# СУЧАСНА МЕТОДИКА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ МЕРЕЖ СТАНДАРТУ IEEE 802.11

Гонтарь І.А., Згуірі Іссам, Журавка А.В.
Науковий керівник – проф. Журавка А.В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії,
тел. (057) 702-13-20)

A research object is the process of information security of wireless networks of the standard IEEE 802.11.

The subject of research is the methods of pentests on wireless networks.

The aim of the work is to identify vulnerabilities of attacks on wireless networks, through using of upgraded system Kali Linux.

Methods of researched are an experiment with scanning and attacking on wireless networks.

Nowadays, wireless networks represent the main way of transferring information. In every company, every home has routers that provide wireless data transmission.

The pentest test is a technique for analyzing and evaluating network security systems or other systems by modeling malicious actions, ranging from unauthorized system actions to internal actions, that is, the intrinsic security of an authorized attacker. The main task of the penetration test is to identify the maximum possible number of vulnerabilities of the information system (IP) for a limited time under certain conditions and condition of the IP. When conducting a penetration test, the following tasks are solved: assessment of the current state of the IP information security system; identification of information system vulnerabilities; the use of identified vulnerabilities to gain unauthorized access or unauthorized access to information to demonstrate the existence of vulnerabilities and the existence of a highly likely threat to the information system; making recommendations to improve the effectiveness of information security in IP.

Simulating the attacker, the cyber security specialist actively analyzes the systems for vulnerabilities in all areas, for example: penetration of the corporate network through system defects.

Thus, the paper discusses the method of detection of IEEE 802.11 network vulnerabilities using Kali Linux [1]. At the same time, this package is a much-needed tool that can be used to find and simulate unauthorized actions to better protect the system, as well as for future cyber-defenses - it is a necessary practice to master and counter cyber attacks. This distribution can also be a very serious weapon in the hands of a hacker. Kali Linux is a very powerful network vulnerability tool for both cyber security (white hackers) and cyber criminals (black hackers), also a Linux distribution based on the Debian kernel. This

operating system contains a large number of tools and utilities that, on the one hand, help you identify security holes in your computer environment or can be a powerful weapon for corporate network damage. The distribution was created by Offensive Security staff. Therefore, the main goal is to find holes in the network. Kali Linux's main strength is its tools. It contains about a dozen tools for analysis, scanning for vulnerabilities, such as: Aircrack-ng is a suite of programs for hacking and testing Wi-Fi network security, allowing you to crack WEP, WPA / WPA2 keys, monitor traffic, sort through WPA-PSK keys, and grab Wi-Fi connection setup keys; Burp suite is a console application for finding vulnerabilities on Internet sites and web applications; Foremost is a console program for recovering files based on their headers, footers and internal data structure; John the Ripper is an open source console program for cracking passwords by the search method; Maltego is a console analytics program. It allows you to find connections between different entities and objects. Allows you to perform open source searches, combine data for analysis, and automatically build dependencies between them; Metasploit is a framework with sophisticated architecture, hundreds of contributors, which includes thousands of modules to automate the exploitation of a huge number of vulnerabilities; Nmap is an open source Kali Linux console application that can be used for network security audits and port scans; Wireshark is a program that allows you to analyze network packets. Has the ability to use it to troubleshoot network problems, analyze applications and communication protocols, and develop applications; jSQL Injection is a Java tool for automatic injection into SQL databases; Hydra is a console program for real-time password retrieval from various online services, as well as more secure applications such as Secure Shell (SSH) and other protocols. The search is performed not by hash, but directly by queries to the server, ie you can check whether the firewalls are properly configured, such attempts are blocked, and whether you can detect such an attack on the server at all. Not only can the Aircrack-ng suite of programs conduct DoS attacks, it can also intercept authentication packages and find keys and more. Along with its multifaceted and multifunctional tools, there are some features that make it more specialized than other distributions, such as: several boot options: standard download, safe mode (Failsafe) and forensic mode. There is also the LUKS Encryption Nuke option, which allows you to immediately remove keys for encrypted data.

Finaly, Kali Linux is also a much-needed tool through which to search for and simulate unauthorized actions to better protect the system, as well as for future cyber-defenses - is a necessary practice for mastering and counteracting cyber attacks. This distribution may also be a serious weapon in the hands of a hacker.

References

1. Kali Linux. Official Documantation [Online Resource].- Access Mode https://docs.kali.org/introduction/what-is-kali-linux.