КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.26.684
УДК 004.62

Партика Ольга Олександрівна
к.ф.-м.н., доцент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0000-0002-3086-3160
olha.o.mykhailova@lpnu.ua

Фіголь Богдан Михайлович
студент кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0009-0004-8306-7303
bohdan.fihol.mkbui.2024@lpnu.ua

Наконечний Тарас Ігорович
аспірант кафедри захисту інформації
Національний Університет «Львівська Політехніка», Львів, Україна
ORCID ID: 0009-0003-4487-9424
taras.i.nakonechnyi@lpnu.ua

ІНТЕГРОВАНИЙ ПІДХІД ДО ВИЯВЛЕННЯ ЗАГРОЗ У BLUETOOTH-ПРОТОКОЛІ ЗА ДОПОМОГОЮ WIRESHARK ТА SPLUNK SIEM

Анотація. У сучасному світі протокол Bluetooth є однією з найпоширеніших технологій бездротового зв'язку, яка використовується для передачі даних між різними пристроями, забезпечуючи їхню мобільність та функціональність. Незважаючи на численні переваги, Bluetooth-протокол залишається вразливим до кіберзагроз, таких як DoS-атаки, спуфінг і передача шкідливих файлів. Ці загрози створюють ризики для конфіденційності, цілісності та доступності даних, а також можуть спричинити збої у роботі пристроїв, що особливо небезпечно в критичних системах, таких як медичне обладнання чи IoT-інфраструктура. Дана стаття присвячена інтегрованому підходу до моніторингу безпеки Bluetooth, який об'єднує можливості Wireshark та Splunk SIEM. Платформу атакуючого побудовано на базі операційної системи Kali Linux, відомої своїми широкими можливостями для реалізації тестів на проникнення та моделювання атак, тоді як платформа жертви функціонувала на Windows 11 — сучасній операційній системі, що широко використовується в різних середовищах. Основними типами атак, що аналізувалися, є DoS-атаки, які викликають відмову в обслуговуванні через перевантаження системи; атаки спуфінгу, які дозволяють зловмисникам маскувати свої пристрої під легітимні; та передача шкідливих файлів, що може спричинити впровадження шкідливого коду. Для кожного типу атак були розроблені та налаштовані відповідні кореляційні правила в Splunk SIEM, що дозволило автоматизувати процес виявлення підозрілих дій. Wireshark використовувався для глибокого аналізу Bluetooth-трафіку, а Splunk забезпечував оперативне сповіщення про аномалії, дозволяючи швидко реагувати на потенційні загрози. Результати експерименту підтверджують ефективність запропонованого підходу. Наприклад, у разі DoS-атак було виявлено значне перевищення кількості пакетів протоколу L2CAP, що дозволило своєчасно визначити джерело загрози. Для атак спуфінгу було використано правила ідентифікації незвичних MAC-адрес, а для передачі шкідливих файлів — фільтрацію даних за певними критеріями, такими як тип файлу чи відправник.

Ключові слова: Bluetooth; DoS-атака; спуфінг; шкідливі файли; Wireshark; Splunk SIEM; виявлення загроз.

ВСТУП

Сучасні технології бездротового зв'язку, серед яких Bluetooth займає важливе місце, активно використовуються для швидкого та зручного обміну даними між пристроями. Bluetooth забезпечує легкість інтеграції, низьке енергоспоживання та зручність у використанні на коротких відстанях, що робить його невід'ємною частиною таких пристроїв, як мобільні телефони, розумні годинники, ноутбуки та інші периферійні засоби. Крім того, Bluetooth стає ключовою технологією для інтернету речей (IoT) та багатьох промислових систем, де він сприяє автоматизації та зручному управлінню пристроями.

Постановка проблеми. Поряд із численними перевагами, Bluetooth-протокол має низку серйозних вразливостей, що робить його привабливою ціллю для кіберзлочинців. Серед найпоширеніших загроз є атаки відмови в обслуговуванні (DoS), спуфінг та передача шкідливих файлів, які становлять ризик для конфіденційності та цілісності даних, що передаються. Атаки типу DoS можуть призвести до перевантаження пристроїв, що знижує їх продуктивність або навіть повністю виводить з ладу. Спуфінг дозволяє зловмисникам маскувати свої пристрої під легітимні, що може призводити до несанкціонованого доступу до конфіденційної інформації користувачів. Крім того, Bluetooth часто використовується для передачі шкідливих файлів, що дозволяє зловмисникам впроваджувати шкідливе програмне забезпечення на пристрої жертв.

Забезпечення надійного захисту від таких загроз є актуальною проблемою, що потребує ефективних методів моніторингу та аналізу трафіку. Інтеграція таких інструментів, як Wireshark і Splunk SIEM, дозволяє детально аналізувати мережевий трафік і оперативно виявляти підозрілу активність у реальному часі. Wireshark забезпечує глибокий аналіз пакетів даних, а Splunk SIEM автоматизує процес моніторингу, генерує кореляційні правила та дозволяє створювати сповіщення про загрози, забезпечуючи своєчасне реагування на атаки.

Таким чином, ця стаття присвячена дослідженню ефективності виявлення та запобігання атакам на Bluetooth-протокол за допомогою Wireshark та Splunk SIEM. Експериментальна частина дослідження зосереджена на трьох основних типах атак: DoS, спуфінгу та передачі шкідливих файлів, що дозволяє проаналізувати методи захисту та моніторингу для забезпечення безпеки Bluetooth-комунікацій.

Аналіз останніх досліджень і публікацій. Bluetooth-протокол, який активно використовується для забезпечення бездротового зв'язку між пристроями, привертає все більше уваги дослідників через вразливості до різних видів атак. Дослідження [1] підкреслюють небезпеку атак типу відмови в обслуговуванні (DoS), які можуть серйозно впливати на роботу пристроїв з обмеженими ресурсами, особливо в середовищах Інтернету речей (IoT). У роботі [2] вивчалися спуфінг-атаки, під час яких зловмисники маскують свої пристрої під легітимні для отримання несанкціонованого доступу до даних, а також були запропоновані методи удосконалення аутентифікації для захисту від таких атак.

Дослідники [3] проаналізували передачу шкідливих файлів через Bluetooth, наголошуючи, що зловмисники можуть використовувати цей канал для доставки шкідливого ПЗ на пристрої жертв. Вони рекомендують впроваджувати контент-фільтри та підвищувати контроль над передаваними файлами для запобігання подібним атакам. У дослідженнях [4] було підтверджено ефективність Wireshark у виявленні підозрілої активності у Bluetooth-мережах, зокрема для виявлення DoS-атак та спуфінгу, завдяки здатності детально аналізувати пакети даних і попереджати про можливі загрози.

Значний інтерес представляє застосування Splunk SIEM, який дозволяє обробляти та аналізувати події безпеки в реальному часі. Дослідники [8] показали, що використання Splunk для кореляції даних може значно знизити рівень помилкових позитивних сигналів та покращити ефективність реагування на загрози. Додатково, у [9] вказується на здатність Splunk інтегрувати різні джерела даних та автоматизувати виявлення аномалій, що дозволяє операторам швидко виявляти і реагувати на інциденти безпеки.

Дослідження [5] охоплює основні питання безпеки Bluetooth, підкреслюючи потребу у вдосконаленні протоколу для протидії сучасним загрозам. Інші дослідники також акцентують увагу на вразливостях Bluetooth, зокрема на можливості зловмисників перехоплювати дані або змінювати пакети, використовуючи недоліки у безпекових механізмах [6], [7].

У роботі [11] розглядається вплив оновлень протоколу Bluetooth на рівень безпеки, зокрема щодо забезпечення захисту від спуфінгу та перехоплення даних. Аналогічні дослідження в галузі покращення криптографічних алгоритмів для Bluetooth виконані у [19], де рекомендується застосування надійних механізмів шифрування для протидії атакам на конфіденційність.

Таким чином, аналіз сучасних досліджень підтверджує необхідність застосування інтегрованих рішень для моніторингу та захисту Bluetooth-з’єднань. Використання інструментів Wireshark і Splunk SIEM є перспективним напрямом, оскільки вони забезпечують комплексний моніторинг та можливість раннього виявлення загроз, підвищуючи надійність і безпеку пристроїв Bluetooth.

Метою статті є дослідження ефективності інтеграції інструментів Wireshark та Splunk SIEM для моніторингу безпеки Bluetooth-протоколу та виявлення типових атак. У рамках цього дослідження акцент робиться на аналізі трьох основних векторів загроз — DoS-атаки, спуфінгу та передачі шкідливих файлів, які є найпоширенішими методами компрометації Bluetooth-з’єднань. Автори даного дослідження мають на меті продемонструвати, як поєднання Wireshark для глибокого аналізу трафіку та Splunk SIEM для автоматизації виявлення загроз дозволяє забезпечити своєчасне реагування на аномальну активність і підвищити загальний рівень захисту Bluetooth-пристроїв.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Налаштування середовища для дослідження

Для проведення дослідження було налаштовано середовище, яке включає платформу для атакуючого та платформу для жертви, а також інструменти для моніторингу та виявлення підозрілої активності. На стороні атакуючого використовується операційна система Kali Linux, яка служить базою для реалізації атак на Bluetooth-протокол. Сторона жертви представлена операційною системою Windows 11, до якої підключені бездротові навушники. Для моніторингу трафіку Bluetooth було інтегровано аналізатор трафіку Wireshark та систему моніторингу Splunk SIEM, налаштовані для безперервного збору даних та автоматичного виявлення аномальної активності.

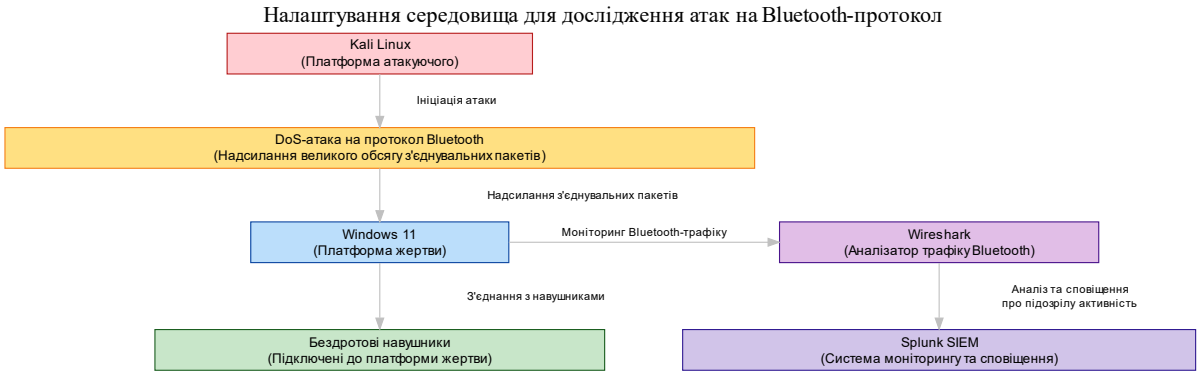

Рис. 1. Схема експериментального середовища для проведення атак на Bluetooth-протокол

Схема на рис. 1 ілюструє взаємозв'язок між компонентами експериментального середовища. Kali Linux (платформа атакуючого) виконує DoS-атаку шляхом надсилання великого обсягу з'єднувальних пакетів до Windows 11 (платформа жертви), до якої підключені бездротові навушники. Wireshark, розміщений на стороні моніторингу, здійснює аналіз трафіку, а Splunk SIEM генерує сповіщення про підозрілу активність у реальному часі, що дозволяє оперативно виявляти та реагувати на потенційні загрози.

Таким чином, налаштування середовища забезпечує повноцінне тестування можливостей Wireshark і Splunk SIEM у виявленні DoS-атак, спуфінгу та передачі шкідливих файлів у Bluetooth-мережах.

Налаштування та сканування адаптера. На першому етапі експерименту виконується налаштування Bluetooth-адаптера на платформі атакуючого, а також сканування для ідентифікації MAC-адрес та назв доступних цільових пристроїв. Це необхідно для визначення точного розташування та ідентифікації цілі, на яку буде спрямовано атаку. Налаштування адаптера здійснюється за допомогою наступної команди:

--hiconfig. Після виконання цієї команди система отримує інформацію про всі доступні Bluetooth-пристрої в радіусі дії атакуючого, включаючи MAC-адреси, що є ключовими для здійснення подальших атак.

Ініціювання DoS-атаки. Після того як ідентифіковано цільовий пристрій за його MAC-адресою, здійснюється ініціювання DoS-атаки. Цей тип атаки спрямований на перевантаження Bluetooth-з'єднання жертви шляхом надсилання великого обсягу з'єднувальних пакетів, що призводить до відмови в обслуговуванні (Denial of Service). Для реалізації атаки використовується спеціально підготовлений Python-скрипт, що надсилає з'єднувальні пакети до цільового пристрою. Команда для запуску скрипта може мати такий вигляд: ***./dos_attack_script.sh 10:63:C8:53:17:D2 512.***

У даній команді вказуються MAC-адреса цільового пристрою (наприклад, 10:63:C8:53:17:D2) і максимальний розмір пакета (в даному випадку — 512 байт), який підтримує протокол Bluetooth. Це забезпечує ефективне перевантаження з'єднання, що є основною метою DoS-атаки.

Аналіз результатів атаки. Успішне завершення DoS-атаки підтверджується, коли цільовий пристрій (жертва) перестає відповідати на запити. Це вказує на те, що пристрій було перевантажено до такої міри, що його обчислювальні ресурси виявилися нездатними обробляти нові вхідні запити, що, зрештою, призводить до відмови в обслуговуванні. Тобто, пристрій жертви фактично «паралізується» і стає недоступним

як для користувача, так і для інших підключених пристроїв. Такий ефект атаки проявляється у вигляді значного зниження продуктивності пристрою, затримки у виконанні команд, або повної неможливості виконувати навіть базові функції. Наприклад, Bluetooth-з'єднання, яке постійно обробляє великий обсяг з'єднувальних пакетів, не встигає забезпечити обробку нових з'єднань або комунікацій, що стає причиною його недоступності. У деяких випадках, пристрій може навіть припинити реагувати на будь-які команди або вимагати перезавантаження для відновлення функціональності. Цей результат є індикатором досягнення мети DoS-атаки, оскільки основною метою зловмисника було створення умов, за яких жертва не зможе користуватися своїм пристроєм або підключатися до інших Bluetooth-пристроїв. Наслідки такої атаки можуть бути особливо шкідливими у випадках, коли пристрій використовується для критичних завдань або має важливі підключення, наприклад, з медичним обладнанням або інфраструктурою Інтернету речей (IoT).

Атака спуфінгу на протокол Bluetooth. Атака спуфінгу на Bluetooth є одним із поширених методів обману, що дозволяє зловмиснику замаскувати свій пристрій під легітимний пристрій жертви, таким чином отримуючи доступ до її мережі або даних. Це досягається шляхом маніпулювання інформацією, яку пристрої використовують для аутентифікації один одного. Такий підхід дозволяє зловмиснику створити ілюзію легітимності, що дає змогу встановити обманне з'єднання та, за певних умов, отримати доступ до конфіденційної інформації, що передається через Bluetooth-з'єднання.

На схемі (рис. 2) відображено покроковий процес реалізації атаки спуфінгу на Bluetooth, що включає кілька важливих етапів.

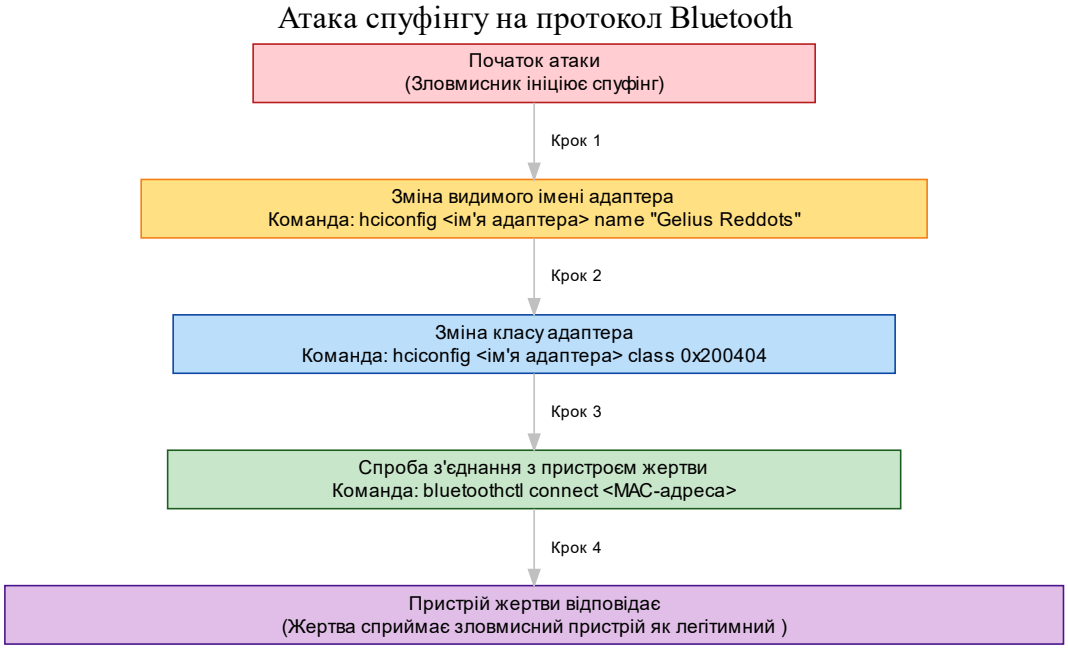

Рис. 2. Атака спуфінгу на протокол Bluetooth

Першим кроком у здійсненні атаки є зміна видимого імені Bluetooth-адаптера зловмисника. Зловмисник змінює назву свого пристрою на ту, що відповідає імені пристрою жертви, наприклад, бездротових навушників жертви, як-от «Gelius Reddots». Це допомагає обманути жертву, створюючи видимість того, що це є легітимний пристрій.

Після зміни імені адаптера зловмисник переходить до наступного кроку, який полягає у зміні класу Bluetooth-адаптера. Клас пристрою визначає його тип та функціональні можливості, і, змінивши клас свого адаптера на клас пристрою жертви, зловмисник може ще більше наблизити характеристики свого пристрою до легітимного. У цьому випадку зловмисник змінює клас свого адаптера на клас навушників, що робить спуфінг більш переконливим і підвищує ймовірність успішного обманного з'єднання.

Останній етап атаки передбачає спробу підключення зловмисника до пристрою жертви. Завдяки попередньому маскуванню під легітимний пристрій жертви, атакуючий пристрій стає більш переконливим для жертви. Це з'єднання може викликати у жертви враження, що її оригінальний пристрій автоматично перепідключився, що знижує підозри та сприяє успішному встановленню зв'язку.

Успішне здійснення цих кроків дозволяє зловмиснику переконати жертву в тому, що він є легітимним пристроєм. Це створює передумови для несанкціонованого доступу до даних жертви або для встановлення подальшого контролю над її пристроєм. Такі атаки є особливо небезпечними, оскільки дозволяють зловмисникам залишатися непоміченими та отримувати доступ до важливої інформації.

Атака спуфінгу може завершитися передачею шкідливого файлу на пристрій жертви без її відома, що дозволяє зловмиснику впровадити шкідливий код у систему жертви. Це стає можливим після успішного маскування пристрою зловмисника під легітимний пристрій жертви та встановлення з'єднання. Передача шкідливого файлу може бути здійснена через Bluetooth-протокол, використовуючи інструменти для відправки файлів без попереднього підтвердження з боку отримувача.

У цьому випадку зловмисник використовує утиліту BlueZ Tools, яка дозволяє надсилати файли на інші пристрої Bluetooth. Команда bluetooth-sendto дає змогу надіслати шкідливий файл на цільовий пристрій, вказавши MAC-адресу жертви та шлях до файлу, що містить шкідливий код. Наприклад: ***bluetooth-sendto --device=<MAC-адреса>*** <шлях_до_файлу>. Ця команда дозволяє зловмиснику безперешкодно надсилати файл на пристрій жертви, оминаючи будь-яке підтвердження з боку користувача. Як наслідок, шкідливий файл може бути збережений на пристрої жертви та запущений автоматично або вручну, якщо користувач випадково відкриє його. Це може призвести до компрометації даних, встановлення троянів або вірусів, а також до порушення конфіденційності та цілісності системи жертви.

Налаштування системи моніторингу та виявлення атак. Для ефективного моніторингу та виявлення атак на протокол Bluetooth у реальному часі було інтегровано два потужні інструменти: Wireshark і Splunk. Така інтеграція дозволяє отримувати детальний аналіз трафіку Bluetooth і здійснювати автоматичне виявлення підозрілої активності, використовуючи комбінацію аналізу пакетів та кореляційних правил.

Wireshark використовується як основний інструмент для захоплення мережевого трафіку, тоді як Splunk виконує роль системи моніторингу і автоматичного сповіщення про аномальну активність. Вибір Wireshark обумовлений його здатністю фільтрувати та зберігати Bluetooth-пакети, тоді як Splunk SIEM забезпечує централізований аналіз подій безпеки та створення правил для виявлення підозрілих дій. Нижче описано основні кроки налаштування цієї системи моніторингу. На рис. 3 наведено блок-схему процесу налаштування системи моніторингу та виявлення атак, що демонструє покрокову інтеграцію інструментів.

ISSN 2663 - 4023

Рис. 3. Налаштування системи моніторингу та виявлення атак Bluetooth

Захоплення трафіку з використанням Tshark. Перший крок у налаштуванні системи моніторингу Bluetooth-трафіку полягає в організації безперервного запису всіх даних, що передаються через Bluetooth-інтерфейс. Для цього використовується TShark — командний інтерфейс Wireshark, який дозволяє здійснювати захоплення трафіку в режимі реального часу та зберігати його у файл для подальшого аналізу. Команда для запуску TShark виглядає наступним чином: ***tshark -i <інтерфейс> > <шлях_до_файлу>***

Де <інтерфейс> — це ім'я Bluetooth-інтерфейсу, який потрібно моніторити, а <шлях_до_файлу> — це шлях до файлу, куди зберігатиметься зібраний трафік. Такий підхід дозволяє забезпечити постійний запис трафіку у файл, який буде доступний для аналізу та моніторингу. Завдяки безперервному запису трафіку можна отримати повну картину активності Bluetooth, що є важливим для виявлення потенційних загроз.

Налаштування Splunk для моніторингу файлу. Наступний крок — це налаштування Splunk для моніторингу файлу, в якому зберігаються дані, зібрані TShark. Splunk налаштовується таким чином, щоб постійно оновлювати та аналізувати цей файл у реальному часі. Коли нові пакети записуються у файл, Splunk автоматично отримує ці дані для подальшого аналізу.

Після налаштування Splunk на моніторинг файлу з трафіком, інструмент починає аналізувати зібрані дані, застосовуючи кореляційні правила, які були налаштовані для виявлення певних типів атак. Це дозволяє в реальному часі виявляти підозрілу активність, наприклад, надмірну кількість пакетів (що може вказувати на DoS-атаку), спуфінг або передачу шкідливих файлів. Splunk генерує сповіщення про виявлену активність, що дозволяє оперативно реагувати на можливі загрози.

ISSN 2663 - 4023

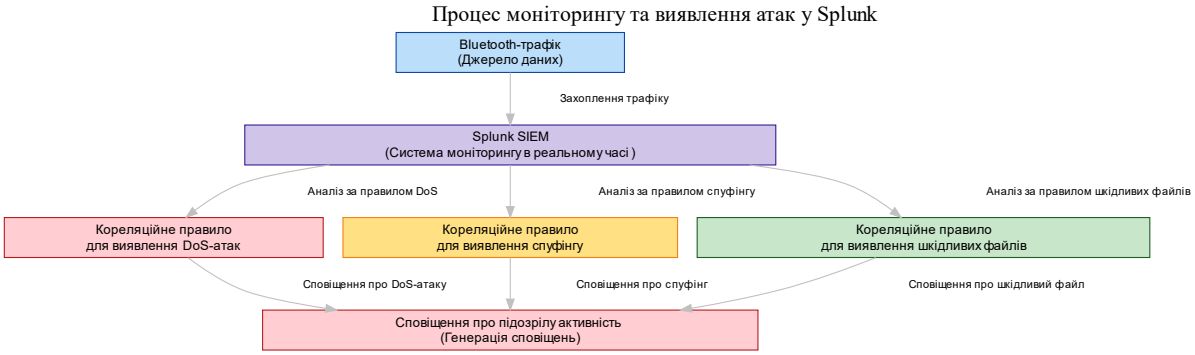

Рис. 4. Налаштування Splunk для моніторингу файлу з Bluetooth-трафіком

Таким чином, інтеграція Wireshark і Splunk створює ефективну систему моніторингу та виявлення атак на Bluetooth-протокол. Постійний моніторинг трафіку, автоматичний аналіз і сповіщення про аномальну активність забезпечують швидке виявлення підозрілих дій і підвищують рівень безпеки мережі Bluetooth.

Кореляційне правило для виявлення DoS-атак. DoS-атака на протокол Bluetooth може проявлятися як аномально висока кількість пакетів, що надсилаються через протокол L2CAP. Для виявлення такої активності застосовується кореляційне правило, яке моніторить кількість пакетів L2CAP, надходження яких перевищує певний поріг. Якщо кількість пакетів від конкретного джерела перевищує допустимий ліміт (наприклад, 1000 пакетів), то система Splunk генерує сповіщення про потенційну DoS-атаку.

index="bluetooth" Protocol=L2CAP
| stats values(extracted_Source) as Source values(Destination) count by Protocol
| where count > 1000

Кореляційне правило для виявлення спуфінгу. Для виявлення спуфінгу застосовується кореляційне правило, яке аналізує підозрілі з'єднання, що надходять з неочікуваних MAC-адрес. Це дозволяє ідентифікувати спроби з'єднання, які не відповідають типовому трафіку мережі, і можуть вказувати на наявність зловмисника, який намагається маскувати свій пристрій під легітимний.

index="bluetooth" Protocol="SMP" AND NOT (extracted_Source IN ("localhost()"))
| table Destination extracted_Source Info

Кореляційне правило для виявлення передачі шкідливих файлів

Передача шкідливих файлів через Bluetooth може становити загрозу для безпеки пристрою жертви. Для виявлення таких спроб у Splunk налаштовано правило, яке відстежує передачу файлів із підозрілими розширеннями (.exe, .ps1, .sh, .app, .bat). Якщо виявлено файл з одним із цих розширень, Splunk генерує сповіщення про потенційну загрозу.

index="bluetooth" Protocol="OBEX" Info IN (*.exe*, *.ps1*, *.sh*, *.app*, *.bat*)
| table Destination extracted_Source Info

Аналіз результатів експерименту. Результати експерименту підтверджують високу ефективність інтеграції Wireshark та Splunk для моніторингу трафіку Bluetooth та виявлення підозрілої активності. Завдяки цій інтеграції вдалося успішно виявити всі три типи атак, включно з DoS-атакою, спуфінгом та передачею шкідливого файлу. Це було досягнуто завдяки правильно налаштованим кореляційним правилам у Splunk, які дозволили автоматично аналізувати вхідний трафік та вчасно виявляти відхилення від норми.

Кожна з атак була ідентифікована за специфічними аномаліями, які були закладені у кореляційні правила. Зокрема, для DoS-атаки використовувалося правило, яке моніторить аномально високу кількість пакетів протоколу L2CAP. Спуфінг виявлявся шляхом моніторингу з'єднань із неочікуваних MAC-адрес, що не відповідали звичному шаблону трафіку. Передача шкідливих файлів визначалась на основі фільтрації певних розширень файлів, які могли вказувати на потенційно шкідливий вміст.

Використання Splunk у режимі реального часу виявилося особливо ефективним, оскільки дозволяло оператору швидко отримувати та аналізувати дані, що є критичним для забезпечення захищеності Bluetooth-комунікацій. Це дає можливість забезпечити швидку реакцію на потенційні загрози, мінімізуючи можливі негативні наслідки від атак. Експеримент показав, що така інтеграція інструментів може стати основою надійної системи моніторингу, що здатна виявляти аномалії з високою точністю.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Результати проведеного дослідження підтверджують ефективність інтеграції Wireshark та Splunk для моніторингу Bluetooth-трафіку і своєчасного виявлення загроз. Розроблені кореляційні правила дозволили успішно ідентифікувати три основні типи атак на Bluetooth-протокол: DoS-атаки, спуфінг та передачу шкідливих файлів. Це доводить, що застосування таких правил може значно підвищити рівень безпеки Bluetooth-з'єднань, автоматизуючи процес виявлення та сповіщення про підозрілу активність.

Інтеграція систем реального часу в Splunk дозволила досягти високої швидкості реагування на інциденти, забезпечуючи операторам можливість оперативно аналізувати підозрілі дії і запобігати потенційним загрозам. Це особливо важливо для захисту пристроїв, що використовують Bluetooth-протокол, зважаючи на їхню вразливість до різних видів атак.

Ефективність виявлення DoS-атак була забезпечена моніторингом аномально високої кількості пакетів протоколу L2CAP, спуфінг виявлявся шляхом аналізу з'єднань з підозрілих MAC-адрес, а передачу шкідливих файлів було визначено за допомогою правил фільтрації підозрілих розширень. Такий підхід показав свою практичну цінність, дозволяючи зосередитися на основних загрозах та забезпечуючи автоматичний аналіз трафіку.

Подальші дослідження можуть бути спрямовані на розширення методів виявлення, включаючи нові типи атак, які можуть з'являтися з розвитком технологій. Розвиток кореляційних правил і застосування машинного навчання для автоматичного виявлення складних аномалій допоможе підвищити адаптивність і надійність системи захисту. Крім того, оптимізація системи моніторингу для обробки великих обсягів трафіку в умовах інтенсивного використання Bluetooth також може бути важливим напрямом подальших досліджень.

Загалом, інтеграція Wireshark та Splunk підтвердила свою дієвість як засобу захисту Bluetooth-мереж від кіберзагроз, що надає можливість для подальшого розвитку систем моніторингу та аналізу безпеки бездротових технологій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ogundokun, A. I., Verma, P., & Dev, K. (2021). Denial-of-service attacks in IoT environments: A systematic review. *IEEE Access, 9,* 9603–9618. https://doi.org/10.1109/ACCESS.2021.9604655
2. Bose, A., & Shrivastava, S. (2022). Bluetooth security vulnerabilities and mitigation techniques. *Advances in Cybersecurity. Springer, Cham*, 118–130. https://doi.org/10.1007/978-3-030-93956-4_7
3. Ullah, M. M., Mehmood, Z., & Iqbal, A. (2023). *Bluetooth attacks: Analysis and mitigation techniques*. arXiv preprint arXiv:2301.03852. https://arxiv.org/abs/2301.03852
4. Martinelli, F., Moriello, G., & Viganò, N. (2020). *On the vulnerability of Bluetooth Low Energy protocol to spoofing attacks.* Purdue University Research. https://www.cs.purdue.edu/news/articles/2020/blesa_ble_vulnerability.html
5. Narayan, N., & Bedi, P. (2020). A survey on security issues in Bluetooth technology. *Wireless Personal Communications, 111(3),* 1643–1664. https://doi.org/10.1007/s11277-019-07079-9
6. Mouheb, D., et al. (2019). Bluetooth security threats and challenges. *Computer Standards & Interfaces, 66,* 103–112. https://doi.org/10.1016/j.csi.2019.103442
7. Perkins, J., & Dunn, B. (2021). Introduction to Bluetooth security and potential attack vectors. *Journal of Information Security and Applications, 62,* 102912. https://doi.org/10.1016/j.jisa.2021.102912
8. Wei, F., et al. (2022). Real-time threat detection in Bluetooth communications using SIEM solutions. *Journal of Network and Computer Applications, 192,* 103150. https://doi.org/10.1016/j.jnca.2022.103150
9. Sahiduzzaman, M., et al. (2021). Application of SIEM in the security monitoring of wireless protocols. *IEEE Transactions on Information Forensics and Security, 16,* 4138–4150. https://doi.org/10.1109/TIFS.2021.3101929
10. Johnson, T., et al. (2020). Comparative study of Wireshark and Splunk for intrusion detection. *Procedia Computer Science, 170,* 645–650. https://doi.org/10.1016/j.procs.2020.03.136
11. Ström, B., et al. (2020). Bluetooth security: The impact of protocol upgrades. *Computer Communications, 154,* 63–70. https://doi.org/10.1016/j.comcom.2020.02.010
12. Lu, R., et al. (2021). Emerging Bluetooth vulnerabilities in IoT devices. *IEEE Internet of Things Journal, 8(10),* 7928–7936. https://doi.org/10.1109/JIOT.2021.3069534
13. Nair, A., & Abraham, S. (2019). Mitigation of Bluetooth MITM attacks in wireless systems. *International Journal of Network Security, 21(4),* 713–722. https://doi.org/10.6633/IJNS.201907_21(4).13
14. Sakamoto, T., et al. (2020). Analysis and classification of Bluetooth DoS attacks using Wireshark. *Security and Communication Networks, 2020*. https://doi.org/10.1155/2020/8581267
15. Lyu, X., et al. (2019). Detection of spoofing and other attacks in Bluetooth networks. *IEEE Transactions on Wireless Communications, 18(12),* 5715–5728. https://doi.org/10.1109/TWC.2019.2947815
16. Yaqoob, I., et al. (2021). IoT security and privacy: A review of Bluetooth vulnerabilities. *Sensors, 21(3),* 753. https://doi.org/10.3390/s21030753
17. Bose, A., et al. (2020). Utilizing SIEM for anomaly detection in Bluetooth communications. *Future Generation Computer Systems, 108,* 727–737. https://doi.org/10.1016/j.future.2020.03.042
18. Gupta, S., & Kumar, S. (2022). Evaluation of Bluetooth-based attacks using network traffic analysis. *International Journal of Communication Networks and Information Security, 14(3),* 291–300.
19. Mayberry, T., et al. (2018). Advances in Bluetooth cryptographic security. *ACM Transactions on Information and System Security (TISSEC), 21(4)*. https://doi.org/10.1145/3281484
20. Raman, S., & Madan, P. (2019). Threats to Bluetooth communications and modern detection mechanisms. *Journal of Computer Virology and Hacking Techniques, 15(3),* 175–188. https://doi.org/10.1007/s11416-019-00332-5.
21. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (26), 2024
ISSN 2663 - 4023

Olha Partyka
Associate professor of the Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-3086-3160
olha.o.mykhailova@lpnu.ua

Bohdan Fihol
Student of the Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0004-8306-7303
bohdan.fihol.mkbui.2024@lpnu.ua

Taras Nakonechnyi
Post-graduate Student of the Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0003-4487-9424
taras.i.nakonechnyi@lpnu.ua

INTEGRATED APPROACH TO DETECTING BLUETOOTH THREATS USING WIRESHARK AND SPLUNK SIEM

Abstract. In the modern world, the Bluetooth protocol is one of the most widespread wireless communication technologies used to transfer data between various devices, ensuring their mobility and functionality. Despite its numerous advantages, the Bluetooth protocol remains vulnerable to cyber threats such as DoS attacks, spoofing, and malicious file transfer. These threats pose risks to data confidentiality, integrity, and availability. They can also lead to device failures and hazards in critical systems such as medical equipment or IoT infrastructure. This article focuses on an integrated approach to Bluetooth security monitoring that combines the capabilities of Wireshark and Splunk SIEM. The attacker's platform is based on the Kali Linux operating system, known for its comprehensive capabilities for implementing penetration tests and attack simulations, while the victim's platform was running Windows 11, a modern operating system widely used in various environments. The main types of attacks analyzed are DoS attacks that cause denial of service due to system overload, spoofing attacks, which allow attackers to disguise their devices as legitimate, and transferring malicious files, which can lead to malicious code. For each type of attack, the corresponding Splunk SIEM correlation rules were developed and configured, which made it possible to automate the process of identifying suspicious activities. Wireshark was used for deep analysis of Bluetooth traffic, and Splunk provided prompt notification of anomalies, allowing a quick response to potential threats. The results of the experiment confirm the effectiveness of the proposed approach. For example, in the case of DoS attacks, a significant excess of L2CAP protocol packets was detected, making it possible to identify the source of the threat promptly. For spoofing attacks, rules for identifying unusual MAC addresses were used, and for the transfer of malicious files, data was filtered by specific criteria, such as file type or sender.

Keywords: Bluetooth; DoS attack; spoofing; malicious files; Wireshark; Splunk SIEM; threat detection.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Ogundokun, A. I., Verma, P., & Dev, K. (2021). Denial-of-service attacks in IoT environments: A systematic review. *IEEE Access, 9*, 9603–9618. https://doi.org/10.1109/ACCESS.2021.9604655
2. Bose, A., & Shrivastava, S. (2022). Bluetooth security vulnerabilities and mitigation techniques. *Advances in Cybersecurity. Springer, Cham*, 118–130. https://doi.org/10.1007/978-3-030-93956-4_7
3. Ullah, M. M., Mehmood, Z., & Iqbal, A. (2023). *Bluetooth attacks: Analysis and mitigation techniques*. arXiv preprint arXiv:2301.03852. https://arxiv.org/abs/2301.03852

4. Martinelli, F., Moriello, G., & Viganò, N. (2020). *On the vulnerability of Bluetooth Low Energy protocol to spoofing attacks.* Purdue University Research. https://www.cs.purdue.edu/news/articles/2020/blesa_ble_vulnerability.html
5. Narayan, N., & Bedi, P. (2020). A survey on security issues in Bluetooth technology. *Wireless Personal Communications, 111(3),* 1643–1664. https://doi.org/10.1007/s11277-019-07079-9
6. Mouheb, D., et al. (2019). Bluetooth security threats and challenges. *Computer Standards & Interfaces, 66,* 103–112. https://doi.org/10.1016/j.csi.2019.103442
7. Perkins, J., & Dunn, B. (2021). Introduction to Bluetooth security and potential attack vectors. *Journal of Information Security and Applications, 62,* 102912. https://doi.org/10.1016/j.jisa.2021.102912
8. Wei, F., et al. (2022). Real-time threat detection in Bluetooth communications using SIEM solutions. *Journal of Network and Computer Applications, 192,* 103150. https://doi.org/10.1016/j.jnca.2022.103150
9. Sahiduzzaman, M., et al. (2021). Application of SIEM in the security monitoring of wireless protocols. *IEEE Transactions on Information Forensics and Security, 16,* 4138–4150. https://doi.org/10.1109/TIFS.2021.3101929
10. Johnson, T., et al. (2020). Comparative study of Wireshark and Splunk for intrusion detection. *Procedia Computer Science, 170,* 645–650. https://doi.org/10.1016/j.procs.2020.03.136
11. Ström, B., et al. (2020). Bluetooth security: The impact of protocol upgrades. *Computer Communications, 154,* 63–70. https://doi.org/10.1016/j.comcom.2020.02.010
12. Lu, R., et al. (2021). Emerging Bluetooth vulnerabilities in IoT devices. *IEEE Internet of Things Journal, 8(10),* 7928–7936. https://doi.org/10.1109/JIOT.2021.3069534
13. Nair, A., & Abraham, S. (2019). Mitigation of Bluetooth MITM attacks in wireless systems. *International Journal of Network Security, 21(4),* 713–722. https://doi.org/10.6633/IJNS.201907_21(4).13
14. Sakamoto, T., et al. (2020). Analysis and classification of Bluetooth DoS attacks using Wireshark. *Security and Communication Networks, 2020*. https://doi.org/10.1155/2020/8581267
15. Lyu, X., et al. (2019). Detection of spoofing and other attacks in Bluetooth networks. *IEEE Transactions on Wireless Communications, 18(12),* 5715–5728. https://doi.org/10.1109/TWC.2019.2947815
16. Yaqoob, I., et al. (2021). IoT security and privacy: A review of Bluetooth vulnerabilities. *Sensors, 21(3),* 753. https://doi.org/10.3390/s21030753
17. Bose, A., et al. (2020). Utilizing SIEM for anomaly detection in Bluetooth communications. *Future Generation Computer Systems, 108,* 727–737. https://doi.org/10.1016/j.future.2020.03.042
18. Gupta, S., & Kumar, S. (2022). Evaluation of Bluetooth-based attacks using network traffic analysis. *International Journal of Communication Networks and Information Security, 14(3),* 291–300.
19. Mayberry, T., et al. (2018). Advances in Bluetooth cryptographic security. *ACM Transactions on Information and System Security (TISSEC), 21(4)*. https://doi.org/10.1145/3281484
20. Raman, S., & Madan, P. (2019). Threats to Bluetooth communications and modern detection mechanisms. *Journal of Computer Virology and Hacking Techniques, 15(3),* 175–188. https://doi.org/10.1007/s11416-019-00332-5.
21. Hulak, H. M., Zhiltsov, O. B., Kyrychok, R. V., Korshun, N. V., & Skladannyi, P. M. (2024). *Information and cyber security of the enterprise.* Textbook. Lviv: Publisher Marchenko T. V.