НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий інститут телекомунікаційних систем

Кафедра телекомунікацій

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Сергій КРАВЧУК
«___»_____2024 р.

Магістерська дисертація

на здобуття ступеня магістра
за освітньо-професійною програмою «Інженерія та програмування інфокомунікацій»
зі спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Аналіз проблем безпеки при використанні MacStealer на прикладі поточних атак»

Виконав:
студент ІІ курсу, групи ТЗ-21мп
Сусоров Юрій Сергійович _____

Керівник:
Завідувач кафедри ТК НН ІТС, д.т.н., професор
Кравчук С.О. _____

Рецензент:
Доцент кафедри ІТТ НН ІТС, к.т.н., доцент
Правило В.В. _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2024 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий інститут телекомунікаційних систем
Кафедра телекомунікацій

Рівень вищої освіти – другий (магістерський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інженерія та програмування інфокомунікацій»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій КРАВЧУК
«___»_____2023 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Сусорову Юрію Сергійовичу

1. Тема дисертації «Аналіз проблем безпеки при використанні MacStealer на прикладі поточних атак», науковий керівник дисертації Кравчук Сергій Олександрович, д.т.н., професор, затверджені наказом по університету від «31» жовтня 2023 р. № 5075-с.

2. Термін подання студентом дисертації 09.01.2024 р.

3. Об’єкт дослідження: Вразливість MacStealer(CVE-2022-47522)

4. Предмет дослідження: Аналіз проблем безпеки, які виникають у результаті використання MacStealer в сучасних атаках

5. Перелік завдань, які потрібно розробити: Виявити можливі заходи безпеки для захисту систем від атак, які використовують MacStealer, Протестувати наявну мережу на виявлення слабких місць у мережі, Встановити важливість

ідентифікації слабких місць у бездротових мережах для підвищення загального рівня безпеки

6. Орієнтовний перелік ілюстративного матеріалу:
Слайд 1 ”Вступ”
Слайд 2 ”Огляд роботи”
Слайд 3 ”Актуальність роботи”
Слайд 4 ”Сучасний стан проблеми”
Слайд 5 ”Мета роботи”
Слайд 6 ”Пояснення змісту нових результатв ч1”
Слайд 7 ”Пояснення змісту нових результатв ч2”
Слайд 8 ”Висновки ”
Слайд 9 “Дякую за увагу”

7. Орієнтовний перелік публікацій:

8. Дата видачі завдання “ 9” жовтня 2022 р.

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Ознайомлення з попередніми дослідженнями та аналіз поточних атак.	Травень 2023	виконано
2	Розробка методики дослідження та налаштування експериментальної платформи	Червень 2023	виконано
3	Виконання експериментальних досліджень та аналіз результатів.	Серпень -липень 2023	виконано
4	Формування висновків та пропозицій щодо поліпшення безпеки	Вересень 2023	виконано
5	Підготовка висновків по роботі	Жовтень 2023	виконано
6	Оформлення результатів по роботі	Листопад-грудень 2023	виконано

Студент Юрій СУСОРОВ

Науковий керівник дисертації Сергій КРАВЧУК

РЕФЕРАТ

Робота обсягом 95 сторінок містить 13 ілюстрацій, 21 таблиці та 23 літературних посилань.

Ця робота спрямована на визначення потенційних загроз і ризиків, пов'язаних з вразливістю CVE-2022-47522 та атакою MacStealer на мережі Wi-Fi з ізольованими клієнтами а також отримання результатів для підвищення безпеки та захисту від цієї вразливості.

Об'єктом дослідження є вразливість CVE-2022-47522 та атака MacStealer на бездротові мережі з ізольованими клієнтами та механізми безпеки мереж Wi-Fi та їхні можливості в захисті від атак на рівні MAC.

Предметом дослідження є технічний аналіз вразливостей, зокрема, взаємозв'язку ізоляції клієнтів та атак на рівні MAC в мережах Wi-Fi.

Для проведення дослідження були використані різноманітні методи аналізу та експериментів. Перший етап дослідження включав глибокий аналіз технічних документів і стандартів, пов'язаних з бездротовими мережами Wi-Fi. Дослідницький процес включав перегляд офіційних специфікацій та стандартів протоколів Wi-Fi з метою зрозуміти основні механізми функціонування мережі та виявити можливі вразливі місця, які можуть бути використані для атак.

Наукова новизна одержаних результатів полягає в комплексному підході до захисту мережі Wi-Fi від атак, подібних до MacStealer, шляхом використання різноманітних технологій та стратегій безпеки.

Було визначено старі методи пом’якшень та на їх основі розроблено нове комплексне рішення яке може бути доповненням до наявних стратегій безпеки мереж.

Ключові слова: кібербезпека, WiFi мережа, MAC, IEEE 802.11,пом'якшення.

ABSTRACT

The 95-page work contains 13 illustrations, 21 tables, and 23 references.

This work aims to identify the potential threats and risks associated with the CVE-2022-47522 vulnerability and the MacStealer attack on Wi-Fi networks with isolated clients, and to obtain results for improving security and protection against this vulnerability.

The object of the study is the CVE-2022-47522 vulnerability and the MacStealer attack on wireless networks with isolated clients and the security mechanisms of Wi-Fi networks and their capabilities in protecting against MAC-level attacks.

The subject of the study is a technical analysis of vulnerabilities, in particular, the relationship between client isolation and MAC-level attacks in Wi-Fi networks.

Various methods of analysis and experiments were used to conduct the research. The first stage of the research included an in-depth analysis of technical documents and standards related to Wi-Fi wireless networks. The research process included reviewing the official specifications and standards of Wi-Fi protocols in order to understand the basic mechanisms of the network and identify possible vulnerabilities that could be used for attacks.

The scientific novelty of the obtained results lies in the comprehensive approach to protecting the Wi-Fi network from MacStealer-like attacks by using various technologies and security strategies.

Old mitigation methods were identified and a new comprehensive solution was developed based on them, which can be an addition to existing network security strategies.

Keywords: cyber security, WiFi network, MAC, IEEE 802.11, mitigation.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

AP	Access point
MFP	Management Frame Protection
PSM	Power Save Modея
QoS	Quality of Service
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
BU	Buffer unit
SA Query	Security Association Query
FTM	Wi-Fi Fine Timing Measurement
PMK	Pairwise Master Key
IEEE	Institute of Electrical and Electronics Engineers
MAC	Media Access Control
IWD	iNet wireless daemon
SAE-PK	Simultaneous Authentication of Equals with Public Key
EAP	Extensible Authentication Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
RADIUS	Remote Authentication Dial-In User Service
BSSID	Basic Service Set Identifier
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
DNS	Domain Name System

ВСТУП

Актуальність роботи. Завдяки постійному розвитку технологій та появі нових загроз,безпека користувачів стає все більш актуальною темою. Атака MacStealer є однією з найбільш поширених та найбільш небезпечних загроз для безпеки користувачів. Ця атака призначена для порушення ізоляції клієнтів та дає можливість перехоплювати та підміняти трафік. Це може призвести до порушення конфіденційності та безпеки даних користувачів. Для захисту від таких атак необхідно проводити дослідження та аналіз проблем безпеки.

Метою роботи дослідження проблем безпеки, пов'язаних із застосуванням MacStealer через аналіз та оцінку поточних атак з метою виявлення ризиків і можливих заходів запобігання.

Завданням роботи є:

1. Проаналізувати стандарт IEEE 802.11
2. Зібрати інформацію про існуючі атаки з використанням MacStealer
3. Виявити можливі заходи безпеки для захисту систем від атак, які використовують MacStealer
4. Протестувати наявну мережу на виявлення слабких місць у мережі
5. Встановити важливість ідентифікації слабких місць у бездротових мережах для підвищення загального рівня безпеки
6. Проаналізувати результати

Об'єктом дослідження є використання MacStealer та вплив його застосування на безпеку систем при поточних атаках.

Предметом дослідження є аналіз проблем безпеки, які виникають у результаті використання MacStealer в сучасних атаках, зокрема, ідентифікація слабких місць і можливих заходів для запобігання таким атакам.

Новизна роботи полягає в тому, щоб дослідити проблеми безпеки, що

виникають при використанні MacStealer та створити надійні методи перешкоджання атаці.

Практичне значення ідентифікація слабких місць у бездротових мережах.

РОЗДІЛ 1
ОГЛЯД МЕХАНІЗМІВ У СТАНДАРТІ IEEE 802.11

У цьому розділі надано огляд механізму енергозбереження та Wi-Fi Management Frame Protection (MFP).

1.1 Механізми енергозбереження Wi-Fi

Механізми енергозбереження були частиною стандарту IEEE 802.11 з моменту його першого випуску в 1997 році. З введенням поправки до IEEE 802.11e, що визначає покращення якості обслуговування (QoS) для бездротових мереж локальної мережі, стандарт отримав більш просунуте енергозбереження механізми.[1,§11.2] Ця поправка дозволила удосконалити управління ресурсами в бездротових мережах і враховувати потреби в якості обслуговування та енергозбереженні. Один з головних механізмів, введених цією поправкою, - це "параметр передачі" (Transmission Opportunity, TXOP), який дозволяє бездротовим пристроям отримувати доступ до мережі на певний час для передачі даних. Цей механізм сприяє ефективному використанню енергії та ресурсів мережі, оскільки він дозволяє пристроям сплячого режиму прокидатися лише тоді, коли є можливість передачі даних.

До інших механізмів енергозбереження в стандарті IEEE 802.11e можна віднести призначення пріоритетів передачі даних залежно від їх важливості та підтримку різних режимів споживання енергії для бездротових пристроїв.

Інші механізми енергозбереження в стандарті 802.11:

1. Power Save Mode (PSM): Power Save Mode - це основний механізм енергозбереження для бездротових пристроїв у стандарті IEEE 802.11. У режимі PSM пристрої можуть входити в сплячий стан і прокидатися періодично, щоб перевіряти наявність даних для передачі. Це дозволяє значно зменшити споживання енергії в режимі очікування.

2. Fast Sleep and Wakeup: Стандарти IEEE 802.11 також включають механізми для швидкого входу у сплячий режим і виходу з нього. Це дозволяє пристроям швидко переходити в режим енергозбереження і відновлювати активну роботу, коли вони готові до передачі або отримання даних.
3. Dynamic Rate Adaptation: Механізми адаптації швидкості передачі даних можуть бути використані для зменшення споживання енергії. Пристрої можуть знижувати швидкість передачі в умовах слабкого сигналу або відстані, що дозволяє зберегти енергію.
4. Frame Aggregation: Механізм агрегації фреймів дозволяє об'єднувати кілька коротких фреймів в один довгий передачі фрейм. Це зменшує накладні витрати на передачу і приймання, що допомагає знизити споживання енергії.
5. Scheduled Wake-up: Механізми розпланованого прокидання можуть бути використані для синхронізації прокидання різних пристроїв в бездротовій мережі. Це дозволяє уникнути зайвих періодів очікування і зменшити час, коли пристрої перебувають у режимі очікування.
6. Adaptive Beacon Interval: Зменшення частоти висилання сигналів маяків (beacons) у мережі також може зменшити споживання енергії. Мережі можуть налаштовувати інтервали висилання маяків в залежності від навантаження та потреб пристроїв.
7. Multicast and Broadcast Optimization: Оптимізація мультикасту та відомостей (broadcast) дозволяє ефективніше використовувати енергію

для передачі таких пакетів, зменшуючи їх зайвість для пристроїв, які не цікавляться цими даними.

Ці механізми разом спрямовані на покращення ефективності та енергозбереження в бездротових мережах IEEE 802.11. Залежно від конкретних потреб і характеристик мережі, різні комбінації цих механізмів можуть використовуватися для досягнення оптимального балансу між якістю обслуговування і енергозбереженням.

1.2 Черга кадрів у стеку Wi-Fi

Важливо розуміти, коли і де кадри ставляться в чергу. У стеку Wi-Fi (або, більш точно, в підсистемі обробки даних фізичного рівня та каналу доступу) кадри ставляться в чергу для передачі через бездротовий канал. Ця черга кадрів використовується для організації доступу до каналу та керування передачею даних між різними пристроями в мережі Wi-Fi. Процес створення та обробки черги кадрів може бути таким:

1. Створення кадрів: Кадри створюються на різних рівнях мережевого стеку, починаючи з рівня мережевого і досягаючи фізичного рівня. На рівні мережі кадри створюються з даних, які потрібно передати, та додаткової інформації, такої як адреси призначення та джерела.

2. Додавання заголовків і футерів: Кожен кадр оточується заголовками та футерами, що містять додаткову інформацію для керування передачею. Наприклад, у бездротовій мережі Wi-Fi заголовки можуть містити інформацію про адреси MAC, контрольну суму та інші параметри, які використовуються для правильної обробки кадру.

3. Черга кадрів: Кадри ставляться в чергу для передачі на фізичний рівень. Ця черга може бути імплементована в драйвері бездротової карти або в операційній системі на рівні мережевого стеку. Кадри можуть бути розміщені в черзі згідно з різними пріоритетами, які визначаються на основі QoS (Quality of Service) інформації або інших параметрів.
4. Керування доступом до каналу: У мережі Wi-Fi, канал доступу координується з використанням протоколу CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Перед передачею кадру пристрій перевіряє, чи є канал вільним, і, в разі необхідності, очікує певний час перед передачею. Це забезпечує уникнення конфліктів із сусідніми пристроями.
5. Передача та отримання кадрів: Кадри виходять із черги і передаються через бездротовий канал. Інші пристрої в мережі слухають канал, і якщо вони впізнають свої адреси в кадрах, вони приймають ці кадри. Кадри також можуть бути підтверджені або повторно передані, якщо не відбулася успішна передача.
6. Видалення з черги: Після успішної передачі кадр видаляється з черги. Якщо передача була невдалим, кадр може бути поміщений назад в чергу для повторної передачі.

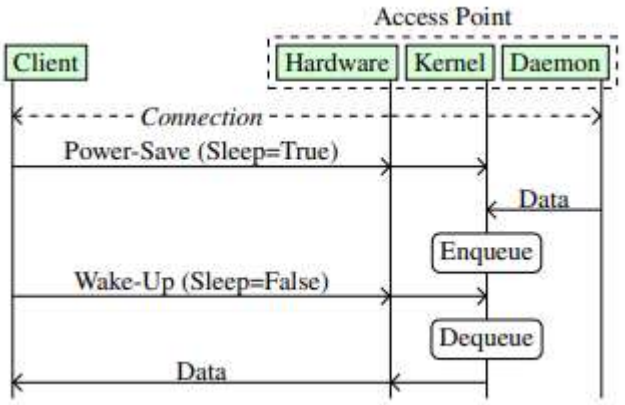

Рис. 1.1 Типовий обмін повідомленнями про енергозбереження між клієнтською станцією та точкою доступу

На рисунку 1.1 проілюстровано типовий обмін повідомленнями про енергозбереження між клієнтською станцією та точкою доступу. У будь-який момент під час підключення клієнтська станція може вказати, що перейде в режим енергозбереження. Для цього клієнт може встановити біт потужності (Power Management bit) у заголовку кадру у бездротовій мережі IEEE 802.11 для вказівки свого режиму споживання енергії. Цей біт називається "Power Management bit" і використовується для вказівки, чи знаходиться бездротовий пристрій в активному (режиму прийому/передачі) або пасивному (режим споживання енергії) стані.Коли клієнт встановлює біт потужності, це означає, що він знаходиться в режимі енергозбереження і не очікує активного обміну даними. Це може бути корисним для економії енергії, коли пристрій не активно взаємодіє з мережею.Коли точка доступу (AP) або інший пристрій бажає передати дані клієнту, він може використовувати цей біт, щоб вимкнути пристрій з режиму енергозбереження і дозволити йому прокинутися для прийому даних. Процес такого "пробудження" може включати в себе висилання

кадрів Beacon або інших спеціальних кадрів, щоб попередити клієнта про наявність даних.Цей механізм дозволяє досягти балансу між енергозбереженням та доступністю для прийому даних у бездротовій мережі, щоб забезпечити оптимальну продуктивність та ефективність роботи пристроїв [2].Коли точка доступу отримує кадри для передачі клієнту, вони буферизуються в черзі передавання ядра,кадри, які призначені для конкретного клієнта, зберігаються в буфері на AP. Це може бути необхідним, коли клієнт перебуває в режимі енергозбереження або недоступний для прийому даних, доки клієнт не вийде з режиму сну (наприклад, опитує дані) або не буде перевищено термін життя кадру (тобто кадр ставиться в чергу лише на максимальний термін). Як довго кадри можуть залишатися в черзі, вважається, що виходить за рамки стандарту.[1,§11.2.3.10] У цей момент часу всі кадри в черзі зберігаються у вигляді відкритого тексту **[**1, рис. 5- 1]. Після того, як клієнт вкаже, що він прокидається, ядро точки доступу може вилучити з черги всі буферизовані кадри, застосувати будь-які операції шифрування та передати їх на клієнтську станцію. На додаток до черги передачі всередині ядра, кадри можуть ставитися в чергу апаратним забезпеченням. Це може бути пов’язано з необхідністю чекати доступу до бездротового каналу або дозволити повторну передачу, коли приймач не підтвердив переданий кадр. Залежно від апаратних можливостей (наприклад, підтримка апаратного шифрування) кадри в черзі можуть зберігатися у вигляді відкритого тексту або зашифровуватися апаратно.

1.3 Буферні кадри

Коли клієнтська станція перебуває в режимі енергозбереження, точка доступу буферизує свої кадри, однак не всі кадри буферизуються. Точка доступу (AP) може буферизувати кадри для клієнта, коли клієнтська станція

перебуває в режимі енергозбереження (Power Save Mode). Проте не всі кадри буферизуються, і це може залежати від різних факторів, таких як тип кадрів, налаштування мережі та пріоритети передачі.

Ось деякі важливі моменти, що стосуються буферизації кадрів для клієнта в режимі енергозбереження:

1. Unicast vs. Broadcast/Multicast Frames: Зазвичай, точка доступу буферизує унікаст-кадри (кадри, адресовані конкретному клієнту), оскільки ці кадри мають призначення лише для конкретного клієнта. Загальномережеві кадри (broadcast або multicast) можуть не буферизуватися, оскільки вони адресовані всім клієнтам в мережі і не мають специфічного адресата.

2. QoS (Quality of Service): Механізми QoS можуть впливати на те, які кадри буферизуються. Наприклад, важливі дані з високим пріоритетом можуть буферизуватися і відправлятися клієнту, навіть якщо він перебуває в режимі енергозбереження.

3. Архітектура мережі: Деякі мережі можуть мати спеціальні налаштування, які визначають, які кадри буферизувати для клієнта в режимі енергозбереження. Наприклад, мережі можуть мати налаштування для включення або вимкнення буферизації для певних клієнтів чи типів кадрів.

4. Специфікація 802.11e: Якщо використовується поправка до стандарту IEEE 802.11e (яка визначає покращення якості обслуговування - QoS), це також може вплинути на те, які кадри буферизуються і передаються в режимі енергозбереження.

Щоб стандартизувати, які кадри можна буферизувати, стандарт IEEE 802.11

визначив одиницю буферизації (BU). Буферизовані блоки можуть бути поставлені в чергу за допомогою механізму енергозбереження, а всі інші мають бути доставлені негайно. Буферні блоки включають блок даних служби MAC (MSDU), сукупний MSDU (A-MSDU) і блок даних протоколу керування MAC (MMPDU). Оскільки не всі кадри MMPDU буферизуються, стандарт визначає низку класифікацій [1, §11.2.2]. В одній із класифікацій визначено, що кадри дії MMPDU (за винятком кадрів точного вимірювання часу), роз'єднання та деаутентифікація є буферними: MMPDU, який передається в одній або кількох діях (за винятком кадру точного вимірювання часу та кадру запиту точного вимірювання часу), роз'єднання або кадру деавтентифікації. Це чітко вказує на те, що не всі типи фреймів можна буферизувати, причому яскравими прикладами типів фреймів без буферизації є повідомлення відповіді автентифікації та асоціації. Важливим прикладом типів фреймів, які підлягають буферизації відповідно до стандарту, є повідомлення запиту асоціації безпеки (SA). Ці повідомлення використовуються для захисту SA за допомогою Wi-Fi Management Frame Protection (MFP).

1.4 Wi-Fi Management Frame Protection

Стандартизовані механізми захисту Wi-Fi Management Frame Protection (MFP) для кадрів керування, включаючи конфіденційність даних, цілісність, автентичність походження та захист від повторного відтворення.Основні механізми Wi-Fi Management Frame Protection включають такі функції:

1. Захист від повторного відтворення (Replay Protection): MFP використовує алгоритми захисту від повторного відтворення, які не дозволяють зловмисникам пересилати раніше перехоплені керуючі кадри. Це

запобігає атакам, які використовують відтворення кадрів для аналізу мережі.

2. Цілісність (Integrity): Механізми цілісності дозволяють виявити будь-які зміни в переданих керуючих кадрах. Якщо дані були змінені під час передачі, це виявляється, і кадр вважається пошкодженим.

3. Автентичність походження (Origin Authentication): MFP використовує методи автентичності для перевірки, що керуючі кадри надійшли від легітимних пристроїв і не були надіслані зловмисниками. Це допомагає запобігти атакам, які спрямовані на відправку фальшивих керуючих кадрів.

4. Шифрування (Encryption): Деякі реалізації MFP можуть використовувати шифрування для забезпечення конфіденційності даних, які містяться в керуючих кадрах. Це важливо для захисту від перехоплення та аналізу надісланих даних.

Wi-Fi MFP визначено в поправці 802.11w і включено до версії базового стандарту 802.11 2012 року. Нові механізми захисту підвищують безпеку надійних фреймів керування, які представляють підмножину усіх фреймів керування. Яскравими прикладами є надійні кадри дій (наприклад, які використовуються для керування спектром) і кадри (повторної) асоціації та автентифікації. За допомогою нових засобів захисту мережі захищені від різноманітних відомих атак, які зловживають кадрами керування, наприклад, атак деавтентифікації, які від’єднують клієнтів від мережі **[**3**]**.

Wi-Fi Alliance зробив Wi-Fi MFP обов’язковим у всіх своїх програмах сертифікації з 2020 року **[**4**]** і Wi-Fi Protected Access 3 (WPA3) **[**5**]**,але ще не

потребує його використання. У результаті цих зусиль зі стандартизації дослідники спостерігали зростаюче впровадження як WPA3, так і MFP [6]. Коли Wi-Fi MFP використовується між двома відповідними станціями, вибрані кадри керування, такі як кадри асоціації та роз'єднання, захищені поточною асоціацією безпеки (SA). Асоціація безпеки — це набір політик і криптографічних ключів, які використовуються для захисту інформації в межах з'єднання та зберігаються кожною стороною асоціації.

Ось як це працює:

1. Встановлення безпеки: Перш ніж дві станції можуть використовувати MFP для захисту керуючих кадрів, вони повинні встановити безпеку між собою. Це може включати в себе процес аутентифікації та обмін ключами для шифрування та захисту кадрів.

2. Формування SA: Коли безпека між станціями встановлена, вони можуть створити спільну асоціацію безпеки (SA). SA - це угода між станціями щодо параметрів безпеки, таких як ключі шифрування та методи захисту.

3. Використання MFP зі SA: Після того як SA встановлено, станції можуть використовувати MFP для захисту керуючих кадрів, які вони обмінюються. Це включає в себе додавання інформації про цілісність, автентичність та інші захисні мітки до цих кадрів.

4. Захист керуючих кадрів: За допомогою MFP і SA керуючі кадри, такі як кадри асоціації та роз'єднання, захищаються від несанкціонованого доступу, зміни або повторного відтворення. Це допомагає ускладнити атаки на рівень керування мережею та забезпечує надійність та безпеку комунікації між станціями.

Якщо станція має існуючу асоціацію безпеки, будь-який кадр асоціації буде тимчасово відхилено точкою доступу, щоб запобігти атакам відмови в обслуговуванні. Згодом точка доступу ініціює процедуру SA Query, щоб визначити, чи клієнт все ще має активну асоціацію безпеки з AP [1, §11.13].Процедура SA Query (Security Association Query) є важливим елементом безпеки Wi-Fi мережі і використовується для перевірки статусу активних безпекових асоціацій між точкою доступу (AP) і клієнтською станцією. Основна ідея полягає в тому, щоб періодично перевіряти, чи актуальні активні безпекові асоціації і чи існують проблеми з ними.Процедура SA Query включає наступні етапи:

1. Ініціація запиту: Точка доступу (AP) ініціює процедуру SA Query, відправивши захищений запит (SA Query Request) до клієнта. Цей запит містить інформацію про SA, яка повинна бути перевірена.

2. Обробка запиту клієнтом: Клієнтська станція отримує захищений запит і перевіряє, чи актуальна та існуюча асоціація безпеки з AP. Якщо асоціація все ще активна, клієнт відповідає на запит.

3. Відповідь клієнта: Якщо активна асоціація існує, клієнт відповідає на запит (SA Query Response) з підтвердженням активної асоціації та іншою відповідною інформацією.

4. Завершення процедури: AP отримує відповідь від клієнта і обробляє її. Якщо асоціація активна і відповідь відповідає очікуваному, то процедура SA Query завершується успішно.

У процедурі SA Query станції обмінюються захищеним запитом і відповіддю. Якщо процедура завершилася успішно, асоціація безпеки

вважається чинною, і станції можуть безпечно продовжувати використовувати асоціацію. Отже, незахищені кадри асоціації можна безпечно відкинути. Якщо процедура не виконується або закінчується час очікування, це вказує на те, що зв'язок може бути невідповідним (наприклад, через незапланованe перезавантаження клієнтської станції), і тому зв'язок безпеки може бути розірвано (тобто клієнтська станція може бути відключена від мережа).

Висновок

Отже, поправка IEEE 802.11e спрямована на покращення QoS і ефективності мережі, в той час як також враховує механізми енергозбереження для підтримки більш раціонального використання енергії в бездротових пристроях.

РОЗДІЛ 2
ВИТІК КАДРІВ ІЗ ЧЕРГИ WI-FI ТА ЗЛОВЖИВАННЯ ЧЕРГОЮ ДЛЯ ЗБОЇВ У МЕРЕЖІ

У цьому розділі йдеться про дослідження поведінки точок доступу у випадку зміни параметрів безпеки кадрів, які знаходяться у черзі. А також оцінено практичний вплив атак на безпеку мережі та її користувачів.

2.1 Недотримання стандарту

Пристрій Wi-Fi не може миттєво передавати пакети, які надходять з верхнього рівня, і на практиці кадри будуть стояти в черзі перед передачею. Наприклад, вони можуть бути поставлені в чергу апаратним забезпеченням, коли приймач перебуває в режимі енергозбереження, поки відправник очікує доступного часу в ефірі або коли кадри ще не підтверджені, і тому може знадобитися повторна передача. Це викликає важливе питання: як повинен поводитися відправник, якщо контекст безпеки змінюється між часом, коли кадр був у черзі, і часом, коли він фактично (повторно) передається? Стандарт згадує функцію старіння для видалення кадрів, які були буферизовані протягом надмірного часу, але не визначає її точну поведінку: «Точна специфікація функції старіння виходить за межі цього стандарту» **[**1**,** §11.2.3.10]. Хоча існують специфікації служби, які гарантують, що станція не повинна надсилати кадри у вигляді відкритого тексту після ввімкнення шифрування, не було знайдено чітких інструкцій щодо обробки змінних контекстів безпеки, а також того, що буферизовані кадри слід видаляти (або тимчасово зберігати), коли пристрій від’єднується або повторно підключається до мережі.

2.2 Модель загрози

Зловмисник може вводити та перехоплювати кадри та маніпулювати контекстом безпеки клієнта-жертви, наприклад, вводити незахищені кадри керування, такі як кадри автентифікації та асоціації. Крім того, зловмисник може підробити стан енергозбереження клієнта-жертви шляхом підробки кадрів, які використовують біт енергозбереження (наприклад, незахищений нульовий кадр даних). Як правило, зловмиснику не потрібні знання мережевих облікових даних, тому він є зовнішньою загрозою. Однак за певних умов витік кадрів захищено ключем мережевої групи, і в цьому випадку для отримання відповідного ключа потрібні мережеві облікові дані[2].

2.3 Загальна стратегія та методологія атаки

Стратегія високого рівня, що лежить в основі атаки витоку черги передавання, ґрунтується на спостереженні, що більшість стеків Wi-Fi не вилучають із черги належним чином або очищають свої черги передавання, коли змінюється контекст безпеки. Як зловмисник,можна зловживати такою поведінкою, підробляючи певні кадри керування під MAC-адресою клієнта-жертви, тим самим спритно втручаючись у контекст безпеки та механізм енергозбереження.

2.3.1 Стратегія атаки

Розглянемо клієнта, який підключений до точки доступу з підтримкою керування живленням. На рисунку 2.1 продемонстровано, як зловмисник може обдурити вразливу точку доступу, щоб отримати витік кадрів, призначених для клієнта-жертви, з її черг передачі.

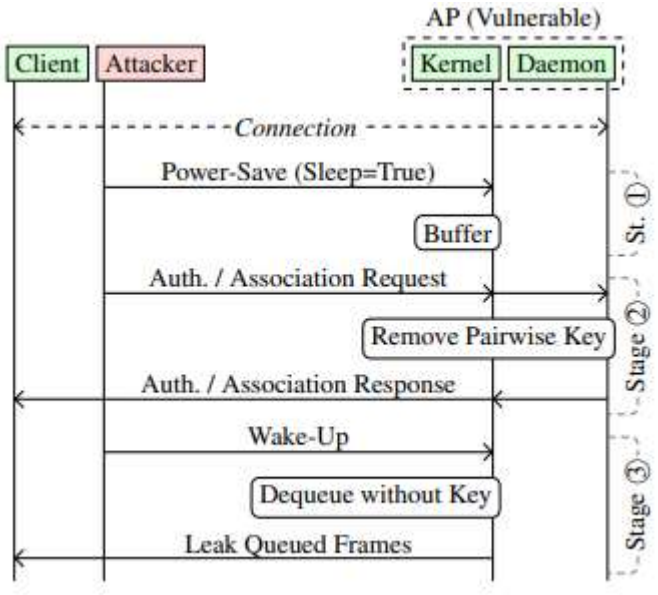

Рис. 2.1 схема отримання витоку кадрів з її черг передачі

1. Зловмисник підробляє незахищений фрейм енергозбереження, щоб обманом змусити точку доступу повірити, що клієнт-жертва переходить у режим енергозбереження. У результаті точка доступу ставить у чергу (тобто буферизує) усі кадри для клієнта, доки клієнт не вкаже, що він вийшов із режиму енергозбереження. Важливо, що на цьому етапі всі кадри ставляться в чергу у вигляді відкритого тексту.

2. Тепер зловмисник прагне обманом змусити точку доступу видалити ключі шифрування клієнта-жертви (тобто, попарний ключ шифрування). Хоча для досягнення цієї мети може знадобитися певна креативність, зазвичай фрейми керування, такі як запити на автентифікацію та (повторне) приєднання, змусять точку доступу оновити свій контекст безпеки. У разі успіху точка доступу більше не має доступу до попарного ключа шифрування для клієнта-жертви.

3. Зловмисник підробляє незахищений кадр пробудження, щоб ініціювати точку доступу для передачі всіх кадрів у черзі для клієнта. Оскільки вразлива точка доступу більше не має попарного ключа шифрування для клієнта, вона може не використовувати шифрування (тобто відкритий текст) або повернутися до ключа шифрування з груповою адресою. У результаті атаки будь-хто в зоні зв'язку вразливої точки доступу може перехопити витік кадрів у вигляді відкритого тексту або зашифрованих за допомогою ключа шифрування з груповою адресою, залежно від відповідної реалізації стека (тобто демон простору користувача, ядро, драйвер, прошивка)[2].

2.4 Витоки фреймів у Linux та апаратному забезпеченні

Для кожного варіанту атаки зловмисник успішно пропускає кадри з черги передачі у вигляді відкритого тексту.

2.4.1 Витоки зашифрованих посилань без ключа шифрування

Попередні реалізації ядра Linux не видаляли кадри даних, коли ключ шифрування більше не був доступний у зашифрованих посиланнях. Натомість його кадри даних передавалися у вигляді відкритого тексту. У законному сценарії це може статися, коли станція від'єднується, поки в черзі передачі точки доступу ще є кадри даних. Щоб цей варіант атаки був успішним, точка доступу не повинна підтримувати повний клієнтський стан (тобто драйвер апаратного забезпечення не підтримує цю функцію). Це стосується старіших ядер Linux (тобто модуль ядра mac80211 за замовчуванням увімкне стан клієнта повної точки доступу, починаючи з Linux 4.5.0) і може застосовуватися до реалізацій драйвера FullMAC (тобто драйвери FullMAC використовують власну

реалізацію модуля mac80211). Через те, що стан клієнта не підтримується повністю, демон простору користувача (наприклад, hostapd) не видалятиме весь стан клієнтської станції (включно з чергою передавання) після отримання, наприклад, запиту на автентифікацію. Зловмисник може використати цю поведінку, щоб видалити попарний ключ і отримати витік усіх кадрів із черги передачі у вигляді відкритого тексту. Розглянемо клієнта, підключеного до точки доступу, яка не підтримує повний стан клієнта. Подібно до схеми атаки на малюнку 2.1, зловмисник може використовувати цю поведінку для витоку кадрів із черги передачі у відкритому вигляді. Змусивши точку доступу буферизувати кадри для клієнта-жертви, зловмисник передає запит на аутентифікацію. Оскільки точка доступу не підтримує повний клієнтський стан, попарний ключ шифрування тепер видаляється без очищення черги передавання. Нарешті, зловмисник може надіслати кадр пробудження, щоб ініціювати процес видалення з черги, і вразлива точка доступу випустить усі свої кадри у вигляді відкритого тексту. Оцінка Ми оцінили Linux 5.5.0 з демонами простору користувача hostapd 2.9, hostapd 2.10 і IWD 1.28 і підтвердили успішність атаки. Для успішної реалізації IWD потрібно надіслати запит на повторну асоціацію (замість запиту на автентифікацію), щоб видалити попарний ключ шифрування. Починаючи з Linux 5.6.0 і далі, кадри даних скидаються ядром, якщо ключ шифрування недоступний у зашифрованих посиланнях, ефективно запобігаючи цьому методу атаки [2].

2.4.2 Повторні передачі

У цьому варіанті атаки знаходимо витік кадрів у відкритому тексті після кількох спроб повторної передачі. Розглянемо законного клієнта, який не може підтвердити кадр (наприклад, через колізії кадрів або погані умови

радіоканалу), тоді апаратне забезпечення повторно передасть кадр. Якщо ці повторні передачі виявляться невдалими, апаратне забезпечення передасть кадри запиту на відправку, а якщо отримано кадр із зрозумілим для відправлення, кадри в черзі повторно передаються ще раз. Зауважте, що зловмисник може використовувати звичайне обладнання для вибіркового блокування **[**7**]** початкової передачі для ініціювання повторної передачі. Тепер розглянемо зловмисника, який передає запит автентифікації без біту сну, щоб видалити парний ключ і розбудити клієнта. Початкова передача буде використовувати відповідне шифрування, як і очікувалося, однак після процедури запиту на надсилання ключ шифрування було видалено, через що остаточна повторна передача буде у відкритому вигляді.

2.4.3 Race Condition

У цій атаці супротивник передає запит автентифікації без біту сну. Ми спостерігаємо стан змагання, що спричиняє видалення ключа шифрування з апаратного забезпечення, який видаляється шляхом запису в регістри, відображені в пам’яті, тоді як інший стан, здається, не оновлюється. У результаті всі кадри в черзі передаються у вигляді відкритого тексту.

2.5 Захисти

Стандарт визначає чіткі процедури для подальших дій після отримання кадрів керування, наприклад, у [**1,** §11.3.4.3] наведено процедуру обробки кадру автентифікації. Однак стандарт не визначає поведінки точки доступу, яка повинна керувати своїми чергами передачі, коли змінюється контекст безпеки. Стає зрозуміло, що така поведінка повинна бути визначена. Визначаємо два підходи, які можна використовувати для захисту поведінки черг передачі: 1.

Перед видаленням попарного ключа шифрування чергу передавання має бути виключено з черги незалежно від статусу енергозбереження клієнтської станції одержувача. Тобто точка доступу робить останню найкращу спробу доставити всі кадри, що зберігаються в черзі передачі. 2. Перед видаленням попарного ключа шифрування слід очистити чергу передавання. Тобто точка доступу скидає всі кадри, що зберігаються в черзі передачі. Тоді і тільки тоді можна видалити попарний ключ шифрування. Зауважте, що ці підходи також охоплюють процедури зміни ключа, тобто видалення простроченого ключа та встановлення нового попарного ключа.

2.6 Зловживання чергою для збоїв у мережі

На додаток до маніпулювання контекстом безпеки для витоку кадрів із черги, точку доступу можна обманом змусити ввімкнути свої механізми енергозбереження для клієнта-жертви. Тобто, оскільки біт живлення в заголовку кадру незахищений, зловмисник може тривіально ввімкнути механізми енергозбереження і таким чином вибірково поставити кадри в чергу в точці доступу. Отже, клієнтські станції вразливі до атак на відключення та відмову в обслуговуванні. У той час як кадри можуть бути заблоковані за допомогою інших методів, наприклад, глушіння або багатоканального MitM, зловживання чергою вимагає менше ресурсів. Для виконання багатоканального MitM потрібні дві карти бездротової мережі, тоді як для цих атак потрібна лише одна. Подібним чином глушіння вимагає більш спеціалізованого обладнання, тоді як ця атака може бути виконана за допомогою будь-якої мережевої карти, яка підтримує введення кадрів. Противник також може комбінувати ці методи глушіння, щоб підвищити загальний рівень успішності блокування кадрів.

2.6.1 Постановка в чергу запитів SA

У першій атаці зі зловживанням чергою передачі показано, як можна використати процедуру SA Query, щоб відключити клієнта від мережі. Згадайте, що стандарт визначає, які кадри керування буферизуються і, таким чином, дозволено ставити в чергу за допомогою механізму енергозбереження [1, §11.2.2] . Кадри запиту та відповіді SA Query передаються як надійні (тобто захищені) кадри дій [1, §9.4.1.11**]**. Однак стандарт явно не виключає їх буферизації (тобто кадри дії буферизуються за певними винятками). Коли станція ставить у чергу повідомлення запиту або відповіді, це може спричинити тайм-аут на приймаючій стороні, оскільки це чутлива до часу процедура безпеки. Як наслідок, зв'язок безпеки має бути зруйновано, фактично від'єднавши жертву від мережі. Враховуючи таку поведінку, точки доступу піддаються новій атаці на роз'єднання на основі черги проти своїх клієнтів, навіть якщо конфігурація мережі передбачає застосування Wi-Fi MFP (наприклад, WPA3).

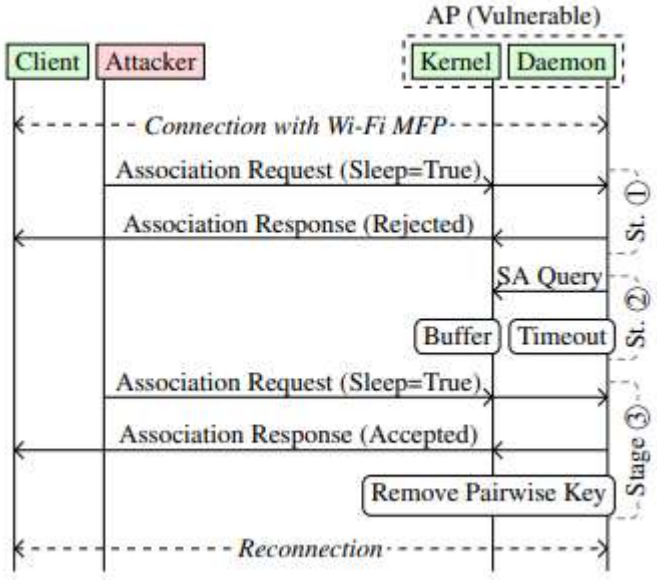

Рис. 2.2 відключення клієнта-жертви в три етапи

2.6.2 Схема атаки

Щоб продемонструвати, як можна використати стандартне визначення,визначаємо наступну атаку. Розглянемо клієнт-жертву, який підключений до вразливої точки доступу, де станції погодилися застосувати захист Wi-Fi MFP. На рисунку 2.2 продемонстровано, як зловмисник може націлитися на вразливу точку доступу, щоб відключити клієнт-жертву в три етапи.

1. Зловмисник підробляє запит асоціації від клієнта-жертви та встановлює біт сну в заголовку кадру. Це позначить жертву-клієнта як сплячу, що призведе до того, що буферизовані кадри будуть поставлені в чергу в точці доступу. Оскільки потрібен WiFi MFP, запит на асоціацію відхилено.

2. У рамках механізмів захисту Wi-Fi MFP точка доступу ініціює процедуру SA Query. Він передає ряд запитів SA Query, які тепер ставляться в чергу ядром. У результаті точка доступу ніколи не отримає відповіді, тому процедура закінчиться, і тепер демон дозволить нові запити на асоціацію.

3. Зловмисник підробляє другий запит на асоціацію, який тепер дозволено точкою доступу. Як визначено процедурою асоціації, точка доступу тепер видаляє попарний ключ шифрування клієнта-жертви. Зауважте, що клієнт мовчки відкидає всі небажані асоційовані відповіді. Крім того, після трьох етапів точка доступу може почати нову 4- сторонню процедуру рукостискання. Однак, оскільки на клієнті все ще встановлені парні ключі, він відповість зашифрованими повідомленнями рукостискання. Точка доступу не може прочитати ці повідомлення, оскільки попередньо видалила попарний ключ

шифрування. У результаті рукостискання не вдасться, фактично від’єднавши жертву від клієнта та точки доступу.

2.6.3 Атака SA Query

Стандарт визначає процедури SA Query для станцій Sub 1 GHz (S1G), які переходять у режим енергозбереження [1, §11.13]. Робота станцій S1G, визначена в поправці IEEE 802.11ah, забезпечує зв'язок на більшій відстані з меншим споживанням енергії **[**8**]**. Таким чином, він чудово підходить для великих сенсорних мереж, додатків Інтернету речей і розумних міст **[**9**]**. Згідно з процедурами запиту SA, станція S1G повинна вийти з режиму сну протягом часу, який не перевищує деякий заздалегідь визначений максимальний інтервал часу очікування, інакше зв’язок безпеки може бути розірвано. Цікаво, що стандарт не визначає поведінку для станцій, що працюють на частотах 2,4 і 5 ГГц, які частіше використовуються. Незважаючи на це, із визначеними процедурами станції залишаються вразливими для атаки. Розглянемо законного клієнта, який спить, зловмисник може просто підробити кадр пробудження, щоб видалити запити з черги. Жодних дійсних відповідей не буде надіслано, оскільки вони не будуть отримані клієнтом, що призведе до демонтажу SA. Таким чином,атака виявляє недоліки стандарту. Щоб запобігти такій атаці, необхідно автентифікувати біт сну та кадри опитування, запобігаючи тому, щоб зловмисник міг маніпулювати станом черги, і сплячий клієнт повинен завжди запитувати точку доступу протягом попередньо визначеного максимального інтервалу очікування, забезпечуючи своєчасне отримання буферизованих запитів SA Query. До того часу станції залишаються вразливими до атаки SA Query.

2.6.4 Постановка в чергу запитів Wi-Fi

FTM Wi-Fi Fine Timing Measurement (FTM), визначене в IEEE 802.11mc і включене в IEEE 802.11-2016, використовується для вимірювання фізичної відстані між двома станціями. Протокол використовує вимірювання часу проходження в обидві сторони та забезпечує точність вимірювання дальності на метровому рівні в середовищах з низькою багатопроменевістю **[**10, 11, 12]. Стандарт IEEE 802.11 визначає, що кадри Wi-Fi FTM не підлягають буферизації та повинні доставлятись без посилання на механізм енергозбереження [1, §11.2.2]. Тобто, незважаючи на те, що кадри Wi-Fi FTM створені як кадри дії, вони явно вказані як виняток буферизованих кадрів. На практиці механізм постановки в чергу впливає лише на кадр запиту Wi-Fi FTM, який передається станцією для ініціювання сеансу вимірювання відстані з іншим відповідним пристроєм. Кадри відповіді Wi-Fi FTM, які відповідають за вимірювання часу проходження туди й назад, обробляються мікропрограмою. Тобто будь-яка критично важлива операція виконується на апаратному пристрої, тому механізми енергозбереження не впливають на неї. Незважаючи на це, коли запит стоїть у черзі, станція не розпочне новий сеанс вимірювання відстані. Така поведінка може наражати клієнтів на потенційно (з точки зору безпеки) збої в вимірюванні відстані.

Розглянемо сценарій, коли клієнтська станція підключена до мережі та потребує регулярного звітування про свою фізичну відстань до точки доступу в контексті геозонування (приклад додаток, наданий Wi-Fi Alliance **[**4**]**). У будь-який момент зловмисник може підробити кадр до точки доступу, що вказує на те, що клієнт переходить у режим енергозбереження. Отже, сеанс вимірювання не буде розпочато, оскільки його запити ставляться в чергу ядром.

Це може призвести до тайм-ауту програми вищого рівня (наприклад, бездротового демона), що, у свою чергу, може ініціювати точку доступу, щоб видалити жертву з геоогороженої зони (тобто точка доступу робить висновок, що клієнт не відповідає, і залишив її геоогорожена зона), або взагалі від'єднайте клієнта від мережі.

2.6.5 Постановка в чергу 4-сторонніх повідомлень рукостискання

На додаток до кадрів дій, націлених раніше, зловмисник може примусово поставити кадри даних у чергу. Під час націлювання на повідомлення в 4-сторонньому рукостисканні, тобто під час процедури підключення, це може тривіально призвести до атаки відмови в обслуговуванні на основі черги. Оскільки ця атака націлена на 4- стороннє рукостискання, вона ефективна проти будь-якого типу конфігурації мережі (наприклад, WPA3).

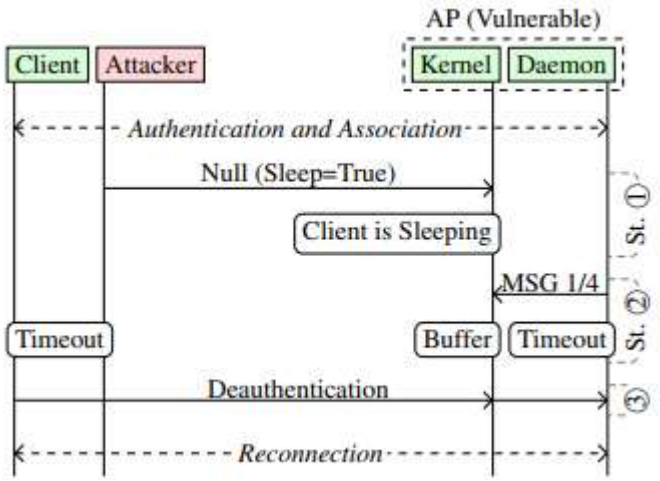

Рис. 2.3 схема деавтентифікації клієнта-жертви

2.6.6 Схема атаки

Розглянемо клієнт-жертву, який підключається до вразливої точки доступу. На рисунку 2.3 продемонстровано, як зловмисник може націлитися на

вразливу точку доступу, щоб запобігти підключенню клієнта-жертви в три етапи.

1. Після процедури асоціації зловмисник підробляє нульовий кадр і встановлює біт сну в заголовку кадру. Це змушує ядро позначати жертву-клієнта як сплячу.

2. Тепер уразлива точка доступу поставить у чергу всі кадри, які можна буферизувати, включаючи перше 4-стороннє повідомлення рукостискання (яке надсилається як кадр даних). Така поведінка призводить до тайм-ауту рукостискання як на точці доступу, так і на клієнті-жертві, оскільки повідомлення рукостискання ніколи не надсилаються.

3. Клієнт-жертва очікує першого 4-стороннього повідомлення рукостискання, але ніколи його не отримує. Отже, тайм-аут перерве процедуру рукостискання, що змусить клієнт-жертву надіслати повідомлення про деавтентифікацію. Оскільки точка доступу все ще буферизує кадри, її повідомлення про деавтентифікацію також не передається клієнту-жертві. Отже, клієнт закінчить час очікування та від’єднається від мережі. Після трьох етапів станції можуть перезапустити процедури підключення, якщо вони налаштовані як такі [2].

2.7.1 Практичний вплив

Щоб продемонструвати практичний вплив атаки,обговоримо можливі наслідки перехоплення кадрів для клієнта.

2.7.2 Зловмисне підключення TCP

У атаці з перевизначенням контексту безпеки (Розділ 5) зловмисник отримає кадри, які є частиною TCP-з'єднань, які жертва раніше ініціювала. Зловмисник може підтвердити ці вхідні TCP-пакети, щоб отримати всі очікувані дані, які сервер намагається надіслати клієнту. Крім того, ці витоку TCP-пакетів розкривають використовувані порядкові номери, які можуть бути використані для викрадення TCPз'єднання та введення даних клієнту або серверу. Зловмисник може використовувати свій власний сервер, підключений до Інтернету, для введення даних у це TCP з'єднання, вводячи сторонні TCP-пакети з підробленою IP-адресою відправника [19, 20]. Цим можна, наприклад, зловживати для надсилання зловмисного коду JavaScript жертві у відкритих HTTP-з'єднаннях з метою використання недоліків у браузері клієнта. Щоб підробити відповіді TCP на адресу клієнта після того, як він дізнався порядкові номери TCP, клієнт повинен повторно підключитися до AP і зробити це до того, як він закриє з'єднання TCP. Щоб переконатися в цьому, зловмисник може надіслати клієнту кадр деаутентифікації з причиною відключення «кадр класу 2 від неавтентифікованої станції» після виконання атаки. Експерименти показали, що це змушує Linux, Windows і iOS повторно підключатися до точки доступу менш ніж за півсекунди. Android відновив підключення менш ніж за 3,5 секунди, що достатньо швидко, щоб згодом ввести дані в активні TCP-з'єднання.

2.7.3 Перехоплення трафіку клієнта

Зловмисник може використовувати виявлені вразливості, щоб дізнатися ідентифікатор порту та транзакції, які використовує клієнт у запитах DNS, які, у свою чергу, можуть бути використані для підробки відповідей DNS і

перехоплення більшості трафіку, надісланого жертвою. Для здійснення цієї атаки зловмисник використовує виявлені нами вразливості, щоб перехопити справжню відповідь DNS щодо жертви. Якщо жертва використовує зашифрований DNS, зловмисник може спробувати заблокувати ці підключення, щоб спонукати жертву повернутися до відкритого DNS через UDP. Пакети можуть бути заблоковані за допомогою методів із розділу 4 або за допомогою багатоканальної позиції MitM **[**22**,** 7**]**. Після того, як зловмисник перехопив відповідь DNS, можна отримати випадковий порт клієнта та ідентифікатор транзакції. Маючи цю інформацію, зловмисник може надсилати підроблені DNS-відповіді зі свого власного сервера в Інтернеті жертві. Зауважте, що протоколи маршрутизації «пакет-впакеті» можуть бути використані для легкого підроблення IP-адреси джерела цієї відповіді DNS **[**20**]**. У Linux, Windows і iOS випадковий ідентифікатор порту та транзакції залишаються дійсними принаймні 6 секунд, цього достатньо, щоб жертва могла повторно підключитися до точки доступу, а зловмисник міг підробити відповідь DNS. Під час тестування Android на Pixel 4 XL випадковий порт і ідентифікатор транзакції залишаються дійсними протягом 5 секунд. У сукупності це дає зловмиснику достатньо часу, щоб спонукати жертву повторно підключитися та вставити підроблену відповідь DNS.

2.7.4 Перехоплення веб-трафіку

Ми можемо перехопити будь-який пакет, який надсилається до клієнта. Це дозволяє здійснювати різні атаки, зокрема перехоплення веб-трафіку. Наприклад, якщо жертва відвідує веб-сайти з відкритим текстом HTTP, зловмисник може викрасти файли cookie жертви. Незважаючи на те, що впровадження HTTPS продовжує зростати **[**23**]**, приблизно 10% відвідувань

веб-сайтів все ще відбувається через підключення у відкритому вигляді**.2** Зловмисник також може перехопити трафік до веб-сайтів локальної інтрамережі, які можуть частіше використовувати відкритий текст HTTP. Коли жертва використовує протоколи шифрування вищого рівня, такі як TLS, зловмисник все одно дізнається IP-адреси, до яких підключається жертва. Це можна поєднати з новими методами аналізу трафіку, наприклад, варіаціями **[**16**]**, щоб дізнатися веб-сайт і веб сторінки, які відвідує жертва.

Висновок

Основною причиною виявлених проблем є те, що стандарт недостатньо чітко визначає зміни контексту безпеки. Найважливішим є те, що зловмисник може витікати фрейми жертви, маніпулюючи захистом тексту у черзі фреймів. Хоча механізми безпеки верхнього рівня, такі як TLS і HTTPS, можуть обмежити ризики, спричинені витоком фреймів Wi-Fi, наприклад, призведуть до витоку IP-адрес, з якими спілкується клієнт, що може розкрити конфіденційну або особисту інформацію. Наприклад, IP-адреса часто може виявити веб-сайт, який відвідує жертва **[**24**]**.

РОЗДІЛ 3
ПЕРЕВИЗНАЧЕННЯ КОНТЕКСТУ БЕЗПЕКИ ЖЕРТВИ

Спочатку зловмисник підключається до точки доступу та створює новий контекст безпеки. Потім точку доступу обманом змушують зв’язати контекст безпеки, який зараз контролює зловмисник, із кадрами, що належать жертві. В результаті зловмисник може розшифрувати кадри, призначені для жертви. Ця атака зловживає недоліками конструкції в тому, як контекст безпеки асоціюється з вихідними кадрами, і її можна використовувати в мережах, схожих на точки доступу.

3.1 Модель загрози

У цьому розділі мета зловмисника — змусити точку доступу передавати кадри в контексті безпеки, контрольованому зловмисником. Щоб зловмисник міг створити контекст безпеки на AP, він повинен мати можливість успішно підключитися до AP. Прикладом таких мереж є корпоративні мережі Wi-Fi, такі як eduroam, або мережі Wi-Fi Passpoint, де користувачі можуть, наприклад, автентифікуватися за допомогою своєї мобільної SIM-карти **[**13**]**. Іншим прикладом є нові мережі SAE-PK WPA3, які є гарячими точками, де користувачі можуть підключатися за допомогою попереднього спільного пароля, але зловмисник не може використовувати цей пароль для створення фальшивих клонів мережі **[**14**]**. Ці мережі налаштовані так, щоб заборонити зв’язок між клієнтами, що запобігає перехопленню одним клієнтом трафіку іншого клієнта, встановлюючи позиції Machine-in-the-Middle за допомогою таких методів, як отруєння ARP **[**15**]**.

3.2 Перевизначення контексту безпеки клієнта

Коли точка доступу передає кадр, відповідний контекст безпеки шукається на основі MAC-адреси відправника та призначення кадру. Це гарантує, що правильні ключі сеансу використовуються для надсилання кадрів кожному клієнту, а ключ групи використовується для захисту широкомовних і багатоадресних кадрів. Проте, якщо зловмисник може змінити контекст безпеки, який AP пов’язує з певною MAC адресою призначення, кадри у черзі передавання будуть захищені за допомогою цього контрольованого зловмисником контексту безпеки.Зловмисник може змінити контекст безпеки, який AP пов’язує з клієнтом, підробивши MAC-адресу клієнта, а потім підключившись до AP. Це змушує точку доступу шифрувати трафік до цього клієнта за допомогою ключів сеансу, якими володіє зловмисник.

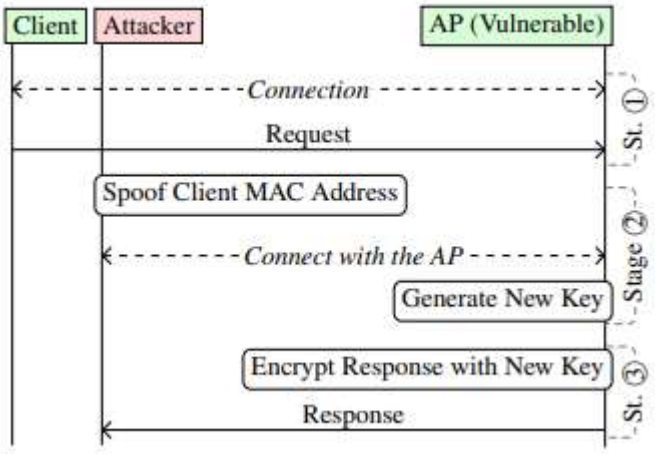

Рис. 3.1 етапи атаки на перевизначення контексту

На рисунку 3.1 проілюстровано окремі етапи цієї атаки:

1. Припустимо, що жертва зараз підключена до AP і збирається отримати кадр, який противник хоче перехопити. Наприклад, жертва може надіслати

HTTP-запит без використання TLS, а зловмисник хоче перехопити відповідь HTTP. Зауважте, що методи аналізу трафіку **[**15, 16**]** можна використовувати для виявлення запитів, відповідь на які зловмисник хоче перехопити.

2. Перш ніж клієнт отримає відповідь, зловмисник підробляє MAC-адресу жертви та підключається до точки доступу, використовуючи власні облікові дані (наприклад, свої особисті облікові дані в корпоративних мережах WPA2 або WPA3). У результаті зловмисник перезаписує контекст безпеки, який AP пов'язує з MAC-адресою жертви, на контекст безпеки, контрольований зловмисником.

3. Тепер точка доступу надсилає кадри на MAC-адресу жертви в контексті безпеки зловмисника. Іншими словами, пакети, призначені для жертви, такі як HTTP відповіді, тепер зашифровані ключами, якими володіє зловмисник. Оскільки пакети, призначені для жертви, тепер зашифровані за допомогою ключів, якими володіє зловмисник, зловмисник може легко їх розшифрувати. Тобто можна обійти шифрування на рівні Wi-Fi. Зауважте, що навіть якщо відповідь зашифровано на вищому рівні за допомогою протоколу, такого як TLS, атака все одно призведе до витоку IP-адрес, до яких підключається жертва. Якщо багатофункціональний пристрій не використовується, це можна зробити шляхом підробки кадрів деавтентифікації. Якщо жертва використовує багатофункціональний пристрій, вразливості реалізації зазвичай все ще можна використовувати для відключення клієнтів [17]. Одним із практичних обмежень атаки є те, що зловмиснику може знадобитися значний проміжок часу, щоб з'єднатися з точкою доступу на етапі 2 атаки, що може призвести до втрати відповіді. Наприклад, під час автентифікації за допомогою протоколів на основі EAP для автентифікації клієнта зазвичай використовується віддалений сервер RADIUS, і зв'язок із цим

сервером може призвести до великих затримок. Якщо відповідь, яку ми хочемо перехопити, надсилається через TCP, це не проблема: відправник автоматично повторно передасть її, якщо не буде підтверджено. Однак для таких протоколів, як UDP, це може бути проблематично, оскільки відповідь може бути пропущена. Атака не залежить від використовуваної схеми автентифікації та шифрування, Головною передумовою є те, що зловмисник повинен мати облікові дані для підключення до мережі, схожої на точку доступу. Зокрема, атака працює проти WPA2 і WPA3 незалежно від їх точних налаштувань.

3.3 Атака на швидке (повторне) підключення

Атака обмежена швидкістю зловмисника, який може підключитися до точки доступу, щоб перевизначити контекст безпеки жертви. Проте стандарт 802.11 надає кілька методів кешування асоціації безпеки та відновлення її пізніше без виконання повного рукостискання. Найстарішим таким методом є кешування попарного головного ключа (PMK). У разі використання кешування PMK точка доступу зберігатиме узгоджений PMK, отриманий у результаті автентифікації 802.1X або SAE-PK. Ідентифікатор PMK (PMKID) використовується для посилання на цю асоціацію безпеки. Припустимо, що мережа складається щонайменше з двох різних ідентифікаторів базового набору послуг (BSSID). Іншими словами,припускаємо, що мережа транслюється принаймні двома точками доступу або однією точкою доступу на двох або більше каналах.

1. Зловмисник спочатку підробляє MAC-адресу жертви та використовує власні облікові дані для підключення до AP1 мережі. AP1 буде кешувати PMK, який було узгоджено під час (часто повільної) автентифікації 802.1X. 2. Жертва з’єднується з AP2, яка кешує PMK, який клієнт погоджує під час рукостискання

802.1X. Більшість точок доступу зберігають лише один кешований PMK для кожної MAC-адреси клієнта. Тому важливо, щоб жертва не підключалася до тієї ж точки доступу, що й зловмисник, інакше кешований PMK зловмисника буде перезаписано. Після підключення жертва надішле запит на сервер, відповідь якого ми хочемо перехопити.

3. Щоб перехопити відповідь сервера, зловмисник використовує кешований PMK для повторного підключення до AP1. Це досягається шляхом включення PMKID у запит на асоціацію. Оскільки кешований PMK (все ще) доступний на AP1, автентифікацію 802.1X можна пропустити, а 4-стороннє рукостискання може бути негайно виконано для узгодження ключів сеансу. Після підключення відповідь AP1 буде надіслано супротивнику. Зауважте, що жертва передала запит через AP2, але відповідь була надіслана противнику через AP1. Це можливо, тому що обидві точки доступу підключені до однієї розподільчої системи, тобто до однієї внутрішньої мережі. Загалом, точка доступу, за допомогою якої клієнт востаннє автентифікувався, буде точкою доступу, яка передає відповідь клієнту. У цьому варіанті атаки не потрібно відключати жертву від мережі. Система розповсюдження перенаправлятиме весь трафік до останньої точки доступу, за допомогою якої MAC-адреса клієнта була востаннє автентифікована. У результаті атака працює, навіть якщо жертва залишається підключеною до іншої точки доступу, тобто використання MFP не впливає на атаку [18].

3.4 Захист

Щоб пом’якшити атаки на мережі, схожі на точки доступу, точка доступу може тимчасово заборонити клієнтам підключатися, якщо вони використовують MAC адресу, яку нещодавно підключили до точки доступу. Це

запобігає зловмиснику від підробки MAC-адреси та перехоплення кадрів, що очікують або стоять у черзі до жертви. Коли можна гарантувати, що користувач за MAC-адресою не змінився, клієнту можна дозволити негайно повторно підключитися. Зауважте, що цю перевірку потрібно виконувати для всіх точок доступу, які є частиною однієї системи розподілу. Щоб безпечно розпізнавати нещодавно підключених користувачів, точка доступу може зберігати зіставлення між MAC-адресою клієнта та його кешованими асоціаціями безпеки (наприклад, їхнім кешованим PMK). Клієнту дозволено негайно (повторно) підключитися за нещодавно використаною MAC-адресою, довівши, що він володіє своїм кешованим зв'язком безпеки, наприклад, підключившись за допомогою правильного кешованого PMK. Інший метод безпечного розпізнавання нещодавно підключених користувачів базується на Ідентифікація EAP, яку вони використовували під час автентифікації 802.1X. Точка доступу може безпечно дізнатися ідентифікатор EAP від RADIUS-сервера, який аутентифікував клієнта **[**19**]**, і може зберігати відображення нещодавно підключених MAC-адрес і їх відповідну ідентифікацію EAP. Коли клієнт підключається, точка доступу перевіряє, чи нещодавно використовувалася його MAC-адреса. Якщо це не так, або якщо це так, і клієнт використовує ту саму ідентифікацію EAP, що й раніше, клієнт може підключитися як зазвичай. Однак, якщо та сама MAC-адреса використовується під іншим ідентифікатором EAP, клієнт змушений чекати заздалегідь визначений проміжок часу, перш ніж зможе успішно підключитися. Наведені вище засоби захисту припускають, що після певної затримки жертві більше не надходитимуть пакети в очікуванні. Щоб запобігти витоку після цієї затримки, клієнти можуть використовувати наскрізне шифрування, наприклад TLS, зі службами, з якими вони спілкуються.

Висновок

Для створення контексту безпеки на точці доступу (AP), зловмиснику необхідно успішно підключитися до мережі, що вимагає дійсних облікових даних та зазвичай є мережею, де користувачі не довіряють один одному. Прикладами таких мереж можуть бути корпоративні мережі Wi-Fi, як eduroam, Wi-Fi Passpoint або нові мережі SAE-PK WPA3.

Зловмисники спрямовують свої атаки на ці мережі, де обмежена взаємодія між клієнтами унеможливлює перехоплення трафіку одним клієнтом від іншого, використовуючи методи, такі як отруєння ARP. Застосування цих методів дозволяє створювати контекст безпеки на точках доступу та контролювати передачу кадрів в цьому контексті, що дає зловмиснику можливість втручатися в безпеку та здійснювати атаки в цьому обмеженому контурі.

Отже, важливо враховувати, що наведені приклади мереж вимагають високого рівня захисту, оскільки вони створюють обмежені умови взаємодії між клієнтами. Належна захищеність та вдосконалення методів автентифікації та авторизації є ключовими аспектами для запобігання можливим атакам та збереження безпеки бездротових мереж, особливо в обмежених контекстах взаємодії між користувачами.

РОЗДІЛ 4
ТЕСТУВАННЯ МЕРЕЖІ ТА ІДЕНТИФІКАЦІЯ СЛАБКИХ МІСЦЬ

В цьому розділі надано інформацію про практичне використання MacStealer та проводиться перевірка мережі на вразливості типу ARP-отруєння та ін.

Алгоритм використання MacStealer

cd research

sudo su

source venv/bin/activate

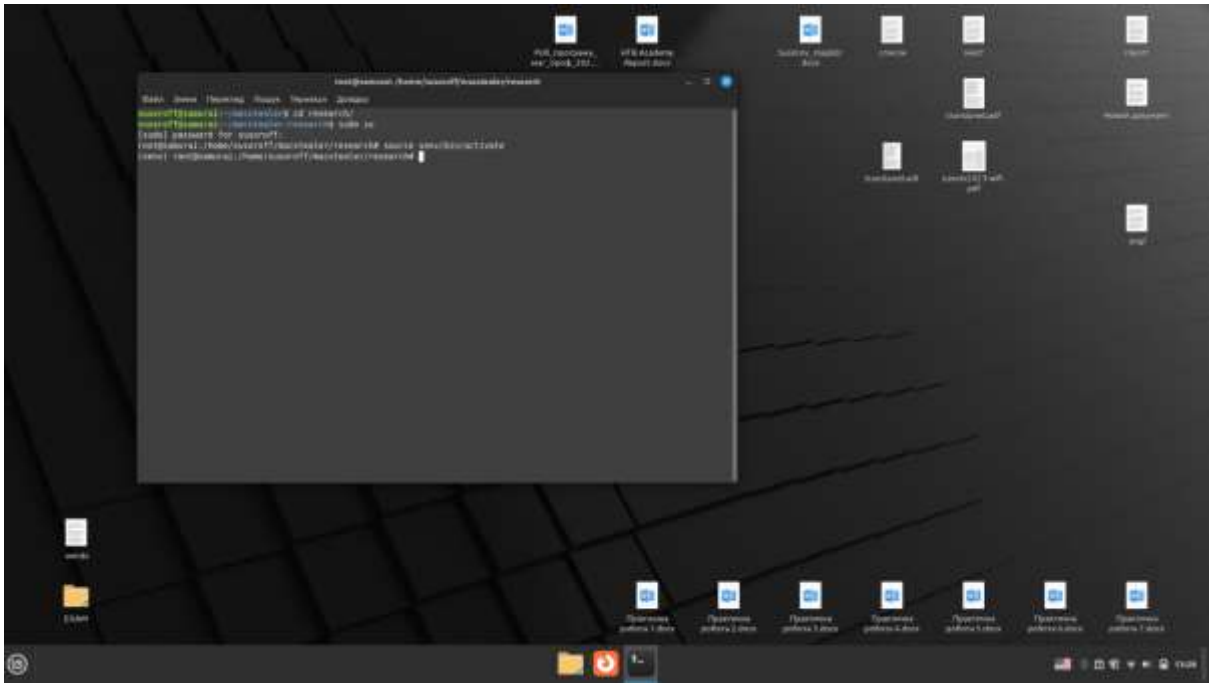

Рис. 4.1 перехід до робочої теки та отримання root

Тепер треба вимкнути Wi-Fi у своєму менеджері мережі, щоб він не заважав MacStealer. Додатково перевіримо за допомогою sudo airmon-ng check, щоб дізнатися, які інші процеси можуть використовувати карту бездротової мережі та можуть заважати MacStealer.

Також можна вимкнути Wi-Fi через командний рядок:

```
nmcli radio wifi off
```

Після вимкнення Wi-Fi у мережевому менеджері потрібно буде виконати таку команду, щоб усе ще мати можливість використовувати Wi-Fi з командного рядка:

```
rfkill unblock wifi
```

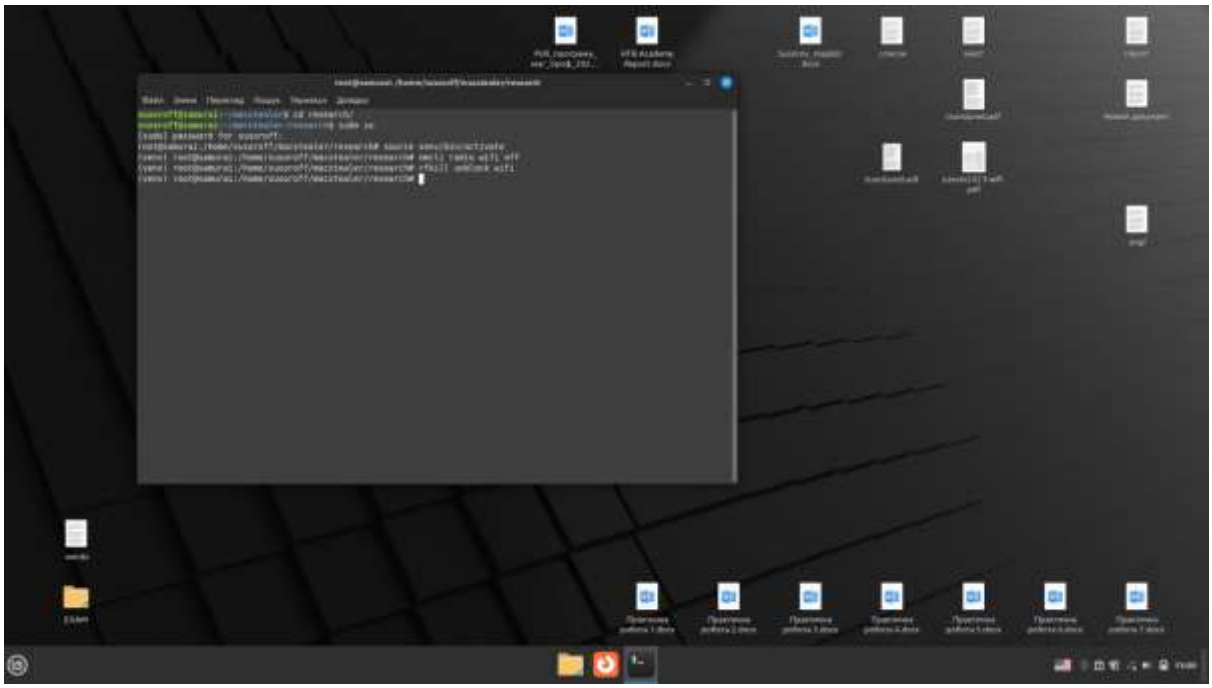

Рис. 4.2 вимкнення Wi-Fi через командний рядок

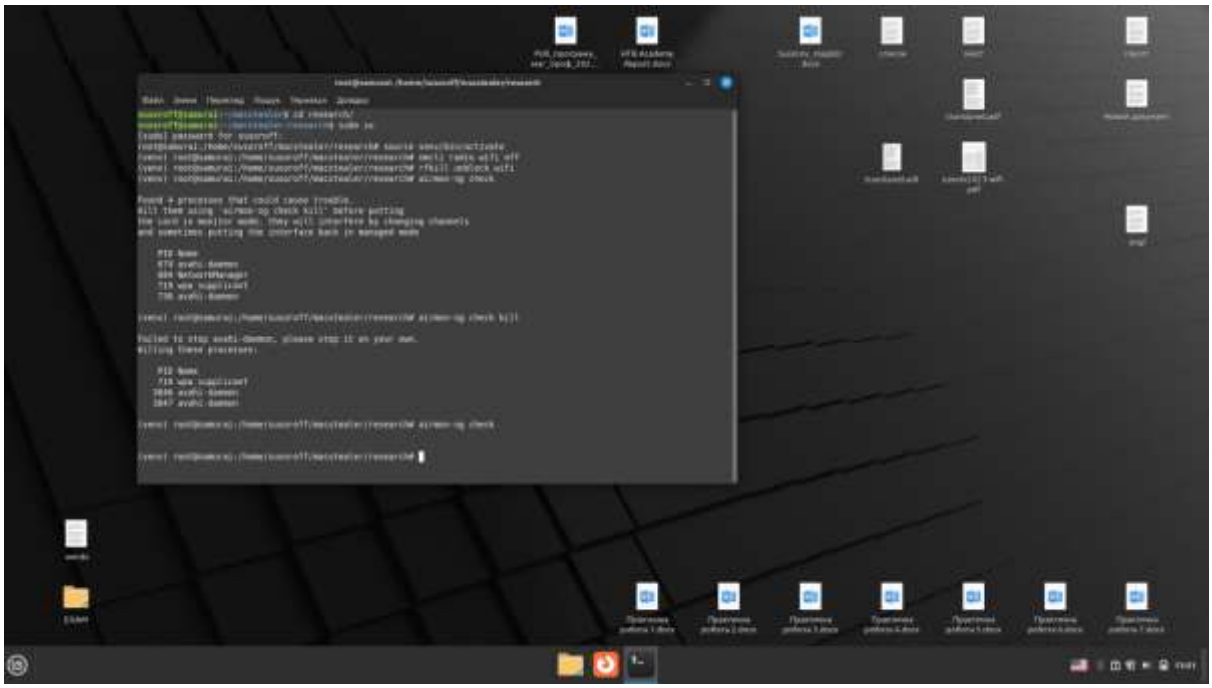

Рис. 4.3 перевірка процесів які використовують мережу

Наступним кроком є редагування client.conf з інформацією про мережу.Це конфігурація для wpa_supplicant, яка має містити два мережеві блоки: один представляє жертву, а інший — атакуючого. Приклад файлу конфігурації для тестування мереж:

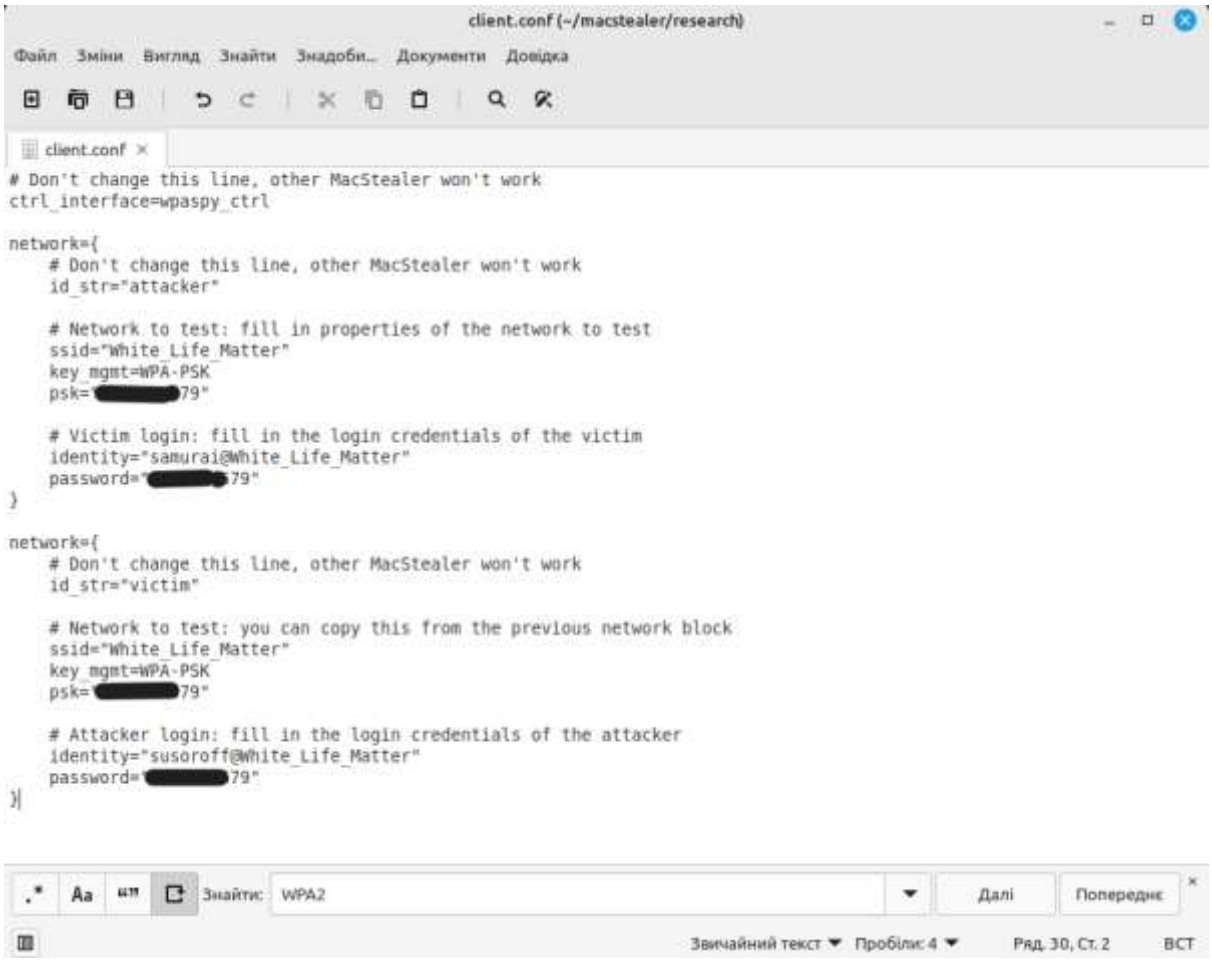

Рис. 4.4 приклад файлу конфігурації

У наведеній нижче таблиці 4.1 наведено типові команди, які ви виконуватимете під час тестування мережі, а також короткий опис того, що робить кожна команда. Під таблицею пояснюються деталі кожної команди.

Таблиця 4.1

Команда	Короткий опис
./macstealer.py wlan0 --ping	Підключення як жертва та перевірка поведінки повторної передачі сервера.
./macstealer.py wlan0 --ping --flip	Підключіться як зловмисник та перевірте поведінку повторної передачі сервера.
./macstealer.py wlan0	Перевірте стандартний варіант атаки з крадіжкою MAC-адреси.
./macstealer.py wlan0 --other-bss	Зловмисник підключається до іншої точки доступу, ніж жертва.
./macstealer.py wlan0 --c2c wlan1	Перевірка трафіку рівня Ethernet клієнт-клієнт (отруєння ARP).
./macstealer.py wlan0 --c2c-eth wlan1	Перевірка трафіку рівня Ethernet (DNS) клієнт-клієнт.

./macstealer.py wlan0 --ping: підключається до мережі за допомогою облікових даних жертви. Після з’єднання TCP SYN надсилається на сервер (який за замовчуванням 8.8.8.8 і може бути змінений). MacStealer перевірить, чи (повторно) передається SYN/ACK і скільки разів. Ви можете використовувати це, щоб підтвердити правильність облікових даних жертви та перевірити, чи правильно налаштований сервер повторно передає відповіді SYN/ACK.

./macstealer.py wlan0 --ping --flip: те саме, що й вищевказаний тест, але тепер сценарій підключатиметься за допомогою облікових даних зловмисника.

Ви можете використовувати це, щоб підтвердити, що облікові дані зловмисника правильні.

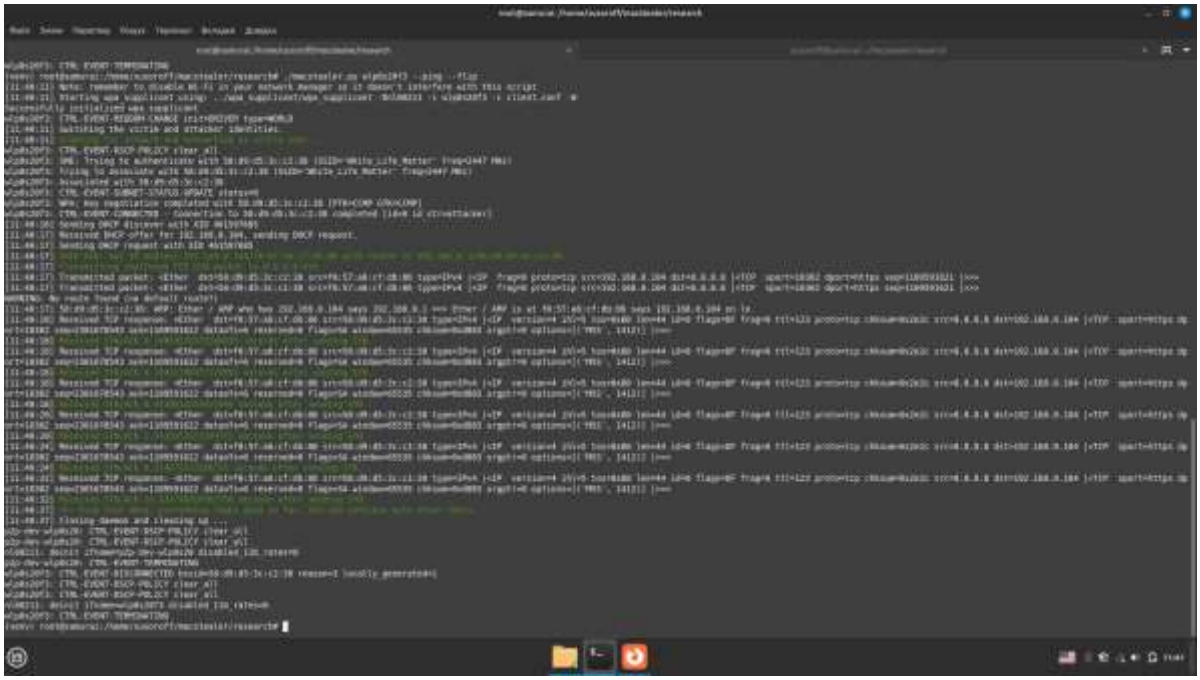

Рис. 4.5 результати з прапорцями --ping --flip

./macstealer.py wlan0: перевіряє стандартний варіант атаки викрадача MAC-адреси. Зловмисник повторно підключається до тієї ж AP/BSS, що й жертва.

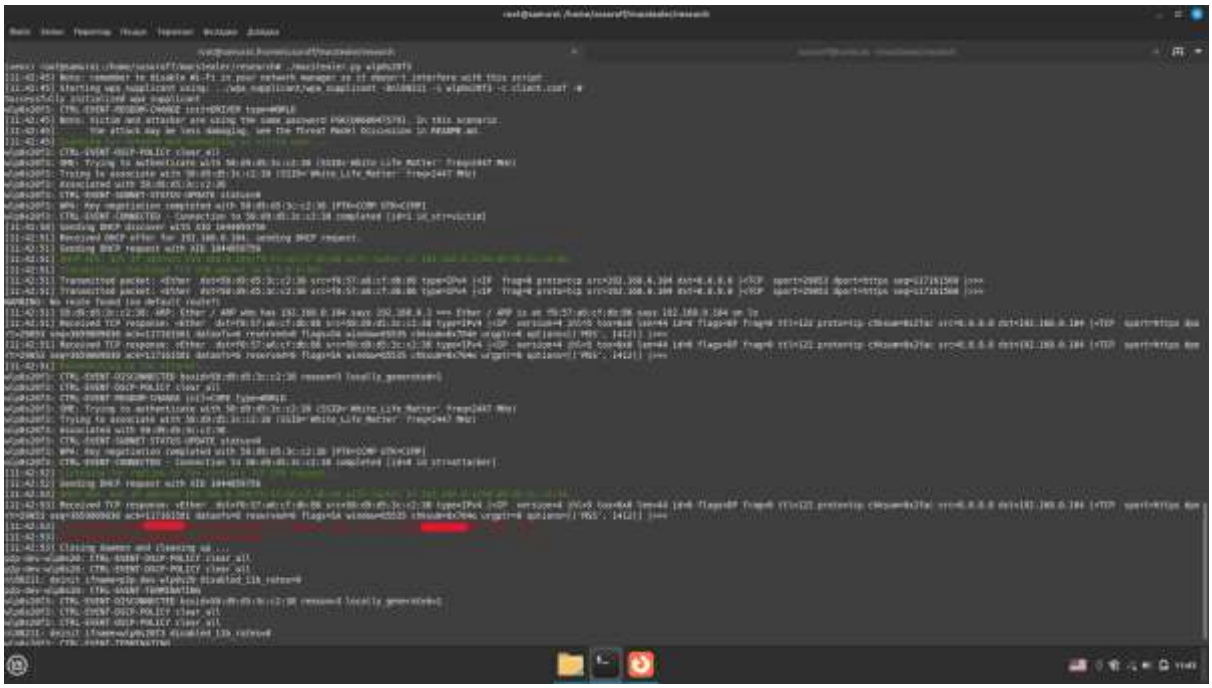

Рис. 4.6 результати стандартного варіанта атаки

Як видно з рисунка 4.6, що система є вразливою до атаки викрадення MAC-адреси, це означає, що система (зокрема, мережевий інтерфейс, що використовується для бездротового з'єднання) не належним чином захищена від атак, які спрямовані на використання або злам MAC-адреси.

Атака викрадення MAC-адреси може призвести до небезпечних наслідків, зокрема:

- Перехоплення трафіку: Зловмисники можуть перехоплювати трафік, який передається між вашим пристроєм і точкою доступу (AP/BSS), використовуючи викрадену MAC-адресу.
- Атаки людини посередника (Man-in-the-Middle): За допомогою викрадення MAC-адреси зловмисники можуть впроваджуватися між вами та точкою доступу, перехоплюючи чи модифікуючи передавані дані.

- Спостереження за мережевою активністю: Атаки на викрадення MAC-адрес можуть дозволити зловмисникам стежити за активністю пристрою в бездротовій мережі.

./macstealer.py wlan0 --other-bss: зловмисник підключається до іншого AP/BSS тієї ж мережі. Мережу, яка (також) вразлива до цього тесту, легше використовувати на практиці.

Використання вразливості викрадення MAC-адреси має сенс, лише якщо ввімкнено ізоляцію клієнта або коли використовуються такі методи, як перевірка ARP, щоб запобігти атакам клієнтів один на одного. В іншому випадку зловмисник може використовувати простіші атаки, такі як отруєння ARP, щоб перехопити трафік. Щоб перевірити, чи ввімкнено ізоляцію клієнта, чи використовується перевірка ARP у мережі, можна використати такі команди:

./macstealer.py wlan0 --c2c wlan1: за допомогою цих аргументів MacStealer перевіряє, чи допускає мережа міжклієнтський трафік ARP-отруєння від зловмисника (wlan1) до жертви (wlan0). Тут wlan1 є другим інтерфейсом бездротової мережі. Потім сценарій перевірить, чи можуть шкідливі ARP-пакети надсилатися від зловмисника до жертви.

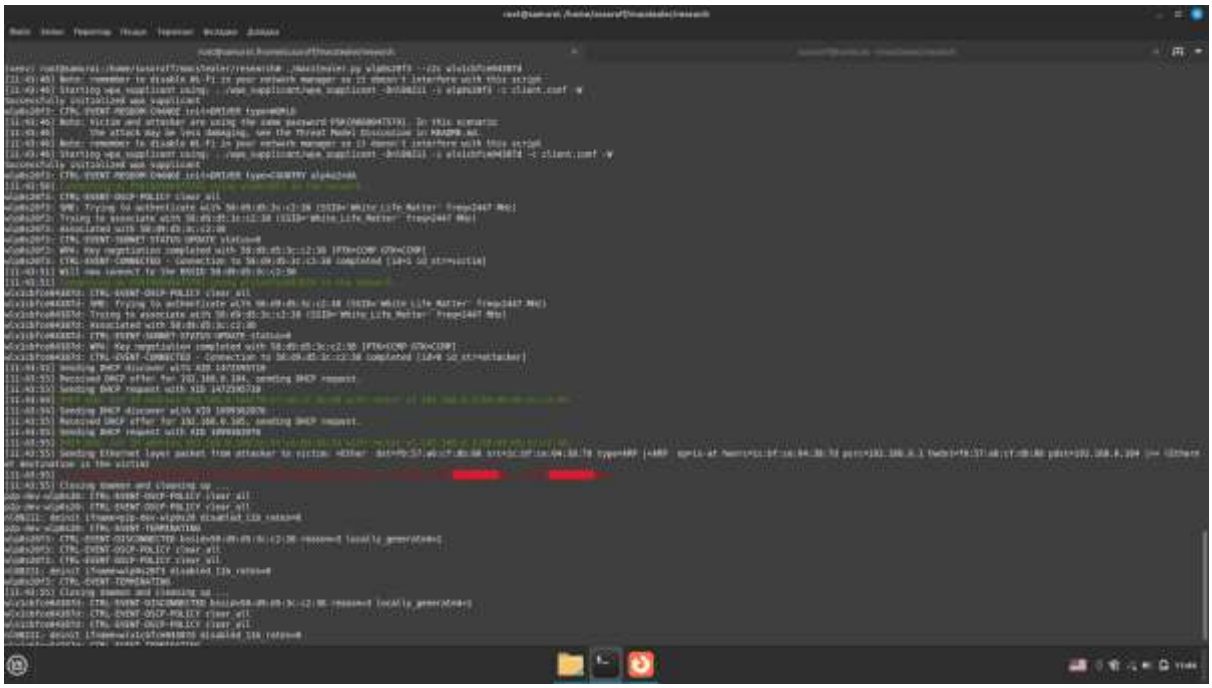

Рис. 4.7 результати виконання програми з прапорцем --c2c

Бачимо на рисунку 4.7, що система вразлива до міжклієнтського трафіку ARP-отруєння, це означає, що ваша мережа дозволяє зловмиснику (представленому інтерфейсом wlan1) відправляти шкідливі ARP-пакети до жертви (представленої інтерфейсом wlan0). ARP-отруєння - це вид атаки, коли зловмисник відправляє неправдиві ARP-відповіді для спроби змінити таблиці маршрутизації на устройствах в мережі. Це може призвести до наступного:

- Отримання неправильних маршрутів: Зловмисник може направляти мережевий трафік через свій власний пристрій, що може призвести до перехоплення чи модифікації даних.
- Атаки на міжклієнтські з'єднання: Зловмисник може спробувати перехопити комунікацію між різними пристроями в мережі, включаючи вашу жертву.

- Підробка мережевого трафіку: Зловмисник може надсилати шкідливий трафік, що виглядає як відомий та довірений, щоб перехопити чи модифікувати дані.

./macstealer.py wlan0 --c2c-eth wlan1: це схоже на наведений вище тест, але замість зловмисних ARP-пакетів зловмисник надішле жертві DNS-пакети.

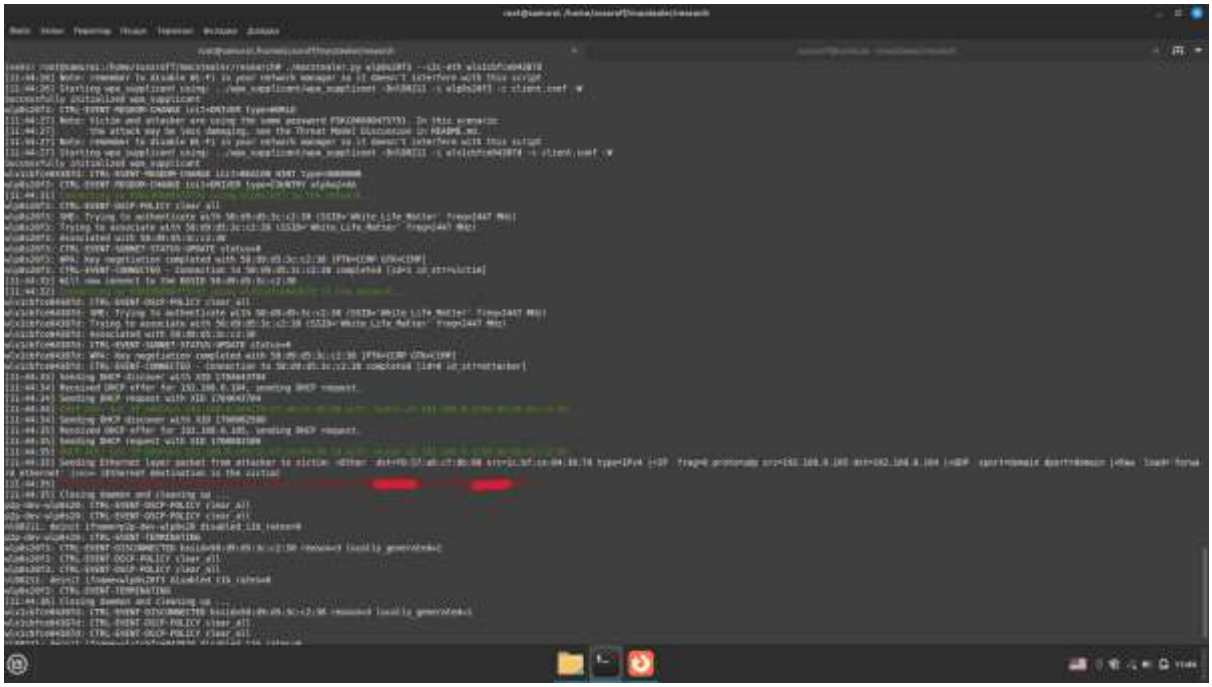

Рис. 4.8 результати виконання програми з прапорцем --c2c-eth

Якщо програма повідомляє, що система вразлива до такого типу атаки (наприклад, відправка DNS-пакетів від зловмисника на жертву), це може мати серйозні наслідки для безпеки мережі:

- DNS-спуфінг (підробка): Зловмисник може надсилати фальшиві DNS-відповіді на запити жертви, перенаправляючи її на підроблені або шкідливі веб-сторінки.

- Перехоплення даних: Зловмисник може перехоплювати DNS-запити жертви, отримуючи доступ до чутливої інформації, такої як відвідувані веб-сайти.
- Атаки на безпеку мережі: Зловмисник може використовувати цей метод для порушення безпеки мережі, здійснюючи атаки типу "людина посередника" чи підробки.

Уразливість крадіжки MAC-адреси слід розглядати як ризик на практиці, якщо трафік клієнт-клієнт заблоковано в будь-якому з двох вищезазначених тестів (тобто, коли ввімкнено ізоляцію клієнта або коли використовуються інші методи, такі як перевірка ARP, щоб запобігти користувачам від зловмисника один одного).

За замовчуванням MacStealer намагатиметься підключитися до однієї AP/BSS за допомогою обох інтерфейсів, тому важливо, щоб обидві мережеві карти бачили однакові мережі (тобто переконайтеся, що обидва мережеві інтерфейси підтримують однакові частотні діапазони та канали). Якщо ви хочете, щоб обидва клієнти підключалися до різних AP/BSS, ви можете використовувати параметр --other-bss.

Ви можете використовувати параметр --flip-id, щоб перевірити, чи дозволений трафік від жертви (wlan0) до зловмисника (wlan1).

Висновок

В даному розділі було показано на практиці процес ідентифікації вразливостей в мережі та показано типові команди які використовуються для тестування.

РОЗДІЛ 5
СПОСОБИ ПОМ'ЯКШЕННЯ АТАК

В цьому розділі надано огляд вже відомим пом’якшенням та оглянуто запропоновані нові.

5.1. Запобігання крадіжці MAC-адреси

Щоб пом’якшити атаку, точка доступу може тимчасово заборонити клієнтам підключатися, якщо вони використовують MAC-адресу, яку нещодавно підключили до точки доступу. Це запобігає зловмиснику від підробки MAC-адреси та перехоплення кадрів, що очікують або стоять у черзі до жертви. Коли можна гарантувати, що користувач за MAC-адресою не змінився, клієнту можна дозволити негайно повторно підключитися. Зауважте, що цю перевірку потрібно виконувати для всіх точок доступу, які є частиною однієї системи розподілу, а точніше, для всіх точок доступу, між якими клієнти можуть переміщатися, зберігаючи свою поточну IP-адресу.

Щоб безпечно розпізнавати нещодавно підключених користувачів, точка доступу може зберігати відображення між MAC-адресою клієнта та його кешованими асоціаціями безпеки (наприклад, їхнім кешованим PMK). Клієнту можна дозволити негайно (повторно) підключитися за нещодавно використаною MAC-адресою, довівши, що він володіє кешованим зв’язком безпеки, пов’язаним із цією MAC-адресою, наприклад, шляхом підключення за допомогою правильного кешованого PMK.

У разі використання мульти-PSK, який також відомий як PSK для станції або PSK ідентифікації , точка доступу може зберігати відображення нещодавно

підключених MAC-адрес і (унікальний) пароль, який вони використовували. Коли клієнт підключається, точка доступу перевіряє, чи нещодавно використовувалася його MAC-адреса. Якщо це не так, або якщо це так і клієнт використовує той самий пароль, що й раніше, клієнт може підключитися як зазвичай. Однак, якщо та сама MAC-адреса використовується з іншим паролем, клієнт змушений чекати заздалегідь визначений проміжок часу, перш ніж зможе успішно підключитися.

Під час використання SAE-PK для захисту точок доступу єдиним відомим нам способом безпечного розпізнавання того, що MAC-адреса повторно використовується тим самим користувачем, що й раніше, є використання кешованих асоціацій безпеки (наприклад, кешованого PMK, пов’язаного з MAC-адреса).

Наведені вище засоби захисту припускають, що після певної затримки жертві більше не надходитимуть пакети в очікуванні. Щоб запобігти витокам після цієї затримки, клієнти можуть використовувати наскрізне шифрування (наприклад, TLS) зі службами, з якими вони спілкуються.

5.2. Аутентифікація 802.1X і розширення RADIUS

Інший метод безпечного розпізнавання нещодавно підключених користувачів базується на ідентифікації EAP, яку вони використовували під час автентифікації 802.1X. Точка доступу може безпечно дізнатися ідентифікатор EAP від RADIUS-сервера , який автентифікував клієнта, і може зберігати відображення нещодавно підключених MAC-адрес і їх відповідний ідентифікатор EAP. Коли клієнт підключається, точка доступу перевіряє, чи нещодавно використовувалася його MAC-адреса. Якщо це не так, або якщо це

так, і клієнт використовує ту саму ідентифікацію EAP, що й раніше, клієнт може підключитися як зазвичай. Однак, якщо та сама MAC-адреса використовується під іншим ідентифікатором EAP, клієнт змушений чекати заздалегідь визначений проміжок часу, перш ніж зможе успішно підключитися.

Однією з проблем є те, що точка доступу може не завжди знати ідентифікаційні дані клієнта 802.1X через проблеми конфіденційності. Наприклад, ця інформація може бути доступна лише на домашньому сервері AAA, а точка доступу отримуватиме платний ідентифікатор користувача лише від сервера RADIUS. Цей ідентифікатор не дозволяє точці доступу розпізнавати дві асоціації одного пристрою/облікових даних, оскільки його значення може постійно змінюватися. Точка доступу отримує анонімний ідентифікатор у відповіді/ідентифікації EAP, наприклад anonymous@realm, і може покладатися на нього, щоб принаймні розпізнавати користувачів із різних сфер.

Щоб запобігти атакам користувачів в одній сфері один на одного без розкриття особи клієнта точці доступу, потрібна співпраця та зміни на сервері RADIUS. Зокрема, RADIUS-сервер можна оновити, щоб допомогти виявити, чи MAC-адреса нещодавно використовувалася іншим користувачем у тій самій області (у даній локальній мережі). Тоді RADIUS-серверу потрібно буде повідомити, коли клієнт від’єднується, щоб він знав, коли MAC-адреса востаннє використовувався одним із його користувачів, і повинен бути поінформований про MAC-адресу будь-якого клієнта, який намагається підключитися.

5.3. Захист MAC-адреси шлюзу

Важливо відзначити, що атака не обмежується перехопленням пакетів, що надходять до клієнтів Wi-Fi. Зловмисник також може спробувати зв’язатися з MAC-адресою стандартного шлюзу або іншого сервера в локальній мережі. Щоб запобігти таким атакам, точка доступу або контролер можуть заборонити клієнтам використовувати MAC-адресу, що дорівнює шлюзу за замовчуванням. Загалом, виявлення дублікатів MAC-адрес можна використовувати, коли клієнт Wi-Fi підключається до мережі, щоб запобігти клієнтам Wi-Fi використовувати MAC-адресу, яка також використовується іншими пристроями в мережі.

5.4. Захист кадрів керування (802.11w)

Використання Management Frame Protection (MFP) зробить атаку складнішою, але не неможливою. Завжди існує якийсь спосіб примусового відключення клієнта від мережі, навіть якщо використовується багатофункціональний пристрій. Інакше кажучи, важко повністю запобігти атакам відключення та деаутентифікації. Зважаючи на це, MFP стане додатковою перешкодою, яку потрібно подолати під час виконання атаки на практиці, тому це може бути корисним пом’якшенням, щоб зробити атаку важчою (але не неможливою) на практиці.

5.5. Використання VLAN

Одним із способів пом’якшення є розміщення різних груп користувачів у різних VLAN. Однак зловмисник все одно зможе здійснити атаку (тобто обійти ізоляцію клієнта) проти інших користувачів у тій же VLAN.

Зауважте, що під час використання мульти-PSK (також відомого як PSK для станції або ідентифікаційний PSK) ви можете розмістити клієнтів у різних

VLAN залежно від пароля, який вони використовують. Іншими словами, ви можете використовувати VLAN для кожного пароля. Це запобігає атакам один одного клієнтами з різними паролями[2].

5.6 Запропоновані пом’якшення

5.6.1 Обмеження доступу до конфігурації точки доступу:

Встановлення паролів та обмеження фізичного доступу до налаштувань точки доступу, що зменшить ризик несанкціонованої зміни налаштувань мережі.

Обмеження доступу до конфігурації точки доступу є важливою частиною стратегії забезпечення безпеки мережі Wi-Fi. Це означає введення певних заходів, які перешкоджають несанкціонованому доступу до налаштувань точки доступу, запобігаючи можливим змінам, що можуть стати джерелом потенційних загроз для безпеки мережі. Важливо встановити сильні паролі або ключі доступу до налаштувань точки доступу. Крім того, фізичний доступ до обладнання має бути обмеженим для упевненості, що тільки авторизовані особи матимуть доступ до конфігурації. Встановлення системи автентифікації, яка підтверджує, що тільки вповноважені особи мають доступ до налаштувань.Ведення журналу доступу до налаштувань точки доступу для виявлення незвичайних або неавторизованих спроб доступу. Регулярна зміна паролів та ключів доступу до налаштувань для уникнення можливих загроз внаслідок компрометації або несанкціонованого доступу.Ці заходи допомагають запобігти несанкціонованій зміні налаштувань мережі та забезпечити високий рівень безпеки точок доступу Wi-Fi. Особливу увагу слід приділити управлінню паролями та фізичної безпеці обладнання, що використовується для управління мережею.

5.6.2 Шифрування мережі Wi-Fi

Використання шифрування, такого як WPA2/WPA3, для захисту передаваних даних між точкою доступу та клієнтами.

5.6.3 Обмеження передачі інформації між клієнтами:

Обмеження передачі інформації між клієнтами в мережі Wi-Fi є важливим заходом для підвищення безпеки та запобігання певним видам атак на рівні MAC. Пропонується такий метод як в**икористання функції Access Control Lists (ACL)**.

Функція Access Control Lists (ACL) є потужним інструментом для управління безпекою мережі та контролю доступу до ресурсів в мережевих пристроях, таких як маршрутизатори чи точки доступу Wi-Fi. Налаштування списків керування доступом через ACL дозволяє обмежувати або дозволяти взаємодію між конкретними пристроями в мережі за допомогою правил фільтрації трафіку.

Основні принципи та можливості використання ACL включають:

- **Фільтрація пакетів даних:** ACL може бути використаний для фільтрації трафіку на основі різних критеріїв, таких як IP-адреси, порти, протоколи тощо. Це дозволяє обмежувати або дозволяти комунікацію між певними пристроями чи мережними сегментами.
- **Керування правами доступу:** ACL дозволяє налаштовувати правила, які визначають, які пристрої можуть здійснювати з'єднання з іншими пристроями у мережі і які ресурси вони можуть використовувати.

- **Захист від несанкціонованого доступу:** Використання ACL дозволяє створювати правила, які блокують небажану комунікацію або запобігають несанкціонованому доступу до ресурсів мережі.
- **Можливість встановлення пріоритетів:** ACL може бути налаштований таким чином, щоб встановлювати пріоритети для різних видів трафіку, дозволяючи пропускати або блокувати трафік залежно від заданих умов.

5.6.4 Використання сегментації мережі:

Використання сегментації мережі є ефективною стратегією для підвищення безпеки та контролю в мережевих середовищах. Ця стратегія передбачає розділення мережі на окремі підмережі чи сегменти залежно від функцій, груп користувачів, типів пристроїв тощо. Для забезпечення безпеки мережі можна виділити такі плюси:

- **Ізоляція ресурсів:** Розділення мережі дозволяє ізолювати групи пристроїв чи користувачів одні від одних, що зменшує ризик неконтрольованого доступу та можливість проникнення атак з одного сегменту мережі на інший.
- **Контроль доступу:** Кожен сегмент мережі може мати свої правила доступу та політики безпеки, що дозволяє адміністраторам керувати доступом до ресурсів та послуг у кожній підмережі.
- **Зменшення ризику розповсюдження атак:** В разі, якщо атака відбувається в одній частині мережі, сегментація допомагає уникнути чи зменшити її вплив на інші частини мережі, оскільки вона обмежує можливість розповсюдження атаки за межі сегментів.

- **Підвищення продуктивності та безпеки:** Сегментація дозволяє збільшити ефективність мережі, оскільки дозволяє кожному сегменту працювати незалежно, а також забезпечує вищий рівень безпеки.
- **Поліпшення управління мережею:** Керування сегментованими частинами мережі може бути спрощеним, оскільки дозволяє швидше виявляти та реагувати на проблеми безпеки чи аномальну активність у кожному окремому сегменті.

5.6.5 Використання інтрузійних виявлення та систем управління безпекою:

Встановлення системи моніторингу, яка виявлятиме аномальну активність в мережі та надасть можливість вчасно реагувати на потенційні загрози.

5.6.6 Створення мережевих політик безпеки:

Створення мережевих політик безпеки є важливим етапом в забезпеченні безпеки мережі та захисті її від потенційних загроз. Це включає в себе розробку, впровадження та виконання суворих правил і налаштувань, які визначають, як повинна функціонувати мережа та які дії дозволені чи заборонені.

5.6.7 Постійне навчання персоналу:

Організація навчань та тренувань для персоналу щодо кібербезпеки, адже соціальна інженерія може бути також значною загрозою для безпеки мережі.

5.6.8 Шифрування чутливої інформації:

Шифрування даних, особливо чутливої інформації, навіть у випадку, якщо мережа вже зашифрована, що допоможе додатково захистити дані від несанкціонованого доступу.

5.6.9 Регулярні аудити безпеки:

Проведення регулярних аудитів безпеки мережі для виявлення вразливостей та вжиття заходів для їх виправлення. Регулярні аудити безпеки мережі є важливою складовою процесу забезпечення безпеки і захисту від потенційних загроз. Ці аудити допомагають ідентифікувати вразливості, слабкі місця та можливі ризики в мережі для того, щоб прийняти необхідні заходи для зміцнення безпеки.

Висновок

У цьому розділу було оглянуто старі методи захисту мережі та запропоновано нові методи які включають комплексний підхід та можуть доповнювати наявні стратегії захисту мережі.

РОЗДІЛ 6
РОЗРОБЛЕННЯ СТАРТАП-ПРОЕКТУ

6.1 Опис ідеї проекту

IntraSecure - це стартап, що пропонує аналіз та вирішення проблем безпеки, пов'язаних з вразливостями маршрутизаторів. Ця ідея проекту має потенціал покращити безпеку мереж, що використовують маршрутизатори, і захищати їх від потенційних загроз та атак. Опис ідеї стартап-проекту продемонстровано у таблиці 6.1.

Таблиця 6.1

Опис ідеї стартап-проекту

Напрямки застосування	Вигоди для користувача
Бізнес-сектор: Підприємства будуть в змозі захищати свої корпоративні мережі та конфіденційні дані від інтрузій і атак, що можуть призвести до втрати інформації або порушення операцій.	Захист від загроз: Користувачі отримають надійний захист від різних видів інтрузій і атак на їхні мережі та системи.
Постачальники послуг Інтернету: Ці компанії можуть забезпечувати високий рівень безпеки для своїх клієнтів.	Моніторинг та сповіщення: Користувачі будуть інформовані про будь-яку підозрілу активність та отримають сповіщення для оперативної реакції.

Продовження таблиці 6.1

Інтернет речей (IoT): Система може бути використана для захисту мереж та систем, що використовуються в сфері IoT, де безпека є критично важливою.	Виявлення вразливостей: Система допоможе користувачам виявити та виправити вразливості в їхніх маршрутизаторах для покращення безпеки.
Розумні міста: Встановлення в містах для захисту розумних мереж та систем, що контролюють інфраструктуру та послуги міста.	Звітність та аналіз: Користувачі зможуть отримувати звіти та аналіз безпеки своїх мереж для подальшого удосконалення.
	Забезпечення неперервності бізнесу: Захист від інтрузій допоможе уникнути перебоїв в роботі та втрати даних.
	Спрощена адміністрація: Всі ці функції допоможуть спростити управління мережами та безпекою.

Визначення сильних, слабких та нетральних характеристик ідеї проекту подано у таблиці 6.2

Таблиця 6.2

№ п/п	Техніко-економічні характеристики ідеї	(потенційні) товари/концепції конкурентів			W (слабка сторона)	N (нейтральна сторона)	S (сильна сторона)
		Мій проект	Rapid7	IBMSecurity Appliance			
1	Використання безкоштовного програмного забезпечення	так	ні	ні			так
2	Непередбачуване зростання вартості	так	ні	ні	так		
3	Індивідуальні можливості кастомізації системи	так	так	так		так	
4	Єдина підтримка апаратної та програмної частини	ні	ні	так		так	

Сильні характеристики:

1. Інтегрований підхід: IntraSecure пропонує інтегрований набір інструментів та сервісів для управління вразливостями і проблемами безпеки. Це дозволяє користувачам отримати все необхідне в одному місці, замість використання різних розрізнених продуктів.
2. Аналіз уразливостей: IntraSecure зосереджується на виявленні та аналізі уразливостей, пов'язаних з обходом ізоляції клієнтів, зокрема вразливості

CVE-2022-47522. Це дає можливість користувачам активно реагувати на цю конкретну загрозу безпеки.

3. Моніторинг в реальному часі: IntraSecure надає систему моніторингу безпеки в режимі реального часу, що дозволяє оперативно виявляти та реагувати на потенційні загрози. Це допомагає уникнути затримок у виявленні і реагуванні на проблеми безпеки.

Слабкі характеристики:

1. Конкуренція: Ринок управління вразливостями і безпекою вже має наявних гравців, які конкурують за увагу клієнтів. IntraSecure повинен розробити ефективну стратегію маркетингу та унікальний продуктовий пропозицій, щоб виділитися серед конкурентів.
2. Новість продукту: IntraSecure є новим проектом, тому він може потребувати часу для встановлення своєї репутації і отримання довіри від клієнтів. Це може бути викликом, оскільки вже існують відомі і встановлені конкуренти на ринку.

Нетральні характеристики:

1. Гнучкість інтеграції: IntraSecure має гнучкі можливості інтеграції з існуючими системами безпеки і інфраструктурою. Це дає користувачам свободу вибору та забезпечує сумісність з різними технологіями безпеки.
2. Експертна підтримка: IntraSecure пропонує експертну підтримку та консультації з питань безпеки. Це може бути перевагою для клієнтів, які шукають додаткову експертну допомогу, але може бути нейтральним фактором для тих, хто вже має власних експертів з безпеки.

Враховуючи ці характеристики, IntraSecure має потенціал вийти на ринок і знайти своє місце серед конкурентів, проте важливо звернути увагу на стратегію маркетингу, розробку продукту та будування довіри клієнтів.

6.2 Технологічний аудит ідеї проекту

Технологічна здійсненність ідеї проекту продемонстрована в таблиці 6.3.

Таблиця 6.3

Технологічна здійсненність ідеї проекту

№ п/п	Ідея проекту	Технології реалізації	Наявність технологій	Доступність технологій
1	Аналіз та вирішення проблем безпеки	Мова програмування Python,Rust	Існуючі бібліотеки, такі як Pandas, Numpy, Sklearn ,Apache Spark для допомоги з аналізом великих обсягів данних	Є доступними та безкоштовними для використання
2		Інші технології	PostgreSQL,HTML, CSS,JavaScript,React	Є доступними та безкоштовними для використання
Обрана технологія реалізації проекту: мова програмування Python				

Python використовується для вирішення великої кількості задач, в різних умовах за рахунок великої кількості бібліотек та простоті використання.

6.3 Аналіз ринкових можливостей запуску стартап-проекту

При дослідженні ринкових можливостей, в першу чергу проведений аналіз попиту: наявність попиту, обсяг, динаміка розвитку ринку. Дані наведені у таблиці нижче(таблиця 6.4).

Таблиця 6.4

Попередня характеристика потенційного ринку стартап-проекту

№ п/п	Показники стану ринку (найменування)	Характеристика
1	Кількість головних гравців, од	2
2	Загальний обсяг продаж	?
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу	Немає
5	Специфічні вимоги для стандартизації, специфікації	Немає
6	Середня норма рентабельності в галузі, %	?

Враховуючи сьогоднішню необхідність ринку рішень стосовно аналізу і вирішення проблем безпеки, за попереднім оцінюванням ринок є привабливим для входження.

Характеристика потенційних клієнтів стартап-проекту подана у таблиці 6.5

Таблиця 6.5

Характеристика потенційних клієнтів стартап-проекту

Потреба, що формує ринок	Потреба в безпеці
Цільова аудиторія (цільові сегменти ринку)	Корпоративні компанії
Відмінності у поведінці різних потенційних цільових груп клієнтів	Великі корпорації можуть мати вимоги до масштабованості, інтеграції з існуючими системами та гнучкості в налаштуванні безпекових політик.
Вимоги споживачів до товару	Ефективне виявлення вразливостей: Клієнти шукають рішення, які можуть швидко та точно виявляти уразливості в їхніх системах, включаючи відомі та нові загрози. ● Аналіз та звітність: Важливо мати зручні засоби для аналізу даних про уразливості, генерації звітів та візуалізації результатів. ● Інтеграція та сумісність: Клієнти можуть вимагати можливостей інтеграції з існуючими системами, які вони вже використовують, або сумісності з популярними стандартами безпеки. • Підтримка та навчання: Клієнти можуть потребувати підтримки, консультацій та навчання для налагодження та ефективного використання рішення

Фактори загроз подано у таблиці 6.6

Таблиця 6.6

Фактори загроз

№ п/п	Фактор	Зміст загрози	Можлива реакція компанії
1	Кібератаки	Зловмисники можуть намагатися зламати систему, отримати незаконний доступ до даних або спричинити шкоду. Компанія повинна мати механізми виявлення, запобігання та відновлення після кібератак, такі як використання брандмауерів, інтрузійних систем виявлення, шифрування даних та забезпечення резервного копіювання.	Реакція компанії на ці фактори загроз повинна включати розробку і реалізацію політик безпеки, надання належної освіти та навчання співробітникам, встановлення відповідних технологічних рішень, проведення регулярного моніторингу та аудитів безпеки, а також співпрацю зі спеціалістами з безпеки для виявлення і врегулювання потенційних загроз.
2	Внутрішні загрози	Інсайдери, такі як співробітники або партнери, можуть намагатися використати свій привілейований доступ для незаконних цілей. Компанія повинна розробити строгі політики доступу та моніторингу, а також надати навчання працівникам щодо безпеки та етичного поводження.	Реакція компанії на ці фактори загроз повинна включати розробку і реалізацію політик безпеки, надання належної освіти та навчання співробітникам, встановлення відповідних технологічних рішень, проведення регулярного моніторингу та аудитів безпеки для виявлення і врегулювання потенційних загроз.

Фактори можливостей подано у таблиці 6.7

Таблиця 6.7

Фактори можливостей

№ п/п	Фактор	Зміст можливості	Можлива реакція компанії
1	Технологічні інновації	Розвиток нових технологій, таких як штучний інтелект, блокчейн, машинне навчання або розширена реальність, може надати компанії конкурентну перевагу.	Компанія може реагувати на цю можливість шляхом активного досліджен-ня та впровадження нових технологій у свої продукти та процеси.
2	Розширення ринків	Можливість зайняти нові ринки або розширити присутність на існуючих ринках може створити нові можливості для збільшення обсягів продажів та заробітку	Компанія може відповісти на цю можливість шляхом розвитку стратегій маркетингу, партнерства з іншими компаніями або розробки нових продуктів або послуг, що задовольняють потреби цього ринку.
3	Покращення ефективності	Застосування нових технологій або процесів може допомогти підвищити ефективність операцій компанії, зменшити витрати та покращити якість продуктів або послуг.	Компанія може реагувати на цю можливість шляхом впровадження автоматизованих систем, оптимізації бізнес-процесів та пошуку нових методів управління.

Ступеневий аналіз конкуренції на ринку подано у таблиці 6.8

Таблиця 6.8

Ступеневий аналіз конкуренції на ринку

Особливості конкурентного середовища	В чому проявляється дана характеристика	Вплив на діяльність підприємства
1. Тип конкуренції: Пряма конкуренція	Компанії прямо конкурують між собою за тих самих клієнтів та ринкову частку. Вони пропонують схожі продукти або послуги, і споживачі мають можливість обирати між ними.	Компанії, що виробляють однакові товари та борються за клієнтів на ринку.
2. Рівень конкурентної боротьби: національний/інтернаціональний	Першим етапом є боротьба за ринок України з подальшим виходом на ринки інших країн	Маркетингова компанія в першу чергу орієнтована на захоплення місцевого ринку
3. Галузева ознака: внутрішньогалузева	Економічна боротьба з конкурентами відбувається в одній галузі економіки, пропонуються аналогічні послуги, що мають архітектурні відмінності у функціонуванні	Пропозиція суттєвих переваг у порівнянні з продуктами конкурентів у визначеній галузі економіки
4. Конкуренція за видами товарів: товарно-видова	Конкуренція відбувається між послугами одного виду.	Постійна робота над забезпеченням високого рівня іміджу компанії
5. За характером конкурентних переваг: неціновa	Передбачається ведення конкурентної боротьби не за рахунок зниження ціни на аналогічні послуги, а за рахунок новизни та унікальних характеристик технології, на якій базується функціонування системи	Акцент на унікальних характеристиках пропонованого товару

Продовження таблиці 6.8

6. За інтенсивністю: марочна	Виведення товару на ринок передбачається під власною маркою	Просування бренду компанії

Аналіз конкуренції в галузі за М. Портером подано у таблиці 6.9

Таблиця 6.9

Аналіз конкуренції в галузі за М. Портером

Складові аналізу	Прямі конкуренти в галузі	Потенційні конку-ренти	Постачаль-ники	Клієнти	Товари-замінники
	Rapid7,IBM Secure	Гнучкі ціни, Патент на продукт	Змінні витрати постачальни-ків	Рівень чутливості до зміни цін	Ціна, лояльність спожива-чів
Виснов-ки	Конкурен-ція інтенсивна, кожен працює в одній сфері	Можливість входу в ринок висока. Потенційні конкуренти присутні	Постачальник може диктувати умови: ціни на послуги	Кожен з клієнтів потребує індивідуальн ого підходу для вирішення його задач	Обмежень для роботи на ринку з боку товарів замінників на даний момент не існує

В результаті проведення аналізу таблиці 6.9, можна зробити висновок, що можливість виходу на ринок з огляду на конкурентну ситуацію є високою. Для виходу на ринок товар в першу чергу повинен пропонувати унікальні характеристики, які відсутні у продуктах конкурентів.

На основі аналізу конкуренції, проведеного в таблиці 6.9, а також із урахуванням характеристик ідеї проекту (таблиця 6.2), вимог споживачів до

товару (таблиця 6.5) та факторів маркетингового середовища (таблиці 6.6 та 6.7), визначається та обґрунтовується перелік факторів конкурентоспроможності, що надається у таблиці 6.10.

Таблиця 6.10

Обґрунтування факторів конкурентоспроможності

№ п/п	Фактори конкурентоспроможності	Обґрунтування
1	Динаміка галузі	Загрози безпеці постійно зростають, оскільки злочинці постійно розробляють нові способи атак і використовують вразливості у системах. Тому, для успішного функціонування IntraSecure, проект повинен бути готовим до аналізу та виявлення нових загроз, а також розробки та впровадження відповідних заходів безпеки.
2	Концепція товару і послуги	IntraSecure пропонує повний цикл роботи з безпекою, починаючи з аналізу потенційних загроз до впровадження заходів безпеки та моніторингу. Він охоплює всі аспекти безпеки мережі, включаючи ідентифікацію вразливостей, виявлення вторгнень, захист від шкідливих програм та зловживань.
3	Після продажне обслуговування	Підтримка системи після її продажу

Фінальним етапом ринкового аналізу можливостей впровадження проекту є складання SWOT-аналізу (матриці аналізу сильних (Strength) та слабких (Weak) сторін, загроз (Troubles) та можливостей (Opportunities) на основі виділених ринкових загроз та можливостей, та сильних і слабких сторін (таблиця 6.11).

Таблиця 6.11

SWOT-аналіз стартап проекту

Сильні сторони: • Інтегроване рішення • Ефективність • Налагоджена інфраструктура	Слабкі сторони: • Висока складність • Залежність від технологій
Можливості: • Ринковий ріст • Технологічний розвиток	Загрози: • Конкуренція • Зміни в законодавстві

Альтернативи ринкового впровадження стартап-проекту наведено у таблиці 6.12

Таблиця 6.12

Альтернативи ринкового впровадження стартап-проекту

№ п/п	Опис профілю цільової групи потенційних клієнтів	Готовність споживачів сприйняти продукт	Орієнтовний попит в межах цільової групи	Інтенсивність конкуренції в сегменті	Простота входу у сегмент
1	Малий бізнес	Переважно готові	Високий	Середня	Легко
2	Корпоративні компанії	Готові	Дуже високий	Висока	Важко

Цільовими групами обрано компанії малого бізнесу, що зацікавлені у поліпшенні систем безпеки, шляхом застосування автоматизованих систем

Базові стратегії в обраних сегментах ринку представлені у таблиці 6.13.

Таблиця 6.13

Визначення базової стратегії розвитку

№ п/п	Обрана альтернатива розвитку	Стратегія охоплення ринку	Ключові конкурентоспроможні позиції	Базова стратегія розвитку
1	Динамічний розвиток з використанням маркетингу та встановлення бізнес-контактів	Підняття рейтингу компанії шляхом маркетингу	Незалежність від посередника, який утримує кошти за свої послуги	Стратегія лідерства по витратах
2	Динамічний розвиток завдяки висвітленню унікальних характеристик надаваємих послуг	Унікальність послуг, для збільшення лояльності клієнта	Використання технології машинного навчання	Стратегія диферен-ціації

Залежно від міри сформованості галузевого ринку, характеру конкурентної боротьби, необхідно обрати одну з трьох стратегій конкурентної поведінки: розширення первинного попиту, оборонну або наступальну стратегію або ж застосувати демаркетинг або диверсифікацію (таблиця 6.14).

Таблиця 6.14

Визначення базової стратегії конкурентної поведінки

№ п/п	Чи є проект першопрохідцем на ринку	Чи буде компанія шукати нових споживачів, або забирати існуючих у конкурентів	Чи буде компанія копіювати основні характеристики	Стратегія конкурентної поведінки
1	Проект не є першопрохідцем	Компанія буде шукати нових користувачів	Компанія буде копіювати найкращі з характеристик конкурентів	Стратегія наслідування лідеру за для економії фінансових ресурсів

На основі вимог споживачів з обраних сегментів до постачальника (стартап-компанії) та до продукту (таблиця 6.5), а також в залежності від обраної базової стратегії розвитку та стратегії конкурентної поведінки була розроблена стратегія позиціонування (таблиця 6.15).

Таблиця 6.15

Визначення стратегії позиціонування

№ п/п	Вимоги до товару цільової аудиторії	Базова стратегія розвитку	Ключові конкурентоспроможні позиції власного стартап-проекту	Вибір асоціацій, які мають сформувати комплексну позицію власного проекту
1	Висока доступність	Стратегія диференціації	Використання технології машинного навчання, що є новітнім підходом к рішенню цієї задачі	Доступність, якість, швидкість

6.4 Розроблення маркетингової програми стартап-проекту

Маркетингова програма - це намічений для планомірного здійснення, об'єднаний єдиною метою та залежний від певних строків комплекс взаємопов'язаних завдань і адресних заходів соціального, економічного, науково-технічного, виробничого, організаційного характеру з визначенням ресурсів, що використовуються, а також джерел одержання цих ресурсів. Основну увагу слід приділяти вибору, значенню та формі інструментів маркетингу, їх об'єднанню в найбільш оптимальний з погляду визначеної мети комплекс, а також розподілу фінансових ресурсів у межах бюджетування маркетингу.

Першим кроком є формування маркетингової концепції товару, який отримає споживач. Для цього потрібно підсумувати результати попереднього аналізу конкурентоспроможності товару (таблиця 6.16).

Таблиця 6.16

Визначення ключових переваг концепції потенційного товару

№ п/п	Потреба	Вигода, яку пропонує товар	Ключові переваги перед конкурентом
1	IntraSecure відповідає потребі в комплексному рішенні для безпеки мережі. У світі, де загрози безпеки стають все більш складними, організації потребують ефективного і надійного засобу для захисту своїх мереж та даних.	IntraSecure пропонує кілька вигод для користувачів. Це включає швидке виявлення загроз безпеки, автоматичне реагування та захист, зниження ризиків і витрат на відновлення після атак, а також поліпшення продуктивності та надійності мережі.	Інтегроване рішення: IntraSecure пропонує повний цикл роботи з безпекою, що охоп-лює аналіз, виявлення та захист, що дозволяє спростити та узгодити процеси безпеки мережі. Ефективність: Завдяки використан-ню автоматизованих засобів та аналітич-них алгоритмів, IntraSecure забезпечує швидку реакцію на загрози безпеки та оптимальне викори-стання ресурсів. Налагоджена інфраструктура: IntraSecure має стабільну та надійну інфраструктуру, що підтримує високу доступність послуг та надійність в роботі.

Надалі розробляється трирівнева маркетингова модель товару: уточняється ідея продукту та послуги, його фізичні складові, особливості процесу його надання (таблиця 6.17).

Таблиця 6.17

Опис трьох рівнів моделі товару

Рівні товару	Сутність та складові
1. Товар за задумом	Товар IntraSecure представляє собою комплексне програмне рішення для безпеки мережі.
2. Товар у реальному виконанні	Властивості: безпека,автоматизація,інтегрованість,гнучкість

Продовження таблиці 6.17

	IntraSecure представляє собою комплексне рішення для безпеки мережі, яке забезпечує виявлення, аналіз та захист від загроз безпеки
	Поставляється у вигляді програмного забезпеченн для власних серверів чи компьютерів
	Назва: IntraSecure
3. Товар із підкріпленням	До продажу: відбувається інсталяція та конфігурування системи, проводяться тренінги для клієнта
	Після продажу: відбувається підтримка програмного забезпечення та його доопрацювання під потреби клієнта
Програмний комплекс, що забезпечує вирішення проблем з безпекою, розповсюджується на основі підписки, захисту підлягає програмний код та програмна реалізація.	

Аналіз системи збуту передбачає визначення ефективності кожного елемента цієї системи, оцінювання діяльності апарату працівників збуту. Аналіз витрат обігу передбачає зіставлення фактичних збутових витрат за кожним каналом збуту і видом витрат із запланованими показниками для того, щоб виявити необґрунтовані витрати, ліквідувати затрати, що виникають у процесі руху товарів і підвищити рентабельність наявної системи збуту.

Дані щодо визначення системи збуту надаються в таблиці 6.18.

Таблиця 6.18

Формування системи збуту

№ п/п	Специфіка закупівельної поведінки цільових клієнтів	Функції збуту, які має виконувати постачальник товару	Глибина каналу збуту	Оптимальна система збуту
1	Власна система збуту	Проведення та розгортання програмного забезпечення на стороні компанії-клієнта	Канал нульового рівня, продаж товару відбувається безпосередньо споживачам через відділ збуту	Оптимальною системою збуту є прямий збут з каналом нульового рівня за відсутності посередників

Концепція маркетингових комунікацій подана у таблиці 6.19

Таблиця 6.19

Концепція маркетингових комунікацій

№ п/п	Специфіка поведінки цільових клієнтів	Канали комунікацій	Ключові позиції, обрані для позиціонування	Завдання рекламного повідомлення
1	Консервативна поведінка, але відкриті до нового,	Соцмережі професійного спрямування, корпоративна пошта	Можливості отримання переліку параметрів	Висвітлити унікальні характеристики продукту

У якості концепції маркетингових комунікацій були обрані інтегровані маркетингові комунікації, де компанія ретельно обмірковує і координує роботу своїх численних каналів комунікації, рекламу в засобах масової інформації, особистий продаж, стимулювання збуту, пропаганду, прямий маркетинг, упаковку товару.

Висновки

В даному розділі був проведений маркетинговий аналіз перспектив реалізації системи що пропонує аналіз та вирішення проблем безпеки та проведене оцінювання можливостей її ринкового впровадження.

В результаті дослідження визначено, що існує можливість ринкової комерціалізації проекту в першу чергу завдяки використанню технологій машинного навчання, що дозволяє наділити продукт унікальними характеристиками, такими як швидкість, прозорість, якість отриманого рішення та великі можливості кастомізації проекту.

Конкурентна ситуація складна але надає перспективи впровадження продукту.В результаті існуючі товари-аналоги створюють прямої конкуренції на ринку України. Це може стати основною проблемою.

Тим не менш проведений аналіз підтверджує, що подальша імплементація проекту є доцільною.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

Магістерська дисертація присвячена глибокому аналізу проблем безпеки, що виникають при використанні MacStealer, як відомого інструменту у сфері кібербезпеки. Ця дослідницька робота виявила ключові аспекти та ризики, які випливають із застосування цього зловмисного інструменту у сучасних кібератаках.

Через проведений аналіз стало зрозуміло що , що цей інструмент представляє серйозні загрози безпеці, особливо в контексті крадіжки конфіденційних даних, паролів та інших чутливих інформаційних ресурсів.

Було досліджено функції стандарту IEEE 802.11 в яких не було знайдено чітких інструкцій щодо обробки змінних контекстів безпеки, а також того, що буферизовані кадри слід видаляти, коли пристрій від'єднується або повторно підключається до мережі. Зловмисник може вводити та перехоплювати кадри та маніпулювати контекстом безпеки клієнта-жертви, наприклад, вводити незахищені кадри керування, такі як кадри автентифікації та асоціації. Ці вразливості створюють потенційні ризики для користувачів та організацій, що використовують та захищають ці системи.

У цій роботі були розглянуті можливі заходи та стратегії для запобігання таким атакам. Було розроблено та запропоновано нові методи пом'якшення такі як: Встановлення паролів та обмеження фізичного доступу до налаштувань точки доступу, що зменшить ризик несанкціонованої зміни налаштувань мережі, налаштування мережі таким чином, щоб обмежити пряму комунікацію між клієнтами, що може запобігти деяким видам атак на рівні MAC, розділення мережі на окремі підмережі для різних груп користувачів або пристроїв, що може зменшити потенційний вплив атак на одну частину мережі на іншу,розробка та виконання суворих мережевих політик безпеки, які включають в себе правила для захисту мережі від потенційних загроз, шифрування даних, особливо чутливої інформації, навіть у випадку, якщо мережа вже зашифрована, що допоможе додатково захистити дані від несанкціонованого доступу.

Також варто додати що ніколи не слід забувати про соціально-інженерний аспект тому постійне навчання персоналу та проведення регулярних аудитів безпеки мережі для виявлення вразливостей та вжиття заходів для їх виправлення є доцільним.

Окремо можна додати встановлення системи моніторингу, яка виявлятиме аномальну активність в мережі та надасть можливість вчасно реагувати на потенційні загрози, ця тема стала основою для розроблення стартап-проекту.

Узагальнюючи, ця дисертація демонструє, що відповідальність за захист від кіберзагроз, таких як MacStealer, лежить не тільки на технічних засобах безпеки, але й на постійному підвищенні обізнаності та відповідальності всіх користувачів мережі. Системи безпеки мають постійно вдосконалюватися, а стратегії захисту мають бути адаптивними до змін у кіберзагрозах для забезпечення ефективного захисту даних та інформаційних ресурсів.

Загалом, ця робота є важливим внеском у розуміння та боротьбу з кіберзагрозами, вона може слугувати доповненням до теперішніх стратегій безпеки, сприяючи зміцненню захисту мережі, та надає підставу для подальших досліджень у цій області для зміцнення кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. IEEE Std 802.11. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, 2020.
2. Usenixsecurity23 [Електронний ресурс] – Режим доступу до ресурсу: https://www.usenix.org/system/files/usenixsecurity23-schepers.pdf
3. Domien Schepers, Aanjhan Ranganathan, and Mathy Vanhoef. On the robustness of Wi-Fi deauthentication countermeasures. In Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '22, page 245–256, New York, NY, USA, 2022. Association for Computing Machinery.
4. Philipp Ebbecke. Protected management frames enhance Wi-Fi network security. https://www.wifi.org/beacon/philipp-ebbecke/protectedmanagement-frames-enhance-wi-fi-networksecurity, 2020 (Accessed 07 June 2022).
5. Wi-Fi Alliance. Security | wi-fi alliance. https://www. wi-fi.org/discover-wi-fi/security, 2022 (Accessed 07 June 2022).
6. Domien Schepers, Aanjhan Ranganathan, and Mathy Vanhoef. Let numbers tell the tale: measuring security trends in Wi-Fi networks and best practices. In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pages 100–105, 2021.
7. Mathy Vanhoef and Frank Piessens. Advanced Wi-Fi attacks using commodity hardware. In Proceedings of the 30th Annual Computer Security Applications Conference, pages 256–265, 2014
8. Weiping Sun, Munhwan Choi, and Sunghyun Choi. IEEE 802.11 ah: A long range 802.11 WLAN at sub 1 GHz. Journal of ICT standardization, 1(1):83–108, 2013.
9. Evgeny Khorov, Andrey Lyakhov, Alexander Krotov, and Andrey Guschin. A survey on IEEE 802.11 ah: An enabling networking technology for smart cities. Computer communications, 58:53–69, 2015.

10. Markus Bullmann, Toni Fetzer, Frank Ebner, Markus Ebner, Frank Deinzer, and Marcin Grzegorzek. Comparison of 2.4 GHz WiFi FTM-and RSSI-based indoor positioning methods in realistic scenarios. Sensors, 20(16):4515, 2020
11. Mohamed Ibrahim, Hansi Liu, Minitha Jawahar, Viet Nguyen, Marco Gruteser, Richard Howard, Bo Yu, and Fan Bai. Verification: Accuracy evaluation of wifi fine time measurements on an open platform. In Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, pages 417–427, 2018
12. Wi-Fi Alliance. Wi-Fi aware | Wi-Fi alliance. https:// www.wi-fi.org/discover-wi-fi/wi-fi-aware, 2022 (Accessed 07 June 2022).
13. Wi-Fi Alliance. Passpoint Specification Ver. 3.2, 2020
14. Wi-Fi Alliance. WPA3 specification version 3.0. https://www.wi-fi.org/file/wpa3- specification, 2020 (Accessed 07 June 2022)
15. Alberto Ornaghi and Marco Valleri. Man in the middle attacks. In Blackhat Conference Europe, volume 1045, 2003
16. Brad Miller, Ling Huang, Anthony D Joseph, and J Doug Tygar. I know why you went to the clinic: Risks and realization of HTTPS traffic analysis. In International Symposium on Privacy Enhancing Technologies Symposium, pages 143–163. Springer, 2014
17. Vera Rimmer, Davy Preuveneers, Marc Juarez, Tom Van Goethem, and Wouter Joosen. Automated website fingerprinting through deep learning. arXiv preprint arXiv:1708.06376, 2017.
18. Verizon. IP latency statistics. https:// web.archive.org/web/20220514091144/https:// www.verizon.com/business/terms/latency/, 2022 (Accessed 07 June 2022).
19. Allan Rubens, Carl Rigney, Steve Willens, and William A. Simpson. Remote Authentication Dial In User Service (RADIUS). RFC 2865, June 2000.
20. Weiteng Chen and Zhiyun Qian. Off-Path TCP exploit: How wireless routers can jeopardize your secrets. In 27th USENIX Security Symposium (USENIX Security 18), pages 1581–1598, 2018
21. Yannay Livneh. Spoofing IP with IPIP. In PoC || GTFO, volume 0x02, 2022

22. Manesh Thankappan, Helena Rifà-Pous, and Carles Garrigues. Multi-channel man-in-the-middle attacks against protected Wi-Fi networks: A state of the art review. arXiv preprint arXiv:2203.00579, 2022

23. Adrienne Porter Felt, Richard Barnes, April King, Chris Palmer, Chris Bentzel, and Parisa Tabriz. Measuring HTTPS adoption on the web. In 26th USENIX security symposium (USENIX security 17), pages 1323–1338, 2017.

24. Simran Patil and Nikita Borisov. What can you learn from an ip? In Proceedings of the Applied Networking Research Workshop, pages 45–51, 2019.