for Scientific Work of Technical University of Moldova (Moldova)

Prof. Jacek Wrobel, Dr. habil., Rector of West Pomeranian University of Technology (Poland)

Prof. Michael Zinigrad, D.Sc., Rector of Ariel University (Israel)

Dr. Mei Lehe, Ph.D., Vice-President of Ningbo Institute of Technology, Zhejiang University (China)

Prof. Plamen Kangalov, Ph.D., Vice-Rector for Academic Affairs of "Angel Kanchev" University of Ruse (Bulgaria)

Dr. Alexander Sychev, Ph.D., Assoc. Professor of Sukhoi State Technical University of Gomel (Belarus)

Dr. Hanna Lilishentseva, Ph.D., Assoc. Professor, Head of the Department of Merchandise of Foodstuff of Belarus State Economic University (Belarus)

Prof. Heinz Leuenberger, Ph.D., Professor of the Institute of Ecopreneurship of University of Applied Sciences and Arts (Switzerland)

Prof. Edward Pospiech, Dr. habil., Professor of the Institute of Meat Technology of Poznan University of Life Sciences (Poland)

Prof. Lali Elanidze, Ph.D., Professor of the Faculty of Agrarian Sciences of Iakob Gogebashvili Telavi State University (Georgia)

Dr. V. Kozhevnikova, Ph.D., Senior Lecturer of the Department of Hotel and Catering Business of Odessa National Academy of Food Technologies, Secretary of the Committee

The jury for the section «Information technologies, automation and robotics»

Head of the jury:

Sergii Kotlyk – Ph.D., Associate Professor, Director of the P.M. Platonov Educational-Scientific Institute of Computer Systems and Technologies "Industry 4.0" of Odessa National Academy of Food Technologies (Ukraine)

Members of the jury:

Piotr Artiemjew - Dr hab., Associate Professor in Decision Systems of the Faculty of Mathematics and Computer Science,University of Warmia and Mazury in Olsztyn (Poland)

Francisco Antonio Augusto – Dr., International Relations Manager of Higher Institute of Information and Communication Technologies (Angola)

Andrey Kuprijanov – Ph.D., Associate Professor of the Department of Software for Computers and Automated Systems of Belarusian National Technical University (Belarus)

Simon Milbert – Vice-President of Xtra Information Management, Inc. (USA)

Ivan Palov – D.Sc., Professor of University of Ruse "Angel Kanchev" (Bulgaria)

Degla Gérard Hugues – Communications and Training Manager of "MAPCOM solutions informatiques" company group (Benin)

Nugzar Kereselidze - Academic Doctor of Informatics (Computer Science), Associate Professor of the Department of Natural Sciences, Mathematics, Technology and Pharmacy, Sukhumi State University (Georgia)

Etibar Seyidzade - Associate Professor of the Department of Computer and Information Technolohies, Baku Engineering University (Azerbaijan)

Vladimir Golenkov, D.Sc., Professor of the Department of Intelligent Information Technologies, Belarusian State University of Informatics and Radio Electronics (Belarus)

Zhanar Omirbekova - Ph.D., Associate Professor of the Department of Automation and Management, Satbayev University (Kazakhstan)

Ivan Palov - D.Sc., Professor of the Department of Power Supply and Electrical Equipment, University of Ruse "Angel Kanchev" (Bulgaria)

Siarhei Palavenia - Ph.D., Associate Professor, Head of the Department of Telecommunication Systems, Belarusian State Academy of Communications (Belarus)

Alexander Goloskokov - Ph.D., Professor of the Department of Software Engineering and Information Technology Management, National Technical University "Kharkiv Polytechnic Institute" (Ukraine)

Peter Nikolyuk - D.Sc., Professor of the Department of Computer Technology, Vasyl Stus Donetsk National University (Ukraine)

Vladimir Palagin - D.Sc., Professor, Head of the Department of Radio Engineering, Telecommunications and Robotics Systems, Cherkasy State Technological University (Ukraine)

Viktor Khobin – D.Sc., Professor, Head of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies (Ukraine)

Valeriy Plotnikov – D.Sc., Professor, Head of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

Sergii Artemenko – D.Sc., Professor, Head of the Department of Computer Engineering of Odessa National Academy of Food Technologies (Ukraine)

Fedir Trishyn - Ph.D., Associate Professor, Vice-Rector on Scientific and Educational Work, Odessa National Academy of Food Technologies (Ukraine)

Valerii Levinskyi – Ph.D., Associate Professor of the Department of Technological Processes Automation and Robotic Systems of Odessa National Academy of Food Technologies (Ukraine)

Viktor Yehorov – Ph.D., Supervisor of the Laboratory of Mechatronics and Robotics of Odessa National Academy of Food Technologies (Ukraine)

Pavlo Lomovtsev – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

Yurii Kornienko – Ph.D., Associate Professor of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

Serhii Shestopalov – Ph.D., Associate Professor of the Department of Computer Engineering of Odessa National Academy of Food Technologies (Ukraine)

Anatoly Galiulin - Ph.D., Associate Professor, Acting Head of the Department of Electromechanics and Mechatronics, Odessa National Academy of Food Technologies (Ukraine)

Secretary of the jury:

Oksana Sokolova – Senior Lecturer of the Department of Information Technology and Cybersecurity of Odessa National Academy of Food Technologies (Ukraine)

RESEARCHING THE SYSTEM FOR VULNERABILITY TO MITM ATTACKS BY CREATING FAKE AP

Authors: ***Ulyana Karpenko, Igor Chebanenko***
Advisor: ***Sergey Krivenko***
Mariupol State University (Ukraine)

Abstract. In the course of the work, security problems of the local wireless wi-fi network were identified, as well as the role of the human factor in the security of wireless connections. One of the ways to implement the Man-in-the-Middle attack by creating a Fake AP has been investigated.

Keywords: *MITM, Fake AP, SSL, WPA, SSID, access point, Kali Linux, aircrack-ng, fluxion.*

I. INTRODUCTION

The term session hijacking is thrown around frequently and encompasses a variety of different attacks. In general, any attack that involves the exploitation of a session between devices is session hijacking. When we refer to a session, we are talking about a connection between devices in which there is state. That is, there is an established dialogue in which a connection has been formally set up, the connection is maintained, and a defined process must be used to terminate the connection. [1]

Despite the fact that MITM has been attacking for many years, it is still relevant due to the fact that it is based on software vulnerabilities of access points or clients, as well as on the features of the ubiquitous 802.11 standard, or rather, on the features of its authentication protocol. Although the standard specifies how a user joins an access point, the way in which that access point is selected is not specified, and there is no mention that it should be authenticated or if it is trusted by default. The solution to this problem was left to the discretion of the operating system hardware and software vendors.

Over time, the number of ways to implement MITM attacks has increased. For example, the attack on sites with the HTTP protocol has been improved to attacks on sites with HTTPS by spoofing certificates and bypassing HSTS. The Rogue AP creation attack evolved into Ewil Twin. And even despite the protection against certificate spoofing by browsers, such attacks are still effective, because this protection can be bypassed.

Public networks are most susceptible to MITM attacks. People with no doubts connect to networks that have no password protection, while an attacker can simply sit down and deploy a Fake AP without bothering to force a client to disconnect from the original network. Despite the fact that target OSs have been updated hundreds of times since the advent of MITM attacks and systems have become more secure, this attack is alive and poses a threat to users. And there is no reason to expect that the standard will be corrected or added in the near future.

II. LITERATURE ANALYSIS

2.1. General information

To understand the principle of a middleman attack, you must first understand how the Internet itself works. Main points of interaction: clients, routers, servers. The most common client-server communication protocol is Hypertext Transfer Protocol (HTTP). Browsing the internet with a browser, email, instant messaging are all done over HTTP. When you enter the address of a web page in your browser's address bar, the client (you) sends a request to display the web page to the server. The packet (HTTP GET request) is transmitted through several routers to the server. The server then responds with a web page that is sent to the client and displayed on its monitor. HTTP messages must be transmitted in a secure manner to ensure confidentiality and anonymity. [2]

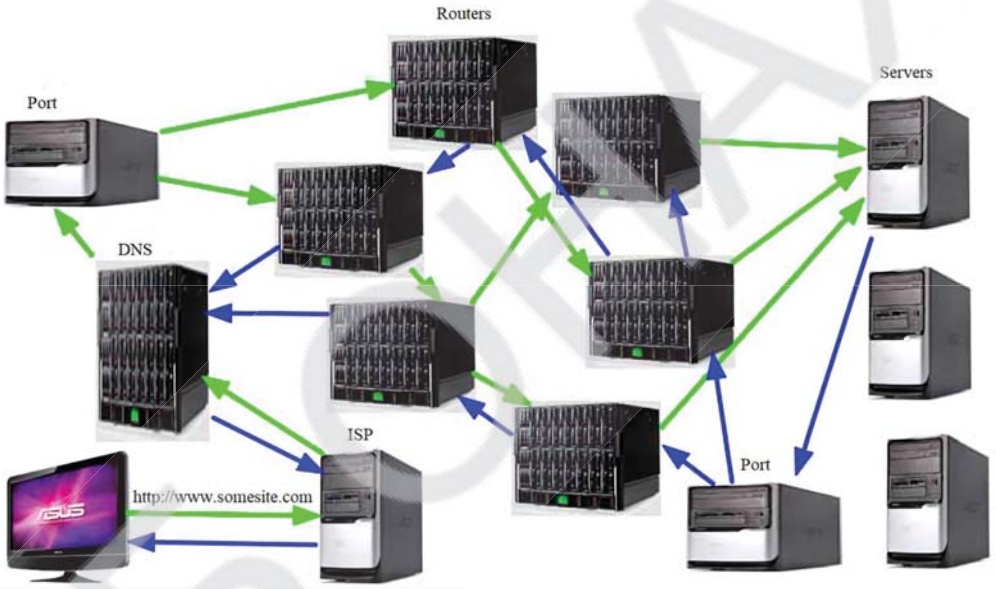

Fig. 5. Client-server communication.

A secure communication protocol must have each of the following properties:
Privacy - Only the intended recipient can read the message.
Authenticity - the identity of the interacting parties has been proven.
Integrity - Confirmation that the message has not been modified in transit.
If any of these rules are not followed, the entire protocol is compromised.

To prevent attacks that exploit APR imperfections, a secure version of the HTTP protocol was created. Transport Layer Security (TLS) and its predecessor, Secure Socket Layer (SSL), are cryptographic protocols that ensure the security of data transmission over a network. Therefore, the secure protocol will be called HTTPS. [2]

Over time, MITM attacks were carried out, finding new ways of implementation, depending on the attacked objects (sites, local networks) and

equipment. The overall goal of this type of attack is one - monitoring and modifying outgoing traffic.

2.2. ARP vulnerability attacks

Address Resolution Protocol (ARP) poisoning is an attack that involves sending spoofed ARP messages over a local area network. It's also known as ARP spoofing, ARP poison routing and ARP cache poisoning.

These attacks attempt to divert traffic from its originally intended host to an attacker instead. ARP poisoning does this by associating the attacker's Media Access Control (MAC) address with the IP address of the target. It only works against networks that use ARP.

ARP poisoning is a type of man-in-the-middle attack that can be used to stop network traffic, change it, or intercept it. The technique is often used to initiate further offensives, such as session hijacking or denial-of-service.

The ARP is a protocol that associates a given IP address with the link layer address of the relevant physical machine. Since IPv4 is still the most commonly used internet protocol, ARP generally bridges the gap between 32-bit IPv4 addresses and 48-bit MAC addresses. It works in both directions.

The relationship between a given MAC address and its IP address is kept in a table known as the ARP cache. When a packet heading towards a host on a LAN gets to the gateway, the gateway uses ARP to associate the MAC or physical host address with its correlating IP address.

The host then searches through its ARP cache. If it locates the corresponding address, the address is used to convert the format and packet length. If the right address isn't found, ARP will send out a request packet that asks other machines on the local network if they know the correct address. If a machine replies with the address, the ARP cache is updated with it in case there are any future requests from the same source.[3]

2.3. Attacks based on mDNS vulnerabilities

Protecting your environment is a complex and critical task. At every turn, it seems, attackers can penetrate your network and abuse its protocols through network redirection attacks, also known as "poisoning attacks." Some protocols are particularly vulnerable to abuse. Learning what attackers might be planning and what antidotes are available can help mitigate damage that poisoning attacks might inflict.

One protocol vulnerable to poisoning attacks is mDNS. The DNS translates human-readable names (such as "website.com") to their associated network locations, represented by an IP address ("x.x.x.x"). A DNS lookup transaction is usually unicast, meaning a single computer will ask a single server to translate a name to an IP address.

Instead of asking a single server, mDNS, a DNS-related protocol, sends out a packet to other hosts around it to essentially crowdsource the answer to the query, "Where is this thing located?" In addition, mDNS is used in conjunction with DNS

service discovery, which helps discover lists of available services via DNS. These features are helpful on home networks where local DNS servers don't exist and computers need to find other local resources such as printers. One serial user of the mDNS protocol is Apple's Bonjour service, meaning that mDNS can be observed in heavy use on networks containing MacOS and iOS devices.

Much like when attackers set out to abuse NetBIOS and LLMNR, mDNS can be abused via an attacker answering an mDNS request and impersonating a legitimate resource or computer on a network. The result is that the attacker can cause a device to send sensitive information directly to the attacker's machine, whether that be a print job for a document containing personal information or worse: a user's credentials. [4]

2.4. DNS Spoofing (DNS Cache Poisoning)

Domain name system (DNS) is the technology that translates domain names (e.g. doubleoctopus.com) to the IP address of the server it corresponds to. DNS is one of the most important infrastructural protocols of the internet and it is meant, among other purposes, to ease communications and relieve humans of the trouble of memorizing the IP address of every server they communicate with. When you type in the address of a domain in your browser, name resolution request is sent to a DNS server, which then looks up the domain name in its directory and returns the IP address of the corresponding server.

DNS spoofing is a type of attack in which a malicious actor intercepts DNS request and returns the address that leads to its own server instead of the real address. Hackers can use DNS spoofing to launch a man-in-the-middle attack and direct the victim to a bogus site that looks like the real one, or they can simply relay the traffic to the real website and silently steal the information.[5]

In regard to DNS, the most prominent threats are two-fold:

DNS spoofing is the resulting threat which mimics legitimate server destinations to redirect a domain's traffic. Unsuspecting victims end up on malicious websites, which is the goal that results from various methods of DNS spoofing attacks.

DNS cache poisoning is a user-end method of DNS spoofing, in which your system logs the fraudulent IP address in your local memory cache. This leads the DNS to recall the bad site specifically for you, even if the issue gets resolved or never existed on the server-end. [6]

Есть множество методов DNS-спуфинга или атак с отравлением кеша, например: man-in-the-middle duping, DNS server hijack, DNS cache poisoning via spam. В нашем исследовании нас интересует исключительно певрый метод.

Where an attacker steps between your web browser and the DNS server to infect both. A tool is used for a simultaneous cache poisoning on your local device, and server poisoning on the DNS server. The result is a redirect to a malicious site hosted on the attacker's own local server. [6]

In order to better understand the danger of such attacks, it is worth mentioning

the losses that they bring.

Data theft can be particularly lucrative for DNS spoof attackers. Banking websites and popular online retailers are easily spoofed, meaning any password, credit card or personal information may be compromised. The redirects would be phishing websites designed to collect your info.

Malware infection is yet another common threat with DNS spoofing. With a spoof redirecting you, the destination could end up being a site infested with malicious downloads. Drive by downloads are an easy way to automate the infection of your system. Ultimately if you're not using internet security, you're exposed to risks like spyware, keyloggers or worms.

Halted security updates can result from a DNS spoof. If spoofed sites include internet security providers, legitimate security updates will not be performed. As a result, your computer may be exposed to additional threats such as viruses or Trojans.

Censorship is a risk that is actually commonplace in some parts of the world. For example, China uses modifications to the DNS to ensure all websites viewed within the country are approved. This nation-level block, dubbed the Great Firewall, is one example of how powerful DNS spoofing can be.

Specifically, eliminating DNS cache poisoning is difficult. Since cleaning an infected server does not rid a desktop or mobile device of the problem, the device will return to the spoofed site. Furthermore, clean desktops connecting to an infected server will be compromised again. [6]

2.5. Rogue (Fake) AP and Evil Twin

A rogue access point is a wireless access point that has been installed on a secure network without explicit authorization from a local network administrator, whether added by a well-meaning employee or by a malicious attacker.

Although it is technically easy for a well-meaning employee to install a "soft access point" or an inexpensive wireless router—perhaps to make access from mobile devices easier—it is likely that they will configure this as "open", or with poor security, and potentially allow access to unauthorized parties.

If an attacker installs an access point they are able to run various types of vulnerability scanners, and rather than having to be physically inside the organization, can attack remotely—perhaps from a reception area, adjacent building, car park, or with a high gain antenna, even from several miles away. [7]

Evil Twin is a more advanced version of the Fake AP attack. Rogue AP can be used in public places where people can easily connect to passwordless access points. The attacker at this time passes all traffic through himself, having the ability to decrypt and read it, receives user data: history of visited sites, logins and passwords, personal correspondence.

An evil twin attack involves an attacker setting up a fraudulent wireless access point – also known as an evil twin – that mimics the characteristics (including the SSID) of a legitimate AP. This attack has existed about as long as wifi has. Users may connect automatically to the evil twin or do so thinking the fraudulent AP is part

of a trusted wifi network. Attackers can expedite this process by affecting the connection to the legitimate AP their device is mimicking. Once users have connected to an evil twin, they may be asked to enter a username/password to gain access via a fraudulent form which goes to the attacker. Or the attacker can simply eavesdrop and intercept any unsecured information users transmit – all without their knowledge. [8]

In order for this attack to work, a few key requirements need to be met. First, this attack requires a user to do some ignorant things. If the target you are selecting is known for being tech-savvy, this attack may not work. An advanced user, or anyone with any cybersecurity awareness training, will spot this attack in progress and very possibly be aware that it is a relatively close-ranged attack. Against a well-defended target, you can expect this attack to be detected and even localized to find you.

Second, a victim must be successfully authenticated from their network, and be frustrated enough to join a totally unknown open network that just appeared out of nowhere and has the same name of the network they trust. Further, attempting to connect to this network (on macOS) even yields a warning that the last time the network was connected to, it had a different kind of encryption. [9]

III. OBJECT, SUBJECT, AND METHODS OF RESEARCH

The object of the research is the problem of wifi connections security, non-compliance with information security rules.

The subject of the research is home wifi networks, in particular, the resistance of the router to a packet injection attack, studying the functionality of wifi adapters, bypassing the existing network protocol.

The aim of this study is a visual demonstration of the vulnerability of a wifi connection to MITM attacks like Rogue AP and Ewil Twin. Using this program, you can also track the influence of the human factor on the security of the network to penetration. Based on the results of the research, we will be able to provide a list of minimum precautions for users.

3.1. Research tools

The operating system Ubuntu 20.04 LTS (Focal Fossa) was chosen for the study. The work was carried out on wifi-adapters: Intel (R) Dual Band Wireless-AC 8265; two Tenda W311Ma adapters, on different chipsets. For an example of the attack, the Mercusys MW301R router was used.

For a successful MITM attack, you need to use several adapters that would support network monitoring functions, packet injection to the router, and the ability to install an access point. The adapter's functionality, as well as its compatibility with the operating system kernel, depends on the installed chipset. At the moment, there is no single reliable base of chips with supported functionality that would be relevant for any time. Using the aircrack-ng software package, you can test the wifi adapter chipset,monitor mode, and batch injection functionality.

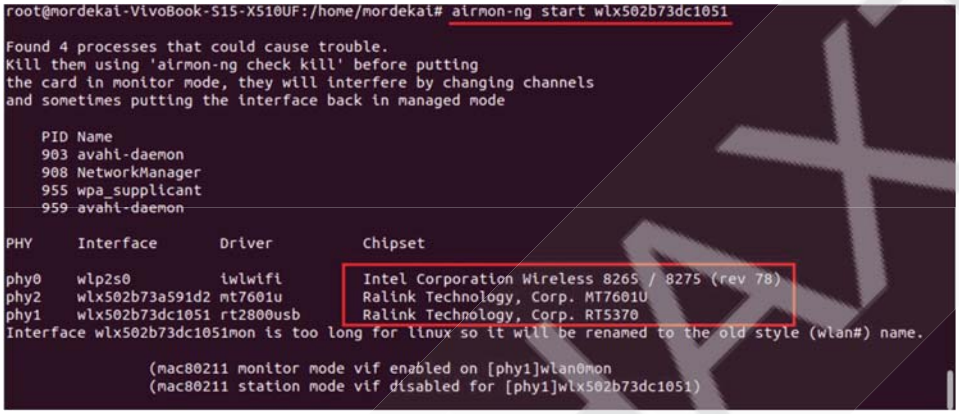

Fig. 6. Switching one of the adapters to monitor mode, viewing chipsets.

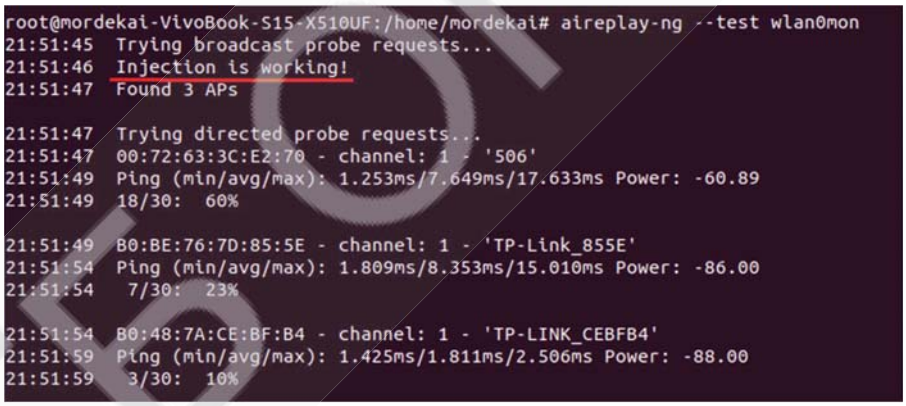

Fig. 3. Batch injection from Tenda W311Ma adapter (MT7601U)

Using the hostapd program, we can deploy a test access point and test the adapter in access point mode. To do this, just create and configure the hostapd configuration file.

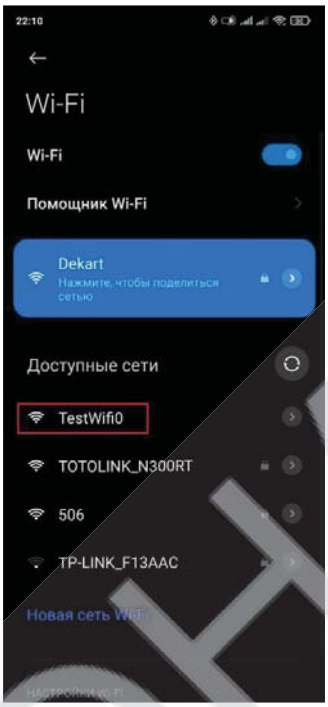

Fig. 4. Test AP display.

Intel (R) Dual Band Wireless-AC 8265 Laptop Internal Adapter provides all the features you need. External adapters are used to monitor the network and perform packet injection on the router.

IV. RESULTS

The program is written in the python programming language for the Ubuntu 20.04 LTS operating system, bash scripts are launched by clicking different keys. Initially, the nearest wifi networks are monitored, the user chooses a target for the attack, as well as wifi adapters (at least two) for carrying out a MITM attack.

The original access point is jammed using aireplay-ng by performing batch injections into the router. Fake AP is installed using hostapd, it is configured in accordance with the data obtained during monitoring. In the configuration file hostapd.conf, the SSID of the original access point for the purpose of copying is written, the driver, channel, and other characteristics are configured. It was decided to use dnsmasq for issuing IP addresses. It is a highly configurable DNS, DHCP and TFTP server designed to provide domain names and related services to small networks.

Then you can choose the target of the attack - the original AP password, or tracking and decrypting traffic passing through the Fake AP.

In the first case, the person disconnects from the original access point and connects to the created one. The screen displays a message about the need to register in the network and a request to enter a password for confirmation. After that, the

point disappears, reconnecting the client to the original network, so you can get the password.

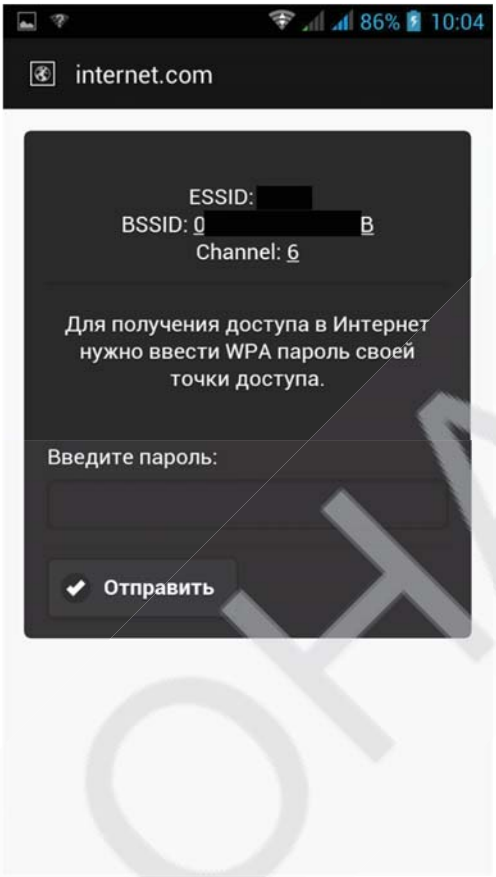

Fig. 5. False message about the need to register on the network.

To track outgoing traffic in the second case, you need to connect an access point to the Internet, this is done using Iptables, which is the standard interface for managing the Netfilter firewall (firewall). Since it is necessary to know the SSID and password of the network in order to intercept outgoing traffic, this is a sophisticated Ewil Twin attack. The captured traffic is decrypted by Airdecap-ng. Airdecap-ng can decrypt WEP / WPA / WPA2 capture files and can also be used to mark up wireless headers from unencrypted wireless capture.

It outputs a new file ending in -dec.cap, which is the decrypted / split version of the input file.

Airdecloak-ng removes WEP cloning from pcap file. It works by reading an input file and fetching packets from a specific network. Each selected package is listed and classified (default status "unknown"). Filters are then applied (in the order specified by the user) in this list. They will change the status of the packages (unknown, unclosed, potentially hidden or hidden). The order of the filters is important because each filter will base its analysis on, among other things, the status of the packages, and different orders will give different results. [10]

The developed application is a tool for testing the system for security. In this

case, not only the resistance of the network to such attacks is checked, but also the

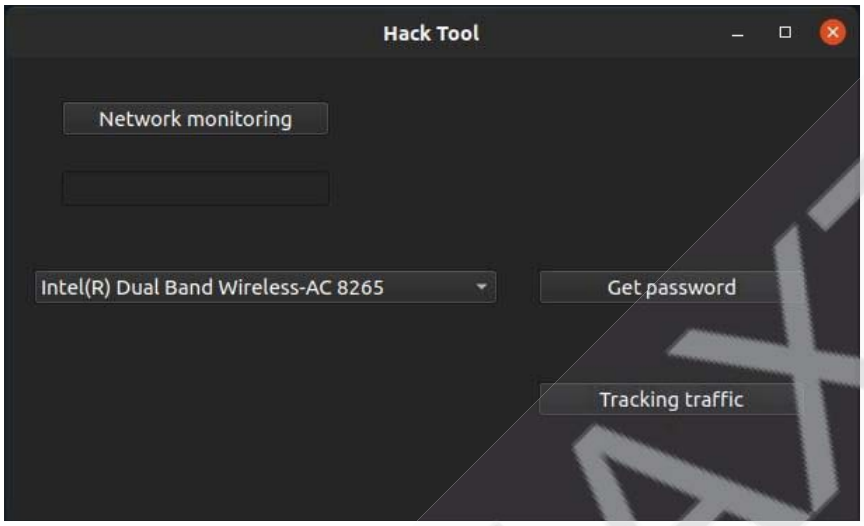

Fig. 6. Itnerface of the application.

impact of social engineering on people.

Fluxion, Wifiphisher, Airgeddon, WiFi-Pumpkin are applications of this kind, but they only work correctly in Kali Linux. They do not have a graphical interface and work from the console. Due to the complexity of configuring and building dependencies, these applications do not work on Ubuntu. Also, when testing networks, difficulties arise associated with the functionality of wifi adapters. Conflicts arise between adapter chipsets and operating system kernel versions, and flashing takes additional time. These are the problems that we encountered in our research.

V. CONCLUSIONS

Man in the Middle is generally a type of attack aimed at violating confidentiality and, in some cases, information integrity. [11] MITM attacks are still being improved and supplemented, bypassing new protection protocols. Wi-Fi is one of the most vulnerable systems. To break them, no physical impact on communication channels and wires is needed. At the moment there are many software solutions for implementing MITM attacks, but each has its own drawbacks. The developed program can act as a simulator for beginners in information security, with the help of which students will develop an understanding of the mediator's attack algorithm. Information security on the client side plays a large role in repelling such attacks. It is difficult to counter this, but for a home network it is enough to at least hide the SSID of the network, removing it from the attacker's field of vision. Using encryption and Cisco WIPS, various IPS / IDS, UEBA, etc. will allow, if not to stop the work of the attacker, then hide it and take measures to catch the criminal, but such measures are more relevant for corporate networks, the work of which is monitored by the system administrator.

VI. REFERENCES

1. Understanding Man-In-The-Middle Attacks - Part 3: Session Hijacking Updated on 5 May 2010. [Electronic resource]. URL: http://www.windowsecurity.com/articlestutorials/authentication_and_encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part3.html/ (date of access: 21.09.20).

2. Все об атаке "Человек посередине" (Man in the Middle, MitM) [Electronic resource]. URL: https://www.anti-malware.ru/analytics/Threats_Analysis/man-in-the-middle-attack (date of access: 10.12.20).

3. ARP poisoning/spoofing: How to detect & prevent it [Electronic resource]. URL: https://www.comparitech.com/blog/vpn-privacy/arp-poisoning-spoofing-detect-prevent/ (date of access: 12.12.20).

4. Poisoning Attacks, Round 2: Beyond NetBIOS and LLMNR [Electronic resource]. URL: https://www.crowe.com/cybersecurity-watch/poisoning-attacks-round-2-beyond-netbios-llmnr (date of access: 12.12.20).

5. What is DNS spoofing Man in the Middle Attack? | Security Wiki [Electronic resource]. URL: https://doubleoctopus.com/security-wiki/threats-and-tools/dns-spoofing/ (date of access: 21.12.20).

6. What is DNS Spoofing and cache poisoning? | Kaspersky [Electronic resource]. URL: https://www.kaspersky.com/resource-center/definitions/dns (date of access: 21.12.20).

7. Rogue access point - Wikipedia [Electronic resource]. URL: https://en.wikipedia.org/wiki/Rogue_access_point (date of access: 21.12.20).

8. Evil Twin Attack [Electronic resource]. URL: https://www.firewalls.com/blog/security-terms/evil-twin-attack/ (date of access: 23.12.20).

9. How to Hack Wi-Fi: Stealing Wi-Fi Passwords with an Evil Twin Attack «Null Byte» [Electronic resource]. URL: https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880/ (date of access: 23.12.20).

10. Airdecap-ng and Airdecloak-ng - Kali Linux [Electronic resource]. URL: https://kalinux.info/tools/airdecap-ng-and-airdecloak-ng.html/ (date of access: 17.01.21).

11. Сеть компании и MitM. Часть 1 [Electronic resource]. URL: https://habr.com/ru/company/acribia/blog/438996/ (date of access: 17.01.21).

International Competition of Student Scientific Works

BLACK SEA SCIENCE 2021

Information Technology, Automation and Robotics

Proceedings

Odessa National Academy of Food Technologies

The collection includes student works of the participants of the competition, which were not included in the number of prize-winners. The texts of the competitive works are published in the form in which they were submitted by the authors. The authors of the articles are responsible for the content and form of submission of the material.

Responsible for the issue: Sergii Kotlyk

Computer typesetting and layout: Oksana Sokolova

Odessa 2021