УДК 004.056
DOI: 10.31673/2409-7292.2022.040001

Шевченко Р.Ю.

АНАЛІЗ ЗАСОБІВ ВІЛЬНОГО ДОСТУПУ ДЛЯ ХАКІНГУ МЕРЕЖ WI-FI

У статті розглянуто найбільш популярні інструменти для злому Wi-Fi мереж, які вільно розповсюджуються у мережі Інтернет. Виявлено переваги та слабкі сторони кожного з інструментів для дослідження та виявлення уразливостей у Wi-Fi мережах. Показано, що при правильному використанні ці засоби можуть бути корисними для правильного налаштування захисту промислових та домашніх Wi-Fi мереж.

Ключові слова: Wi-Fi мережа, WEP, WPA, захист, злам мережі.

Вступ

Мережі Wi-Fi стали звичним явищем як для бізнесу, так і в побуті. Багато з цих безпроводових мереж захищені паролем і для виходу в Інтернет потрібно знати пароль. Інструменти безпроводового злому розроблені не лише для атак, а і щоб допомогти захистити ці безпроводові мережі. Деякі з них призначені для отримання доступу до пароля мережі та самої мережі. Інші надають інформацію про структуру та трафік, що проходить через мережу, інформуючи про наступні атаки. Існує багато інструментів для злому Wi-Fi. Розглянемо деякі з них.

Безпроводові мережі та хакерство

Безпроводові мережі базуються на стандартах IEEE 802.11, визначених Інститутом інженерів з електротехніки та електроніки (IEEE) для спеціальних мереж або інфраструктурних мереж. Інфраструктурні мережі мають одну або кілька точок доступу, які координують трафік між вузлами. Але в ad hoc мережах точки доступу немає і кожен вузол підключається одноранговим способом.

У безпроводовій локальній мережі можна знайти два типи вразливостей. Перший – погана конфігурація, а другий – погане шифрування. Погана конфігурація може бути спричинена адміністратором, який керує мережею. Це може бути слабкий пароль, відсутність налаштувань безпеки, використання конфігурацій за замовчуванням та інші проблеми, пов’язані з користувачем.

Погане шифрування пов’язане з ключами безпеки, які використовуються для захисту безпроводової мережі. Ці вразливості існують через проблеми з протоколами WEP або WPA.

WEP та WPA шифрування

WEP і WPA є двома основними протоколами безпеки, які використовуються в локальній мережі Wi-Fi. WEP (Wired Equivalent Privacy), є застарілим протоколом безпеки, який було представлено ще в 1997 році, як частину перших стандартів 802.11. Він був слабким і в протоколі було виявлено кілька серйозних недоліків. Тепер його можна зламати за лічені хвилини. Новий протокол безпеки Wi-Fi був представлений у 2003 році. Цей новий протокол отримав назву Wi-Fi Protected Access (WPA). Хоча зараз більшість маршрутизаторів використовують WPA або WPA2, третя версія під назвою WPA3 була сертифікована кілька років тому та призначена для заміни існуючих протоколів.

Щоб отримати несанкціонований доступ до мережі, потрібно зламати ці протоколи безпеки. Багато інструментів можуть зламати шифрування Wi-Fi. Ці інструменти можуть скористатися слабкими сторонами WEP або використовувати атаки підбору пароля на WPA/WPA2/WPA3.

Інструменти для злому Wi-Fi

Засоби безпроводового злому бувають двох типів. Один можна використовувати для сніффінгу мережі та спостереження за тим, що відбувається у мережі. Інший тип інструменту використовується для злому ключів WEP/WPA. Це популярні інструменти, які використовуються для злому безпроводових мереж і усунення несправностей у мережі.

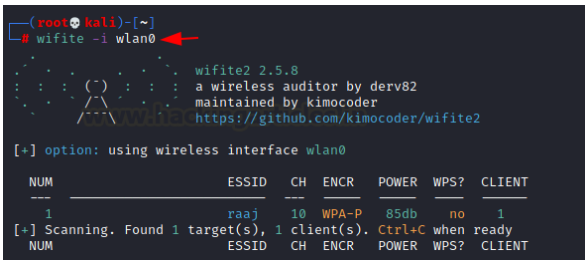
Aircrack-ng – один із найпопулярніших інструментів для злому безпроводових паролів, який можна використовувати для злому 802.11a/b/g WEP і WPA. Aircrack-ng використовує найкращі алгоритми для відновлення безпроводових паролів шляхом перехоплення пакетів.

Коли буде зібрано достатню кількість пакетів, він намагається відновити пароль. Щоб зробити атаку швидшою, він реалізує стандартну атаку FMS з деякими оптимізаціями.

Компанія, яка розробила цей інструмент, також пропонує онлайн-підручник, у якому можна дізнатися, як встановити та використовувати цей інструмент для злому безпроводових паролів. Він постачається як дистрибутив Linux, Live CD і образ VMware. Можна використовувати будь-який з них. Він підтримує більшість безпроводових адаптерів і майже гарантовано працює. Якщо використовується дистрибутив Linux, єдиним недоліком інструменту є те, що він вимагає більш глибоких знань Linux. Якщо ви не вмієте працювати з Linux, вам буде важко користуватися цим інструментом. У цьому випадку можна спробувати Live CD або образ VMWare. VMWare Image потребує менше знань, але він працює лише з обмеженим набором хост-ОС, і підтримуються лише USB-пристрої.

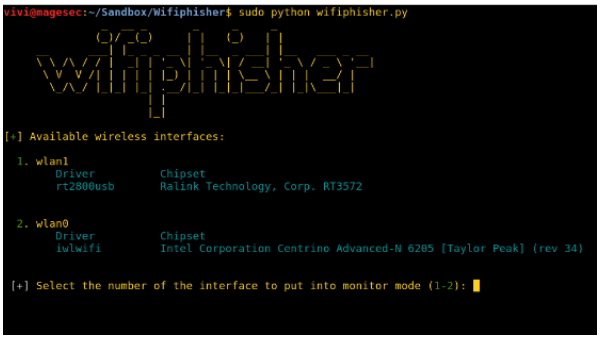
Перш ніж почати використовувати це, переконайтеся, що безпроводова карта може вводити пакети. Потім запустіть злом WEP. Прочитайте онлайн-підручник на веб-сайті, щоб дізнатися більше про інструмент. Якщо ви виконаєте ці кроки належним чином, ви зможете успішно зламати мережу Wi-Fi, захищену за допомогою WEP.

Wifite – це сценарій Python, призначений для спрощення аудиту безпеки безпроводового зв'язку. Він запускає наявні інструменти безпроводового злому для вас, усуваючи необхідність запам'ятовувати та правильно використовувати різні інструменти з їх різноманітними опціями.

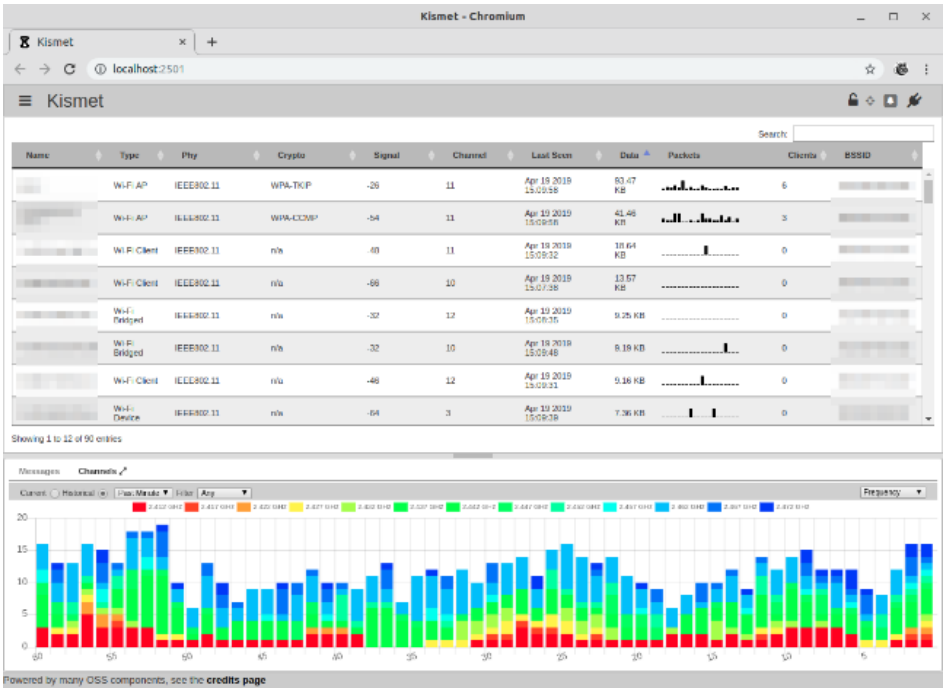


Wifite2 – це повна переробка оригінального інструменту Wifite. Він розроблений для роботи з дистрибутивами Kali Linux і ParrotSec Linux. Перед запуском Wifite рекомендується встановити додаткові інструменти, оскільки вони необхідні для виконання деяких підтримуваних атак.

Wifiphisher – це інструмент, розроблений для здійснення атак типу "людина посередині", використовуючи асоціацію Wi-Fi. Переконуючи безпроводових користувачів підключитися до шахрайської точки доступу, Wifiphisher надає зловмиснику можливість перехоплювати, контролювати або змінювати їхній безпроводовий трафік. Wifiphisher також дозволяє зловмиснику здійснювати веб-фішингові атаки. Їх можна використовувати для збору облікових даних користувача для сторонніх сайтів або облікових даних мережі Wi-Fi. Крім того, Wifiphisher розроблений як модульний, що дозволяє досвідченим користувачам писати власний код для розширення його можливостей.

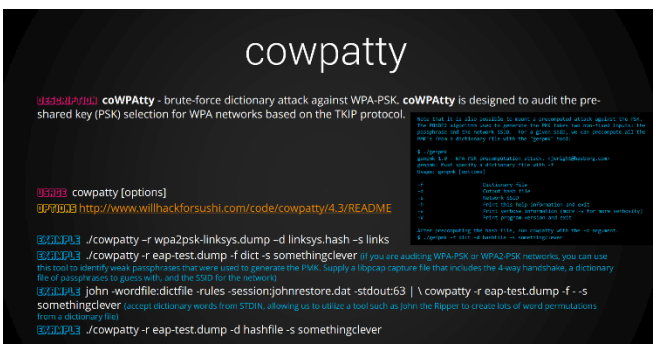


Kismet – це сніфер безпроводової мережі, який працює з Wi-Fi, Bluetooth, програмно визначеним радіо (SDR) та іншими безпроводовими протоколами. Він пасивно збирає пакети, що транслюються поблизу, і аналізує їх, щоб виявити навіть приховані мережі Wi-Fi. Kismet підтримується в усіх операційних системах (за допомогою WSL у Windows) і активно підтримується. Останній випуск 2020 року суттєво змінив архітектуру системи, щоб покращити продуктивність і додати нові функції.



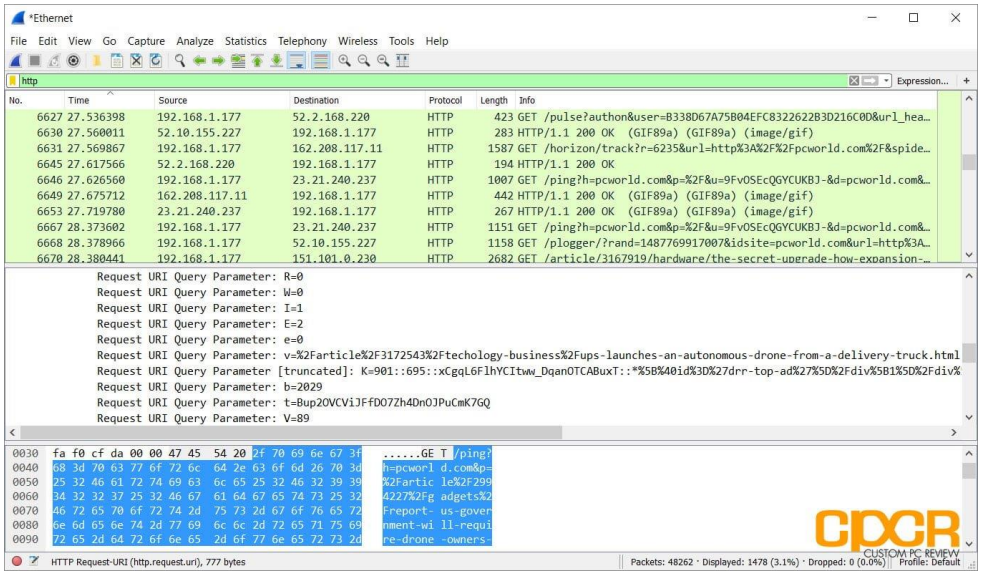
inSSIDer – популярний сканер Wi-Fi для операційних систем Microsoft Windows і OS X. Сканер Wi-Fi inSSIDer може виконувати різні завдання, включаючи пошук відкритих точок доступу Wi-Fi, відстеження потужності сигналу та збереження журналів із записами GPS. inSSIDer працює за моделлю freemium. Основні функції доступні безкоштовно, але деякі функції вимагають платного членства.

CoWPAtty – це автоматизований інструмент атаки за словником для WPA-PSK. Він працює на ОС Linux. Ця програма має інтерфейс командного рядка та працює зі списком слів, який містить пароль для використання в атаці. Користуватися інструментом просто, але повільно. Це тому, що хеш використовує PBKDF2 з 4096 ітераціями для створення потенційної парольної фрази з мережевого SSID і пароля. Оскільки кожне обчислення PBKDF вимагає часу, це робить атаку підбору пароля дуже повільною. Однак CoWPAtty має райдужну таблицю, призначену для пом'якшення цієї проблеми. Оскільки багато маршрутизаторів мають

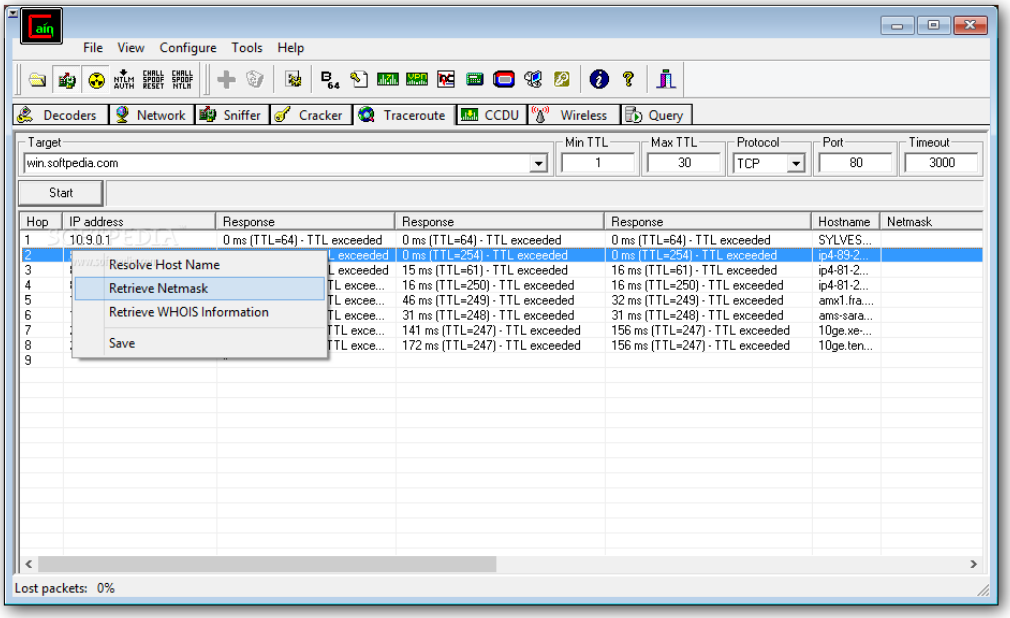


загальні SSID, для цих SSID і загальних паролів було створено попередньо обчислені таблиці. Якщо цільова мережа одна з них, тестування її за попередньо обчисленим словником відбувається набагато швидше.

Wireshark – це аналізатор мережевих протоколів. Він дозволяє перевірити, що відбувається у вашій мережі. Ви можете захоплювати пакети в реальному часі та перевіряти їх на високому рівні або переглядати значення окремих полів у пакеті. Він працює на Windows, Linux, OS X, Solaris, FreeBSD та інших. Wireshark розроблено так, щоб бути зручним для користувача і має багато функціональних можливостей. Це найбільш корисно, якщо ви добре розумієте мережеві протоколи та можете ефективно інтерпретувати трафік, який перехоплюєте.

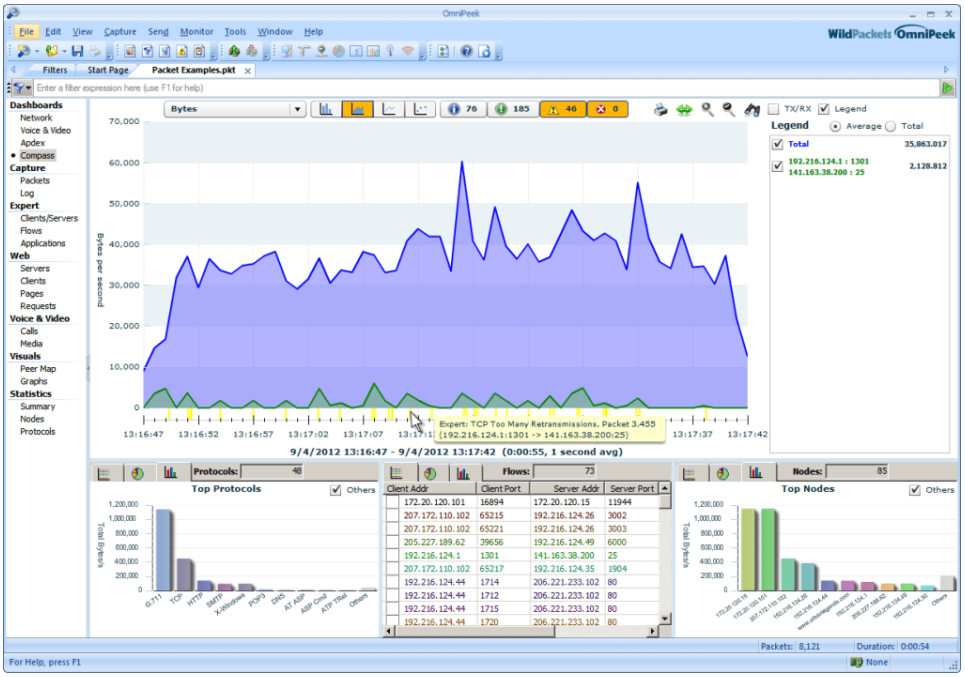


AirJack – це інструмент для впровадження пакетів Wi-Fi 802.11. Цей безпроводовий інструмент злому дуже корисний для введення підроблених пакетів і виведення мережі з ладу за допомогою атаки на відмову в обслуговуванні. Цей інструмент також можна використовувати для атаки типу "людина посередині" в мережі.



OmniPeek – ще один чудовий інструмент аналізатора пакетів і мережевого аналізатора. Цей інструмент комерційний і підтримує лише операційні системи Windows. OmniPeek включено до цього списку, незважаючи на те, що він комерційний інструмент завдяки

широкому набору функцій. Цей інструмент призначений як комплексне рішення для керування мережею Wi-Fi і включає захоплення пакетів, декодування протоколу, мережеву діагностику та усунення несправностей і навіть відтворення та аналіз голосового та відеотрафіку для діагностичних цілей.



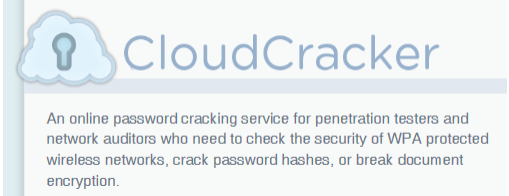
Airgeddon розроблено як універсальний інструмент для аналізу безпеки безпроводових мереж. Щоб досягти цього, він об'єднує кілька існуючих інструментів і забезпечує єдиний інтерфейс командного рядка для всіх них. Це допомагає зменшити складність виконання перевірок безпеки Wi-Fi, оскільки інтерфейс командного рядка Airgeddon проведе вас через процес і обробляє взаємодію з усіма основними інструментами.

Kali Linux NetHunter

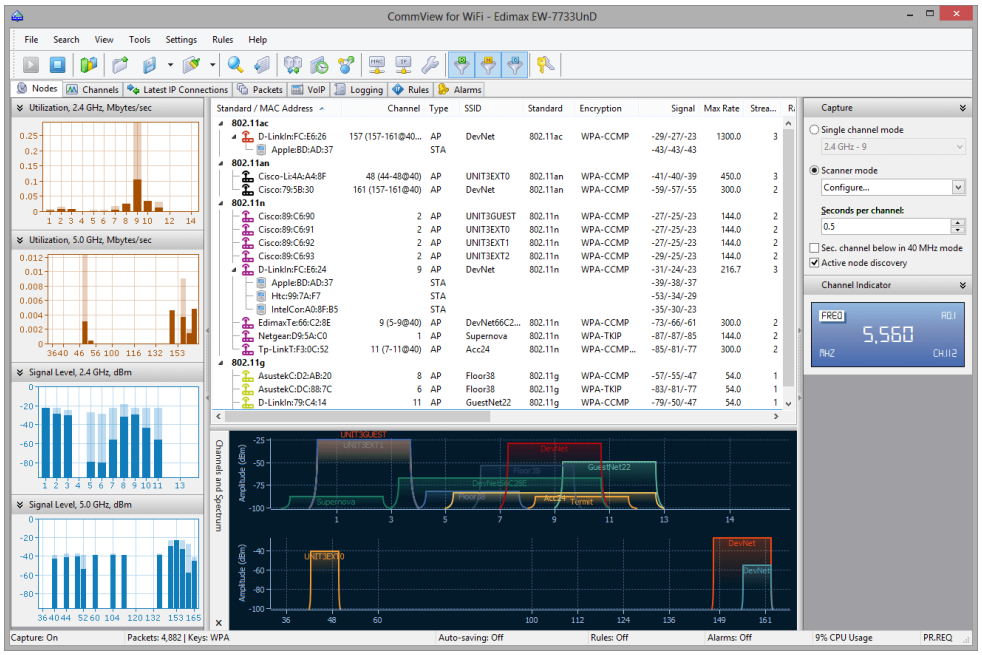
Інструменти, які обговорювалися досі, були зосереджені на безпроводовому зламі з настільного комп'ютера. Однак зростання мобільних пристроїв також надихнуло на створення кількох інструментів злому, призначених для смартфонів і подібних пристроїв.

Kali Linux NetHunter є одним із прикладів такої програми. Це повністю відкрита платформа для проникнення Android, розроблена для роботи на телефонах Nexus. Окрім інструментів, орієнтованих на Wi-Fi, NetHunter також містить повний набір інструментів Kali Linux.

CloudCracker – онлайн-інструмент підбору паролів для зламу мереж Wi-Fi, захищених WPA. Цей інструмент також можна використовувати для злому різних хешів паролів, оскільки він має величезний словник із приблизно 300 мільйонів слів для здійснення атак.



CommView для WiFi – це ще один популярний інструмент безпроводового моніторингу та аналізатора пакетів. Він оснащений простим для розуміння графічним інтерфейсом. Він чудово працює з мережами 802.11 a/b/g/n/ac. Він фіксує кожен пакет і відображає корисну інформацію у вигляді списку. Ви можете отримати корисну інформацію, таку, як точки доступу, станції, рівень сигналу, мережеві підключення та розподіл протоколів. Перехоплені пакети можна розшифрувати за допомогою визначених користувачем ключів WEP або WPA. Цей інструмент в основному призначений для адміністраторів мереж Wi-Fi, фахівців із безпеки, домашніх користувачів, які хочуть контролювати свій трафік Wi-Fi, і програмістів, які працюють над програмним забезпеченням для безпроводових мереж.



Висновки

Спроба отримати несанкціонований доступ до безпроводових мереж є незаконною в більшості юрисдикцій. Якщо ви хочете потренуватися з цими інструментами, використовуйте безпроводову мережу, якою ви володієте, або таку, де у вас є дозволи власника мережі.

Інструменти моніторингу та усунення несправностей безпроводового зв'язку в основному призначені для мережевих адміністраторів і програмістів, які працюють над програмним забезпеченням на основі Wi-Fi. Ці інструменти допомагають, коли деякі ваші системи мають проблеми з підключенням до мережі. Вони також цінні для червоних команд і тестувальників проникнення, які шукають потенційні вразливості для використання.

Перелік посилань

1. Howard Poston. 13 popular wireless hacking tools [updated 2021]. https://resources.infosecinstitute.com/topic/13-popular-wireless-hacking-tools/

2. Tamara Radivilova, Hassan Ali Hassan. Test for penetration in Wi-Fi network: attacks on WPA2-PSK and WPA2-Enterprise. https://arxiv.org/ftp/arxiv/papers/1805/1805.06691.pdf

3. James Wells. WiFi Hacking for Beginners Learn Hacking by Hacking WiFi networks (2017). https://www.academia.edu/35314753/WiFi_Hacking_for_Beginners_Learn_Hacking_by_Hacking_WiFi_networks_2017_pdf_By_James_Wells

4. Lawrence Williams. How to Hack WiFi Password: Guide to Crack Wi-Fi Network. https://www.guru99.com/how-to-hack-wireless-networks.html

Надійшла: 16.10.2022 Рецензент: д.т.н., професор Савченко В.А.