Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Савич Нікола Властімірович

на здобуття ступеня вищої освіти магістра

Метод виявлення атак типу Man-in-the Middle у безпроводних мережах

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

Шифр КРМКБЗІ. 2301149.23.01.17 ПЗ

Виконав студент 2 курсу група КБЗІм-23 Нікола САВИЧ
Керівник доктор техн. наук, доцент Михайло КАСЯНЧУК

Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

19 12 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Магістр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Освітня програма Кібербезпека та захист інформації

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ _____
2 09 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Савичу Ніколі Властіміровичу

1 Тема роботи Метод виявлення атак типу Man-in-the Middle у безпроводних мережах
Керівник роботи доктор.техн.наук, професор Михайло КАСЯНЧУК
Затверджено наказом ректора університету від 26 08 2024 № 60
2 Строк подання студентом кваліфікаційної роботи на кафедру _____
3 Вихідні дані до роботи Метод виявлення атак типу Man-in-the Middle у безпроводних мережах
4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ, Дослідження предметної області і постановка задачі, алгоритми виявлення атак типу "людна посередині в безпроводних мережах", Розробка методу виявлення та запобігання для атаки "man-in-the-middle", в безпроводних мережах, Дослідження та експерименти атаки «людина посередині» в бездротових мережах, висновки,
5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 2 09 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Ґрунтовне ознайомлення та дослідження предметної галузі	15.09.2024	Виконано
Визначення змісту, структури кваліфікаційної роботи	22.09.2024	Виконано
Підготовка першого розділу кваліфікаційної роботи	29.09.2024	Виконано
Підготовка другого розділу кваліфікаційної роботи	10.10.2024	Виконано
Підготовка третього розділу кваліфікаційної роботи	20.10.2024	Виконано
Підготовка статті/тези за темою кваліфікаційної роботи	4.11.2024	Виконано
Підготовка четвертого розділу кваліфікаційної роботи	17.11.2024	Виконано
Підготовка та оформлення ілюстративного матеріалу	24.11.2024	Виконано
Оформлення кваліфікаційної роботи	24.11.2024	Виконано
Попередній захист кваліфікаційної роботи	27.11.2024	Виконано
Захист кваліфікаційної роботи на засіданні ЕК	19.12.2024	Виконано

Студент _____ Нікола САВИЧ

Керівник кваліфікаційної роботи _____ Михайло КАСЯНЧУК

АНОТАЦІЯ

Тема кваліфікаційної роботи магістра: “Метод виявлення атак типу Man-in-the Middle у безпроводних мережах”

Автор роботи: Савич Н.В.

Керівник роботи: Касянчук М.М.

Пояснювальна записка: 86 с., 34 мал., 3 таб., - дод., 70 джерел.

Ключові слова: туманні обчислення; Людина в середині атака; Система виявлення вторгнень; Система запобігання вторгненню; Мережева безпека, MITM.

Об’єктом дослідження є атаки типу Man-in-the Middle у безпроводних мережах

Предметом дослідження є виявлення атак Man-in-the Middle у безпроводних мережах

Метою кваліфікаційної роботи магістра є розробка методів виявлення атак Man-in-the Middle в безпроводних мережах.

При атаках MITM зловмисник виступає посередником між клієнтом і роутером. Зловмисник може стежити за всім мережевим трафіком між ними. Зловмисник може просто стежити за трафіком або навіть змінювати повідомлення, що відправляються між ними. Це призведе до порушення конфіденційності та цілісності повідомлень, що відправляються між клієнтом маршрутизатором.

У роботі був запропонований метод виявлення та визначення місцезнаходження зловмисника MITM у бездротових мережах шляхом обчислення часу проходження сигналу туди й назад (RTT)

9.12.2024

ANNOTATION

Theme of quliaication work: "Man-in-the-Middle attack detection method in wireless networks"

Author of the work: Savych N.V.

Head of work: Kasianchuk M.M.

Explanatory note: 86 pages, 34 figures, 3 tables, - add., 70 references.

Keywords: fuzzy computing; Man in the middle attack; Intrusion detection system; Intrusion prevention system; Network security, MITM.

The object of research is Man-in-the-Middle attacks in wireless networks

The subject of the study is the detection of Man-in-the-Middle attacks in wireless networks

The goal of quliaication work is to develop methods for detecting Man-in-the-Middle attacks in wireless networks.

In MITM attacks, the attacker acts as an intermediary between the client and the router. An attacker can monitor all network traffic between them. An attacker can simply monitor the traffic or even change the messages sent between them. This will compromise the confidentiality and integrity of messages sent between the client and the router.

The paper proposed a method to detect and locate the MITM attacker in wireless networks by calculating round-trip time (RTT) and calculating the received signal strength (RSS) from the access point, if there is an attacker, these values are higher than and greater than absence of an intruder (longer delay time).

9.12.2024

ЗМІСТ

Вступ 9
1 Дослідження предметної області та постановка задачі 10
1.1 Теоретичний опис проблеми 11
1.2Типи атак MITM. 13
1.3Підготовка моделі, опис цілей 15
1.4 Виявлення атак типу “людина посередині” в безпроводних мережах 18
1.5 Виявлення та запобігання атаки “ man-in-the middle” в туманних обчисленнях 21
1.6Запобігання атак «людина посередині» в бездротовій технології wi-fi 23
1.7 Атака “Людина посередині” 27
2 Алгоритм виявлення атак типу “людина посередині” в безпроводних мережах 31
2.1. Методи виявлення атак 31
2.2. Алгоритми роботи методу. 33
2.3. Підготовка до експерименту 37
2.4. Висновки 40
3 Розробка методу виявлення та запобігання для атаки “ man-in-the middle” в бездротових мережах 44
3.2. Постановка задачі 45
3.3. Проведення експериментів 47
3.4. Збір інформації 54
3.5. Висновки 59
4 Дослідження та експерименти атаки «людина посередині» в бездротових мережах 60
4.1. Збір даних та підготовка до реалізації експерименту 61
4.2. Проведення експериментів 66
4.3. Висновки 82
Висновки 84
Перелік джерел посилань 86

Додаток А 93
Додаток В 103

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

MITM – Атаки “Людина посередині”

ARP – Протокол розпізнавання адрес

DNS – Підміна сервера доменних імен

IP – Протокол мережевого рівня

IDS – Система виявлення вторгнень

IPS – Система запобіганню вторгнень

FN – Вузли туману

LTE – long Tearm Evolution

SSL – Secure Socket Layer

TST – Transport Security Layer

AES – Advanced Encryption System

ВСТУП

Атаки типу "людина посередині" (MITM) стають дедалі популярнішими через зростання використання смартфонів і програмного забезпечення, що дає зловмисникам можливість легко отримувати вашу конфіденційну інформацію. Така атака дозволяє хакерам перехоплювати зв'язок між двома сторонами, наприклад, між людиною та програмою або клієнтом і сервером, а також видавати себе за одну зі сторін, щоб маніпулювати даними або викрасти їх.

Основною метою таких атак є отримання важливих даних, як-от платіжна інформація чи облікові записи для входу. MITM-атаки найчастіше виникають у середовищах з недостатніми заходами безпеки, такими як відсутність шифрування або автентифікації. Вони можуть відбуватися, коли хакер перехоплює дані між пристроями, наприклад, між веб-браузером на комп'ютері або мобільному пристрої та сервером.

Зловмисники можуть використовувати ці атаки для отримання платіжних карток, банківських даних або паролів. Вони можуть також спробувати змінити дані, які передаються, щоб заразити пристрій шкідливим ПЗ. Особливо вразливі до MITM-атак мережі з низьким рівнем безпеки, зокрема публічні Wi-Fi мережі, де користувачі можуть навіть не помітити, що їхня інформація скомпрометована.

Атаки MITM можуть приймати різні форми, але зазвичай вони включають перехоплення даних, перенаправлення їх на інший сервер і, якщо потрібно, розшифрування. Це особливо небезпечно під час входу на сайти або сервіси, де потрібна захищена автентифікація. Такі атаки зазвичай націлені на веб-сайти онлайн-банкінгу або електронної комерції, що дає зловмисникам доступ до конфіденційної інформації користувачів.

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ

Бездротові мережі набули популярності через свою зручність і здатність забезпечувати достатню пропускну здатність для щоденних задач, а також портативність. Останнім часом загальнодоступні Wi-Fi мережі значно зросли в кількості, що призвело до збільшення їх використання. Однак, у таких мережах існує ризик атаки типу "людина посередині" (MITM), коли зловмисник може знаходитися між користувачем і постачальником послуг, спостерігаючи за трафіком, що передається між ними.

Зловмисник, моніторячи цей трафік, може отримати доступ до конфіденційної інформації, наприклад, паролів, а також впливати на цілісність і конфіденційність повідомлень, що передаються. Хоча існує варіант використання віртуальної приватної мережі (VPN) для захисту, це коштовний і не завжди доступний метод. Одним із можливих рішень є аналіз збережених мережевих даних для виявлення потенційних загроз і можливих атак.

Публічні Wi-Fi мережі сьогодні використовуються дуже часто, але через проблеми з безпекою, підключення до таких мереж може призвести до ситуації, коли в мережі може бути присутній зловмисник. Він може реалізовувати різноманітні MITM-атаки, що ставить під загрозу безпеку даних користувачів.

Атака починається з перехоплення. Щоб завадити вам досягти цільового місцезнаходження, кіберзлочинець намагається перехопити вашу інтернет-активність на цьому етапі. На етапі дешифрування злочинець непомітно розшифровує зашифровані з’єднання та декодує вкрадені дані, щоб створити враження, що за цим не стоїть монстр.Типовий метод перехоплення даних складається з наступних етапів:

– Наприклад, коли користувач відвідує веб-сайт, який використовує протокол передачі гіпертексту (HTTP) або незахищену публічну точку доступу, зловмисник може виявити будь-яку можливу шкідливу мережеву активність, встановивши аналізатор пакетів;

– Зловмисник отримує інформацію користувача після входу на зламаний веб-сайт і використовує її, щоб переслати його на шахрайський;

– Зловмисник може отримати доступ до всіх користувацьких ресурсів оригінального веб-сайту за допомогою підробленого веб-сайту, який імітує справжній і збирає всі відповідні дані користувача;

– Перехоплені дані розшифровуються на етапі дешифрування. Цей важливий етап дозволяє зловмиснику інтерпретувати дані та використовувати їх для своєї вигоди; потім вони можуть викрасти ідентифікаційні дані або, наприклад, втручатися в роботу компанії.

1.1 Теоретичний опис проблеми

При атаках типу "людина посередині" (MITM) зловмисник виступає посередником між клієнтом і роутером, що дозволяє йому стежити за всім мережевим трафіком, що передається між ними. Зловмисник може лише спостерігати за трафіком або навіть змінювати повідомлення, що передаються, що порушує конфіденційність та цілісність цих даних. Це особливо небезпечно, якщо веб-сайти не використовують методи шифрування, оскільки зловмисник може отримати доступ до паролів та іншої чутливої інформації, яку передає користувач.

Такі атаки часто спрямовані на зв'язок між клієнтом і сервером з метою викрадення облікових даних для аутентифікації або виконання несанкціонованих дій, наприклад, грошових переказів від імені клієнта. Однак націлювання на всіх користувачів у мережі є складним завданням для зловмисника, оскільки він повинен бути посередником для кожного користувача в мережі, що вимагає значних обчислювальних і мережевих ресурсів [1].

Але моніторинг трафіку конкретного цільового користувача може здійснюватися навіть за допомогою звичайних обчислень та мережевої потужності. Якщо зловмисник знає лише MAC-адресу користувача, він може діяти як законний маршрутизатор для клієнта та як законний клієнт для маршрутизатора, або ж він може викрасти особистість клієнта.

Для визначення того, чи має експеримент значний ефект, можна використовувати статистичну значущість. Вона може з'ясувати, чи належать дані

два набори даних до однієї генеральної сукупності чи ні. Дуже популярними тестами статистичної значущості є t-критерій, тест Man-nWhitenyU і тест xi-квадрат.

Під час використання веб-сайтів дані про час, витрачений на передачу пакетів, зберігаються окремо. Це дозволяє створити набір даних, який містить інформацію про час, необхідний для доставки пакетів до конкретних веб-сайтів. Коли виникає потреба виявити атаку, порівнюються затримки часу з минулих даних і поточні затримки, щоб виявити можливу аномалію або атаку.

Однак, тимчасові затримки залежать від швидкості мережі, яка може значно варіюватися в залежності від конкретної мережі, що ускладнює точність виявлення атак. Крім того, моніторинг лише кількох веб-сайтів залишає інші ресурси уразливими, оскільки зловмисники можуть атакувати сайти, які не потрапляють до цього моніторингу, що робить їх вразливими для MITM-атак або інших видів атак.

Автори в [1] класифікують атаки MITM на основі таких параметрів, як місцезнаходження зловмисника, методи уособлення та використання каналу зв'язку. Ґрунтуючись на класифікації методів уособлення, надаються етапи виконання для кожного класу MITM. Також можна розглядати існуючі заходи протидії та обговорення порівнянь між ними. Наприкінці мого аналізу буде обговорюватися категоризація механізмів запобігання MITM.

У [2] обговорюється огляд MITM для класифікації та аналізу атак MITM. Атаки MITM класифікуються на основі різних параметрів, таких як місцезнаходження зловмисника, методи зонування та характер каналу.

У документі атаки MITM поділяються на MITM НА ОСНОВІ СПУФІНГУ, BGP MITM, TLS/SSL MITM та атаку MITM на основі помилкової базової станції.

Автори в [3] збирають, класифікують, ґрунтовно оцінюють найбільш популярні атаки на 802.11, і аналізуючи їх сигнатури. По-друге, було запропоновано загальнодоступний набір даних, що містить багате поєднання звичайного трафіку та трафіку атак на мережі 802.11. Також надаю досить широку оцінка набору даних з перших рук з використанням декількох алгоритмів

машинного навчання та особливостей даних. Також пояснюються інструменти, які можуть бути використані для запуску атак MITM в бездротових мережах.

1.2 Типи атак MITM

Кіберзлочинці застосовують кілька методів для проведення атак типу "людина посередині" (MITM), щоб отримати доступ до пристроїв і конфіденційних даних користувачів:

– Викрадення облікових записів: Зловмисники можуть вкрасти облікові записи електронної пошти банків або фінансових установ, які мають доступ до приватної інформації та грошей. Вони можуть стежити за листуванням клієнтів і отримувати дані про операції безпосередньо всередині банку;

– Фальшиві електронні листи: У більш небезпечних випадках, кіберзлочинці можуть видавати себе за банк і надсилати клієнтам електронні листи з проханням повторно ввести свої облікові дані або, ще гірше, перерахувати кошти на рахунок зловмисника. Це часто поєднується з соціальною інженерією, де зловмисники намагаються завоювати довіру жертв;

– Отруєння кешу DNS: Зловмисники можуть змінити записи DNS, щоб перенаправити законний онлайн-трафік на фальшиві веб-сайти, які виглядають так, як звичні і надійні ресурси. Це дозволяє обдурити користувачів і змусити їх ввести особисту інформацію на шахрайському сайті;

– Спуфінг і соціальна інженерія: Використовуючи техніки спуфінгу, зловмисники можуть переконати користувачів перейти на підроблений веб-сайт і виконати небезпечні дії, як-от переказ грошей або сплата комісій. Це дозволяє зловмисникам зібрати якомога більше конфіденційної інформації від жертви;

– ARP спуфінг: Кіберзлочинці можуть використовувати протокол ARP для зміни зв'язку між адресами Інтернету та MAC-адресами в локальній мережі. В результаті, комп'ютер жертви підключатиметься не до справжнього мережевого шлюзу, а до пристрою зловмисника. Це дозволяє зловмиснику перехоплювати

трафік і отримувати чутливу інформацію, включаючи особисті дані, збережені в браузері жертви.

Усі ці методи дозволяють зловмисникам отримувати доступ до конфіденційних даних, порушувати цілісність інформації та виконувати шкідливі дії без відома користувача.

Файл cookie — це невеликий фрагмент даних, що зберігається в комп'ютерах. Дані, зібрані веб-браузером і збережені локально на комп'ютері користувача, називаються файлами cookie браузера, які іноді називають файлами cookie HTTP. Веб-сайти можуть покращити взаємодію з користувачем, запам'ятовуючи інформацію за допомогою файлів cookie браузера.

Наприклад, якщо файли cookie ввімкнено, користувачі можуть уникати повторного введення однієї й тієї самої інформації у формі, наприклад свого імені та прізвища.

Щоб бути ефективним, крадіжка файлів cookie веб-переглядача повинна поєднуватися з іншим методом атаки MITM, наприклад прослуховуванням WiFi або захопленням сесії.

Використовуючи один із інших підходів MITM, кіберзлочинці можуть отримати доступ до пристрою користувача, викрасти файли cookie браузера та використовувати всі можливості атаки MITM.

Отримавши доступ до файлів cookie браузера, зловмисники можуть отримати паролі, номери кредитних карток та іншу особисту інформацію, яку користувачі часто зберігають.

Свого роду атака MITM, відома як «викрадення сеансу», виникає, коли зловмисник чекає, доки жертва зареєструється в програмі, наприклад електронної пошти або банківських послуг, перш ніж вкрасти файл cookie сеансу. Після цього зловмисник входить в обліковий запис жертви за допомогою файлу cookie, але з браузера зловмисника.

Сеанс — це точка даних, яка позначає короткий потік інформації між двома пристроями або між користувачем і комп'ютером. Оскільки сеанси ідентифікують користувачів, які ввійшли на веб-сайт, зловмисники використовують їх. Проте

зловмисники повинні діяти швидко, оскільки сеанси закінчуються через заздалегідь визначений період, який може становити лише кілька хвилин.

Протокол HTTP є фізичним проявом безпечного онлайн-спілкування. Веб-сайт із HTTPS безпечний і надійний. Під час атаки HTTPS-спуфінгу сеанс браузера перемикається на незахищений веб-сайт або веб-сайт на основі HTTP без відома або згоди користувача.

Кіберзлочинці можуть стежити за поведінкою користувачів і викрадати розкриті особисті дані за допомогою цього перенаправлення.

Атаки типу «людина посередині», які призначені для приховування, може бути важко виявити. Є кілька способів визначити, чи були ви ціллю атаки MITM.

Інструменти для аналізу пакетів і моніторингу мережі, такі як Wireshark і tcpdump, можуть допомогти у пошуку незвичайного трафіку у вашому IT-середовищі.

Антивірусне програмне забезпечення та програмне забезпечення для захисту від зловмисного програмного забезпечення може допомогти виявити несхвалені програми та код, які вставив зловмисник типу "людина посередині".

1.3 Підготовка моделі, опис цілей

Автори в [4] детектують атаку за допомогою алгоритмів машинного навчання. Виявлення шкідливих користувачів за допомогою регресійного навчання є важливим методом для виявлення кібератак, зокрема атак ботнетів. Регресійні моделі застосовуються для аналізу великих обсягів даних, що дозволяє виявляти аномалії у поведінці користувачів або пристроїв. У цьому випадку модель навчена на реальному наборі даних, що містить інформацію про атаки ботнетів, і вона може допомогти виявити підозрілу активність, яка вказує на наявність зловмисного програмного забезпечення або шкідливих користувачів.

Цей підхід базується на тому, що атаки ботнетів часто мають специфічні патерни трафіку, які можна виявити за допомогою алгоритмів регресії. Наприклад,

можна оцінювати такі характеристики, як частота запитів, IP-адреси, час активності, типи переданих даних і багато інших параметрів. Моделі регресії допомагають прогнозувати й ідентифікувати аномальні ситуації, що можуть свідчити про напад.

Це дозволяє автоматизувати процес виявлення атак, знижуючи навантаження на аналітиків безпеки і надаючи інструмент для оперативного реагування на потенційні загрози

Автори [7] в досліджують вразливість Long Term Evolution (LTE) до радіочастотного глушіння, спуфінгу та сніфінгу. Також обговорюється допомога адверсей за допомогою перевірки повідомлень LTE.

Також буде огляд методи захисту від спуфінгу та глушіння LTE. Потрібно зосередитись на проблемах, загрозах та рішеннях, що стосуються питань конфіденційності та безпеки медичних виробів. Не мало важливим є описання підготовки бездротової мережі Wi-Fi у виробничій системі, з системами виявлення вторгнень Snort і Kismet; для подальшої оцінки під ударом.

Система атаки складається з цільової машини та машини зловмисника, яка працює під керуванням операційної системи Kali Linux, як зображено на рисунку 1.1. Обидва комп’ютери підключені до однієї бездротової мережі Wi-Fi, забезпечуючи їм спільне мережеве середовище для комунікації. Зловмисник заздалегідь отримав доступ до ключа шифрування цієї мережі, що дозволяє йому перехоплювати трафік між пристроями. Для реалізації атаки Man-In-The-Middle (MITM) використовується спеціалізований інструмент **mitmf** (Man-In-The-Middle Framework), який забезпечує широкий набір функцій для виконання перехоплення та модифікації даних у реальному часі. Цей інструмент потрібно попередньо встановити на цільову машину, після чого він може бути запущений для отруєння таблиць ARP і перенаправлення трафіку через пристрій зловмисника. Таким чином, атакуючий отримує можливість шпигувати за інформацією, змінювати дані в пакеті або здійснювати інші шкідливі дії.

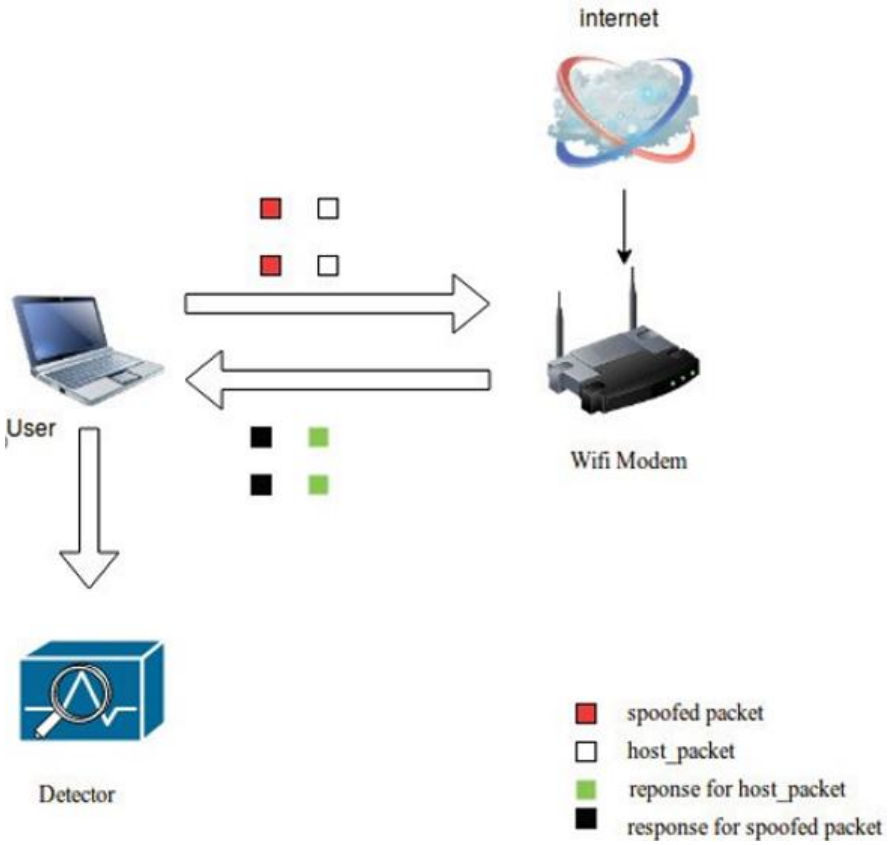


Рисунок 1.1. – Модель проведення атаки.

Зловмисник знає адресу контролю доступу до медіа (MAC) цільового комп'ютера. Зловмисники володіють бездротовою мережевою картою, яка здатна працювати в режимі монітора. Для цього експерименту використовується бездротовий адаптер Realtek AR8812AU USB 2.4 і 5 ГГц.

Фреймворки mitmf вимагають цільову адресу інтернет-протоколу (IP), IP-адресу мережевого шлюзу Wi-Fi. Після того, як аргументи будуть надані, він виступить посередником між клієнтом і маршрутизатором.

Для моніторингу трафіку мережі Wi-Fi використовується інструмент під назвою Airmon-ng. Цей інструмент здатний контролювати весь трафік всіх мереж, що знаходяться в зоні досяжності бездротової карти. Для цього бездротова карта повинна працювати в режимі монітора.

Маючи ідентифікатор базового набору служб (BSS) мережі, інструмент може контролювати виключно цю конкретну мережу.

Також весь трафік мережі може бути скинутий у файл даних. Аналіз дампу даних за допомогою wireshark і з MAC-адресою цілі, дасть IP-адресу цілі в мережі

Wi-Fi. IP-адресу шлюзу мережі можна дізнатися за допомогою команди net route, яка перерахує IP-адресу шлюзу всіх доступних інтерфейсів. Після надання всіх двох аргументів зловмисна машина відправить пакети з IP-адресою цілей, MAC-адресою зловмисників на маршрутизатор і пакетами з IP-адресою маршрутизатора.

MAC-адреса зловмисників направлена на цільову машину, яка видає себе за законний маршрутизатор і клієнт для цілі та маршрутизатора відповідно. Тепер кожен запит від клієнта буде відправлятися зловмиснику, який для цього експерименту відправляється безпосередньо на роутер без будь-яких змін. Усі відповіді також надсилаються зловмиснику, і вони надсилаються на цільову машину без будь-яких змін.

Якщо між клієнтом і веб-сайтом, який використовується, немає механізмів шифрування, це може призвести до розкриття зловмиснику конфіденційної інформації, яку він потім може використовувати для запуску атак з видаванням себе за іншу особу.

1.4 Виявлення атак типу “людина посередині” в безпроводних мережах

Інформаційна безпека охоплює всі заходи та стратегії, спрямовані на захист інформації від різних загроз. Це включає запобігання несанкціонованому доступу до даних, їх захопленню чи витоку третіми особами, а також забезпечення цілісності та доступності інформації. Основними цілями інформаційної безпеки є:

– Захист інформації: забезпечення того, щоб інформація не потрапляла в руки сторонніх осіб, а також запобігання її змінам чи знищенню;

– Цілісність інформації: гарантування, що інформація не буде змінена або пошкоджена під час зберігання чи передачі;

– Конфіденційність: забезпечення, щоб доступ до інформації мали лише ті особи, які мають на це право;

– Безперервний доступ: забезпечення безперервного функціонування системи, навіть у випадку атак чи технічних збоїв, для надання постійного доступу до інформаційних ресурсів.

Таким чином, інформаційна безпека забезпечує захист від різних загроз, таких як несанкціонований доступ, втручання, зловмисні атаки та інші, що можуть порушити роботу систем або призвести до втрати чи змін інформації.

З огляду на сьогоднішні технології та потреби, необхідно коротко охарактеризувати поняття доступності, цілісності та конфіденційності, які є основними елементами інформаційної безпеки, як показано на рисунок 1.2.

Рисунок 1.2. – Основні елементи інформаційної безпеки.

Зловмисники прагнули перехопити повідомлення між двома кінцевими точками, щоб вони могли скомпрометувати конфіденційність і скомпрометувати цілісність шляхом модифікації повідомлення, а також поставити під загрозу доступність, видаливши або знищивши повідомлення та припинивши з'єднання.

Коли зловмисники націлені на організацію, це призводить до великих економічних втрат.

Атака типу Man in the Middle (MITM) є однією з найбільш ефективних атак для отримання повного контролю над даними, що передаються між двома пристроями. Вона є особливо небезпечною для мереж Wi-Fi, оскільки дозволяє зловмиснику стати посередником між двома сторонами, які спілкуються через мережу.

Процес атаки MITM полягає в тому, що зловмисник вставляється між пристроєм, який хоче пройти аутентифікацію (наприклад, користувач або клієнт), і сервером або системою, що виконує перевірку автентичності. Це дозволяє зловмиснику перехоплювати та читати всю передану інформацію, а також змінювати її, не привертаючи уваги жертв. Також може бути перехоплене конфіденційне повідомлення, таке як паролі або платіжні дані.

Таким чином, атака MITM створює серйозну загрозу для конфіденційності та безпеки переданої інформації, оскільки зловмисник може не лише спостерігати за трафіком, але й маніпулювати ним, вводячи помилкові дані або викрадаючи чутливу інформацію.

Доступність означає, що інформація доступна авторизованим користувачам. По суті, це гарантія того, що ваша система та дані доступні авторизованим користувачам, коли це необхідно. Подібно до конфіденційності та цілісності, доступність також має велике значення. Цілісність у світі інформаційної безпеки означає збереження точності та повноти даних.

Йдеться про захист даних від зміни або неправомірного використання неавторизованою стороною. Цілісність передбачає збереження стабільності та достовірності даних протягом усього їх життєвого циклу. Дані не можна змінювати під час передачі, і необхідно вжити запобіжних заходів, щоб гарантувати, що дані не можуть бути змінені неавторизованими людьми.

Конфіденційність інформації, означає захист інформації від розкриття стороннім особам. Конфіденційно стосується захисту інформації будь-який несанкціонований або скрупульозний доступ, який може спричинити загрозу для вашої організації.

Атаки типу "людина посередині" (MitM) є старою і водночас складною загрозою для мережевих обчислювальних систем. Вона включає в себе прослуховування з'єднання, вторгнення в з'єднання, перехоплення повідомлень і послідовну зміну даних. Ця проблема була широко вивчена, і існує безліч варіацій основної атаки.

Атаки Man in the Middle (MitM), незважаючи на те, що вони існують вже досить довго, все ще залишаються популярними серед кіберзлочинців в Інтернеті. Ці атаки зберігають свою ефективність, оскільки дозволяють зловмисникам перехоплювати та маніпулювати даними, що передаються між двома сторонами.

Основною метою атак MitM є перехоплення зв'язку між клієнтом і сервером, зокрема для отримання чутливих даних, таких як облікові дані для аутентифікації. Це може включати паролі, логіни або інші ідентифікаційні дані, які дозволяють зловмиснику отримати доступ до систем або ресурсів жертви.

Для пом'якшення цієї загрози були запропоновані різні методи та підходи, які можуть допомогти запобігти або мінімізувати наслідки таких атак. Однак, попри наявність технологій захисту, атаки MitM все ще залишаються серйозною проблемою, особливо у випадках недостатньої безпеки на рівні з'єднань або у відкритих мережах.

1.5 Виявлення та запобігання атаки “ man-in-the middle” в туманних обчисленнях

Обсяг, швидкість і правдивість даних зростають в геометричній прогресії. Прогнозується, що до 2030 року обсяг даних в Інтернеті досягне 35 трильйонів гігабайт. Однак сорок відсотків (40%) цих даних необхідно аналізувати на пристроях, фізично близьких до Інтернету речей.

Тому необхідно фізично наближати обчислювальні пристрої до краю хмари, ближче до IoT-пристроїв. Це і призвело до розвитку обчислень Fog.

Туманні або периферійні обчислення – це форма обчислень, коли пристрої (Fog), фізично близькі до пристроїв кінцевих користувачів (Things), обробляють дані від імені хмари, щоб зменшити затримку. Будь-який пристрій з обчислювальними, сховищевими та мережевими підключеннями можна вважати вузлом/пристроєм туману. Туман і хмара доповнюють один одного.

Вони забезпечують взаємозалежність і взаємовигідні послуги для того, щоб зробити можливим зв'язок, обчислення, контроль і зберігання даних у всій системі. Таким чином, атакувати вузол туману так само добре, як і атакувати хмару, зберегти його простіше, оскільки він має більш обмежені ресурси.

Атака MitM – це тип атаки, що здійснюється зловмисним внутрішнім користувачем на два комп'ютери шляхом прикидання одному, що він і є інший. МітМ може бути двох категорій: Прослуховування та Маніпуляція.

Прослуховування є пасивним, оскільки супротивника цікавить лише інформація, що проходить. У маніпуляціях MitM зловмисник змінює дані, маскуючи їх під початкового відправника.

Крім того, мотивація до виявлення та запобігання MitM висока, оскільки це, мабуть, найпоширеніша атака в системах туманних обчислень. Це пов'язано з тим, що архітектура туману за своєю суттю схожа на атаку MitM, оскільки вузол туману знаходиться між хмарою та кінцевим пристроєм (Thing). Тим самим, даючи можливість зловмиснику сховатися з виду. Крім того, туманні вузли обробляють глибоко особисту інформацію, таку як історія хвороби, ліки та стан здоров'я людини.

Вони також обробляють іншу важливу інформацію, таку як швидкість, напрямок і пункт призначення транспортних засобів. У будь-якому випадку така інформація може виявитися згубною в чужих руках. Крім того, туманні вузли є більш привабливими для зловмисників, оскільки вони мають меншу обчислювальну потужність і знаходяться ближче до зловмисника, ніж до хмари.

Однак, у зв'язку з великою кількістю і різноманітністю вузлів в туманних обчисленнях, звичайні методи безпеки, такі як облікові дані безпеки, можуть бути важкими, якщо не неможливими, для застосування. Крім того, вузли туману часто

обмежені в ресурсах; Тому необхідні енергоефективні методи безпеки. Метою даного дослідження є визначення економічно ефективних методів виявлення та запобігання атакам MitM на рівні туману в мережі туманних обчислень.

Запропонована система використовує вузли Intrusion Detection System (IDS), стратегічно розташовані в мережі для досягнення виявлення атак, і використовує полегшене шифрування для запобігання атакам.

1.6 Запобігання атак «людина посередині» в бездротовій технології wi-fi

У кожній мережі є набір функцій, необхідних для її роботи. Ці функції у них різні, і вони утворюють шари. Кожен шар подається попереднім і подається наступним.

Такою моделлю є модель TCP/IP і вона складається з чотирьох шарів. Шари складаються з прикладного рівня, транспортного рівня, рівня інтернету та канального рівня. На рисунку 1.3, представлена мережа, в основі якої лежить модель TCP/IP. Коли Система I хоче передати дані до Системи II, прикладний рівень Системи I згенерує дані, а потім вони будуть відправлені на транспортний рівень. Транспортний рівень у Системі I відповідає за відкриття порту в системі, і після цього дані будуть доставлені на Інтернет-рівень.

Описаний процес відображає модель передачі даних через мережу, використовуючи концепції, подібні до моделі OSI (Open Systems Interconnection). Кожен рівень цієї моделі виконує специфічні функції, що забезпечують надійний зв’язок між пристроями. На фізичному рівні передаються електричні або бездротові сигнали, які забезпечують базову комунікацію між обладнанням. Канальний рівень відповідає за визначення способу передачі пакетів через мережу, використовуючи протоколи, такі як Wi-Fi або Ethernet. На мережевому рівні визначається маршрут передачі даних, забезпечуючи їхнє перенаправлення через IP-адреси. Транспортний рівень, наприклад через TCP, відповідає за розбиття даних на пакети, контроль помилок і перевірку їхньої доставки. На

сеансовому рівні встановлюється і підтримується сеанс зв’язку між пристроями, забезпечуючи синхронізацію передачі даних.

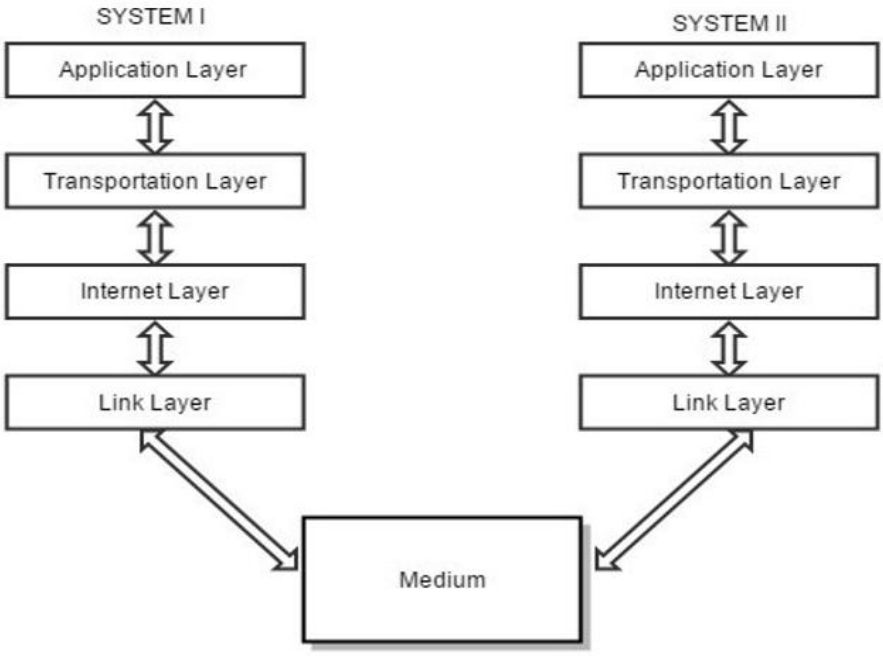


Рисунок 1.3. – Потік даних TCP/IP між двома системами.

– Інтернет-рівень (або рівень мережі) використовує IP-адреси для маршрутизації даних між пристроями в мережі. Встановлюється шлях для передачі даних від одного пристрою (системи I) до іншого (системи II);

– Канальний рівень відповідає за фізичну передачу даних через мережу. Він перетворює дані в двійковий потік (битову послідовність), який можна передавати через різні носії — дротові (кабелі), бездротові (Wi-Fi) або оптичні (оптоволоконні канали) методи;

– Канальний рівень II системи забезпечує коректність даних, що передаються. Він здійснює корекцію помилок, які можуть виникнути під час передачі через мережу, і після цього передає дані на вищі рівні для подальшої обробки;

– Дані передаються через всі рівні OSI-моделі, поки не досягають прикладного рівня, де вони стають доступними для користувачів або застосунків,

і можуть бути використані для виконання різних задач, наприклад, для отримання веб-сторінки чи обміну повідомленнями.

Цей процес може бути здійснений в обох напрямках — від системи I до системи II та навпаки, забезпечуючи обмін даними між різними мережевими пристроями.

Модель OSI (Open Systems Interconnection) була розроблена міжнародною організацією ISO для стандартизації обміну даними між різними комп'ютерними системами. Вона складається з семи шарів, кожен з яких виконує свою специфічну функцію для забезпечення передачі даних між пристроями в мережі. Ось ці шари:

– Фізичний рівень: Забезпечує фізичну передачу даних через мережу (кабелі, радіохвилі тощо);

– Канальний рівень: Контролює помилки на фізичному рівні та забезпечує надійність зв'язку;

– Мережевий рівень: Визначає маршрути для передачі даних між мережами, використовуючи IP-адреси;

– Транспортний рівень: Забезпечує надійну передачу даних між кінцевими точками з'єднання, як-от TCP або UDP;

– Сеансовий рівень: Керує з'єднаннями та сесіями між комп'ютерами, забезпечує синхронізацію та керує відновленням з'єднання після збоїв;

– Представницький рівень: Відповідає за перетворення даних у формат, зрозумілий для додатків (наприклад, шифрування);

– Прикладний рівень: Взаємодіє безпосередньо з користувачем або додатками, забезпечуючи доступ до мережевих послуг (наприклад, електронної пошти чи веб-сайтів).

У порівнянні з моделлю TCP/IP, яка складається з лише чотирьох рівнів, модель OSI надає більш детальний опис функцій мережі, дозволяючи точніше описати роль кожного рівня. Модель TCP/IP можна розглядати як спрощену версію моделі OSI, в якій певні шари об'єднані, що дозволяє зосередитися на реальних аспектах роботи мережі та ефективності передачі даних.

Загалом, модель OSI є корисною теоретичною основою для розуміння принципів роботи мереж, тоді як модель TCP/IP більше застосовується для реального використання в Інтернеті.

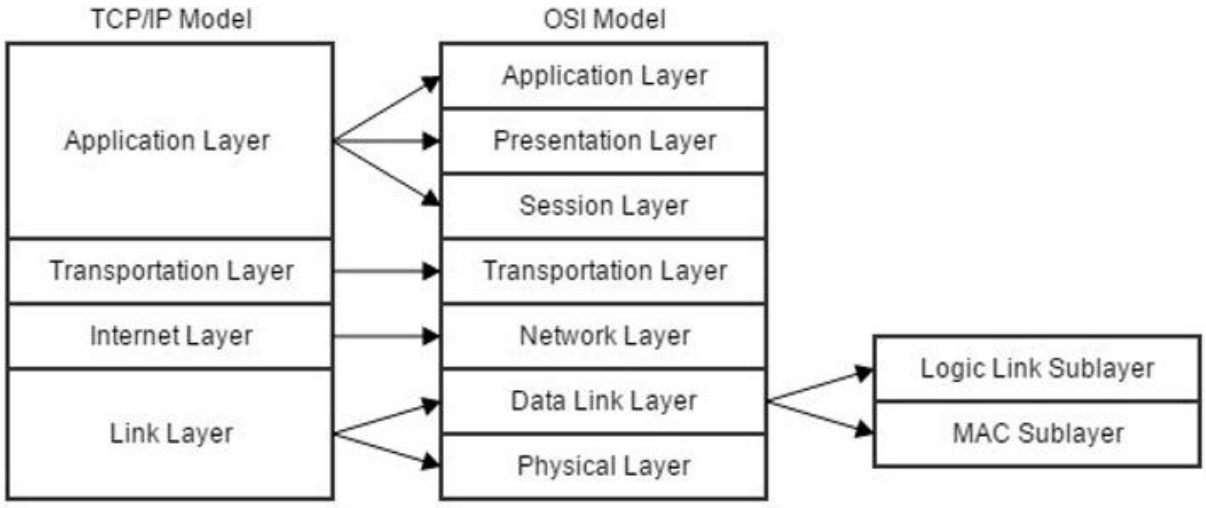


Рисунок 1.4. – Моделі TCP/IP та OSI

Моделі OSI та TCP/IP: Модель OSI містить сім шарів, у той час як модель використовує лише чотири, інтегруючи деякі з них. Це дозволяє TCP/IP бути більш адаптованим до реальних умов роботи мережі. У OSI модель має окремі шари для сесії, презентації та додатків, тоді як в TCP/IP ці функції об'єднані в один рівень. Протокол IP в TCP/IP відповідає мережевому рівню OSI, а TCP — транспортному.

Канальний рівень і підрівень MAC: У моделях OSI та TCP/IP канальний рівень відповідає за коректну передачу даних між пристроями в локальних мережах. У моделі OSI канальний рівень має два підрівні: Logical Link і MAC (Media Access Control). MAC рівень відповідає за доступ до фізичних середовищ передачі і управління доступом до каналу. Протоколи, як CSMA/CD для Ethernet, визначають правила того, як вузли в мережі можуть одночасно отримувати доступ до загального каналу передачі, мінімізуючи зіткнення даних.

Ethernet: Ця технологія використовує мідні кабелі (наприклад, UTP), що дозволяє забезпечити надійне з'єднання через фізичні канали зв'язку. Ethernet працює в різних режимах: напівдуплексний та повнодуплексний. У

напівдуплексному режимі передача та прийом даних відбуваються по черзі, а в повнодуплексному — одночасно.

Wi-Fi: Відмінність від Ethernet полягає в тому, що Wi-Fi використовує радіочастоти для передачі даних через повітря, що дозволяє забезпечити бездротовий зв'язок. Залежно від протоколу, використовуються різні частотні діапазони (2,4 ГГц і 5 ГГц). Важливо зазначити, що Wi-Fi не здатна надавати повнодуплексний зв'язок через один канал; для цього використовуються різні канали для передачі і прийому.

Протоколи IEEE 802.11b, 802.11g працюють на частоті 2,4 ГГц, що забезпечує більшу зону покриття, але з обмеженою швидкістю.

Протоколи IEEE 802.11a та 802.11n працюють на 5 ГГц або обох діапазонах для досягнення більш високих швидкостей, але з меншою зоною покриття.

Вибір частоти і каналу для Wi-Fi залежить від географічного регіону, в якому мережа працює, що обмежує кількість доступних каналів для передачі даних. Ethernet і Wi-Fi використовують однакові мережеві протоколи на канальному рівні, але сильно відрізняються на фізичному рівні. Ethernet має високу швидкість і надійність через використання проводів, тоді як Wi-Fi надає більшу гнучкість і мобільність, але може стикатися з проблемами в плані швидкості та зони покриття, особливо на великих відстанях або в умовах перешкод.

1.7 Атака “Людина посередині”

Механізми захисту, зокрема шифрування WPA/WPA2, є досить ефективними для захисту даних, що передаються в мережах Wi-Fi. Хоча передача інформації відбувається в відкритому ефірі, що дозволяє її перехоплення зловмисниками, сучасні засоби захисту забезпечують достатній рівень безпеки для більшості користувачів та можуть запобігти більшості атак.

Однак існують атаки, які неможливо заблокувати за допомогою стандартних методів безпеки, і в таких випадках дані важко захистити. Одним із таких видів атак є атака Man-In-The-Middle (MITM). Цей тип атаки дозволяє зловмиснику

перехоплювати будь-яку передану інформацію в бездротовій мережі, працюючи незалежно від існуючих механізмів захисту.

Зловмисник створює додаткове з'єднання між клієнтами мережі та їхньою точкою доступу, передаючи всі дані через свою точку доступу. Клієнти, вірячи, що вони підключені до легітимної точки доступу, можуть продовжувати користуватися Інтернетом та своїми програмами, але весь трафік при цьому контролюється зловмисником.

Як показано на рисунку 1.5, зловмисник, використовуючи два мережевих адаптери, може обійти законну точку доступу. Транслюючи той самий SSID і маючи вищу потужність сигналу, ніж справжня точка доступу, він може переконати нових клієнтів підключитися до фальшивої точки. Крім того, зловмисник може відключити клієнтів, які підключені до легітимної точки доступу, а потім заманити їх підключитися до своєї підробленої точки доступу.

Такі атаки можуть бути неефективними проти мереж Wi-Fi з високим рівнем захисту, оскільки зловмисник не має доступу до парольної фрази. Крім того, відкриті мережі без захисту можуть викликати підозри у користувачів. У той час, мережі Wi-Fi зі слабким захистом або відкриті мережі є простими мішенями для подібних атак. Відкриті мережі можна зустріти практично скрізь, і вони часто мають високий обсяг трафіку через те, що надають безкоштовний доступ до Інтернету.

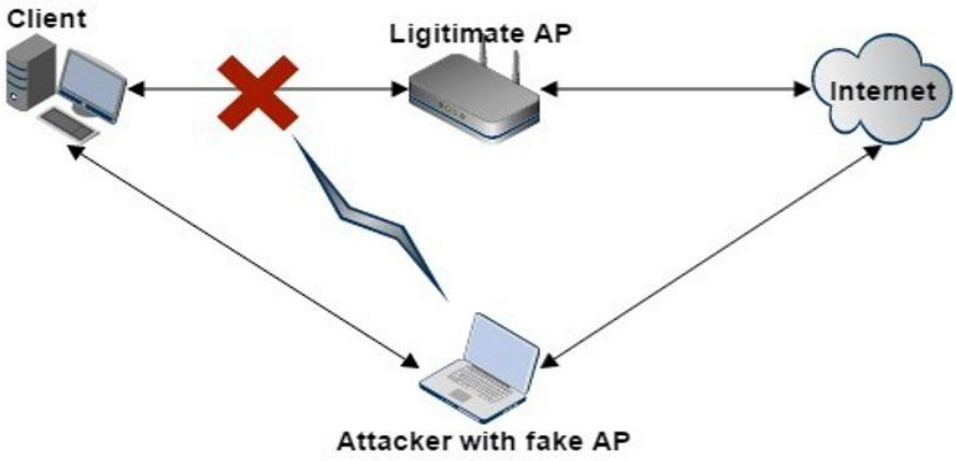


Рисунок 1.5. – Модель атаки «Людина посередині»

Такі точки доступу можна знайти, наприклад, в аеропортах чи на автобусних станціях, і через те, що використання заходів безпеки в них ускладнене, вони не мають належного захисту, що робить їх ідеальними цілями для атак MITM. У цьому дослідженні будуть тестуватися лише відкриті мережі.

ESS (Extended Service Set) — це система, що об'єднує кілька BSS (Basic Service Set) у межах однієї території. Точки доступу в ESS зазвичай з'єднані між собою через дротову мережу.

У середовищі ESS кожна точка доступу має свою унікальну ідентифікацію BSS, відому як BSSID. Проте для зручності управління всі точки доступу в ESS використовують спільну ідентифікацію, що називається ESSID.

Щоб досягти цього, всі точки доступу повинні бути в одній підмережі та бути підключені до одного маршрутизатора. Максимальний розмір ESSID становить 32 байти, і він може бути буквено-цифровим. У такій мережі всі пристрої повинні бути налаштовані на використання одного і того ж ESSID, інакше вони не зможуть обмінюватися даними, наведено на рисунку 1.6.

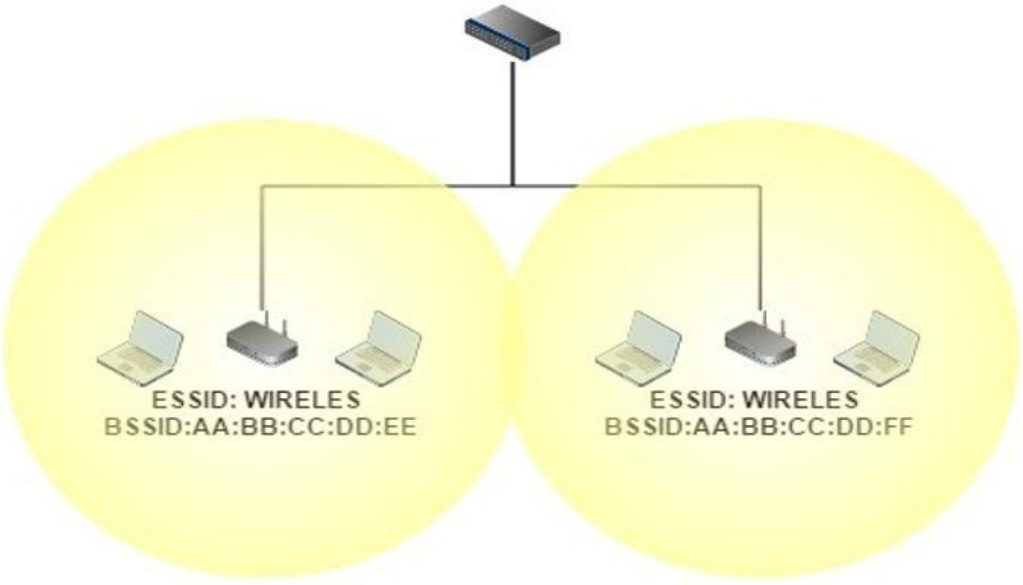


Рисунок 1.6. – Розширений набір послуг

може включати в себе кілька різних BSSID в межах великої мережі, і ці ідентифікатори можуть змінюватися в будь-який момент.

ESSID є назвою мережі, яку передають так, щоб користувачі могли її ідентифікувати і підключитися до неї через свої мережеві пристрої.

Кожна бездротова мережа має власні механізми безпеки, які обмежують доступ зловмисників до переданих даних, але рівень їхньої надійності залежить від обраної конфігурації та технології. Найпростіші методи, такі як фільтрація MAC-адрес, базуються на дозволі доступу лише для певного списку пристроїв, але вони легко обходяться шляхом підміни MAC-адреси зловмисником. Приховані ESSID (ім’я мережі) лише приховують її з публічного огляду, але це не є перешкодою для спеціалізованих інструментів сканування.

Аутентифікація за допомогою застарілого WEP, хоч і забезпечує базовий рівень захисту, є вразливою до швидких атак через слабкість алгоритму шифрування.

Сучасніші стандарти WPA/WPA2 значно підвищують рівень безпеки за рахунок складніших алгоритмів шифрування, таких як AES, але їхній захист може бути зведений нанівець при використанні слабких паролів або через атаки на протоколи аутентифікації, наприклад, через захоплення handshake. Саме тому використання комплексного підходу, наприклад WPA3 із довгими складними паролями та регулярним оновленням ключів, є ключовим для мінімізації ризиків.

2 АЛГОРИТМ ВИЯВЛЕННЯ АТАК ТИПУ “ЛЮДИНА ПОСЕРЕДИНІ” В БЕЗПРОВОДНИХ МЕРЕЖАХ

Після впровадження бездротових мереж, вони швидко здобули популярність завдяки зручності використання без необхідності прокладати дроти та можливості передавати інформацію через повітря. Однак за цією зручністю стоїть певна ціна, адже радіосигнали можуть досягати не лише передбаченого приймача, а й будь-якого іншого пристрою в радіусі кількох сотень метрів. Це означає, що будь-хто, навіть без спеціальних знань, може увірватися в мережу, що робить бездротові мережі не лише зручними, але й вразливими для злому.

У цьому розділі розглядається один із типів атак на бездротові мережі, відомий як атака "людина посередині" (MITM). Буде розглянуто, які слабкі сторони призводять до таких атак, як їх виявити, а також способи захисту від них.

Зокрема, буде запропоновано метод виявлення атак MITM через аналіз часових міток заголовків TCP-пакетів. На основі цих міток можна виміряти затримки, порівнюючи середні значення затримок поточного з'єднання з даними, отриманими з попередніх сеансів. Це дозволяє виявити пакети з аномально довгими затримками, що може бути ознакою атаки.

Також буде продемонстровано, як за допомогою цього методу можна встановити порогові параметри для точної ідентифікації атак MITM з мінімальною ймовірністю помилкових спрацьовувань. Такий метод може бути використаний як ефективний засіб для запобігання атакам. Проте на даному етапі цей підхід є більш ефективним у статичних системах, де затримки стабільні та не піддаються великим варіаціям.

2.1. Методи виявлення атак

Перш за все, зловмисники можуть перехоплювати трафік між двома кінцевими точками (жертвами) за допомогою спуфінгу, що дозволяє їм отримувати дані без відома жертви. Одним із важливих типів такої атаки є ARP-спуфінг

(спуфінг протоколу вирішення адрес), що дозволяє зловмисникам перехоплювати дані, маніпулюючи відображенням IP-адрес на MAC-адреси.

ARP відповідає за відображення IP-адрес на фізичні адреси MAC і зберігає ці відображення в кеші ARP. Зловмисники можуть відправляти фальшиві ARP повідомлення в мережу, змінюючи відповідність IP-адреси і MAC-адреси, завдяки чому їхні пристрої отримують доступ до трафіку, призначеного іншому комп'ютеру. Цей метод дозволяє зловмисникам стати "людиною посередині" (MITM), перехоплюючи і змінюючи трафік між пристроями.

Коли фальшиве ARP повідомлення досягає цільового пристрою, воно змінює таблицю ARP на ньому, в результаті чого трафік починає йти через зловмисника. Зловмисник не тільки перехоплює цей трафік, але і може змінювати його або перенаправляти на інші місця, наприклад, до свого власного сервера, без відома легітимних користувачів.

Існують різні методи захисту від таких атак:

– ARP Defender та ARP Guard - інструменти для виявлення ARP-спуфінгу, які можуть блокувати фальшиві ARP повідомлення в мережі;

– Криптографічне рішення: S-ARP (Secure ARP) використовує шифрування для автентифікації ARP-відповідей, що дозволяє запобігти підробці ARP;

– Апаратне рішення: деякі мережеві комутатори реалізують динамічне тестування ARP, що дозволяє додатково забезпечити захист від ARP-спуфінгу.

Іншою поширеною атакою є DNS-спуфінг або підміна сервера доменних імен. DNS-запити є незашифрованими, що дозволяє зловмисникам перехоплювати трафік і перенаправляти його на фальшиві вебсайти. Ця атака відома як підміна DNS-кешу, коли зловмисники замінюють записи DNS на скомпрометованому сервері, направляючи користувачів на фальшиві ресурси.

DNSSEC (DNS Security Extensions) — це протокол, що додає додаткові методи перевірки для захисту DNS, запобігаючи підмінам.

Ще одним важливим аспектом є атака підміни IP. У цьому випадку зловмисники змінюють адресу джерела в заголовках пакетів, змушуючи приймача думати, що пакет надійшов з надійного джерела. Такі атаки можуть

використовуватися для перехоплення або зміни трафіку між двома легальними вузлами, роблячи зловмисника "людиною посередині".

Для захисту від підміни IP необхідно впроваджувати моніторинг мережі для виявлення аномальних активностей, використовувати фільтрацію пакетів і застосовувати надійні методи перевірки та аутентифікації.

DHCP-спуфінг — це атака, коли зловмисник підміняє DHCP-сервер і починає перенаправляти трафік на себе. Щоб захиститися від цієї атаки, можна використовувати відстеження DHCP та фільтрацію підроблених повідомлень.

Протоколи безпеки, такі як SSL і TLS, забезпечують захист даних, що передаються через Інтернет, але вони можуть бути обійдені за допомогою атаки через підробку сертифікатів. У такій ситуації зловмисник може змусити жертву прийняти підроблений сертифікат, встановити з ним з'єднання і потім перехоплювати та змінювати всі повідомлення, що передаються між сервером і користувачем.

Для захисту від таких атак важливо правильно налаштовувати безпеку з'єднань, використовувати надійні сертифікати та перевіряти їх автентичність.

2.2. Алгоритми роботи методу.

У цій роботі буде розглянуто метод своєчасного виявлення атак типу "людина посередині" (MitM) при підключенні до знайомих веб-сайтів в умовах немобільних систем. Основна ідея полягає в аналізі часу затримки TCP-пакетів для виявлення аномалій, характерних для таких атак.

Пропоноване рішення базується на використанні міток часу TCP-пакетів, які дозволяють обчислювати затримку між передачею та отриманням послідовних пакетів. Порівнюючи середнє значення затримок в поточній сесії з даними, зібраними з попередніх сесій з тим самим сервером або вебсайтом, можна виявити аномальні затримки, які можуть свідчити про те, що трафік перехоплюється або змінюється зловмисником.

Цей метод дозволяє виявити атаки MitM без потреби в додаткових засобах автентифікації, покладаючись лише на аналіз часу передачі даних між кінцевими точками. За допомогою порівняння затримок в поточній сесії з еталонними значеннями, отриманими з попередніх підключень, можна ефективно ідентифікувати підозрілі аномалії, що виникають через проміжний контроль трафіку атакуючим.

Як працює цей метод:

– Збір еталонних даних: Для кожної сесії з конкретним сервером або вебсайтом зберігаються дані про затримки TCP-пакетів. Це можуть бути дані з кількох попередніх підключень, які використовуються як еталони.

– Порівняння затримок: Під час нової сесії між користувачем і вебсайтом вимірюються затримки TCP-пакетів. Якщо затримки значно відрізняються від еталонних значень (наприклад, вони значно довші або непередбачувані), це може вказувати на атаку.

– Виявлення аномалій: Якщо затримки перевищують певний поріг або відрізняються від очікуваних, можна запідозрити, що між користувачем і сервером знаходиться третя сторона, яка перехоплює трафік (зловмисник).

– Необхідність в автентифікації: Важливо зазначити, що цей метод не вимагає жодної додаткової автентифікації або використання криптографії, а покладається лише на вимірювання і порівняння часу, що є його основною перевагою в простоті реалізації.

Цей підхід може бути ефективним для виявлення атак MitM у мережах з низьким рівнем безпеки, де традиційні методи автентифікації або шифрування можуть бути складними або відсутні. Однак він також має свої обмеження, наприклад, залежність від стабільності затримок у мережі та можливих змін у поведінці мережі через зовнішні фактори.

Розглянемо такий сценарій: Аліса починає підключення до веб-сайту Boogle у той час, коли вона перебуває на домашньому комп'ютері. З'єднання перехоплюється Євою та змінюється, перш ніж його пересилають до Boogle. Ця дія займає деякий час t_1. Boogle отримує TCP-пакети та надсилає відповідь Алісі.

Знову ж таки, Єва перехоплює з'єднання перед тим, як переслати пакети Алісі, а це займає час t_2.

Нарешті, Аліса знову отримує відповідь від Бугла в той час. Затримка цього з'єднання дорівнює $\tau = t_s + t_r$. На основі даних попередніх кон- екцій ми можемо обчислити середнє значення μ та оцінити мінімальну затримку, спричинену перехопленням Eves $(t_1 + t_2) = \delta$, і вибрати поріг виявлення $\theta > \mu$ такий, що $t_i + \delta_i > \theta > \tau_i$,i = 1, 2... .

Запропонована гіпотеза полягає в тому, що шляхом збору та аналізу пакетів затримок безпечних з'єднань, можна оцінити виявлення атаки MitM і не спричинити помилкові спрацьовування від нормальних з'єднань. Так як його важко оцінити, для тестування було обрано якомога нижчий поріг і перевірено його на помилкові спрацьовування. Отже, маємо свою нульову гіпотезу $H_1 : T_i$

Аьтернативна гіпотеза вигладає наступним чином $H_1 : T_i < i = 1,2, \dots$.

Для ефективного виявлення атак "людина посередині" (MitM) за допомогою міток часу TCP-пакетів важливо враховувати кілька ключових припущень, які можуть вплинути на точність та надійність цього методу. Ось деякі з них, які були враховані в даному підході:

– Статичність кінцевих точок: Це припущення є критичним, оскільки воно передбачає, що дві кінцеві точки (наприклад, користувач і сервер) не змінюють свого фізичного місцезнаходження в мережі. Якщо кінцеві точки будуть переміщатися, то мережеві умови можуть змінюватися, і це може призвести до змін у затримках, які важко пояснити без залучення зовнішніх факторів, таких як атака.

– Постійна швидкість каналу зв'язку: Припускається, що швидкість каналу зв'язку між кінцевими точками залишається стабільною протягом сесії. Це дозволяє припустити, що затримки, виміряні для TCP-пакетів, будуть досить передбачуваними і не повинні значно змінюватися, якщо мережеві умови залишаються сталими.

– Еталонне значення затримки: Для того щоб порівнювати затримки TCP-пакетів, ми припускаємо, що принаймні один раз було отримано безпечне

з'єднання, яке дозволяє нам встановити середнє значення затримок між двома кінцевими точками. Це значення може бути використано як еталон для порівняння з подальшими сесіями. Якщо затримки значно відрізняються від цього еталонного значення, це може сигналізувати про наявність зловмисника.

– Відсутність шкідливих кінцевих точок: Важливо також припустити, що жодна з кінцевих точок не є шкідливою. Це означає, що немає внутрішніх загроз або скомпрометованих пристроїв, які можуть змінювати або маніпулювати часом передачі даних. Це дає можливість вважати, що будь-які аномалії в затримках пов'язані з зовнішніми факторами, такими як атака MitM.

– Точність вимірювання часу: Для реалізації цього методу критично важливо мати точну синхронізацію часу на обох кінцевих точках. Якщо є серйозні розбіжності в часі між пристроями, це може вплинути на точність обчислення затримок і порівняння їх з еталонними значеннями. Тому передбачається, що обидві кінцеві точки мають можливість точно вимірювати час надходження пакетів, що дозволяє точно визначити затримки.

– Загальні наслідки цих припущень: Якщо всі припущення виконуються, то метод виявлення атак MitM за допомогою аналізу затримок TCP-пакетів є досить ефективним для виявлення аномалій. Однак будь-яке відхилення від цих припущень може призвести до помилкових спрацьовувань або неправильних висновків, тому важливо враховувати фактори, які можуть впливати на мережеві умови, як-от мережеві перегрузки, зміни конфігурації мережі, або навіть природні коливання в затримках, зумовлені інтернет-провайдерами чи фізичними відстанями між точками.

Цей метод може бути особливо корисним у ситуаціях, де застосування складних криптографічних протоколів або автентифікацій є недоцільним або неможливим, але він також має свої обмеження в специфічних умовах.

2.3. Підготовка до експерименту

Для тестування та аналізу можливості виявлення атак "людина посередині") за допомогою аналізу міток часу TCP-пакетів була розроблена тестова установка, що складається з кількох ключових елементів. Ось деталі описаного підходу:

Прототип на Python 2.6: Основою тестової установки є прототип, написаний на Python 2.6. Цей прототип використовує бібліотеки pcapy та impacket для захоплення та аналізу мережевих пакетів. pcapy: бібліотека для захоплення мережевих пакетів, яка дозволяє працювати з даними, що передаються по мережі. impacket: набір бібліотек Python для роботи з мережевими протоколами. Вона дозволяє аналізувати пакети і перетворювати IP-адреси на більш зручні для людини адреси, як-от URL.

Використання Squid 3 як зловмисника MitM: В якості зловмисника для реалізації атаки MitM використовувався налаштований проксі-сервер Squid 3. Squid дозволяє перехоплювати та змінювати HTTP-запити та відповіді між клієнтом та сервером. Це дозволяє зловмиснику бути між двома кінцевими точками і маніпулювати мережевим трафіком.

Збір даних за допомогою скрипта: Скрипт запускається на пристрої, який використовує браузер Mozilla Firefox для завантаження веб-сайту протягом 2 хвилин. Під час цього процесу скрипт займається моніторингом TCP-пакетів. Вся отримана інформація, зокрема IP-адреси джерела та призначення, перетворюється на URL-адреси для подальшого аналізу. Якщо URL-адреса призначення знаходиться в списку спостереження, то програма збирає відповідні дані з пакетів, включаючи мітки часу, номери послідовностей та номери підтвердження. Всі старіші пакети з однаковими даними видаляються, щоб уникнути дублювання інформації.

Обчислення затримки: Якщо URL-адреса джерела знаходиться в списку спостереження, програма проводить перевірку номера підтвердження. Номер підтвердження пакета мінус один порівнюється з вже збереженими номерами послідовностей. Якщо знаходиться збіг, то на основі міток часу обчислюється затримка між пакетами. Отримані затримки додаються до списку і розраховується

середнє значення поточних затримок. Для оптимальної роботи прототипу дані, де затримка перевищує одну секунду, видаляються.

Оптимізація роботи прототипу: Очищення даних із затримкою більше однієї секунди: Цей крок є важливим для фільтрації аномальних затримок, які можуть бути спричинені різними факторами, такими як надмірне навантаження на мережу чи інші проблеми, не пов'язані з атакою. Вилучення таких даних дозволяє оптимізувати процес аналізу та уникнути помилкових спрацьовувань.

Загальна схема роботи прототипу: Прототип збирає мітки часу для кожного TCP-пакета, пов'язаного з URL-адресами, які цікавлять дослідника. Зібрані дані аналізуються на основі затримок між пакетами. Порівняння середніх затримок дозволяє виявляти аномалії в мережевому трафіку, що можуть свідчити про наявність атаки MitM, особливо якщо затримки відрізняються від нормальних значень.

Переваги та обмеження тестової установки: Безшумний метод виявлення: Використання лише міток часу для обчислення затримок дозволяє виявляти аномалії без необхідності автентифікації або додаткових складних алгоритмів. Легкість в інтеграції: Оскільки метод використовує базові засоби моніторингу TCP-пакетів, його можна легко інтегрувати у вже існуючі мережеві протоколи та інструменти.

Обмеження: Обмеження на час: Прототип працює лише за умови, що хоча б один безпечний сеанс був успішно встановлений для отримання еталонних затримок. Потрібна стабільність мережі: Для ефективної роботи методу необхідно, щоб мережеві умови залишались стабільними без значних змін у затримках, зумовлених перегрузками або проблемами з маршрутизацією. Обмеження на мобільні системи: Прототип було розроблено для немобільних систем, де мережеві затримки зазвичай стабільні. У мобільних мережах, де затримки можуть змінюватися через фізичне переміщення, точність аналізу може бути знижена. Ця установка надає корисний інструмент для дослідження та моніторингу атак MitM в мережах, де додаткові протоколи безпеки або криптографічні методи не застосовуються або є надмірними для деяких випадків.

Під час збіжності протоколу маршрутизації можуть виникати тимчасові петлі пересилання, через які пакети можуть зазнавати надмірно великих затримок. Такі затримки не відображають реальну продуктивність мережі і мають розглядатися як аномальні значення під час оцінки затримки, рисунок 2.1.

Прототип відстежує середню затримку поточного сеансу μ_0 і робить попередження при $\mu_0 > \theta$, де θ – поріг виявлення. Якщо з'єднання безпечне, зібрані дані зберігаються з оновленим середнім і стандартним відхиленням.

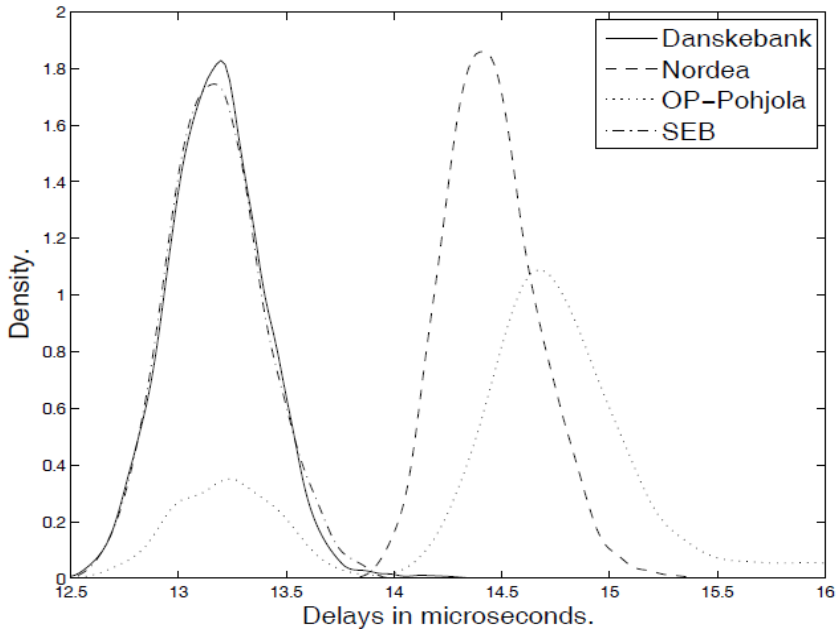


Рисунок 2.1. – Затримка в обидві сторони, яка часто може бути акомпенсована усіченим нормальним розподілом.

Семплінг здійснювався шляхом аналізу TCP-пакетів протягом 24 годин. Для цього скрипт підключався до цільового веб-сайту з інтервалом у дві хвилини. Після цього провели другий тест на тому ж веб-сайті, спрямовуючи підключення через проксі-сервер для моделювання атаки "людина посередині" (MitM).

Також потрібно включити деякі запобіжні заходи проти впливу дисперсії σ_2 в інтернет-трафіку. Найкращим способом впоратися з усім цим було б використання простого порогу виявлення $\theta = \mu + \sigma$, де μ і σ— середнє значення і стандартне відхилення від попередніх з'єднань. Він повинен мати можливість виявляти всі атаки MitM без ризику багатьох помилкових спрацьовувань.

Таким чином, нульова гіпотеза виглядає: $H_0: \tau_i \geq \mu + \sigma$ а альтернативна гіпотеза: $H_1: \tau_i \geq \mu + \sigma$. Щоб перевірити гіпотезу оптимального θ, були зібрані дані за допомогою систематичної вибірки від чотирьох великих скандинавських фінансових компаній : Nordea, SEB, Danske Bank і OP-Pohjola Group.

Таблиця 2.1. Статистичні параметри за результатами тестування.

URL-адреса	Частота	s	Хв.	M	99-й процентиль	ϑ = поріг	Макс	$\tau_{i>}\vartheta$	Мін. Проксі
www.dankse bank.com	12600	3.163	12.48	13.28	14.30	16.44	200.2	0.29%	22.65
www.nordea.com	13570	2.465	13.48	14.58	15.40	17.04	220.6	0.73%	22.79
www.op.fi	5644	2.036	12.53	14.53	16.21	16.57	27.63	0.46%	23.20
www.sebgroup.com	5921	2.234	12.55	13.31	13.90	15.54	94.37	0.54%	23.21

2.4. Висновки

Був запропонований ефективний метод виявлення та визначення місцезнаходження зловмисника типу "людина посередині" (MitM) у бездротових мережах. Основою цього методу є вимірювання часу проходження сигналу туди й назад (RTT) та аналіз потужності отриманого сигналу (RSS) від точки доступу. У разі присутності зловмисника ці показники зазнають значних змін: затримка (RTT) збільшується, а потужність сигналу (RSS) може відхилятися від норми.

Для виявлення зловмисника використовується аналіз аномалій у мережевих характеристиках. Цей процес потребує збору достатньої кількості даних про RTT під час передачі сигналів між відправником і одержувачем, що дозволяє створити статистичну модель для виявлення відхилень.

Одним із ключових компонентів є протокол синхронізації годинників. Він передбачає передачу повідомлень із позначками часу, що забезпечує введення постійної затримки для всіх з’єднань. Якщо зловмисник втручається в зв'язок і не

може забезпечити постійну затримку, його можна виявити завдяки аналізу відмінностей у часових характеристиках.

Модифікація рівня управління доступом до медіа (MAC) також сприяє виявленню зловмисника. Для з'єднання вузли обмінюються підтвердженнями (ACK). Якщо зловмисник перебуває між вузлами, він може намагатися надсилати підтвердження раніше, ніж це передбачено, що є явною ознакою його присутності.

Фізичний рівень також відіграє важливу роль у виявленні. Інформація, така як потужність сигналу (RSS), є складною для підробки. У статичних умовах точка доступу передає сигнал із певною потужністю на довірені приймачі. Якщо у зловмисника значення RSS не відповідає очікуваним параметрам, це може свідчити про його присутність.

Загалом, метод базується на аналізі характеристик RTT, RSS, синхронізації годинників та поведінки вузлів, що дозволяє ефективно виявляти потенційні атаки MitM у бездротових мережах.

Статистичні параметри за результатами моїх тестів ми можемо побачити в таблиці 2.1. Усі затримки від проксі-з'єднань були значно більшими, ніж порогові значення, сформовані з нормальних з'єднань. Різниця між мінімальною затримкою від проксі та порогом становить понад 6 мс у кожному наборі даних.

На рисунку 2.1, ми бачимо функції щільності ймовірності затримки пакетів, нижчої за 99-ту квантильну точку.

Незважаючи на те, що різниця між мінімальним і 99-м процентилем становить менше 5 мс при кожному з'єднанні, максимальна затримка значно перевищує 99-й процентиль. Оскільки кількість пакетів з такою екстремальною затримкою дуже мала, вони представляють дуже рідкісні події в мережі.

Велика частина затримок зосереджена поблизу середнього значення з усіченим лівим хвостом і довгим правим хвостом. Виняток становлять затримки від www.op.fi , які утворюють два піки, це, ймовірно, викликано тими пакетами, що надходять з двох різних місць.

На рисунку 2.2 показані затримки до 30 мікросекунд від www.op.fi розташовані за часом їх прибуття. Мінімальна затримка через проксі – 23.20

мілісекунд, виявлення обмолоту - 16.57 мілісекунд, а частота не є актуальною інформацією з точки зору звичайних зловмисників.

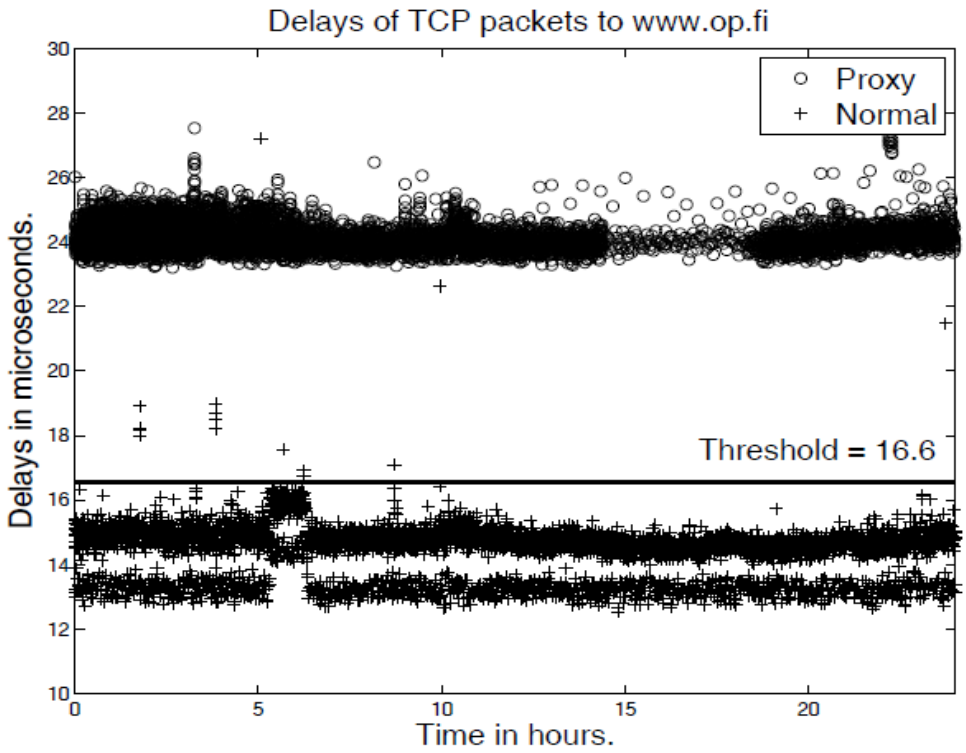


Рисунок 2.2. – Приклад, якби це була справжня атака MitM, прототип помітив би її зі 100% точністю.

У цьому розділі детально розглянуто метод виявлення атак типу "людина посередині" (MitM) та його практичне застосування. Метод базується на аналізі таких параметрів, як час проходження сигналу (RTT), потужність сигналу (RSS) та інші ключові характеристики. Результати випробувань підтвердили ефективність запропонованого підходу у виявленні атак MitM. Помилкові спрацьовування є рідкісними і трапляються лише за умов, які не характерні для нормальної роботи мережі.

Попри високу ефективність, метод має обмеження. Для його коректного функціонування потрібні стаціонарні пристрої, які не змінюють свого фізичного положення, та стабільне інтернет-з'єднання. Це обмежує його застосування у мобільних середовищах або за умов нестабільного зв’язку. Водночас метод чудово

підходить для моніторингу та захисту критичних мережевих ресурсів, особливо у мережах із високими вимогами до безпеки.

Методологія може бути корисною для захисту невеликої кількості важливих ресурсів, наприклад, у комерційних інтернет-провайдерів, де захист даних є критично важливим. Його додатковою перевагою є мінімальний рівень хибнопозитивних результатів, який становить лише 0.46%. Це забезпечує високу точність навіть у ситуаціях, де помилкові спрацьовування є небажаними.

У реальних сценаріях атаки MitM метод демонструє 100% ефективність, що підтверджує його потенціал для забезпечення мережевої безпеки. Таким чином, запропонований підхід є надійним і перспективним інструментом для виявлення та нейтралізації загроз у сучасних мережах.

3 РОЗРОБКА МЕТОДУ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ДЛЯ АТАКИ “ MAN-IN-THE MIDDLE” В БЕЗДРОТОВИХ МЕРЕЖАХ

З появою великої кількості пристроїв Інтернету речей (IoT) обсяги даних, які обробляються постачальниками хмарних послуг, значно зросли, що спричинило збільшення затримок у роботі хмарних сервісів. Це, своєю чергою, впливає на продуктивність багатьох IoT-додатків. Для мінімізації цих затримок у мережі використовуються обчислювальні пристрої, розташовані ближче до кінцевого користувача, які називаються "вузлами туману". Вузли туману дають змогу обробляти частину даних на місці, зменшуючи потребу у відправленні інформації до віддалених дата-центрів.

Хоча дата-центри мають значні ресурси (обчислювальну потужність, енергетику та пам'ять), вузли туману такими ресурсами не володіють. Це ускладнює використання традиційних методів запобігання вторгненням, які можуть створювати додаткові затримки або значне енергоспоживання. Тому виникає потреба у створенні ресурсоефективних, але водночас потужних систем безпеки для захисту шару туману від атак.

У цьому розділі розглянуто можливості застосування систем виявлення вторгнень (IDS) і систем запобігання вторгнень (IPS) для протидії атакам типу "людина посередині" (MitM) у середовищі туману.

– Системи виявлення вторгнень (IDS): IDS складаються з вузлів, які регулярно опитують сусідні вузли, розташовані на відстані одного стрибка, для виявлення підозрілих дій;

– Системи запобігання вторгнень (IPS): IPS використовують легковагові методи шифрування для протидії атакам типу MitM та їх варіаціям, включаючи підслуховування, модифікацію пакетів та атаки з використанням червоточин.

Запропоновані рішення спрямовані на забезпечення безпеки шару туману без значного впливу на продуктивність або енергоспоживання, що робить їх придатними для ресурсомісткого середовища IoT.

3.2. Постановка задачі

На рисунку 3.1 показана типова розподілена мережа туману. У цій мережі пристрої IoT запитують послуги з вузлів туману. Туманні вузли зазвичай мають вищі ресурси, ніж пристрої IoT, і вони фізично ближчі до пристроїв IoT порівняно з хмарними серверами. Таким чином, отримання послуг від вузлів туману зменшує затримку.

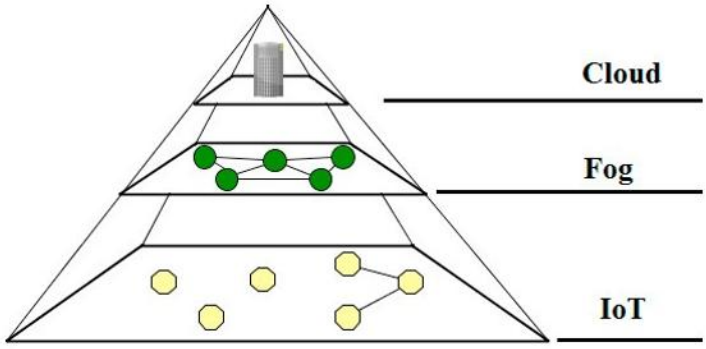


Рисунок 3.1. – Мережева архітектура розподіленої мережі туману.

Вузли туману та пристрої IoT можуть використовувати будь-яке середовище та протокол для зв'язку. Якщо вони використовують одне і те ж середовище і протокол, обидва вузли IoT і туман користуються наступним:

– Менша складність дизайну, оскільки лише один мережевий стек і усувається необхідність перетворення пакетів з однієї форми в іншу;

– Відсутність пакетного перетворення, знижує енергоспоживання і затримку мережі.

На рисунку 3.2 наведена схема запропонованої системи. Особливістю цієї системи є її симетрія та близькість розташування вузлів, які забезпечуються завдяки принципу розгортання вузлів IDS на мінімальній відстані, яка становить один стрибок. Такий підхід дозволяє значно зменшити затримку при обробці даних і підвищити ефективність системи. Вузли IDS розташовуються таким чином, щоб мати безпосередній доступ до тих вузлів, які вони спостерігають, використовуючи концепцію колісних спиць, що забезпечує оптимальну топологію мережі.

Кожен вузол IDS відіграє ключову роль у забезпеченні безпеки мережі, виконуючи моніторинг мережевих процесів та оперативно виявляючи скомпрометовані вузли або дії зловмисників. У разі виявлення загрози вузол IDS не лише реєструє інцидент, але й негайно передає повідомлення сусіднім вузлам у межах своєї зони доступу.

Ці вузли отримують інструкцію припинити зв’язок із виявленим скомпрометованим вузлом, що дає змогу оперативно знизити ризик поширення загрози та підтримати стабільність і безпеку всієї системи. Такий підхід забезпечує швидку реакцію на потенційні атаки та ефективний захист мережі.

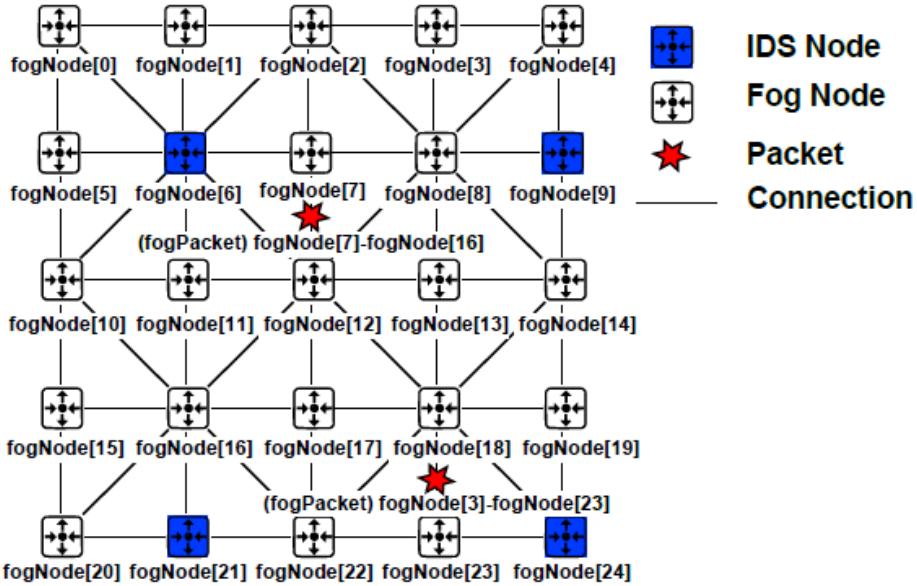


Рисунок 3.2. – Мережа туману, змодельована за допомогою OMNET++.

Крім того, пакети маршрутизуються від джерела до місця призначення шляхом спочатку переміщення пакетів у вигляді кількох стрибків уздовж осі Y (тобто вгору або вниз). Пакети рухаються в цьому напрямку, поки не досягнуть ряду пункту призначення. Потім пакети рухаються вздовж осі X (тобто назад або вперед), поки не досягнуть пункту призначення.

3.3. Проведення експериментів

У цьому дослідженні розглядається сценарій атаки типу "людина посередині" (MitM) у шарі туману, де зловмисник перехоплює пакети, що передаються між хмарою, IoT-пристроями та вузлами туману. Зловмисник має обчислювальні ресурси, які перевищують ресурси вузлів туману, але поступаються можливостям хмарної інфраструктури. Ця різниця в ресурсах відіграє важливу роль у визначенні можливостей і обмежень зловмисника.

Хоча зловмисник може бути обізнаний про існування вузлів IDS і принципи роботи протоколу, він не має доступу до деталей їхньої роботи. Це зумовлено тим, що характер опитувань вузлами IDS був запрограмований заздалегідь під час їх налаштування, що ускладнює передбачення цих дій.

Система складається з двох типів вузлів:

– Вузли туману (FN): Відповідають за надання послуг IoT-пристроям з мінімальною затримкою;

– IDS-вузли: Виконують функцію моніторингу та забезпечення безпеки.

Забезпечення безпеки:

– Шифрування: Для забезпечення конфіденційності система використовує симетричне шифрування AES (Advanced Encryption System), яке відоме своєю надійністю. Заголовки пакетів не шифруються, щоб зменшити затримку передачі;

– Обмін ключами: Для встановлення ключів шифрування використовується алгоритм Діффі-Хеллмана, який є стандартом у криптографії;

– Ключі: Вузли IDS отримують ключі з хмари і передають їх вузлам FN, забезпечуючи безпечний початковий обмін.

Алгоритм опитування вузлів FN:

– IDS-вузол надсилає зашифрований пакет, який містить ціле число (корисне навантаження);

– Вузол FN розшифровує пакет, виконує операцію множення корисного навантаження на 2, потім знову шифрує результат і надсилає його назад вузлу IDS;

– IDS-вузол аналізує отриману відповідь і оцінює її коректність, щоб перевірити надійність вузла FN.

Переваги системи:

– Надійність: Використання AES та алгоритму Діффі-Хеллмана забезпечує високий рівень криптографічного захисту;

– Ефективність: Система оптимізована для роботи з обмеженими ресурсами вузлів туману;

– Безпека: Навіть якщо зловмисник має доступ до пакетів, шифрування корисного навантаження та використання передбаченого алгоритму опитування значно ускладнюють атаку.

Цей підхід забезпечує надійний захист шару туману від атак Man-In-The-Middle (MitM) та їхніх варіантів, завдяки використанню механізмів, які забезпечують аутентифікацію, цілісність і конфіденційність даних. Водночас такий підхід оптимізує затримку передачі даних і знижує енергоспоживання, що є критичним для пристроїв з обмеженими ресурсами. Для підвищення рівня безпеки можна впроваджувати складніші методи обчислень, такі як криптографічні операції за модулем, які ускладнюють компрометацію ключів шифрування.

Ці операції можуть забезпечувати контроль автентичності даних на кожному етапі передачі. У разі, якщо повернутий пакет не відповідає заданим критеріям, вузол системи виявлення вторгнень (IDS) може оперативно визначити, що приймач або передавач є скомпрометованим або діє як шкідливий вузол. У таких випадках IDS може ініціювати блокування підозрілих пакетів, перенаправлення трафіку або надсилання сповіщення адміністратору для подальшого розслідування, запобігаючи можливим загрозам і мінімізуючи наслідки атаки.

На рисунку 3.3 та у Таблиці 3.1 наведені відповідно псевдокод і таблиця істинності, які ілюструють, як саме вузол IDS здійснює опитування кожного вузла системи. Це дозволяє з високою точністю ідентифікувати скомпрометовані вузли та забезпечити безперебійну роботу мережі.

```
1:  t_out ← timeout                                   // t_out and t_0 To be set by network administrator
2:  t_0 ← allowed Delay                               // "i" are set of nodes under supervision of a given IDS node
3:  for each fog node i do
4:     t_1 ← time()                                   // get current time
5:     t_2 ← 0
6:     pkt ← x                                        // x is randomly generated unsigned integer
7:     IDS sends pkt to fog node i
8:     repeat
9:        t_2 ← time()                                // While waiting for packet keep checking time
10:       Δ ← t_2 − t_1
11:    until (Reply_pkt received OR Δ > t_out )
12:    if ( Δ > t_out) then
13:       if (Reply_pkt not received) then
14:          attack is possibly wormhole              // Once Δ > t_out IDS stops listening for Reply_pkt
15:       end if
16:    else
17:       y ← Extract fog Node's answer from Reply_pkt   // Fog node should change x to 2x and reply to IDS
18:       if (Δ > t_0 AND Reply_pkt is received AND y ≠ x × 2) then
19:          attack is possibly packet altering or lack of context
20:       else if (Δ > t_0 AND Reply_pkt is received AND y = x × 2) then
21:          attack is possibly altering
22:       else if (Δ < t_0 AND Reply_pkt is received AND y ≠ x × 2) then
23:          attack is possibly eavesdropping
24:       else
25:          fog node is not compromised
26:       end if
27:    end if
28: end for
```

Рисунок 3.3. – Псевдокод алгоритму

Вузол IDS виконує додаткові перевірки шляхом вимірювання часу проходження пакета допиту в обидва напрямки — від себе до цільового вузла та назад. Якщо зафіксований час перевищує заздалегідь встановлене порогове значення, це є індикатором потенційної загрози. Така поведінка може бути спричинена тим, що вузол-кандидат здійснює небажані дії, наприклад, копіює або навмисно змінює пакети, що порушує нормальний процес передачі даних.

Крім того, у разі, якщо відповідь на пакет допиту взагалі не надходить, це також розцінюється як підозріла активність. У таких ситуаціях можна припустити, що вузол отримав запит, але свідомо не виконав його обробку згідно з протоколом. Це може свідчити про реалізацію атаки типу "червоточина", коли зловмисник перехоплює пакети без наміру повертати відповідь, прагнучи уникнути виявлення системою контролю.

Реакція IDS на аномальну активність:

– Аномальні затримки: Якщо час відповіді перевищує порогове значення, IDS фіксує це як загрозу;

– Відсутність відповіді: Якщо відповідь на допит не надходить, це також викликає тривогу, що вказує на ймовірну дію зловмисника;

– Аналіз результатів: У будь-якому з цих випадків IDS проводить аналіз виявлених аномалій, що дозволяє ідентифікувати вузли, які порушують нормальну роботу мережі.

Таблиця 3.1. Таблиця істинності для IDS

$\Delta >$ *рекламу*		$\Delta >$ *t0*	відповісти pkt отримано	$y \neq x \times 2$	Напад	Коментар
0		0	0	0	0	Чекаємо відповіді pkt
0		0	0	1	x	Не можливо, відповідь pkt ще не отримано
0		0	1	0	0	Вузол в безпеці
0		0	1	1	1	Напад, підслуховування або відсутність контексту
0		1	0	0	x	Чекаємо відповіді pkt
0		1	0	1	x	Не можливо, відповідь pkt ще не отримано
0		1	1	0	1	Атака, можливо, зміна контенту
0		1	1	1	1	Атака, можливо, зміна контенту або відсутність контексту
1		0	0	0	x	Неможливо, *tout* > *t0*
1		0	0	1	x	Неможливо, *tout* > *t0*
1		0	1	0	x	Неможливо, *tout* > *t0*
1		0	1	1	x	Неможливо, *tout* > *t0*
1		1	0	0	1	Напад, можливо, напад червоточини
1		1	0	1	x	Не можливо, відповідь pkt не отримано
1		1	1	0	x	**Неможливо, якщо Δ >** *рекламувати відповідь* pkt ігнорується
1		1	1	1	x	**Неможливо, якщо Δ >** *рекламувати відповідь* pkt ігнорується

Запропонована система моделюється за допомогою OMNET++, який є потужним інструментом для створення імітаційної моделі мережевих систем. У таблиці 3.2 наведено параметри моделювання, які використовуються для оцінки продуктивності та ефективності запропонованого підходу. До основних параметрів відносяться енергетичні характеристики вузлів, такі як споживання енергії під час передачі, прийому та очікування, а також параметри зв’язку, що базуються на стандарті Wireless Hart.

Цей стандарт забезпечує низьке енергоспоживання, високу надійність зв’язку та передбачає використання технології частотного хопінгу для мінімізації перешкод. Крім того, у симуляції враховуються такі аспекти, як дальність передачі, рівень сигналу та затримка, які дозволяють оцінити реалістичність функціонування системи в умовах різних сценаріїв. Це дає змогу глибше проаналізувати вплив параметрів на загальну продуктивність та стабільність мережі.

Таблиця 3.2. Налаштування параметрів для моделювання

НД	Параметр	Цінність	Коментар
1	Розмір пакета	1500 *байтів*	Розмір пакета в байтах
2	Затримка процесу (*ρp*)	0.5 *сек*	Час, необхідний для обробки даних (секунди)
3	Розслідувати час (*tinvest)*	2 *сек*	Час IDS займає до наступного циклу розслідування
4	Тайм-аут пакета	0.5 *сек*	Кількість секунд, протягом яких пакет вважається втраченим
5	Напруга (*B*)	3.0 *B*	Напруга, що живить систему
6	холостий хід (*Ii*)	320 *мкА*	Вимоги до струму прослуховування бездротового холостого ходу Hart
7	Потужність передачі (*Itx*)	19.3 *мА*	Потужність бездротової передачі Харта
8	Потужність прийому (*Irx*)	21.5 *мА*	Живлення бездротового прийому Харта
9	Годинник MCU (f)	4.0 *МГц*	Процесор MCU працює в МГц
10	Шифрування /Дешифрування Cycle (*Ncrypto*)	7, 429 *циклів*	Використовуючи AES, тактові цикли, необхідні для en- Шифрування і дешифрування складають 6, 637 *циклів* і 7, 429 *циклів* відповідно. Макса обрали за найгірший сценарій
11	Струм MCU (*Irun*)	140 *мкА/МГц*	Необхідний струм під час обробки даних MCU
12	Струм сну MCU (*Isleep*	37 *мкА/МГц*	Необхідний струм під час сну MCU

У запропонованій системі обрано WirelessHART через його популярність у промислових застосунках, де він забезпечує високу надійність і стабільність

роботи мережі. Це особливо важливо в умовах, де необхідно підтримувати безперервність зв'язку і захист даних в складних промислових середовищах.

Для реалізації системи запобігання вторгненням (IPS) у цьому дослідженні було обрано AES (Advanced Encryption Standard) через його простоту впровадження та високий рівень безпеки для шифрування даних. AES є одним із найнадійніших і найбільш широко використовуваних стандартів шифрування, який гарантує конфіденційність і цілісність даних під час передачі. Цей стандарт є надзвичайно ефективним для захисту від атак типу MitM (Man-in-the-Middle), а також інших кіберзагроз, оскільки він забезпечує шифрування та захист даних від несанкціонованого доступу чи змін, що є критично важливим для забезпечення безпеки мережі.

На рисунку 3.4 (a) наведено графік затримки системи для трьох різних конфігурацій: з активованими вузлами IDS і шифруванням, без вузлів IDS, а також без шифрування. За результатами вимірювань середня затримка системи з розгорнутими вузлами IDS становить 2,6655 секунди. Для порівняння, середня затримка системи без IDS і шифрування дорівнює 2,6268 секунди. Це свідчить про те, що накладні витрати на затримку при розгортанні систем IDS та IPS складають 40 мілісекунд, що є прийнятним показником для забезпечення безпеки.

Додатково, на рисунку 3.4 (b) показано, скільки часу потрібно вузлам IDS для виявлення атак у системі.

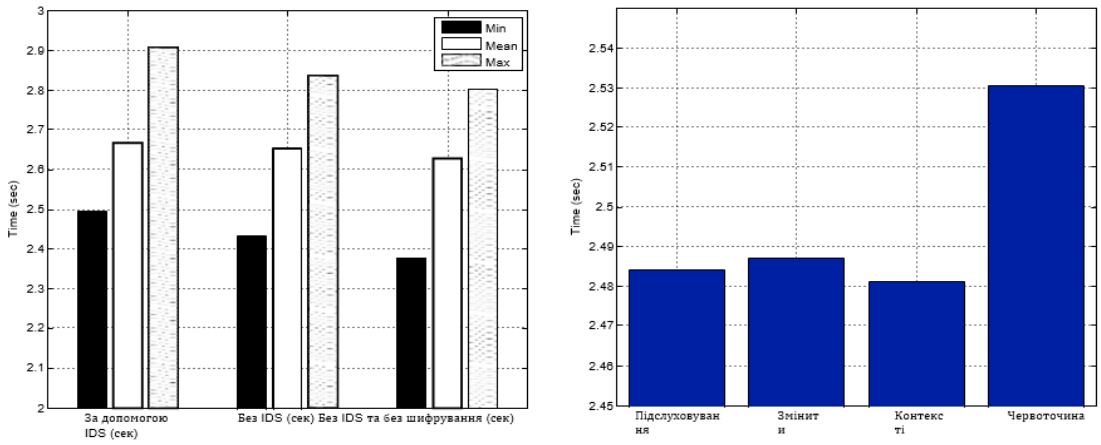


Рисунок 3.4. – Затримка сервісів та виявлення атак, де (a) затримка послуг у шарі туману, (б) тривалість туманй який виявляе атаку

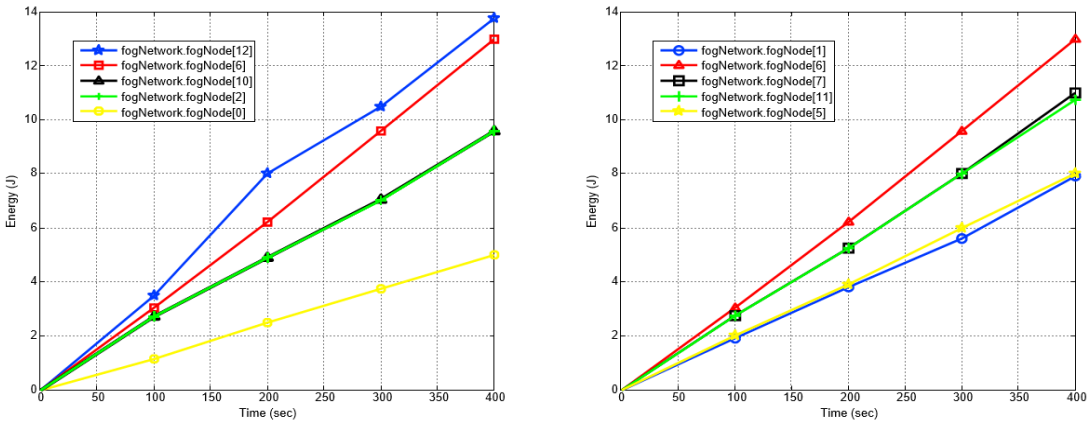
Маючи на увазі, що зонд вузла IDS вузлів через кожне t дослідження = 2.

Через 0 секунд після останнього сеансу розслідування (див. Таблицю 3.2, 3.3) можна побачити, що час, який проходить до виявлення нападу, варіюється від 2.4810сек до 2.5303сек. Час виявлення атаки Wormhole довший, оскільки вузли IDS повинні гарантувати, що відповідь на IDS-пакет не була затримана через шумне середовище.

На рисунку 3.4, також видно, що вузол IDS займає 2.5 секунд для виявлення атаки червоточини. Так як вузол IDS чекає тільки tinvestigate = 2.0 секунд між розслідуваннями, то фактичний час виявлення, тобто час, необхідний вузлу IDS для виявлення атаки з початку сеансу розслідування, дорівнює tdescovery 0.5 сек.

На рисунку 3.5 (a), (b) показано сукупне споживання енергії системою протягом 400 секунд моделювання. Вузли 0, 1, 2, 5, 6, 7, 10, 11 та 12 були обрані з мережі на рисунку 3.2. Видно, що енергія ІДС в обох випадках більше, ніж енергія ФНС. Це пов'язано з тим, що вузли IDS періодично досліджують кожен вузол на відстані однієї надії.

Отже, він має спілкуватися вісім разів, тоді як кожен ФН має спілкуватися один раз під час випробувань. Крім того, ФН здійснює менше восьми передач між слідчими засіданнями. Це означає, що в завантаженій мережі IDS буде споживати менше енергії, ніж FN, оскільки FN будуть спілкуватися між собою частіше, ніж з вузлами IDS.



а) енергія вузлів 0, 2, 10, 12 і 6. б) енергія вузлів 1, 7, 11, 5 і 6.

Рисунок 3.5. – Сукупне енергоспоживання деякого обраного вузла в запропонованій системі.

Реалізована система складається з двох типів вузлів: вузлів туману (FN) та -вузлів. Вузли туману (FN) надають послуги для пристроїв IoT нижнього рівня, забезпечуючи зменшену затримку у передачі даних. У процесі реалізації ці вузли отримують ключі шифрування з хмари, після чого ці ключі розподіляються серед вузлів туману.

Для забезпечення безпеки даних система використовує техніку симетричного шифрування на основі Advanced Encryption Standard (AES), що гарантує високий рівень захисту переданих даних. Для обміну ключами шифрування між вузлами використовується перевірений криптографічний метод — обмін ключами Діффі-Хелмана. Цей метод дозволяє ефективно забезпечити захист і конфіденційність обміну даними, навіть у відкритих мережах, що є критично важливим для захисту від атак типу MitM (Man-in-the-Middle) та інших загроз.

3.4. Збір інформації

Мережеві інтерфейси (NIC), що працюють згідно зі стандартом IEEE , підтримують шість основних режимів роботи, кожен з яких виконує специфічні функції в рамках бездротових мереж:

— у цьому режимі мережевий інтерфейс функціонує як точка доступу, забезпечуючи зв'язок і з'єднання для клієнтських пристроїв;

— мережевий інтерфейс працює як клієнт, підключаючись до наявних точок доступу;

– Ad Hoc — цей режим призначений для організації простих однорангових мереж без центральної точки доступу;

– Mesh — використовується для створення сітчастих топологій мережі, де вузли можуть безпосередньо підключатися один до одного;

– Repeater — забезпечує ретрансляцію сигналу Wi-Fi, що розширює зону покриття мережі;

– Monitor — дозволяє мережевому інтерфейсу перехоплювати всі пакети, що проходять через мережу, незалежно від їх призначення. Це робить режим Monitor ідеальним для збору і аналізу мережевого трафіку.

У Wi-Fi мережах пакети даних зазвичай передаються через точку доступу, але кожен пристрій отримує тільки ті дані, що призначені для його конкретної MAC-адреси. Пакети з іншими MAC-адресами ігноруються пристроєм.

Для моніторингу всіх переданих даних у мережі мережевий інтерфейс переводиться в режим Monitor, що дозволяє перехоплювати всі пакети, які проходять через мережу. Це робить режим Monitor ідеальним для аналізу і збору інформації про мережевий трафік.

Для реалізації атаки типу Man-in-the-Middle (MitM) у цьому дослідженні використовується спеціальний дистрибутив Linux — Backtrack 5R3, який надає всі необхідні інструменти для проведення експериментів та досліджень у сфері кібербезпеки.

Як продемонстровано на рисунку 3.6, кожна точка доступу у Wi-Fi-мережі вибирає свою унікальну MAC-адресу як BSSID. У прикладі, наведеному в роботі, ESSID цільової точки доступу має назву «Тестовий Wi-Fi». Додатково було встановлено, що два клієнти, з MAC-адресами BC:EE:7B:3E:FB:F7 і 00:21:27:DE:09:68, підключені до законної точки доступу з MAC-адресою 00:1F:9F:CF:7B:6D. Водночас, точка доступу працює на 6-му каналі, який використовується для передачі даних між клієнтами та мережею.

Цей детальний підхід дозволяє краще зрозуміти організацію мережі та взаємодію між її компонентами, а також забезпечує умови для проведення експериментів із забезпеченням або порушенням безпеки мережі. За допомогою моделювання можна тестувати різні сценарії атак і оцінювати ефективність запропонованих механізмів захисту, наприклад, виявлення та нейтралізації шкідливих вузлів або помилок у маршрутизації.

Крім того, це створює можливість оптимізації енергоспоживання вузлів і затримки передачі даних у мережах із реальними обмеженнями. Такий підхід

надає цінний інструментарій для досліджень у сфері безпеки та стабільності мережевих систем.

Рисунок 3.6. – Результати збору інформації.

Метою фальшивої точки доступу є підключення до законної мережі та використання цього з'єднання для обходу будь-яких заходів безпеки, які можуть бути впроваджені. Добре спроектована та впроваджена фальшива точка доступу здатна не залишати запасів для реагування механізмів вторгнення та запобігання, якщо атака організована та здійснюється зсередини мережі цілей.

Зловмисник може створити та встановити фальшиву точку доступу до мережі двома способами.

Протокол IEEE 802.11x підтримує функцію Repeater, яка дозволяє зловмисникам створювати фальшиві точки доступу для перехоплення даних. Це досить простий спосіб реалізації атаки, оскільки він не потребує складної настройки мережі. Однак цей метод має деякі обмеження:

– Обладнання — для такої атаки необхідно придбати відповідне обладнання, що може бути дорогим;

– Безпека мережі — багато мережевих адміністраторів відключають можливість підключення неавторизованих пристроїв до мережі, що знижує ймовірність успішної атаки, особливо в корпоративних мережах.

Тому цей підхід більше підходить для домашніх мереж або слабко захищених систем.

Більш ефективним і складнішим методом є створення програмної точки доступу, яка може бути реалізована за допомогою персонального комп'ютера з двома і більше мережевими інтерфейсами (NIC). У цьому випадку одна з карт підключається до легітимної мережі, а інша створює фальшиву точку доступу, забезпечуючи доступ до мережі через Wi-Fi або Ethernet. Хоча реалізація цього методу є складнішою з технічної точки зору, він є значно дешевшим, оскільки не потребує додаткового обладнання, а тільки відповідного програмного забезпечення.

Такий підхід дозволяє зловмисникові ефективно маніпулювати даними і здійснювати атаку типу Man-in-the-Middle (MitM), що дає йому змогу перехоплювати, змінювати або втручатися в мережевий трафік без значних витрат на обладнання.

Беручи до уваги вищезазначене, для відпрацювання в даній дисертації буде реалізований другий шлях. Фальшива точка доступу буде налаштована на трансляцію точно такого ж ESSID із законним, у цьому випадку «Test Wifi». На малюнку 3.7 показаний код і результат його виникнення.

Рисунок 3.7. – Код і результат фальшивого AP.

Як видно з малюнка 3.7 вище, фальшивий АП був створений за допомогою мішеней ESSID "Test Wifi". Він також працює в каналі «1» від NIC mon1. Разом із фальшивою точкою доступу було створено віртуальний інтерфейс "at0".

Цей віртуальний інтерфейс буде використовуватися пізніше для підключення підробленої точки доступу до Інтернету. Виконання етапу збору інформації ще раз відкриє корисну інформацію.

Як показано на рисунку 3.8, підроблений АП має такий же ESSID і робочий канал, як і легітимний. Однак у результатах є два винятки. Фальшива точка доступу має інший BSSID, а саме MAC-адресу, а потужність передачі нижча, ніж законна потужність передачі. Однак підміна MAC-адреси законної точки доступу – це дія, яку буде виконано на наступних кроках. Крім того, фальшиву точку доступу можна налаштувати для підтримки механізмів безпеки, таких як WEP і WPA/WPA2, але оскільки цільова точка доступу не має реалізованого механізму безпеки, ця дія вважається непотрібною.

З моменту створення фальшивої точки доступу і вона знаходиться в робочому стані, зловмисник чекає, поки клієнти підключаться до неї. Пристрої Wi-Fi мають механізм, який дозволяє вибирати свою Wi-Fi мережу автоматично. Коли пристрій Wi-Fi увімкнено, він починає видавати запити датчика, щоб виявити будь-яку з бездротових мереж, які були підключені в минулому. Всі ці мережі зберігаються в PNL (списку бажаних мереж). Пристрій Wi-Fi спочатку виконає пошук за найбільш використовуваним ESSID, а потім продовжить це робити, доки список не буде охоплено.

На рисунку 3.8 показані запити зонда, які передаються від клієнта з MAC-адресою 2C:D0:5A:55:8D:FF. Перехоплюючи ці запити зонда, які не зашифровані, зловмисник може витягнути багато корисної інформації про клієнта. На малюнку

3.6 клієнт з MAC-адресою 2C:D0:5A:55:8D:FF раніше був підключений до двох інших мереж з ESSID "HK1" і "Thomson1C73EC" разом з "Test Wifi".

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	00:21:27:DE:09:65	-57	0 - 1	18	56	
(not associated)	18:86:AC:EF:74:CC	-68	0 - 1	0	2	
(not associated)	BC:EE:7B:3E:FB:F7	-35	0 - 1	0	38	
(not associated)	2C:D0:5A:55:8D:FF	-28	1 - 1	82	40	HK1,Thomson1C73EC,Test Wifi

Рисунок 3.8. – Запит зондування.

У даному досліджені реалізації атаки MITM було використано спеціальний дистрибутив Linux, який отримав назву Backtrack 5R3. Для того, щоб NIC був

переведений в режим моніторингу, використовувалась команда airmon-ng, а для початку збору інформації була використаная команда airmon-ng.

3.5. Висновки

У цьому розділі було проаналізовано можливості використання систем виявлення вторгнень (IDS) та систем запобігання вторгнень (IPS) для боротьби з атаками типу Man in the Middle (MitM), зокрема через застосування спеціальних вузлів IDS. В якості основного механізму для системи IPS був обраний алгоритм шифрування AES з розміром ключа та блоку 128 біт, що забезпечує високий рівень безпеки при мінімальних витратах на ресурси. Це дозволяє ефективно захищати мережу від атак, гарантуючи шифрування даних.

Для зменшення затримки системи було інтегровано вузли IDS, які виконують регулярне опитування туманних вузлів (FN), розташованих на відстані одного стрибка. Ці вузли IDS аналізують реакції на запити, оцінюючи час доставки пакетів, контекст отриманих відповідей і вміст переданих даних. Такий підхід дозволяє швидко виявляти скомпрометовані вузли або інші аномалії в мережі.

Затримка, пов'язана з використанням системи IDS-IPS, складає 40 мс, що є досить низьким показником. Однак це досягається за рахунок обмежень часу, необхідного для розслідування. Цей час прямо пропорційний затримці мережі, а також залежить від енергетичних витрат, пов’язаних із роботою вузлів IDS. Тому дуже важливо оптимально налаштувати час розслідування в IDS для забезпечення мінімальної затримки та енергоефективності в туманному шарі.

Враховуючи ці фактори, у майбутніх розробках передбачається перехід до динамічного налаштування параметра затримки (t0), що дозволить адаптувати систему до змін у характеристиках мережі, наприклад, у бездротових мережах, де затримки можуть бути більш непередбачуваними.

4 ДОСЛІДЖЕННЯ ТА ЕКСПЕРИМЕНТИ АТАКИ «ЛЮДИНА ПОСЕРЕДИНІ» В БЕЗДРОТОВИХ МЕРЕЖАХ

В даній роботі розглядається проблема атак типу Man-in-the-Middle (MITM) в бездротових мережах, де зловмисник використовує фальшиву точку доступу для обману клієнтів, перехоплюючи їхній трафік. Метою роботи є виявлення та запобігання таким атакам, створення фальшивої точки доступу для імітації законної та проведення атаки "відмова в обслуговуванні" (DoS) для вибивання клієнтів із їхньої точки доступу, що примушує їх підключатися до фальшивої точки доступу. Після успішної атаки трафік клієнтів перехоплюється, щоб отримати доступ до їхньої особистої інформації.

Етапи реалізації:

– Створення фальшивої точки доступу (AP): Для проведення атаки MITM створюється точка доступу, яка імітує характеристики законної, що дозволяє обманути користувачів і змусити їх підключитися до фальшивого пристрою;

– Атака DoS на законну точку доступу: Це здійснюється для того, щоб змусити клієнтів відключитися від справжньої точки доступу та підключитися до фальшивої. Така атака може бути здійснена за допомогою спеціалізованих інструментів, що порушують з’єднання між клієнтами та їхньою точкою доступу;

– Перехоплення трафіку: Після того як клієнти підключаються до фальшивої точки доступу, трафік між ними та мережею перехоплюється. Зловмисник може використовувати цей доступ для збирання чутливої інформації, такої як логіни, паролі та інші персональні дані.

Виявлення та запобігання атакам MITM: Для захисту від таких атак буде розроблена система, що використовує базу даних законних точок доступу. Система буде здійснювати сканування мережі на наявність фальшивих точок доступу, порівнюючи їх з уже відомими в базі даних. Якщо система виявить точку доступу, яка не відповідає жодній з законних точок, вона автоматично заблокує її, забороняючи її підключення клієнтам. Це дозволить знизити ймовірність успішної атаки MITM.

Технічна реалізація:

– Інструменти: Для проведення експериментів були використані дистрибутиви Backtrack 5R3 та Kali Linux, які містять необхідні утиліти для аналізу мережі та проведення атак;

– Мова програмування: Для розробки системи виявлення та запобігання атак була обрана мова Python. Вона дозволяє створити ефективне рішення для автоматичного сканування точок доступу та їх верифікації.

4.1. Збір даних та підготовка до реалізації експерименту

Для того, щоб реалізувати успішний MITM, деякі дії повинні бути прикриті з боку зловмисників. Ці дії поділяються на 4 етапи, як це видно на рисунок 4.1 нижче. Перший етап атаки – збір інформації. Зловмисник зосереджується на зборі корисної інформації щодо цільової точки доступу. Коли цей етап буде завершено, почнеться другий етап – налаштування підробленого AP.

Використовуючи інформацію з попереднього етапу, підроблений AP повинен мати ті ж характеристики, що й цільовий AP. Такі характеристики, як ESSID і канал, повинні бути ідентичними. Крім того, фальшива точка доступу повинна підключатися до Інтернету, щоб переконати клієнтів у своїй законності та захопити більше трафіку.

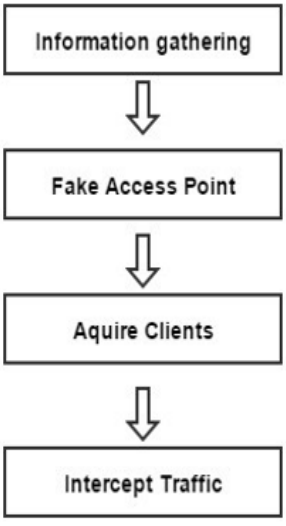


Рисунок 4.1. – Процедура атаки «Людина посередині»

Перших двох етапів достатньо, щоб налаштувати фальшиву точку доступу та виконати атаку MITM. Але для того, щоб отримати хороші результати, фальшива точка доступу повинна зібрати достатню кількість клієнтів.

Це можна зробити двома методами, і ці методи складають третій етап.

У першому способі зловмисник просто чекає, коли клієнт випадково підключиться до фальшивої точки доступу і почне захоплювати його трафік. Цей спосіб не вимагає ніякої активності з боку нападника, але такий підхід не є ефективним.

У другому способі зловмисник може провести серію різних атак на користувачів або на законну точку доступу, щоб заглушити з'єднання між ними. Це змусить клієнтів, які підключені до законної точки доступу перепідключитись до фальшивої. Нарешті, останнім етапом є перехоплення трафіку, який спрямовується через фальшиву точку доступу.

Мережеві інтерфейси (NIC), які працюють під егідою IEEE 802.11x, мають шість режимів роботи. Це режими Master, Managed, Ad Hoc, Mesh, Repeater і Monitor. У режимі Master NIC діє як точка доступу, а в керованому режимі NIC діє як клієнт для точки доступу. Режими ad hoc та Mesh призначені для мереж без точок доступу та сітки відповідно , а режим ретранслятора повторно передає сигнал Wi-Fi.

У мережі Wi-Fi пакети передаються точкою доступу, що означає, що всі клієнти в зоні досяжності можуть отримувати цю трансляцію, але дані доставляються кожному клієнту на основі MAC-адреси призначення . Решта переданих даних, якщо призначення MAC-адреси відрізняється, ігноруються клієнтами. Для того, щоб контролювати всі передані дані, NIC повинен бути переведений в режим Monitor. У цьому режимі NIC здатний захоплювати всі дані незалежно від їх цільової MAC-адреси, що робить цей режим ідеальним для збору інформації .

У даній роботі для реалізації атаки MITM буде використовуватися спеціальний дистрибутив Linux, який отримав назву Backtrack 5R3. Для того, щоб

NIC був переведений в режим моніторингу, буде використовуватися команда airmon-ng, а для початку збору інформації буде використовуватися команда airmon-ng.

Рисунок 4.2 ілюструє результати, що відбулися під час розвідки.

Як видно з рисунка 4.2, кожна точка доступу вибирає свою MAC-адресу як свій BSSID, а ESSID цільової точки доступу - це «Тестовий Wi-Fi».

Додатково два клієнти, з MAC адреси BC:EE:7B:3E:FB:F7 і 00:21:27:DE:09:68, підключені до законної точки доступу з MAC-адресою 00:1F:9F:CF:7B:6D і каналом, на якому транслюється точка доступу, є 6.

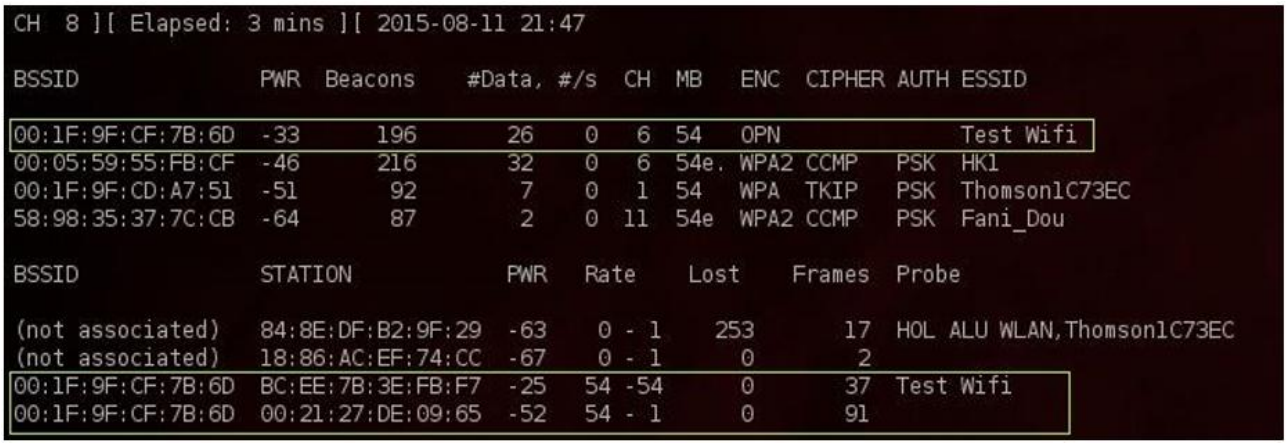


Рисунок 4.2. – Результати збору інформації

Фальшива точка доступу створюється для підключення до законної мережі, що дає змогу зловмисникові обійти заходи безпеки, які можуть бути впроваджені. Якщо така точка доступу спроектована і налаштована правильно, вона може бути дуже ефективною, що ускладнює виявлення атаки системами виявлення чи запобігання вторгненням, особливо коли атака проводиться зсередини цільової мережі. Зловмисник може створити фальшиву точку доступу та підключити її до мережі двома основними способами.

Протокол IEEE 802.11x підтримує функцію Repeater, що дозволяє зловмисникові встановити додаткову точку доступу в мережі для перехоплення даних. Цей метод реалізується досить просто з технічної точки зору, оскільки не

вимагає складної настройки. Однак він має високий ризик, оскільки потребує спеціального обладнання, що може бути дорогим для зловмисника.

Багато мережевих адміністраторів відключили можливість для неавторизованих користувачів додавати свої мережеві пристрої, тому ця атака найчастіше може бути спрямована на слабші цілі, такі як домашні мережі.

Більш ефективним підходом є створення програмної точки доступу, яка підключається до законної мережі через Wi-Fi або Ethernet. Хоча це більш складно з технічної точки зору, цей метод є дешевшим, оскільки для його реалізації достатньо мати персональний комп'ютер з двома або більше мережевими інтерфейсами та відповідне програмне забезпечення.

У даній роботі буде використано саме цей метод. Фальшива точка доступу буде налаштована таким чином, щоб транслювати той самий ESSID, що й законна точка доступу — в даному випадку «Test Wifi». Рисунок 4.3 демонструє код та результат його виконання.

Рисунок 4.3. – Код і результат фальшивого AP

Як видно з рисунка 4.3 вище, фальшивий АП був створений за допомогою мішеней ESSID "Test Wifi". Він також працює в каналі «1» від NIC mon1. Разом із фальшивою точкою доступу було створено віртуальний інтерфейс "at0". Цей віртуальний інтерфейс буде використовуватися пізніше для підключення підробленої точки доступу до Інтернету. Виконання етапу збору інформації ще раз відкриє корисну інформацію.

Як показано на рисунку 4.4, підроблений АП має такий же ESSID і робочий канал, як і легітимний. Однак у результатах є два винятки.

Фальшива точка доступу має інший BSSID, а саме MAC-адресу, а потужність передачі нижча, ніж законна потужність передачі. Однак підміна

MAC-адреси законної точки доступу – це дія, яку буде виконано на наступних кроках.

Крім того, фальшиву точку доступу можна налаштувати для підтримки механізмів безпеки, таких як WEP і WPA/WPA2, але оскільки цільова точка доступу не має реалізованого механізму безпеки, ця дія вважається непотрібною.

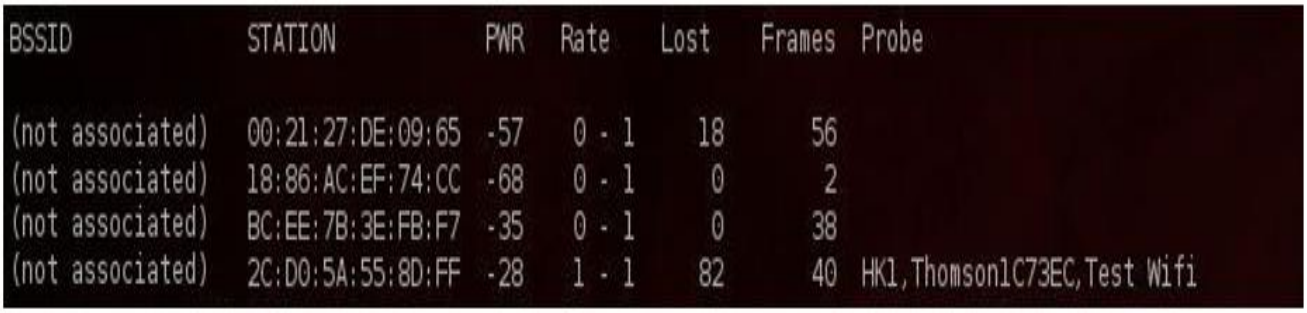
Рисунок 4.4. – Нові результати збору інформації.

Як показано на рисунку 4.4, підроблений АП має такий же ESSID і робочий канал, як і легітимний. Однак у результатах є два винятки. Фальшива точка доступу має інший BSSID, а саме MAC-адресу, а потужність передачі нижча, ніж законна потужність передачі. Однак підміна MAC-адреси законної точки доступу – це дія, яку буде виконано на наступних кроках. Крім того, фальшиву точку доступу можна налаштувати для підтримки механізмів безпеки, таких як WEP і WPA/WPA2, але оскільки цільова точка доступу не має реалізованого механізму безпеки, ця дія вважається непотрібною.

З моменту створення фальшивої точки доступу і вона знаходиться в робочому стані, зловмисник чекає, поки клієнти підключаться до неї. Пристрої Wi-Fi мають механізм, який дозволяє вибирати свою Wi-Fi мережу автоматично. Коли пристрій Wi-Fi увімкнено, він починає видавати запити датчика, щоб виявити будь-яку з бездротових мереж, які були підключені в минулому. Всі ці мережі зберігаються в PNL (списку бажаних мереж). Пристрій Wi-Fi спочатку виконає пошук за найбільш використовуваним ESSID, а потім продовжить це робити, доки список не буде охоплено.

На рисунку 4.5 показані запити зонда, які передаються від клієнта з MAC-адресою 2C:D0:5A:55:8D:FF.

Перехоплюючи ці запити зонда, які не зашифровані, зловмисник може витягнути багато корисної інформації про клієнта.



BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	00:21:27:DE:09:65	-57	0 - 1	18	56	
(not associated)	18:86:AC:EF:74:CC	-68	0 - 1	0	2	
(not associated)	BC:EE:7B:3E:FB:F7	-35	0 - 1	0	38	
(not associated)	2C:D0:5A:55:8D:FF	-28	1 - 1	82	40	HK1,Thomson1C73EC,Test Wifi

Рисунок 4.5. – Запити зондування.

Просто створення фальшивої точки доступу недостатньо для успішного виконання атаки MITM. Навіть користувачі без глибоких знань в мережевих технологіях можуть зрозуміти, що з'єднання з підробленою точкою доступу є ненадійним, що може призвести до їх відключення через відсутність доступу до Інтернету.

Тому для ефективності атаки фальшива точка доступу повинна бути підключена до джерела Інтернету. Це дозволить їй забезпечити своїх клієнтів необхідним підключенням, одночасно відкриваючи можливість для перехоплення більш конфіденційних даних. Існують два основні методи для забезпечення підключення до Інтернету через фальшиву точку доступу: використання мостової точки доступу та маршрутизованої точки доступу.

4.2. Проведення експериментів

На рисунку 4.6, представлений огляд конструкції алгоритму, виражений за допомогою блок-схеми. Далі буде більш детально проаналізовано алгоритми та функції, які будуть написані. Система працює в середовищі Linux через термінал, без підтримки графічного інтерфейсу користувача (GUI) і виконується з використанням мови програмування Python.

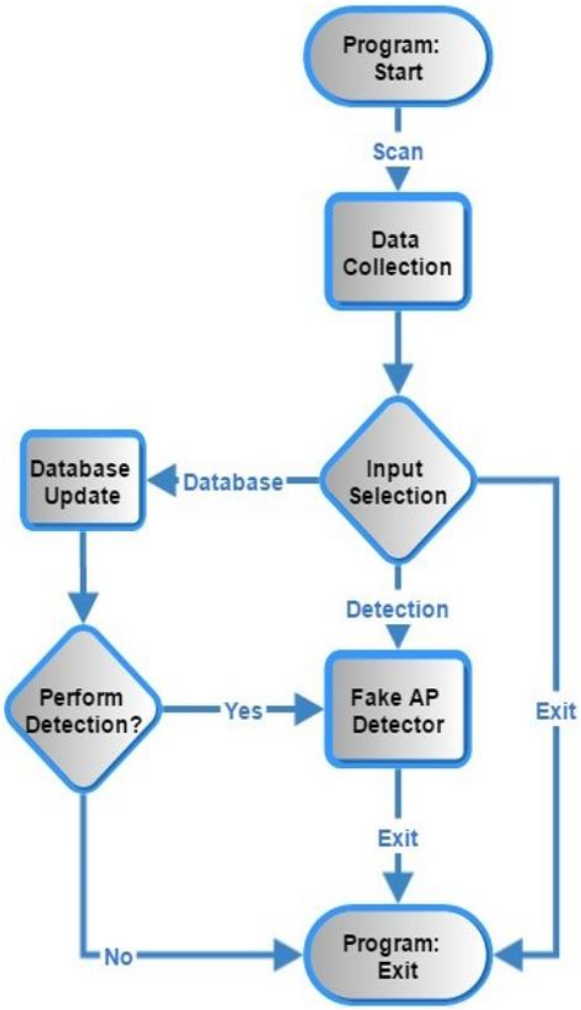


Рисунок 4.6. – Загальна блок-схема механізму, який зможе виявляти та активно запобігати нападу «Людина посередині».

Програма складається з трьох основних модулів: Збір даних, Оновлення бази даних та Fake AP detector. Система має можливість бути зупиненою або через пряме втручання користувача, або після завершення запитуваних операцій. Вона надає можливість виявлення фальшивої точки доступу на основі попередньо збереженого списку захисту або оновленої бази даних, а також здійснення операцій без виявлення, якщо вибрано лише оновлення бази даних.

У системі реалізовано всі функції, необхідні для виявлення та запобігання атакам MITM, як описано в попередніх розділах. Модулі розроблені на Python у середовищі Linux, що дозволяє ефективно обробляти запити та виконувати операції. Структура реалізації відповідає проекту, описаному раніше.

Для кращого розуміння процесу будуть надані фрагменти коду для кожного модуля із поясненнями, що допоможуть зрозуміти, як працює кожен етап програми. Кожен блок коду буде супроводжуватися роз'ясненнями, щоб пояснити його функціональність та роль у загальній системі.

Першим етапом роботи програми є ініціалізація або створення бази даних, у якій будуть зберігатися всі відомості про фальшиві точки доступу. Це критично важливо для коректної роботи детекторів, оскільки здатність виявляти фальшиві точки залежить від наявних у базі даних даних. Якщо база даних не активна, система лише спостерігає за навколишніми точками доступу, без здатності реагувати на атаки.

Для створення та налаштування бази даних використовується сервер MySQL. Він налаштований за допомогою стандартних параметрів (ім’я користувача, пароль та IP-адреса хоста), що спрощує підключення до бази. Підключення здійснюється через модуль MySQLdb.connect на Python, який після встановлення з'єднання передає його в об'єкт dbconnection.

Подальша взаємодія з базою даних здійснюється через курсор, який є ключовим елементом для виконання SQL-команд. Курсор прив'язується до активного з'єднання з базою даних, що забезпечує стабільне та безперервне виконання запитів протягом всього часу роботи програми. Це дозволяє системі ефективно управляти транзакціями, обробляти великі обсяги даних та забезпечувати узгодженість операцій.

За допомогою курсора можна виконувати різноманітні операції, такі як вибірка даних, вставка, оновлення або видалення записів у базі. Крім того, курсор підтримує покрокове проходження по записах, що є особливо корисним для складних операцій аналізу чи обробки даних. Завдяки інтеграції курсора з логікою програми, можна динамічно генерувати SQL-запити та обробляти результати в реальному часі, адаптуючи їх до потреб користувача чи системи.

Важливо, що правильне закриття курсора після виконання всіх необхідних операцій гарантує звільнення ресурсів та запобігання витокам пам’яті, що є критичним для стабільної роботи багатокористувацьких систем. Таким чином,

курсор відіграє фундаментальну роль у забезпеченні ефективності та надійності роботи програм, які використовують бази даних, створюючи основу для подальших етапів аналізу, обробки та зберігання інформації.

```
# Preparation of MySQL database
try:
    try:
# Connecting to MySQL server using default username and password and host IP address
  db_connection = MySQLdb.connect(host='127.0.0.1', user="", passwd="")
  print "Connection MySQL successful\n"
    except:
  print "Wrong username/password or MySQL Server is down\n"
  sys.exit(2)

    handler = db_connection.cursor()

# Creation of the database MITMDB
    comand = "show databases like 'MITMDB'"
    handler.execute(comand)
    if handler.rowcount <= 0:
      comand = 'CREATE DATABASE IF NOT EXISTS MITMDB'
      handler.execute(comand)

# Usage of the database MITMDB
    comand = 'USE MITMDB'
    handler.execute(comand)

# Load or Create the table where the APs metrics will be stored based on the SSID
    comand = "show tables like 'ssidtables'"
    handler.execute(comand)
    if handler.rowcount <= 0:
  comand = '''CREATE TABLE IF NOT EXISTS ssidtables (
      id MEDIUMINT NOT NULL AUTO_INCREMENT, PRIMARY KEY (id), mac TEXT, ssid TEXT, Txpower INTEGER, channel NUMERIC, Code TEXT, Encryption TEXT, Authentication TEXT)
      '''
  handler.execute(comand)

# Load or Create the table with the AP protection list
    comand = "show tables like 'protectionlist'"
    handler.execute(comand)
    if handler.rowcount <= 0:
  comand = '''CREATE TABLE IF NOT EXISTS protectionlist (
      id MEDIUMINT NOT NULL AUTO_INCREMENT, PRIMARY KEY (id), mac TEXT, ssid TEXT, min_Txpower INTEGER, max_Txpower INTEGER, channel NUMERIC, Code TEXT, Encryption TEXT, Authentication TEXT)
```

Рисунок 4.8 – Створення баз даних

```
39          '''
40      handler.execute(comand)
41
42  # Load or Create the table where the De-authentication attributes are
        stored
43      comand = "show tables like 'atributes'"
44      handler.execute(comand)
45      if handler.rowcount <= 0:
46      comand = '''CREATE TABLE IF NOT EXISTS atributes (
47          option_indic varchar(255), option_variable varchar(255))
48          '''
49      handler.execute(comand)
50
51  # Empties the table ssidtables
52      comand = 'Truncate table ssidtables'
53      handler.execute(comand)
54  except:
55      print "Error in MySQL\n"
56      sys.exit(2)
```

Рисунок 4.8 – Створення баз даних.

При створенні бази даних і її таблиць програма автоматично ініціалізує кілька значень за замовчуванням, які потім будуть використані в механізмі деаутентифікації для коректної роботи. Як уже зазначалося, для правильного функціонування механізму деаутентифікації необхідні два ключові параметри: тривалість атаки деаутентифікації та кількість її повторів.

Значення за замовчуванням для тривалості атаки деаутентифікації встановлено на нуль секунд, що означає, що атака триватиме лише миттєво, якщо інші параметри не будуть задані. Кількість повторів атаки за замовчуванням дорівнює одному, тобто атака буде виконуватися лише один раз. У випадку, якщо база даних вже містить збережені параметри, програма автоматично завантажить ці значення з бази даних, замінюючи параметри за замовчуванням. Це дозволяє зберігати налаштування між сесіями та робить налаштування програми зручнішими для подальших запусків.

```
#Deauthentication Initialisation Options
try:

# Set de-authentication duration
  comand = "select option_variable from atributes where option_indic = '
    deauth_time'"
  handler.execute(comand)
  if handler.rowcount <= 0:
      comand = "insert into atributes values('deauth_time','0')"
      handler.execute(comand)

# Set de-authentication repetitions
  comand = "select option_variable from atributes where option_indic = '
    deauth_repeat'"
```

Рисунок 4.9 – Ініціалізація параметрів деаутентифікації.

```
  handler.execute(comand)
  if handler.rowcount <= 0:
      comand = "insert into atributes values('deauth_repeat','1')"
      handler.execute(comand)
except:
  print "Error in Class 'InitialDeauthOptions'\n"
```

Рисунок 4.10 – Ініціалізація параметрів деаутентифікації.

Програма повинна перевести бездротовий мережевий інтерфейс (NIC) в режим моніторингу для збору інформації про навколишні точки доступу. Спочатку програма перевіряє наявність підключеного NIC за допомогою підпроцесу Popen, що дає можливість запускати нові процеси, взаємодіяти з їхніми вихідними каналами та отримувати результат виконання.

Підпроцес Popen використовує модуль communication, який відповідає за зчитування вихідних даних через PIPE. Зібрані дані передаються на стандартний вивід дочірнього процесу.

Для перевірки наявності бездротового NIC виконується команда iwconfig, яка надає інформацію про всі бездротові мережеві карти системи Linux. Після цього, за допомогою тієї ж технології запуску підпроцесів, викликається

інструмент airmon-ng, який входить до складу пакету для аудиту безпеки. Цей інструмент дозволяє перевести NIC в режим моніторингу.

Програма перевіряє, чи успішно змінений режим на моніторинг. Якщо один із підпроцесів не вдається запустити або виникає помилка при виконанні, програма припиняє свою роботу і завершує зв'язок з базою даних через клас

```
# Preparing Monitor Interface
try:
    out = Popen("iwconfig", stdout=PIPE).communicate()[0]
    wifi_iface = ""
    mon_nic = ""
    if "wlan" in out:
  wifi_iface = out[0:6].strip()
    else:
  print "\n\nNo wireless NIC present!!\n"
  print "Please connect a wireless NIC and try again"
  Termination("DATABASE")
  sys.exit(2)

# Check if mon interface is not disabled
    airmon_data = Popen("airmon-ng", stdout=PIPE).communicate()[0]
    if 'mon' in airmon_data:
```

Рисунок 4.11 – Ініціалізація параметрів деаутентифікації.

```
  print "\n\nMonitor mode on wireless NIC detected."
  print "Please deactivate monitor mode on wireless NIC and try again\n"
  Termination("DATABASE")
  sys.exit(2)
except:
  print "Error in Preparing Monitor Interface\n"
```

Рисунок 4.12 – Ініціалізація параметрів деаутентифікації.

При успішному завершенні попередніх підмодулів модуль ініціює створення режиму Монітора для бездротового NIC. Підмодуль активує та

деактивує бездротовий NIC за допомогою модуля os.system для виклику команди ifconfig.

Після цього бездротовий NIC переходить у режим монітора за допомогою інструменту airmon, і результати передаються moninface дитині. Використовуючи цей дочірній елемент, аутпут чергується з непотрібних символів для отримання імені інтерфейсу monito.

Нарешті, модуль виконує перевірку деяких можливих програм, які можуть порушити роботу системи, і припиняє їх роботу за допомогою модуля os.system.

```
# Creating Monitor Interface
try:

# Shut dwon and reactivate wireless NIC
    print "Setting up wireless NIC: " + wifi_iface + "\n"
    os.system('ifconfig ' + wifi_iface + ' down')
    os.system('ifconfig ' + wifi_iface + ' up')

    print "Active wireless NIC: " + wifi_iface + "\n"

# Enable Monitor mode
    print 'Enabling Monitor mode'
    wireless_nic = Popen(["airmon-ng", "start", wifi_iface], stdout=PIPE).
    communicate()[0]

# Deleted the unnecessary characters from the output
    if 'mon' in wireless_nic:
      print wireless_nic[-33:-1].strip()
      mon_nic = wireless_nic[-7:-2].strip(")")

# Terminate harmful services
    if 'NetworkManager' in wireless_nic:
  print "\n Terminating 'NetworkManager'"
  os.system("service network-manager stop")
    if 'wpa_supplicant' in wireless_nic:
  print "\n Terminating 'wpa_supplicant'"
  os.system("pkill wpa_supplicant")
```

Рисунок 4.13 – Створення інтерфейсу Monitor

До того моменту, коли бездротовий мережевий адаптер перейде в режим монітора, модуль буде готовий ініціювати сканування. Інструментом, який використовується для сканування найближчих точок доступу, є airodump-ng, але оскільки він за замовчуванням має деякі файли збереження, підмодуль видаляє їх.

Інструмент запускається за допомогою Popen, згаданого раніше, і тимчасово зберігає результати сканування у файлі csv. Результат процесу передається дитині-аіродумпу.

Завершуючи сканування, модуль створює порожній словник результатівAPs, де будуть зберігатися відсканованні результати. Для фільтрації результатів система використовувала програму Scapy. Scapy — це програма маніпулювання пакетами, деякі з її модулів якої дозволяють користувачеві захоплювати, підробляти та витягувати інформацію з мережевих кадрів, дротових або бездротових. Дуже важливим модулем цієї програми є модуль sniff, який дозволяє програмі витягувати значення для виконання необхідної фільтрації.

```
# Remove the old output from airodump
try:
    os.system('rm out.csv-01.*')
except:
  print "Error deleting Airodump csv file\n"

# Scanning for available SSIDs
print "SCANNING FOR ACTIVE Wi-Fi NETWORKS"
print "\n\n"
try:

#Scan and save results
    airodump = Popen(["airodump-ng", "--output-format", "csv",  "-w", "out.
    csv", mon_nic])

    resultAPs = {}

#Sniff values from scanned data
    sniff(iface=mon_nic, prn=ap_discovery, count=20, store=False, lfilter=
    lambda p: (Dot11Beacon in p or Dot11ProbeResp in p))

    airodump.terminate()
    db_connection.commit()
except:
  print "Error in available SSIDs\n"
```

Рисунок 4.14 – Сканування та збір даних і фільтрація

Параметри модуля сніффа такі:

– iface: У цьому полі зберігається інтерфейс монітора

– prn: У цьому полі зберігаються результати виконання функцій класу ap-discovery

– count: Скільки результатів має обробляти модуль Sniff

– store: Якщо результати мають зберігатися на постійній основі

– lfilter: Виконайте фільтрацію та передайте результати відповідно до налаштувань

Для вказівки Scapy, які саме мережеві кадри потрібні для роботи системи, використовуються функції Dot11Beacon та Dot11ProbeResp. Ці функції фільтрують і зберігають тільки кадри маяків та запитів зонду, що надсилаються точками доступу, оскільки вони містять усю необхідну інформацію для подальшої обробки.

Операція фільтрації здійснюється за допомогою анонімних функцій lambda мови Python, які дозволяють проводити обробку без прив'язки до імені. Це дозволяє ефективно фільтрувати та обробляти дані, які відповідають заданим критеріям.

Після завершення процесу сканування результати фільтруються для отримання інформації про точки доступу. Викликається клас ap-discovery, і за допомогою Scapy проводиться обробка отриманих даних. Адресу BSSID точки доступу можна знайти в третьому полі захоплених кадрів, а результат передається у змінну bssid. Для витягнення SSID з кадрів використовується функція Dot11Elt, після чого значення SSID зберігається у словнику resultAPs.

```
1
2 # Parsing Scapy parameters
3 def ap_discovery(packet):
4     try:
5
6 # Search the frame's third address to find the BSSID
7    bssid = packet[Dot11].addr3
8    if bssid in resultAPs:
9        return
10   p = packet[Dot11Elt]
11   cap = packet.sprintf("{Dot11Beacon:%Dot11Beacon.cap%}"
```

Рисунок 4.15 – Підмодуль виявлення BSSID і SSID

```
12          "{Dot11ProbeResp:%Dot11ProbeResp.cap%}").split('+')
13
14    ssid = None
15
16 # Search the frame to find the SSID
17    while isinstance(p, Dot11Elt):
18        if p.ID == 0:
19      ssid = p.info
20        p = p.payload
21
22 # Store the SSID
23    resultAPs[bssid] = (ssid)
24      except:
25    print "Error in Class 'ap_discovery'\n"
```

Рисунок 4.16 – Підмодуль виявлення BSSID і SSID.

Після того, як ідентифікатори SSID та BSSID отримано з кадрів маяків, модуль переходить до наступного етапу обробки — розбору CSV-файлу. Цей етап є критичним для систематизації та збереження виміряних показників, отриманих під час сканування. Дані з файлу CSV використовуються для оцінки стану мережі, якості сигналу та ідентифікації доступних точок доступу.

Процес розбору починається з відкриття CSV-файлу за допомогою функції open мови Python. Після відкриття файлу підмодуль застосовує спеціалізовані інструменти для читання його вмісту. Як тільки дані оброблено, підмодуль зберігає їх у базі даних. Цей процес включає передачу та валідацію даних перед записом, що забезпечує їхню цілісність і достовірність.

Збережена інформація потім може бути використана для побудови детальних карт покриття мережі, що дозволяє візуалізувати зони сильного і слабкого сигналу. Це дає змогу ідентифікувати найбільш ефективні точки доступу, оптимізувати їх розташування та забезпечити рівномірне покриття для всіх користувачів. Крім того, ці дані можуть слугувати основою для виконання складніших аналітичних завдань, таких як прогнозування перевантаження в мережі, адаптація параметрів

роботи вузлів у реальному часі або підвищення стійкості системи до можливих збоїв і атак. Такий підхід сприяє не лише підвищенню ефективності роботи системи, але й забезпечує гнучкість для подальшого масштабування мережі.

```
1
2 # Parsing the airodump-ng output
3 def CsvParse():
4     try:
5
6     # Opens the csv output file from airodump-ng
7   f = open('out.csv-01.csv', 'rb')
8   try:
9
10      # Reader object is created and zeros are replaced with "null"
11      reader = csv.reader(x.replace('\0', '') for x in f)
12
13    # The rows of the file are checked again and placed in order
14      for row in reader:
15    if 'BSSID' in row:
16        continue
17    if 'Station MAC' in row:
18        break
19    if len(row) < 1:
20        continue
21    # The parsed results are stored into the database
```

Рисунок 4.17 – Розбір вихідних даних Airodump-ng csv

```
22    comand = "insert into ssidtables (mac,ssid,Txpower,channel,Code,
      Encryption,Authentication) values(%s,%s,%s,%s,%s,%s,%s)"
23    handler.execute(comand, (row[0].strip(), row[13].strip(), row[8].strip
      (), row[3].strip(), row[6].strip(), row[5].strip(), row[7].strip()))
24      db_connection.commit()
25
26     # Sub-module terminated
27  finally:
28      f.close()
29    except:
30  print "Error in Class 'CsvParse'\n"
```

Рисунок 4.18 – Розбір вихідних даних Airodump-ng csv

Тестова установка в цьому експерименті спробує емулювати реальне середовище з декількома точками доступу, яке зазвичай зустрічається в громадських місцях.

Було вирішено покрити площу 90 м2 за допомогою одного SSID без будь-якого захисту, щоб зробити тест максимально наближеним до реальних сценаріїв. Місце, де буде проходити експеримент, зображено на малюнку 4.7.

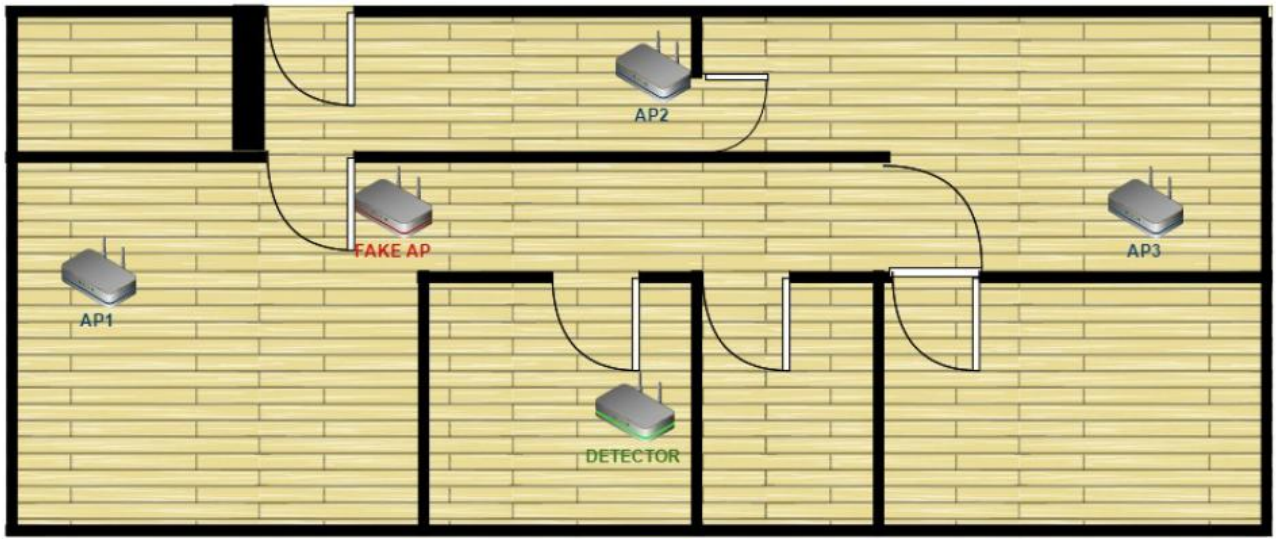


Рисунок 4.19. – Огляд тесту налаштованого з усіма учасниками.

Тестова установка складається з п’яти учасників: трьох законних точок доступу (AP1, AP2, AP3), фальшивої точки доступу та детектора. Всі точки доступу працюють на одному SSID за протоколом 802.11g, на одинадцятому каналі в діапазоні 2,4 ГГц, з максимальною потужністю передачі. Ці точки доступу покривають всю територію закладу.

Детектор розміщений в центрі приміщення та працює під управлінням дистрибутива Kali Linux, що дозволяє йому використовувати бездротовий NIC у режимі монітора. Система має зовнішню бездротову карту NIC з знімною всеспрямованою антеною з коефіцієнтом посилення 9 дБі, що покращує як прийом, так і передачу сигналу.

Фальшива точка доступу (Fake AP) буде розміщена між AP1 і AP2, що дозволяє їй ефективно залучати клієнтів з обох точок доступу. Для зручності та стабільності фальшива точка доступу буде стаціонарною, що дозволить уникнути

проблем з ослабленням сигналу та втратою з'єднання, яке може виникнути при її русі. Вона працюватиме під управлінням дистрибутива Backtrack 5R3 Linux і буде мати зовнішню бездротову карту NIC з антеною з високим коефіцієнтом посилення 13 дБі, що забезпечить більший діапазон сигналу.

Для тестування спочатку система буде перевірена на здатність виявляти і додавати до списку захисту три законні точки доступу, які мають унікальний BSSID і належать різним виробникам. Якщо ці точки доступу будуть успішно додані до списку захисту, то можна активувати фальшиву точку доступу. Протестований сценарій включає перевірку здатності системи виявляти фальшиву точку доступу та ініціювати процес деаутентифікації для відключення клієнтів від цієї точки доступу.

Фальшива точка доступу буде налаштована на трансляцію того ж SSID, що й законні точки доступу, проте її BSSID залишиться стандартним. Бездротовий NIC фальшивої точки доступу буде оснащений антеною з високим коефіцієнтом посилення 13 дБі, а канал її роботи буде відповідати каналу законних точок доступу. Це забезпечить максимальну ймовірність підключення клієнтів, оскільки всі умови для підключення будуть ідентичні законним точкам доступу.

Положення фальшивого АП ілюстровано на малюнку 4.8.

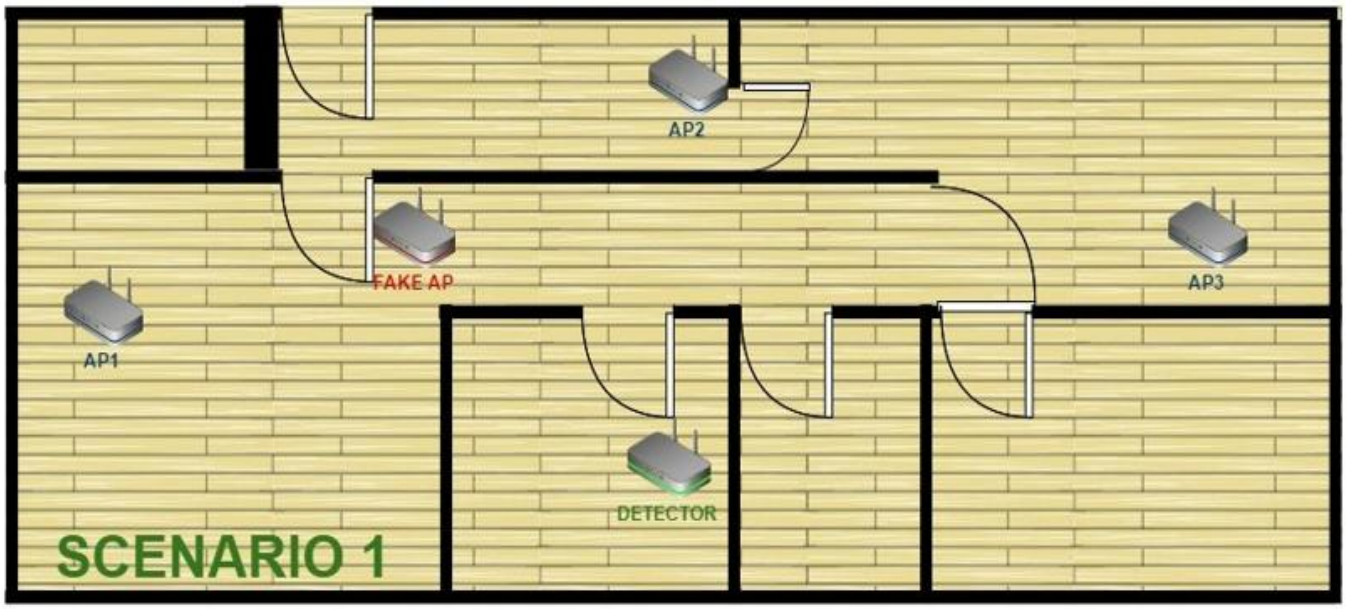


Рисунок 4.20. – Огляд налаштування данного сценарію.

Очікуваний результат сценарію полягає в тому, що система виявлення та запобігання (IDS) повинна успішно виявити фальшиву точку доступу, яка транслює той самий SSID, що й законні точки доступу. При цьому система визначає фальшиву точку доступу, орієнтуючись на унікальний BSSID, який відрізняється від BSSID законних точок доступу. Це є критичним для правильного виявлення фальшивих точок доступу, оскільки SSID сам по собі не є достатнім для виявлення, а BSSID є унікальним ідентифікатором кожної точки доступу.

У першому сценарії фальшива точка доступу почала передавати сигнал із тим самим SSID, що і зазначено в описі тесту. Оскільки система вже мала базу даних із законними точками доступу, їй не потрібно було виконувати оновлення бази даних. Після сканування бездротових мереж, система порівняла отримані результати з уже збереженими точками доступу в базі даних. Згідно з результатами, на рисунку 4.9 показані результати сканування, де зеленим кольором позначено законні точки доступу, а червоним — фальшиву точку доступу з BSSID

Після виявлення фальшивої точки доступу модуль Fake AP Detector активувався, спираючись на порівняння BSSID і визначив, що одна з точок доступу є підробленою. Система одразу повідомила користувача про наявність фальшивої точки доступу в зоні і, після цього, завантажила підмодуль деаутентифікації. Завдяки цьому, система зможе активувати бездротовий NIC в режимі моніторингу, що дозволяє переходити до наступного етапу атаки, тобто деаутентифікації підключених клієнтів.

Це дозволить ефективно відключити клієнтів від фальшивої точки доступу, запобігаючи їхньому підключенню до підроблених мереж, створених зловмисниками. Таким чином, система захисту не лише нейтралізує потенційну загрозу перехоплення даних, але й мінімізує ризики, пов’язані з маніпуляціями з мережею, такими як перенаправлення трафіку, крадіжка облікових даних або встановлення шкідливого програмного забезпечення. Додатково, автоматичне відключення клієнтів і перенаправлення їх до легітимної мережі дозволяє зберегти стабільність і доступність мережі для користувачів.

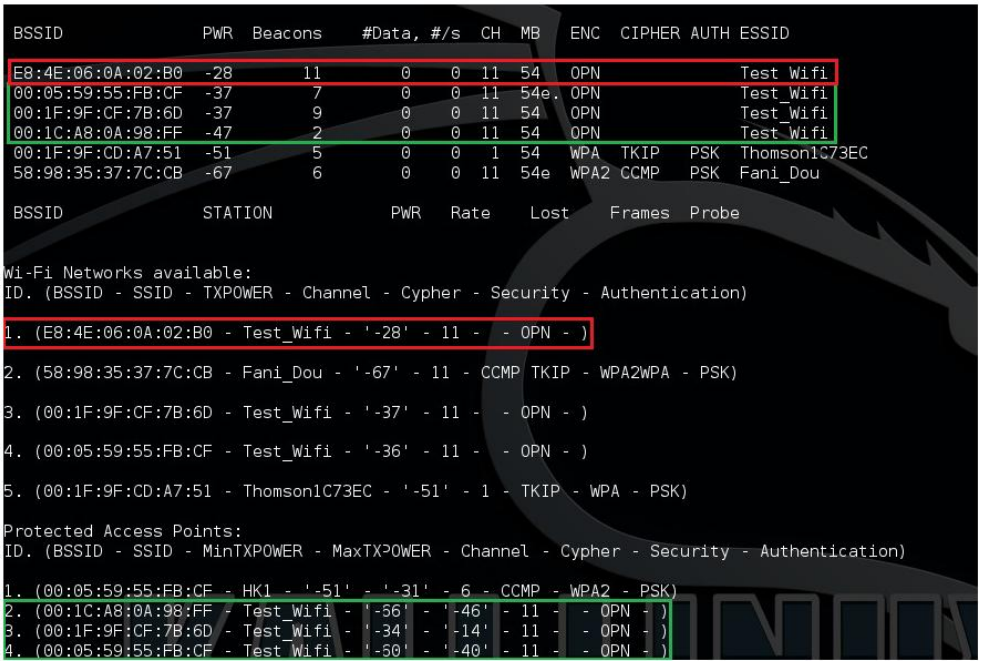


Рисунок 4.21. – Виявлення фальшивої точки доступу на основі BSSID.

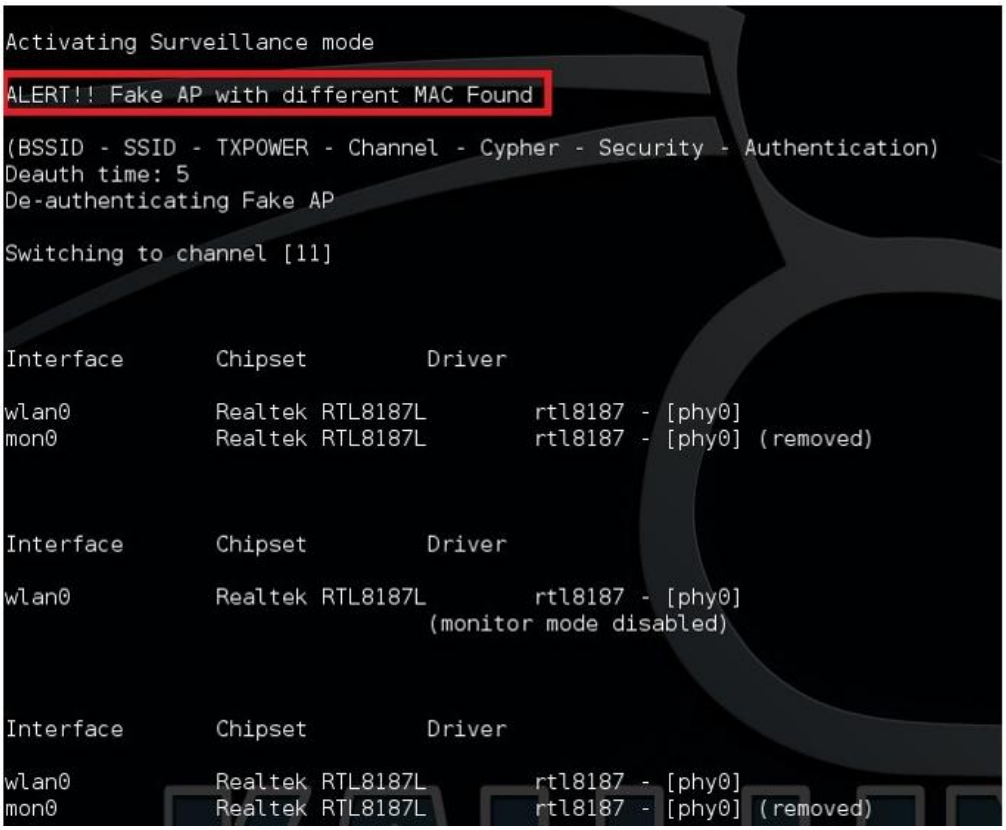


Рисунок 4.22 – Відображення оповіщення та підготовка до деаутентифікації

Як тільки бездротовий мережевий інтерфейсний контролер (NIC) буде належним чином підготовлений і готовий до роботи, він розпочне процес деаутентифікації у відношенні фальшивої точки доступу, яка ідентифікується на

основі її унікального BSSID. Цей процес дозволяє від'єднатися від підробленої точки доступу, щоб забезпечити безпеку бездротової мережі та уникнути загроз, пов'язаних із підробкою. На ілюстрації, представленій у вигляді схеми під номером 4.9.2, детально показано весь алгоритм деаутентифікації, який застосовується до фальшивих точок доступу. Такий підхід дозволяє ідентифікувати небажані з'єднання на рівні BSSID і своєчасно перервати їх.

Успішне виявлення фальшивих точок доступу та запобігання підключенню до них ґрунтується саме на аналізі BSSID, що є унікальним ідентифікатором для кожного доступного пристрою. Цей метод дозволяє точніше визначати небезпечні підключення в межах мережі та уникати їхнього впливу на безпеку даних користувача.

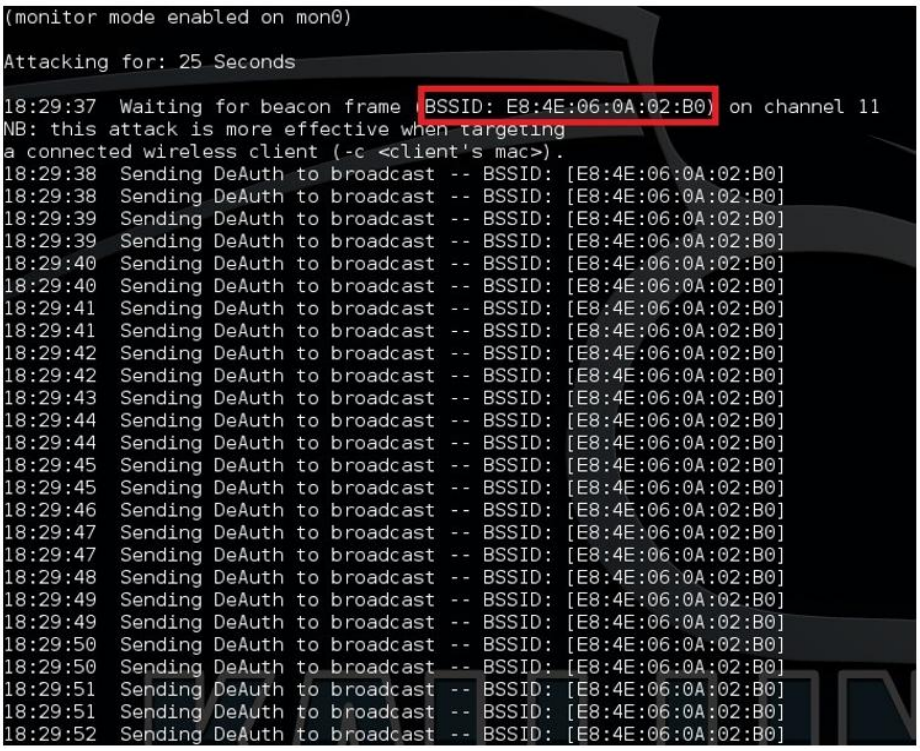


Рисунок 4.23 – Деаутентифікація до фальшивої точки доступу

4.3. Висновки

У цьому розділі було досліджено проблему виявлення та запобігання атакам типу MITM (Man-in-the-Middle) через мережі 802.11x, що важливо для

забезпечення безпеки бездротових мереж. Однією з основних проблем є відсутність шифрування на канальному рівні, що дозволяє зловмисникам легко втручатися в комунікацію і перехоплювати чутливу інформацію, яка передається через відкриті бездротові мережі.

Зловмисник може підключитися до такої відкритої мережі та створити небезпечний міст до Інтернету, ставши несанкціонованим провайдером бездротового з'єднання. Це дозволяє йому виконувати атаки, такі як підміна точок доступу та перехоплення даних клієнтів. Щоб усунути цю загрозу, було створено приватний DHCP-сервер, що дозволяє зловмиснику виступати як "підставний" інтернет-провайдер. Результати показали, що навіть за умови шифрування даних на вищих рівнях OSI, вони все одно можуть бути перехоплені, якщо зловмисник має доступ до канального рівня і використовує відповідні інструменти.

Ключовою проблемою для зловмисників є необхідність обдурити клієнтів та змусити їх підключитися до фальшивих точок доступу. Якщо точка доступу імітує законну точку з тим самим SSID і високими характеристиками, то клієнти можуть підключатися до неї без підозр. Проте зловмисник може втратити свою перевагу, якщо не вдасться правильно налаштувати підроблену точку доступу, оскільки вона повинна мати той самий BSSID і працювати на тому ж каналі, що й законна точка доступу.

Рішенням цієї проблеми стала система виявлення фальшивих точок доступу, яка збирає інформацію про законні точки доступу, зберігаючи їх параметри в базі даних. Регулярне сканування мережі дозволяє виявити нові точки доступу та порівняти їх характеристики з тими, що містяться в базі даних. Якщо точка доступу має однаковий SSID, але відрізняється за BSSID або іншими параметрами, вона вважається підозрілою та може бути атакована системою.

Проте існує ситуація, коли підроблена точка доступу бере на себе всі характеристики законної точки, включаючи SSID, BSSID, і канал. У такому випадку система не зможе ідентифікувати фальшиву точку доступу, і вона може пропустити цю атаку.

ВИСНОВКИ

В цій роботі ми дізнались, що атаки типу "людина посередині" (MITM) сьогодні стають все більш поширеними. Встановлення програмного забезпечення та програм на смартфони стає популярнішим, ніж будь-коли, що дає злочинцям простий спосіб отримати вашу інформацію.

У першому розділі, було вияснено, що атаки MITM – це старі, але дуже потужні атаки. У більшості атак цілями будуть сервери або постачальники послуг. Але в атаках MITM мішенями є клієнти. Успішний запуск атаки надає зловмисникам дані, які можуть вплинути на нормальний соціальний та економічний статус індивіда в суспільстві. Хоча атаку можна виявити за допомогою зовнішньої бездротової картки, використання бездротової картки щоразу є трудомістким процесом.

У другому розділі був запропонований метод виявлення та визначення місцезнаходження зловмисника MITM у бездротових мережах шляхом обчислення часу проходження сигналу туди й назад (RTT) та обчислення потужності отриманого сигналу (RSS) від точки доступу, якщо є зловмисник, ці значення вищі за них і більші, ніж відсутність зловмисника (більший час затримки).

Виявити зловмисника можна за допомогою незвичайних сигналів у мережевих облікових записах за допомогою експериментальних даних, таких як потужність сигналу та час затримки, тому можна його виявити, взявши зразки та обліковуючи RTT під час процесу передачі даних між відправником та одержувачем.

У третьому розділі я досліджував можливість застосування систем виявлення вторгнень (IDS) та систем запобігання вторгнень (IPS) для атак Man in the Middle (MitM) з використанням вузлів IDS. Для IPS використовується шифрування/дешифрування AES (128 біт, розмір ключа та блоку).

Для того, щоб забезпечити зниження затримки, в систему були введені спеціальні вузли, відомі як вузли IDS. Кожен вузол IDS опитує туманні вузли на

відстані одного стрибка та аналізує їхню реакцію з точки зору контенту, контексту та часу прибуття.

У четвертому розділі було розглянуто проблему, яка полягає в тому, що необхідно було знайти метод для виявлення та запобігання атакам MITM через мережі 802.11x. Проблема може бути розширена до ситуації, коли немає шифрування даних, що передаються через канальний рівень даних, через простоту використання з боку громадськості. Ця ситуація ідеально підходить для зловмисного користувача, щоб втрутитися та перехопити приватну інформацію від користувачів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. М. Конті, Н. Драгоні та В. Лесик, "Огляд людини в середніх атаках", в IEEE Communications Surveys and Tutorials, том 18, No 3, с. 2027-2051.
2. Бхушан, Б., Саху, Г., і Рай, А. К. Атака "людина посередині" в бездротових і комп'ютерних мережах - огляд. 3-тя міжнародна конференція на Досягнення в обчислювальній техніці, зв'язку та автоматизації (ICACCA) (осінь).
3. К. Коліас, Г. Камбуракіс, А. Ставру та С. Грицаліс, "Виявлення вторгнень у мережах 802.11: емпірична оцінка загроз та публічний набір даних", в IEEE Communications Surveys and Tutorials, том 18, No 1, с. 184-208.
4. А. К. Чорппат, Т. Альпкан та Х. Боче, "Байєсівські механізми та методи виявлення для бездротової мережі зі зловмисними користувачами", в IEEE Transactions on Mobile Computing, том 15, No 10, с. 2452-2465.
5. Прихована небезпека: атака "людина посередині" в мережах - Ahmet EFE, 1GizemKALKANCI 2, Mehmet DONK 3, Serhat CİHANGİR 4, Ziya UYSAL51Dr, CISA, CRISC, PMP, Внутрішній аудитор, Агентство розвитку Анкари, Туреччина.
6. Дакоста, І., Ахамад, М., і Трейнор, П. Не довіряйте нікому іншому: виявлення атак MITM на SSL/TLS без третіх сторін. Конспект лекцій з інформатики, 199–216.
7. М. Ліхтман, Р. П. Джовер, М. Лабіб, Р. Рао, В. Мароєвич та Дж. Х. Рід, "Глушіння, спуфінг та сніфінг LTE/LTE-A: оцінка загроз та пом'якшення", у журналі IEEE Communications, том 54, No 4, с. 54-61
8. Виявлення та локалізація атак типу "людина посередині" у фіксованих бездротових мережахЦзіцянь Донг, Рендольф Есподжо, Ю Ван та Веньцзе ЧжуанШкола інженерних та комп'ютерних наук, Нью-Йоркський технологічний інститут, Нью-Йорк, США. https://smarteyetechnology.com/blog/confidentialit y-integrity-availability-basics-of-information-security /
9. Людина посередині-атаки: розуміння простими словами Авіджіт Малліка*, Абід Ахсанб, Мхіа доктор медицини. Джаглул Шахадата і Цзя-Чі Цу

10. Чень, З., Го, С., Чжен, К., і Ян, Ю. *Моделювання атаки "людина посередині" в бездротових мережах. Міжнародна конференція з бездротового зв'язку, мереж та мобільних обчислень.* DOI:10.1109/wicom.2007.562

11. М. Алічеррі та А. Керомітіс. Подвійна перевірка кількох шляхів проти людини посередині нападів. Комп'ютери та зв'язок, сторінки 557 – 563,

12. Ж. Беленгер і К. Калафате. Недорогий вбудований ідентифікатор для моніторингу та запобігання атакам типу "людина посередині" на дротові локальні мережі. Нова інформація безпеки, системи та технології, сторінки 122 – 127.

13. Б.-Ю. Чой, С. Мун, З.-Л. Чжан, К. Папагіаннакі, і К. Діот. Аналіз затримки пакетів «точка-точка» в оперативній мережі. Двадцять третя щорічна спільна конференція IEEE Computer and Communications Societies, 3:1797 – 1807.

14. Т. Ельтето і С. Молнар. Про розподіл затримок в обидві сторони в мережах tcp/ip. Локальні комп'ютерні мережі, сторінки 172–181.

15. У. Хенгартнер, С. Мун, Р. Мортьє, К. Діот. Виявлення та аналіз шлейфів маршрутизації в трасуванні пакетів. Семінар з вимірювання Інтернету ACM Sigcomm, сторінки 107–112.

16. К. Луки. Формальні методи аналізу криптографічних протоколів: нові проблеми та тенденції. Вибрані області в комунікаціях, 21(1):44–54.

17. Г. Наяк і С. Самаддар. Різні смаки атаки "людина посередині", наслідки та можливі рішення. Комп'ютерні науки та інформаційні технології, 5:491 – 495.

18. М. Ордін і М. Джурджіу. На шляху до захисту з'єднань клієнт-сервер від «людина посередині»Нападів. «Електроніка і телекомунікації», сторінка 127– 130. К. Папгірноакі, С. Мун, К. Фрейлі, П. Тіран

19. К. Діот. Вимірювання та аналіз затримки одного стрибка в магістральній ip мережі. Вибрані області в комунікаціях, 21(6):908 – 921.

20. author = "Chibiao Liu, James Yu", title = "Рішення для автентифікації WLAN та асоціативних DoS-атак", journal = "IAENG International Journal of Computer Science, 34:1, IJCS3414".

21. author = "Le Wang, Alexander M. Wyglinski", title = "Комбінований підхід для розрізнення різних типів атак глушіння проти бездротових мереж".

22. author = "Zouheir Trabelsi, Kadhim Hayawi, Arwa Al Braiki, Sujith Samuel Mathew",, title = "Мережеві атаки та захист: практичний підхід",publisher = "CRC Press",

23. author = "Колін Кнудсен", title = "Смартфони, планшети та мобільна революція", url = "http : www.coadydiemar.com/html/rbvolume62012.html",

24. author = "Абід Хусейн, Назар А. Сакіб, Усман Камар, Мухаммад Зія та Хасан Махмуд", title = "Радіочастотне глушіння з урахуванням протоколу в Wi-Fi та комерційних бездротових мережах", journal = "ЖУРНАЛ ЗВ'ЯЗКУ ТА МЕРЕЖ".

25. author = "Simon S. Lam", title = "Протокол множинного доступу Carrier Sense для локальних мереж", author = "Anna M. Johnston, Peter S. Gemmell", title = "Authenticated Key Ex- change Provably Secure against the Man-in-the-Middle Attack",

26. В. Тернер, К. МакГілліврей, Д. Гау, Р. Кларк, М. Моралес, Б. Краус, Idc futurescape: Всесвітній Інтернет речей прогнози, в: IDC, F. Комп'ютинг, Інтернет речей: розширити хмару

27. К. Лі, З. Цінь, Е. Новак, К. Лі, Захист sdn інфраструктури мереж IoT–Fog від атак mitm, IEEE Internet of Things Journal 4 (5) (2017) 1156–1164. doi:10.1109/JIOT.2017.2685596.

28. J. Ni, K. Zhang, X. Lin, X. S. Shen, Забезпечення безпеки туманних обчислень для додатків Інтернету речей: проблеми та рішення, IEEE Communica- tions Surveys Tutorials 20 (1) (2018) 601–628. doi:10.1109/COMST.2017.2762345.

29. Ю. Десмедт, Атака "людина посередині", в: Енциклопедія криптографії та безпеки, Springer, с. 759–759.

30. Б. Поттер, Б. Флек, 802.11 Безпека, серія O'Reilly, O'Reilly Media, Incorporated.ьURL https://books.google.com.sa/books?id=RVQ4GgKeEtgC

31. І. Стойменович, С. Вен, Парадигма туманних обчислень: сценарії та питання безпеки, Федеративна конференція з комп'ютерних наук та інформаційних систем, 2014, с. 1–8. doi:10.15439/2014F503.

32. Б. Н. Б. Еканаяке, М. Н. Халгамуге, А. Саєд, Огляд: питання безпеки та конфіденційності туманних обчислень для Інтернету речей (IoT), Springer

International Publishing, Cham, 2018, с. 139–174. URL https://doi.org/10.1007/978-3-319-70688-7_7

33. С. Хан, С. Паркінсон, Ю. Цінь, Безпека туманних обчислень: огляд поточних додатків і рішень безпеки, Журнал хмарних обчислень 6 (1)

34. М. Чіанг, Т. Чжан, Туман і IoT: огляд дослідницьких можливостей, IEEE Internet of Things Journal 3 (6) 854–864.

35. К. Чжао, Л. Ге, Дослідження безпеки Інтернету речей, в: Обчислювальний інтелект і безпека (CIS), 9-та Міжнародна конференція на, IEEE, 2013, с. 663–667.

36. Ж.-к. ЯНГ, Б.-х. ФАНГ, Модель безпеки та ключові технології для Інтернету речей, Журнал Китайських університетів пошти та телекомунікацій 18 109–112.

37. С. Бабар, А. Станго, Н. Прасад, Д. Сен, Р. Прасад, Запропонована вбудована структура безпеки для Інтернету речей (IoT), в: Бездротовий зв'язок, автомобільні технології, інформаційна теорія та технологія аерокосмічних та електронних систем (Wireless VITAE), 2-га міжнародна конференція на, IEEE, с. 1–5.

38. J. Liu, Y. Xiao, C. P. Chen, Аутентифікація та контроль доступу в Інтернеті речей, в: Семінари з розподілених обчислювальних систем (ICD-CSW), 32-га міжнародна конференція on, IEEE , с. 588–592.

39. Д. Кім, С. Кваліфікованата масштабована інфраструктура відкритих ключів для бездротових сенсорних мереж, в: Міжнародний симпозіум з мережевих робіт, комп'ютерів та комунікацій, с. 1–5. doi:10.1109/SNCC.2014.6866514.

40. М. Моханапрія, І. Крішнамурті, Модифікований протокол dsr для виявлення та видалення селективної атаки чорних дір у манеті, Computers & Electrical Engineering 40 (2) 530–538.

41. Б. Азіз, Г. Гамільтон, Виявлення атак "людина посередині" за точним часом, Третя міжнародна конференція з нової безпеки , систем і технологій, с. 81-86. doi:10.1109/SECURWARE.

42. С. М. Гласс, В. Мутхуккумарасамі, М. Портманн, Виявлення атак типу "людина посередині" та "червоточина" в бездротових mesh-мережах Міжнародна конференція з передових інформаційних мереж та додатків, с. 530–538. doi:10.1109/AINA.131.

43. А. Патан, Безпека самоорганізованих мереж: MANET, WSN, WMN, VANET, CRC Press. URL https://books.google.com.sa/books?id=ZtBnZoijaDcC

44. J. Eriksson, S. V. Krishnamurthy, M. Faloutsos, Truelink: Практична протидія атаці червоточини в бездротових мережах, в: Мережеві протоколи, ICNP'06. Матеріали 14-ї міжнародної конференції IEEE 2006 року, IEEE, с. 75–84.

45. Д. П. Яблон, Обмін автентифікованими ключами лише за допомогою надійного пароля, ACM SIGCOMM Computer Communication Review 26 (5) 5–26.

46. Т. Д. Чунг, Р. Ібрагім, В. С. Асірвадам, Н. Саад, С. М. Хассан, Аналіз енергоспоживання бездротового адаптера для промислової бездротової мережі виконавчих механізмів, Procedia Computer Science 105 227–234.

47. М. Ніксон, Т. Раунд Рок, Порівняння wirelesshart і isa100. 11a, Whitepaper, Emerson Process Management 1–36.

48. Т. Айзенбарт, С. Кумар, Огляд реалізацій легкої криптографії, IEEE Design & Test of Computers 24 (6).

49. "Simon Eberz, Martin Strohmeier, Matthias Wilhelm, Ivan Martinovic", title = "Практична атака "людина посередині" на протоколи генерації ключів на основі сигналу "

50. "Константінос Пелехрініс, Маріос Іліофоту та Шрікант В. Крішна- мурті", title = "Відмова в обслуговуванні в бездротових мережах: випадок глушників", journal = "IEEE COMMUNICATIONS SURVEYS AND TUTORIALS".

51. "Син Нам, Донгвон Кім та Чонгеун Кім", title = "Покращений ARP: запобігання отруєнню людиною в середині на основі ARP"

52. "Іхун Чжоу, Дапен Ву, Скотт М. Неттлз", title = "Аналіз та запобігання атакам на відмову в обслуговуванні на рівні MAC для систем Stock 802.11"

53. "Араш Хабібі Лашкарі, Мір Мохаммад Сейєд Данеш, Бехранг Самаді", title = "Огляд протоколів безпеки бездротового зв'язку (WEP, WPA та WPA2/802.11i)"

54. "Топе Олуфон, Карлін Е-А Кемпбелл, Стівен Хоул, Капілан Радхакр- ішнан та Ар'я Седіг", title = "Пом'якшення зовнішніх загроз у бездротових локальних мережах", journal = "Міжнародний журнал комунікаційних мереж та інформаційної безпеки (IJCNIS)",

55. "Кен Танг, Маріо Герла", title = "ТРАНСЛЯЦІЙНИЙ SUP-ПОРТ MAC LAYER У БЕЗДРОТОВИХ МЕРЕЖАХ 802.11",

56. "Hongqiang Zhai1, Younggoo Kwon and Yuguang Fang", title = "Аналіз ефективності протоколів IEEE 802.11 MAC у бездротових локальних мережах".

57. "Пітер Валіан і Тодд К. Уотсон", title = "NETREG: СИСТЕМА РЕЄСТРАЦІЇ DHCP З АВТОМАТИЧНИМ СПОЛУЧЕННЯМ", рік = "2000"

58. "Benjamin E. Henty", title = "Короткий навчальний посібник з шарів PHY та MAC стандарту IEEE 802.11b",

59. "Kalpana Sharma, Mrinal Kanti Ghose", title = "Wireless Sensor Net- works: Огляд її загроз безпеці",

60. "Вішну Навда, Аніруддха Бохра, Самрат Гангулі, Ден Рубенштейн", title = "Використання стрибків каналів для підвищення стійкості 802.11 до атак глушіння",

61. "Хайдун Ся та Хосе Карлос Брустолоні", title = "Зміцнення веб-браузерів проти атак "людина посередині" та підслуховування"

62. "Мар тін Бек, Ерік Тьюз", title = "Практичні атаки проти WEP та WPA"

63. "Арістідес Мпіціопулос, Даміанос Гавалас, Харалампос Констан- топулос та Грамматі Панціу", title = "Огляд атак глушіння та контрзаходів у WSN".

64. "Moffat Mathews, Ray Hunt", title = "ВОЛЮЦІЯ АРХІТЕКТУРИ БЕЗПЕКИ БЕЗДРОТОВОЇ ЛОКАЛЬНОЇ МЕРЕЖІ ДО IEEE 802.11i (WPA2)",

65. "Рольф Оппліге, Ральф Хаузер та Девід Бейсін", title = "SSL/T LS Session-Aware User AuthenticationOr Як ефективно перешкодити людині посередині",

66. "Алехандро Проано, Лукас Лазос", title = "Вибіркові атаки глушіння в бездротових мережах"

67. "Алі Хаміє, Лінда Мокдад", title = "Виявлення атак радіоперешкод у VANET",

68. "Python. Документація Python", title = "Вбудовані функції", url = "https : docs.python.org/ 2/library/functions.htmlisinstance"

69. "Підручники з Python", title = "Метод заміни рядків Python", url = "http : www.tutorialspoint.com/python/stringreplace.htm",

70. "Python. Документація Python", title = "Читання та запис файлу CSV", url = "https : docs.python.org/ 2/library/csv.html",

ДОДАТОК А
(обов’язковий)

ЛІСТИНГ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Модуль 1 “Створення баз даних”

```
1 # Preparation of MySQL database
2 t ry :
3 t ry :
4 # Connecting to MySQL serverusingdefaul t username and password and hos t
IP addr e s s
5 db connection = MySQLdb. connect ( hos t=' 1 2 7 . 0 . 0 . 1 ' , us e r="" ,
passwd="" )
6 pr int "Connection MySQL successfulnn"
7 exc ept :
8 pr int "Wrong username /password or MySQL Se rve r i s downnn"
9 sys . e x i t ( 2 )
10
11 handler = db connection . cursor( )
12
13 # Cr eat ion o f the database MITMDB
14 comand = "show databas e s l i k e 'MITMDB' "
15 handl e r . exe cut e ( comand)
16 if handl e r . rowcount <= 0 :
17 comand = 'CREATE DATABASE IF NOT EXISTS MITMDB'
18 handl e r . exe cut e ( comand)
19
20 # Usage o f the database MITMDB
21 comand = 'USE MITMDB'
22 handler . execute ( comand)
23
24 # Load or Create the t ab l e where the APs metrics wi l l be s t o r ed based on
```

```
the SSID
25 comand = "show tables like'ssidtables' "
26 handl e r . execute (comand)
27 if handl e r . rowcount <= 0 :
28 comand = ' ' 'CREATE TABLE IF NOT EXISTS ssidtables (
29 id MEDIUMINT NOT NULL AUTO INCREMENT, PRIMARY KEY ( id ) ,
mac TEXT,
s s i d TEXT, Txpower INTEGER, channel NUMERIC, Code TEXT, Encrypt ion
TEXT
, Authent i cat ion TEXT)
30 ' ' '
31 handl e r . execute ( comand)
32
33 # Load or Create the t ab l e with the AP p r o t e c t i o n l i s t
34 comand = "show t a b l e s l i k e ' p r o t e c t i o n l i s t ' "
35 handl e r . exe cut e ( comand)
36 i f handl e r . rowcount <= 0 :
37 comand = ' ' 'CREATE TABLE IF NOT EXISTS p r o t e c t i o n l i s t (
38 id MEDIUMINT NOT NULL AUTO INCREMENT, PRIMARY KEY ( id ) ,
mac TEXT,
s s i d TEXT, min Txpower INTEGER, max Txpower INTEGER, channel
NUMERIC,
Code TEXT, Encrypt ion TEXT, Authent i cat ion TEXT)
39 ' ' '
40 handl e r . exe cut e ( comand)
41
42 # Load or Create the t ab l e where the De□authent i c a t i on a t t r i b u t e s ar e
s t o r ed
43 comand = "show t a b l e s l i k e ' a t r i b u t e s ' "
44 handl e r . exe cut e ( comand)
```

```
45 i f handl e r . rowcount <= 0 :
46 comand = ' ' 'CREATE TABLE IF NOT EXISTS a t r i b u t e s (
47 o p t i o n i n d i c varchar (255) , o p t i o n v a r i a b l e var char (255) )
48 ' ' '
49 handl e r . exe cut e ( comand)
50
51 # Empties the t ab l e s s i d t a b l e s
52 comand = ' Truncate t a b l e s s i d t a b l e s '
53 handl e r . exe cut e ( comand)
54 exc ept :
55 pr int "Er ror in MySQLnn"
    56 sys . e x i t ( 2 )
```

Модуль 2 “Ініціалізація параметрів деаутентифікації.”

```
1 #Deauthent i cat ion I n i t i a l i s a t i o n Options
2 t ry :
3
4 # Set de-authent i c a t i on durat ion
5 comand = " s e l e c t o p t i o n v a r i a b l e from a t r i b u t e s where o p t i o n i
n d i c = '
deauth t ime ' "
6 handl e r . exe cut e ( comand)
```

```
7 i f handl e r . rowcount <= 0 :
8 comand = " i n s e r t int o a t r i b u t e s va lue s ( ' deauth t ime ' , ' 0 ' ) "
9 handl e r . exe cut e ( comand)
10
11 # Set de-authent i c a t i on r e p e t i t i o n s
12 comand = " s e l e c t o p t i o n v a r i a b l e from a t r i b u t e s where o p t i o n i n d i c = '
    deauth r epeat ' "
13 handl e r . exe cut e ( comand)
14 i f handl e r . rowcount <= 0 :
15 comand = " i n s e r t int o a t r i b u t e s va lue s ( ' deauth r epeat ' , ' 1 ' ) "
16 handl e r . exe cut e ( comand)
17 exc ept :
    18 pr int "Er ror in Clas s ' Ini t i a lDe authOpt i ons 'nn"
```

Модуль 3 “Ініціалізація параметрів деаутентифікації.”

```
1 # Prepar ing Monitor I n t e r f a c e
2 t ry :
3 out = Popen ( " iwc onf i g " , s tdout=PIPE) . communicate ( ) [ 0 ]
4 w i f i i f a c e = ""
5 mon nic = ""
6 i f "wlan" in out :
7 w i f i i f a c e = out [ 0 : 6 ] . s t r i p ( )
8 e l s e :
9 pr int "nnnnNo wi r e l e s s NIC pr e s ent ! ! n n"
10 pr int " Pl eas e connect a wi r e l e s s NIC and t ry again "
```

```
11 Termination ( "DATABASE" )
12 sys . e x i t ( 2 )
13
14 # Check i f mon i n t e r f a c e i s not di s abl ed
15 ai rmon data = Popen ( "airmon□ng" , s tdout=PIPE) . communicate ( ) [ 0 ]
16 i f 'mon ' in ai rmon data :
17 pr int "nnnnMonitor mode on wi r e l e s s NIC de t e c t ed . "
18 pr int " Pl eas e d e a c t i v a t e monitor mode on wi r e l e s s NIC and t ry again nn"
19 Termination ( "DATABASE" )
20 sys . e x i t ( 2 )
21 exc ept :
22 pr int "Er ror in Prepar ing Monitor I n t e r f a c e nn"
```

Модуль 4 “ Створення інтерфейсу Monitor”

```
1 # Creating Monitor Interface
2 t ry :
3
4 # Shut dwon and r e a c t i v a t e wi r e l e s s NIC
5 pr int " Se t t ing up wi r e l e s s NIC: " + w i f i i f a c e + "nn"
6 os . system( ' i f c o n f i g ' + w i f i i f a c e + ' down ' )
7 os . system( ' i f c o n f i g ' + w i f i i f a c e + ' up ' )
8
9 pr int "Act ive wi r e l e s s NIC: " + w i f i i f a c e + "nn"
10
11 # Enable Monitor mode
12 pr int ' Enabl ing Monitor mode '
```

```
13 wi r e l e s s n i c = Popen ( [ "airmon□ng" , " s t a r t " , w i f i i f a c e ] , s
tdout=PIPE) .
communicate ( ) [ 0 ]
14
15 # Deleted the unne c e s sary c h a r a c t e r s from the output
16 i f 'mon ' in wi r e l e s s n i c :
17 pr int wi r e l e s s n i c [ □33: □1] . s t r i p ( )
18 mon nic = wi r e l e s s n i c [ □7: □2] . s t r i p ( " ) " )
19
20 # Terminate harmful s e r v i c e s
21 i f 'NetworkManager ' in wi r e l e s s n i c :
22 pr int "nn Terminating 'NetworkManager ' "
23 os . system( " s e r v i c e network□manager s top " )
24 i f ' wpa suppl i cant ' in wi r e l e s s n i c :
25 pr int "nn Terminating ' wpa suppl i cant ' "
26 os . system( " p k i l l wpa suppl i cant " )
27 exc ept :
28 pr int "Er ror in Cr eat ing Monitor I n t e r f a c e nn"
```

Модуль 5 “Сканування та збір даних і фільтрація”

```
1 # Remove the old output from airodump
2 t ry :
3 os . system( ' rm out . csv □01._ ' )
4 exc ept :
5 pr int "Er ror d e l e t i n g Airodump csv f i l e nn"
6
7 # Scanning f o r a v a i l a b l e SSIDs
8 pr int "SCANNING FOR ACTIVE Wi□Fi NETWORKS"
9 pr int "nnnn"
```

```
10 t ry :
11
12 #Scan and save r e s u l t s
13 airodump = Popen ( [ "airodump□ng" , "□ □output□format " , " csv " , "□w" ,
" out .
csv " , mon nic ] )
14
15 r e sul tAPs = fg
16
17 #S n i f f va lue s from scanned data
18 s n i f f ( i f a c e=mon nic , prn=ap di s cove ry , count=20, s t o r e=Fal se , l
f i l t e r=
lambda p : (Dot11Beacon in p or Dot11ProbeResp in p) )
19
20 airodump . t e rminat e ( )
21 db conne c t ion . commit ( )
22 exc ept :
23 pr int "Er ror in a v a i l a b l e SSIDsnn"
```

Модуль 6 “Підмодуль виявлення BSSID і SSID”

```
1
2 # Par s ing Scapy parameter s
3 de f ap di s c o v e r y ( packet ) :
4 t ry :
5
6 # Search the frame ' s t hi rd addr e s s to f i n d the BSSID
7 bs s id = packet [ Dot11 ] . addr3
8 i f bs s id in r e sul tAPs :
9 r e turn
10 p = packet [ Dot11Elt ]
```

```
    11 cap = packet . s p r i n t f ( "fDot11Beacon:%Dot11Beacon . cap%g"
12 "fDot11ProbeResp:%Dot11ProbeResp . cap%g" ) . s p l i t ( '+' )
13
14 s s i d = None
15
16 # Search the frame to f i n d the SSID
17 whi l e i s i n s t a n c e (p , Dot11Elt ) :
18 i f p . ID == 0 :
19 s s i d = p . i n f o
20 p = p . payload
21
22 # Stor e the SSID
23 r e sul tAPs [ bs s id ] = ( s s i d )
24 exc ept :
    25 pr int "Er ror in Clas s ' ap di s c o v e r y 'nn"
```

Модуль 7 “Розбір вихідних даних Airodump-ng csv”

```
    1
    2 # Par s ing the airodump□ng output
    3 de f CsvParse ( ) :
    4 t ry :
    5
    6 # Opens the csv output f i l e from airodump□ng
    7 f = open ( ' out . csv □01. csv ' , ' rb ' )
    8 t ry :
    9
    10 # Reader obj e c t i s c r e a t ed and z e r o s ar e r epl a c ed with " n u l l "
    11 r eade r = csv . r eade r ( x . r e p l a c e ( ' n0 ' , ' ' ) f o r x in f )
    12
    13 # The rows o f the f i l e ar e checked again and plac ed in orde r
```

```
14 f o r row in r eade r :
15 i f 'BSSID ' in row :
16 cont inue
17 i f ' St a t i on MAC' in row :
18 break
19 i f l en ( row) < 1 :
20 cont inue
21 # The par sed r e s u l t s ar e s t o r ed int o the database
22 comand = " i n s e r t int o s s i d t a b l e s (mac , s s id , Txpower , channel , Code ,
Encryption , Authent i cat ion ) va lue s (%s ,%s ,%s ,%s ,%s ,%s ,%s ) "
23 handl e r . exe cut e ( comand , ( row [ 0 ] . s t r i p ( ) , row [ 1 3 ] . s t r i p ( ) , row
[ 8 ] . s t r i p
( ) , row [ 3 ] . s t r i p ( ) , row [ 6 ] . s t r i p ( ) , row [ 5 ] . s t r i p ( ) , row [ 7 ] . s t
r i p ( ) ) )
24 db conne c t ion . commit ( )
25
26 # Sub□module terminated
27 f i n a l l y :
28 f . c l o s e ( )
29 exc ept :
30 pr int "Er ror in Clas s ' CsvParse 'nn"
```

ДОДАТОК Б ПЕРЕЛІК НАУКОВИХ ПРАЦЬ

Сертифікат № 2024-112-1

Міністерство освіти і науки України
Хмельницький національний університет

СЕРТИФІКАТ

Савич Нікола Властімірович

учасник XVI Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2024»
24 години участі (0,8 ECTS credits)

Голова оргкомітету АПКН-2024

Олег СИНЮК
проректор Хмельницького національного
університету з наукової роботи,
доктор технічних наук, професор

м. Хмельницький
15-16 листопада 2024

E-mail: apkt.khnu@gmail.com

ДОДАТОК В

РЕЗУЛЬТАТИ НАУКОВИХ ПУБЛІКАЦІЙ

Міністерство освіти і науки України
Хмельницький національний університет

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами XVI Всеукраїнської науково-практичної конференції
«Актуальні проблеми комп'ютерних наук АПКН-2024»

15-16 листопада 2024

Хмельницький 2024

УДК 004.891

Савич Н.В., Стецюк М.В., Мусіюк А.В.

Хмельницький національний університет

ОГЛЯД ТЕХНОЛОГІЙ БЕЗПЕКИ ДЛЯ ІНТЕРНЕТУ РЕЧЕЙ ТА ПОТЕНЦІЙНІ РІШЕННЯ

IoT відкриває великі можливості у багатьох сферах людської діяльності, що може значно вплинути на життя людей. Підключення невеликих чутливих пристроїв до Інтернету дає змогу здійснювати всеохоплюючі обчислення. У цій роботі представлено огляд існуючих технологій і протоколів безпеки для Інтернету речей, а також розглянуто найбільш поширені механізми захисту, їхні особливості та способи застосування в IoT. Додатково проаналізовано проблеми, пов'язані із забезпеченням безпеки в IoT, та запропоновано можливі рішення для подолання цих викликів.

IoT opens up great opportunities in many areas of human activity, which can greatly affect people's lives. Connecting small, sensitive devices to the Internet enables pervasive computing. This work presents an overview of existing technologies and security protocols for the Internet of Things, and also examines the most common security mechanisms, their features and how they are used in IoT. In addition, the challenges related to security in IoT are analyzed and possible solutions to overcome these challenges are proposed.

Інтернет речей (IoT) – це мережа пристроїв, кожний з яких автоматично збирає та обмінюється даними по мережі, тобто інтернет речей – це взаємодія між декількома пристроями, речами та об'єктами. Концепція цієї нової технології полягає в тому, щоб автоматизувати роботу та підключати пристрої через Інтернет які використовуються в багатьох секторах та галузях, таких як споживчі програми, бізнес-додатки, урядові програми. Кількість пристроїв інтернет речей у всьому світі нині обчислюється мільярдами.

Пристрої інтернет речей можуть мати інтелектуальні можливості для збору, аналізу і навіть прийняття рішень без втручання людини, тому в системі інтернет речей безпека є найвищою вимогою. По-перше, відомі загрози безпеці, вразливості та атаки традиційних систем інформаційних технологій (IT) природно успадковуються. По-друге, багато додаткових векторів атак безпеки включені проти більш простих пристроїв IoT. Більшість пристроїв будуть безпосередньо підключені до Інтернету, щоб бути безпосередньо доступними, і це також робить їх безпосередньо схильними до кількох видів атак безпеки, особливо відмови в обслуговуванні (DoS). Типова локальна мережа буде включати значно більшу кількість пристроїв з обмеженими ресурсами. Це не тільки робить великий набір пристроїв IoT значно вразливішим і менш здатним справлятися з атаками безпеки, але також призводить до додаткових труднощів при розробці та впровадженні

рішень безпеки, які доступні за ціною для пристроїв IoT з обмеженими можливостями[1].

У мережних пристроях, таких як камери, було виявлено багато недоліків, наприклад жорстко закодовані облікові дані, відкриті порти Telnet і класичні помилки, такі як впровадження команд SQL (Structured Query Language). У разі неправильного використання шкідливі агенти можуть призвести до таких катастроф як атака DDoS (Distributed Denial of Service) ботнетом Mirai [2]. На рисунку1 показано, як можуть поширюватися приховані вразливості.

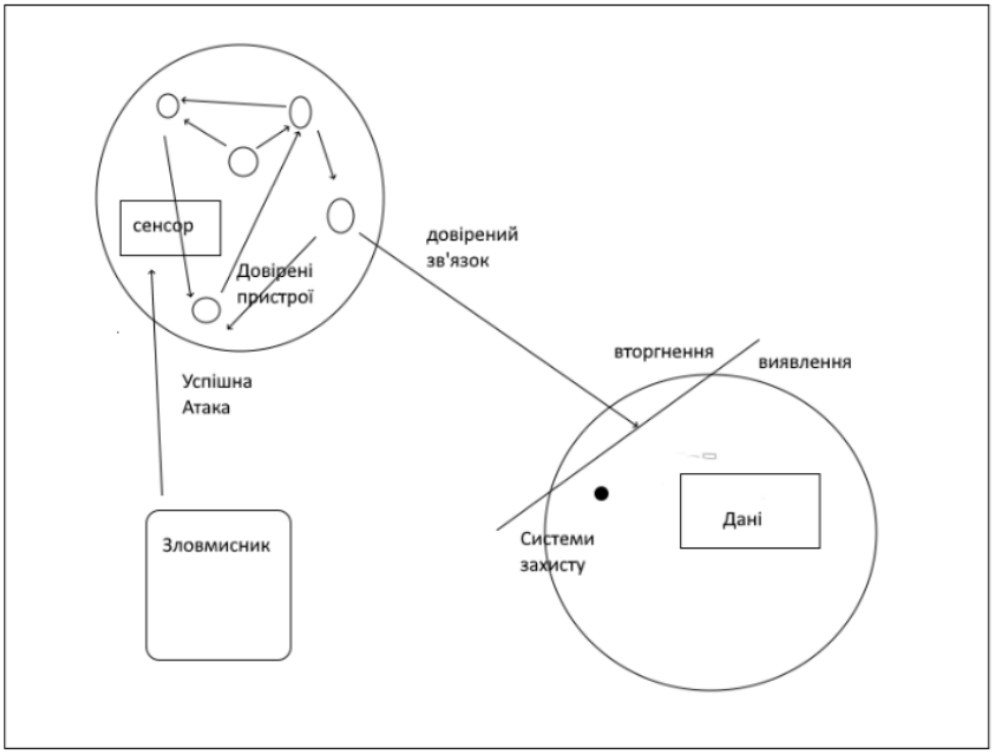


Рисунок 1 – Модель атаки на систему

Шкідливе ПЗ може захопити контроль над мережевим пристроєм залежно від рівня захищеності системи та вмінь зловмисника. Власник системи, недооцінюючи ризики, може зекономити на захисті периферійної системи, яка, хоча й не є основною ціллю, може використовуватися для атак на важливіші об'єкти. Підвищена чутливість до загроз може призвести до блокування надійних з'єднань через хибні тривоги. Це особливо актуально для мереж з численними партнерами та неповним контролем.

Для безпеки комунікацій між пристроями IoT застосовуються стандартизовані протоколи, що регулюють побудову та управління мережами,

зокрема IEEE 802.15.4, IPsec і DTLS. IoT спершу використовував існуючу інтернет-інфраструктуру, але нестача автоматичних налаштувань в IPv4 та інші труднощі стимулювали розробку нових технологій, як-от маршрутизація та масштабованість, що сприяло його широкому впровадженню у сфери охорони здоров'я, промисловості та розумних будівель[3].

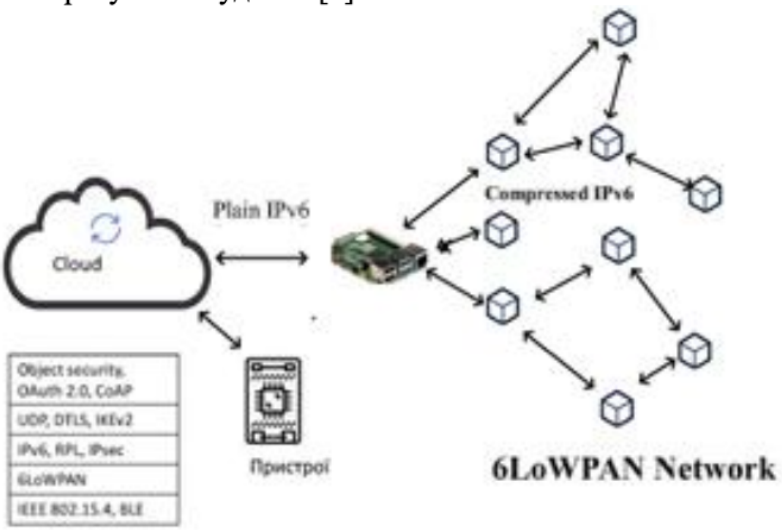


Рисунок 2 – Приклад мережі IoT з різними протоколами і технологіями

На прикладному рівні для IoT використовується OAuth 2.0 для контролю доступу, CoAP для обміну даними і безпеки, а також стандарти UDP та DTLS для захисту трафіку. При потребі IPsec можна налаштувати через IKEv2.

IPv6 надає масштабоване адресне простір, а протокол RPL оптимізований для мереж з низьким енергоспоживанням. Стандарт 6LoWPAN забезпечує стиснення та фрагментацію пакетів для сумісності з IEEE 802.15.4.

На канальному і фізичному рівнях часто використовуються IEEE 802.15.4 та BLE з додатковими механізмами безпеки. IoT-стек базується на відкритих протоколах, що дозволяє їхнє дослідження та вдосконалення спільнотою, зокрема на прикладному рівні CoAP або MQTT та транспортному рівні UDP або TCP [4].

На рисунку 2 представлений IoT-стек, що базується на кількох протоколах, кожен з яких відповідає за певний рівень і забезпечує власні механізми безпеки. На рівні представлення даних використовується CBOR — формат стиснення даних, який оптимізує передачу для обмежених IoT-пристроїв. Його супроводжує COSE, який забезпечує підпис і шифрування об'єктів CBOR, дозволяючи створювати легкі криптографічні ключі, хеші та цифрові підписи. На рівні обміну повідомленнями застосовується CoAP — спеціалізований протокол для обмежених пристроїв, що легко інтегрується з HTTP для роботи в широких мережах. CoAP забезпечує захищену комунікацію через OSCORE (шифрування CBOR) або DTLS, який дозволяє обмін зашифрованими повідомленнями через UDP і підходить для

промислових, домашніх і смарт-міських застосувань. OSCORE забезпечує наскрізний захист повідомлень між вузлами за допомогою COSE, захищаючи повідомлення CoAP на рівні застосунків від відтворення.

Для стиснення заголовків IPv6 і забезпечення захищеного з'єднання через транспортний режим у мережах 6LoWPAN використовується IPsec. На канальному і фізичному рівнях працюють стандарти IEEE 802.15.4 і BLE. IEEE 802.15.4 визначає фізичний та канальний рівні для мереж із низьким енергоспоживанням, тоді як BLE забезпечує легке з'єднання як енергоефективна альтернатива. OAuth 2.0 дозволяє авторизацію без передачі облікових даних, забезпечуючи безпечний доступ до ресурсів. MQTT, побудований на основі TCP, підтримує обмін даними за моделлю публікації-підписки, що є легким рішенням для IoT і M2M, мінімізуючи трафік і надійно працюючи в умовах ненадійного з'єднання[5].

Забезпечення безпеки в IoT передбачає використання протоколів на кожному рівні стека. Наприклад, на прикладному рівні застосовуються **CBOR** для ефективного стиснення даних та **OSCORE**, який забезпечує наскрізний захищений зв'язок між клієнтом і сервером у протоколі CoAP. Сам **CoAP** підтримує обмін даними між пристроями та сумісний із HTTP, що дозволяє його інтеграцію з класичними Інтернет-системами. Для захисту CoAP на транспортному рівні використовується **DTLS**, який забезпечує безпечний обмін через UDP, тоді як **MQTT** застосовує TCP разом із **SSL/TLS** для захисту даних під час публікації та підписки на повідомлення.

На мережевому рівні безпеку забезпечує **IPsec**, який дозволяє захищений транзит між вузлами за допомогою IPv6, а **6LoWPAN** стискає IP-заголовки, оптимізуючи трафік для обмежених мереж. На фізичному рівні широко використовується стандарт **IEEE 802.15.4**, який шифрує дані в сенсорних мережах за допомогою AES-CCM*, тоді як **Bluetooth Low Energy** (BLE) дозволяє енергоефективний і безпечний обмін із можливістю додаткового захисту через білі списки приватних адрес [6,7].

Для організації доступу до ресурсів в IoT застосовується **OAuth 2.0,** який розділяє ролі клієнтів і власників ресурсів, забезпечуючи надійну авторизацію.

Кожен рівень стека безпеки Інтернету речей (IoT) незалежний і забезпечує власні механізми захисту. Наприклад, стандарт **IEEE 802.15.4** застосовує блочне шифрування AES-CCM для захисту даних; це варіант алгоритму AES-CCM, який додає можливість використання лише функцій шифрування, з фіксованим розміром ключа 128 біт і блоку відкритого тексту. На мережевому рівні безпека ґрунтується на IPv6, де IP-безпека (IPSec) виступає основним механізмом для захищеного з'єднання з Інтернетом. Безпека на транспортному рівні залежить від протоколу на прикладному рівні: якщо використовується **CoAP**, то транспортний рівень — це **UDP** з безпекою **DTLS**; якщо ж розгорнуто **MQTT**, то задіяний **TCP** з **SSL/TLS** для захисту.

Інтернет речей є однією з найактуальніших сфер досліджень, адже IoT — це взаємодія між численними пристроями, речами й об'єктами. У такій системі захист і

конфіденційність даних стають ключовими питаннями, особливо при передачі чутливої інформації через IoT-мережі для обробки та зберігання в хмарі. У даній роботі представлено огляд поточних технологій і протоколів безпеки для IoT, включаючи механізми захисту конфіденційності. У майбутньому планується створити полегшену схему автентифікації, що дозволить ефективно захистити пристрої IoT, ураховуючи їх обмежені можливості.

Перелік посилань

1. Ахметов, Д. А. Безпека IoT: сучасні виклики та рішення. / Д. А. Ахметов, І. М. Лисенко – Київ: Наукова думка, 2021. – 264 с.
2. Головко, П. С. Протоколи для Інтернету речей: особливості та реалізація. / П. С. Головко – Харків: ХНУРЕ, 2022. – 198 с.
3. Руденко, В. В. IoT та кібербезпека: захист мережевих пристроїв. / В. В. Руденко, Н. М. Мороз – Львів: Львівська політехніка, 2023. – 312 с.
4. Литвиненко, О. Ю. Моделі безпеки для IoT-платформ. / О. Ю. Литвиненко – Одеса: Одеський національний університет, 2020. – 157 с.
5. Сіренко, М. Д. IoT-мережі та їх захист: посібник. / М. Д. Сіренко, А. С. Черненко – Дніпро: Дніпропетровський університет, 2021. – 288 с.
6. Петрова, Н. С. Механізми захисту даних в IoT: аналіз і розробка. / Н. С. Петрова – Київ: КПІ ім. Ігоря Сікорського, 2022. – 204 с.
7. Іваненко, Т. В. IoT в промисловості: концепції та проблеми безпеки. / Т. В. Іваненко – Харків: ХНУРЕ, 2023. – 325 с.
8. Карпенко, Л. А. Протоколи безпеки для IoT: огляд і застосування. / Л. А. Карпенко, І. Г. Смирнов – Вінниця: ВНТУ, 2020. – 152 с.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Савича Ніколи Властімировича
ПІБ здобувача вищої освіти

Студента ФІТ, 2 курсу, групи КБЗІм-23-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а) та надаю свою згоду на обробку й збереження університетом моєї роботи в інституційному репозитарії Хмельницького національного університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-обчислювального комплексу StrikePlagiarism та/або програмнотехнічного засобу Anti-Plagiarism) і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення текстових збігів в роботах.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

11.12.2024р.
дата

підпис

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Нікола Савич

Співавтор:

Назва: Метод виявлення атак типу Man-in-the-Middle у безпроводових мережах

Експерт: Микола Стецюк

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:8.7%

Коефіцієнт подібності 2:1.2%

Мікропробіли: 0

Заміна букв: 1

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2024-12-17 10:04:55.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2024-12-17 Старший викладач Сергій Мостовий

Дата 12.17.24 Сергій М. експерт

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 10%**

	Документ		Сумарний збіг по Базі Даних	
ID: 160418 Назва: Метод виявлення атак типу Man-in-the Middle у безпроводних мережах Додано в БД: 2024-12-17 Автора: Савич Нікола Керівники: Стецюк М.В. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	119312	974	1688 (1%)	21 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Метод виявлення атак типу Man-in-the-Middle у безпроводових мережах

Автор: Савич Нікола Властимірович

Спеціальність: 125 – Кібербезпека та захист інформації

Освітня програма:Кібербезпека та захист інформації

Науковий керівник: професор.техн.наук, доцент Касянчук Михайло Миколайович

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 91.3%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 99.9%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Виявлені модифікації стосуються математичних формул і не є порушенням академічної доброчесності.

Керівник роботи _____ Михайло КАСЯНЧУК

Гарант ОП _____ Віра ТІТОВА

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студент Савич Нікола Властімірович

Тема Метод виявлення атак типу Man-in-the Middle у безпроводних мережах

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека та захист інформації

Обсяг кваліфікаційної роботи освітнього ступеня «магістр»:

кількість листів креслень - ; кількість сторінок записки 78

1. Кваліфікаційна робота спрямована на виявлення атак типу Man-in-the Middle у безпроводних мережах. Здійснено глибокий аналіз існуючих методів і моделей, запропоновано новий підхід виявлення атак типу Man-in-the Middle у безпроводних мережах

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота відповідає поставленому завданню як в теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У роботі використано сучасні методи та досягнення в області атак типу Man-in-the Middle у безпроводних мережах У першому розділі було вияснено, що атаки MITM – це старі, але дуже потужні атаки. Другий розділ присвячено методу виявлення та визначення місцезнаходження зловмисника MITM у бездротових мережах шляхом обчислення часу проходження сигналу туди й назад (RTT) та обчислення потужності отриманого сигналу (RSS) від точки доступу, якщо є зловмисник, ці значення вищі за них і більші, ніж відсутність зловмисника (більший час затримки). У наступних розділах реалізовано метод виявлення виявлення атак типу Man-in-the Middle. Проведено дослідження атак типу Man-in-the Middle у безпроводних мережах.

4. Позитивні сторони роботи Позитивні сторони проекту Робота добре структурована, чітко висвітлені всі етапи дослідження. Використані сучасні інструменти та підходи, що свідчить про якість проведеного дослідження..

5. Негативні сторони роботи Відсутність належної уваги до вразливостей, які можуть виникати в динамічних мережевих умовах, що ускладнює універсальне застосування запропонованого методу. Залежність результатів від стабільності швидкості зв'язку та статичності кінцевих точок, що обмежує його ефективність у мобільних середовищах або в умовах із змінними мережевими параметрами

6. Оцінка графічного оформлення та пояснювальної записки роботи В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал дипломної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та наскрізно пов'язаний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Презентаційний та ілюстративний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження _____

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «задовільно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) _____
Мартинюк Валерій Володимирович
завідувач кафедри АКІТР, доктор технічних наук, професор

«17» грудня 2024. _____ (підпис)