ИССЛЕДОВАНИЕ АКТУАЛЬНОГО ИНСТРУМЕНТАРИЯ KALI LINUX ДЛЯ ПРОВЕДЕНИЯ ТЕСТОВ НА ОЦЕНКУ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ

М.М. Ковцур, *к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, maxkovzur@mail.ru;*
А.А. Миняев*, к.т.н., доцент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, minyaev@gmail.com;*
В.А. Цыганов*, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, cyganov.vladimir.@gmail.com.*

УДК 004.056.5

Аннотация. В настоящее время актуальность безопасности в проводных и беспроводных сетях является одним из самых важных вопросов в сфере информационной безопасности. Многие организации используют для проверки сетей операционную систему *Kali Linux.* Она предназначена для проведения тестов на оценку безопасности, в том числе беспроводных сетей. В состав инструментов *Kali Linux* входит несколько инструментов, работающих как из командной строки, так и из базового графического интерфейса. Эти инструменты можно использовать для перевода сетевого интерфейса в режим перехвата беспроводного трафика. В данной работе представлены результаты исследований актуального инструментария в *Kali Linux* для проведения тестов на оценку безопасности беспроводных сетей.

Ключевые слова: *Kali Linux*; набор инструментов; тест на проникновение; несанкционированный доступ; проверка безопасности; сеть.

EXPLORING THE LATEST KALI LINUX TOOLKIT FOR CONDUCTING REVERSE SECURITY TESTS FOR WIRELESS NETWORKS

Maxim Kovtsur, *Ph.D., Associate Professor, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
A.A. Minyaev*, Ph.D., Associate Professor, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich;*
V.A. Tsyganov*, St. Petersburg state university of telecommunications n/a prof. M.A. Bonch-Bruevich.*

Annotation. Currently, the relevance of security in wired and wireless networks is one of the most important issues in the field of information security. Many organizations use the Kali Linux operating system to check networks. It is designed to conduct tests for conducting security assessment tests, including wireless networks. The Kali Linux tools include several tools that work both from the command line and from the basic graphical interface. These tools can be used to switch the network interface to wireless traffic interception mode. This paper presents the results of research on the current tools in Kali Linux for conducting tests to assess the security of wireless networks.

Keywords: Kali Linux; toolset; pentesting; unauthorized access; security check; network.

Введение

Беспроводные сети являются одним из наиболее уязвимых компонентов в сфере информационной безопасности. Это связано с тем, что они работают на

открытых частотах и могут быть доступны для любого желающего. Кроме того, многие беспроводные сети не защищены должным образом, что делает их уязвимыми для атак.

Инструментарий *Kali Linux*

Kali Linux – дистрибутив *Linux*, специально разработанный для тестирования на проникновение и оценку безопасности. Кроме того, *Kali Linux* содержит большой набор инструментов для тестирования беспроводных сетей.

Из публикаций Храмцова Д.О., Миняева А.А. [1-2] была выявлена проблема в использовании устаревшего инструментария *Kali Linux* для проведения тестов на проникновение.

Целью проведения исследования является выявление актуальных инструментов для проведения тестирований беспроводных сетей.

Задачами являются рассмотрение стандартных инструментов *Kali Linux* и их виды атак, а также проведение анализа популярности запросов в поисковой системе *Yandex* среди пользователей.

В данном исследовании были рассмотрены инструменты, которые идут по умолчанию в *Kali Linux.* Ниже представлена таблица, в которой указан инструмент и его вид атаки на беспроводную сеть. В табл. 1 приведены инструменты и виды их атак.

Таблица 1.

Инструмент	Вид атаки
Airgeddon	Деаутентификация и извлечение хеша (*WPA/WPA*2/*PSK*) трафика
Airmon-ng	Управление беспроводными интерфейсами (перевод в режим мониторинга)
Airserv-ng	Запуск сервера для захвата пакетов
Airodump-ng	Сбор информации о беспроводных сетях
Bully	Атака на *WPS* (брут-форс *WPS*)
Cowpatty	Атака на протокол *WPA/WPA*2
Fern Wifi Cracker	Атака на *WEP/WPA/WPA*2 с помощью словаря
GISKismet	Сбор информации о беспроводных сетях
Hostapd-wpe	Создание ложной точки доступа с поддержкой *WPE*
Iw	Управление беспроводными интерфейсами
Kismet	Сбор информации о беспроводных сетях
Kismetdb	Сбор информации о беспроводных сетях
Mdk3	Отказ в обслуживании (*DoS*)
Minidwep-gtk	Атака на *WEP*-защищенные сети

Инструмент	Вид атаки
Pixiewps	Атака на *WPS*-защищенные беспроводные сети
Pyrit	Атака на *WPA/WPA2-PSK* сети
Reaver	Атака на *WPS*-защищенные беспроводные сети
Wifiphisher	Фишинговая атака на беспроводные сети
Wifite	Атака на *WEP, WPA/WPA2-PSK* сети

После изучения базовых инструментов *Kali Linux* и видов атак, было проведено исследование по оценке актуальности каждого инструмента с помощью сервисов *Wordstat.yandex.* и *Google Trands*. Данные сервисы показывают статистику запросов в поисковой системе *Yandex* и *Google* за последний месяц. В табл. 2 представлена статистика запросов в поисковой системе *Yandex* за период 09.03.2023-09.04.2023.

Таблица 2.

Инструмент	Количество запросов в поисковой системе *Yandex*, шт.
Airgeddon	627
Airmon-ng	618
Airserv-ng	2
Airodump-ng	549
Bully	97
Cowpatty	182
Fern Wifi Cracker	384
GISKismet	2
Hostapd-wpe	19
Iw	70
Kismet	4823
Mdk3	118
Minidwep-gtk	9
Pixiewps	352
Pyrit	667

Инструмент	Количество запросов в поисковой системе *Yandex*, шт.
Reaver	349
Wifiphisher	1601
Wifite	3535

В табл. 3. Представлена статистика запросов в поисковой системе *Google* за период 09.03.2023-09.04.2023.

Таблица 3.

Инструмент	Количество запросов в поисковой системе *Google*, шт.
Airgeddon	329
Airmon-ng	518
Airserv-ng	0
Airodump-ng	385
Bully	33
Cowpatty	71
Fern Wifi Cracker	201
GISKismet	0
Hostapd-wpe	4
Iw	43
Kismet	961
Mdk3	322
Minidwep-gtk	11
Pixiewps	352
Pyrit	667
Reaver	349
Wifiphisher	774
Wifite	1011

По результатам сбора статистики запросов в поисковых системах *Yandex* и *Google* (табл. 2, табл. 3) были составлены гистограммы, в которых наглядно представлены результаты статистики запросов в поисковых системах *Yandex* и *Google* за период 09.03.2023-09.04.2023. На рис. 1 представлена гистограмма по количеству запросов в поисковой системе *Yandex* за период 09.03.2023-09.04.2023.

Рисунок 1

На рис. 2 представлена гистограмма по количеству запросов в поисковой системе *Google* за период 09.03.2023-09.04.2023.

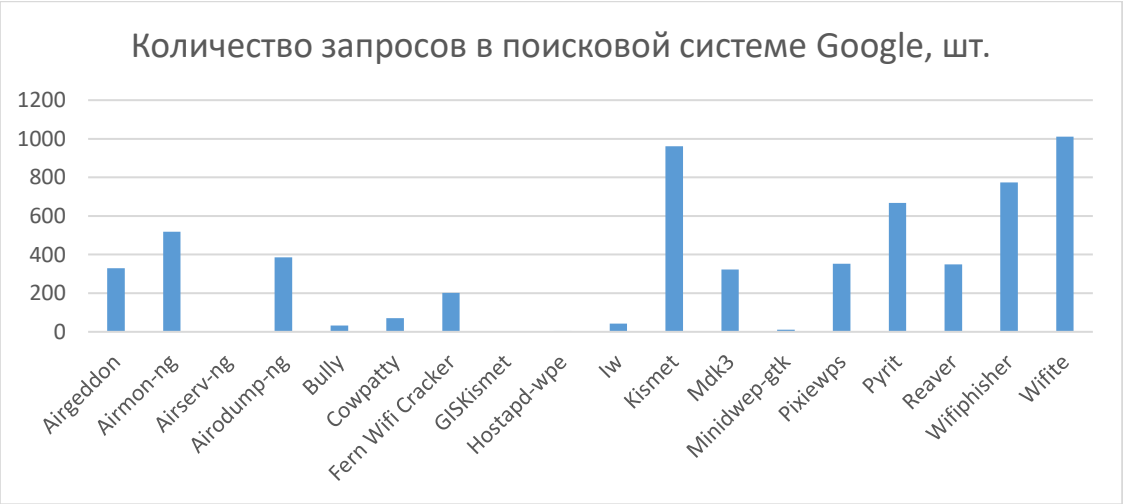

Рисунок 2

На рис. 3 представлена гистограмма по количеству запросов в поисковой системе *Google* и *Yandex* за период 09.03.2023-09.04.2023.

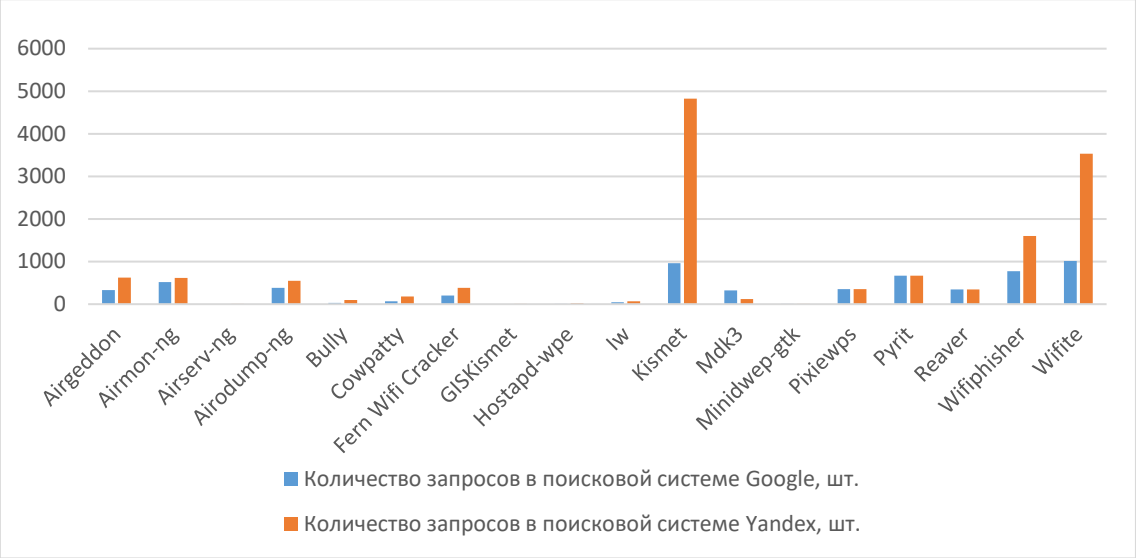

Рисунок 3

Заключение

Исходя из проведенного исследования сделан вывод, о том, что одними из актуальных инструментов для проведения тестов на безопасность сетей являются *Kismet, Wifite, Wifiphisher*. Для выполнения поставленной цели выявление актуальных инструментов для проведения тестирований беспроводных сетей были выполнены соответствующие задачи рассмотрения стандартных инструментов *Kali Linux* и видов их атак, а также проведения анализа популярности запросов в поисковой системе *Yandex* среди пользователей.

Литература

1. Буянов Д.С. Информационная безопасность в социальных сетях. Молодой ученый, 2018. – № 39 (225). – С. 14-16. (дата обращения: 09.04.2023).
2. Храмцова Д.О., Миняева А.А. Проблемы безопасности, связанные с использованием сетей семейства стандартов IEEE 802.11, информационная безопасность регионов России (ИБРР-2021). – С. 395. (Дата обращения: 09.04.2023).
3. Balueva A., Desnitsky V., Ushakov I. Approach to detection of denial-of-sleep attacks in wireless sensor networks on the base of machine learning. Studies in Computational Intelligence, 2020. – 868. – С. 350-355.
4. Герлинг Е.Ю., Зебзеев Е.А., Киструга А.Ю. Разработка метода анализа трафика беспроводной сети на базе WPA2 ENTERPRISE // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). XI Международная научно-техническая и научно-методическая конференция. Санкт-Петербург, 2022. – С. 334-339.
5. Федорова А.Э., Герлинг Е.Ю., Ахрамеева К.А., Андрианов В.И. Разработка структуры веб-интерфейса для системы анализа трафика беспроводной сети // Информационная безопасность регионов России (ИБРР-2021). Материалы XII Санкт-Петербургской межрегиональной конференции. Санкт-Петербург, 2021. – С. 394.
6. Штеренберг С.И., Москальчук А.И., Красов А.В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения. Информационные технологии и телекоммуникации, 2021. – Т. 9. – № 1. – С. 47-58.

7. Дрепа В.Е., Киструга А.Ю., Ковцур М.М., Кузьмина О.И., Петров В.А. Исследование метода FINGERPRINTING для определения местоположения беспроводного клиента IEEE 802.11 // Заметки ученого, 2022. – № 3-2. – С. 137-141.