УДК 004.75+004.77
DOI: https://doi.org/10.30837/IYF.IRTTPI.2024.505

# МЕТОДИ ТЕСТУВАННЯ ВРАЗЛИВОСТЕЙ БЕЗДРОТОВИХ МЕРЕЖ НА БАЗІ KALI LINUX

Завгородній Я.О.
Науковий керівник – ст. викл. Медведєв Є.О.
Харківський національний університет радіоелектроніки,
каф. КРіСТЗІ, м. Харків, Україна
тел. +38(057) 702-14-30, e-mail: yaroslav.zavhorodnii@nure.ua

Wireless networks have become ubiquitous. They are used worldwide in various aspects of life: at home, at work, and in public places to connect to the Internet and conduct business or personal matters.

Despite all the advantages of streamlining business and life, there are certain drawbacks in the form of risks. The insecurity of wireless networks has caused many problems in terms of intrusions into banks, companies, and government organizations. The frequency of these attacks only increases as network administrators are not fully aligned when it comes to securing wireless networks.

The report discusses the Kali Linux operating system, specifically the built-in tools that can be used to test the vulnerabilities of wireless networks.

Бездротові мережі стали присутніми всюди. Вони використовуються по всьому світу в різних сферах життя: вдома, на роботі, а також у громадських місцях для підключення до інтернету та ведення бізнесу або особистих справ.

Незважаючи на всі переваги спрощення бізнесу та життя, існують певні недоліки у вигляді ризиків. Незахищеність бездротових мереж призводить до багатьох проблем при вторгненнях до банків, компаній та урядових організацій. Частота цих атак лише зростає, оскільки адміністратори мереж не повністю узгоджені, коли мова йде про забезпечення безпеки бездротових мереж. У докладі розглянута операційна система Kali Linux, а саме вбудовані інструменти, які можна використовувати для тестування слабких місць бездротових мереж.

Kali Linux – один із найпопулярніших продуктів для проведення тестів на проникнення, обладнаний великою кількістю інструментів, розділених для зручності на багато категорій. Нижче будуть розглянуті деякі з них, необхідні для перевірки безпеки Wi-Fi мереж.

Базові вбудовані програми Kali Linux:

1. Aircrack-ng - це програма для зламу ключів 802.11 WEP (Wired Equivalent Privacy) та WPA-PSK (Wi-Fi Protected Access), яка може відновлювати ключі після захоплення достатньої кількості пакетів даних. Програма працює за допомогою реалізації стандартної атаки FMS (Flight

Management System) разом з деякими оптимізаціями, такими як атаки KoreK, а також атаки PTW. Це робить атаку набагато швидшою порівняно з іншими інструментами злому WEP. Інтерфейс є стандартним, і для роботи з цією програмою потрібні деякі навички використання команд.

Основні нові функції додатка Aircrack-NG включають в себе:

• покращена документація та підтримка;
• підтримка більшої кількості карт/драйверів;
• підтримка більшої кількості операційних систем та платформ;
• атака за допомогою словника WEP;
• атака фрагментування;
• режим міграції WPA;
• покращена швидкість проведення атаки.

2. Ghost Phisher— це локальна програма для аудиту безпеки та атак на бездротові мережі, написана з використанням мови програмування Python та графічної бібліотеки Python Qt GUI. Програма може емулювати точки доступу та розгортати різні внутрішні мережеві сервери для мережевої взаємодії, тестування на проникнення та рибальських атак.

3. Kismet є інструментом для аудита безпеки бездротових мереж, а також виконує функції системи виявлення вторгнень. Крім того, Kismet може використовуватися з будь-якими бездротовими мережними картами, які підтримують відповідний режим спостереження (для мереж стандартів 802.11b, 802.11a, 802.11g та 802.11n).

4. Pixiewps - це інструмент, який використовується для офлайн перебору піну WPS шляхом використання низької або неіснуючої ентропії окремих точок доступу (атака pixie dust). Програмне забезпечення призначене лише для освітніх цілей.

5. Reaver - це програма, яка використовується для перебору піну WPS для отримання доступу до Wi-Fi мережі з типом шифрування WPA/WPA2. У середньому, інструмент витрачає від 5 до 11 годин на відкриття пароля від цільової точки доступу у вигляді тексту.

6.Wifite - це засіб для проведення бездротової атаки в автоматичному режимі. Вона була створена для використання з дистрибутивами Linux, які використовуються для тестування на проникнення, такими як Kali Linux, Pentoo, BackBox. Програма може перевіряти багато WiFi мереж з типами шифрування WEP, WPA і WPS одночасно. Wifite налаштовується всього кількома командами. Також до складу цієї програми входять інші попередньо встановлені інструменти в систему, такі як Reaver, Bully та інші. Цей інструмент використовується для проведення аудиту безпеки бездротових мереж.

7.Fern Wifi Cracker - це програма для проведення аудиту безпеки бездротових мереж, написана на мові програмування Python та бібліотеці Python Qt GUI. Цей програмний продукт може взламувати та відновлювати паролі WEP/WPA/WPS точок доступу, а також запускати різноманітні ата-

ки на провідні та бездротові мережі.

З перелічених вище інструментів лише Fern Wifi Cracker має графічний інтерфейс. Це спрощує роботу з ним.

Інструмент Wifite, незважаючи на відсутність явного графічного інтерфейсу, об'єднав у собі багато з перелічених вище інструментів, таких як Reaver, Pixiewps та інші. Порівнюючи обидва ці інструменти, Wifite проявив себе краще з точки зору функціональності та часу отримання результатів. Крім того, він об'єднав у собі багато інструментів, завдяки чому можна вибирати тип атаки навіть комбінувати їх.

За допомогою перелічених вище інструментів, що знаходяться у вільному доступі, фахівці з інформаційної безпеки можуть перевіряти доступні точки доступу та бездротові мережі на наявність вразливостей. Проте слід пам'ятати, що використання Kali Linux як основної системи може бути нецільовим через обмежений функціонал. Усі інструменти Kali Linux так чи інакше можуть працювати разом. Тому оцінити конкретний інструмент достатньо складно. Наприклад, якщо в системі буде відсутній Reaver і Pixiewps, то атаки з використанням цих інструментів у Wifite будуть неможливі. Усі інструменти для оцінки вразливостей - це великий комплекс, в якому всі вони пов'язані між собою.

Список використаних джерел

1. Ramachandran V, Buchanan C, Kali Linux Wireless Penetration Testing Learn to Penetrate Wi-Fi and Wireless Networks to Secure your System from Vulnerabilities, 2nd Edition, Packt Publishing, 2015, ISBN-10: 1783280417

2. Broad J, Bindner A, Hacking with Kali – Practical Penetration Testing Techniques, Elsevier, 2014., ISBN: 978-0-12-407749-2.

3. McClure S, Scambray S J, Kurtz G, Hacking Exposed: Network Security Secrets & Solutions, Chapter Wireless Hacking, Computing McGraw-Hill, 2012, ISBN-10: 0072121270

4. The 10 Top Hacking Tools in Kali Linux, Hacking Tutorials (2015, July 16). Retrieved from: https://www.hackingtutorials.org/wifi-hacking-tutorials/top-10-wifi-hacking-tools-in-kali-linux/(дата звернення: 22.02.2024)

5. Официальный сайт Kali Linux [Электронный ресурс]. – Режим доступа: https://tools.kali.org/tools-listing, (дата звернення: 20.02.2024)

6. Антипов, І. Є. Удосконалення моделі Wi-Fi мережі з метою запобігання вторгненням / І. Є. Антипов, Є. Ю. Бондар, Т. А. Василенко // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. – Харків, 2014. – Вип. 177. - С. 60 - 63.