УДК 004.057.4: 004.056
DOI: 10.31673/2409-7292.2019.023236

В.В. Марченко, Л.П. Крючкова

РАДІОМОНІТОРИНГ ЧАСТОТНИХ КАНАЛІВ МЕРЕЖІ WI-FI

Розглянуто можливості і особливості використання інструментів Kali Linux для здійснення радіомоніторингу частотних каналів мережі Wi-Fi.

***Ключові слова*:** утиліта, handshake, MAC адреса, BSSID, WPA, WEP, точка доступу, Wi-Fi, комунікації, безпроводова мережа, скрипт, моніторинг.

Вступ

В даний час ефективність діяльності організацій визначається захищеністю їх інформаційних систем. Разом з тим інфраструктура інформаційних систем часто містить вузли та системи, порушення безпеки яких може призвести до нанесення значного збитку для ведення бізнесу в організації. Для запобігання таких випадків, як правило, після відповідного аналізу, формується перелік актуальних загроз і розробляється комплекс заходів щодо їх нейтралізації. Зокрема проводяться такі заходи, як періодичний моніторинг захищеності інформаційних систем і усунення виявлених вразливостей.

Останнім часом велика увага приділяється новому напрямку в області захисту інформації – адаптивній безпеці мережі, що включає в себе дві основні технології: аналіз захищеності (Security Assessment) та виявлення атак (Intrusion Detection). У загальному розумінні управління вразливостями (Vulnerability Management) – процес, спрямований на запобігання використанню відомих вразливостей, потенційно існуючих в мережі. Основний очікуваний результат – суттєве ускладнення або повне виключення можливостей для порушників використання цих вразливостей і, відповідно, зниження витрат на ліквідацію наслідків атак.

Однією з найбільш затребуваних і перспективних технологій є безпроводовий зв'язок. За допомогою безпроводових технологій організовуються точки доступу в Інтернет, будуються локальні мережі. Використання безпроводових технологій надає багато переваг і забезпечує гнучкість в побудові бізнес-процесів. Особливо це стосується управління рухомими об'єктами, складської логістики, місць масового відвідування, готельного бізнесу та об'єктів, де неможливо або складно організувати проводову мережу.

Сімейство стандартів IEEE 802.11 [1] використовує протоколи передачі даних, що працюють на частоті 2,4 ГГц і забезпечують швидкість від 11 Мбіт/с до 54 Мбіт/с, утворюючи, таким чином, WLAN (Wireless Local Area Network – безпроводова локальна мережа). Для захисту від зловмисників в стандарті IEEE 802.11 протоколів передбачено комплекс заходів безпеки: аутентифікація, шифрування трафіку, прив'язка до MAC-адреси тощо.

Kali Linux – один з дистрибутивів Linux, інструментами якого можуть користуватись як хакери, так і фахівці з інформаційної безпеки. Метою даної публікації є розгляд можливостей і особливостей використання інструментів Kali Linux для здійснення радіомоніторингу частотних каналів мережі Wi-Fi.

Інструменти Kali Linux

1. Утиліта airmon-ng

airmon-ng – скрипт, який може використовуватися для включення режиму спостереження на безпроводовому інтерфейсі. Він також може використовуватися для переведення з режиму спостереження в режим керування. Введення команди airmon-ng без параметрів відобразить статус інтерфейсів. Вона може виводити список / вбивати програми, які можуть втручатися в роботу безпроводової карти а також встановлює вірні джерела в директорії /etc/kismet/kismet.conf [2].

wlan0 – назва інтерфейсу, який планується використати (може бути **wlan0, wlan1** тощо). Після того як карту було переведено в режим моніторингу, маємо інтерфейс **wlan0mon.**

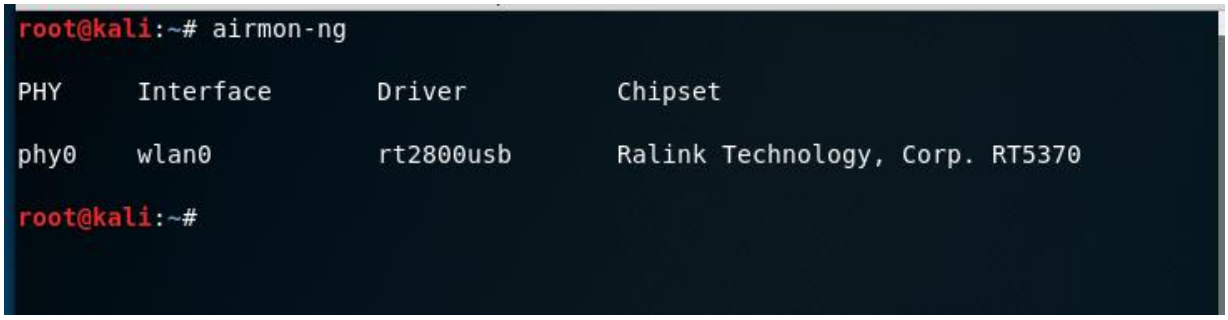

Рис. 1. Перегляд доступних безпроводових мережевих карт

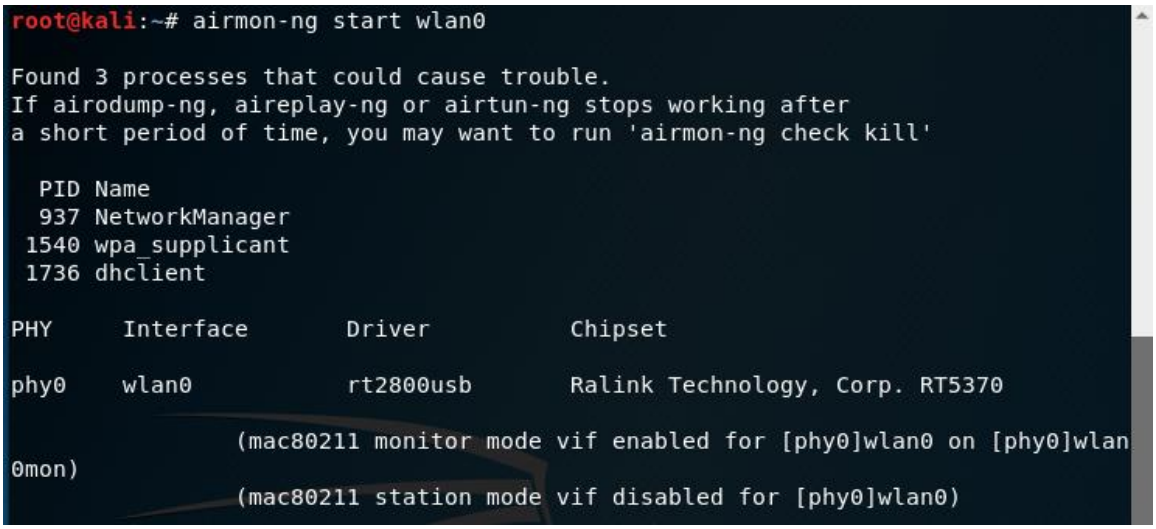

Рис. 2. Переведення безпроводової мережевої карти в режим моніторингу

2. Утиліта airodump-ng

airodump-ng – інструмент для захоплення безпроводових пакетів (є однією з програм aircrack-ng). Вона захоплює сирі фрейми 802.11 для використання їх в aircrack-ng. Якщо є підключений до комп'ютера GPS ресивер – airodump-ng здатна записувати координати знайдених точок доступу. Додатково, airodump-ng записує в текстовий файл всі деталі всіх побачених точок доступу і клієнтів [3].

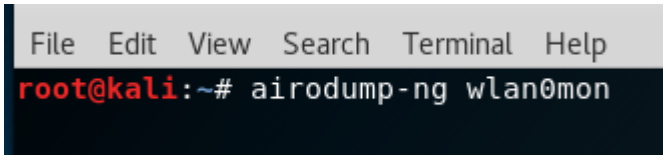

Рис. 3. Використання команди airodump-ng на інтерфейсі wlan0mon

BSSID – MAC адреса маршрутизатора;

PWR – рівень сигналу, повідомлений картою (визначається драйвером). Зростання рівня сигналу означає наближення до точки доступу або станції. Якщо BSSID PWR дорівнює -1, значить драйвер не підтримує повідомлення про рівень сигналу. Якщо PWR дорівнює -1 для деяких станцій, значить це пакет, який прийшов з точки доступу клієнту, але клієнтська передача перебуває поза зоною дії картки. Якщо всі клієнти мають PWR -1, це означає, що драйвер не підтримує повідомлення про рівень сигналу.

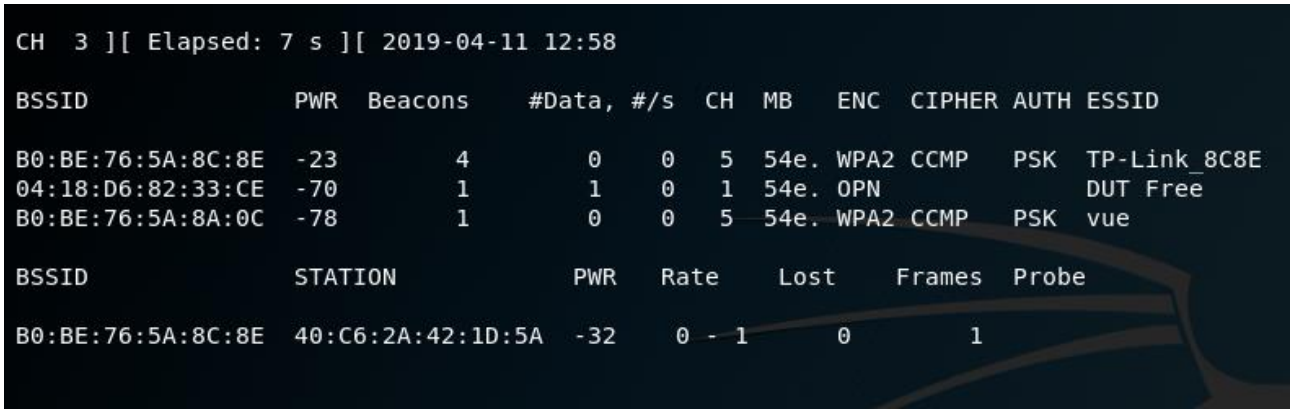

Рис. 4. Результат сканування частотного діапазону 2.4 ГГц

Beacons – число переданих цією точкою доступу «маячків» – пакетів, що оповіщають найближчі пристроїв про існування цієї безпроводової мережі, рівень сигналу, її імені (BSSID / ESSID) та іншої інформації. Використовується для підключення. За замовчуванням точки доступу зазвичай налаштовані на передачу маячків кожні 100 мс (10 разів в секунду), але інтервал можна збільшити до 1/с. Відсутність маячка не свідчить про відсутність безпроводової мережі – в прихованому (hidden) режимі точка доступу не передає маячки, але до неї можна підключитися, якщо знати точне ім'я мережі.

#Data – **к**ількість захоплених пакетів даних (якщо WEP, вважаються тільки унікальні IV), включаючи широкомовні пакети даних.

#/S – кількість пакетів даних в секунду, виміряна за останні 10 секунд.

CH – номер каналу (береться з пакетів маяків). Примітка: іноді можуть бути захоплені пакети з інших каналів.

MB – максимальна швидкість, яку підтримує точка доступу. Якщо MB = 11, це 802.11b, якщо MB = 22 це 802.11b +, а більш високі швидкості це 802.11g. Точка (після 54) означає підтримку короткої преамбули, 'e' показує, що мережа має включений QoS (802.11e).

ENC – використовуваний алгоритм шифрування. OPN = немає шифрування, "WEP?" = WEP або вище (недостатньо даних для вибору між WEP і WPA / WPA2), WEP (без знаку питання) показує статичний або динамічний WEP, і WPA або WPA2 якщо представлені TKIP або CCMP або MGT.

CIPHER – виявлений шифр. Один з CCMP, WRAP, TKIP, WEP, WEP40 або WEP104. Не обов'язково, але зазвичай TKIP використовується з WPA, а CCMP зазвичай використовується з WPA2. WEP40 показується коли індекс ключа більший 0. Стандартний стан: індекс може бути 0-3 для 40 біт і повинен бути 0 для 104 біт [3].

AUTH – використовуваний протокол аутентифікації. Один з MGT (WPA/WPA2 використовує окремий сервер аутентифікації), SKA (загальний ключ для WEP), PSK (попередньо узгоджений ключ для WPA/WPA2) або OPN (відкритий для WEP).

WPS – відображається тільки при вказівці ключа --wps (або -W). Якщо точка доступу підтримує WPS, перше поле колонки показує підтримувану версію. Друге поле вказує на спосіб зміни WPS (може бути більш ніж один метод, розділені комою): USB = метод USB, ETHER = Ethernet, LAB = Label, DISP = Display, EXTNFC = Зовнішній NFC, INTNFC = Внутрішній NFC, NFCINTF = Інтерфейс NFC , PBC = Натисканням кнопки, KPAD = Keypad. Locked відображається коли налаштування точки доступу заблоковано.

ESSID – так званий SSID, який може бути порожнім, якщо активовано приховування SSID. В цьому випадку airodump-ng спробує відновити SSID із зондованих запитів асоціювання.

STATION – MAC адреса кожної асоційованої станції або станцій в пошуках точки доступу для підключення. Клієнти, що не асоційовані з точкою доступу, мають BSSID "(not associated)".

Rate – це значення відображається тільки при використанні одного каналу. Перший номер – це остання швидкість даних від точки доступу (BSSID) Клієнту (STATION). Другий номер – це остання швидкість даних від Клієнта (STATION) до точки доступу (BSSID).

Lost – означає кількість втрачених пакетів від клієнта.

Визначення кількості втрачених пакетів: є поле, що показує порядок кожного некерованого фрейма, тому можна відняти номер передостаннього з номера останнього і таким чином дізнатися, скільки пакетів втрачено.

Packets (Frame) – кількість пакетів даних відправлених клієнтом.

Probes – ESSID прозондована клієнтом. Це мережі, до яких клієнт намагається підключитися, якщо він не підключений в даний час.

Перша частина – це знайдені точки доступу. Друга частина – це список знайдених безпроводових клієнтів, станцій. Спираючись на потужності сигналу, можна визначити місце розташування даної станції командою airodump-ng –w (OURFILE) –c (ch) –bssid (MAC) interface [3].

3. Перехоплення handshake

З технічної точки зору, handshake в безпроводових мережах – це обмін інформацією між точкою доступу і клієнтом в момент підключення клієнта до неї. Ця інформація містить різноманітні ключі, обмін відбувається в кілька стадій. Детальний опис процесу підключення до безпроводової точки доступу наведено в [4].

З практичної точки зору важливо знати наступне:

- handshake можна захопити під час підключення клієнта, який знає валідний пароль, до безпроводової точки доступу;
- handshake містить достатньо інформації для розшифровки пароля.

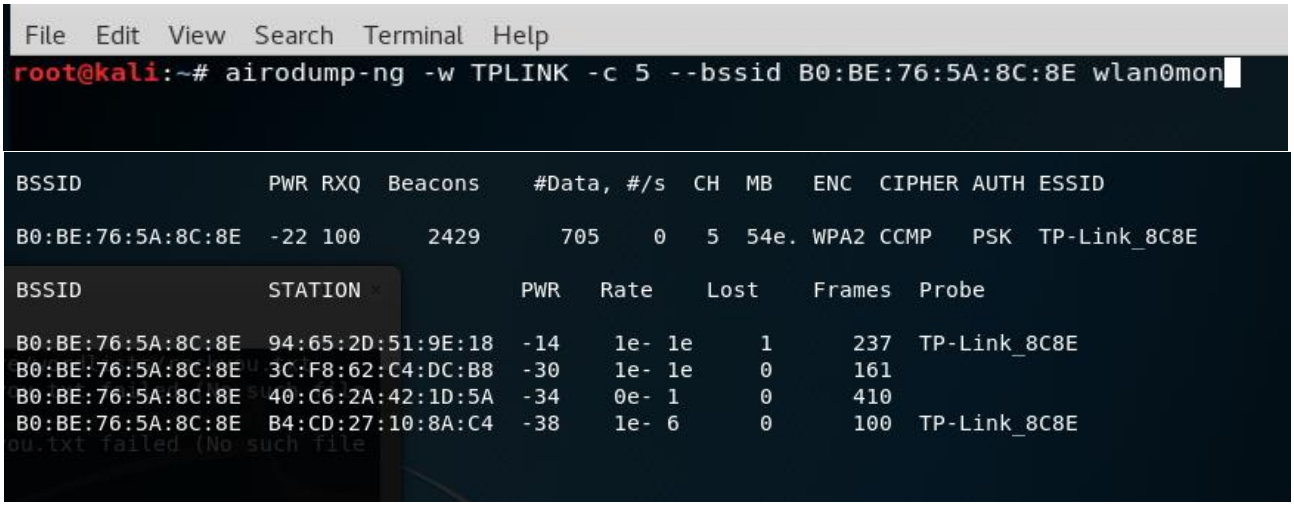

Рис. 5. Використання знайдених даних для отримання handshake

4. Утиліта aireplay-ng

aireplay-ng використовується для ін'єкції фреймів.

Головна функція – генерація трафіку для подальшого використання в aircrack-ng для злому WEP і WPA-PSK ключів. Існують різні атаки, які можуть спричинити деаутентифікацію (роз'єднання користувачів) з метою захоплення handshake WPA, фальшивої аутентифікації, інтерактивного повтору пакетів, вручну сконструйованих ARP запитів в ін'єкціях і зворотного завантаження ARP запитів. З інструментом packetforge-ng можливо створювати довільні фрейми [5].

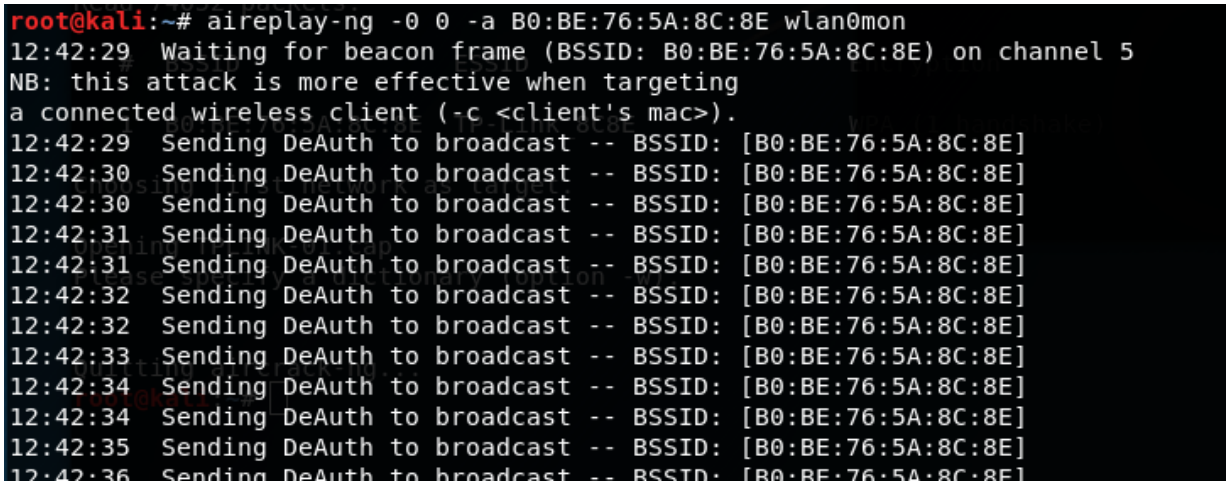

Рис. 6. Використання зловмисником утиліти aireplay-ng для отримання handshake

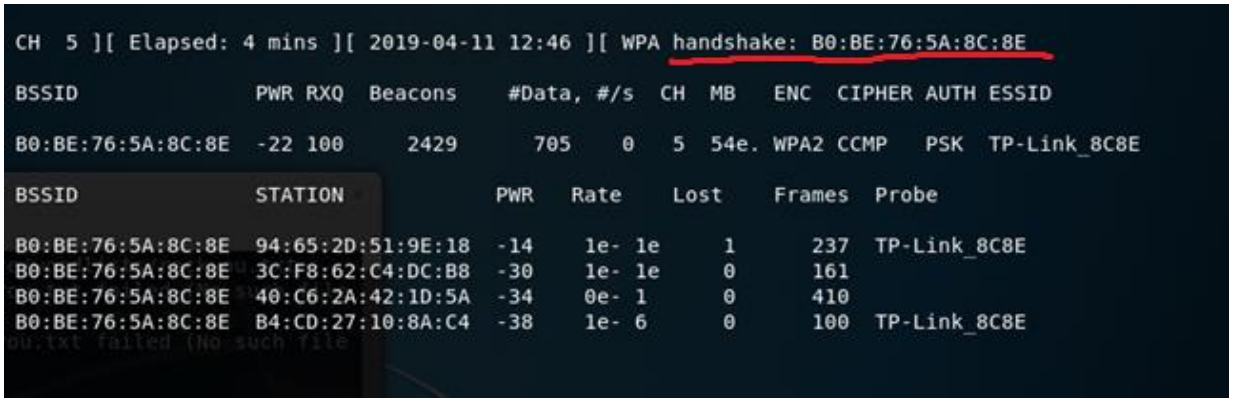

Рис. 7. Результат отримання зловмисником handshake

Висновки

1. Kali Linux – один з дистрибутивів Linux, інструментами якого можуть користуватись як хакери, так і фахівці з інформаційної безпеки.
2. Kali Linux максимально приховує свою присутність в мережі, щоб захистити себе від потенційних атак.
3. Використання моніторингу включає: географічний аналіз пакетів, спостереження за трафіком у мережі, аудит незахищених каналів (наприклад, захищених за допомогою WEP).
4. Режим моніторингу дозволяє визначати кількість використовуваних в даний час пристроїв Wi-Fi.
5. Вибір найменш завантажених каналів у мережі дозволяє забезпечити електромагнітну сумісність мережі Wi-Fi.

Список використаної літератури

1. Стандарты Wi-Fi [Електронний ресурс] – Режим доступу до ресурсу: http://1234g.ru/wifi/standarty-wifi.
2. Инструменты Kali Linux. Описание Airmon-ng [Електронний ресурс] – Режим доступу до ресурсу: https://kali.tools/?p=406.
3. Инструменты Kali Linux. Описание Airodump-ng [Електронний ресурс] – Режим доступу до ресурсу: https://kali.tools/?p=411.
4. Захват рукопожатий (handshake) в Kali Linux [Електронний ресурс] // HackWare.ru – Режим доступу до ресурсу: https://hackware.ru/?p=86.
5. Инструменты Kali Linux. Описание Aireplay-ng [Електронний ресурс] – Режим доступу до ресурсу: https://kali.tools/?p=483.

Надійшла: 5.06.2019 Рецензент: д.т.н., проф. Кожухівський А.Д.