УДК 004.056

Немировський В. О.
Лукічов В. В.

Засіб для тестування на проникнення Wi-Fi роутера

Вінницький національний технічний університет

Анотація

У сучасному світі бездротові мережі є основою цифрової інфраструктури, що робить їх потенційною мішенню для зловмисників. Проблема тестування на проникнення Wi-Fi роутерів є надзвичайно актуальною, оскільки незахищеність мереж може призвести до витоку конфіденційної інформації, несанкціонованого доступу та інших кіберзагроз. Традиційні методи захисту, такі як шифрування та фільтрація MAC-адрес, мають свої недоліки і можуть бути обійдені зловмисниками. У даній роботі розглянуто підходи до тестування безпеки Wi-Fi мереж, зокрема методи аналізу трафіку, виявлення вразливостей шифрування та імітації атак для оцінки рівня захисту. Запропоновано інструмент для тестування на проникнення Wi-Fi роутера, який дозволяє виявляти потенційні загрози та оцінювати ефективність захисних механізмів.

Ключові слова: Wi-Fi безпека, тестування на проникнення, шифрування, вразливості, кіберзахист, атаки на бездротові мережі, автоматизований аналіз.

Abstract

In today's world, wireless networks form the foundation of digital infrastructure, making them a potential target for attackers. The issue of penetration testing for Wi-Fi routers is highly relevant, as network vulnerabilities can lead to data leaks, unauthorized access, and other cybersecurity threats. Traditional protection methods, such as encryption and MAC address filtering, have their weaknesses and can be bypassed by attackers. This paper examines approaches to Wi-Fi security testing, including traffic analysis methods, encryption vulnerability detection, and attack simulation to assess the level of protection. A penetration testing tool for Wi-Fi routers is proposed, allowing for the identification of potential threats and evaluation of security mechanisms.

Keywords: Wi-Fi security, penetration testing, encryption, vulnerabilities, cyber protection, wireless network attacks, automated analysis.

Вступ

Захист бездротових мереж є однією з ключових задач інформаційної безпеки в умовах зростаючої кількості атак на Wi-Fi інфраструктуру. Незахищені або неправильно налаштовані мережі можуть стати об'єктом атак, що призводить до перехоплення трафіку, крадіжки конфіденційних даних або повного контролю над мережею.

Традиційні методи забезпечення безпеки, такі як шифрування WPA2/WPA3, приховування SSID та фільтрація MAC-адрес, можуть бути недостатньо ефективними, якщо зловмисник використовує сучасні методи злому, наприклад, атаки типу KRACK або Evil Twin. Тому для оцінки безпеки Wi-Fi мереж необхідні інструменти тестування на проникнення, що дозволяють виявляти слабкі місця в конфігурації роутера та вживати відповідні заходи для їх усунення.

У цій роботі розглянуто методи тестування на проникнення Wi-Fi роутера, їхні можливості та обмеження, а також запропоновано програмний інструмент для проведення аналізу безпеки мереж.

Результати дослідження

Розроблений інструмент для тестування на проникнення Wi-Fi роутера реалізований із використанням мови програмування Python та бібліотек Scapy, Aircrack-ng і PyShark. Його основні можливості включають:

– Аналіз бездротового трафіку, збір та аналіз пакетів для виявлення незахищених точок доступу та відкритих мереж.
– Перевірка стійкості шифрування, тестування мереж на можливість злому WEP, WPA, WPA2 методом перебору паролів та атак словникового типу.
– Імітація атак, проведення атак Evil Twin, Deauthentication Attack для оцінки стійкості клієнтів Wi-Fi мережі до таких загроз.
– Виявлення підроблених точок доступу, розпізнавання атак на рівні SSID спуфінгу та аналіз

ідентифікаційних параметрів мережі.

– Автоматизований аудит безпеки, формування звіту про знайдені вразливості та рекомендації щодо їх усунення.

Flutter для мобільних пристроїв має суттєві обмеження, оскільки Android не дозволяє отримувати низькорівневий доступ до Wi-Fi-адаптера для аналізу мережевого трафіку та перехоплення хендшейків. Для реального пентесту це непридатний варіант.

Крім того, реалізовано модуль для автоматичного аналізу хендшейків, який дозволяє визначати слабкі паролі за допомогою гібридних методів перебору та словникових атак із використанням графічних процесорів (GPU) для прискорення обчислень. Також передбачено можливість виявлення активних атак у режимі реального часу, що допомагає фіксувати спроби проникнення в мережу.

Flutter для мобільних пристроїв має суттєві обмеження, оскільки Android не дозволяє отримувати низькорівневий доступ до Wi-Fi-адаптера для аналізу мережевого трафіку та перехоплення хендшейків. Для реального пентесту це непридатний варіант.

Тестування інструменту проводилося в лабораторних умовах з використанням різних моделей Wi-Fi роутерів. Результати дослідження показали, що більшість мереж із застарілим шифруванням WEP можуть бути зламані за короткий проміжок часу, тоді як мережі з WPA2 при слабких паролях також залишаються вразливими. Атаки Evil Twin виявили високу ефективність проти користувачів, які не перевіряють сертифікати мереж. Запропонований інструмент продемонстрував можливість швидкого виявлення загроз та оцінки рівня безпеки бездротової мережі.

Додатково проведено аналіз ефективності різних алгоритмів перебору паролів, що дозволило визначити оптимальні стратегії для атак на Wi-Fi. Було виявлено, що комбінування атак на основі попередньо зібраних баз даних паролів (наприклад, RockYou) та використання розподілених обчислень дає найкращі результати для швидкого злому слабких ключів.

Висновки

Розроблений засіб для тестування на проникнення Wi-Fi роутера дозволяє виявляти критичні вразливості бездротових мереж та перевіряти їхню захищеність від сучасних атак. Він забезпечує можливість аналізу трафіку, перевірки стійкості шифрування, моделювання атак та автоматизованого аудиту безпеки. Отримані результати демонструють необхідність використання комплексного підходу до захисту Wi-Fi мереж, зокрема регулярного оновлення прошивок, вибору складних паролів та впровадження додаткових заходів безпеки.

Подальші дослідження можуть бути спрямовані на розширення можливостей інструменту, зокрема, інтеграцію штучного інтелекту для автоматичного розпізнавання аномалій у трафіку та покращення механізмів атаки на основі машинного навчання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Python.org [Електронний ресурс] – Режим доступу: https://www.python.org/
2. Beale J., Wright J. "Hacking Exposed Wireless: Wireless Security Secrets & Solutions". McGraw-Hill, 2019.
3. Aircrack-ng Documentation [Електронний ресурс] – Режим доступу: https://www.aircrack-ng.org/documentation.html
4. Scapy Library [Електронний ресурс] – Режим доступу: https://scapy.net/
5. Vanhoef M., Piessens F. "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2". IEEE Security & Privacy, 2020.

Немировський Владислав Олександрович — студент групи 1БС-21б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vladislavnemirovskij@gmail.com

Nemyrovskyi Vladyslav O. – student 1BS-21b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: vladislavnemirovskij@gmail.com

Науковий керівник: Лукічов Віталій Володимирович — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: lukichov.vitalyi@vntu.edu.ua

Supervisor: Lukichov Vitalii V. — Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical, e-mail: lukichov.vitalyi@vntu.edu.ua